UNIVERSIDAD DE VALPARAISO
Facultad de Ciencias Económicas y Administrativas
Escuela de Auditoría

PLANIFICACION Y EJECUCION DE UN ENFOQUE DE AUDITORIA, CONSIDERANDO LAS CARACTERISTICAS Y RIESGOS INHERENTES DE LOS SISTEMAS DE INFORMACION COMPUTACIONALES

Memoria para optar al Título de
Contador Auditor

PROFESOR GUIA:
Sr. Manuel Reyes M.

PROFESOR INFORMANTE:
Sr. Héctor Acevedo A.

Máximo Peña Arancibia

1997

UNIVERSIDAD DE VALPARAÍSO

FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS

ESCUELA DE AUDITORÍA

PLANIFICACIÓN Y EJECUCIÓN DE UN ENFOQUE DE AUDITORÍA, CONSIDERANDO LAS CARACTERÍSTICAS Y RIESGOS INHERENTES DE LOS SISTEMAS DE INFORMACIÓN COMPUTACIONALES

MEMORIA PARA OPTAR EL TÍTULO DE CONTADOR AUDITOR

Auditoría Computacional
Computación Aplicada
Procesamiento electrónico de datos
Planificación Estratégica
Control interno

PROFESOR GUIA
SR. MANUEL REYES M.

PROFESOR INFORMANTE
SR. HECTOR ACEVEDO A.

MAXIMO PEÑA
ARANCIBIA

1997

HISTORIA DE LA COMPUTACION

LA COMPUTACION

En la historia de la humanidad, se han producido hitos tan importantes, que han sido capaces de generar un cambio en la evolución del desarrolló y la cultura. Dichos cambios fueron en un momento lentos y en cierta forma lineales, en otros instantes, tuvieron por la relevancia de los descubrimientos un impacto exponencial en el crecimiento y evolución de la humanidad. Uno de estos hitos fue el descubrimiento de la máquina del vapor como fuente de energía, lo que multiplicó el trabajo que podía realizar el hombre. Su impacto fue tan importante que se habló entonces de la Revolución Industrial.

Esta Revolución Industrial transformó la Sociedad Artesanal de esa época, en la cual pocas personas acudían con requerimientos de determinados productos a los Maestros (zapateros, sastres, pintores, etc.), quienes eran las pequeñas unidades productivas de la época. Estos maestros trabajaban en pequeños talleres con unos cuantos aprendices y esperaban los pedidos de quienes tenían poder comprador. Pero la lentitud de la producción y sus elevados costos, no permitían el consumo masivo de dichos productos. Sin embargo, la aparición de la máquina cambió radicalmente este esquema, al multiplicar el poder del músculo humano, multiplicó asimismo la producción, bajó los costos, y contrariamente a lo que se creyó en esa época, la máquina como resultante general, no reemplazo al hombre, por el contrario, fue generadora de fuentes de trabajo. Nació la Sociedad Industrial y la época en que los empresarios esperaban la llegada de clientes muy seleccionados dio paso a empresarios que ofrecen sus productos al consumidor.

Esta Sociedad Industrializada impuso fuertes requerimientos de control en la organización y sus procesos, como asimismo nuevas técnicas de planificación y coordinación de actividades. Se generó la necesidad de formalizar métodos modernos de administración acordes con estas nuevas necesidades ello originó nuevas disciplinas como la Teoría General de Sistemas, la Cibernética y otras que dan gran importancia a la información, considerándola un recurso básico en el caso específico de la gestión de las organizaciones.

El problema ya no es controlar un pequeño volumen de producción y una cantidad de clientes que hasta se podía memorizar, el problema es ahora, la diversidad de artículos, la gran cantidad de bienes producidos, el personal que se requiere, los insumos, etc. Por esto, mantener al día las cuentas corrientes de cada cliente, pagar oportunamente, hacer flujos de caja por concepto de ingresos esperados, conocer saldos, controlar las ventas y otras, no es en absoluto fácil por no decir, en algunos casos, imposible. Nace entonces la inquietud de generar una nueva máquina que reciba como insumo "datos", la procese y "produzca" información elaborada y ordenada según los requerimientos del usuario: Una máquina que

sea ahora la "extensora" de la mente humana. Aparece así el computados cuyo vertiginoso desarrollo dará origen a lo que podemos llamar con propiedad Segunda Revolución, cuyo impacto es apreciable en lo que se ha dado en llamar la Sociedad Informatizada en reemplazo o complemento de la actual Sociedad Industrializada. No significa esto que dejaran de existir las industrias, al contrario, son cada días más necesarias, más complejas, pero paradojalmente, el computador la puede humanizar y perfeccionar.

El computador, podemos definirlo como una máquina electrónica que, apoyada en distintos componentes físicos y mediante el uso de energía, procesa información internamente representa en caracteres 0 y 1 (base binaria), por ejemplo:

El 1 de base decimal es igual a 0001 en base binaria (considerando cuatro posiciones)

El 4 de base decimal es igual a 0100 en base binaria (considerando cuatro posiciones).

El 5 de base decimal es igual a 0101 en base binaria (considerando cuatro posiciones).

El 9 de base decimal es igual a 1001 en base binaria (considerando cuatro posiciones).

etc.

La computación es, en consecuencia, el estudio del computador y su aplicación en diversos tipos de sistemas y de su impacto como máquina procesadora de información.

GENERACIONES DE COMPUTADORES

Debido al gran impacto tecnológico, desde el primer computador propiamente tal, a la fecha la evolución de estas máquinas ha sido vertiginosa; a tal punto, que es dificil predecir el desarrollo futuro de dichos equipos.

A continuación se describen, las características más relevantes de estas generaciones de computadores :

1. Primera Generación (1942-1948)

Esta primera generación se caracterizó por la utilización de tubos de vacío como componentes principales del procesador central (UCP); para almacenar datos, usaban condensadores de capacidad limitada (hasta 1.000 dígitos). Su mantenimiento era dificil, sobre todo por las altas temperaturas que generaban sus componentes (tubos) y por la cantidad de ellos que se quemaban. El costo promedio de procesamiento de cada dígito decimal a ser almacenado era del orden de US$ 10 y podía realizar hasta un máximo de 10.000 operaciones por, segundo. Su único modo de operación era BATCH. Para almacenar datos en forma masiva se utilizaban tarjetas y papel perforado.

2. Segunda Generación (1948-1964)

En esta segunda generación de computadores se incorporan los transistores como componentes e la Unidad Central de Proceso en reemplazo de los tubos de vacío, con lo cual se ganó mayor velocidad de operación mayor confiabilidad, Mejores costos (US$ 1 por dígito almacenado), menor cantidad de calor y mayor capacidad de operación.

Para almacenar datos que pudieran ser procesados a mayor velocidad se ocupan núcleos de ferrita; y para almacenar grandes cantidades de datos se empiezan a utilizar las cintas y los discos magnéticos, lo que también significó que bajaran los costos de almacenamiento. Aumentó el espectro de problemas que se podían resolver y se incorporó definitivamente a los procesos administrativos. Además, al computador se le agregaron dispositivos para entrada de datos y entrega de resultados en distintas formas, a pesar de esto, su modo de procesamiento siguió siendo BATCH.

3. Tercera Generación (1964-1970)

La invención del Circuito Integrado (CI), conocido con el nombre de Chip, marca el comienzo de esta nueva generación.

Un chip es un circuito electrónico miniaturizado que se instala sobre piezas de silicona y que hace el trabajo del transistor. Lo grandioso del invento fue que, así como un

transistor reemplazaba a varios tubos al vacío, un chip reemplazaba miles de transistores. Los computadores se redugeron grandemente de tamaño, y dieron paso a la creación de máquinas más pequeñas, que se conocieron como minis, minicomputadores.

4. Cuarta Generación (1970-1981)

En los años setenta, el proceso de miniaturización tuvo otro gran éxito y se ideó algo así como un superchip, es decir, un chip que estaba formado por otros chips, circuito integrado dentro de otros circuitos integrados. La revolución fue total, y se pasó de los minis a los micro, a los microcomputadores.

En la actualidad, estos circuitos están en todas partes : juegos electrónicos, calculadoras, relojes digitales, equipos de video, discos compactos, tarjetas electrónicas de créditos, y en un sinnúmero de lugares.

Otro gran invento de la época fue el diquete. Desde la segunda generación, los datos podían ser almacenados indefinidamente en cintas electromagnéticas y en discos de metal. La IBM inventó, en los inicios de los setenta, el disco flexible, lo que facilitaba enormemente el almacenamiento de datos.

5. Quinta Generación (1981 hasta la actualidad)

En 1981, los japoneses anunciaron al mundo un plan decenal para desarrollar la quinta generación de computadores. Se esperaba computadores que pudieran entender la voz humana y ser manejados por cualquier persona. Esto hoy en día, es prácticamente, una realidad, aunque es cierto que nos hemos demorado más de diez años previstos.

Otro elemento fundamental era el estudio de inteligencia artificial (IA), esfuerzo para poder imitar, en el computador, el proceso de conocimiento en el ser humano : cómo recibe información, cómo la procesa y cómo la abstrae. Se apuntaba a que el computador tomara decisiones.

En esto parece haber más dudas y esperanza que concreciones. Obviamente, se ha avanzado en ls denominados sistemas expertos, por ejemplo, Estos "aprenden", o mejor, repiten reglas suministradas por un programa respecto de la solución de problemas previamente estudiados por el ser humano. En el caso de Tratamientos médicos, por ejemplo, el computador puede aprender a diagnosticar o a formular según características y síntomas que un examen de sangre y un examen fisico del enfermo presenten. Sus decisiones podrán ser acertadas en la medida en que conozca todas las reglas (es decir, todas las posibilidades de análisis que aria el médico si estuviese examinando él mismo paciente).

Es difícil este campo de la inteligencia artificial y, como decíamos anteriormente, las dudas continúan y se siguen esperando los resultados.

INDICE

Tema *Página*

Tema *Página*

Tema *Página*

INTRODUCCION

La realidad que nos circunda nos muestra cada día con mayor intensidad que el procesamiento electrónico de datos (EDP) ha cubierto un amplio espectro de aplicaciones debido, fundamentalmente, a dos de sus características principales: generación de información contable y rapidez en su elaboración. Cualquier razonamiento con respecto al futuro indica que los ambientes computarizados serán cada día más comunes.

Es evidente que la información utilizada por los entes en general ha variado en las últimas décadas. Del mismo modo lo han hecho las necesidades de generación de esa información y los medios para procesarla.

En la década de los años 1950, en el ambiente de aplicaciones contables la información era en general procesado manualmente, con un alto costo salarial, riesgos en cuanto a su exactitud, poca o nula flexibilidad y, en ciertos casos, con graves defectos en cuanto a su pronta preparación (oportunidad).

Con la evolución de la tecnología aplicada al desarrollo de equipos de computación se produjeron sucesivos progresos en relación con el medio de procesamiento y lenguajes utilizados. Así es como por los años 1960 aparecen los primeros computadoras con un sentido comercial, utilizando básicamente elementos mecánicos y electrónicos precarios (en comparación con las actuales generaciones). Estos primeros sistemas, de dimensiones físicas considerables, representaron un gran avance en cuanto a la generación de información, en relación con los procesos manuales utilizados hasta entonces.

A partir de allí y hasta nuestros días se produjo una incesante evolución de esta tecnología hasta llegar a niveles de agilidad en el procesamiento y capacidad de almacenamiento de información que hacen pensar en un futuro en el cual el uso de la computación será generalizado, aún en aplicaciones domésticas.

Paralelamente a la evolución de los sistemas computarizados se fue observando cada vez en forma más amplia la utilización del EDP en la generación de información contable y de gestión.

Dependerá, obviamente, de la envergadura de la organización y de la magnitud y complejidad de la información que maneje el ente, el hecho de contar con sistemas computarizados más o menos complejos. Lo que no se puede dejar de lado es que el uso del procesamiento electrónico de datos es hoy un medio de generación de información aplicado en la mayoría de las empresas, independientes de su tamaño.

Esto significa que los auditores deben acostumbrarse a realizar revisiones y emitir su opinión profesional sobre datos e información que surgen de sistemas computarizados. Por tal motivo es importante que se conozca el tipo de implicancias y efectos que sobre la tarea profesional causa el procesamiento electrónico de datos.

Por lo anterior se desprende que en toda auditoria en la actualidad debemos abarcar los siguientes puntos:

- Planificar y ejecutar un enfoque de auditoria que responda a los riesgos presentes en los Sistemas de Información Computarizados (CIS).
- Comprender las modernas tecnología CIS y concentrarse en los aspectos que tanto desde una perspectiva de auditoría como de servicio al cliente, puedan tener importancia para la auditoria.

Cada vez es más frecuente encontramos con una mezcla de diversas tecnologías de sistemas de información en nuestras auditorías. Algunos clientes utilizan sistemas tradicionales basados en lotes. Los sistemas de información modernos generalmente incluyen ingreso interactivo de datos y procesamiento de actualización inmediata y pueden incorporar tecnologías de telecomunicaciones y de base de datos. Los mini y microcomputadores son frecuentemente utilizados como parte integral de redes de computación más extensas y también como sistemas independientes. Los ambientes típicos están caracterizados por una mezcla de tecnologías; un ambiente que ha evolucionado a medida que nuestros clientes han adoptado e integrado una tecnología cambiante a lo largo de los años.

Los Sistemas de Aplicación son un Conjunto de Programas agrupados en módulos hasta conformar los Sistemas que al actuar juntos, entregan valor agregado que facilita la eficiencia y eficacia en las operaciones.

En la presente memoria no pretende cubrir todos los aspectos relacionados con los Sistemas de Información Computarizados sino solo aquellos relacionados con Sistemas de Aplicación de procesos que tengan implicancia contable. Del mismo modo, no se tocaran temas como Comunicaciones, Periféricos, y cualquier otro tema que se aleje del ámbito de la Auditoria de Estados Financieros y que más bien corresponden a Auditoria Especial al área de Sistemas Computarizados.

Como estructura se determino esquematizar el desarrollo de esta memoria comenzando por las implicancias en la Planificación de la Auditoria de Estados Financiero que se generan por el procesamiento electrónico de datos, destacando el análisis de los riesgos típicos a todos los ambientes computarizados donde existe procesamiento electrónico de datas. Hecha el alcance respecto a la Planificación de la Auditoria de Estados Financieros, se presenta el tema C.A.T. (Técnicas de Auditoria COMPUTACIONAL) sus Técnicas y Herramientas que se ocupan en la ejecución de C.A.T como parte del desarrollo de la Auditoria de Estados Financieros. Por ultimo, se desarrolla el tema de Software como puntal en el análisis de los Sistemas Aplicativos para poder cubrir adecuadamente en el

aspecto de seguridad tanto de los datos como de los sistemas relacionados con los mismos, tanto en plataforma mono usuario y multiusuario.

El objetivo central que motivo el desarrollar e investigar acerca del tema "PLANIFICACIÓN Y EJECUCIÓN DE UN ENFOQUE DE AUDITORÍA, CONSIDERANDO LAS CARACTERÍSTICAS Y RIESGOS INHERENTES DE LOS SISTEMAS DE INFORMACIÓN COMPUTACIONALES" es poder dar a conocer a toda la comunidad universitaria la importancia trascendental que el buen dominio de este tema tiene en la calidad profesional del auditor dado la clara automatización de los procesos que se aprecia hoy en día y que a futuro tendería hacia la automatización total y es para ese futuro que los auditores deben estar preparados. Del mismo modo, la Auditoria de Estados Financieros debe retroalimentarse de este nuevo escenario para poder cubrir con su trabajo todos los riesgos relacionados con la generación de Estados Financieros a través de procesamiento electrónico de datos y son estos datos que deben ser validados para poder opinar en forma veraz acerca de la razonabiliad de la información contenida en los Estados Financieros.

Terminología

La "jerga" de computación puede ser confusa, especialmente cuando los términos no son aplicados uniformemente. Para reducir esta confusión, se han incluido a continuación las explicaciones de ciertos términos utilizados (o evitados) a lo largo de esta memoria. Además se han incluido otros términos de computación en el Glosario.

- Computadores centrales (mainframe), mini y microcomputadores

Las distinciones entre mainframe, mini y microcomputador cada vez son menos precisas. Por ejemplo, con algunos de los microcomputadores actuales se puede procesar mayor cantidad de datos en menos tiempo que en algunos mainframe de diez años atrás. Por esta razón, estos términos fueron utilizados muy poco frecuentemente y solamente cuando ha sido necesario ilustrar un punto que no pudo ser explicado de otro modo.

- Procesamiento centralizado, descentralizado y distribuido

  Para los fines de esta memoria estos términos han sido definidos de la siguiente manera:

  - *Centralizado*. Un sistema en el cual todo el procesamiento se realiza en una misma instalación.
  - *Descentralizado*. Un sistema integrado por dos (o más) equipos de procesamiento de información operados por la misma organización pero con comunicaciones limitadas o nulas entre ellos.
  - *Procesamiento distribuido de datos*. Un sistema compuesto por un conjunto coordinado de recursos de procesamiento de información implantados en uno o más centros relativamente independientes tales como centros de cómputos, terminales inteligentes, etc. interconectados por facilidades de comunicación de datos. Se caracterizan por utilizar información compartida y por la interconexión de los sistemas de aplicación entre los centros de procesamiento.

- Ingreso de datos, oportunidad del procesamiento y acceso a los datos

  Se utilizan los siguientes términos:

  - *Interactivo o no interactivo*, de acuerdo con la forma de ingreso de los datos.
  - *Actualización inmediata o diferida*, de acuerdo con el momento del procesamiento.
  - *Acceso directo o secuencial*, de acuerdo con el método de acceso a los datos.

Cuando el ingreso de datos es interactivo, se utiliza un programa de aplicación para editar (por ej., confirmar que no se omite ninguna información importante) y validar (por ej., confirmar que el número de cuenta es una información válida), a medida que la información es ingresada. Después de editar y validar cada transacción, el procesamiento de la operación puede ser completado en forma inmediata o diferida. En el modo no interactivo, la edición y validación de los datos no son realizadas en el momento de su ingreso y el procesamiento no se completa en forma inmediata.

La oportunidad del procesamiento de datos se refiere al instante en que las transacciones son procesadas para la actualización de los archivos de datos. Como lo indican los términos, la actualización inmediata se refiere al procesamiento y actualización de archivos a medida que cada transacción es ingresada. La actualización diferida es a veces denominada procesamiento por lotes porque generalmente las transacciones son agrupadas en lotes para su procesamiento. Las transacciones pueden ser agrupadas manualmente antes del ingreso de datos o mediante programas que las registran en un archivo temporario de transacciones antes de la actualización del archivo de datos.

Acceso secuencial significa que el computador debe leer todos los registros anteriores hasta que encuentre el deseado. El acceso directo permite la lectura de cualquier registro específico sin necesidad de leer los demás.

En esta memoria, el término "cliente" se utiliza para referirnos a la organización auditada. En la práctica, podemos ser empleados por un tercero, por ejemplo, un inversor u otro suministrador de capital.

CAPITULO I
DESARROLLO DEL PLAN DE AUDITORIA

I. Consideraciones Generales

1. Características Específicas de los Sistemas Computadorizados

El hecho de que nuestros clientes utilicen sistemas computadorizados no afecta nuestros objetivos de auditoría globales o por componente. Sin embargo, existen ciertas características específicas de dichos sistemas que pueden afectar el tipo de evidencia de auditoría que obtenemos. Dichas características son las siguientes:

- *Procesamiento uniforme de las transacciones.* El procesamiento computadorizado somete uniformemente todas las transacciones similares a las mismas instrucciones de procesamiento; la posibilidad de errores al azar, un problema de control que se presenta en ambientes manuales, queda substancialmente reducida. No obstante, aún cabe la posibilidad de que los datos ingresados al computador para su procesamiento puedan incluir errores o ser incompletos.

- *Posibilidad de errores e irregularidades no detectadas.* La posibilidad de que ciertos individuos, incluyendo a aquéllos que realizan procedimientos de control, accedan a los datos sin autorización, o los alteren sin dejar evidencias visibles, puede ser mayor en los sistemas computadorizados que en los sistemas manuales. Ello se debe a que la información es almacenada en forma electrónica, con una menor participación del hombre en el procesamiento, reduciéndose por consiguiente la oportunidad de detectar manualmente los accesos no autorizados. Por lo general, los recursos de información tienden a estar concentrados en los ambientes CIS.

- *Potencial para una mayor supervisión gerencial.* Los sistemas computadorizados ofrecen a la gerencia una amplia variedad de herramientas analíticas que pueden ser utilizadas para revisar y supervisar las operaciones de la organización,

- *Rastro de las transacciones.* El diseño de algunos CIS da como resultado que el rastro de las transacciones, que puede ser utilizado para propósitos de auditoría, sólo es conservado por poco tiempo o en forma electrónica.

CAPITULO I
DESARROLLO DEL PLAN DE AUDITORIA

I. Consideraciones Generales

1. Características Específicas de los Sistemas Computadorizados

El hecho de que nuestros clientes utilicen sistemas computadorizados no afecta nuestros objetivos de auditoría globales o por componente. Sin embargo, existen ciertas características específicas de dichos sistemas que pueden afectar el tipo de evidencia de auditoría que obtenemos. Dichas características son las siguientes:

- *Procesamiento uniforme de las transacciones.* El procesamiento computadorizado somete uniformemente todas las transacciones similares a las mismas instrucciones de procesamiento; la posibilidad de errores al azar, un problema de control que se presenta en ambientes manuales, queda substancialmente reducida. No obstante, aún cabe la posibilidad de que los datos ingresados al computador para su procesamiento puedan incluir errores o ser incompletos.

- *Posibilidad de errores e irregularidades no detectadas.* La posibilidad de que ciertos individuos, incluyendo a aquéllos que realizan procedimientos de control, accedan a los datos sin autorización, o los alteren sin dejar evidencias visibles, puede ser mayor en los sistemas computadorizados que en los sistemas manuales. Ello se debe a que la información es almacenada en forma electrónica, con una menor participación del hombre en el procesamiento, reduciéndose por consiguiente la oportunidad de detectar manualmente los accesos no autorizados. Por lo general, los recursos de información tienden a estar concentrados en los ambientes CIS.

- *Potencial para una mayor supervisión gerencial.* Los sistemas computadorizados ofrecen a la gerencia una amplia variedad de herramientas analíticas que pueden ser utilizadas para revisar y supervisar las operaciones de la organización,

- *Rastro de las transacciones.* El diseño de algunos CIS da como resultado que el rastro de las transacciones, que puede ser utilizado para propósitos de auditoría, sólo es conservado por poco tiempo o en forma electrónica.

- *Segregación de funciones incompatibles.* Ciertos controles, ejecutados por diferentes individuos en los sistemas manuales, pueden ser concentrados en los sistemas en los que se utiliza procesamiento computadorizado. Esto puede resultar en una menor segregación de funciones incompatibles. Sin embargo, los sistemas computadorizados pueden permitir que se implante una segregación de funciones incompatibles más rigurosa ya que pueden existir controles basados en el software (tales como identificaciones del usuario y contraseñas).

- *Iniciación automática o ejecución posterior de transacciones mediante el computador.* La iniciación de ciertas transacciones, o ciertas funciones de procesamiento pueden ser efectuadas automáticamente por el computador. Pueden o no existir evidencias visibles de estos pasos de procesamiento.

- *Los controles manuales dependen de la confiabilidad del procesamiento computadorizado.* El procesamiento computadorizado puede producir información utilizable para realizar controles manuales. La efectividad de estos procedimientos de control manual puede depender de la efectividad de los controles sobre la integridad y exactitud del procesamiento computadorizado.

- *Dependencia de los controles directos respecto de los controles generales.* La efectividad de los controles computadorizados y de las funciones de procesamiento computadorizadas puede verse disminuida si no se establecen controles generales adecuados.

2. Utilización del Computador como Herramienta de Auditoría

Si un cliente utiliza un sistema computadorizado para procesar información financiera significativa, es posible que consideremos necesario o ventajoso utilizar el computador para facilitar la ejecución de los procedimientos de auditoría. Las técnicas a disposición de los equipos de trabajo para este propósito se denominan técnicas de auditoría computadorizadas. Durante el proceso de planificación debemos estar alertas a las ventajas que nos pueden proporcionar estas técnicas.

Las técnicas de auditoría computadorizadas pueden ayudar en la planificación y ejecución de la auditoría en circunstancias en donde se presentan uno o una combinación de los siguientes factores:

- Existe una pérdida significativa del rastro de auditoría.
- Esperamos depositar confianza de auditoría en controles y funciones de procesamiento computadorizadas.
- No existen alternativas prácticas.
- Se puede lograr una auditoría más eficaz y eficiente.
- Es importante demostrarle al cliente que estamos utilizando herramientas y técnicas modernas en nuestro trabajo de auditoría.
- Estas técnicas nos otorgan la oportunidad de ampliar nuestra gama de servicios al cliente.
- Deseamos agregar valor a la auditoría mediante:
    - El examen del contenido de los archivos significativos de transacciones y datos permanentes y la comunicación de los hallazgos a la gerencia superior.
    - Recomendaciones sobre mejoras en el diseño de los sistemas y en los controles CIS dirigidas a la gerencia superior y al comité de auditoría.

Las técnicas de auditoría computadorizadas tienen cada vez una mejor relación costo/beneficio debido a cambios recientes y anticipados en el hardware y software de computación y en el diseño de los CIS. Por ejemplo:

- Con mayor frecuencia las aplicaciones más complejas incluyen técnicas de procesamiento tales como ingreso interactivo de datos, actualización inmediata de archivos de datos, bases de datos y procesamiento distribuido, En estos sistemas encontramos cada vez más:
    - Pérdidas significativas del rastro de auditoría.
    - Que es eficiente depositar confianza en los controles y funciones de procesamiento computadorizadas que implican el uso de software de sistemas y/o de aplicación.

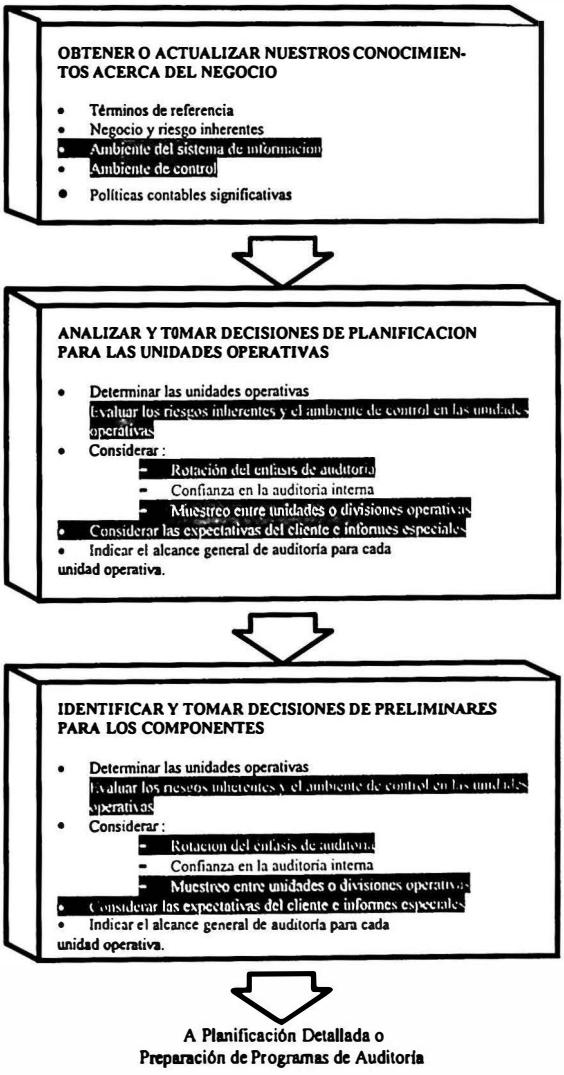
II. Planificación Estratégica

1. Introducción

La planificación estratégica requiere que el socio y el gerente apliquen sus conocimientos más recientes del cliente para analizar el negocio, realizar evaluaciones preliminares de riesgo sobre las diferentes partes del negocio, tomar decisiones de planificación sobre las partes o unidades del negocio, identificar componentes y establecer el enfoque de auditoría esperado.

En la Tabla siguiente se ilustra el proceso de planificación estratégica. Se han destacado los aspectos de la planificación que son mayormente afectados por la utilización por nuestros clientes de sistemas computadorizados.

DESARROLLO DE LA ESTRATEGIA DE AUDITORIA



2. Obtener o Actualizar Nuestros Conocimientos Acerca del Negocio

Existen dos aspectos de esta etapa de la planificación estratégica que pueden ser significativamente afectados por la utilización de sistemas computadorizados por parte del cliente:

- Ambiente del sistema de información.
- Ambiente de control.

2.1 Ambiente del sistema de información

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

- Estructura organizativa de las operaciones CIS.
- Naturaleza de la configuración CIS.
- Naturaleza y alcance del procesamiento computadorizado de la información para las principales áreas de los estados financieros o tipos de transacciones.

A.- Estructura organizativa de las operaciones CIS

La obtención de una comprensión general del ambiente de los sistemas de información debe comenzar con la estructura organizativa y administración del mismo. Esta comprensión permite al equipo de trabajo analizar el ambiente de control. También facilita la evaluación de la complejidad de los sistemas computadorizados del cliente y el probable grado de participación de los especialistas en auditoría CIS en la planificación detallada y en la ejecución de los procedimientos de auditoría planificados. Finalmente, la comprensión de la estructura organizativa y gerencial del departamento CIS proporciona generalmente

las bases para establecer una relación de trabajo efectiva con el personal responsable de los sistemas computadorizados del cliente.

Esta información debe incluir:

- Identificación del responsable del Departamento CIS.
- De quién depende dicha persona.
- Si existe un comité de dirección CIS ("steering committee").
- Si el grupo CIS está organizado en forma centralizada, o descentralizada entre varias unidades operativas.

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 todos los clientes.

Las organizaciones que poseen 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 CIS 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 se pueden realizar en el departamento usuario.

Gerencia

La responsabilidad general por la planificación, organización, dirección y control de las actividades de procesamiento de datos generalmente recae en un individuo. El título de esta persona puede variar según la organización (por ejemplo, gerente de procesamiento de datos, gerente de sistemas de información, director de administración de información, vice-presidente-administración de información). El lugar en que este individuo (y por consiguiente, el departamento CIS) se ubica dentro de la jerarquía de una organización también varía.

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 a los sistemas computadorizados como sistemas de información gerencial (o sea, sistemas que pueden procesar cualquier tipo de información que permita a la gerencia tomar decisiones, sin tener en cuenta si la información es de naturaleza financiera). A raíz de este nuevo concepto, los sistemas computadorizados 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 de¡ nivel gerencial dentro de las cuales se clasifican las funciones del departamento CIS:

- Sistemas y programación.
- Operaciones.

La función de sistemas y programación consiste en el desarrollo de sistemas y modificaciones a los mismos y la función de operaciones incluye la responsabilidad por el procesamiento diario. Nuestra preocupación fundamental con respecto a la organización de un departamento CIS es que su personal no realice funciones incompatibles. Un paso importante para alcanzar este objetivo es que exista una clara división (segregación) 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 del cliente; el hecho de que el cliente no posea grupos de "sistemas y programación" y "operaciones" no significa necesariamente que estas funciones no estén adecuadamente segregadas.

La segregación de funciones es un control general, es decir, un control que no proporciona satisfacción directa con respecto a las aserciones correspondientes a cada componente, pero que puede contribuir significativamente a la efectividad de los controles directos. Solamente es importante para nosotros desde la perspectiva de auditoría si nuestra intención es confiar en los controles directos. Por consiguiente, la segregación de funciones generalmente es considerada en profundidad en la planificación detallada, una vez que los controles directos potencialmente clave han sido identificados.

La organización y conducción del departamento CIS son consideradas en la planificación estratégica a fin de analizar el ambiente de control y determinar la complejidad relativa de los sistemas computadorizados del cliente. El socio y gerente a cargo son los responsables de decidir qué cantidad de información se requiere sobre la organización y conducción de los sistemas computadorizados del cliente para lograr los objetivos de la planificación estratégica. El análisis sobre las actividades típicas de un departamento CIS que se incluyen a continuación, ha sido presentado a fin de completar la información y no implica que en todos los trabajos se deba obtener información detallada con respecto a la segregación de funciones durante la planificación estratégica.

Los títulos y/o responsabilidades de los subgrupos pueden variar y probablemente así ocurra entre las distintas organizaciones. Por esta razón, debemos concentrarnos en las tareas que los individuos realizan (o tienen la oportunidad de realizar) para determinar si existe una adecuada segregación de funciones.

Función de sistemas y programación

Gerente de sistemas y programación. Trabaja junto con el gerente del departamento CIS en determinar las prioridades de los proyectos necesarios para cubrir las necesidades de información de la organización. Coordina y controla las actividades de los responsables de la programación de sistemas, del administrador de la base de datos (si existiera), de la programación de los sistemas de aplicación, y de su mantenimiento.

- *Grupo de Sistemas*: el software de sistemas es usado para facilitar la operación de todo el sistema de computación, a diferencia del software de aplicación que se usa para procesar transacciones e información de acuerdo con los requerimientos de los usuarios. El software de sistemas comprende: el sistema operativo, programas utilitarios, editores, métodos de acceso a archivos, sistemas de administración de base de datos y el software de control de acceso .

  El personal del grupo de sistemas es habitualmente el mejor capacitado del Departamento CIS. Sus responsabilidades incluyen el mantenimiento efectivo y la operación eficiente del software de sistemas. También puede participar en el planeamiento y evaluación del hardware y software y en el mantenimiento y modificación de software adquirido a proveedores externos.

  La mayoría de las organizaciones que poseen grandes sistemas de computación tienen, por lo menos, un programador de sistemas. Los programadores de sistemas usualmente cuentan con los conocimientos técnicos necesarios para hacer cambios en programas en código objeto (es decir, en lenguaje de máquina). No obstante, se debe

recalcar que la tarea de modificar el código objeto es técnicamente muy difícil y normalmente esto no presenta un riesgo de auditoría significativo.

Las responsabilidades propias de los programadores de sistemas requieren que tengan acceso a poderosos programas utilitarios y a editores. Estas herramientas pueden ser utilizadas para hacer cambios a los datos y programas sin generar un rastro de auditoría para fines de control. Por este motivo, se deberá controlar y supervisar rigurosamente el uso de estas herramientas.

El software de control de acceso puede ser utilizado para controlar y restringir el uso de dichas herramientas y para generar automáticamente un registro de actividad cada vez que se las utiliza. Dicho registro debería ser utilizado por la gerencia del Departamento para supervisar las actividades de los programadores de sistemas. Todos los accesos inusuales al sistema deberían ser investigados a fondo.

Los programadores de sistemas deberían tener prohibido el acceso a las versiones en código fuente de los programas de aplicación o a la documentación de los programas. El acceso a dicha información los pondría en una posición en la cual podrían manipular el procesamiento con mayor facilidad.

- *Administración de base de datos*: en una organización que utiliza tecnología de base de datos, diversos usuarios utilizan indistintamente los mismos datos. En estos casos, un grupo de Administración de la base de datos es responsable por la definición, organización, protección y eficiencia de la base de datos en uso, incluyendo la definición de procedimientos para el acceso y almacenamiento de los datos. Al individuo que lidera este grupo suele denominárselo Administrador de la Base de Datos (DBA).

  Mantener la integridad de la información de una base de datos requiere que se establezcan procedimientos especializados y el uso de software específico. Las responsabilidades del Administrador de la Base de Datos incluyen además el control del software de administración de base de datos y del acceso y las modificaciones que se efectúen al contenido del diccionario/directorio de datos.

- *Grupo de desarrollo de sistemas de aplicación*: los miembros de este grupo trabajan junto con los departamentos usuarios para analizar sus necesidades de información y desarrollar los programas de computación que satisfagan tales necesidades. Este grupo está formado por: analistas de sistemas, analistas/programadores y programadores que generalmente trabajan en equipo bajo la supervisión de un "líder de proyecto". Cada miembro del equipo es responsable de una parte del desarrollo de la aplicación, tal como se describe a continuación:

- *Analistas de sistemas*, trabajan en estrecho contacto con los usuarios en la definición de problemas y oportunidades para el desarrollo de sistemas de aplicación. Evalúan las alternativas, recomiendan aquellas que consideran más apropiadas para satisfacer las necesidades del usuario y desarrollan el diseño general del sistema para la alternativa seleccionada.
- *Analistas/programadores*, son responsables del desarrollo de las especificaciones detalladas de los programas de computación, basándose en el diseño general realizado previamente por los analistas de sistemas.
- *Programadores*, toman las especificaciones detalladas de los programas y codifican las instrucciones; compilan y prueban los programas; escriben la documentación destinada al usuario, personal de operaciones (quienes implantan el sistema) y al grupo de mantenimiento (quienes se encargan del mantenimiento); y prueban el nuevo sistema.

- *Grupo de mantenimiento (modificación) de programas*: este grupo es responsable por las modificaciones que se realizan a los programas ya existentes. Dependiendo de la envergadura de las modificaciones, es posible que deban cumplirse las mismas etapas que para el desarrollo de nuevas aplicaciones (o sea, definición del problema, análisis, diseño, etc.).

  Las personas responsables del diseño y desarrollo del software de aplicación poseen un conocimiento detallado sobre las funciones de procesamiento de dicho software. Por ello, deben tener prohibido operar el computador, incluso durante la prueba de los programas. Tampoco deberían tener acceso a los programas de producción (es decir, programas utilizados para el procesamiento cotidiano), a las instrucciones de ejecución de trabajos y a los archivos de datos que se utilicen para las corridas de producción. Al separar estas funciones se reducen las oportunidades de que directa o indirectamente se vea afectada la confiabilidad de la información contenida en los archivos de datos, al alterarse la ejecución de los programas durante su procesamiento.

  Algunas organizaciones separan las responsabilidades por el desarrollo de los programas de aplicación y su mantenimiento posterior. Una razón para ello es reducir la posibilidad de modificaciones no autorizadas a los programas de aplicación durante el mantenimiento de rutina. Los programadores involucrados en el desarrollo de un programa son los que están en mejores condiciones de efectuar modificaciones no autorizadas cuando se llevan a cabo las modificaciones por mantenimiento de rutina, ya que cuentan con un profundo conocimiento sobre las funciones del programa.

Otras organizaciones no separan las responsabilidades por el desarrollo y mantenimiento de los programas. Consideran que los programadores responsables por el desarrollo de los sistemas pueden mantener los programas en forma más eficiente que los programadores que no participaron en su desarrollo.

Función de operaciones

Gerente de operaciones. Es responsable de la operación diaria del computador, lo cual típicamente implica coordinar y controlar las actividades del personal responsable de las siguientes funciones: preparación de datos, operaciones, transmisión de datos, biblioteca, control y seguridad.

- *Preparación de datos*: el grupo a cargo de la preparación de datos es responsable por la conversión de los datos a un formato que pueda ser leído por el computador, usando dispositivos tales como pantallas, dispositivos de grabación sobre discos o cintas, lectoras de caracteres ópticos (OCRs), de reconocimiento de la voz humana y terminales de teletipo. Por lo general, la función de preparación de datos es realizada por los departamentos usuarios en los sistemas de actualización inmediata. El personal del departamento CIS con frecuencia es el responsable de la preparación de datos para el procesamiento de actualización diferida (por lotes).

- *Operaciones.* El grupo de operaciones es responsable por mantener el equipo en operación, controlar el desempeño del sistema, responder a los mensajes del software de sistemas y del software de aplicación (por ej., montaje de cintas o de discos, de acuerdo con lo que solicita el sistema operativo) y coordinar la mezcla de trabajos a ser procesados por el computador para lograr un uso eficiente y efectivo del equipo.

  Debe prohibirse a los operadores del computador efectuar modificaciones a los programas y acceder a las versiones en lenguaje fuente y a toda documentación relacionada con los mismos. El acceso físico al computador que los operadores tienen para poder desempeñar sus tareas habituales les permite manipular el procesamiento, si tienen los conocimientos necesarios sobre los programas de aplicación. Si los operadores tienen acceso al código fuente, se les debería prohibir el acceso a los editores on line que permiten modificar el código fuente.

  Para reducir el grado de control que un operador tiene sobre el procesamiento se pueden utilizar los paquetes de programación automática de trabajos (job scheduling) o los dispositivos de programación de trabajos del software de administración de operaciones. De esta manera, se reduce el riesgo de que el operador pueda iniciar

actividades de procesamiento no autorizadas durante períodos de inactividad o durante paradas momentáneas del procesamiento habitual.

- *Transmisión de datos.* Este grupo es responsable de asegurar que la organización cuente con los dispositivos necesarios de comunicación. Ello incluye evaluar, implantar, instalar y operar controladores de comunicaciones, protocolos de transmisión de datos y redes de comunicaciones. Una vez que el equipo está en uso, los miembros de este grupo son responsables de controlarlo y mantenerlo. También intervienen cuando se debe solucionar algún problema en la transmisión de datos.

- *Biblioteca.* Esta función implica el mantenimiento y control de la biblioteca física de la instalación, la cual contiene los archivos de datos y de programas. Sus dos responsabilidades principales son, asegurarse de que los archivos (tanto de datos como de programas) sólo sean utilizados para fines autorizados y mantener los medios usados para el almacenamiento de archivos en condiciones de uso apropiadas.

  Muchas organizaciones almacenan sus datos y programas en dispositivos de almacenamiento de acceso directo o DASD, permitiendo el acceso on line a los mismos en todo momento. Esto aumenta la importancia de la función de administración de biblioteca. Si no se las controla adecuadamente, cualquiera podría acceder a las versiones de producción del software de aplicación y a los archivos de datos (es decir, a las versiones utilizadas para el procesamiento diario).

  En esta situación la función de bibliotecario es usualmente desempeñada por dos programas de software de sistemas, el software de administración de operaciones y el software de administración de bibliotecas El software de administración de operaciones puede usarse para controlar el acceso a los archivos en discos o en cintas dirigiendo la secuencia de comandos de control de las tareas. La función más importante del software de administración de bibliotecas es controlar el estado de los programas de producción y las diversas versiones en códigos fuente de los programas de aplicación cuando se realizaron cambios a las mismas.

- *Control.* Es responsabilidad del grupo de control administrar el flujo de datos entre los usuarios y el centro de cómputos y entre el grupo de preparación de datos y el sector de operación. En ciertos entornos puede ser necesario establecer una función de control a fin de que exista una adecuada segregación de funciones. Sus principales funciones incluyen:

- Recibir la documentación de entrada que envían los usuarios, evaluar su integridad y razonabilidad, verificar los totales de control e ingresar los datos pertinentes en un registro.
- Enviar la documentación de entrada al sector de preparación de datos o al sector de operaciones, según corresponda (por ej.: si va a ser leído por una lectora de caracteres ópticos y está por lo tanto en un formato que puede ser leído directamente por el computador).
- Reunir, una vez finalizada la etapa de preparación, todos los datos de entrada (documentos fuente y en formato legible por el computador) y verificar que se hayan preparado todos los datos necesarios para la corrida de producción.
- Recibir del grupo de operaciones (una vez finalizada la corrida de producción) los informes de salida y los datos en formato legible por el computador, controlar su integridad, revisarlos para detectar errores obvios y enviar los informes de salida y los datos fuente a los usuarios y los datos de entrada en formato legible por el computador al sector de preparación de datos.

La necesidad e importancia de la función de control de datos ha ido disminuyendo a medida que los nuevos sistemas de computación utilizan entrada de datos interactiva (en vez de no-interactiva, característica de los sistemas de procesamiento con actualización diferida).

- *Seguridad.* El uso cada vez más frecuente de sistemas de información sofisticados ha llevado a la creación de una función especializada de seguridad de datos. El funcionario a cargo de la seguridad de datos (DSO: Data Security Officer) es responsable de la formulación de políticas relativas a seguridad de datos, privacidad y protección de las instalaciones de procesamiento de datos en casos de incendios, actos de vandalismo, robos y uso inadecuado (puede incluir también el planeamiento para recuperación en caso de desastre).

  Generalmente el DSO también es responsable de la implantación y control de las políticas y procedimientos relativos a la seguridad de los datos, incluyendo la autorización de nuevos usuarios, el control de las contraseñas de acceso y el seguimiento de los informes de violaciones a la seguridad generados por el software de control de acceso. El DSO debe estar capacitado para identificar los indicadores de actividades de procesamiento no autorizadas o inusuales, los intentos de acceso no autorizados y responder a éstos de inmediato siguiendo las pautas establecidas en las políticas de seguridad. Como los DSO normalmente poseen conocimientos detallados sobre los

controles de acceso de sus organizaciones, es necesario que se les prohiba ejecutar programas de aplicación.

Cambios que pueden afectar la estructura organizativa

Las estructuras organizativas de los departamentos CIS evolucionan continuamente, principalmente en respuesta a los cambios tecnológicos. Pero, como la teoría organizativa y la tecnología de hardware y software continúa avanzando, las estructuras organizativas probablemente cambien. Existen tres nuevos conceptos que probablemente tengan gran impacto en la organización y administración de sistemas computadorizados:

- La creciente capacitación del usuario, unida a una tecnología cada vez más avanzada (por ej.: los lenguajes de cuarta generación), crean un entorno de sistemas en el cual los usuarios participan más activa y directamente. Los días en que los usuarios se contentaban 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 computadores 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 computadorizados.

- Debido a la rápida y permanente evolución de la tecnología, los sistemas computadorizados están en un estado de cambio continuo. 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.

B.- Naturaleza de la configuración CIS

En la planificación estratégica, es necesario considerar los riesgos inherentes y de control asociados con los sistemas computadorizados. Para ello, resultará conveniente obtener una visión general de la configuración CIS. Esta información también nos puede ayudar a considerar la magnitud y complejidad de los sistemas computadorizados del cliente y en qué medida los especialistas en auditoría CIS deberían participar en las etapas de planificación detallada y ejecución de la auditoría.

Los sistemas de computación varían en tamaño desde un individuo que utiliza en un computador personal un software comprado hasta cientos de personas que utilizan un software sofisticado en redes de computación que abarcan docenas de computadores grandes y pequeños. Muchas organizaciones procesan los datos de todos los usuarios en una instalación central de procesamiento. No obstante, la disminución en el costo del hardware y los avances en la tecnología de transmisión de datos y servicios permiten que, con mayor frecuencia, las organizaciones puedan dispersar sus sistemas computadorizados utilizando procesamiento descentralizado o procesamiento distribuido de datos.

La estructura del sistema en uso puede tener implicancias de auditoría significativas. Por ejemplo, en un sistema centralizado existe a menudo, pero no siempre, una única organización CIS y un sólo tipo de software de aplicación y de sistemas en uso. Esto le permite al auditor lograr una comprensión de los sistemas del cliente 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 CIS, 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 (CPUs).
- Si las CPUs están interconectadas.
- Si el procesamiento es principalmente 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 CIS 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.
- Utilitarios con significación de auditoría y control.
- Software de recuperación de datos (query).
- Lenguajes de cuarta generación.

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

El alcance de la recopilación de información en la planificación estratégica varía según los trabajos. Por ejemplo, en el caso de clientes importantes con diversas unidades y sistemas descentralizados o distribuidos, resultará más eficiente obtener la mayor parte de la información enumerada anteriormente durante la planificación detallada. En el caso de pequeños clientes con sistemas centralizados, la información puede ser obtenida con más facilidad. El socio y gerente a cargo del trabajo son los responsables de determinar qué cantidad de información se requiere para lograr los objetivos de la planificación estratégica. Debe destacarse que la información que no fue obtenida durante la planificación estratégica debe ser obtenida durante la planificación detallada si se deposita confianza en los controles de procesamiento y funciones de procesamiento computadorizadas.

Cuando la información es transferida electrónicamente entre unidades de procesamiento y/o entre unidades de entrada remota de datos y unidades de procesamiento, es conveniente obtener un esquema de la red de transmisión de datos (por ej., una descripción gráfica de los lugares de procesamiento y de entrada remota de datos). El esquema de la red indicará si los medios de transmisión de datos (que implican diversos grados de riesgo de accesos no autorizados a la información) entre las diversas unidades y lugares de operación son:

- Redes privadas (líneas alquiladas).
- Redes públicas (acceso por discado).
- Redes de valor agregado (VAN).
- Redes locales (LAN).

C.- Naturaleza y alcance del procesamiento computadorizado de la información para las principales áreas de los estados financieros o tipos de transacciones

Como parte de nuestra comprensión de los sistemas computadorizados del cliente, es necesario considerar en qué grado el cliente ha computadorizado el procesamiento de las transacciones e información significativa para los estados financieros. Esta información será útil para evaluar el riesgo inherente y de control e identificar la naturaleza de las aptitudes requeridas para la planificación y ejecución de la auditoría con respecto a los sistemas computadorizados.

El nivel de detalle de la información a obtener en la planificación estratégica varía según factores tales como el tamaño y complejidad de los sistemas computadorizados del cliente y si la planificación detallada fue o será realizada para los componentes correspondientes. Entre los ejemplos del tipo de información que puede ser obtenida sobre los sistemas que respaldan los principales componentes de los estados financieros o tipos de transacciones se incluyen:

- Objetivo del sistema.
- Modificaciones significativas al sistema desde la última vez que se realizó una planificación detallada.
- Interfaces dentro del sistema y con otros sistemas.
- Volumen aproximado de transacciones procesadas por el sistema.
- Nombres de los paquetes de software comprados que se utilizan en la organización.
- Métodos de ingreso de datos (interactivo o no interactivo).
- Tipo de procesamiento (independiente o distribuido por redes).
- Resultados recientes de los trabajos de auditoría interna relacionados con el sistema.

En un examen recurrente, resulta conveniente que en la planificación estratégica nos concentremos en las modificaciones a los sistemas del cliente. 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 implicancias de dichas modificaciones sobre nuestro enfoque de auditoría deben ser consideradas sin demora en el proceso de planificación.

2.2 Ambiente de control

El ambiente de control es el conjunto de condiciones en el cual operan los sistemas de control. Al evaluar el ambiente de control, tenemos en cuenta el enfoque hacia el control por parte del directorio y la gerencia superior, la organización gerencial y el marco para ejercer el control gerencial. 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 CIS, conjuntamente con la gerencia superior de la organización, es la responsable de la planificación, organización, dotación de personal, dirección y control del departamento. Una buena gerencia brinda el beneficio obvio de asegurar que el procesamiento de datos sea realizado en forma eficiente y que el departamento reciba los fondos adecuados para permitir el efectivo desempeño de sus responsabilidades.

Una función importante de la gerencia del departamento CIS 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 financiera. Si los empleados perciben que la gerencia del departamento CIS 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 que 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 del cliente, seleccionar controles y funciones de procesamiento computadorizadas 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 computadorizados que deben ser considerados en la evaluación de la efectividad de un ambiente de control.

- El enfoque hacia el control por parte del directorio y de la gerencia superior.
  - En qué medida el estilo gerencial del departamento CIS se caracteriza por la planificación o improvisación.
  - Importancia que la gerencia del departamento CIS 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 CIS ante situaciones urgentes.

- Organización gerencial.
  - La posición del jefe del departamento CIS en la estructura organizativa del cliente.
  - El nivel de rotación del personal del departamento CIS.
  - Si la delegación de responsabilidades y autoridad dentro del departamento CIS es adecuada, y en qué medida la autoridad y las responsabilidades delegadas han sido definidas y comprendidas.
  - Si la gerencia del departamento CIS comprende el concepto de segregación de funciones y si están 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 CIS 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 CIS.
  - Si los planes y presupuestos financieros son utilizados para controlar los costos del departamento CIS.
  - 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 CIS identifica y responde a situaciones inusuales o excepcionales.

3. Analizar y Tomar Decisiones de Planificación para las Unidades Operativas

En la segunda etapa de la planificación estratégica, el socio y gerente a cargo dividen el negocio del cliente en unidades manejables, tales como subsidiarias, divisiones o establecimientos. Luego, toman las decisiones de planificación para cada unidad y asignan las responsabilidades a los grupos de trabajo correspondientes.

En el caso de un cliente con diversas unidades, la identificación de las unidades operativas y la delegación de responsabilidades para dichas unidades puede preceder a la

actualización de nuestra comprensión del negocio. En estas situaciones, la comprensión y el análisis del negocio puede ser realizado por el equipo de auditoría responsable de cada unidad operativo, en cuyo caso sería conveniente considerar los temas sobre sistemas computadorizados. *Obtener o actualizar nuestros conocimientos acerca del negocio*, a nivel de la unidad operativo en lugar de hacerlo para el cliente en general.

Cuando existen clientes con diversas unidades operativas que utilizan sistemas comunes (por ej., hardware, software y procedimientos de control/operativos) en todas las unidades resultará eficiente obtener la información, una sola vez para todas las unidades. En el caso de clientes que no utilizan sistemas comunes en todas las unidades, se deberá analizar en qué medida los sistemas varían entre ellas. Por ejemplo, se podrá obtener información una sola vez para los grupos de unidades que utilizan los mismos sistemas. En el caso de clientes descentralizados, puede ser necesario obtener la información por separado en cada unidad.

4. Identificar y Tomar Decisiones Preliminares para los Componentes

La etapa final de la planificación estratégica requiere la determinación de los componentes significativos para cada unidad operativo y la toma de decisiones preliminares con respecto al enfoque de auditoría esperado para los componentes individuales.

4.1 Evaluación 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 computadorizados 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, contables y de control no se ven afectados por los medios utilizados para procesar los datos y son aplicables tanto a entornos manuales como computadorizados, la forma e implantación de los controles diseñados para reducir al mínimo los riesgos propios de los sistemas computadorizados pueden ser diferente.

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

- El grado en que el cliente ha computadorizado el procesamiento de la información para las principales áreas de los estados financieros y tipos de transacciones.
- La complejidad relativa de los sistemas computadorizados del cliente.

- La eficiencia de la estructura organizativa de los sistemas computadorizados del cliente.
- En qué medida el negocio del cliente depende de los sistemas computadorizados.
- El uso de software de sistemas "sensitivos" que puede permitir a empleados expertos realizar cambios no autorizados a los datos y programas.

4.2 Consideración de la rotación del énfasis de auditoría

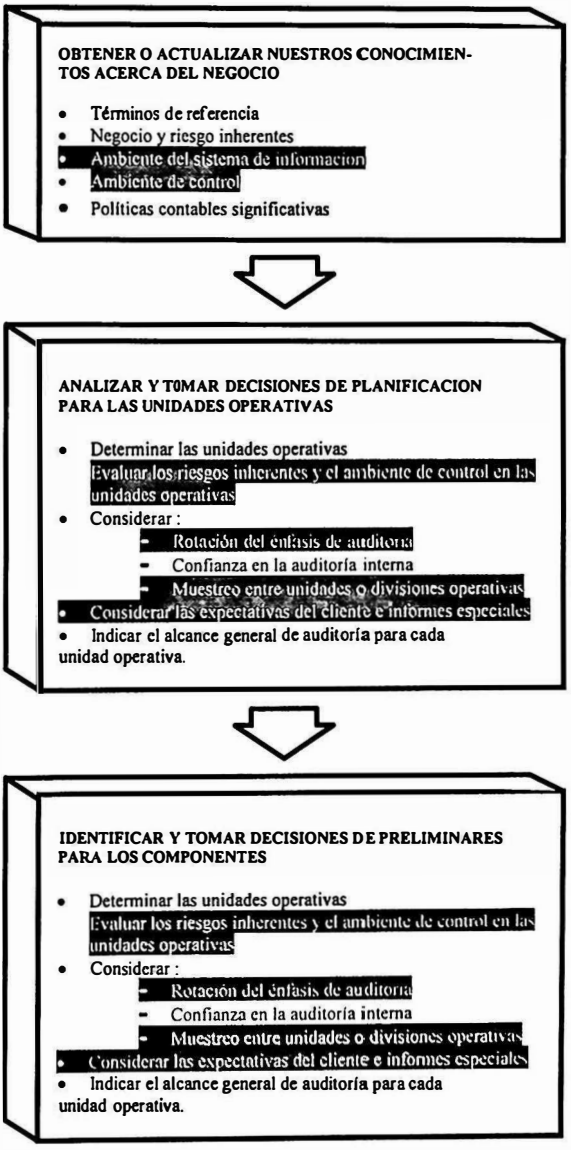
Si en años anteriores hemos obtenido evidencia de que los controles clave y las funciones de procesamiento computadorizadas operan con un alto grado de confiabilidad, podremos optar por confiar en nuestro conocimiento acumulado como base del plan de rotación del énfasis de auditoría.

Si se adopta un plan de rotación y se espera confiar en los controles y funciones de procesamiento computadorizadas para el período bajo examen basados en los conocimientos acumulados en años anteriores, requiere la aplicación de ciertos procedimientos mínimos. Estos procedimientos incluyen indagaciones apropiadas durante el año corriente para determinar si han ocurrido cambios significativos en los controles clave, incluyendo las funciones de procesamiento computadorizadas sobre las cuales se depositará confianza. Si los controles clave son computadorizados, existe el riesgo de que su operación sea afectada por cambios en los programas relevantes. Si los procedimientos de cambios a los programas no son eficientes, existe la posibilidad de que se hayan realizado cambios no autorizados en los programas que no serían detectados por las indagaciones apuntadas específicamente a los controles clave. Por consiguiente, nuestros procedimientos de indagación deben ser ampliados para incluir la consideración de la efectividad de los procedimientos de cambios a los programas y otros controles importantes del departamento CIS.

III.- Planificación Detallada

1. Introducción

Con frecuencia puede suceder durante la planificación estratégica que nuestra comprensión de un componente no sea 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 computadorizadas en que podríamos confiar. Esta información es obtenida durante la planificación detallada.



A menudo, el aspecto de la planificación detallada que insume más tiempo en un ambiente CIS es la obtención de información adicional para los componentes y, específicamente, las actualizaciones de sistemas. En esta etapa es cuando obtenemos y documentamos (o actualizamos) la comprensión de los aspectos relevantes de los sistemas de información del cliente y los controles generales relacionados.

Independientemente de si la actualización de sistemas es realizada o si la comprensión del sistema es obtenida por primera vez, es importante tener en cuenta que el propósito para el cual obtenemos una comprensión de los sistemas de información del cliente es identificar los controles clave potenciales, es decir aquellos controles y funciones de procesamiento computadorizadas en las que podemos confiar para proporcionar satisfacción para el objetivo de auditoría de un componente.

Un aspecto importante de la actualización de sistemas es la consideración de los riesgos de auditoría asociados con el uso de sistemas computadorizados por parte del cliente. Hemos definido cuatro riesgos inherentes de aplicación y tres riesgos inherentes del departamento CIS que, están presentes cuando, los clientes, le utilizan sistemas computadorizados para procesar información significativa para los estados financieros. Estos riesgos, juntamente con los controles que puedan ser implantados por el cliente para reducirlos a niveles aceptables, son tratados posteriormente, como obtención de información adicional sobre los componentes - Riesgos de aplicación y Riesgos del Departamento CIS, respectivamente.

Por razones de eficiencia en la planificación, sólo debemos obtener una comprensión más detallada de los sistemas del cliente cuando esperamos depositar confianza en los controles, incluyendo las funciones de procesamiento computadorizadas, a fin de lograr el objetivo de auditoría para el componente. No obstante, como servicio adicional al cliente, podemos optar por considerar los sistemas con mayor detalle del que sería necesario para la auditoría.

1.1 Categorías de control interno

Para facilitar nuestra comprensión de los controles, éstos han sido clasificados de la siguiente manera.

a) Ambiente de control: el ambiente de control ya fue definido en la planificación estratégica y por lo tanto debe recurrirse a esta información en esta etapa de la memoria.

b) Controles directos: son aquellos diseñados para evitar o detectar errores o irregularidades que afectarían los estados financieros y aquellas funciones de procesamiento computadorizadas que involucran el desarrollo de un aspecto esencial del procesamiento de transacciones e información directamente relacionada, desde su exposición hasta la información en los estados financieros. Estos controles y funciones de procesamiento computadorizadas respaldan directamente las aserciones correspondientes a los componentes individuales y, por lo tanto, constituyen fuentes de satisfacción de auditoría. Los controles directos abarcan controles gerenciales e independientes, controles de procesamiento y funciones de procesamiento computadorizadas y controles para salvaguardar activos.

c) Controles generales: son aquellos que contribuyen significativamente a la efectividad de los controles directos. Abarcan la segregación de funciones incompatibles y controles del departamento CIS. Los controles generales no proporcionan satisfacción directa con respecto a las aserciones correspondientes a los componentes. Al considerar la confianza en los controles directos como una fuente de satisfacción de auditoría, debemos considerar si las deficiencias de los controles generales pueden afectar la efectividad del control directo.

En la planificación detallada nos concentramos en obtener y documentar una comprensión sobre los controles directos y generales para los componentes en los que esperamos confiar en la evidencia de control.

Los objetivos gerenciales de un sistema de información, contable y de control no están afectados en gran medida por los métodos utilizados para procesar datos y son aplicables tanto a los sistemas de información manuales como a los computadorizados. No obstante, la forma de algunos controles y cómo son aplicados puede ser diferente.

Algunos controles se realizan mediante la combinación de procedimientos computadorizados y manuales. Por ejemplo, un programa de computación puede generar un informe de todas las transacciones que no reúnen ciertos criterios, pero la investigación y seguimiento de estos ítems se realizará manualmente. Algunos controles sólo existen en un

ambiente CIS, como por ejemplo los controles sobre cambios a los programas de computación. Mas adelante se describen los riesgos de auditoría que se encuentran en un ambiente CIS y los controles que pueden ser implantados para reducir estos riesgos a un nivel aceptable.

1.2 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 a pagar en el que los informes de recepción y las facturas del proveedor son apareadas por el computador. Este proceso es un control directo que puede proporcionarnos evidencia, por ejemplo de que las compras representan mercaderías recibidas. Si se pudieran efectuar cambios no autorizados a los programas que realizan esta tarea, no podremos confiar en este control directo. Por consiguiente, la ausencia de un control adecuado sobre cambios a los programas (normalmente considerado 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 con respecto a las aserciones.

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 computadorizadas. Sin embargo, es probable que deseemos considerar ciertos controles generales con mayor detalle respondiendo a expectativas del cliente.

Debemos tener cuidado de no depositar demasiado énfasis en la denominación de "controles generales". Esto es especialmente importante cuando se trata de sistemas computadorizados sofisticados como los que incluyen aplicaciones múltiples e interactivas. Bajo estas circunstancias, los controles generales pueden ser diferentes en los distintos sistemas de aplicación. Por ejemplo, los procedimientos sobre cambios a los programas en el sistema de cuentas a pagar de una organización pueden ser diferentes de los procedimientos empleados para la aplicación de costos de producción.

También debemos ser cuidadosos cuando nos referimos a los "controles del departamento CIS". En organizaciones descentralizadas existen diversas funciones tradicionales del departamento CIS que pueden ser realizadas por los usuarios. Por ejemplo, los usuarios pueden ser responsables de un determinado desarrollo de sistemas y de actividades de mantenimiento. Por consiguiente, los "controles del departamento CIS"

pueden incluir procedimientos realizados tanto dentro de los departamentos usuarios como dentro del departamento CIS.

1.3 Distinción entre controles directos y funciones de procesamiento computadorizadas

Las funciones de procesamiento son determinados pasos del sistema del cliente que se ocupan de las transacciones e información relacionada desde su origen hasta su inclusión en los estados financieros o en el documento que corresponda. Incluyen tareas tales como cálculo, registración, comparación y acumulación de información contable y general. Pueden ser manuales o computadorizadas (lo cual cada vez es más frecuente). Los controles pueden ser acciones realizadas por la gerencia, un representante o un empleado del cliente o un software, o pueden incluir dispositivos para salvaguardar activos a fin de asegurar que las decisiones gerenciales son cumplidas y para evitar o 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, registración, 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 constituyen funciones significativas dentro del proceso contable, ya que están directamente relacionadas con las aserciones de los estados financieros.

Las funciones de procesamiento que representan controles como así también las que son aspectos esenciales del proceso contable (pero no son controles) pueden ser funciones de procesamiento "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 del componente, (por ejemplo, depositar confianza en las funciones de procesamiento para lograr satisfacción de que las aserciones son válidas, puede ser más eficiente que otros procedimientos de auditoría). En segundo lugar, cuando no se puede lograr confianza, el auditor aún necesita obtener evidencia, en este caso evidencia sustantivo, de que los aspectos esenciales de la función de procesamiento han sido realizados satisfactoriamente para las transacciones procesadas, es decir, que las aserciones relevantes de los estados financieros son válidas.

En un ambiente manual, generalmente existe una relación "uno a uno" entre las funciones y los controles de procesamiento. Por ejemplo, los cálculos básicos manuales

generalmente son controlados por un segundo individuo (por lo menos en forma selectiva). Nuestro interés en este tipo de ambiente suele estar en los controles. Sin embargo, en un sistema computadorizado es probable que esta relación "uno a uno" no exista; es improbable que, por ejemplo, los cálculos básicos realizados por un computador sean controlados en forma manual. Esto se debe a que si el software está adecuadamente desarrollado para realizar una función particular de procesamiento y está adecuadamente protegido contra cambios no autorizados, realizará esta función sin error. Por consiguiente, podremos confiar en este tipo de función de procesamiento computadorizada de la misma manera que confiamos en los controles.

2. Obtención de información Adicional sobre los Componentes - Riesgos de Aplicación

2.1 Introducción

Esta sección analiza los cuatro riesgos de auditoría al nivel de aplicación en el procesamiento de las transacciones e información relacionada, que son comunes a la mayoría de los sistemas computadorizados y, por lo tanto, son aplicables al procesamiento de las transacciones en la mayoría de los grupos de componentes. Nuestra consideración de estos riesgos durante la planificación detallada aumenta en importancia cuánto más computadorizado sea el sistema.

Los cuatro riesgos CIS que son típicamente considerados a través de la implantación de controles de aplicación (controles que normalmente varían según el sistema de aplicación) son los siguientes:

a) 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.
b) Los datos permanentes y de transacciones ingresados para su procesamiento pueden ser imprecisos, incompletos o ser ingresados más de una vez.
c) Los datos rechazados y las partidas en suspenso pueden no ser identificadas, analizadas o corregidas.
d) 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 o inexacta o en el período contable incorrecto.

Además de los controles aquí descritos, también constituyen fuetes potenciales de satisfacción de auditoría ciertos controles gerenciales e independientes, funciones de procesamiento computadorizadas y controles de procesamiento manuales. Algunos ejemplos son:

- Comparación de documentación (por ejemplo, cantidades y precios de las facturas, informes de recepción y órdenes de compra).
- Aprobación por los usuarios o automáticamente por el computador de las transacciones basándose en el cumplimiento satisfactorio de los pasos previos de procesamiento (por ejemplo, aprobación de órdenes de compra, registración de facturas de proveedores, desembolsos por medio de transferencias electrónicas de fondos).

El auditor no debe esperar que sus clientes hayan implantado todos los controles tratados bajo cada riesgo. En algunos casos, uno de los controles descriptos puede ser suficiente para reducir el riesgo a un nivel aceptable. En otros, puede ser necesaria una combinación de controles. También pueden existir casos en los que no se encontrarán ninguno de los controles aquí tratados pero en los que el cliente ha implantado otros controles que reducen adecuadamente los riesgos presentes.

El determinar si los controles existentes proporcionan una base suficiente para obtener confianza de auditoría es una cuestión de criterio profesional. Las consideraciones a tener en cuenta al evaluar la efectividad de los procedimientos de control incluyen los riesgos específicos presentes, la naturaleza de los controles que han sido implantados, la forma en que han sido implantados y su relación con otros controles.

Relación entre las características del sistema y los cuatro riesgos al nivel de aplicación

Los equipos de trabajo con frecuencia deciden confiar en la evidencia de control para las aserciones relacionadas conciertos grupos de componentes, por ejemplo, ingresos por ventas y cuentas a cobrar, existencias y costos de producción, compras y cuentas a pagar, remuneración.

Existen dos tipos de características del sistema:

- Características que se relacionan con los cuatro riesgos de auditoría CIS al nivel de aplicación.
- Características que se relacionan con otros aspectos esenciales del procesamiento de las transacciones e información relacionada.

Al concentrar nuestra atención en las características del sistema estamos considerando implícitamente los cuatro riesgos al nivel de aplicación.

Ejemplo

Las características del sistema para la actividad del negocio "Facturación" del componente Ingresos por ventas y Cuentas a cobrar. Cuatro de las características del sistema pueden ser directamente relacionadas directamente relacionadas con los cuatro riesgos comunes de auditoría CIS al nivel de aplicación.

Característica del sistema	*Riesgo de auditoría*
• El acceso a las funciones de procesamiento de facturas y notas de crédito y a los registros de datos relacionados está restringido.	• 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.
• Todos los datos de las facturas y notas de crédito son ingresados para su procesamiento en forma completa y precisa y sólo una vez.	• Los datos permanentes y de transacciones ingresados para su procesamiento pueden ser imprecisos, incompletos o ser ingresados más de una vez.
• Las facturas y notas de crédito rechazadas o no apareadas son identificadas, analizadas y corregidas en forma oportuna.	• Los datos rechazados y las partidas en suspenso pueden no ser identificadas, analizadas o corregidas.
• Los datos de las facturas y las 'notas de crédito son procesados en forma completa y precisa en el período contable adecuado, incluyendo la transferencia de datos a otros sistemas.	• 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 o inexacta o en el período contable incorrecto.

El resto de las características del sistema está relacionado con otros aspectos esenciales del procesamiento de las transacciones de ingresos por ventas e información relacionada.

El análisis de los controles que sigue a continuación trata sobre los cuatro riesgos de auditoría CIS al nivel de aplicación.

Consideración de posibles debilidades

Al considerar las implicancias de auditoría de las posibles debilidades del sistema del cliente, debe tenerse en cuenta la importancia de las características del sistema. Si el cliente no posee controles de procesamiento o funciones de procesamiento computadorizadas 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 CIS al nivel de aplicación y otros aspectos esenciales del procesamiento, es importante considerar de qué manera el cliente alcanza los objetivos de las características si no existen controles de procesamiento o funciones de procesamiento computadorizadas. A menudo, esto requiere confianza en los controles gerenciales y controles independientes (por ej., el énfasis de la gerencia puede recaer en controles de detección más que en controles de prevención). Si no existen controles mitigantes, es posible que debamos reevaluar el alcance de los procedimientos sustantivos planificados.

2.2 Acceso a las funciones de procesamiento de las transacciones o registros de datos resultantes

A.- 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

B.- Medios de control

El riesgo descripto se refiere a la posibilidad de acceso no autorizado a las funciones de procesamiento de los programas de aplicación o a los registros de datos resultantes a través de los procedimientos normales de iniciación, autorización y registración de transacciones. También existe el riesgo de que personas no autorizadas puedan tener acceso directo a la información almacenada o a los programas de aplicación utilizados para procesar la información a través del software de sistemas u otras vías de acceso.

Hay dos aspectos de importancia relativos al control del acceso a las funciones de procesamiento de los programas de aplicación o registros de datos resultantes:

- Si el acceso sólo es otorgado a quienes no desempeñan funciones incompatibles.
- Si se prohiben los accesos no autorizados.

La posibilidad de que una persona no autorizada lea la información almacenada en los archivos de datos, particularmente aquellos que contienen información confidencial, como por ejemplo, nóminas de remuneraciones, listados de clientes, fórmulas de productos y secretos comerciales, generalmente resulta un tema de preocupación para nuestros clientes. Si no existen controles que lo impidan, podremos hacer una recomendación al respecto a la gerencia. No obstante, cuando no se pueden agregar, eliminar ni modificar datos, es muy improbable que esta posibilidad de "lectura solamente" afecte nuestro enfoque de auditoría.

Segregación de funciones

El principio de asignar tareas a quienes no tengan funciones de procesamiento incompatibles es el mismo tanto si el procesamiento es manual o computadorizado. Las responsabilidades deben ser distribuidas de forma tal que el acceso de los empleados a las funciones de procesamiento computadorizadas no los habilite para llevar a cabo funciones incompatibles. Por ejemplo, no debería autorizarse a un mismo empleado el acceso a las funciones de procesamiento para ingresar facturas, informes de recepción y de compras.

La segregación de funciones es un control general. No obstante, en un ambiente CIS los controles basados en software que normalmente son utilizados para restringir el acceso a las funciones de procesamiento de transacciones o a los registros de datos resultantes pueden constituir un medio efectivo para asegurar dicha segregación. Debido a la concentración de datos y programas que generalmente hay en un ambiente CIS, las

funciones pueden estar segregadas en el aspecto organizativo, pero esta segregación no será efectiva sin controles de acceso basados en software.

Control del acceso

En aquellos sistemas computadorizados en los que el ingreso de datos no es interactivo, la restricción de¡ acceso a las funciones de procesamiento del software de aplicación es relativamente sencilla. Por lo general, ello, se logra mediante controles de procesamiento por lotes.

Los recientes avances en la tecnología CIS han ampliado el acceso a los sistemas computadorizados y, por consiguiente, a la información almacenada en los archivos del computador. Con mayor frecuencia se permite el acceso, lectura y uso de datos computadorizados a los departamentos usuarios. Pero una vez que se otorga el acceso a los sistemas computadorizados aumenta el riesgo de acceso no autorizado. Por ejemplo, existe el riesgo de que empleados 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 accede, un sólo individuo podría llegar a realizar tareas incompatibles. Es muy raro que una organización otorgue a un mismo empleado tan amplio acceso.

En ambientes en los que los datos son ingresados o están a disposición de los usuarios en forma interactiva, el control del acceso resulta más complicado, La efectividad del control dependerá, por lo general, del uso de software que permita el acceso del usuario a ciertas funciones de procesamiento computadorizadas, pero no a otras. Por ejemplo, se puede autorizar a un usuario a leer datos pero no a modificarlos. En realidad, los controles de acceso programados pueden considerarse como una manera de implantar electrónicamente la segregación de funciones. El uso de software crea la oportunidad de lograr una segregación de funciones más efectiva que la que puede lograrse en un ambiente manual. Debido al amplio rango de datos y programas que son potencialmente accesibles para una persona que tiene acceso a un sistema computadorizado moderno, la segregación de funciones por sí sola raramente constituirá un control efectivo.

También se utiliza software y ocasionalmente hardware, para definir qué funciones puede realizar un individuo, a qué datos puede acceder y cómo restringir a esa persona en consecuencia. Se utilizan varios mecanismos para lograr estos controles, incluyendo:

- Menúes.
- Normas/perfiles de acceso.
- Acceso a los datos por programa.
- Dispositivos de acceso a los datos/programas.
- Dispositivos de seguridad de terminales, incluyendo dispositivos de acceso personalizado o "tarjetas inteligentes".

Existen tres etapas dentro del control de acceso: identificación, autenticación y permiso/rechazo. Las funciones de identificación y autenticación, es decir, identificar al usuario y probar quien dice ser, son realizadas independientemente del acceso a las funciones y datos particulares del procesamiento. Estos aspectos del control de acceso son relevantes al riesgo de acceso no autorizado al sistema, más que 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 acceder y, a menudo, las opciones con que contará una vez que haya accedido a los datos.

El permiso/rechazo 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 aplicación, o a ambos. Los principales elementos de software de sistemas que pueden ser utilizados solos o combinados para restringir el acceso incluyen:

- Software de control de acceso.
- Monitores de teleprocesamiento.
- Software de control de comunicaciones.
- Software de administración de base de datos.

Las consideraciones sobre control de acceso relacionadas con estos elementos de software de sistemas y de aplicación están resumidas en la Tabla.

ELEMENTOS DEL SOFTWARE DE SISTEMAS

CONTROLES :	Monitor de teleprocesamiento	Software de control de acceso	DBMS	Software de control de comunicaciones	Programa de aplicación
Menúes	1	-	-	-	2
Normas/perfiles de acceso	3	4	-	5	6
Acceso a los datos por programa	-	7	8	–	-
Acceso a los datos/programas por dispositivos	9	10	-	11	-

1. Un monitor de teleprocesamiento presenta un menú de programas, (pero no las funciones de procesamiento dentro de los programas), que el usuario puede utilizar. El monitor de teleprocesamiento le permite utilizar al usuario sólo las funciones indicadas. En algunos casos, los menúes pueden ser adaptados a determinados individuos o grupos.

2. Las funciones indicadas en los menúes, que a menudo son denominadas "transacciones", son grupos de programas conectados a través de un "código de transacción". Estas transacciones y programas no son un software de sistemas sino aplicaciones escritas y/o implantadas por el cliente.

3. Los monitores de teleprocesamiento incluyen sus propios mecanismos de control de acceso, Las personas, individualizadas mediante sus propias identificaciones u otro tipo de códigos, están limitadas a códigos de transacciones, archivos, programas, etc. específicos.

4. El software de control de acceso es el principal medio de control de acceso a las funciones y datos en la mayoría de los sistemas computadorizados IBM. Incluye un perfil (también conocido como esquema o tabla de seguridad) para cada usuario y/o grupo. Estas tablas son utilizadas por el software de control de acceso para permitir o rechazar acceso a los códigos de transacciones, programas, archivos de datos y a algunos registros específicos de los archivos.

5. El software de control de comunicaciones restringe el acceso de usuarios individuales y/o dispositivos a las aplicaciones autorizadas. Observe que las aplicaciones a las que controla este software son de un nivel muy alto; por ejemplo, monitores de

teleprocesamiento tales como CICS y editores on line tales como TSOIISPF son considerados aplicaciones y no así las existencias o la nómina de remuneraciones.

6. Las aplicaciones pueden incluir restricciones de acceso basadas en tablas o archivos internos que van más allá de las limitaciones disponibles a través de otros medios. Por ejemplo, el software de control de acceso puede limitar a un empleado de la Sección Personal a las funciones de aplicación de remuneraciones, pero el sistema de aplicación en sí mismo podría ser utilizado para impedirle el acceso al procesamiento de datos de remuneraciones de ejecutivos.

7. El software de control de acceso puede ser utilizado para permitir el acceso de individuos o grupos a archivos específicos. Además, el software de control de acceso puede restringir el acceso a archivos a través de programas específicos. Esta técnica es conocida como "ruteo" ("pathing") o "registración".

8. Los sistemas de administración de base de datos pueden limitar el tipo y cantidad de datos disponibles para un programa, y pueden limitar lo que el programa puede hacer con los datos (por ej., leer, actualizar, eliminar, etc.). En los mainframes IBM, el DBMS controla las "vistas lógicas" de los programas; se necesitan otros medios (por ej.,: software de control de acceso o monitores de teleprocesamiento) para restringir el acceso de los usuarios a los programas.

9. Los monitores de teleprocesamiento pueden determinar qué programas pueden ser ejecutados desde terminales específicas.

10. El software de control de acceso puede determinar a qué programas, datos y otros recursos se puede acceder desde terminales específicas.

11. El software de control de comunicaciones incluye funciones para limitar el acceso a través de líneas remotas a aplicaciones específicas de alto nivel, como por ejemplo, monitores de teleprocesamiento tales como CICS y editores on-line tales como ISPF/TSO.

C.- Análisis de los controles

Menúes

Un menú es un listado de funciones expuesto en la pantalla de una termina¡ para dirigir al usuario a las funciones apropiadas. Muchos de los diseñadores de sistemas de aplicación utilizan menúes 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 menúes pueden ser armados para implantar la segregación de funciones.

Todas las funciones de un sistema de aplicación pueden ser indicadas en un menú "principal". En este caso la selección de una función determinada puede impedir la selección de actividades incompatibles (por ej., procesamiento de informes de recepción y facturas de proveedores). También se pueden desarrollar menúes para usuarios o grupos de usuarios específicos. A los usuarios sólo se les permite acceder a sus propios menúes (por ej., por software de control de acceso) pero pueden utilizar cualquiera de las funciones incluidas en esos menúes.

Normas/perfiles de acceso

El software de control de acceso, los monitores de teleprocesamiento, el software de control de comunicaciones y otros 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 qué grupo pertenece un individuo y lo que se le permite hacer a un usuario con un recurso determinado. Aunque existen algunas diferencias en los mecanismos utilizados por los diferentes productos, ellos tienen ciertos elementos básicos:

- Un identificador único para cada individuo. Esta puede ser la identificación del usuario, identificación "log on", u otro término parecido, el que es autenticado por el uso de una contraseña. Esta misma combinación de identificación del usuario y contraseña se utiliza para el acceso al sistema.
- Alguna forma de asociar o vincular a un individuo con un grupo de usuarios con privilegios de acceso similares.
- Una lista de recursos protegidos (o en algunos casos, desprotegidos) y un mecanismo para asociarlos con los grupos usuarios.
- Un mecanismo para determinar qué funciones (por ej., leer, escribir, ejecutar, eliminar) le son permitidas a un usuario autorizado respecto de los programas y datos.

- Un mecanismo de supervisión e información para detectar intentos de acceso no válidos al sistema, funciones, programas, datos u otros recursos CIS.

Acceso a los datos por programa

En ciertos casos, la restricción de acceso a los datos es aplicada en dos etapas. Los programas están limitados con respecto a los datos a los que pueden acceder y/o actualizar, y los individuos están limitados con respecto a los programas que pueden utilizar. Por consiguiente, son restricciones de acceso a los datos para los individuos.

Los sistemas de administración de base de datos (DBMS) restringen el acceso de los programas a "vistas lógicas" de la base de datos, El software de control de acceso puede limitar el acceso de los individuos a programas específicos. Los DBMS también pueden determinar qué programas pueden acceder a qué datos. Cuáles son los mecanismos de control que se utilizarán, es una cuestión de diseño.

Acceso a los datos/programas por dispositivos

De la misma manera en que se limita a los individuos 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 (por ej., transferencia internacional de fondos), 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.

Debe tenerse en cuenta que aún cuando todos los individuos de un área física determinada tengan los mismos privilegios de acceso, las restricciones de acceso por dispositivos no eliminan la necesidad de que cada usuario se identifique individualmente. Cuando los usuarios comparten las identificaciones se pierde la posibilidad de asignar responsabilidades individuales.

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. Algunos de los dispositivos de seguridad de terminales más comunes se detallan en la siguiente tabla.

CONTROLES DE SEGURIDAD DE TERMINALES

- Instalación de cerraduras o dispositivos similares en las terminales, para permitir el uso de las mismas sólo a quienes posean las llaves correspondientes.
- Circuitos internos que identifican físicamente a la terminal como autorizada a acceder a la aplicación en cuestión. Este dispositivo puede interactuar con el sistema central para denegar el acceso desde una terminal que no contenga los circuitos de seguridad apropiados.
- Mecanismos de retrodiscado (dial-back), que aseguran que los usuarios acceden al sistema desde lugares autorizados. Una vez que el usuario se ha conectado y ha ingresado la identificación o contraseña apropiada, la terminal es desconectada, el computador central llama automáticamente al número de teléfono autorizado de la terminal y otorga el acceso. Sin embargo, este mecanismo puede ser burlado mediante la activación de ciertos dispositivos de los equipos telefónicos para derivar el llamado a otra terminal,
- Rutinas de bloqueo activadas automáticamente por el software de seguridad cuando se cumplen ciertas condiciones. Por ejemplo, el software de control de acceso puede ser programado para denegar el acceso si se ingresan más de tres contraseñas incorrectas o para cancelarlo, si se intentan realizar más de tres tipos de transacciones inválidas, o si una terminal permanece inactiva durante un determinado número de minutos en el curso de una sesión, indicando que un usuario autorizado pudo haber olvidado finalizar formalmente la sesión.
- Se utilizan dispositivos para terminales que pueden identificar la voz del usuario autorizado, sus huellas digitales, firma u otras características particulares de identificación. Estos dispositivos proporcionan un mayor nivel de seguridad, no obstante, no están aún muy difundidos ya que no han sido perfeccionados técnicamente y son relativamente caros.

D.- Obtención de evidencia de control

Segregación de funciones

La prueba de la segregación de funciones puede incluir:

- Análisis de las responsabilidades de aquellos empleados a quienes se les asignan partes significativas del procesamiento de información. Para ello debe determinarse si las responsabilidades de iniciación de las transacciones están separadas de las responsabilidades de aprobación, procesamiento y registración de las mismas. Debemos asegurarnos de que todos los procedimientos por los cuales las transacciones e información directamente relacionada es iniciada o ingresada para su procesamiento hayan sido evaluados, incluyendo los reingresas de transacciones rechazadas.
- Observar a los empleados mientras desempeñan sus tareas para determinar si cumplen con las responsabilidades asignadas.

Controles de acceso

Obtener evidencia con respecto a los controles de acceso a las funciones de procesamiento y datos requiere conocimientos tanto de la estructura organizativa del cliente como de la implantación técnica de los controles de acceso computadorizados. A menudo será necesaria una estrecha coordinación con un especialista en auditoría CIS que esté familiarizado con el software y hardware del cliente. La prueba de los controles de acceso programados puede incluir uno o más de los siguientes procedimientos:

- Obtener, revisar y analizar los perfiles o tablas de seguridad del monitor de teleprocesamiento, software de control de acceso o DBMS. El propósito de esta prueba es determinar si el acceso a las funciones de procesamiento del software de aplicación o a los datos relacionados está apropiadamente restringido para que los usuarios no autorizados y aquellos a quienes se les hayan asignado funciones potencialmente incompatibles no puedan acceder a los mismos. Las características de los perfiles deben ser acordadas con la gerencia del cliente. Es importante analizar la compatibilidad de funciones entre los departamentos como así también dentro de un mismo departamento.
- Intentar desplazarse de un menú de aplicación a otro para determinar si existe la posibilidad de realizar funciones incompatibles. Esta prueba nos permitirá determinar la efectividad de las restricciones de acceso funcionales y a la vez mejora nuestro conocimiento de la estructura del menú autorizado para el sistema.
- Determinar si el paquete de software de seguridad en el cual se deposita confianza ha sido adecuadamente implantado desde el punto de vista técnico. El propósito de este paso es determinar si su uso proporciona el nivel de control deseado y verificar que no puede ser eludido con facilidad.

- Determinar la distribución de funciones. Es razonable suponer que el acceso a las funciones más sensitivas sólo será permitido a un reducido grupo de individuos y el acceso a las funciones menos sensitivas podrá ser otorgado a una mayor cantidad de individuos. En este sentido, sería útil realizar un análisis de funciones de aplicación por cantidad de usuarios.

2.3 Datos ingresados para su procesamiento

A.- Riesgo

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

B.- Medios de control

Los datos de computación son de dos formas básicas: datos de transacciones y datos permanentes, Los datos de transacciones se relacionan con las transacciones individuales producto de las operaciones diarias. Los datos permanentes son utilizados en forma recurrente y a menudo incluyen:

- Datos de referencia general (por ejemplo, nombres y domicilios, códigos de referencia, de categoría y de estado).
- Datos contables (por ej., remuneraciones, tasas de interés, depreciación, descuentos, costos unitarios de las existencias, etc.).
- Indicadores en los registros de¡ computador que dirigen los programas de aplicación a los valores apropiados de tablas (por ejemplo, tasas de depreciación) o a instrucciones específicas de un programa para registros de archivos especificados (por ejemplo, precios especiales a clientes, omisiones en los informes estándar de excepciones).

La significación de auditoría de los datos permanentes es que pueden ser utilizados por los programas de aplicación para generar valores y transacciones dentro del computador sin intervención humana o entradas adicionales. Dado que estos datos serán utilizados por programas en cada ciclo de procesamiento, ya sea para calcular los valores de las transacciones ingresadas o para generar transacciones y registraciones adicionales, es esencial que sean autorizados, completos y precisos al ser ingresados y que todos los cambios posteriores a los datos con significación de auditoría sean controlados adecuadamente por los usuarios. Una vez que un dato permanente ha sido modificado, afectará los procesamientos posteriores que utilicen dicho dato hasta que sea nuevamente modificado. Salvo mención en contrario, los controles tratados en esta sección son aplicados tanto a los datos de transacciones como a los datos permanentes.

Controles de edición y validación

La mayoría de las aplicaciones computadorizadas utilizan rutinas para editar y validar los datos ingresados, 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, por ejemplo, datos que están fuera de un determinado rango de razonabilidad. Este último mecanismo restringe la magnitud de los errores que podrían pasar inadvertidas. En una aplicación de liquidación de remuneraciones, por ejemplo, un control de validación puede evitar el procesamiento de un jornal a tarifas horarias superiores a las autorizadas por el convenio colectivo de trabajo.

Los controles de edición y validación normalmente son aplicados cuando se ingresan los datos, si el ingreso de datos es interactivo, el usuario recibirá inmediatamente la indicación de corregir los datos que contienen los errores o que no fueron ingresados correctamente. A menudo, los programas de edición y validación acumulan totales de control periódicos para verificar la integridad y exactitud del ingreso de datos a través de controles de sesión o listados de transacciones. Los listados de transacciones son copias impresas de todas las transacciones o datos permanentes ingresados cuyos detalles son posteriormente corroborados con los documentos fuente originales.

Los controles de edición y validación pueden contribuir significativamente a la exactitud de¡ ingreso de datos. Sin embargo, probablemente no sean los únicos controles en los cuales decidamos confiar. También deberíamos considerar otros controles de procesamiento y funciones de procesamiento computadorizadas que contribuyan a la exactitud de los datos. Por ejemplo, en las aplicaciones de cuentas a pagar puede verificarse la exactitud de las facturas ingresadas mediante una función computadorizada de comparación que rechace las facturas cuando las cantidades facturadas no concuerden con las cantidades pedidas y recibidas. Esta función puede proporcionarnos evidencia de control con respecto al ingreso de facturas, informes de recepción y órdenes de compra, y puede resultar más eficiente confiar en ella que en tres verificaciones de controles de edición y validación.

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.

CONTROLES DE EDICION Y VALIDACION

- *Controles de formato.* Los controles de formato aseguran que cada campo tenga el formato de datos apropiado (numérico, alfabético o alfanumérico) y la cantidad adecuada de caracteres.
- *Control de campos faltantes.* Los controles de campos faltantes son diseñados para asegurar que todos los campos de datos importantes hayan sido completados. Los controles de combinación se utilizan en forma similar para requerir que se ingresen datos en un determinado campo cuando se ingresan datos en campos conexos o dependientes.
- *Controles de límite o razonabilidad.* Los controles de límite son implantados para asegurar que los datos estén dentro de o no excedan ciertos límites. Los controles de límite identifican e impiden el procesamiento de una transacción irrazonable, por ejemplo, una remuneración horaria excesiva. Los controles de razonabilidad incluyen controles cruzados, por ejemplo, que las facturas de proveedores de servicios no sean imputadas a una cuenta de existencias.
- *Controles de validación.* Los controles de validación se utilizan para asegurar que los datos ingresados sean compatibles con los datos permanentes o del archivo maestro. Por ejemplo, una vez que se ha controlado el formato de los datos, el control de validación compara los datos ingresados (tales como códigos de proveedores, números de cuenta, etc.) con registros de los archivos maestros para determinar su validez.
- *Controles de procesamiento duplicado.* Los controles de procesamiento duplicado identifican los números de documento o lotes que son ingresados para su procesamiento más de una vez.
- *Pruebas de correlación o de combinación de campos de datos.* Estos controles comparan datos de diferentes campos para probar su razonabilidad en base a criterios especificados en los programas de aplicación. Por ejemplo, un sistema de liquidación de haberes puede controlar que no se efectúen pagos por horas extra al personal ejecutivo.
- *Códigos de integridad de campos.* Los códigos de integridad de campos se utilizan para verificar la exactitud de los datos durante el proceso de ingreso, incluyendo la transmisión de los mismos.
- *Controles de balanceo.* Estos controles aseguran que ciertas transacciones balanceen a cero, por ejemplo, débitos y créditos de un asiento de diario.
- *Dígitos verificadores.* Los dígitos verificadores son utilizados para verificar la integridad de un campo. Requieren del uso de un dígito adicional incluido en los campos numéricos (por ejemplo, números de cuenta). Como parte de la validación de datos, se realiza un cálculo con los otros dígitos cuyo resultado debe ser igual al dígito verificador. Este procedimiento es comúnmente utilizado para asegurar que se ingresen números de cuenta de clientes o proveedores correctos y válidos.

C.- Obtención de evidencia de control

Dentro de la prueba de los controles de edición y validación es necesario determinar si:

- Las rutinas de procesamiento programadas que contienen los controles de edición y validación funcionan de la manera esperada.
- Los controles que aseguran que las transacciones rechazadas sean identificadas y mantenidas en archivos en suspenso funcionan de la manera esperada y no puedan ser eludidos.
- Empleados autorizados de los departamentos usuarios han tomado las medidas adecuadas con respecto a las excepciones o errores incluidos en los listados generados por el computador.

Para completar estos pasos se requiere usualmente una combinación de pruebas para determinar la efectividad de los controles programados de edición y validación y para confirmar lo adecuado de las medidas tomadas por los empleados de los departamentos usuarios con respecto a las transacciones rechazadas y condiciones de error. Posteriormente se analizan las técnicas para evaluar los procedimientos de seguimiento que los departamentos usuarios llevan a cabo con respecto a transacciones rechazadas y condiciones de error.

2.4 Datos rechazados y partidas en suspenso

A.- Riesgo

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

B.- Medios de control

Una aplicación bien diseñada debe controlar cada transacción rechazada manteniendo un registro de la misma hasta que sea corregida. En la Tabla que sigue se enumeran los posibles controles programados sobre estas partidas en suspenso. Las partidas rechazadas deben ser incluidas en todos los informes de excepción posteriores hasta que el usuario apropiado o el grupo de control de datos tomen las medidas correctivas necesarias. Al ser reingresadas, las transacciones rechazadas deben ser sometidas a los mismos controles de edición y validación aplicables a las transacciones originales.

En un ambiente interactivo de ingreso de datos, la persona que ingresa la transacción es inmediatamente advertida de que existe una condición de error o excepción, a fin de que la misma sea corregida. También existe la posibilidad de que la transacción sea incluida en un archivo de partidas en suspenso para su posterior corrección y reprocesamiento, probablemente por un supervisor.

CONTROLES PROGRAMADOS SOBRE PARTIDAS EN SUSPENSO

- Se utilizan controles programados para asegurar su apareamiento en ciclos posteriores de procesamiento con los registros maestros, y la eliminación de las partidas apareadas del archivo de partidas en suspenso.
- Registración de todos los movimientos de ingreso y egreso de los archivos en suspenso, para proporcionar un rastro de auditoría. Los movimientos iniciados por medios manuales y los generados automáticamente por el sistema deben ser señalados por separado.
- Se utilizan controles de actualización para asegurar que los totales de control al inicio y cierre de cada ciclo de procesamiento puedan ser conciliados.
- Se preparan informes de excepción periódicos identificando claramente las partidas de valores inusualmente altos o pendientes desde hace mucho tiempo.
- Se preparan análisis periódicos de la antigüedad de las partidas pendientes.
- Se utilizan programas de consulta para listar todas o parte de las partidas en suspenso cuando se lo requiera.

La efectividad de estos controles programados dependerá de la efectividad de los

CONTROLES SOBRE PARTIDAS EN SUSPENSO

- Conciliación del movimiento neto de partidas en suspenso con los informes de actualización de archivos para cada ciclo de procesamiento.
- Control de todos los ajustes iniciados por los usuarios con documentos de ingreso autorizados.
- Investigación de las excepciones informadas por el sistema (por ejemplo, partidas pendientes y montos significativos antiguos) para determinar si se han tomado las medidas correctivas adecuadas, especialmente con respecto a los cortes contables.
- Los documentos usados para asignar, transferir o cancelar las partidas en suspenso deben ser sometidos, como mínimo, a los mismos controles aplicables a los demás documentos de ingreso. Estos documentos deben ser autorizados y controlados por la gerencia de los departamentos usuarios.

En algunos casos, los datos serán rechazados por el sistema, sin retenerse ningún tipo de registro en un archivo. En este caso, cobran importancia los procedimientos de seguimiento para asegurarnos que las transacciones rechazadas sean posteriormente analizadas y corregidas.

CONTROLES SOBRE TRANSACCIONES RECHAZADAS

- Mantenimiento de un registro de partidas rechazadas y de su posterior reprocesamiento.
- Preparación de lotes separados de rechazos corregidos. Este procedimiento nos permite asegurarnos de que todos los rechazos sean investigados y corregidos.
- Corrección de los rechazos por errores en los documentos fuente a cargo del departamento usuario emisor de éstos; devolución de los documentos corregidos para su reprocesamiento bajo los controles normales de ingreso, incluyendo autorización.
- Análisis periódicos de rechazos, por significatividad, causa, antigüedad y corte.
- Esto permite a la gerencia determinar si los rechazos son causados por procedimientos de ingreso inadecuados y evaluar el impacto de dichos errores.
- Detalle de los rechazos pendientes al cierre de cada período contable.
- Procesamiento manual de datos rechazados (por ejemplo, preparación manual de una factura de venta o boleta de contado). Este control es ineficiente, pero puede ser viable cuando los volúmenes de rechazos son muy bajos. En estos casos, los datos computadorizados relacionados deben ser actualizados de inmediato con las transacciones manuales, las que deberán ser adecuadamente autorizadas.

Para contribuir a una adecuada segregación de funciones, la autoridad para vulnerar las condiciones de excepción debe ser limitada. Puede ser necesario prohibir las correcciones on line de ciertos tipos de errores o excepciones, por ejemplo, un pago de remuneraciones inusualmente grande o un desembolso a un proveedor no autorizado. Asimismo, el personal del departamento CIS no debería estar autorizado a realizar dichas correcciones.

C.- 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 apareados 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 responsable de asegurar que estas transacciones sean posteriormente corregidas.

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

- En archivos separados físicamente.
- En registros separados dentro de los 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 apareadas 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.

La corrección de las partidas en suspenso puede ser efectuada automáticamente por el computador o a través de ajustes ingresados por el usuario. En ambos casos, el usuario es responsable del correcto procesamiento de los datos.

D.- Obtención de evidencia de control

La prueba de los controles programados sobre partidas en suspenso puede incluir los siguientes pasos:

- Examinar las conciliaciones efectuadas por el cliente de los movimientos de ingreso y egreso de los registros en suspenso,
- Determinar que el cliente cumpla con los procedimientos de revisión y seguimiento de las partidas en suspenso.
- Obtener el listado de partidas en suspenso pendientes; seleccionar algunas partidas y determinar que las transacciones hayan sido correctamente registradas y/o eliminadas del archivo en suspenso.
- Diseñar y utilizar transacciones de prueba para confirmar que las transacciones inválidas son rechazadas e incluidas en archivos en suspenso e informes de excepción que serán investigados por el departamento usuario correspondiente.

A fin de evaluar si los procedimientos de seguimiento de los departamentos usuarios relativos a las transacciones rechazadas funcionan apropiadamente pueden aplicarse los siguientes procedimientos:

- Controlar la conciliación de¡ movimiento neto de¡ total de partidas rechazadas.
- Seleccionar y examinar una muestra de transacciones incluidas en los informes de excepciones o errores durante el período bajo examen y:
  - Determinar, a través de observación e indagación, si las excepciones han sido resueltas por personal del departamento usuario correspondiente.
  - Determinar que las transacciones hayan sido reingresadas para su procesamiento de acuerdo con los procedimientos establecidos.

- Diseñar y utilizar transacciones de prueba para determinar que las transacciones inválidas son adecuadamente rechazadas e informadas.

2.5 Procesamiento y registración de transacciones

A.- 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 o inexacta o en el período contable incorrecto.

B.- Medios de control

Si el formato de los datos no es correcto o si su compatibilidad con los datos existentes no ha sido verificada o si los programas de aplicación del cliente no funcionan de la manera deseada, los registros contables relevantes pueden ser actualizados en forma incorrecta o incompleta, o no ser actualizados durante el procesamiento. Los controles que pueden mitigar este riesgo serán descriptos a continuación.

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. Como alternativa, se puede efectuar una conciliación manual de los documentos utilizados.

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. Los totales de los campos críticos por tipo de transacción son automáticamente acumulados durante la sesión de ingreso interactivo de datos y conservados para su. posterior comparación con los saldos actualizados.

CONTROLES DE SESION

- A medida que los datos son ingresados, se deben acumular en un archivo de transacciones los totales de Control separados para cada terminal y para cada tipo de transacción.
- Al final de la sesión, el computador registra e informa el total de partidas acumuladas en el archivo de transacciones.
- Una vez actualizado el archivo maestro, se aplican los siguientes procedimientos:
  - Actualización de los registros de control del archivo maestro en base al registro de control del archivo de transacciones.
  - Acumulación programada de los registros individuales del archivo maestro para su conciliación con el registro de control de dicho archivo.
  - Emisión de un informe de actualización del archivo maestro, incluyendo el saldo total al inicio del ciclo, total de movimientos del día por tipo de transacción y saldo total al final del ciclo.

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. La comparación puede ser efectuada para asegurarse de que todos los documentos han sido. Procesados y que no se han ingresado transacciones desde fuentes, no autorizadas.

Ocasionalmente, en reemplazo de los controles por lotes, los listados de transacciones pueden ser cotejados con los documentos de ingreso de datos (es más usual

que esto se realice en el caso de modificaciones a los datos permanentes, que suelen ser de bajo volumen, que para datos de transacciones).

CONTROLES POR LOTES

- Preparación de totales de control/ciegos de los campos considerados críticos. Los totales ciegos son totales de control generados mediante la suma de campos numéricos en los lotes de documentos. Si bien carecen de sentido por sí mismos, estos totales pueden ayudar a identificar errores u omisiones, la suma de los códigos de cuenta utilizados en un lote de asientos de diario es un ejemplo de total ciego. Si uno o más de los códigos de cuenta fuesen ingresados incorrectamente, el total de los códigos ingresados no coincidiría con el total ciego.
- Preparación y aprobación de carátulas de lote y formularios de detalle de envíos, que incluyan totales de control para su posterior balanceo. La aprobación de estos formularios por la gerencia de las áreas usuarias contribuye a asegurar que los lotes ingresados para su procesamiento provienen de fuentes autorizadas.
- Control numérico de los lotes, que ayuda a detectar lotes no autorizados e identificar lotes faltantes.
- Mantenimiento de un registro de control por lotes. Este registro debe ser mantenido por cada departamento usuario para facilitar el seguimiento de los lotes remitidos para procesamiento y para detectar modificaciones a los lotes una vez que éstos salen del departamento usuario. Los controles que aseguran que el último lote de cada período contable sea procesado son particularmente importantes.
- Conciliación por personal de los departamentos usuarios de los totales de control con los totales de salida, para establecer que no se hayan perdido o agregado datos durante el procesamiento y para asegurar la exactitud del ingreso y procesamiento de datos. El individuo responsable por la conciliación no debe tener responsabilidades incompatibles, tales como la preparación de datos.
- Mantenimiento de un registro de lotes con errores y la naturaleza de éstos. Este registro resulta valioso, ya que la existencia de errores frecuentes o recurrentes puede indicar que no se siguen procedimientos adecuados.
- Balanceo de totales de lote, es decir, cálculo y conciliación de los totales de control con los datos de las carátulas de lotes.

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. Los posibles controles de balanceo programados son enumerados en la siguiente Tabla.

CONTROLES DE BALANCEO PROGRAMADOS

El saldo inicial del ciclo de procesamiento corriente es igual al saldo final del ciclo anterior (controles de ciclo a ciclo).

La suma de[saldo inicial más las transacciones procesadas es comparada con el saldo final del ciclo corriente (controles de actualización de archivos),

El saldo después del primer programa o paso de procesamiento del ciclo corriente es comparado con el saldo inicial más las transacciones procesadas en ese paso de procesamiento, y así sucesivamente a través de cada paso sucesivo del sistema (controles de programa a programa).

- El total de los saldos de los registros individuales después de la actualización es comparado con el saldo neto del archivo de control (controles de revisión y acumulación).
- El programa que lee o procesa el archivo calcula en forma independiente la cantidad de registros contenidos en el mismo y su valor. Estos totales son luego comparados con el registro de control del archivo para asegurar que el mismo ha sido íntegramente procesado (controles de registro).
- Los campos críticos por tipo de transacción son automáticamente totalizados durante la sesión de ingreso de datos para su posterior comparación con los saldos actualizados (controles de sesión, solamente en sistemas interactivos).
- En sistemas de actualización inmediata de archivos, mantenimiento de un registro de control del archivo maestro, incluyendo:
  - Resumen de las transacciones traspasadas desde el registro diario de transacciones (log).
  - Total de los saldos al inicio de cada día o turno.
  - Total de los saldos al final de cada día o turno, Este total debe ser conciliado

con la suma de los dos puntos anteriores.

- En sistemas de base de datos, revisiones programadas periódicas del contenido de dicha base a fin de acumular las partidas individuales para su conciliación con un registro de control.
- En sistemas contables integrados en los cuales existe una actualización inmediata de dos o más archivos, balanceo periódico de los registros de control de cada archivo.

Control de rótulos internos 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 controles para asegurar la exactitud e integridad del proceso de transmisión de datos son enumerados en la siguiente Tabla . Los dispositivos estándar del software de transmisión de datos producen un cálculo de "prueba" (utilizando un algoritmo preestablecido) con la información incluida en la transmisión. El resultado de dicho algoritmo es registrado en un mensaje de encabezamiento previo a la transmisión. Cuando el mensaje es recibido se realiza el mismo cálculo y el resultado es comparado con la información registrada en el encabezamiento. Si se detectan diferencias en el proceso anterior se le solicitará al remitente que vuelva a transmitir la información.

CONTROLES DE TRANSMISION DE DATOS

- Registro y recálculo de la "prueba" en los mensajes de encabezamiento.
- Confirmación de partidas individuales o de grupos de partidas ingresadas al sistema retransmitidos a las terminales para ser leídos o impresos.
- Numeración secuencial de las partidas por el computador, utilizando códigos de identificación específicos para cada transacción ingresada desde cada terminal.
- Generación de informes de números de secuencia faltantes o duplicados.
- Utilización de registros de final de transmisión para verificar que todas las partidas hayan sido correctamente transmitidas.

Procedimientos 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 inmediata. En estas situaciones, no se dispondrá de documentos impresos de respaldo (back up) y la posibilidad de determinar si una transacción. fue completamente procesada antes de la interrupción quedará anulada.

PROCEDIMIENTOS DE REENGANCHE Y RECUPERACION

- Procedimientos para la recreación de los datos permanentes en caso de destrucción o pérdida. Dichos procedimientos pueden incluir :
- Copiado o vuelco cíclico (dumping) de los datos permanentes a cintas o discos. A intervalos preestablecidos se copia el contenido de los archivos creados o modificados desde el vuelco anterior. La frecuencia de los vuelcos debe ser determinada en función del volumen, sensitividad de los datos, frecuencia de procesamiento, etc.
- Retención de los archivos de transacciones y documentos de ingreso posteriores a la más reciente copia de los datos permanentes.
- Mantenimiento de registros de transacciones u otros registros de datos actualizados para la recuperación automática de transacciones procesadas parcialmente.
- Impresión periódica o específica de los registros de transacciones para identificar los pasos de procesamiento completados para las partidas individuales.
- Definición de los períodos de retención de los duplicados de archivos de datos permanentes y de transacciones.
- Prueba periódica de los procedimientos automáticos de recuperación.
- Actualización de un duplicado de¡ archivo de datos permanentes simultáneamente con el archivo principal. Este es un procedimiento alternativo al vuelco cíclico en algunas aplicaciones interactivas.
- En los sistemas de base de datos:
- Registro de imágenes "antes y después" de los elementos de datos actualizados.
- Utilización de programas utilitarios para controlar la coherencia de los indicadores internos de la base de datos u otros vínculos entre los elementos de datos.
- Prevención y/o detección de situaciones de "bloqueo" (deadiock) durante el procesamiento
- Mantenimiento de registros de transacciones separados físicamente de la base de datos.

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.

CONTROLES DE CORTE PROGRAMADOS

- Tablas calendario incluidas en el software de aplicación para comparaciones internas con las fechas de las transacciones.
- Procedimientos para controlar el procesamiento completo y oportuno de los datos ingresados.
- Informes de las excepciones a los criterios de corte.
- Controles de rótulos de encabezamiento de archivos para asegurarse de que al cierre de cada período contable se actualicen las versiones correctas de los archivos de datos.
- En sistemas de procesamiento distribuido de datos:
- Conciliación de los datos procesados localmente en un determinado período
- con los ingresados para procesamiento central.
- Conciliación de los saldos de los archivos locales y centrales al cierre de cada período.
- En los sistemas contables integrados, procedimientos para asegurar que se
- mantenga un rastro de auditoría para los totales de control y para las transacciones individuales transferidas entre sistemas (es decir, bajo control de programas).
- En sistemas de base de datos, controles para asegurar un adecuado corte entre los datos de cada día.

Cuando los sistemas de actualización diferida de archivos son integrados, los sucesivos pasos de procesamiento son ejecutados por subsistemas separados, en orden lógico, siendo los lotes de datos transferidos progresivamente de una aplicación a la otra. En estos sistemas, habitualmente encontraremos un rastro visible de controles de ciclo a ciclo, que permite la conciliación de los totales de ingreso originales con los totales de actualización de archivos.

En los sistemas de actualización inmediata, los datos relacionados con más de una aplicación pueden ser actualizados simultáneamente. Por ejemplo, una transacción de venta puede actualizar simultáneamente los registros de cuentas a cobrar y existencias. En estos sistemas los controles tradicionales de ciclo a ciclo pueden no existir, y el potencial de pérdida del rastro de auditoría es significativo. Los totales de control de sesión para la actualización de cada archivo de datos deben ser informados a los usuarios para ser conciliados.

Muchos sistemas automáticamente generan transacciones o realizan cálculos en los que la gerencia confía sin revisión ulterior. Por ejemplo, algunos sistemas computadorizados de compras y cuentas a pagar tienen acceso a información de lotes óptimos de compra, y no sólo calculan puntos de pedido sino que también generan órdenes de compra de reaprovisionamiento por las cantidades óptimas.

Con frecuencia, estos sistemas no utilizan documentos fuente impresos para respaldar las transacciones generadas o los cálculos efectuados fuera de los documentos creados por el sistema. En estos sistemas, los controles de balanceo programados, los controles de rótulos internos de archivos y los controles de transmisión de datos (todos los cuales han sido tratados anteriormente) son de suma importancia. Asimismo, cuando resulte posible, deben incorporarse controles para validar las transacciones generadas automáticamente y para prevenir o detectar transacciones erróneas. Tal como sucede en relación con el ingreso de datos, las instrucciones de los programas deben incluir rutinas de edición y validación,

CONTROLES SOBRE DATOS GENERADOS Y CALCULOS PROGRAMADOS

- Recuento de los registros de archivos leídos para la generación de datos.
- Controles de actualización de archivos y balanceo para las transacciones generadas.
- Conciliación de los recuentos de registros y actualizaciones de archivos informadas.
- Controles de razonabilidad sobre los datos generados.
- Revisión post-procesamiento de la autorización y razonabilidad de las transacciones y cálculos (para una muestra de partidas individuales y global).
- Secuencia numérica de las transacciones generadas.
- Mantenimiento de un registro de transacciones generadas por el sistema (rastro de auditoría).
- Emisión de una copia impresa de los datos generados para su posterior autorización, revisión y conciliación por los usuarios.
- Revisión y seguimiento de partidas significativas incluidas en los informes de excepción.
- Controles sobre cambios a los datos permanentes utilizados para la generación de datos.

Extracción y presentación de información contable y gerencial

A menudo se extrae información contable y gerencial de los archivos actualizados para preparar estados financieros e informes gerenciales, por ejemplo:

- Informes de excepción de saldos (por ejemplo, cuentas a cobrar con antigüedad superior a X días).
- Totales, resúmenes y análisis de archivos (por ejemplo, análisis por antigüedad de cuentas a cobrar vencidas).
- Cálculo de provisiones y devengamientos (por ejemplo, cálculo de la previsión para deudores incobrables).

- Gráficos y estadísticas gerenciales (por ejemplo, estratificación de créditos por valor o categoría de ventas.

Esta información podrá ser presentada diaria, mensual, trimestral o anualmente o a pedido, según las necesidades de la gerencia. Si esta información es considerada como una fuente potencia¡ de evidencia de auditoría, el auditor debe ser consciente del riesgo de errores en la lógica de los programas de aplicación que ocasionen que la información de salida sea incompleta o inexacta, por ejemplo:

- Lectura incompleta de los registros o campos de datos de un archivo (bypassing).
- Exclusión de registros, campos de datos o transacciones relevantes de los informes resumen o de excepción.
- Duplicación de información en las salidas de¡ computador.
- Cálculos incorrectos aplicados a los datos antes de su extracción y presentación.
- Totales informados que no representan los valores de los saldos o transacciones individuales.
- Inclusión de campos de datos incorrectos en informes resumen (por ej., debido a la definición de indicadores de programa incorrectos).
- Uso de códigos incorrectos de resumen y categorización de datos por los programas de aplicación.
- Presentación de información por un período contable incorrecto.
- Modificaciones a los datos después de su extracción de los archivos, mientras son mantenidos en archivos intermedios o de impresión, debido a una lógica errónea de los programas de impresión.

El auditor debe ser también consciente de la actual tendencia hacia la utilización de herramientas de computación por parte de los usuarios finales ; el riesgo mencionado precedentemente se incremento cuando los usuarios no tienen un adecuado conocimiento de programación:

- Uso de lenguajes de cuarta generación (4GLs) para recuperar información, en forma regular o a pedido (incluyendo cálculos) de archivos de datos, para su propio uso y bajo su propio control.
- Uso de hardware y software para bajar (download) datos desde un mainframe a un microcomputador para su posterior análisis, resumen, e información utilizando software basado en microcomputadores.

- Análisis de los datos "bajados" a un microcomputador que luego son transferidos a archivos de un mainframe (uploading) para su posterior resumen, etc. e información.
- Ingreso de parámetros proporcionados por paquetes de aplicación, que permiten variar cálculos, generar datos, resúmenes, totalizaciones, criterios de selección, etc., de una corrida de un programa a otro.
- Uso de software de planillas electrónicas para generar información contable y gerencia¡, con el riesgo adicional de que se apliquen fórmulas incorrectas o inexistentes, falta de controles de balanceo, etc.

La existencia de un rastro de auditoría adecuado es un procedimiento importante para asegurar que la gerencia pueda identificar las transacciones y saldos individuales incluidos en los totales v resúmenes del computador

CONTROLES SOBRE LA EXTRACCION Y PRESEIVTACION DE INFORMACION CONTENIDA EN ARCHIVOS MAGNETICOS

Procedimientos programados

- Rastro de auditoría para identificar la inclusión de transacciones y saldos individuales en totales y resúmenes emitidos por el computador.
- Recuento de los registros de archivos leídos en el análisis y extracción de datos.
- Controles de razonabilidad aplicados a los totales y resúmenes del computador.
- Conciliación de los totales y resúmenes del computador con los registros de control de archivos.
- Controles de registros faltantes y duplicados.
- Controles de programa a programa cuando se utiliza más de un programa en secuencia para el análisis, extracción y presentación de datos.

Procedimientos del usuario

- Conciliación de totales generados por el computador con la información de salida relacionada.
- Controles de razonabilidad de la información de salida (global y muestras).
- Conciliación de los informes de recuento de registros con registros manuales y la información de salida relacionada.
- Especificación de los criterios para informes de excepción.
- Adecuado seguimiento de los informes de excepción.
- Distribución restringida de información de salida confidencial.

C.- Obtención de evidencia de control

La prueba de los controles con respecto a la integridad y exactitud del procesamiento puede incluir procedimientos para determinar si :

- Las rutinas programadas funcionan de la manera esperada.
- Los controles programados que aseguran que las transacciones rechazadas sean identificadas e incluidas en archivos en suspenso funcionan de la manera esperada y no pueden ser vulnerados.
- El personal de los departamentos usuarios ha tomado medidas apropiadas con respecto a las excepciones o errores.

Para completar estos pasos se requiere usualmente una combinación de procedimientos para determinar la efectividad de las funciones y controles programados, y para confirmar lo apropiado de las medidas tomadas por los empleados de los departamentos usuarios con respecto a las transacciones rechazadas y a los errores. Posteriormente se tratan las pruebas de los procedimientos de seguimiento a cargo de los departamentos usuarios en relación con las transacciones rechazadas y a los errores.

Con frecuencia, el uso de transacciones de prueba es la forma más directa y eficiente de probar las funciones y controles de procesamiento computadorizado.

Documentos fuente prenumerados

Si el software de aplicación ha sido programado para asignar números de referencia a las transacciones ingresadas para procesamiento, controlar su secuencia numérica y producir informes de excepción de los documentos faltantes, puede evaluarse este control de la siguiente manera:

- Obteniendo los informes de excepción y verificando que las excepciones informadas hayan sido adecuadamente seguidas.
- Utilizando técnicas de auditoría asistidas por computador, tales como:
  - Técnicas de transacciones de prueba (datos de prueba o procedimientos de prueba integrada).
  - Módulos de auditoría incorporados a los programas.

Controles por lotes

Si los controles por lotes sobre el ingreso de datos son considerados clave, puede probarse su efectividad de la siguiente manera:

- Recalculando los totales de control por lotes a partir de los documentos fuente.
- Siguiendo lotes seleccionados hasta el registro de control de datos.
- Verificando, para períodos seleccionados, que la función de control de datos haya comprobado la secuencia numérica de los lotes a través de todas las etapas del procesamiento.
- Verificando, para períodos seleccionados, que las transacciones rechazadas sean prontamente resueltas.
- Confirmando que los procedimientos de revisión de la autorización de los datos ingresados para procesamiento sean efectivos.
- Probando los procedimientos existentes para la cancelación de los documentos de ingreso.

Controles de sesión

Dado que los controles de sesión son efectuados por el software de aplicación, el único método efectivo para probar los mismos es a través de técnicas de transacciones de prueba. Si la aplicación ha sido programada para generar informes de excepción posteriores a la actualización, será necesario determinar que las excepciones informadas sean analizadas y resueltas en un plazo razonable.

Controles de balanceo programados

Al igual que los controles de sesión, los controles de balanceo programados son efectuados por el software de aplicación y sólo pueden ser probados en forma efectiva mediante el uso de técnicas de transacciones de prueba,

Controles de transmisión de datos

Por lo general, no es necesario preocuparse acerca de los dispositivos estancar del software de control de telecomunicaciones, una vez que se ha establecido que se utiliza el paquete apropiado y que el algoritmo de cálculo ha sido correctamente implantado. En ciertas ocasiones, especialmente en instituciones financieras, en las que montos

significativos de fondos son transferidos automáticamente en base a transmisiones de datos, los procedimientos y controles de transmisión podrán merecer una consideración especial. En este caso, se trata de un área especializada que escapa al alcance de este volumen.

Procedimientos de reenganche y recuperación

Los procedimientos de reenganche y recuperación pueden ser probados de la siguiente manera:

- Determinar, a través de una revisión de los registros del computador (logs) y de indagaciones al personal de los departamentos usuarios y CIS, la frecuencia de fallas del sistema y el nivel de conocimiento y satisfacción que de los procedimientos de recuperación tienen los usuarios.
- Comprobar, para una muestra de días en los cuales se suscitaron fallas, que se hayan seguido procedimientos de recuperación adecuados.
- De no haber habido fallas en el sistema, controlar que los procedimientos de recuperación hayan sido claramente definidos y documentados, y que hayan sido probados.
- Controlar que los registros de datos (logs) sean revisados y retenidos verificando que se mantengan copias de los archivos maestros según lo establecido.

Transacciones generadas

La prueba de los controles sobre transacciones generadas puede incluir:

- Controlar, por referencia a los datos fuente, que los datos sean generados en el momento correcto.
- Confirmar que los usuarios hayan revisado las salidas impresas, tanto por partidas individuales como globalmente, y que las partidas inusuales hayan sido investigadas.
- Seleccionar, de las salidas impresas, una muestra de transacciones generadas y:
  - controlar los datos permanentes con los registros del usuario tales como nóminas de personal y listas de precios.
  - controlar las imputaciones contables con las copias impresas del mayor general
  - controlar cálculos y sumas
  - revisar las salidas impresas y obtener explicaciones satisfactorias de los usuarios acerca de las partidas más significativas o inusuales
  - comparar los totales con registros del usuario

- Controlar las conciliaciones efectuadas por los usuarios de los informes de actualización de archivos.
- En ausencia de salidas impresas adecuadas, utilizar datos de prueba para controlar el correcto funcionamiento de los programas más importantes.

Cálculos programados

Los controles sobre cálculos programados pueden ser probados mediante:

- Selección, a partir de las salidas impresas, de una muestra de transacciones y recreación de los cálculos para comprobar su exactitud.

- Utilización de datos de prueba para controlar el correcto funcionamiento de los programas de cálculo.

3. Obtención de Información Adicional sobre los Riesgos del Departamento CIS

3.1 Introducción

Los controles generales son aquellos controles que contribuyen a la efectividad de los controles directos. No proporcionan satisfacción directa en relación con las aserciones correspondientes a los componentes. Si pensamos confiar en los controles directos como fuente de evidencia de auditoría para las aserciones, debemos considerar si las debilidades de los controles generales pueden afectar la efectividad de los controles directos. Los controles generales incluyen:

- Controles del departamento CIS.
- Segregación de funciones incompatibles.

A continuación trataremos los riesgos del departamento CIS que pueden ser importantes para nuestros trabajos en clientes que utilizan sistemas computadorizados, y los controles, generalmente conocidos como controles generales, diseñados para reducir estos riesgos a un nivel aceptable.

El determinar si los controles existentes proporcionan una base adecuada para obtener confianza de auditoría es una cuestión de criterio profesional. La efectividad de los controles depende de los riesgos existentes en el ambiente específico del cliente, la

naturaleza de los controles implantados, la forma en que fueron implantados y su vinculación con otros controles.

No siempre se dará el caso que en todos los clientes existan todos los controles descriptos en las secciones de medios de control. En algunos casos, uno de los controles descriptos puede ser suficiente para reducir el riesgo a un nivel aceptable. En otros casos, probablemente sea necesaria una combinación de controles. También encontraremos clientes en los que no se ha implantado ninguno de los controles aquí descriptos aunque cuentan con otros controles que mitigan los riesgos existentes.

No se debe suponer automáticamente que los controles del departamento CIS son iguales para todos los controles directos, ya que ciertos controles del departamento CIS pueden ser específicos para determinadas aplicaciones o quizás existan variaciones entre los controles directos para la misma aplicación. Por ejemplo, el software de control de acceso puede ser utilizado para restringir el acceso a diversos sistemas de aplicación. No obstante, la efectividad de dicho software a menudo depende de los parámetros especificados por separado para cada control de procesamiento y función de procesamiento computadorizada.

Los tres riesgos típicos que pueden ser reducidos a niveles aceptables mediante la implantación de controles del departamento CIS son los siguientes:

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

Desde una perspectiva de auditoría, nos interesamos en la efectividad de los controles directos, incluyendo las funciones de procesamiento computadorizadas, ya que pueden proporcionar evidencia directa con respecto a las aserciones, No obstante, también nos interesaremos en los controles generales ya que éstos pueden contribuir a la efectividad de los controles directos. Los controles generales no suelen ser considerados como controles clave por sí mismos; sin embargo, en la medida en que influyan sobre la confiabilidad de los controles directos clave, incluyendo las funciones de procesamiento computadorizadas, los controles directos y controles generales podrán, en conjunto, ser considerados controles clave.

Consideración de debilidades en los controles del departamento CIS

Es necesario considerar el efecto de las debilidades de los controles del departamento CIS sobre los respectivos controles directos potencialmente clave. Si esas debilidades afectan significativamente la confiabilidad de los controles directos potencialmente clave, el equipo a cargo del trabajo debe considerar las siguientes alternativas:

- Identificar los controles directos potencialmente clave alternativos que proporcionen satisfacción para las aserciones pero que no sean afectados por las debilidades identificadas en los controles del departamento CIS.
- Realizar procedimientos sustantivos para determinar si las debilidades de los controles del departamento CIS han afectado la operación de los controles directos potencialmente clave durante el período. Por ejemplo, el software de administración de bibliotecas podría ser utilizado para generar informes de modificaciones a programas específicos para su posterior investigación, cuando los controles sobre dichos cambios son débiles.
- Reevaluar el alcance de los procedimientos sustantivos utilizados para obtener satisfacción para las aserciones.

Muchos de los controles descriptos)en esta sección son aplicables a los ambientes "típicos" de un cliente. La ausencia de los controles que aquí se analizan, especialmente en sistemas pequeños, no significa necesariamente que no se podrá depositar confianza en el sistema. Pueden existir controles mitigantes que reducen el riesgo a un nivel aceptable. Por ejemplo:

- Una segregación de funciones del departamento CIS menor a lo deseable puede ser mitigada por procedimientos del departamento usuario tales como una estrecha supervisión gerencia¡ del computador y restricción física del acceso a los archivos y programas de datos.
- El riesgo de cambios no autorizados a los programas puede ser significativamente reducido si el cliente sólo usa software comprado a terceros y no se tiene acceso al código fuente.
- El riesgo de acceso no autorizado por terceros puede no ser significativo si los terceros normalmente no tienen acceso al sistema y no se utilizan telecomunicaciones.

Es importante recalcar que la naturaleza de los sistemas computadorizados del cliente puede ser más importante que la magnitud de su negocio para decidir si el cliente tiene un "sistema de computación pequeño". Existen pequeñas empresas que poseen

sistemas sofisticados, y organizaciones más grandes, particularmente las de procesamiento descentralizado o distribuido que tienen "sistemas de computación pequeños".

3.2 Estructura organizativa y procedimientos de operación CIS

A.- Riesgo

La estructura de organización y los procedimientos operativos del Departamento CIS no garantizan un ambiente de procesamiento de datos que conduzca a la preparación de información financiera confiable.

B.- Medios de control

Para que los controles directos resulten efectivos, las actividades de¡ departamento CIS deben estar organizadas de tal manera que:

- Los empleados del Departamento CIS no realicen funciones incompatibles.
- Las actividades de los programadores de sistemas y otros empleados técnicamente capacitados sean supervisadas y la utilización de software sensitivos sea adecuadamente controlada.

Segregación de tareas en el Departamento CIS

En un departamento CIS centralizado típico, es conveniente separar las responsabilidades relativas a cada una de las siguientes funciones:

- Administración.
- Análisis de sistemas, diseño y programación de aplicaciones.
- Mantenimiento de¡ 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 microcomputadores.

Es posible que a medida que aumente la sofisticación y complejidad de los sistemas de información de una organización, se emplee personal mejor capacitado, se utilicen recursos más sofisticados y se asigne al personal funciones de una mayor especialización. Debemos evaluar las funciones que puede llevar a cabo la gerencia del Departamento CIS, los programadores de sistemas, los programadores de aplicaciones y los operadores.

ESTRUCTURA ORGANIZATIVA CIS

Segregación de las funciones de los usuarios

- El personal CIS tiene prohibida la iniciación y aprobación de transacciones.
- El personal CIS tiene prohibido el acceso a registros contables preparados manualmente, excepto documentos fuente.
- Los documentos fuente son manipulados dentro de¡ departamento CIS sólo por personal de las áreas de preparación y control de datos.

Segregación dentro del Departamento CIS

- Las siguientes funciones son llevadas a cabo por diferentes personas:
  - Gerencia
  - Análisis de sistemas, diseño y programación de aplicaciones
  - Mantenimiento del software de sistemas (apoyo técnico)
  - Operación del computador (incluyendo la biblioteca de archivos)
  - Control de datos
  - Seguridad de datos
- Los analistas y programadores de sistemas tienen prohibida la puesta en marcha y operación del computador, incluso para prueba de programas.
- Los programadores no tienen acceso directo a las bibliotecas de programas o a los archivos de datos utilizados para las corridas de producción.
- Los operadores tienen prohibido efectuar cambios a los programas y datos.
- Existen procedimientos adecuados en lo referente a :
  - Rotación de tareas/turnos
  - Vacaciones
  - Finalización de la relación laboral (por ej.: relevo inmediato, anulación de contraseñas, etc.)

Administración de base de datos (DBA)

- Segregación de la función de DBA de:
  - Control operativo diario del sistema
  - Implantación y ejecución de procedimientos de seguridad
  - Ejecución de procedimientos de reenganche y recuperación
  - Diseño y codificación de programas de aplicación
  - Análisis y programación de sistemas
  - Gerencia de departamentos usuarios

Sistemas computadorizados pequeños

En los sistemas computadorizados pequeños, los usuarios pueden efectuar funciones que tradicionalmente tiene a su cargo el personal del Departamento CIS. La gerencia debe tratar de compensar la falta de segregación de ciertas funciones diseñando sistemas que tengan tanta segregación de funciones como sea posible e implantando controles compensatorios como los descriptos en la Tabla.

SEGREGACION DE FUNCIONES - POSIBLES CONTROLES COMPENSATORIOS

- Responsabilizar a los departamentos usuarios por :
  - Mantener registros por tipo de transacción.
  - Los totales de control del archivo de datos permanentes.
  - Conciliar los datos ingresados para su procesamiento con la información de salida.
  - Revisar todos los datos de entrada e informes de salida considerados significativos.
- Supervisión permanente de las operaciones del computador.
- Ubicación de los equipos de computación en áreas a la vista de la gerencia.
- Retirar el compilador del sistema y restringir el acceso al mismo.
- Retirar los utilitarios sensitivos del sistema y restringir el acceso a los mismos.
- Restringir el acceso a las funciones de procesamiento de los programas de aplicación a través del uso de menúes y/o software de control de acceso.

Controles operativos del departamento CIS

Una efectiva segregación de funciones incompatibles en ambientes computadorizados requiere que se restrinja el acceso del personal a los programas de aplicación y de sistemas y a los datos. Para ello, muchas empresas implantan controles especialmente diseñados para restringir el acceso (o supervisar los accesos otorgados) y asegurarse de que no se lleven a cabo actividades no autorizadas, Los controles descriptos en esta sección incluyen:

- Manuales de operación y controles operativos diarios.
- Supervisión de usuarios privilegiados.
- Control sobre software sensitivos.
- Controles sobre el desarrollo de sistemas.

C.- 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. Los operadores del computador, por ejemplo, deben contar con instrucciones escritas a ser seguidas ante una eventual interrupción del procesamiento y para su reinicio. 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.

CONTROLES OPERATIVOS DIARIOS

- En todos los turnos existen supervisores o jefes de turno.
- Los registros de operación son revisados por la gerencia.
- Los trabajos realizados en cada turno son comparados con un cronograma.
- Las corridas no previstas en el cronograma deben ser autorizadas antes de ejecución,
- Se utilizan rótulos internos de encabezamiento para todos los archivos en cinta o disco.
- Se mantienen bibliotecas separadas de producción y prueba,
- Los programas de aplicación utilizados para el procesamiento de transacciones sólo pueden ser obtenidos de la biblioteca de producción.
- Existen controles de software de biblioteca para verificar que la versión correcta de un programa es utilizada.
- El software de programación de tareas es utilizado para asegurar que sólo se realicen las tareas autorizadas.

Supervisión de usuarios privilegiados

Los usuarios privilegiados son aquellos que tienen prerrogativas especiales, o acceso especial a los sistemas o información que podría permitirles llevar a cabo funciones conflictivas. Algunos empleados (por ej.: programadores de sistemas y funcionarios a cargo de la seguridad de datos) pueden necesitar acceso a información especial a fin de poder cumplir efectivamente su tarea. Las actividades de los usuarios privilegiados deben ser estrictamente supervisadas para asegurarse de que sólo ejecuten las funciones autorizadas.

Control sobre software sensitivos

El software de sistemas controla el funcionamiento de un computador. Aunque no procesa los datos contables, 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 saltear 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 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 SUPERZA están diseñados para facilitar "arreglos rápidos" del software de sistemas, programas objeto y archivos de datos, evitando de esa forma inconveniente o demoras en el procesamiento. De igual forma, los editores 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.

Para controlar el uso de estas herramientas de software es preciso limitar la cantidad de personas que pueden acceder a las mismas y supervisar su uso.

Controles sobre el desarrollo de sistemas

Es clara la importancia de los sistemas de aplicación en la contabilización, procesamiento e información de los datos de la organización. Tanto la gerencia como los auditores pueden estar interesados en el proceso de desarrollo de sistemas de un cliente. A la gerencia le interesa porque le permite asegurarse de que los sistemas están adecuadamente diseñados, probados e implantados y que se han incluido controles adecuados. A los auditores les interesa porque les permite determinar que los sistemas que procesan la información significativa para los estados financieros incluyen, una vez implantados, controles adecuados y operan de la manera esperada. Los procedimientos para el desarrollo, prueba e implantación de sistemas deben ser realizados en conformidad con las normas adoptadas por el Departamento CIS.

CONTROLES SOBRE SOFTWARE SENSITIVOS

- Todas las nuevas incorporaciones a la biblioteca de software deben ser autorizadas.
- El acceso a y uso de las funciones de los software sensitivos están limitados (por medio de software de control de acceso) a aquellos empleados que las requieren para cumplir con las tareas asignadas.
- El uso de software sensitivos es supervisado mediante un software de control de acceso que genera un registro automático (log) cada vez que se utiliza.
- Todas las instancias de uso de estas herramientas son registradas e informadas a la gerencia CIS para su revisión,
- Existen controles para evitar que se copien o redenombren los utilitarios.
- Los utilitarios sensitivos (por ej., SUPERZAP) son retirados de las bibliotecas on line y se guardan separados; para su utilización deben cumplirse procedimientos de autorización adecuados.
- El administrador de la base de datos controla los accesos a la biblioteca del DBMS por medio de programas utilitarios.

D.- Obtención de evidencia de control

La verificación de la segregación de funciones incluye los siguientes procedimientos:

- Análisis de la efectividad con que se han segregado las funciones incompatibles.
- Indagación a los empleados a fin de confirmar nuestra comprensión de sus responsabilidades laborales y las correspondientes limitaciones.
- Observación, cuando fuese apropiado, del desempeño de los empleados, de la supervisión que se ejerce sobre los mismos y de la efectividad aparente de la misma.
- Análisis, observación y prueba de la efectividad de los medios existentes para restringir el acceso a las instalaciones físicas, documentación de programas fuente y otros recursos que deban estar protegidos.

La verificación de la segregación de tareas dentro del Departamento CIS es similar a la de un ambiente manual. Sin embargo, en un ambiente computadorizado, la efectividad con que se segregan las funciones incompatibles puede depender en gran medida de la efectividad de los controles operativos del departamento, de los procedimientos relativos a cambios a los programas y de los controles de acceso general. En un ambiente CIS en el que los programas y datos son almacenados electrónicamente, pueden ser necesarios los controles de acceso basados en software para asegurar la segregación de funciones.

Manuales de operación y controles operarios diarios

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

Las posibles pruebas de los controles operativos diarios incluyen:

- Examinar los informes del sistema de registración de trabajos (job accounting) 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.

Supervisión de usuarios privilegiados

Cuando se utiliza software de control de acceso para restringir el acceso a utilitarios sensitivos y editores on line y para generar los informes correspondientes, podemos:

- Establecer si el software de control de acceso ha sido adecuadamente implantado para asegurar que los informes de actividad sean generados adecuadamente.
- Observar y probar la forma en que los supervisores utilizan dichos informes para supervisar las actividades de los empleados.
- Determinar que los dispositivos del software de control de acceso no puedan ser eludidos mediante software sensitivos.

Debemos tener en cuenta que la existencia y uso de utilitarios y editores on line puede permitir, y eventualmente ocultar, errores e irregularidades. No obstante ello, son herramientas importantes y muchas organizaciones permiten su uso bajo diversas circunstancias.

Los procedimientos que podremos aplicar respecto de los usuarios privilegiados incluyen:

- Determinar qué empleados deben ser considerados usuarios privilegiados.

- Establecer si la gerencia revisa los informes generados, ya sea por el software de control de acceso o por el software de administración de bibliotecas a fin de determinar si el acceso a los programas de aplicación y a los archivos de datos está autorizado.

Control sobre software sensitivos

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

- Obtener un listado de todos los software sensitivos.
- Obtener comprensión de los controles que aseguran que todos los software instalados estén autorizados y registrados.
- Partiendo de los directorios de las bibliotecas, seleccionar una muestra de módulos de software de sistemas y verificar la autorización de la gerencia CIS para su incorporación.
- Determinar si los controles de acceso a los software sensitivos son adecuados y si funcionan de la manera esperada.
- Confirmar que la gerencia supervisa el uso de estos software y que quede constancia de dicha supervisión.
- En aquellos casos en que los utilitarios son mantenidos separados, 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

Como nos ocupamos principalmente de los sistemas de producción (es decir, sistemas utilizados para procesamiento de operaciones diarias), es improbable que, para obtener evidencia de auditoria, 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 ejemplos :

- 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 si el usuario está satisfecho de que en las especificaciones se hayan incorporado sus requerimientos,

- Determinar a través de conversaciones con los usuarios y el personal del departamento ClS, el alcance de las modificaciones realizadas en las aplicaciones contables significativas y si la participación del usuario fue la necesaria en el desarrollo de sistemas.

3.3 Procedimientos para cambios a los programas

A.- Riesgo

Los programadores pueden realizar cambios incorrectos no autorizados en el software de aplicación, lo cual reducirá la confiabilidad de la información financiera procesada en el sistema.

Los cambios a los programas o actividades de "mantenimiento" incluyen las tareas necesarias para que el software continúe 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.

Los procedimientos de una organización para la modificación del software deben estar adecuadamente formulados y documentados para asegurarse de que los programas, una vez modificados, operan de la manera deseada y que, durante el proceso de mantenimiento del programa, el software no es manipulado para fines no autorizados.

B.- 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 financiera 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 CIS. En ausencia de controles adecuados, no existirá forma de asegurar que los controles y las

funciones de procesamiento computadorizadas son efectivas y han funcionado durante el período examinado.

El proceso para modificar substancialmente 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 motivos para el pedido de modificaciones deben ser documentados y aprobados por un nivel gerencial apropiado.
- 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 (no por los operadores o usuarios).
- Los cambios deben ser respaldados por documentación. La documentación juega un papel importante en el mantenimiento del software. Facilita la tarea 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 y los resultados (informes y salidas de datos) producidos por el sistema (output).

- Las pruebas del software modificado deben ser realizadas en primer lugar por los programadores (lo ideal es que sean realizadas por un equipo de prueba independiente). Las pruebas deben incluir todas las posibilidades y no deben ser realizadas simplemente en base a una muestra de datos reales. Una vez que el equipo de prueba/programadores está satisfecho de los cambios al sistema, los usuarios deben probarlo para asegurarse de que sus necesidades han sido satisfechas.
- 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. (Nótese que el software de bibliotecas generalmente produce en forma automática un registro de los cambios realizados en el software).
- El gerente a cargo del desarrollo y programación de aplicaciones debe asegurarse de que los cambios de códigos 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.

Las modificaciones significativas a los programas que se utilizan para el procesamiento de datos contables y financieros pueden afectar los criterios de auditoría relativos a los controles clave y funciones de procesamiento computadorizadas. En este caso puede ser necesario modificar los procedimientos de auditoría y la frecuencia con que son aplicados. Es también probable que cuando se han efectuado cambios importantes a los programas debamos modificar nuestras técnicas de auditoría computadorizadas.

C.- Análisis de los controles

La alteración del "código fuente" de un programa (escritas 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 status" 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 interfaces 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 (link edited) y reingresado a la biblioteca de producción. (Nota algunos lenguajes de programación son de tipo "interpretativo", lo que significa que la versión del programa en código fuente puede ser ejecutada sin necesidad de compilación).

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 software de "comparación de códigos 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.

El cliente también debería tener un procedimiento para asegurarse de que el. código fuente del programa sea una representación precisa del código objeto (lenguaje del computador). Si éste no fuera el caso, la comparación de los códigos fuente puede no revelar todos los cambios realizados en los programas que se están utilizando para el procesamiento de datos (es decir, el programa código objeto).

Sistemas computadorizados pequeños

No se puede generalizar con respecto a la efectividad de los procedimientos de cambios a los programas en los sistemas computadorizados 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.

D.- Obtención de evidencia de control

Podemos obtener evidencia de auditoría sobre la confiabilidad de los procedimientos de cambios a los programas seleccionando cambios representativos y determinando si los procedimientos de revisión y aprobación han sido respetados. Los cambios efectuados a los programas pueden ser determinados en base a los dispositivos automáticos de numeración ascendente del software de administración de bibliotecas o a los informes automáticos generados cada vez que el programa es modificado.

La efectividad del enfoque descripto en el párrafo anterior depende de la existencia e implantación efectiva de bibliotecas separadas de prueba y de producción. Los controles en vigencia deberían asegurar que los programadores sólo puedan hacer cambios a los

programas en las bibliotecas de prueba. Por lo tanto, tendremos que confirmar que los programadores:

- Sólo pueden acceder a los programas de aplicación en las bibliotecas de prueba.
- No pueden transferir los programas modificados a producción si no se han cumplido los procedimientos en vigencia para cambios a los programas.

Estos objetivos pueden ser alcanzados de la siguiente forma:

- Determinando si se han establecido bibliotecas separadas de producción y de prueba, en forma tal que sea técnicamente posible restringir el acceso de los programadores a los programas de producción,
- Revisando los perfiles de autorización del software de control de acceso para determinar que las bibliotecas de producción sean recursos restringidos a los que los programadores no puedan acceder.
- Determinando que los comandos de administración del software de control de acceso no permitan a los programadores eludir los dispositivos de restricción de acceso.

CONTROLES SOBRE CAMBIOS A LOS PROGRAMAS

Iniciación, aprobación y documentación

- Iniciación y aprobación por los usuarios de todos los cambios a los programas.
- Documentación completa de todos los cambios a los programas.
- Revisión y aprobación de todos los cambios a los programas por el nivel de supervisión.

Procedimientos de prueba

- Uso de bibliotecas separadas de prueba/producción.
- Restricción del acceso de programadores a las bibliotecas de producción (utilizando software de bibliotecas o software de control de acceso).
- Aprobación de los resultados de las pruebas por los usuarios y supervisores de programación.

Procedimientos de implantación

- Implantación de controles sobre la transferencia de los programas desde las bibliotecas de prueba a las de producción.
  - En código fuente para compilación
  - Por los operadores
- Uso de software de administración de bibliotecas para:
  - Registrar e informar los cambios efectuados
  - Modificar los números de versión de los programas
  - Codificar los programas sensitivos

Mantenimiento

- Mantenimiento off line de una versión autorizada de cada programa y:
  - Reemplazo a intervalos irregulares
  - Uso de software de comparación de códigos fuente para identificar los cambios realizados.
- Los "arreglos" de emergencia aplicados en forma directa a los programas de producción son:
  - Informados para su revisión por los supervisores de programación.
  - Informadosalagerenciadeldepartamentousuarioparasuposterioraprobación.
- No se les permite a los programadores utilizar software sensitivos para realizar cambios a los programas.

Segregación de funciones

- Entre los usuarios, programadores de sistemas, operadores del computador, empleados a cargo del ingreso de datos, y programadores de aplicaciones.

Enfoques alternativos

Si no existen fuertes controles sobre los cambios a los programas, deben considerarse enfoques alternativos. Por ejemplo, se podrían solicitar informes específicos generados por el software de administración de bibliotecas o por el software de control de acceso. El software de administración de bibliotecas puede ser programado para identificar y preparar un informe cada vez que se modifica la versión de producción del programa, mediante determinados dispositivos automáticos incluidos en algunos paquetes de administración de bibliotecas. Dicho informe listará las instancias en que una versión modificada de un programa de aplicación es ingresada al nivel de producción. Podríamos reprocesar datos de prueba cuando se hayan efectuado cambios que afecten controles o funciones de procesamiento con significación de auditoría. La eficiencia de este enfoque dependerá de la frecuencia con que se efectúen cambios al software de aplicación. Para ampliar la viabilidad práctica de este enfoque puede ser conveniente coordinar las pruebas con los auditores internos.

Otro enfoque puede consistir en determinar que no se hayan introducido modificaciones a los programas, aun cuando los controles sobre dichos cambios sean débiles. Para ello se pueden utilizar dispositivos del software de administración de bibliotecas que, en forma automática, indican la fecha y aumentan el número de versión de los programas de producción. También se dispone de paquetes de software que comparan el código fuente del programa con una copia de control e identifican las diferencias para que sean investigadas por el equipo de trabajo.

Estos enfoques dependerán de nuestra posibilidad para determinar si:

- El software de administración de bibliotecas ha sido adecuadamente programado para generar un informe por cada nueva versión de un programa.
- Los dispositivos automáticos de control de versiones del software no pueden ser eludidos.
- Los cambios a los programas fuente son identificados e informados por los dispositivos de comparación de código fuente,
- Los programas en código fuente son una representación exacta de los programas en código objeto.

3.4 Acceso general a los datos o programas de aplicación

A.- Riesgo

Personas no autorizadas (empleados o terceros) pueden tener acceso directo a los archivos de datos o programas de aplicación utilizados para procesar transacciones permitiéndoles realizar cambios no autorizados a los datos o programas.

B.- Medios de control

En los ambientes computadorizados sofisticados los aspectos relacionados con el acceso exceden la mera restricción del acceso del usuario. Muchos de nuestros clientes permiten que terceros, tales como sus clientes, representantes y proveedores tengan acceso a sus sistemas computadorizados. Las personas que acceden al sistema, sea cual fuere el motivo, pueden estar en condiciones de eludir las rutinas normales de procesamiento de transacciones y así generar y ocultar errores o irregularidades. Debemos identificar las posibles vías de acceso no autorizado a fin de poder apreciar el eventual impacto de dichos accesos sobre los estados financieros.

Muchos de los procedimientos operativos tienen como objetivo controlar el acceso del personal del Departamento CIS a los recursos del sistema. A menudo, la efectividad de dichos procedimientos depende de una efectiva implantación y uso de software de control de acceso, registros (logs) de operación e informes especiales para la gerencia.

La forma más común de restringir el acceso es a través de identificaciones del usuario y contraseñas. El acceso será otorgado si el sistema recibe la combinación correcta de identificación/contraseña. No obstante, para que este sistema sea efectivo debe utilizarse software para:

- Interactuar con las solicitudes de acceso de los usuarios a programas o datos.
- Permitir o rechazar el acceso teniendo en cuenta si la identificación o contraseña han sido definidas en el sistema y si el usuario está autorizado para realizar la función solicitada.

Las rutinas de software que restringen o permiten el acceso generalmente están incluidas en el software de sistemas, pero pueden ser incluidas en el software de aplicación (por ej., en los menúes) o, menos frecuentemente, en los dispositivos de seguridad terminales. Algunos de los software de sistemas que pueden ser utilizados para restringir el acceso son los siguientes:

- Software de control de comunicaciones.
- Monitores de teleprocesamiento.
- Software de control de acceso.
- Sistemas de administración de base de datos (DBMS).

Es importante comprender que la naturaleza y efectividad de los dispositivos de control de acceso del software de sistemas dependen de:

- Capacidades y características del paquete/componente de software en uso.
- Forma de implantación desde el punto de vista técnico.
- Interrelación del software con otro software de sistemas usado por el cliente (por ejemplo, condiciones que pueden facilitar la anulación de los controles).
- Procedimientos administrativos relacionados con el uso del software de sistemas (por ejemplo, revisión y seguimiento de los intentos de acceso no válidos).

C.- Análisis de los controles

Identificaciones del usuario/contraseñas

Para controlar el acceso mediante terminales, se le asigna al usuario una identificación única (por ej., número de empleado) que sea interpretada por el sistema como identificación del usuario. Sin embargo, pocas veces este código es conocido sólo por el usuario.

Debería requerirse al usuario que además de su identificación ingrese su contraseña antes de ser autorizado a leer información o ejecutar funciones de procesamiento computadorizadas (por ej., funciones que permitan el ingreso y procesamiento de transacciones o la posibilidad de modificar o eliminar datos). El uso de la contraseña brinda control sobre el acceso en el caso de que una persona no autorizada pretenda acceder al sistema utilizando una identificación y terminal autorizada. La identificación le indica al sistema quién es el usuario" la contraseña comprueba que el usuario sea legítimo.

El uso de identificaciones/contraseñas compartidas (es decir, la práctica de compartir contraseñas entre los integrantes de un grupo de usuarios relacionados) debe ser evitado dado que aumenta la probabilidad de que la confidencialidad de la contraseña se vea afectada.

Las contraseñas e identificaciones del usuario pueden no ser efectivas si no son confidenciales. Generalmente, las contraseñas son almacenadas en archivos de datos y el acceso a estos archivos debe a su vez ser restringido mediante contraseñas o codificación (por ej., criptográfica). Se pueden utilizar dispositivos de un software de control de acceso especial para facilitar el mantenimiento y mejorar la efectividad de los sistemas de identificación y contraseñas.

Software de control de acceso

Además de restringir el acceso al nivel de aplicación, paquetes de software de control de acceso, tales como o software equivalente incluido en algunos sistemas operativos, puede ser utilizados para mitigar el riesgo de acceso no autorizado al sistema.

Debemos determinar si el cliente utiliza software de control de acceso, pero no debemos conformarnos con su mera existencia. El software de control de acceso es flexible y puede ser implantado con diversos grados de efectividad.

Registro de operaciones (o de consola)

Un registro de operaciones es creado por el sistema operativo. Dicho registro incluye un detalle completo de cada actividad de procesamiento corrida en el computador. Este registro puede ser revisado por el personal de operaciones para detectar actividades de procesamiento inusuales.

El personal de operaciones puede rechazar la recomendación de revisar los registros de consola como un medio de control. Podrían argüir que los registros son demasiado voluminosos como para ser revisados y que, por ello, cualquier revisión sería superficial y poco efectiva. Esto puede ser cierto; sin embargo, este inconveniente puede ser solucionado utilizando software de generación de informes para generar informes acerca de determinados tipos de actividades de procesamiento.

SOFTWARE DE CONTROL DE ACCESO - POSIBLES CONTROLES

- Restringir el acceso (en base a perfiles de seguridad incorporados al software) a aquellos elementos del sistema que deban ser controlados, por ej. : archivos de datos, terminales, bibliotecas de programas de producción, tablas de contraseñas, editores on line y utilitarios.
- Definir las funciones autorizadas para cada persona, por ej. : un usuario puede estar autorizado a leer información, pero no a actualizarla, puede tener acceso, pero sólo desde una terminal específica.
- Supervisar y registrar determinadas actividades y generar informes especiales para su revisión por la gerencia, por ej.: emisión de un listado de todas las instancias en que un usuario privilegiado accede al sistema o cuando se verifica una violación de seguridad predefinida.
- Controlar los sistemas de contraseñas generando informes de mantenimiento a fin de identificar las fechas en que las contraseñas deben ser cambiadas; la, desconexión de terminales luego de transcurrido un período de inactividad (indicando que un usuario pudo haber olvidado hacer la desconexión); e individualizando las identificaciones/contraseñas involucradas en actividades inusuales o en intentos de acceso no autorizados.

PERFIL SUGERIDO DE ACCESO A LOS RECURSOS

	Usuarios de Recursos			
RECURSOS:	Usuarios	Programadores de Aplicaciones	Programadores de Sistemas	Operadores
Controles computadorizados y funciones de procesamiento de los programas de aplicación	Si	No	No	No
Registros de datos	Si	Biblioteca y datos de prueba solamente	Restringido	No
Programas de Aplicación	No	Biblioteca de prueba solamente	Restringido	No
Informes de control de tareas	No	Biblioteca y datos de prueba solamente	Restringido	Restringido
Programas utilitarios	No	Biblioteca y datos de prueba solamente	Restringido	Restringido
Editores on line	No	Biblioteca y datos de prueba solamente	Restringido	Restringido
Sistema operativo y otros códigos de software de sistemas	No	No	Biblioteca y datos de prueba solamente. Acceso restringido a la biblioteca de producción.	No

Clave

Sí	Debe otorgarse el acceso teniendo en cuenta las segregación de funciones incompatibles
No	No debe permitirse el acceso
Restringido	Debe otorgarse el acceso, sólo si las actividades desarrolladas pueden ser controladas y supervisadas

Restricción del acceso físico

La restricción del acceso físico al computador, terminales, programas de aplicación y documentación relacionada puede mejorar el control. Existen muchas organizaciones que instalan el computador en un lugar separado físicamente, A los programadores especialmente, pero también a otro tipo de personal no operativo, se le debería prohibir el acceso directo a dicho lugar. De esta manera, se limitan las oportunidades de acceder a los programas y datos. En la siguiente Tabla se enumeran los posibles controles de acceso físico.

CONTROLES DE ACCESO FISICO

Terminales

- Las terminales están instaladas en sectores asegurados con cerraduras u otros dispositivos.
- Las terminales están instaladas en sectores supervisados.
- El acceso a las terminales sólo está permitido a los operadores y otras personas autorizadas.
- Se requiere presentación de identificaciones físicas (por ej., tarjetas magnéticas o llaves) para operar una terminal.

Sala de computación

- El acceso a la sala de computación es controlado mediante tarjetas de acceso, llaves o códigos de combinación.
- Las tarjetas y llaves sólo son entregadas a personas autorizadas y existen procedimientos para controlar la emisión y devolución de estos dispositivos de acceso.
- Se organizan turnos de acceso para los visitantes, ingenieros o personal de limpieza.

Otros

- La gerencia del departamento CIS y el personal de seguridad de datos es automáticamente informado sobre las personas que se retiran de la empresa.
- Una vez utilizados, los datos y programas son retirados del área de operaciones y trasladados a una biblioteca de archivos segura.
- La documentación de sistemas y programas sólo está disponible para los analistas y programadores.

La tendencia hacia el procesamiento distribuido, los mini y microcomputadores ha sido acompañada por una reducción en el énfasis sobre los controles de acceso físico. En los ambientes computadorizados actuales, la restricción del acceso físico a todas las terminales es prácticamente imposible. Cada vez más se confía en diversos software para restringir el acceso físico a los programas y datos.

Sistemas computadorizados pequeños

Existen sistemas computadorizados pequeños que no poseen dispositivos de telecomunicaciones y, por lo tanto, no existe la posibilidad de que terceros tengan acceso al sistema. En estas circunstancias, el riesgo de acceso no autorizado a los recursos del sistema no será significativo. Si el acceso no autorizado fuera un problema significativo (tanto desde la perspectiva de auditoría como de servicio al cliente) existen controles adicionales que podrán ser implantados, tales como los siguientes:

- Software de control de acceso en microcomputadores como así también en minicomputadores y mainframes.
- Controles físicos sobre los archivos que contienen programas y datos sensitivos.

D.- Obtención de evidencia de control

Cuando se diseñan pruebas de los controles de acceso general se debe tener presente que ningún sistema de seguridad es invulnerable. Siempre se pueden identificar medios a través de los cuales ciertos individuos podrían burlar el sistema. Ciertas organizaciones asignarán, a sabiendas, tareas incompatibles a un mismo individuo porque el costo o la dificultad que implica su segregación no es aceptable para ellas.

Software de control de acceso

Puede utilizarse software de control de acceso para reducir el riesgo de acceso no autorizado a los sistemas computadorizados. Dependiendo de las características del sistema del cliente, pueden aplicarse uno o más de los siguientes procedimientos para probar los controles sobre el acceso no autorizado implantados a través de un software de control de acceso:

- Observar los controles de acceso al sistema para confirmar nuestra comprensión del proceso.
- Obtener copia de los perfiles de seguridad y tablas de contraseñas e identificaciones del usuario asociadas con el acceso a recursos protegidos (por ej.: archivos de datos, programas, utilitarios, editores on line, etc.), y revisarlas para determinar su integridad y consistencia con nuestra comprensión de las restricciones al acceso.

- Intentar llevar a cabo violaciones a la seguridad (en conjunto con funcionarios del cliente) para establecer que el software de seguridad restringe el acceso de manera efectiva y que los intentos de violación son incluidos en los informes de seguridad.
- Seleccionar una muestra de informes de seguridad y verificar que el funcionario a cargo de la seguridad de datos u otro empleado responsable haya investigado las violaciones informadas, y haya supervisado y efectuado el seguimiento de las actividades de los usuarios privilegiados.
- Analizar las interacciones del paquete de software de seguridad con los demás paquetes de software de sistemas utilizados por el cliente (por ej.: sistemas operativos, monitores de teleprocesamiento, DBMS, etc.). El objetivo de este procedimiento es: 1) determinar si todos los dispositivos de los paquetes de software interrelacionados necesarios para hacer que el software de seguridad sea operativo han sido activados; y 2) determinar si existen dispositivos de otro software de sistemas en uso que inhiban la efectividad del software de control de acceso.

Registro de operaciones (o de consola)

La revisión por parte de la gerencia de los registros de operaciones y el seguimiento de las partidas inusuales, aumentan la efectividad de los controles del departamento CIS, reduciendo el riesgo de que se realicen cambios no autorizados a los programas y datos de aplicación. Si consideramos esta revisión como un control clave, debemos:

- Obtener información del registro de operaciones y determinar la naturaleza de la información contenida en el mismo, como por ejemplo la descripción de los programas que han sido corridos, usuarios que han accedido al sistema, etc.
- Determinar si se ha informado alguna actividad inusual.
- Establecer si la gerencia ha investigado las actividades inusuales.

Informes gerenciales especiales

Al igual que con los registros de operaciones, nuestra preocupación con relación a los informes gerenciales especiales generados por paquetes de software de sistemas (en especial por el software de control de acceso) radica en saber cómo son utilizados por la gerencia para controlar y supervisar el acceso y las operaciones. Para determinar si estos informes son efectivamente utilizados con fines de control, debemos revisar algunos informes y verificar que se efectúe un adecuado seguimiento de las actividades inusuales.

Restricción del acceso físico

Si se considera que los controles que restringen el acceso físico a los recursos del sistema, incluyendo computadores, terminales, software, datos y documentación relacionada, son clave, podemos probarlos de la siguiente manera:

- Observar los controles físicos sobre el acceso a la sala de computación, biblioteca de cintas, documentos, datos y documentación de los programas.
- Obtener listados del personal que tiene acceso a cada una de las áreas de los lugares en donde están instalados los computadores y determinar si estos listados han sido autorizados.
- Determinar que la documentación de sistemas y programas sólo esté a disposición de los empleados autorizados.
- Probar las registraciones y autorizaciones de entregas y devoluciones de cintas y archivos de discos hacia y desde la biblioteca.
- Obtener listados de las terminales y considerar su seguridad física.
- Analizar los procedimientos de seguridad en turnos nocturnos y de fin de semana con los operadores y personal de seguridad.

CAPITULO II
HERRAMIENTAS Y TECNICAS DE AUDITORIA COMPUTARIZADA

I. Introducción

Se utiliza la expresión Técnicas de Auditoria Computadorizadas para referirse a todas aquellas técnicas que utilizan computadores, programas y datos de computación para obtener evidencia de auditoría.

Cuando desarrollamos nuestro plan de auditoría debemos planteamos los siguientes interrogantes:

- ¿ Existen oportunidades para utilizar técnicas computadorizadas?
- ¿Cuál es la evidencia de auditoría específica que puede ser obtenida a través del uso de técnicas computadorizadas?
- ¿ Qué tipo de técnica computadorizada debería utilizarse?

Las decisiones de planificación tomadas en respuesta a estos interrogantes, deberían ser documentadas poniendo especial énfasis en la relación entre las técnicas a ser utilizadas y la evidencia de auditoría a ser alcanzada.

1. Tipos de técnicas de auditoría computadorizadas

Las técnicas computadorizadas más frecuentemente utilizadas son:

a) ***Programas de recuperación y análisis.*** Estos programas son programas de computación escritos de acuerdo con especificaciones de auditoría para organizar, combinar, calcular, analizar o extraer datos computadorizados y para rehacer cálculos y otras funciones de procesamiento computadorizadas como ayuda para nuestro trabajo de auditoría, especialmente para la obtención de evidencia sustantivo.

b) ***Recuperación, análisis de datos y otras técnicas utilizando microcomputadores.*** Se pueden transferir datos de un mainframe a microcomputadores (downloading) para luego revisarlos, estratificarlos, probar los cálculos, seleccionarlos, analizar estadísticas, etc, Estas técnicas permiten la transferencia de las pruebas de auditoría de un sistema de información central a un ambiente de trabajo individual.

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

La elección entre programas de recuperación, análisis y otras técnicas utilizando microcomputadores y técnicas de transacciones de prueba está basada principalmente en la evidencia que se desea obtener. Por lo general, los programas de recuperación y análisis nos ayudan a obtener evidencia sustantivo, donde lo que se busca es seleccionar datos, calcular montos y obtener totales de archivos. Las técnicas que utilizan microcomputadores son también típicamente usadas para obtener evidencia sustantivo, utilizando datos transferidos del sistema central del cliente (downloading). Las técnicas de transacciones de prueba son utilizadas para obtener evidencia de que los controles de procesamiento y funciones de procesamiento computadorizadas operan en forma efectiva.

2. Elección de técnicas alternativas para la obtención de evidencia sustantiva

Una vez que se ha tomado la decisión de que una técnica computadorizada será utilizada para obtener evidencia sustantivo, se deberá considerar la efectividad de las técnicas alternativas en relación con su costo. A menudo, el equipo a cargo del trabajo podrá elegir entre diversos enfoques alternativos. Existen diversas consideraciones que pueden afectar las decisiones, incluyendo:

- El software disponible (ya sea el utilizado por el cliente o proporcionado por auditores).
- La disponibilidad del personal del departamento CIS del cliente y la capacidad técnica del mismo.
- Los controles sobre los sistemas computadorizados del cliente.
- La percepción del cliente de nuestros servicios.
- Otras consideraciones relacionadas con el trabajo (por ej., capacitación en el terreno del personal a cargo).
- La posibilidad de volver a utilizar los mismos programas en años futuros.
- Si el cliente dispone de programas que sólo requieran modificaciones menores para adaptarse a nuestras necesidades.

Es difícil generalizar con respecto a la relación costo/beneficio de las técnicas disponibles. Los equipos de trabajo deben seleccionar los procedimientos más efectivos y eficientes para las circunstancias de sus clientes. No obstante, las siguientes consideraciones ayudarán a los equipos de trabajo a cargo del desarrollo de nuevas técnicas computadorizadas a evaluar la relación costo/beneficio de las técnicas más comúnmente utilizadas.

- En primer lugar, considerar si es conveniente que el personal del cliente desarrolle programas utilizando su propio software de recuperación.
- Si ello no fuera conveniente, considerar el uso de módulos de recuperación de datos del sistema usado por los auditores.
- Finalmente, considerar la relación costo/beneficio de que el personal de auditoría confeccione los programas utilizando el software del cliente o bien paquetes de software de auditoría.

Con frecuencia, resulta eficiente que el cliente desarrolle programas de recuperación y análisis con su propio software ya que su personal estará familiarizado con el mismo y con los datos relacionados. En este caso, el equipo de trabajo debe determinar si:

- El cliente está dispuesto a asignar personal para el desarrollo de los programas.
- Los programas desarrollados por el cliente pueden ser controlados por auditores durante su diseño, prueba y ejecución.
- Los programas pueden ser desarrollados por el cliente dentro del tiempo necesario.
- El personal del cliente tiene la aptitud y la experiencia necesaria para desarrollar los programas.

Si los programas de recuperación y análisis no pueden ser efectiva y eficientemente desarrollados por el cliente, podremos decidir desarrollar los programas nosotros mismos. La transferencia de los datos del cliente a un microcomputador y el desarrollo de la revisión de los mismos mediante un software de microcomputación es generalmente la forma más eficiente de obtener evidencia de auditoría. Esta técnica tiene la ventaja de que, una vez que los datos han sido transferidos al microcomputador, se podrán realizar selecciones y cálculos adicionales con facilidad.

Si los datos no pueden ser transferidos, la alternativa más conveniente puede ser la de escribir nuestro propio programa de recuperación y análisis. Se pueden utilizar varias fuentes posibles de software para desarrollar los programas. Por ejemplo:

- Paquetes de software de auditoría.
- Software de recuperación de información.
- Programas utilitarios.
- Lenguajes convencionales de programación.

II. Fuentes de Programas de Recuperación y Análisis

1. Paquetes de software de auditoría

Los paquetes de software de auditoría permiten la generación de programas de computación a través de especificaciones del usuario relativamente simples. Las instrucciones necesarias para realizar tareas típicas de auditoría no necesitan ser codificadas dado que la codificación está incluida en el paquete. Para especificar las tareas de auditoría que deseamos que el programa ejecute, debemos proporcionarle información sobre el equipo de computación a ser utilizado y seleccionar la rutina o combinación de rutinas preprogramadas que deseamos.

Normalmente, la utilización de paquetes de software de auditoría incluye cuatro etapas.

- *Etapa 1 - Desarrollo del programa de auditoría específico.* Normalmente, los paquetes incluyen una biblioteca de rutinas de auditoría. El programa generador construye un programa de auditoría basándose en los parámetros ingresados y en las rutinas de auditoría seleccionadas. El programa podrá ser utilizado de inmediato o guardado para su posterior utilización.
- *Etapa 2 - Generación del programa fuente.* El programa codificado en la Etapa 1 es traducido a un lenguaje de alto nivel como, por ejemplo, COBOL. Como resultado, se obtiene un programa fuente que puede ser guardado para su posterior utilización o compilado de inmediato (véase Etapa 3). Por lo general, existe la posibilidad de aumentar la cantidad o complejidad de las tareas de auditoría agregando al programa fuente producido, el código escrito directamente en lenguaje de alto nivel. Las instrucciones adicionales del programa son normalmente denominadas "codificación propia".
- *Etapa 3 - Compilación del programa fuente.* El programa fuente es procesado con el programa compilador estándar del fabricante del computador, el cual lo traduce al lenguaje de máquina. El programa compilado se denomina programa objeto.
- *Etapa 4 - Ejecución.* El programa objeto es ejecutado utilizando los datos del cliente y se generan informes (con archivos de salida opcionales).

Esta descripción general sobre el funcionamiento de los paquetes de software de auditoría es, obviamente, una simplificación. Cada paquete de software de auditoría es único y diseñado para ser utilizado con determinados tipos de hardware y software. En el diagrama se resume la forma en que operan dichos paquetes.

El uso de paquetes de software de auditoría tiene las siguientes ventajas:

- Generalmente han sido suficientemente probados como para asegurar que funcionan en forma adecuada.
- Han sido diseñados para satisfacer necesidades específicas de auditoría.
- Frecuentemente se dispone de cursos de capacitación para su uso.
- Se puede obtener asistencia técnica para su utilización.

Sin embargo, existen ciertas desventajas comunes a todos los paquetes de software de auditoría que deberíamos conocer, incluyendo limitaciones en:

- La cantidad de archivos que pueden ser leídos.
- El tipo de estructuras de registros y representaciones de datos en archivos a los que se puede acceder.
- La cantidad de selecciones y cálculos de auditoría que pueden especificarse.
- Las posibilidades existentes para rehacer lógicas complejas en los programas de los clientes.
- El número de informes de auditoría que pueden ser producidos en cada procesamiento de un archivo.
- El formato de los informes de salida.

Ejemplos de paquetes de software de auditoría son: CARS y PANAU DIT.

2. Software de recuperación de información

Muchos de nuestros clientes han instalado en sus sistemas de computación software diseñado para la confección de informes, recuperación de información especializada y auditoría interna. El software de este tipo suele ser denominado "software de recuperación de información" o "generadores de informes". En aquellos casos en que podemos satisfacernos acerca de la integridad de operación del software de sistemas instalado por el cliente, deberíamos considerar el uso de software de este tipo como una fuente de programas de recuperación y análisis.

El uso de software de recuperación de información instalado por el cliente es recomendado debido a que, por estar ya instalado en el computador, es probable que el cliente esté familiarizado con sus características, por lo que suele ser la fuente más eficiente de programas de recuperación y análisis. Suele observarse una mayor predisposición de los clientes para ayudarnos en el desarrollo de aplicaciones cuando utilizamos su propio software. Además, el uso de los sistemas del cliente nos permite demostrar nuestro conocimiento de la tecnología de ,computación y, asimismo, contribuye a mejorar nuestra imagen ante el cliente.

Algunos de los ejemplos de software de recuperación de información son Easytrieve y FOCUS.

En las instalaciones de computación de los clientes encontramos una cantidad cada vez mayor de medios de consulta (o lenguajes de consulta). Los lenguajes de consulta funcionan, por lo general, de igual forma (aunque con menores posibilidades) que los paquetes de recuperación de información o los generadores de informes. Los lenguajes de consulta son habitualmente interactivos y son diseñados para que su uso sea sencillo. Los medios de consulta habitualmente están presentes en:

- Sistemas de administración de base de datos (DBMS).
- Instalaciones de minicomputadores, como utilitarios de uso general.
- Paquetes de contabilidad, como rutina opcional.

Entre los medios de consulta más comunes se incluyen Quik, Quiz y Query.

3. Programas utilitarios

Los programas utilitarios son otra fuente de software instalado por el cliente que puede ser utilizado para la ejecución de procedimientos de auditoría. Han sido diseñados para llevar a cabo tareas específicas de procesamiento de datos de naturaleza rutinaria y para que su uso sea sencillo. Estos programas son generalmente provistos por el fabricante del computador o por proveedores de software, aunque, ocasionalmente, los programadores de sistemas los desarrollen por su cuenta. El usuario proporciona sus instrucciones al programa utilitario en forma de parámetros que identifican los archivos de entrada y de salida, la función que debe ser realizada y los criterios de selección (cuando sea aplicable). Por lo general, no pueden especificarse otras operaciones lógicas que aquellas ya codificadas. Los programas utilitarios pueden ser utilizados en conjunto con otros tipos de software, como por ejemplo generadores de informes, para reducir los tiempos de programación. Algunos programas utilitarios típicos son: DFU, Ditto, ZAP y SUPERZAP.

Las funciones que los programas utilitarios pueden realizar incluyen:

- Clasificación de archivos de datos.
- Fusión de varios archivos de datos en uno solo.
- Copia de archivos de datos.
- Impresión de todo o parte de los archivos de datos.
- Búsqueda en un archivo de datos de registros que contengan determinados valores en un campo de datos dado.

4. Lenguajes convencionales de programación

Por lo general, la manera menos eficiente de preparar nuevos programas de recuperación y análisis es utilizar lenguajes convencionales de programación (por ej.: COBOL). El uso de estos lenguajes requiere un alto nivel de conocimientos técnicos para desarrollar y correr los programas, como así también conocer el lenguaje de programación. Se requieren instrucciones de programación detalladas aún para realizar un procedimiento simple. Sin embargo, cuando no se dispone de programas de software de auditoría u otro software de recuperación de datos, o cuando pueden ser utilizados los recursos del cliente, un programa convencional puede ser la alternativa más conveniente.

5. Resumen de fuentes de programas de recuperación y análisis

Las fuentes de programas de recuperación y análisis son resumidas en la siguiente Tabla.

FUENTES DE PROGRAMAS DE RECUPERACION Y ANALISIS

Fuentes	Usos	Ventajas	Desventajas	Otras consideraciones	Frecuencia de uso
Paquetes de software de auditoría	• Recuperación de información. • Rehacer cálculos del cliente, analizar excepciones, etc.	• Ya se han desarrollado algunas rutinas de auditoria. • Generalmente fácil de usar • Tiempo de desarrollo relativamente corto. • Reducen la necesidad de depositar confianza en el personal CIS del cliente. • Pueden ser instalados en oficinas de los auditores. • Probados. • Cursos de capacitación disponibles.	• Limitados a ambientes específicos. • Limitaciones de cantidad y estructura de los archivos a los que se pueden acceder. • Se requieren conocimientos técnicos de programación para las aplicaciones complejas. • Mayor costo y tiempo de desarrollo para las rutinas no estándar que el software de recuperación de información.	• Debe ser comprados e instalados	• Común
Software de recuperación de información	• Recuperación de información. • Rehacer cálculos del cliente, analizar excepciones, etc.	• Ya está instalado • Generalmente fáciles de usar • Apoyo técnico disponible del personal del cliente • El cliente puede haber desarrollado programas que satisfacen o pueden ser adaptados para alcanzar los requerimientos de auditoría.	• Posibles pérdidas de independencia. • Se requieren controles para asegurar la confiabilidad e integridad de los programas almacenados en las bibliotecas de programas de los clientes. • Puede no tener orientación especifica de auditoría.	• Se requiere autorización para utilizar el software del cliente.	• Común, y lo será aún más en el futuro.
Utilitarios	• Como ayuda de otros programas de recuperación y análisis, por ej., copia o clasificación de archivos. • Consultas de auditoría simples.	• Fáciles de usar	• Específicos para ciertos ambientes. • Producen poco o ningún rastro de auditoría. • Relativamente inflexible, (puede llevar a cabo únicamente funciones definidas).	• Usualmente se lo utilizan conjuntamente con otras técnicas de recuperación y análisis.	• Común
Lenguajes convencionales de programación	• Rutinas de auditoría especializadas que no pueden ser desarrolladas con programas de otras fuentes.	• Repetición de cálculos complejos.	• Se requiere capacidad técnica de programación. • Desarrollo y mantenimiento costoso	• La fuente menos eficiente de programas de recuperación y análisis.	• Poco común
Recuperación y análisis de datos utilizando micro-computadores.	• Recuperación de información a través de datos transferidos desde mainframe. • Transferencia de programas de auditoría a los mainframes.	• Fáciles de usar. • Software de microcomputador fácilmente disponible. • Cursos de capacitación disponible.	• Complejidad de las conexiones micromainframe	• Nuestro personal está familiarizado con su uso	• Común y lo será aún más en el futuro.

III. Usos de Programas de Recuperación y Análisis

El uso de programas de recuperación y análisis puede brindar ventajas sobre los procedimientos manuales tradicionales en cuanto a practicidad y eficiencia. Algunas de estas ventajas son:

- La información puede reordenarse en formatos que permitan un uso más eficiente para la auditoría.
- Los datos pueden ser clasificados y seleccionados con mayor rapidez y precisión.
- Un archivo de datos completo puede ser revisado en menos tiempo del que se requiere para seleccionar una muestra pequeña en forma manual.
- Los ítems con significatividad de auditoría pueden ser identificados y listados rápidamente para su posterior revisión.

El propósito general del uso de programas de recuperación y análisis es mejorar la eficiencia y efectividad de la auditoría. En aquellos casos en que haya pérdidas importantes de rastros de auditoría visibles de las actividades de procesamiento de datos, puede ser necesario el uso de estos programas para obtener evidencia de auditoría. Los programas de recuperación y análisis pueden ser particularmente útiles para:

- Obtener muestras y selecciones de auditoría para las pruebas e indagaciones que realizará el equipo de trabajo.
- Realizar cálculos con los datos del cliente.
- Resumir, reclasificar y comparar datos en archivos separados para permitir que el trabajo planificado pueda ser completado de la forma más efectiva y eficiente posible.

Asimismo, la mayor cobertura de las transacciones y datos permanentes y los datos de salida de los programas de recuperación y análisis nos permitirá, con frecuencia, efectuar recomendaciones útiles a la gerencia del cliente referidas a los controles de procesamiento y funciones de procesamiento computadorizadas, y al contenido de los archivos de datos. Esto es porque los programas de recuperación y análisis son frecuentemente aplicados a todos los registros de un archivo de datos, en tanto que los procedimientos manuales son generalmente dirigidos a una muestra de los mismos.

Una vez que se ha desarrollado un programa para un procedimiento de auditoría, el mismo puede ser ampliado con muy poco esfuerzo adicional para incluir análisis adicionales. La ampliación de un programa de recuperación y análisis puede permitir la eliminación de otros procedimientos manuales. Por ejemplo, si en el plan original se prevé

la obtención de una muestra de saldos de cuentas a cobrar para su confirmación, pueden agregarse rutinas que verifiquen los totales del archivo de cuentas a cobrar e impriman los pedidos de confirmación.

1. Informes de excepciones

Los programas de recuperación y análisis pueden ser utilizados para seleccionar transacciones en base a criterios específicos. Cuando los registros contables son visibles y el volumen de transacciones es pequeño, las transacciones que satisfacen criterios predef lnidos pueden ser seleccionadas manualmente. Sin embargo, cuando los datos son archivados sólo en formato legible por el computador o cuando el volumen de transacciones es muy grande, podría ser necesario o más eficiente utilizar programas de computación para identificar dichas transacciones. Cada transacción puede ser evaluada y aquellas que resulten de interés, extractadas para su revisión. A menudo, un mismo programa puede seleccionar diversos tipos de excepciones. Algunos ejemplos de informes de excepciones incluyen:

- Impresión de las cuentas a cobrar que superan un determinado monto o que están vencidas.
- Impresión de pagos inusualmente grandes.
- Impresión de los datos correspondientes a ítems potencialmente obsoletos, de baja rotación o de aquellos con stock excesivo.

2. Selección de muestras

La mayoría de los paquetes de software de auditoría contienen rutinas preprogramadas que pueden ser utilizadas para seleccionar muestras de auditoría. Las muestras pueden ser seleccionadas automáticamente entre diversas alternativas, incluyendo selección al azar estratificada o no estratificada, selección sistemática (por ej.: un ítem cada "N" número de ítems) o selección con probabilidad proporcional al tamaño (muestreo de unidades monetarias). Las selecciones requeridas pueden ser codificadas, aun cuando no existan rutinas preprogramadas, utilizando el lenguaje del paquete de software. Sin embargo, este método puede no ser tan eficiente como el uso de las rutinas preprogramadas de un software de auditoría.

Una vez llevada a cabo la selección, puede ser impresa en distintos formatos. Por ejemplo, un programa usado para una circularización de cuentas a cobrar puede imprimir

los datos ordenándolos por secuencia numérica según el código del deudor o en orden alfabético por el nombre del deudor.

Los ejemplos de aplicaciones de muestreo incluyen:

- Confirmaciones de cuentas a cobrar, cuentas de ahorro, cuentas de préstamos y cuentas a pagar.
- Altas de activos fijos.
- Desembolsos.
- Registros de personal.
- Items de existencias para su inspección física.

3. Prueba o ejecución de cálculos

Los sistemas computadorizados habitualmente llevan a cabo cálculos internos que resultan en asientos en el mayor general. Los programas de recuperación y análisis pueden ser utilizados para probar los cálculos programados, ya sea rehaciendo los mismos, o mediante comprobaciones globales de razonabilidad. Los ejemplos de cálculos que pueden ser probados incluyen:

- Depreciaciones.
- Anticuación de cuentas a cobrar.
- Ingresos o egresos por intereses.
- Valuación de existencias.

Adicionalmente, podemos utilizar programas de recuperación y análisis para realizar nuestros propios cálculos.

4. Prueba de imputaciones

Los programas de recuperación y análisis pueden ser utilizados para verificar las registraciones en las cuentas del mayor general, acumulando las transacciones detalladas incluidas en códigos de cuenta seleccionados para su conciliación con los totales resultantes del procesamiento real, como por ejemplo la distribución de:

- Compras a cuentas a pagar y a rubros de activo, existencias y/o gastos.
- Ventas a las cuentas de deudores y análisis de ventas.
- Remuneraciones a las correspondientes cuentas de costos.

5. Totales de archivos

Los programas de recuperación y análisis pueden ser utilizados para revisar las sumas y multiplicaciones en los registros individuales contenidos en los archivos, a fin de que los montos puedan ser comparados con los registros externos. Algunos ejemplos son:

- Suma de saldos de los registros individuales de cuentas de deudores para su conciliación con el saldo del mayor general.
- Producto de las unidades de existencias por su costo para su conciliación con el monto de existencias registrado.

6. Resumen y clasificación de datos

A menudo, la forma en que la información es almacenada o presentada no es conveniente para la ejecución de los procedimientos de auditoría. Se pueden preparar programas de recuperación y análisis para resumir y reordenar la información de la manera más conveniente. Estos son algunos ejemplos:

- Reordenamiento y resumen de los pagos a proveedores, ordenados por proveedor y listados en orden descendente.
- Reordenamiento y resumen de cobranzas de deudores para su comparación con los créditos registrados en las cuentas individuales de cada deudor.
- Estratificación de datos para la selección de muestras o revisiones analíticas.

7. Comparación de datos en archivos separados

Los programas de recuperación y análisis pueden ser utilizados para aparear datos de dos o más archivos. Esta función puede proporcionar una manera eficiente de relacionar la información utilizada por diversos sistemas de aplicación. Como ejemplos de apareamiento se incluyen:

- Archivos de desembolsos con archivos maestros para establecer si los pagos se efectúan sólo a proveedores autorizados.
- Archivos de remuneraciones del período corriente y anterior para identificar altas y bajas de personal.
- Resultados de inventarías físicos con registros permanentes de existencias para identificar discrepancias.

8. Comparación de datos con los registros contables

Los programas de recuperación y análisis pueden ser utilizados para comparar la evidencia de auditoría con los registros contables del cliente. Un ejemplo podría ser la comparación de los recuentos de existencias con los registros permanentes de existencias y la comparación de las respuestas a la circularización con los saldos de las cuentas a cobrar.

9. Preparación de informes y papeles de trabajo

Además de los informes producidos como resultado de los procedimientos descriptos anteriormente, se pueden preparar muchos otros informes tales como planillas llave y estados financieros comparativos en un formato de auditoría específico.

IV. Recuperación, Análisis de Datos y Otras Técnicas Utilizando Microcomputadores

Los recientes avances tecnológicos proporcionan a los usuarios conexiones entre microcomputadores y computadores centrales. Estas conexiones pueden brindarnos la oportunidad de perfeccionar nuestros procedimientos de auditoría, facilitando el acceso a los datos de los archivos computadorizados del cliente. Asimismo, nos brindan otras oportunidades y desafíos para satisfacer las expectativas de nuestros clientes.

Algunos ejemplos de las formas en que dichas conexiones pueden colaborar en nuestro trabajo incluyen:

- Transferencia de los archivos del cliente a microcomputadores y análisis de datos u otras funciones de auditoría relacionadas ("downloading").
- Aplicación de técnicas de revisión analítica, tales como comparación de los estados financieros del cliente en diferentes fechas, o de los estados financieros y datos relacionados con estadísticas relativas a la industria,
- Análisis estadísticos usando datos del cliente y bases de datos públicas.
- Preparación de planillas llave, consolidaciones, etc.
- Diseño y prueba de programas de recuperación y análisis en el microcomputador para transferirlos al y ejecutarlos en el computador central ("uploading").

Las conexiones entre microcomputadores y computadores centrales facilitan nuestro acceso a los datos y flexibilizan la ejecución de los procedimientos de auditoría. Permiten que el microcomputador se transforme en un mecanismo de ingreso, procesamiento y salida de datos además de ser una unidad independiente.

1. El downloading como herramienta de auditoría

A continuación se enumeran posibles aplicaciones de auditoría realizando downloading.

- Transferencia del balance de saldos del cliente a planillas llave.
- Transferencia de datos trimestrales seleccionados al microcomputador para revisiones trimestrales.

- Datos financieros y operativos significativos para su revisión analítica por categoría de gasto, centro de costo, división o línea de producto, con el objeto de realizar:
  - Comparaciones de saldos.
  - Análisis de tendencia histórica.
  - Análisis de índices.
  - Análisis de variaciones.

- Cartera de inversiones para verificar los precios a través de conexiones con bases de datos públicas tales como Compuserve o Prestel.
- Selección en el computador central de las cuentas para circularización a fin de transferirlas al módulo de circularización de cuentas a cobrar del paquete de auditoría para su control, impresión de las cartas de confirmación y resumen de los resultados.
- Aplicación de los programas de muestreo estadístico del paquete de auditoría a los datos transferidos.
- Para clientes con numerosas cuentas bancarias (p.ej.: comercios minoristas) transferencia de los números de cuenta y saldos para proceder a su confirmación, impresión de cartas de confirmación y análisis de variaciones con respecto a períodos anteriores.
- Transferencia a los microcomputadores de los datos sobre existencias para crear una base de datos de las mismas, y usar el software de microcomputación para:
  - Seleccionar los ítems a recontar.
  - Examinar los listados para identificar ítems inusuales.
  - Reordenar los ítems utilizando análisis del tipo "¿ qué pasaría si?" (what if). - Detectar niveles excesivos de existencias.
  - Detectar ítems de poco movimiento.
- Transferencia al microcomputador de los precios y cantidades de existencias de las líneas de productos más significativas para compararlas con períodos anteriores y el uso proyectado.

- Para entidades financieras, transferencia de los saldos de préstamos, tasas de interés e información sobre unidades monetarias a fin de crear una base de datos de los préstamos en el microcomputador y emplear el software para: - Calcular índices.
  - Calcular tasas de retorno.
  - Clasificar por unidad monetaria o por tasa de interés.
  - Calcular devengamientos.
  - Seleccionar préstamos para su confirmación.
- Transferencia de datos financieros de importancia a un modelo en el microcomputador a fin de comprobar si se están cumpliendo cláusulas complejas de los contratos de préstamo.
- Selección en el computador central de ítems de cuentas a pagar a fin de transferirlos al microcomputador para imprimir las confirmaciones y resumir los resultados.
- Transferencia de los saldos de cuentas significativas a un modelo en el microcomputador para hacer cálculos de:
  - Previsión por vacaciones.
  - Distribución de utilidades.
  - Planes de pensiones.
  - Gratificaciones al personal.
- Transferencia de los montos de previsiones impositivas, incluyendo impuestos diferidos y prueba de los cálculos.
- Transferencia de los balances de saldos en moneda extranjera por país para realizar su traducción.
- Para compañías de seguros, transferencia de los datos históricos y financieros necesarios para analizar las reservas.

Además de usar el downloading para realizar procedimientos de auditoría, debemos conocer las expectativas del cliente y las oportunidades de brindar servicios adicionales. Algunos ejemplos son:

- Transferencia de datos para ayudar en decisiones de comprar/alquilar.
- Desarrollo de modelos de planificación financiera, utilizando datos transferidos del computador central,
- Análisis de costos por línea de producto, división o planta.
- Análisis de los efectos impositivos de consideraciones relativas a nuevas situaciones.

Los beneficios potenciales del uso del "downloading" en el proceso de auditoría incluyen:

- Eliminación de la necesidad de digitación para ingresar al microcomputador los datos de los archivos computadorizados del cliente. Esto mejora la eficiencia de auditoría y elimina el riesgo de errores de digitación.
- Acceso a los datos del cliente y reducción de dependencia del personal CIS del cliente para obtenerlos. Si bien la asistencia del cliente es indispensable durante el proceso de implantación, el downloading puede reducir la necesidad de tener que recurrir al cliente en forma reiterada para programar y aplicar las técnicas de auditoría computadorizadas.
- Oportunidad de crear una base de datos en el microcomputador a la que se puede acceder a través de software de microcomputadores (como, por ejemplo: DBASE, Easytrieve Plus PC, etc.) para poder llevar a cabo muchos de los cálculos que antes se realizaban en computadores grandes. Esto nos brinda una mayor flexibilidad en la oportunidad y frecuencia de aplicación de nuestros programas a los datos del cliente.
- Oportunidad de reorientar los esfuerzos del personal de auditoría hacia la interpretación de los datos del cliente y a la búsqueda de métodos de prueba, en vez de ingresar datos o llevar a cabo análisis manuales.
- Refuerzo de los procedimientos de auditoría mejorando la naturaleza de los procedimientos realizados o aumentando la cobertura de auditoría.
- Demostración a los clientes de nuestro conocimiento y utilización de las tecnologías más recientes.
- Maximización de las oportunidades de servicios relacionados con las necesidades del cliente de integrar el downloading a su propio ambiente,
- Refuerzo de las relaciones con el personal del cliente, en especial con el personal de procesamiento de datos.

También debemos considerar las desventajas potenciales del downloading antes de ponerlo en práctica. Por ejemplo:

- Los aspectos técnicos de la conexión y ejecución de este tipo de transferencia probablemente requieran que el personal de auditoría no pueda llevar a cabo estas tareas sin la asistencia técnica del cliente o de los especialistas CIS.
- El costo de los productos para transferencia de datos varía en relación con su nivel de sofisticación. Algunos son bastante caros y junto con el costo de la asistencia técnica necesaria, pueden resultar ineficientes en relación con la evidencia de auditoría que se espera obtener.

- Los clientes pueden manifestar preocupación con respecto a la seguridad de los datos con motivo de nuestra posibilidad de acceder a ellos en forma directa. Estos temas deben ser tratados al inicio de nuestra planificación.

Al considerar el uso del downloading, debemos plantearnos las siguientes preguntas:

- ¿ Se llevan a cabo actualmente procedimientos de auditoría en microcomputadores (o podrían llevarse a cabo)? La eficiencia de determinados procedimientos de auditoría realizados con microcomputadores puede aumentar con el uso del downloading.
- ¿ Requiere el procedimiento que sé digite un volumen significativo de datos? El downloading maximiza los beneficios en los casos en que el ingreso de datos es significativo.
- ¿Es el procedimiento un procedimiento recurrente de auditoría?. El costo inicial de la implantación del downloading debe ser evaluado basándose en el período de beneficio esperado; los procedimientos recurrentes brindan un mayor retorno sobre la inversión efectuada.
- ¿ Se logrará mayor satisfacción de auditoría? El downloading es de gran valor en aquellas situaciones en que se mejora la naturaleza de nuestros procedimientos (mediante el uso de software de microcomputación) o se incremento la satisfacción de auditoría.
- ¿ Ha establecido el cliente una conexión entre los microcomputadores y el computador central? La existencia de esta conexión en las instalaciones del cliente puede tener influencia positiva sobre la opción de utilizar downloading.

Al decidir entre downloading y correr programas de recuperación y análisis en el computador central, la decisión estará influida por la necesidad de análisis posteriores de la información. Para propósitos de recuperación de información, informes y utilización de rutinas típicas (por ejemplo, suma, clasificación, estratificación, cálculos, etc.) el procesamiento a través del computador central puede ser más eficiente. La conveniencia de utilizar downloading puede estar influida por la necesidad de elaborar información, realizar análisis "what if" y procedimientos de revisión analítica que son adecuados para efectuarse en un microcomputador.

Si el cliente no cuenta en su instalación con una conexión microcomputadores/computador central, debe evaluarse cuidadosamente la conveniencia económica (relación costo/beneficio) de su incorporación. La implantación, sin una adecuada planificación previa, puede resultar costosa. Si el ambiente no es propicio para un

downloading (por ej.: si el cliente no está convencido de su conveniencia) es raro que se pueda implantar con éxito.

1.1 Mecánica del downloading

La mecánica del downloading puede ser resumida de la siguiente manera:

- Identificación de los datos que serán transferidos desde el computador central al microcomputador. (A menudo, el grupo a cargo del trabajo transfiere únicamente los datos que se necesitan para un posterior análisis en lugar de transferir el archivo completo).
- Determinación del método que se utilizará para transferir datos desde el computador central al microcomputador. (En algunos casos, se establece una conexión directa entre los computadores. En otros, los datos del cliente son copiados en una cinta magnética y luego, desde una unidad de cintas se podrán transferir los datos desde la cinta al microcomputador.)
- Si fuera necesario, conversión de los datos del cliente a un formato que pueda ser utilizado por software de microcomputación. (A menudo, los computadores centrales emplean métodos de representación de datos que difieren de los utilizados por los microcomputadores. Por ejemplo, los computadores centrales IBM utilizan un método de representación de datos denominado EBCDIC, en tanto que los microcomputadores emplean ASCII).

A continuación se tratarán estos y otros aspectos del downloading en forma más detallada.

Datos a ser transferidos

Una parte importante en la decisión de aplicar el downloading es definir qué datos serán transferidos. Tenemos la opción de transferir uno o más archivos completos o datos seleccionados extraídos de uno o más archivos. La decisión de transferir archivos completos puede ser adecuada en ciertos casos pero, en la práctica, la transferencia de archivos completos puede no ser necesaria para una gran cantidad de procedimientos de auditoría. Debemos tener en cuenta que la capacidad de los discos rígidos de los microcomputadores es considerablemente menor a la de los archivos de computadores grandes. Otra razón para no transferir archivos enteros es que el procesamiento en los microcomputadores es más lento que en los computadores grandes, El tiempo que lleva explorar todos los datos hasta obtener la información deseada puede resultar excesivo e inclusive intolerable en muchos

microcomputadores. Por ello se recomienda emplear, cuando sea posible, software tales como generadores de informes para seleccionar la muestra deseada en el computador central y sólo transferir al microcomputador los datos necesarios para efectuar los análisis planeados.

Método para la transferencia de datos

El problema de la conexión física puede ser resuelto ya sea conectando los dos computadores (por medio de un cable coaxial o por cable bipolar de cobre) o utilizando una línea de comunicación de datos tal como una línea telefónica. Cuando se usan líneas telefónicas es necesario que tanto el computador emisor como el receptor cuenten con un módem. El módem traduce las señales digitales del computador emisor en las señales analógicas necesarias para las líneas telefónicas y luego las vuelve a traducir en señales digitales para uso del computador receptor. Las conexiones por cable coaxial, si bien son más caras, son las más utilizadas porque permiten mayor velocidad de transferencia y proximidad al computador central. Las líneas telefónicas son más lentas para transferir datos, pero son más económicas; generalmente se utilizan si nos encontramos en un lugar alejado del computador central del cliente.

La transferencia de datos puede ser facilitada si el microcomputador es definido como una terminal del computador central. Este procedimiento es denominado emulación de terminal y se realiza mediante la instalación de una tarjeta de emulación en el microcomputador. Luego, se instala el software correspondiente en el microcomputador, el cual también es a menudo instalado en el computador central. Existen cientos de productos que emulan cada una de las docenas de tipos de terminales. Algunos de estos productos incorporan dispositivos de traducción de datos (véase a continuación).

Conversión de datos

Una vez que los datos son transferidos al microcomputador deben ser convertidos al formato del software de aplicación que reside en el equipo (por ej., Lotus 1-2-3).

La forma más sencilla de transferencia de archivos utiliza un protocolo de comunicaciones denominado comunicación "asincrónica". Conjuntamente con un dispositivo de conversión de datos, los paquetes de comunicación asincrónica nos permiten transferir datos de los computadores del cliente a los microcomputadores de los auditores. Estos paquetes se utilizan con frecuencia con líneas telefónicas para transferir datos de computadores centrales a microcomputadores ubicados en localidades alejadas. Este software permite transferir los datos al microcomputador pero no los convierte a un formato

que pueda ser leído por un software de aplicación. La conversión debe ser efectuada ya sea por el software de aplicación o por medio de otras técnicas de programación. El módulo de Conversión de Datos del software de los auditores realiza esta tarea para determinados módulos del paquete de auditores, como así también para diversos software de aplicación de uso difundido.

Existen software más sofisticados que automáticamente convierten los datos transferidos a formatos que son aceptados por los más conocidos paquetes de aplicación para microcomputadores. Algunos de estos paquetes están preparados para usos genéricos, como por ejemplo Tempus Link y Tempus Data (de Micro Tempus) que pueden emplearse en distintos tipos de instalaciones de computadores centrales y que convierten los datos en el microcomputador a formatos aceptados por el Lotus 1-2-3 y DBASE, entre otros. En la mayoría de los casos, estos productos son comercializados por los proveedores de software de aplicación (p.ej.: el Expertlink lo vende MSA; el PC Link lo vende Mc Cormick & Dodge; la serie /Answer la venden Informatics e IBM).

Los software más sofisticados disponibles para downloading son aquellos paquetes que contienen software de aplicación compatibles tanto con microcomputadores como con computadores centrales. Los productos para microcomputación han sido desarrollados por proveedores de software que, o bien reproducen la funcionalidad del paquete para computadores centrales, o están diseñados para competir con los paquetes más conocidos de microcomputación independientes. Algunos ejemplos de estos paquetes son: FOCUS para computadores grandes y PC Focus para microcomputadores, Pansophic Systems' Easytrieve para computadores grandes e Easytrieve Plus PC para microcomputadores. Este tipo de paquetes probablemente existan en aquellos clientes en donde ya se utilice el software para computadores centrales de los proveedores mencionados.

1.2 Unidades de cinta

En ciertos ambientes probablemente no se pueda implantar el downloading a un microcomputador mediante técnicas de telecomunicación (ya sea por cable coaxial o por líneas telefónicas), resultando más fácil obtener una copia de los datos en una cinta magnética. Esto puede ocurrir en circunstancias como las siguientes:

- El cliente ya tiene los datos en formato de cinta magnética o tiene la posibilidad de producirlos rápidamente.
- El personal de PW no está familiarizado con las conexiones entre el computador central y los microcomputadores existentes en las instalaciones del cliente.

- Los archivos de los clientes son mantenidos por un servicio externo y los servicios de recuperación de datos son costosos.
- El perfil del usuario atribuido al auditor no permite una transferencia adecuada de los datos sin tener que realizar cambios.
- El cliente no cuenta con los recursos necesarios (humanos, software y/o hardware) para realizar el downloading con técnicas de telecomunicaciones.
- El computador central tiene capacidad limitada o demora mucho tiempo en completar un trabajo o el cliente restringe nuestro uso del computador central.

Como alternativa a las telecomunicaciones podemos usar una unidad de cinta para transferir datos de los archivos del cliente al microcomputador. Por lo general, con pequeñas modificaciones los archivos del cliente pueden ser cargados en la unidad de cinta y, utilizando el software de ésta junto con cierta codificación especial, los datos contenidos pueden ser convertidos al formato adecuado para transferirlos a los programas de aplicación específicos del microcomputador. Generalmente los software de auditoría incluye un dispositivo para transferir los datos del cliente utilizando unidades de cinta. La transferencia de datos requiere un determinado conocimiento técnico sobre el ingreso de datos en la cinta magnética por lo cual normalmente el personal de auditoría no podrá realizar estas tareas sin la debida asistencia técnica,

1.3 Consideraciones sobre seguridad y control

Cuando se considera el acceso directo a los archivos computadorizados del cliente, surgen consideraciones sobre seguridad y control. Estas consideraciones rigen tanto para el downloading como para el acceso directo a través de terminales. Normalmente, debemos someternos a los mismos procedimientos de seguridad vigentes en la organización del cliente. Con el objeto de no inquietar al cliente, se puede usar una copia del archivo cuando se aplica el downloading.

En los casos de transferencia de datos con propósitos de realizar procedimientos de auditoría, surgen consideraciones sobre control relativas a la integridad de los datos. Se deben establecer procedimientos para obtener totales de control que concilien con los registros del cliente, (para asegurarse de que no se han efectuado ajustes posteriores a la transferencia de los datos). El auditor deberá asegurarse de que los totales de control coincidan con los registros.

La mayoría de los productos de software más sofisticados que se utilizan para conectar los microcomputadores con los computadores centrales, permiten perfiles del usuario complejos que pueden ser utilizados para restringir el acceso a campos sensitivos

por empleados autorizados. Debemos asegurarnos que el perfil utilizado por el auditor no provoque una transferencia incompleta de los datos. Podría ser difícil y hasta imposible detectar estas transferencias incompletas utilizando totales de control. Debemos concentrarnos en entender las limitaciones inherentes del perfil que estamos utilizando.

Las técnicas que se describen a continuación no son comúnmente utilizadas como parte de los procedimientos de auditoría ya que, por lo general, son más difíciles, insumen más horas de trabajo y su desarrollo e implantación son costosos. Sin embargo, existen ciertos casos en que pueden ser efectivas y eficientes.

1.4 Módulos de auditoría incorporados

Los módulos de auditoría incorporados son programas escritos y compilados dentro de un programa de aplicación para realizar procedimientos de auditoría conjuntamente con el procesamiento. Pueden formar parte del procesamiento de una aplicación de rutina o pueden funcionar sólo cuando se los activa específicamente. Esta técnica nos permite supervisar y analizar el procesamiento de las transacciones en forma continua, como parte del procesamiento cotidiano del cliente. Por ejemplo, un módulo de auditoría incorporado en un programa de cuentas a cobrar del cliente puede incluir una rutina de auditoría para acumular todas las transacciones asociadas con cuentas específicas de deudores durante un período determinado, con el objeto de establecer si las facturas, créditos y cobranzas. están adecuadamente registradas y acumuladas. Las transacciones seleccionadas por el módulo pueden ser informadas inmediatamente o, lo que es más habitual, registradas en un archivo de auditoría al cual podemos acceder en una fecha posterior.

Es preferible que los módulos de auditoría sean diseñados durante el desarrollo del sistema. Se requiere una profunda comprensión del sistema a fin de identificar, en el momento adecuado, las funciones de auditoría que serán incorporadas al programa de aplicación. Las desventajas de este sistema son el costo de diseño y programación del módulo y el tiempo adicional que se requiere para procesar las transacciones en el módulo.

También se presenta una importante consideración de control de auditoría ya que estaremos confiando en la presencia de controles para evitar accesos no autorizados, tanto al módulo incorporado como al archivo de auditoría, Además, los módulos pueden tener que ser modificados si se modificaron los programas de aplicación. También existe la posibilidad de que no se nos notifique de tales modificaciones.

La técnica de módulos de auditoría incorporados es costosa. Su costo y la necesaria participación del cliente pueden ser difíciles de justificar. No obstante, cuando se la utiliza en las circunstancias apropiadas, puede tener una buena relación costo-beneficio e inclusive ser necesaria. Puede ser particularmente efectiva cuando se prueban sistemas de

actualización inmediata u otro tipo de sistemas interactivos que procesan un gran volumen de transacciones en los que no existen rastros de auditoría visibles y los archivos de transacciones son destruidos en un corto plazo.

1.5 Análisis de información sobre registro de trabajos ("job accounting")

El análisis de la información sobre registro de trabajos puede ser utilizado para probar ciertos controles del departamento CIS, como por ejemplo los controles de acceso a los recursos de los sistemas computadorizados.

La mayoría de los sistemas operativos de los computadores incluyen un software que controla e informa acerca de los recursos que utiliza el sistema (p.ej.: los sistemas MVS de IBM utilizan un paquete de software denominado System Management Facility) incluyendo, para cada trabajo procesado, los archivos utilizados, la fecha y hora de procesamiento y el tiempo que éste insumió. Estos informes son empleados habitualmente por la gerencia para controlar las actividades de procesamiento de datos y para supervisar la eficiencia del uso del equipo.

Los informes sobre registro de trabajos permiten obtener satisfacción en cuanto a que sólo se han procesado trabajos autorizados y que se han utilizado los archivos de discos y cintas apropiados. Sin embargo, los listados pueden ser tan voluminosos que sean difíciles de revisar. De ser así, se puede utilizar un programa de recuperación que extraiga los datos relevantes basándose en pautas de excepción preestablecidas.

1.6 "Enganches" (hooks) de auditoría

Los "hooks" de auditoría son puntos en los programas de aplicación denominados, salidas" (exits), que le permiten al auditor insertar comandos para procesamientos especiales de auditoría. Esta técnica le permite al auditor modificar una aplicación estándar o un programa para llevar a cabo un proceso que respalde una actividad de auditoría. Por ejemplo, un programa utilitario utilizado para reorganizar una base de datos puede incluir un "hook" para agregarle una codificación adicional que permita acumular totales y recontar registros de la base de datos. Esto nos permite obtener totales de control en forma independiente y como subproducto del procesamiento normal del sistema.

1.7 Uploading

El uploading es el proceso inverso al downloading y consiste en la transferencia de datos desde un computador pequeño a uno más grande, por lo general un computador

central. Un ejemplo de uso de un microcomputador como herramienta de uploading es cuando el microcomputador se utiliza para crear programas de computación para luego ser transferidos y ejecutados en el computador central. Esto se ve habitualmente en el uso de paquetes "front-end" para microcomputadores, que se combinan con paquetes de recuperación o report writers de computadores grandes. Otros ejemplos de uploading son:

- Uso del microcomputador como generador de datos de prueba con el fin de transferirlos al computador central. Los datos de prueba transferidos del microcomputador pueden ser procesados para propósitos de auditoría.
- Los módulos de auditoría incorporados pueden ser programados en el microcomputador y transferidos para su ejecución en el computador central. Si bien tales procedimientos normalmente son preprogramados para su integración a los sistemas del cliente, este dispositivo nos proporciona flexibilidad y la posibilidad de ejecutar los programas al azar.

Los problemas técnicos del uploading son similares a los del downloading. Sin embargo, existen menos productos en el mercado con capacidad de uploading con conversión a los lenguajes del computador central. Por lo general, solamente los paquetes más sofisticados de software (con aplicaciones integradas para computadores centrales y microcomputadores) cuentan con esta facilidad (p.ej.: Easytrieve Plus PC y otros paquetes de recuperación similares). Si se utiliza la técnica de uploading, será necesario efectuar una programación a medida.

Si bien los clientes normalmente apoyan las actividades de downloading, suelen ser más reacios en lo referente a uploading. Todo procedimiento de uploading debe estar sujeto a las mismas normas de seguridad aplicables al ingreso de datos. Desde el punto de vista de auditoría, los procedimientos de seguridad y control relacionados con uploading deben ser acordados de antemano con el cliente.

1.8 Software de entrada para microcomputadores (front-ends) para recuperación de otros software

En respuesta a la creciente tendencia hacia el software destinado al usuario final, muchos proveedores de paquetes de recuperación para computadores grandes han introducido al mercado software de entrada para microcomputadores, el cual está conectado con el software del computador central. Estos paquetes varían en cuanto a sofisticación y facilidad de uso. En el límite mínimo de funcionalidad, algunos programas apenas permiten a los auditores crear pedidos de informes en el microcomputador para su transferencia y ejecución en el computador central. En el rango más alto de funcionalidad, algunos paquetes son versiones para microcomputadores de las versiones para computadores grandes y cuentan con las mismas posibilidades en lo que respecta a integración de uploading y downloading. Debemos conocer qué paquetes de recuperación emplean nuestros clientes y debemos estar al tanto de todos los paquetes front-end comercializados por el proveedor. Para determinar la potencial utilidad del paquete front-end para la auditoría se debe considerar lo siguiente:

- Extensión de la curva de aprendizaje para poder aplicar el mismo.
- Necesidad de asesoramiento de especialistas en auditoría CIS.
- Facilidad de entrada y edición de datos.
- Facilidad de preparación y edición de informes.
- Flexibilidad en la recuperación de errores.
- Claridad de los mensajes de error.
- Utilidad de los dispositivos de ayuda on line.
- Facilidad de referencia en la documentación.
- Biblioteca de rutinas estándar.
- Posibilidad de almacenar rutinas "a medida".

1.9 Bases de datos públicas

La proliferación de microcomputadores y de las conexiones entre microcomputadores y computadores centrales, ha dado lugar a la aparición de servicios externos de bases de datos. En un principio, las bases de datos públicas eran una especie de boletines diseñados por y para los aficionados a ciertos temas con el objeto de compartir intereses comunes. Como consecuencia de la popularidad y sencillez del uso de los paquetes de comunicación asincrónica, ha crecido la posibilidad de acceso a bases de datos de terceros. Estos servicios de terceros incluyen empresas tales como Compuserve, Prestel y

Dun & Bradstreet, donde se puede obtener información variada, como por ejemplo, cotizaciones de acciones, bonos y otros instrumentos que cotizan en la Bolsa. Para acceder a estos servicios, es necesario suscribirse y además contar con un modem.

Debemos considerar la posibilidad de aplicar estos servicios como parte de la planificación de auditoría. Por ejemplo, podríamos utilizar una base de datos pública para obtener las cotizaciones de la cartera de inversiones de un cliente y transferir la información a un paquete de aplicación de microcomputador diseñado para calcular el valor neto de las mismas.

V. Técnicas de Transacciones de Prueba

Las técnicas de transacciones de prueba permiten obtener satisfacción de auditoría ingresando al sistema computadorizado del cliente una muestra de transacciones para luego comparar los resultados obtenidos con los predeterminados. Son desarrolladas para probar controles de procesamiento y funciones de procesamiento computadorizadas, tales como:

- Ingreso de transacciones significativas o de otro tipo de información, por ejemplo: cantidades, precios y montos de las facturas de proveedores.
- Aprobación de transacciones, por ejemplo: aprobación interactiva, (a través de una pantalla), de órdenes de compra o transferencias y desembolsos de fondos por medios electrónicos.
- Cálculos, por ejemplo sumas y multiplicaciones.
- Apareamiento, por ejemplo: cantidades del informe de recepción con las facturas, totales calculados con totales de control.
- Extracción de información de los archivos del computador, por ejemplo-. obtener cantidades para nuevos pedidos o costos de determinados ltems de existencias,
- Actualización de archivos, por ejemplo, agregar, modificar o eliminar información almacenada en archivos electrónicos.
- Clasificación de información en un orden predeterminado.
- Modificación del formato de los datos para permitir su transferencia entre sistemas.
- Impresión de informes o lectura de información por pantalla, por ejemplo: transacciones rechazadas, tales como facturas de proveedores cuyas cantidades no coinciden con las de los informes de recepción.

Los principales tipos de técnicas de transacciones de prueba son los siguientes:

- Datos o lotes de prueba.
- Procedimiento de prueba integrada (ITF - lntegrated Test Faciiity).
- Pruebas on line.

1. Datos o lotes de prueba

Una de las primeras técnicas diseñadas para probar los controles de procesamiento y funciones de procesamiento computadorizadas fueron los lotes de prueba en tarjetas perforadas. En la actualidad se cuenta con métodos más eficientes de almacenamiento y procesamiento de prueba de datos que las tarjetas perforadas. No obstante, el término "lote de prueba" se sigue empleando pese a que ha cambiado la forma en que se almacenan y procesan los datos de prueba. En la Tabla Bl.4 se ilustra la técnica de datos de prueba. Esta ilustración describe cómo se utilizan las técnicas de datos de prueba para determinar si las rutinas de edición y otros controles de procesamiento y funciones de procesamiento computadorizadas funcionan de acuerdo con lo previsto.

Cuando se emplean técnicas de datos de prueba, las transacciones de prueba son normalmente procesadas por los programas del computador en un modo "no productivo", o sea, en forma separada del procesamiento normal. Las transacciones de prueba son registradas (actualizadas) en archivos simulados o archivos para copia de datos (o sea, no se utilizan archivos "vivos"). Las transacciones de prueba pueden ser seleccionadas de las transacciones reales, de las que se utilizaron para probar el software de aplicación durante la etapa de desarrollo y aceptación, o pueden ser transacciones diseñadas específicamente en base a los requerimientos de la prueba. Una vez finalizado el procesamiento, los resultados reales de la prueba son comparados con los resultados predeterminados para asegurarnos de que el programa de producción opera de la manera prevista.

El uso de técnicas de datos de prueba no requiere conocimientos técnicos profundos del procesamiento u operación del computador pero sí requiere que se comprenda el diseño del sistema, incluidos los controles de procesamiento y funciones de procesamiento computadorizadas.

Al emplear la técnica de datos de prueba deben tenerse en cuenta los siguientes aspectos:

- Las transacciones de prueba deben ser diseñadas "a medida" para cada sistema de aplicación.

- Sólo es necesario probar una vez cada control y función de procesamiento computadorizada, ya que normalmente se puede confiar en la consistencia del procesamiento que realiza el computador, siempre que existan controles satisfactorios del departamento CIS.
- Una vez desarrollados, los lotes de prueba pueden volver a ser usados en auditorías sucesivas, siempre y cuando los programas de aplicación no hayan sido modificados. En este caso, es muy probable que los datos de prueba deban ser modificados.
- Cuando los lotes de prueba deban cubrir un amplio alcance, su desarrollo y ejecución pueden requerir un considerable insumo de tiempo. Debemos ser selectivos y solamente llevar a cabo pruebas sobre los controles y funciones de procesamiento computadorizadas en las que deseamos confiar (es decir, controles clave).
- Los resultados reflejarán las condiciones del momento en que se ejecutaron los datos de prueba. Normalmente, se requerirá obtener evidencia de que los controles y las funciones de procesamiento computadorizadas fueron protegidas de cambios no autorizados durante el período bajo examen.
- Debemos asegurarnos de que se prueban copias válidas de los programas de producción que se emplearon durante todo el período contable bajo examen.
- La prueba de los programas del cliente debe ser realizada inmediatamente antes de las corridas de cierre del período,
- En ciertos casos, es preferible el enfoque alternativo de utilizar un procedimiento de prueba integrada, el que es tratado a continuación.

Si hemos decidido confiar en los controles y funciones de procesamiento computadorizadas, el uso de técnicas de datos de prueba puede ser la manera más efectiva de probar la continua efectividad de dichos controles y funciones.

2. Procedimiento de prueba integrada (ITF)

El ITF también es habitualmente conocido como la técnica de "miniempresa" o „empresa simulada". Una forma efectiva de controlar las transacciones de prueba es establecer una entidad "simulada" en el archivo de datos reales del cliente (por ejemplo: cuentas de una filial o subsidiaria) en las cuales se registran las transacciones de prueba. En un ITF, las transacciones de prueba son procesadas a través del sistema en un modo productivo, o sea, utilizando los mismos procedimientos de ingreso y procesamiento de datos Que se emplean para las transacciones reales pero se deberá tener la precaución de excluir la "empresa simulada" de la información final del cliente.

Los ITF son normalmente utilizados para controlar los sistemas integrados. El procesamiento de la información es "integrado" cuando los datos ingresados o generados automáticamente, actualizan archivos de datos utilizados en más de una aplicación. Por ejemplo, el ingreso de datos de despachos puede generar automáticamente las facturas de venta y registrar totales de resumen en las cuentas del mayor general de existencias, costo de ventas, ventas y cuentas a cobrar.

Aunque un ITF puede ser implantado para cualquier sistema de aplicación, esta técnica es más efectiva cuando se ha perdido el rastro de auditoría o cuando la complejidad del sistema dificulta el seguimiento del flujo de las transacciones. Las mejores situaciones para el uso de un ITF son aquellos sistemas que utilizan procedimientos de ingreso de datos en forma interactiva y procesamiento con actualización inmediata para grandes volúmenes de datos. Esta técnica es especialmente útil para probar controles y funciones de procesamiento computadorizadas integradas y complejas.

Al emplear un ITF debemos asegurarnos que las transacciones de prueba no ingresan a los registros contables reales o en caso de ingresar son eliminadas. Las medidas para que esto suceda así deben ser desarrolladas y tratadas con los niveles gerenciales correspondientes en una etapa inicial de la planificación de auditoría.

3. Pruebas on line

Lo adecuado de los controles de procesamiento y la efectividad de las funciones de procesamiento computadorizadas son muy importantes cuando el ingreso de datos se efectúa en modo interactivo y los registros contables son actualizados de manera inmediata (o almacenados temporariamente para su procesamiento posterior sin una futura intervención del usuario). En este tipo de sistemas, las pruebas de edición y validación de datos evitan la aceptación de transacciones erróneas o no autorizadas. La mayoría de los sistemas que tienen ingreso de datos interactivo están diseñados para rechazar inmediatamente las transacciones inválidas sin dejar evidencia de este rechazo. Por este motivo, puede no existir un rastro visible que nos permita confirmar que sólo hayan sido aceptadas las transacciones válidas. También, el riesgo de que las transacciones rechazadas no sean identificadas, analizadas y corregidas en forma oportuna puede ser mayor. La prueba on line puede ser el único medio efectivo de probar los controles de edición y validación.

Cuando se aplica la prueba on line para probar los controles de edición y validación, se intenta ingresar una transacción que no debería ser aceptada por el sistema para su procesamiento. Luego de efectuar intentos con distintas combinaciones de transacciones

válidas y no válidas, podremos determinar que las transacciones no válidas son rechazadas por el software y que las válidas son aceptadas,

Las pruebas on line deben ser planificadas en forma adecuada conjuntamente con el personal del cliente antes de llevarlas a cabo, Existe la posibilidad de que el sistema acepte una transacción "errónea". Si esto sucediera, debemos asegurarnos junto con el personal del cliente, de que la transacción sea reversada.

Las pruebas on line son una técnica efectiva y muy utilizada para probar los controles de edición y validación on line. Son de fácil uso y pueden llevarse a cabo sin mayores interferencias en el sistema de aplicación del cliente. El tiempo que generalmente se requiere para llevar a cabo esta prueba es mínimo en relación con la satisfacción de auditoría que se logra. Si se utiliza la técnica ITF, las pruebas on line constituyen generalmente una parte del ITF. No obstante, las pruebas on line pueden llevarse a cabo sin emplear técnicas ITF.

Las pruebas on line también pueden ser utilizadas para probar los controles que evitan el acceso no autorizado a través de terminales. Habitualmente se utilizan identificaciones del usuario y contraseñas para controlar el acceso, lo cual también constituye un medio electrónico para llevar a la práctica la segregación de funciones. Las pruebas on line pueden ser utilizadas para probar la efectividad con que se restringen los accesos no autorizados.

El cuadro comparativo de la Tabla resume el uso, ventajas y desventajas, otras consideraciones y la frecuencia de uso de las principales técnicas de transacciones de prueba.

Nota: Como sucede con otras evidencias de control, el equipo a cargo del trabajo necesitará obtener evidencia de que los controles y las funciones de procesamiento computadorizadas probadas con técnicas de transacciones de prueba han operado en forma efectiva durante el período bajo examen y no únicamente en el momento en que las técnicas son aplicadas.

IV. Uso de Técnicas de Transacciones de Prueba

A continuación se describen los procedimientos de auditoría específicos que se pueden llevar a cabo con las técnicas de transacciones de prueba. En la *Sección C2, Transacciones de Prueba*, se incluyen ejemplos específicos del uso de estas técnicas, tomados de trabajos reales.

1. Verificación de los controles de edición y validación

La mayoría de los sistemas de aplicación computadorizados incorporan controles de edición y validación que informan o rechazan transacciones faltantes, duplicadas o potencialmente erróneas. Se pueden probar tales controles ingresando transacciones de prueba para confirmar que:

- Los números de cuenta de los proveedores son verificados en un archivo de datos permanentes de proveedores autorizados antes de la preparación de los cheques correspondientes.
- Los números de facturas de proveedores que se ingresan más de una vez son informados o rechazados para impedir que se dupliquen los pagos.
- Se llevan a cabo pruebas de edición de los campos críticos de datos para poder detectar los errores ocurridos durante la preparación de los documentos fuente o durante el ingreso de datos.

2. Prueba de informes de excepción

Muchas aplicaciones producen informes de excepción durante el procesamiento para poder identificar las transacciones que no cumplen con las pautas de aceptación predeterminadas. La revisión y resolución de las excepciones e ítems en suspenso informados puede contribuir a evitar errores de importancia, Mediante el procesamiento de transacciones de prueba que contengan excepciones, se puede determinar si las transacciones incorrectas son rechazadas e incluidas en archivos de ítems en suspenso y en los informes de error correspondientes. Es probable que se requieran ciertos procedimientos manuales para verificar que el cliente haya tomado las medidas correctivas necesarias en relación con los errores incluidos en dichos informes. Las transacciones que están en suspenso a la fecha del cierre contable pueden afectar significativamente los estados financieros.

Entre las pruebas que pueden llevarse a cabo se incluyen las siguientes:

- Determinar si se informan como excepciones los registros de tiempo de empleados que totalizan una cantidad de horas superior al parámetro preestablecido.
- Determinar si se registran como ítems en suspenso aquellas cobranzas que no pueden ser comparadas con (registradas en) los registros del cliente.
- Determinar si se informan como excepciones las cuentas a cobrar vencidas que superen un período preestablecido.

- Determinar si se informan como excepciones los pagos a proveedores que superen un monto preestablecido.

3. Prueba de los cambios a los datos permanentes

Los controles sobre los cambios a los datos permanentes nos permiten confirmar la corrección de la información al impedir o detectar las modificaciones erróneas o no autorizadas. Al intentar procesar cambios erróneos (de acuerdo con funcionarios del cliente), podemos confirmar que los errores son adecuadamente informados para su seguimiento y corrección.

4. Prueba de comparaciones, cálculos, registraciones y acumulaciones

Las transacciones de prueba pueden ser preparadas y sometidas a funciones de procesamiento computadorizadas tales como cálculos, imputaciones y acumulaciones. Si los resultados reales concuerdan con los previstos, existirá una razonable seguridad de que las funciones de procesamiento computadorizadas funcionan de la manera esperada. Algunos ejemplos de funciones de procesamiento que pueden ser probadas son:

- Precios y cantidades de facturas de proveedores comparadas con las órdenes de compra y de recepción.
- Cálculos de las remuneraciones brutas y netas.
- Sumas y multiplicaciones.
- Provisión por compras recibidas pero no facturadas.
- Acumulación de costos de existencias.
- Cálculos de intereses.
- Depreciación de activos fijos.
- Anticuación de cuentas a cobrar.
- Resúmenes de distribución de cuentas a pagar.

5. Prueba de totales de control

Se pueden utilizar controles de sesión, recuento de registros y otros totales de control generados durante el procesamiento para detectar transacciones no autorizadas, faltantes, duplicadas o erróneas. Se pueden emplear transacciones de prueba ingresadas y procesadas como un lote o sesión separada para verificar que los totales de control generados por el sistema sean correctos.

V. Consideraciones sobre el Personal

Debemos considerar la posibilidad de solicitar al cliente la colaboración de su personal para el desarrollo y codificación de los programas de recuperación y análisis, y las transacciones de prueba. Esto presenta las siguientes ventajas:

- El personal del cliente está familiarizado con las operaciones CIS, archivos de datos y equipos de computación de la empresa, lo cual contribuye a reducir el tiempo de desarrollo y procesamiento de las aplicaciones de auditoría.
- Los programas pueden ser desarrollados más rápidamente si el cliente cuenta con personal que sea usuario frecuente del software de auditoría.
- El personal del departamento usuario puede sernos útil en la selección de las transacciones que elegimos para ser probadas.

La decisión de usar técnicas de auditoría computadorizadas desarrolladas por el cliente no debe basarse sólo en estas ventajas. Existen otros aspectos que deben tenerse en cuenta, a saber:

- El personal del cliente puede tener mayores oportunidades de manipular los datos, ya que conocen las pruebas de auditoría que se llevan a cabo.
- La disponibilidad de empleados competentes del cliente que pueden completar el trabajo dentro de los plazos establecidos para nuestro examen.
- La independencia del personal del Departamento de Auditoría Interna del cliente .
- La disponibilidad de nuestro personal con experiencia apropiada para revisar el trabajo hecho por el cliente.
- El esfuerzo que implica obtener una razonable seguridad de que las técnicas desarrolladas por el cliente producen resultados precisos y confiables.

Los programas de recuperación y análisis contienen a menudo instrucciones que indican el alcance y criterios de selección, así como también otro tipo de información importante acerca de los procedimientos que se llevan a cabo. Como sucede con cualquier otro procedimiento de auditoría, si el personal del cliente conoce nuestros criterios de selección y el alcance del trabajo, puede llegar a interferir en los resultados de nuestros procedimientos o pueden registrar transacciones incorrectas o fraudulentas. Por lo tanto, y siempre que sea posible, debemos restringir el acceso del cliente a este tipo de información.

Si existen debilidades en los controles del departamento CIS o si no los hemos revisado, debemos considerar cuidadosamente si es conveniente emplear técnicas de

auditoría computadorizadas desarrolladas por el cliente. Tal vez la conclusión sea que el tiempo y el costo de evaluar los controles del cliente, o de establecer por nuestra cuenta los controles apropiados, superan los beneficios que se obtendrían con el uso de técnicas desarrolladas por el cliente.

Las mismas consideraciones se presentan cuando las técnicas de auditoría computadorizadas son desarrolladas por el personal del Departamento de Auditoría Interna del cliente. Debemos asegurarnos de que los auditores internos mantengan un control adecuado durante las etapas de desarrollo, prueba y procesamiento y que documentan la evidencia de su trabajo y de los controles aplicados en base a los mismos requerimientos que rigen para nuestros propios trabajos.

Cuando desarrollamos técnicas de auditoría computadorizadas, podemos requerir la asistencia del cliente en la obtención o preparación de la información técnica, incluyendo descripciones de archivos y especificaciones de los equipos instalados, Por lo general, será más eficiente utilizar para estas tareas personal del cliente que realizarlas nosotros mismos.

VI. Consideraciones sobre las Instalaciones de Computación

Los programas de recuperación y análisis o las técnicas de transacciones de prueba pueden ser procesadas en el computador del cliente, en un servicio externo de computación o en nuestros propios computadores.

Cuando se utilice el computador del cliente, se deben evaluar los controles del departamento CIS del cliente, a fin de asegurarnos de que nuestros programas o datos de prueba no sean alterados durante el procesamiento, ya sea en forma intencional o involuntario. La existencia de debilidades de control puede afectar la confianza en los resultados obtenidos del procesamiento.

El uso del computador del cliente tiene las siguientes ventajas:

- Usualmente no existe un costo directo del tiempo de computador utilizado.
- El cliente puede brindar asistencia técnica y apoyo operativo.
- Al observar el procesamiento podemos obtener una mejor comprensión de los controles del departamento CIS del cliente.

Por otra parte, se deben considerar las siguientes desventajas potenciales:

- Puede ser más difícil alcanzar el nivel deseado de control de auditoría.
- El software provisto por los auditores puede no ser compatible con el computador del cliente, o su instalación puede insumir mucho tiempo y ser costosa.

El uso de un servicio externo de computación debe ser considerado cuando:

- El cliente está distante de nosotros, o cuando no existe la suficiente disponibilidad de tiempo en su computador.
- Una parte importante de la evidencia de auditoría se obtiene a través de los programas de recuperación y análisis y los controles del Departamento CIS son débiles.
- El costo de emplear un servicio externo es inferior al costo de desarrollar un programa compatible con el sistema del cliente.

Un aspecto importante a tener en cuenta al considerar el uso de un servicio externo son los costos adicionales en que puede incurriese. Estos costos, por lo general, son significativos. Por ejemplo, el bloqueo incorrecto de datos para aumentar la cantidad de lecturas y búsquedas puede tornar costoso un procedimiento que, de lo contrario, sería barato.

En determinadas circunstancias, los procedimientos de auditoría computadorizados también pueden ser procesados en los computadores de la firma. Son válidas al respecto las consideraciones mencionadas para un servicio externo, con la excepción de que normalmente no necesitaremos satisfacernos acerca de los controles del departamento CIS.

VII. Relación Costo/Beneficio

Antes de comenzar con el trabajo detallado para la implantación de los procedimientos de auditoría computadorizados, es esencial evaluar el costo en términos e beneficio que proporciona a la auditoría en general, La relación costo/beneficio del uso de técnicas computadorizadas dependerá, por lo general, de la complejidad de la aplicación y de los costos previstos para las técnicas alternativas, Puede suceder que a veces las técnicas computadorizadas sean el único procedimiento de auditoría disponible.

Antes de comprometer recursos se debe hacer una estimación del tiempo y de los costos inherentes a su implantación. Al realizar un análisis de costo/beneficio, se deben considerar los beneficios que se obtendrán a lo largo de varios años. Al realizar esta estimación se debe evaluar la posibilidad de que, en el futuro, la aplicación sea modificada (ya sea como consecuencia de cambios en los sistemas y programas o ante cambios en nuestro enfoque de auditoría). Es responsabilidad del socio a cargo decidir si se amortizan o no los costos de desarrollo.

1. Costos de desarrollo inicial

Los costos de desarrollo son afectados por:

- La complejidad de la aplicación.
- El procedimiento a realizar.
- El personal necesario para:
  - Obtener la información técnica y efectuar la planificación.
  - Capacitar al equipo de trabajo en el uso de la técnica.
  - Diseñar, preparar, compilar, probar y documentar la técnica.
  - Mantener los programas y datos de prueba.
- La asistencia que recibiremos del personal del cliente (ya sea del Departamento CIS u otros).
- Los costos adicionales, tales como el costo del tiempo de computador necesario para probar y procesar los programas, suministros y otros servicios especiales tales como transcripción de claves.

2. Costos recurrentes y ahorros anuales

Los costos recurrentes que habitualmente hay que considerar incluyen:

- El costo del personal necesario para :
  - Reinstalar el software, si no está instalado en el lugar de procesamiento.
  - Modificar la aplicación si fuese necesario.
  - Presenciar el procesamiento si fuese necesario.
  - Realizar el seguimiento y las pruebas de los informes de salida.
  - Preparar la documentación.
- Los costos adicionales, tales como costo del tiempo del computador, suministros y servicios especiales.

Al analizar el tema de los costos de desarrollo inicial se debe prestar especial atención a la documentación del sistema de aplicación relacionado con la respectiva técnica de auditoría computadorizada. La documentación se utiliza para obtener una comprensión del sistema, incluyendo los contenidos y formatos de los programas y archivos de datos más importantes. Si la documentación está desactualizada, incompleta o es inexacta, es posible que el desarrollo de la técnica de auditoría computadorizada insuma mucho más tiempo.

El uso de técnicas de auditoría computadorizadas generará a menudo significativos ahorros recurrentes. Habitualmente, las pruebas manuales pueden ser reducidas substancialmente, lo cual deriva en importantes ahorros de dinero y además permite la reasignación a otros trabajos del personal que de lo contrario, estaría realizando las pruebas manuales.

Si bien es difícil establecer pautas precisas para la estimación de costos y ahorros, se pueden hacer estimaciones preliminares de costo/beneficio razonables al considerar por primera vez el uso de técnicas de auditoría computadorizadas; las que deben ser revisadas al finalizar el proceso de planificación. Es posible que los costos estimados para el desarrollo y operación de las técnicas de auditoría computadorizadas reflejen un ahorro en el primer año de uso, en especial si involucran archivos de datos voluminosos o la obtención de datos que, de otra manera, no estarían disponibles. Sin embargo, lo más habitual es obtener un punto de equilibrio transcurridos uno o dos años desde el momento del desarrollo inicial; si el punto de equilibrio se logra recién después de dos años es difícil que se pueda justificar el costo de la aplicación.

Es importante destacar que el análisis costo/beneficio debe incluir otras consideraciones además de las monetarias. También debemos reconocer los importantes beneficios no monetarios, como por ejemplo:

- Satisfacción de las expectativas del cliente en cuanto al uso de técnicas de auditoría computadorizadas.
- Mayor seguridad en el trabajo de auditoría al contar con la posibilidad de probar un archivo de datos completo.
- El personal de auditoría involucrado en el desarrollo y procesamiento de la aplicación computadorizada obtiene una mejor comprensión de los sistemas del cliente.
- El efecto positivo en el equipo de trabajo, al comprobar que se automatizan los procedimientos repetitivos y monótonos que antes se hacían manualmente.
- La oportunidad de "agregar valor" al trabajo de auditoría, al poder efectuar recomendaciones a la gerencia superior referidas a mejoras en los controles, procedimientos de información, etc., como resultado de la aplicación de procedimientos de auditoría computadorizados.

VIII. Controles

1. Consideraciones sobre los controles

Las consideraciones relativas a los controles deben formar una parte integral de las decisiones de utilizar técnicas de auditoría computadorizadas.

En algunos casos depositaremos nuestra confianza en ciertos controles CIS del sistema de aplicación del cliente que estamos probando, para asegurarnos de la exactitud de la información de salida de la aplicación de auditoría.

Por lo general, las consideraciones más importantes sobre controles del departamento CIS con respecto al uso de técnicas computadorizadas son las relativas a una adecuada segregación de tareas entre los usuarios, programadores y operadores del computador y a que existan controles adecuados para restringir el acceso al software de aplicación y del sistema y a los archivos de datos. En el caso de una aplicación de auditoria que depende de éstos y otros controles generales, será necesario obtener y documentar una comprensión de los controles y obtener evidencia de que operan en forma efectiva. Si un programa de recuperación y análisis se prueba por sí mismo (autoprueba) y es en su totalidad de naturaleza sustantivo, no se requiere confiar en los controles del departamento CIS.

Aunque un programa de recuperación y análisis se autopruebe, no existe seguridad de que los archivos de datos sean exactos y completos en tanto no existan procedimientos que aseguren que las transacciones son completa y correctamente procesadas en los períodos contables adecuados y que están protegidas contra accesos no autorizados. Por ejemplo, si se ingresan datos incorrectos en los formularios de entrada o si se extravían las transacciones antes de ser ingresadas, el archivo de datos coincidirá con los totales de control pero no estará completo ni exacto. En otras palabras un programa de recuperación y análisis que se autoprueba no proporcionará automáticamente la evidencia de auditoría apropiada.

Si necesitamos confirmar que los archivos de datos son completos y exactos, será necesario realizar las pruebas adecuadas. La integridad del archivo de datos puede ser probada comparando los totales del archivo con los registros llevados externamente y utilizando otros procedimientos de auditoría para probar que todos los ltems que deberían haber sido incluidos en los totales externos, hayan sido incluidos.

También se deben evaluar los procedimientos de respaldo de archivos y programas del cliente, ya que muchas organizaciones no cuentan con un sistema adecuado.

Los programas de recuperación y análisis o transacciones de prueba no deben ser procesados a menos que exista algún tipo de copia de respaldo de los archivos o programas de datos.

El principal objetivo de establecer controles sobre las técnicas de auditoría computadorizadas es proporcionar una adecuada seguridad de que:

- El programa de recuperación y análisis o los datos de prueba alcanzarán el objetivo preestablecido. (Desarrollo)
- No se han producido manipulaciones o uso no autorizado de los programas o datos de prueba desde la última vez que se utilizaron. (Custodia)
- Los programas son aplicados a los archivos de datos correspondientes y los datos de prueba son procesados por el programa correspondiente. (Ejecución).

Estas consideraciones son tratadas en forma más detallada a continuación.

Desarrollo

- ¿ Qué importancia tiene la técnica de auditoría computadorizada en el esfuerzo total de auditoría necesario para satisfacernos de una aserción en particular?
- ¿ Se utilizarán los programas de recuperación y análisis o los datos de prueba existentes o se desarrollarán nuevas técnicas de auditoría computadorizadas?
- ¿Quién escribirá los nuevos programas o preparará las nuevas transacciones de prueba: personal de auditores o personal del cliente?
- ¿ Qué software se va a utilizar como fuente de los programas: el de auditoría externa o el que tiene instalado el cliente?
- ¿ Qué experiencia tiene el personal de auditoría externa o del cliente en el uso del software de auditoría seleccionado?

Custodia

- ¿Quién custodiará los programas de recuperación y análisis o los datos de prueba mientras no se los usa?
- ¿Si los programas o datos de prueba son guardados en la biblioteca de una instalación, ¿ son adecuados los controles para prevenir accesos y modificaciones no autorizadas? ¿ Retiene los auditores una copia?

Ejecución

- ¿ En qué medida se autoprueba el programa de recuperación y análisis?
- ¿ Dónde se procesarán los programas o datos de prueba: los auditores, en el equipo del cliente o en un servicio externo de computación?
- ¿Son adecuados los controles del departamento CIS en las áreas que pueden afectar el procesamiento de la aplicación de auditoría?

Estas consideraciones se verán afectadas por la complejidad de cada aplicación de auditoría en relación con el hardware, software y recursos humanos disponibles. Por ejemplo, un sencillo programa de recuperación que utiliza un utilitario de consulta on line para analizar los pagos de cuentas seleccionadas en el seguimiento de la circularización de cuentas a cobrar, requerirá menor preocupación por los aspectos mencionados y una menor planificación que en el caso del desarrollo de un complejo programa de un paquete de software para realizar diversos procedimientos de recuperación y reprocesamiento de información. La primera aplicación puede ser realizada por personal de auditoría sin necesidad de asistencia de un especialista, para la segunda se necesita la participación de un especialista.

2. Posibles controles

Algunos ejemplos de los posibles controles en cada categoría son:

Desarrollo

- El programa de recuperación y análisis o la técnica de transacciones de prueba debe ser planificada y documentada.
- Se deben efectuar pruebas para asegurar que la lógica de los programas de recuperación y análisis es correcta.

Custodia

- Si el programa de recuperación y análisis o las transacciones de prueba son mantenidas en la biblioteca del cliente, se deben considerar los controles de biblioteca para prevenir accesos no autorizados.
- Antes de correr nuevamente un programa deberá ser comparado con la última corrida para asegurarnos de que no se le han efectuado modificaciones.

- Se debe mantener en nuestros archivos una copia de los programas y transacciones de prueba.

Ejecución

- Asegurarse de que se prepara la documentación necesaria y que la misma describe cómo se debe correr la aplicación de, auditoría, cuándo y qué archivos y programas se deben utilizar.
- Obtener un listado del programa y del estado de ejecución de tareas con sus correspondientes resultados para aseguramos de que se emplearon las versiones correctas de los programas y de que los programas de recuperación y análisis leyeron los archivos correctos.
- Conciliar los totales producidos por una aplicación de transacciones de prueba con totales de auditoría predeterminados.
- Revisar el registro de operaciones para verificar si hubo interferencias en la corrida de la aplicación de auditoría y para determinar si se utilizaron los archivos y programas correctos.
- Considerar la conveniencia de presenciar el procesamiento.

Uno de los métodos más importantes para controlar los programas de recuperación y análisis es desarrollar aplicaciones que se autoprueban. Las técnicas de transacciones de prueba, por su naturaleza, se autoprueban, por ej., la información de salida se concilia con resultados predeterminados. Las siguientes características están usualmente presentes en los programas de recuperación y análisis que se autoprueban:

- Los totales de control pueden ser conciliados con los registros contables del cliente.
- La lógica de los programas es relativamente simple,
- Se utilizan controles para detectar errores de lógica que podrían inadvertidamente eliminar registros erróneos para informes de excepciones.
- El número total de registros de un archivo leídos cuando se preparan informes de excepciones o se seleccionan pruebas de auditoría, se informan para su conciliación con los registros del cliente.

Debemos tener en cuenta que los controles que rodean algunas instalaciones de micro y minicomputadores son tales que debemos tener mayor precaución en asegurarnos de que los programas de recuperación y análisis se autoprueban.

En la siguiente Tabla se resumen controles que pueden ser importantes tanto para los programas de recuperación y análisis como para las técnicas de transacciones de prueba. En la Tabla se incluyen ejemplos de debilidades en los controles del cliente que pueden afectar la confiabilidad de las técnicas de auditoría computadorizadas, además de consideraciones sobre su incidencia en el uso de estas técnicas. Si bien la lista dista de ser completa, ayuda a pensar en la relación "causa y efecto" al planificar el uso de las técnicas de auditoría computadorizadas.

PROGRAMAS DE RECUPERACION Y ANALISIS

Técnica	Posibles Controles
Paquetes de software de auditoría	• Revisar los controles sobre el acceso a programas y archivos de datos. • Controlar los informes de ejecución de tareas para asegurar que el nombre del archivo (dataset) coincide con el de] archivo de producción. • Identificar los campos de valores para su conciliación con los registros contables. • Revisar y probar la lógica del programa. • Comparar los campos detallados con los diseños de lo registros del cliente. • Considerar la conveniencia de presenciar el procesamiento.
Software de recuperación	• Posiblemente requiera mayor confianza de información en los controles de acceso. • Desarrollar aplicaciones que se autoprueben. • Considerar la conveniencia de presenciar el procesamiento. • Si fue desarrollado por el cliente, evaluar la independencia y revisar la segregación de funciones. • Revisar y probar la lógica del programa. • Controlar los informes de ejecución de tareas para asegurar que el nombre de[archivo (dataset) coincide con el del archivo de producción.
Programas utilitarios	• Revisar los controles sobre modificaciones al software de sistemas. • Desarrollar una aplicación que se autopruebe para asegurar que se procesan todos los registros. • Controlar los informes de ejecución de tareas para asegurar que se utilizan el archivo (dataset) y utilitario correctos. • Revisar los parámetros de uniformidad y razonabilidad.
Lenguajes convencionales	• Revisar el código fuente para asegurar que la programación lógica del programa sea correcta, • Compilar cada corrida del programa desde una copia fuente adecuada. • Considerar la conveniencia de presenciar el procesamiento. • Controlar los informes de ejecución de tareas para confirmar que se utilizan el archivo y el programa correctos, • Desarrollar una aplicación que se autopruebe.
Datos o lotes de prueba	• Revisar los informes de ejecución de tareas para asegurar que las versiones empleadas de los programas son las correctas. • Considerar los controles sobre modificaciones a los programas. • Considerar la estructura organizativa y los procedimientos operativos del departamento CIS. Conciliar los datos ingresados con los totales procesados en forma manual. • Prueba on line de los controles de validación. • Realizar los controles en forma sorpresivo. • Considerar los controles sobre acceso no autorizado a programas y archivos de datos.
Procedimiento de prueba	• Asegurar que el acceso a la entidad simulada integrada es adecuadamente restringido. • Considerar los controles sobre modificaciones a los programas. • Considerar la estructura organizativa y los procedimientos operativos del departamento CIS. • Seguimiento manual de las rutinas de rechazo de datos, • Considerar los controles sobre acceso no autorizado a programas y archivos de datos. • Asegurar que se registran adecuadamente todas las transacciones simuladas.
Pruebas on-line	• Planificación anticipada con el cliente. • Llevar a cabo las pruebas durante el horario normal de procesamiento. • Asegurar que se efectúa el seguimiento de todos los rechazos. • Asegurar que todos los asientos "erróneos" son reservados.

IX. Documentación

La documentación es una parte importante de nuestro control sobre las técnicas de auditoría computadorizadas. La documentación de estas técnicas es similar a la de cualquier otra técnica de auditoría que debe ser lo necesariamente extensa a fin de:

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

Existen diversos métodos de documentación. Uno de ellos (según la complejidad de la aplicación) es preparar dos juegos de papeles de trabajo. Las planillas de documentación acumulativa de planificación brindan información básica sobre la naturaleza de la aplicación y el ambiente CIS, los papeles de trabajo corrientes registran la información relativa a la corrida de la aplicación del año corriente, junto con los informes de salida para su inclusión en el archivo corriente.

En la siguiente Tabla se detallan los ítems sugeridos para su inclusión en las planillas acumulativas de planificación que cubren la planificación de auditoría y el desarrollo de la aplicación y, para los papeles de trabajo corrientes que cubren la evidencia de auditoría del año corriente.

ASPECTOS SUGERIDOS PARA DOCUMENTACION

PLANIFICACION

- Evidencia de auditoría específica a obtener.
- Descripción de la técnica computadorizada seleccionada. Quién escribirá los programas de recuperación y análisis.
- Quién preparará los datos de prueba.
- Dónde y cómo serán procesados.
- Consideraciones sobre los controles.
- Personal necesario y contactos con el cliente.
- Estimación del tiempo necesario.
- Estimaciones preliminares de[costo/beneficio.
- Naturaleza del trabajo que se realizará con los datos resultantes.

PROGRAMA DE RECUPERACION Y ANALISIS Y DOCUMENTACION DE DATOS DE PRUEBA

- Detalles de los procedimientos de auditoría realizados (datos probados) mediante la aplicación de auditoría.
- Detalle de las rutinas probadas (edición, validación, cálculo, etc.)-
- Detalles relativos a la preparación de[programa, incluyendo el software y los controles usados durante el desarrollo.
- Especificaciones de la corrida incluyendo entrada, pasos del procesamiento y salida de datos.
- Información de los sistemas, incluyendo diseño de archivos, formato de los registros, descripción de los campos y cursogramas (si fuera necesario)
- De qué forma fue probado el sistema.
- Documentación del programa final (listados de programas, cursograma o descripción narrativa).
- Copia de las transacciones de prueba y resultados predeterminados.

EVIDENCIA DE AUDITORIA DEL AÑO CORRIENTE

- Controles del cliente que afectan el procesamiento de la aplicación de auditoría.
- Los resultados obtenidos.
- Detalles del trabajo de auditoría realizado sobre los resultados,
- Resolución de los errores, excepciones o partidas inusuales detectadas.
- Problemas administrativos y técnicos detectados y cómo fueron solucionados.
- Conclusión (en relación con los requerimientos de auditoría)
- Recomendaciones a la gerencia.
- Sugerencias de mejoras para años futuros.
- Comparación de costos reales con los presupuestados.

X. Implantación de los Programas de Recuperación y Análisis

1. Consideraciones sobre Factibilidad

Las etapas enunciadas a continuación son presentadas en una secuencia lógica para facilitar su tratamiento; en la práctica suele suceder que algunas de ellas se llevan a cabo al mismo tiempo o en distinto orden:

- Obtención de información técnica.
- Definición de la evidencia de auditoría específica y otros requerimientos.
- Preparación del plan detallado de trabajo.
- Reconsideración de las decisiones de planificación de auditoría.

1.1 Obtención de información técnica

La primera etapa de implantación consiste en obtener la información técnica necesaria para diseñar y escribir los programas de recuperación y análisis. La información que se requiere habitualmente incluye:

- Una descripción del computador a ser utilizado, incluyendo sus equipos periféricos y las características físicas de los archivos de entrada y salida.
- Detalles del software del sistema operativo del cliente y de los utilitarios disponibles.
- Documentación de sistemas, como cursogramas y descripciones narrativas, para obtener un conocimiento del sistema y los programas.
- Copia de los diseños de archivos para comprender qué campos están incluidos en los archivos.
- Definiciones y descripciones de los campos y de los códigos de transacción, para comprender qué información se incluye en cada campo.
- Copias de los vuelcos de archivos de datos para verificar la exactitud de los diseños de los archivos y otra documentación que se considere necesaria.

La cantidad de información técnica necesaria depende de los requerimientos de programación del software de auditoría a utilizar y de la complejidad de la aplicación y del sistema en que se procesarán los programas.

Siempre que sea posible, se debe solicitar al personal de procesamiento de datos que proporcione la información y confirme su exactitud e integridad. Esto contribuye a asegurar que los programas sean eficientemente desarrollados. La información debe ser

cuidadosamente analizada, ya que esta revisión puede develar aspectos desconocidos cuando se consideró el uso de técnicas de auditoría computadorizadas. En este momento se deben evaluar cuidadosamente los requerimientos preliminares de los programas para determinar si existen posibilidades de que los mismos sean alcanzados.

1.2 Definición de la evidencia de auditoría específica y otros requerimientos

La evidencia de auditoría a ser obtenida y los requerimientos para los programas deben ser definidos en términos específicos para facilitar la implantación del diseño del programa. Las especificaciones pueden incluir:

- El archivo del cual se deben seleccionar los datos,
- Los campos a ser totalizados.
- Los campos adicionales a ser calculados.
- Los criterios de selección de muestras o de realización de cálculos.
- La información que debe ser incluida en los informes de salida y su formato.

1.3 Preparación del plan detallado de trabajo

Los arreglos efectuados para obtener los recursos necesarios, los responsables de las distintas tareas, la fijación de fechas clave y la comunicación de información a las personas apropiadas pueden ser detallados en un plan de trabajo. Este plan debe incluir lo siguiente:

- Obtención de copias de los archivos de datos necesarios.
- Obtención de asistencia técnica y administrativa para actividades tales como la preparación de informes de ejecución de tareas y de archivos y para cargar el software de auditoría en el sistema del cliente.
- Preparación del diseño detallado del programa y de las especificaciones lógicas.
- Preparación de los parámetros del programa o código fuente.
- Compilación y prueba del programa,
- Obtención de suministros tales como formularios preimpresos, archivos de cintas "scratch", etc.
- Programación del tiempo de uso del computador y otros recursos (por ejemplo: disponibilidad de las terminales) para el procesamiento.
- Definición de los procedimientos y documentación de control,
- Asegurarse de que se utilizan los archivos correctos.
- Distribución de los resultados.

- Determinación de las pruebas de auditoría para el seguimiento de los resultados.

1.4 Reconsidoración de las decisiones de planificación de auditoría

Las decisiones preliminares de planificación de auditoría y la estimación de costos y beneficios debe ser reconsiderada a la luz de la información adicional obtenida. Se deben reconsiderar las herramientas de auditoría disponibles y las consideraciones de planificación tratadas en planificación y Control de las Técnicas de Auditoría Computadorizadas, incluyendo :

- ¿Qué software se va emplear para escribir los programas?
- ¿Quién escribirá y correrá los programas?
- ¿Qué procedimientos de control se van a aplicar y cómo se documentará el trabajo?
- ¿Cuáles son los costos y ahorros previstos?
- ¿Cuánto tiempo insumirá el desarrollo?

2. Diseño y Prueba de los Programas

El diseño y prueba de los programas generalmente involucro los siguientes aspectos:

- Especificaciones detalladas.
- Controles programados.
- Programación.
- Compilación del programa.
- Prueba del programa.

2.1 Especificaciones detalladas

Las especificaciones detalladas que se describen a continuación son importantes ya que proporcionan un plan lógico por etapas en base al cual se pueden escribir y mantener los programas. Estas especificaciones incluyen información relativa a los archivos de datos, informes de ejecución de tareas y pasos detallados del programa. Cuando los programas son escritos por alguien que no pertenece al equipo de trabajo, debemos participar en la definición de las especificaciones.

Las especificaciones detalladas deben ser desarrolladas en base a la información técnica obtenida ya los requerimientos específicos definidos durante la planificación del programa. El grado de detalle requerido dependerá de la complejidad del programa que será

desarrollado. Un programa simple puede ser desarrollado en base a la información de planificación sin necesidad de contar con especificaciones detalladas adicionales.

La información técnica obtenida anteriormente se utilizará para especificar:

- Entradas y salidas de información a y de los archivos, incluyendo medios magnéticos usados, información relativa a los rótulos internos y externos, etc..
- Equipos necesarios para el procesamiento incluyendo unidades de discos y de cintas, terminales e impresoras.
- Secuencia del procesamiento de programas y archivos.

Esta y toda otra información relacionada será habitualmente utilizada por el programador para preparar los informes de ejecución de tareas para el sistema operativo. Los informes de ejecución de tareas proporcionan el vínculo entre el programa a ejecutar y el sistema operativo del computador. A través de una serie de instrucciones los informes de ejecución de tareas:

- Conceden autorizaciones para la corrida del trabajo.
- Asignan los equipos periféricos necesarios para ejecutar el trabajo.
- Ponen en marcha el sistema de registración de trabajos.
- Especifican el programa a ser ejecutado.
- Especifican los archivos a ser utilizados.
- Inician la ejecución del programa.
- Determinan el nivel de registración del trabajo.

El programador debe desarrollar las especificaciones detalladas del programa para que la evidencia de auditoría y otros requerimientos a ser obtenidos puedan ser traducidos a instrucciones codificadas. Para esto se necesita una definición clara de:

- Las operaciones a llevar a cabo.
- Los campos de entrada en los que se realizarán las operaciones.
- Los controles programados para la aplicación.
- Los datos de salida esperados.

Es útil reverenciar en forma cruzada cada ítem de los resultados a ser obtenidos con los campos de datos de entrada, a través de la lógica del programa. Por ejemplo:

Datos de salida	Procesamiento	Datos de entrada
Campo AAA	Se imprime sin cambios desde	Campo xxx.
Total AAA	Valor total de todos los ítems en	Campo xxx.
Campo WWW	Calculado por multiplicación del	Campo zzz por el yyy.

2.2 Controles programados

Los siguientes controles programados contribuyen a que una aplicación se autopruebe.

- Desarrollo de totales monetarios de control. Generalmente es conveniente que los valores monetarios de los campos clave de los registros de ingreso sean totalizados e impresos por el programa para ser cotejados posteriormente con los totales de control que se llevan fuera del Departamento CIS. De lo contrario, puede ser difícil verificar que se está empleando una copia correcta del archivo de datos.
- Desarrollo de otros totales de control en puntos apropiados de la lógica del programa. Los totales de control que permiten verificar la exactitud de la lógica del programa pueden incluir:
  - Recuento del número de registros leídos en cada archivo de entrada. Los recuentos pueden ser luego cotejados con totales de control de registros. Esta técnica es recomendada aún cuando se está en condiciones de generar y balancear totales de control monetarios, ya que brinda seguridad adicional de que el programa está procesando una copia completa del archivo de datos.
  - Los totales de control "paso a paso" para las aplicaciones que usan varios programas permiten asegurar que no se pierdan inadvertidamente los registros durante el procesamiento y brindan asimismo un rastro de auditoría.
  - Recuento de registros y totales de control para los registros que cumplan y no cumplan con los criterios de selección. Por ejemplo: el total de cuentas a cobrar seleccionadas en base a una estratificación y el total de cuentas no seleccionadas son impresos a fin de determinar si todas las cuentas fueron sometidas a los parámetros de selección de muestras. Estos totales permiten asegurar que cada registro ha sido examinado o probado en base a los criterios especificados y que las transacciones pasaron a través de los correspondientes puntos de la lógica del programa. Estos totales son de especial importancia cuando el programa contiene una gran cantidad de puntos de decisión o caminos lógicos. El uso de los totales permite detectar errores de programación que pueden ocurrir cuando la lógica del programa no está preparada para condiciones imprevistas.

- Verificación de rótulos internos estándar. Estos rótulos contienen información que puede ser utilizada para verificar si el nombre, versión y fecha de creación de un archivo son correctos. Cuando los archivos no cuentan con estos rótulos o si no son verificados con los programas de recuperación y análisis, es importante llevar a cabo conciliaciones luego del procesamiento para confirmar si se utilizaron los archivos adecuados.

Aunque se hayan implantado controles programados apropiados, la ausencia de controles manuales sobre el procesamiento de transacciones puede resultar en archivos incompletos o inexactos, ya que puede ser que no todas las transacciones hayan sido ingresadas al sistema, algunas pueden haber sido procesadas en el período contable inadecuado o algunas de las ingresadas al sistema pueden ser inexactas o estar duplicadas. Si los archivos son inexactos o incompletos, la evidencia de auditoría obtenida de los programas de recuperación y análisis será incompleta o inexacta. Por otra parte, los programas de recuperación y análisis pueden indicar que los archivos son inexactos, por ejemplo, que contienen registros duplicados, registros simulados, etc.

2.3 Programación

La tarea decodificar el programa se ve simplificada si se cuenta con especificaciones bien definidas. La codificación puede ser realizada por un miembro del equipo de trabajo o por personal del cliente, como por ejemplo los auditores internos.

Toda codificación que no sea realizada por miembros del equipo de trabajo debe ser revisada por un miembro del equipo que esté familiarizado con el lenguaje de programación, para confirmar que el trabajo ha sido realizado según las especificaciones detalladas que fueron proporcionadas. Si no existe ningún miembro del equipo de trabajo que conozca el lenguaje de programación, las pruebas del programa deben ser más exhaustivas.

2.4 Compilación del programa

Una vez preparado el programa fuente, generalmente se lo compila a un formato ejecutable (programa objeto). Es preferible que el programa sea compilado en la instalación en la que será ejecutado.

La compilación del programa normalmente da lugar a mensajes de error o advertencias relativas al programa. Estos mensajes deben ser revisados para tomar las medidas correctivas necesarias, para lo cual puede requerirse ayuda técnica de especialistas.

Una vez obtenida una compilación correcta, se debe probar el programa objeto generado por el proceso de compilación.

2.5 Prueba del programa

El objeto de la prueba del programa es asegurar la exactitud de su lógica y proporcionar una razonable seguridad de que se alcanzarán los requerimientos deseados. Aún después de un proceso exitoso de compilación pueden subsistir errores en la lógica del programa.

El alcance de la prueba varía de un programa a otro. Por lo general, las pruebas son más detalladas si:

- Se trata de un programa "vivo" existente, usado o modificado para obtener un requerimiento específico (ya que un error en ese programa puede ser duplicado en el programa utilizado para propósitos de auditoría).

- La codificación del programa estuvo a cargo de personal del cliente (programadores o auditores internos)

- El programa contiene una lógica compleja.
- Se utilizó un lenguaje de programación convencional. Estos lenguajes son más difíciles de utilizar que otras fuentes de software de auditoría y, por lo tanto, existen más posibilidades de cometer errores.
- El programa no se autoprueba.

En el caso de programas sencillos, se puede obtener una adecuada satisfacción de que el programa funciona de acuerdo con lo previsto mediante la inclusión de controles programados adecuados y el control de los datos resultantes.

Los programas pueden ser probados por los siguientes métodos:

- *Prueba de escritorio.* Este es un método preliminar que puede ser usado junto con otros métodos de prueba. Se prepara una muestra de transacciones de prueba. Una vez que se completa la codificación, las transacciones son procesadas manualmente a través de la lógica del programa.

- *Datos de prueba..* Este método de prueba de la lógica del programa es similar a las técnicas de transacciones de prueba. El programa es procesado usando un archivo de datos de transacciones de prueba, se concilian los totales de control y se verifica la exactitud de los resultados del programa comparándolos con una tabla de resultados esperados. Las transacciones de prueba deben representar todas las variaciones significativas de tipos de transacciones que puedan existir en los archivos de datos sometidos a prueba y deben asegurar que se prueban todos los caminos lógicos relevantes que incluye el programa.
- *Muestra pequeña.* Utilizando este método se imprime un cierto número de registros seleccionados del archivo de entrada antes del procesamiento y del de salida después del procesamiento. Los datos de entrada procesados son controlados mediante un seguimiento manual hasta los registros de salida. Este método es similar al de prueba de escritorio, ya que el procesamiento es reproducido manualmente con el fin de verificar que el programa produce resultados correctos. Por lo general insume menos tiempo que el método de datos de prueba y brinda mayor seguridad que la prueba de escritorio, ya que se verifican resultados del procesamiento real.

Al margen del método de prueba que se utilice, cuando se detectan diferencias entre los resultados reales y los esperados se debe determinar si las mismas se originan en errores en los resultados predeterminados o en errores de lógica del programa. Si el programa tiene errores, es necesario corregir los enunciados fuente, compilar el programa y repetir el proceso de prueba.

Se debe conservar una copia de control del programa probado en código fuente y en un formato que pueda ser leído por el computador para usos futuros. Si nosotros conservamos el programa no será necesario probar el programa cada vez que se lo utilice en el futuro.

3. Procesamiento del Programa

Cuando se utilizan programas de recuperación y análisis, se deben tener en cuenta dos aspectos desde el punto de vista de control:

- Que no haya habido acceso no autorizado al programa desde la última ejecución.
- Que el programa sea procesado con los archivos de datos apropiados, completos y exactos.

Algunos procedimientos indicados para cumplir con estos objetivos son:

- Archivar los programas e informes de ejecución de tareas en bibliotecas protegidas por un software de control de acceso tal como RACF. El acceso sólo debe estar permitido a los miembros del equipo de trabajo.
- Imprimir los rótulos internos de encabezamiento de los archivos a los que se accede, para su posterior comparación, si fuera aplicable, con:
  - Los vuelcos de archivo obtenidos en la etapa del desarrollo original del
  - programa.
  - Fechas de creación, nombres y números de serie de los grupos de datos
  - incluidos en los registros de biblioteca.
  - Listado de los informes de ejecución de tareas.
- Comparar los totales de control desarrollados por el programa con los registros contables del cliente.
- Solicitar al operador que retenga los archivos usados por el programa hasta tanto sean controlados los totales de control.
- Una vez completados los procedimientos, realizar una copia en cinta del programa.
- Borrar el programa si no es mantenido en una biblioteca de programas adecuadamente protegida.
- Obtener una copia de control del programa, si fuera posible, una copia del registro de consola y todas las copias de los datos de salida.
- Presenciar el procesamiento.

3.1 Presenciando el procesamiento

Presenciar el procesamiento de los programas de recuperación y análisis constituye, en cierto grado, un aspecto de control. Cuando se presencia el procesamiento tenemos la posibilidad de:

- Examinar los rótulos externos de los archivos en disco o en cinta que se acceden con el programa. Esto permite confirmar que se usan los archivos correctos y que se procesan todos los volúmenes de los archivos múltiples.
- Comparar las salidas del programa con los totales de control externos antes de abandonar la sala del computador.
- Observar las intervenciones de los operadores. Llevar a cabo el seguimiento de aquellas intervenciones que no aparezcan impresas en el registro de consola para determinar el motivo por el cual no fueron impresas y si dicha intervención puede afectar la integridad

de los datos de salida. Si se comprueba la existencia de intervenciones de este tipo, será conveniente formular recomendaciones a la gerencia.

Sin embargo, el efecto de control de nuestra presencia durante el procesamiento es limitado ya que :

- Si el cliente tiene la intención de alterar la copia del archivo que utiliza el programa, puede hacerlo antes de nuestro arribo para presenciar la ejecución.
- En un ambiente de multiprocesamiento pueden existir otros programas, además del nuestro, que sean ejecutados en forma simultánea y puede resultar difícil obtener el uso exclusivo del computador para la ejecución de nuestro programa.

Estos inconvenientes subsisten aún cuando actuamos como operadores y ejecutamos el programa. El control sobre la integridad y exactitud de los datos y sobre la no interferencia del cliente, puede ser mejor logrado a través de los controles tratados anteriormente en esta sección.

3.2 Procesamiento en servicio externos

Cuando se utiliza un servicio externo, se deben considerar los procedimientos de control sugeridos anteriormente. Debemos estar razonablemente satisfechos de que los controles del servicio externo son satisfactorios. Los pasos adicionales que se describen a continuación contribuyen a proteger la confidencialidad de los datos del cliente:

- Las copias de los archivos de computación sólo pueden ser dejadas en el servicio externo durante el tiempo estrictamente necesario para ejecutar el programa.
- Los rótulos externos de los archivos no deben ser identificados por el nombre del cliente sino por un código numérico, por ejemplo el número de serie del volumen.

XI. Diseño de las Transacciones de Prueba

El diseño de las transacciones de prueba involucro las siguientes etapas:

- Especificaciones detalladas.
- Desarrollo de las transacciones de prueba.
- Determinación de los resultados esperados,
- Conversión de las transacciones de prueba a un formato legible por el computador.

1. Especificaciones detalladas

Las especificaciones son importantes porque proporcionan un plan lógico paso por paso, en base al cual se deben desarrollar las transacciones de prueba. Cuando las transacciones de prueba son preparadas por una persona ajena al equipo de trabajo, la definición de las especificaciones debe estar a cargo en forma conjunta de la persona encargada de prepararlas y de un miembro del equipo de trabajo.

Las especificaciones detalladas deben ser desarrolladas en base a la información técnica obtenida y considerando la evidencia de auditoría a ser obtenida, definida durante la planificación. El grado de detalle depende de la complejidad de las transacciones de prueba a ser preparadas. Una aplicación sencilla puede ser preparada sólo en base a la información obtenida durante la planificación sin necesidad de otras especificaciones detalladas, mientras que una aplicación compleja requerirá de especificaciones con mayor detalle,

Las especificaciones deben incluir :

- Los programas de aplicación del cliente y los tipos de transacciones a ser probados.
- Las fuentes de las transacciones de prueba que serán utilizadas.
- Los documentos y campos de entrada para los cuales se probarán las rutinas de edición.
- Los controles y las funciones de procesamiento computadorizadas que serán probadas.
- Los informes de control que se deben generar.
- Los archivos de transacciones y los datos permanentes que puedan ser requeridos.
- Las conciliaciones posteriores y otras pruebas de auditoría a ser efectuadas sobre los resultados obtenidos.

La necesidad de contar con especificaciones detalladas de las transacciones de prueba no se ve afectada por el método utilizado para su preparación. Aún cuando las transacciones de prueba sean transacciones reales pendientes de procesamiento, se necesita una descripción de la naturaleza y propósito de cada prueba para poder seleccionar las

transacciones apropiadas. La colaboración del personal del cliente puede ser necesaria para investigar los motivos de resultados inesperados en las pruebas.

A menudo, nuestro objetivo es probar controles y funciones de procesamiento computadorizadas que comparan los datos ingresados con los datos permanentes o que utilizan los datos ingresados para actualizar un archivo de datos permanentes. Por lo tanto, si no se utilizan transacciones reales para la prueba, las especificaciones detalladas pueden requerir el desarrollo de un archivo de datos permanentes de prueba (archivo simulado de datos permanentes). Este archivo puede contener tanto un pequeño número de registros de datos permanentes reales como datos ficticios (creados por nosotros) para que las transacciones de prueba puedan ser procesadas con registros de datos permanentes correspondientes.

Un archivo de datos permanentes de prueba de cuentas a cobrar, por ejemplo, puede ser utilizado para probar :

- Las rutinas de edición que rechazan las transacciones en las cuales el código del deudor que figura en el registro de despacho no se encuentra en el archivo de datos permanentes.
- Si el programa imputa las ventas a la cuenta correcta de cada deudor y acumula correctamente los saldos.
- Si los nombres de los deudores, números y saldos de cuenta son registrados en el listado de saldos.
- La suma del listado de saldos de cuentas a cobrar.

2. Desarrollo de las transacciones de prueba

Las especificaciones bien definidas simplifican la tarea de desarrollar las transacciones de prueba. Generalmente, los datos son preparados por un miembro del equipo de trabajo pero puede ser necesaria la asistencia técnica de personal del cliente que esté familiarizado con el diseño del sistema.

Existen cuatro métodos principales para obtener o desarrollar transacciones de prueba :

- Crear transacciones de prueba.
- Obtener las transacciones de la biblioteca de prueba del cliente.
- Seleccionar las transacciones de prueba entre los datos reales recientemente procesados o que están a punto de serio.
- Utilizar generadores de transacciones de prueba. Estos son paquetes de software diseñados para producir transacciones de prueba basándose en parámetros ingresados por

el usuario, (generalmente no se justifica comprar un generador de transacciones de prueba sólo para desarrollar las muestras, pero puede ser que ya exista uno en el departamento CIS del cliente).

Cuando se prueban rutinas de edición es conveniente, por lo general, crear transacciones de prueba no válidas; esto se logra alterando un campo en una transacción válida. Sin embargo, para cada transacción no válida sólo se debe probar una rutina de edición ya que si la transacción tiene dos o más errores puede resultar difícil establecer el motivo específico del rechazo.

Para decidir cuál de los métodos se debe emplear para preparar las transacciones de prueba, la consideración más importante es obtener una selección de datos representativa que permita probar en forma adecuada las rutinas seleccionadas a fin de proporcionar la evidencia de auditoría deseada, Otro aspecto a tener en cuenta es que los datos de prueba deben ser preparados de la manera más eficiente.

3. Determinación de los resultados esperados

Una vez preparadas las transacciones de prueba, se deben calcular los resultados esperados como producto de su procesamiento a través del sistema.

La determinación de los resultados de las pruebas de rutinas de edición no es complicada y normalmente consiste en preparar un listado de las transacciones que deben ser rechazadas y el motivo del rechazo. De igual forma, se pueden determinar los totales de salida ya que no son más que los cálculos de determinados campos de las transacciones de prueba. Por lo general, se debe incluir por lo menos una transacción válida en los datos de prueba.

La determinación de los resultados esperados en aplicaciones sencillas no insume mucho tiempo. Con frecuencia, los datos de prueba sólo necesitan contener de diez a quince transacciones, Por lo tanto, los resultados esperados podrán ser preparados relativamente rápido. La determinación de los resultados esperados en el caso de cálculos programados más complejos, debido a la cantidad de variables involucradas, como por ejemplo, el cálculo de la remuneración de empleados que trabajan por hora, puede insumir más tiempo.

4. Conversión de las transacciones de prueba a un formato legible por el computador

Es importante verificar que las transacciones de prueba sean correctamente convertidas a un formato legible por el computador. Una conversión incorrecta puede derivar en una interpretación errónea de los resultados de la prueba. Si posteriormente se

detecta un error en la conversión de los datos puede ser necesario procesar nuevamente las transacciones de prueba.

Si el dispositivo que convierte las transacciones de prueba a un formato legible por el computador produce un listado impreso, se podrá comparar la totalidad de las transacciones de prueba de los documentos fuente con las incluidas en el listado mencionado. Cuando se utilizan terminales, podemos elegir entre ingresar las transacciones personalmente o presenciar el ingreso de las mismas para confirmar que las transacciones de prueba han sido ingresadas correctamente.

XII. Procesamiento de Transacciones de Prueba

Cuando se aplica una técnica de transacciones de prueba se deben tener en cuenta dos aspectos desde el punto de vista de control :

- Que no haya habido acceso no autorizado a las transacciones de prueba desde la última ejecución.
- Que las transacciones de prueba sean procesadas con los programas correspondientes.

Algunos posibles procedimientos para cumplir con estos objetivos son :

- Utilizar transacciones de prueba que hayan estado bajo nuestro control.
- Imprimir los rótulos internos de encabezamiento de los archivos a los que se accede para su posterior comparación con:
  - Fechas de creación, nombres y números de serie incluidos en los registros de biblioteca para los archivos de producción, o en los archivos de auditoría para los archivos de datos de prueba permanentes empleados.
  - Listado de los informes de ejecución de tareas utilizados para el procesamiento real.
  - Nombre o número de identificación del programa utilizado para el procesamiento real.
- Solicitar al operador que retenga los archivos usados durante el procesamiento de transacciones de prueba hasta tanto sean controlados los totales de control.
- Obtener una copia de control de las transacciones de prueba, una copia del registro de consola, si fuera posible, y las copias de los datos de salida.
- Solicitar una impresión (vuelco) de parte del contenido de los archivos de prueba para compararlos con la copia de control de auditoría.
- Considerar la conveniencia de presenciar el procesamiento.

Los procedimientos de control varían según si las transacciones de prueba ya han sido utilizadas o si son desarrolladas por primera vez. Puede resultar útil presenciar el procesamiento para resolver eventuales problemas de ingreso de datos.

Siempre que se utilicen transacciones reales para la prueba, las mismas deben ser en lo posible procesadas como un lote separado. Esto permite separar las transacciones de prueba para comparar los resultados reales del procesamiento con los resultados predeterminados.

En los casos en que se utilicen procedimientos de prueba integrada o pruebas on line debemos asegurarnos de que exista personal disponible del cliente adecuadamente capacitado para corregir la registración de las transacciones de prueba y asegurarnos de que las mismas sean excluidas de los registros contables del cliente.

XIII. Ejemplos de Técnicas de Auditoría Computacional

Implantó el sistema (aproximadamente 4.500.000). Los datos históricos están a disposición del personal de los depósitos y de la sección de control de materiales de la Casa Matriz a través de un generador de informes. Los datos históricos incluyen información necesaria para determinar el tiempo de demora en la entrega, el punto y la cantidad del nuevo pedido, y el análisis del uso y obsolescencia.

El personal gerencial y operativo apropiado recibe diversos listados con información relativa a las partidas contenidas en el sistema. Además, se puede acceder por consulta directa al sistema a través de alguna de las 25 terminales instaladas, para obtener información relativa a cantidades disponibles, listados de recuento de existencias por unidad, listados de despacho ordenados por fecha prevista de entrega y último precio pagado para determinadas partidas de existencias.

1. Antecedentes de auditoría

Anteriormente los procedimientos de auditoría utilizados para probar exactitud, integridad y corrección se llevaban a cabo mediante indagación, observación, recálculo y a través de referencias a documentos fuente. No se había considerado seriamente el desarrollo de programas de recuperación y análisis ya que se sabía que el sistema de existencias iba a ser transformado, adoptando el diseñado e implantado en la Casa Matriz, La conversión del sistema ya ha sido completada.

TABLA

A: Gerente de Auditoría

□

De: Encargado de Auditoría

□

Ref.: Programa de Recuperación y Análisis para Existencias

□

El propósito de este memorando es documentar, para referencia futura, el estudio de factibilidad llevado a cabo la semana pasada conjuntamente con nuestro equipo de auditoría. Visitamos las oficinas de UAI para evaluar la posibilidad de utilizar su paquete de software de auditoría a fin de llevar a cabo gran parte de la revisión prevista en el plan de auditoría para el rubro existencias. Identificamos el archivo a utilizar, del cual le adjunto una copia del diseño de sus campos con las explicaciones necesarias Se puede acceder con facilidad a este archivo empleando el paquete auditoría del cliente. En el pasado, no hemos tenido problemas de disponibilidad de tiempo del computador. El archivo de existencias es preparado semanalmente, pero como los informes más importantes son preparados en forma mensual creo que será más conveniente usar la copia de un, fin de mes. Si bien el memorando de planificación establece que todo el trabajo se llevará a cabo sobre saldos al 30 de septiembre, creemos conveniente volver a ejecutar el programa al cierre del ejercicio para obtener evidencia de auditoría adicional. Propongo los siguientes requerimientos detallados para este programa:

- Revisar las sumas y multiplicaciones del archivo, obteniendo subtotales por sección.
- Sumar las partidas recibidas y aún no facturadas a fin de verificar que la provisión sea adecuada.
- Comparar el costo estándar con el último precio pagado y listar las partidas en las que la diferencia sea muy significativa.
- Listar las partidas de poco movimiento, comparando el uso durante el año con la cantidad en existencias.
- Listar las existencias significativas que no hayan sido recontadas durante alguno de los recuentos físicos cíclicos que realizó UAI durante el año.
- Listar los ajustes de existencias más significativos.
- Seleccionar una muestra de items para hacer un control detallado de costos.
- Listar las partidas en las cuales el stock disponible esté muy por debajo del punto de nuevo pedido.

- Listar las partidas recibidas aún no facturadas con un saldo significativo.
- Listar todas las partidas con stock negativo.
- Listar las existencias con valor cero.
- Listar las partidas en las cuales la unidad de compra sea distinta a la unidad de despacho.

El análisis preliminar de costo/beneficio realizado para el programa de recuperación y análisis de existencias debería ser modificado a 118 horas (de las cuales ya hemos insumido 16) para tareas de desarrollo y 78 horas de ahorros identificados por la reducción de procedimientos manuales. Basándome en la mayor satisfacción de auditoría que creo se obtendrá al poder aplicar nuestras pruebas a todo el archivo, sugiero que se proceda a utilizar los procedimientos de auditoría computadorizados. Le agradeceré me haga saber:

- Si está o no de acuèrdo con el procedimiento.
- Cuáles de las pruebas mencionadas desea realizar sobre los saldos al 30 de septiembre y cuáles desea repetir al cierre del ejercicio.
- Si tiene alguna preferencia en cuanto a límites de valor para cada prueba o si tiene alguna sugerencia relativa a pruebas adicionales que se podrían incluir en el programa.

TABLA

Diseño del Archivo de Existencias

Campo N°	Descripción del Campo	Nombre del Campo	Byte
1	Status	STATUS	1
2	Altura	HEIGHT	2
3	Número de grupo	GROUPNO	3
4	Longitud	LENGHT	2
5	Descripción (abreviada)	DESCR1	20
6	Descripción	DESCR2	20
7	Número de depósito	WHSNO	1
8	Número de sección	SECTIONNO	2
9	Unidad de despacho	ISSUEUNIT	4
10	Estante	BINLOC	8
11	Proveedor preferido	PREFVDOR	4
12	Demora en la entrega (días)	LEADTIME	2
13	Precio unitario (a valor st.)	STDCST	6
14	Cantidad óptima de pedido	ECORDERO TY	4
15	Punto de nuevo pedido	ORDPOINT	4
16	Cantidad pedida	OTYONORD	4
17	Fecha último pedido	DTLSOR	4
18	Stock disponible	POH	4
19	Stock sin cargo	NCOH	4
20	Consumo último mes	MTDUSAGE	4
21	No. última O. compra	LSPONO	4
22	No. O. compra pendiente	CURRPO	4
23	Campo de relleno		1
24	Consumo último año	YTDUSAGE	6
25	Ultimo precio pagado	LSTPDP	6
26	Cantidad aún no facturada	OTYNOINV	4
27	Recibido aún sin facturar (std)	RCVNPO	6
28	Diferencia (std. vs. valor real)	BALANCE	6
29	Fecha último recuento	DTLSCN	4
30	Ajuste de existencias físicas	BINADJ	4
31	Código impositivo	TAXCODE	1
32	Condiciones de pago	PAYTERMS	2
33	Despachar a	SHIPOCODE	2
34	Descuento comercial	TRADEDISC	3
35	Código de arancel	DUTYCODE	2
36	Fecha último despacho	DTLSIS	4
37	Porcentaje de impuesto	TAXPCT	3
38	Campo de relleno		8
39	Peso	WEIGHT	4
40	Unidad de compra	PURUNITS	4
41	Tasa de arancel	DUTYRATE	3
42	Factor de conversión	CONVFTP	2
43	Recuento despachos último mes	MTDUSE	2
44	Recuento despachos último año	YTDUSE	3
45	Campo de relleno		10
46	Campo de relleno		7
47	Fecha última actualización	DTLSPC	3
48	Precio lista (precio de venta)	LISTPR	6
49	Código del fabricante	MFGCS	8
50	Tamaño del paquete	PKGSIZ	4
51	Fecha de despacho	DELVRY	4
52	Profundidad	DEPTH	5
53	No. de referencia de stock	REFNO	2
54	Campo de relleno		4
			40
			280

2. Resultados

El programa fue escrito y probado en el tiempo previsto y demostró ser una herramienta eficiente para obtener evidencia de auditoría.

Como resultado del seguimiento efectuado sobre los datos resultantes se efectuaron recomendaciones a la gerencia tendientes a eliminar una rutina defectuosa del programa de existencias que había dado lugar a la aparición de unidades de existencias negativas y a incrementar la frecuencia de los recuentos cíclicos de partidas de alto valor. La gerencia de la empresa quedó muy bien impresionada por el uso que hicimos de su software de auditoría; asimismo, decidió preparar informes mensuales de existencias, similares a varios de los informes generados por nuestro programa.

En conclusión, si bien los programa de recuperación y análisis son más costosos durante el primer año de aplicación que las técnicas manuales alternativas, el retorno sobre la inversión representado por la identificación de problemas potenciales (que eventualmente podrían haberse vuelto importantes) es satisfactorio; asimismo, se espera alcanzar en dos años el punto de equilibrio entre el costo del programa y el costo del tiempo insumido en las tareas manuales.

.15 Listados y extractos de informes

A continuación se detallan los informes generados y los procedimientos de auditoría que se llevaron a cabo durante su seguimiento. En las hojas siguientes se incluyen extractos de los siguientes informes.

- Lenguaje de programación, Tabla 1.
- Existencias de poco movimiento, Tabla 2.
- Existencias no recontadas durante el ejercicio, Tabla 3.
- Existencias con valor cero, Tabla 4.

Informe	*Procedimientos de seguimiento*
Existencias por sección	Comparar los valores de existencias con los montos del mayor general. Asegurarnos que el informe concuerda con nuestro entendimiento de la actividad de cada sección.
Comparación del costo unitario con el último precio pagado	Examinar cuidadosamente la valuación del ítem No. 140420 y considerar la necesidad de ajustar el precio estándar (diferencia significativa con el último precio pagado).
Partidas de poco movimiento	Considerar la necesidad de desvalorizar estas partidas. Revisar el listado de existencias de poco movimiento de la gerencia e investigar las razones por los eventuales casos de existencias no listadas por el programa.
Existencias no recontadas	Considerar la inclusión de los items significativos durante el ejercicio en las pruebas de recuento físico. Investigar por qué estos ítems aún no han sido recontados
Listado de ajustes significativos de existencias	Modificar el programa para que cuente y sume todos los ajustes de existencias, separando los ajustes positivos de los negativos. El programa identificó sólo los ajustes positivos superiores a $1.000.
Items recibidos pero no facturados	Comprobar la provisión por este concepto.
Existencias negativas	Asegurarse de que el informe imprime los ítems cuyo saldo de existencias es negativo. Investigar los saldos negativos significativos.
Existencias con valor cero	Investigar por qué estos ítems no se venden como rezago; conservar el informe para comprobar que al año siguiente no se les asigne un valor.
Unidad de despacho distinta a unidad de compra	Asegurarse de que se calcula correctamente el costo estándar, tomando en cuenta las diferentes unidades de medida que se utilizan.

TABLA I

EXTRACTO DEL LENGUAJE DE PROGRAMACION

```
                                REQUEST NUMBER 01
NOTE,
NOTE, THESE CALCULATIONS DONE HERE JUST ONCE, AVAILABLE FOR
NOTE, ALL SUBSEQUENT REQUESTS:
NEWFLD,GDSTX,18.'GOOD INVENTORY QUANTITY'
NEWFLD,INVVAL,F10.2,'INVENTORY VALUE'
COMP,R8,GDSTX = POH-NCOH
COMP,R8,INVVAL = GDSTXxiSSUEPRICE
NEWFLD,DTCSOR,16,'DATE LAST ORD'
NEWFLD,DTCSCN,16,'AUDIT DATE'
NEWFLD,DTCSIS,16,'LAST ISSUE DATE'
NEWFLD,DTCSPC,16,'DATE UPDATED'
COMP,R8,DTCSOR = DTLSOR + 72000
COMP,R8,DTCSCN = DTLSCN + 72000
COMP,R8,DTCSIS = DTLSIS + 72000
COMP,R8,DTCSPC = DTLSPC + 72000
NOTE,
NOTE,
TITLE, INVENTORY BY SECTION.
NEWFLD,COUNT, 16,'COUNTER'
COMP,A3,COUNT = 1
OPTION,SUMMARY
SORT,SECTND(2)
PRINT,RCVNPO(S),INVVAL(S),COUNT(S)
END

                                REQUEST NUMBER 02

TITLE, COMPARISON OF ISSUEPRICE TO LAST COST PAID.
TITLE, (COST PAID MINUS ISSUEPRICE. 10% OF ISSUE PRICE.)
NEWFLD,PRDIFF,Fll.3,'PRICE DIFFERENCE'
NEWFLD,ISPRIO,F12.3,'IOPCT ISSUEPRICE'
COMP,A3,PRDIFF= LSTPDP-ISSUEPRICE
COMP,A3,ISPRIO= ISSUEPRICE(1)
SELECT,INVVAL.GT.(1000000).AND.PRDIFF.GT.ISPRIO.AND.WNSNO.EQ.('G')
OPTION,STDSP = L,OVFLO = 0
PRI NT,REFNO, INVVAL(S), DESCR2, ISSUEPRICE, LSTPDP, DTCSOR, LSPOND
END

                                REQUEST NUMBER 03

TITLE,SLOW MOVING INVENTORY
SELECT,INVVAL.GT.(1000000).AND.GDSTX.GT.YTDUSE
PRINT,REFNO,INVVAL,DESCR2,GDSTX,YTDUSE,DTCSIS
END

                                REQUEST NUMBER 04

TITLE,INVENTORY NOT COUNTED IN YEAR.
NEWFLD,YRAUD.12.'YEAR AUDITED'
COMP,A3,YRAUD = DTCSCN/1000
SELECT,INVVAL.GT.(1000000).AND.YRAUD.LT.(9)
NEWFLD,DATEl.18.'AUDIT DATE'
PRINT,REFNO,INVVAL(S).DESCR2,BINLOC,POH,NCOH,YTDUSE,DTCSCN
END
```

TABLA 2

EXISTENCIAS DE POCO MOVIMIENTO

EXISTENCIAS DE POCO MOVIMIENTO

REFERENCIA	VALOR DE LAS EXISTENCIAS	DESCR. 2	STOCK DISPONIBLE	CONSUMO ULTIMO AÑO	VALOR DE LA FECHA DE DESPACHO
0014263	24.680,23	Rueda	92	4	84.352
0011607	169.465,23	Derivación	21	1	84.237
0014261	28.305,80	Rueda	136	15	84.244
0026626	14.488,32	Rueda	56	0	83.284
0026557	24.715,58	Anillo	864	84	85.222
0025586	14.052,90	Ventilador	6	0	84.138
0023331	51.723,50	Horquilla	291	21	84.269
0140429	1.548.907,50	Riel	29.503	0	84.195
0140168	893.178,00	Riel	11.451	15	85.262
0151939	14.405,40	Polea	200	0	84.219
0172496	102,016.47	Junta	217	4	85.262
0177015	13,475.00	Cilindro de propano	350	0	78.000
0186853	85.471,85	Kit	2.350	0	85.195
0118986	166.151,68	Almohadilla	1.312	97	85.268
0118987	574.523,20	Almohadilla	2.740	0	84.162
0243405	58.650,00	Kit	170	0	85.251
TOTAL	3.784.210,66				

TABLA 3

EXISTENCIAS NO RECONTADAS DURANTE EL EJERCICIO

EXISTENCIAS NO RECONTADAS DURANTE EI EJERCICIO

REFERENCIA	VALOR DE LAS EXISTENCIAS	DESCR.2	UBICACION FISICA DEL STOCK	STOCK DISPONIBLE	CONSUMO ULTIMO AÑO
0020828	24.018,47	Eje	A-2-A	20	31
0023331	51.723,50	Horquilla	STL-Playón	291	221
0025586	14.052,80	Ventilador	74ABO3AA	6	0
0028557	24.715,58	Anillo	I7AHOIAA	864	784
0026637	18.988,10	Zapata	Rampa-I	2.700	15.433
0026626	14.488,32	Rueda	Playón	56	0
0014261	26.305,80	Rueda	STL-Playón	136	115
0014263	25.680,23	Rueda	Playán	82	444
0014264	107.243,53	Rueda	STL-Playón	428	2.720
0014265	72.594,28	Rueda	STL-Playón	234	307
0187445	214.192,00	Unión	Playón	13.387	30.514
0188853	85.471,85	Kit		2.350	0
0177015	13.475,00	Cilindro de propano	Playón	350	0
0151939	14.405,40	Polea	Playón	200	0
0163055	1.409.318,97	DFO-2	Taller	2.898.551	12.179.858
0118986	166.151,68	Almohadilla	Playón	1.312	297
0126324	29.787,12	Cabezal	STL-Playón	36	299
0118987	574.523,20	Almohadilla	Playón	2.740	0
0126482	11.131,28	Placa	STL-Playón	129	383
0131951	110.354,10	Cupla	Playón	219	509
0114620	16.862,39	Gula	R-1802	1	1
0114619	16.862,39	Guía	R- 1802	1	1
0243405	58.850,00	Kit	Playón	170	0
TOTAL	3.101.195,99				

TABLA 4

EXISTENCIAS CON VALOR CERO

EXISTENCIAS CON VALOR CERO

REFERENCIA	VALOR DE LAS EXISTENCIAS	UBICACION	DESCR. 2	PRECIO	POH	FECHA ULTIMO DESPACHO
0010996	0.00	O3AE23FA	REGULADOR	0.000	1	84.029
0010958	0.00	O3AE23BA	REGULADOR	0.000	1	78.000
0010993	0.00	O4DAO7BA	REGULADOR	0.000	1	78.000
0010935	0.00	25ABO6HA	GENERADOR	0.000	1	78.000
0010938	0.00	16DCO7BA	ARRANCADOR	0.00	2	84.205
0010953	0.00	25ABO6BA	GENERADOR	0.000	1	78.000
0010956	0.00	O7DAO7CA	REGULADOR	0.000	1	81.345
0010929	0.00	25ABO6HA	ARRANCADOR	0.000	1	78.000
0010677	0.00	19AGO6CA	REFRIGERADOR	0.000	1	85.146
0010931	0.00	15BBO7AA	ARRANCADOR	200.000	1	78.000
0010933	0.00	25AHO7AA	ARRANCADOR	0.000	1	82.329
0010676	0.00	30-6-8	INYECTOR	0.000	2	78.040
0010493	0.00	01 CAOL FJ	SELLO	0.000	1	78.000
0010430	0.00	O5RGI7CA	BOMBA	0.000	1	79.064
0010447	0.00	2IAAO5BA	BLOCK	0.000	2	82.126
0010424	66.60	OICDO8EA	SEPARADOR	66.600	2	85.017
0010303	0.00	RK-114	BOMBA	0.000	1	79.062
0010420	44.50	O5CiO7CA	SEPARADOR	44.500	4	85.017
0010297	0.00	RK-114	BOMBA	0.000	1	79.962
0010183	0.00	RK-93-T	BASTIDOR	0.000	8	78.000
0011026	0.00	O4AE22DA	MAGNETO	0.000	2	85.012
0011007	0.00	O5CC2OEA	REGULADOR	0.000	1	84.203
0011011	0.00	O3AD23FA	REGULADOR	0.000	1	81.036
0011012	0.00	16BCO7BA	GENERADOR	0.000	2	82.308
0011013	0.00	16AJO8BA	REGULADOR	0.000	1	79.068
0020828	24.018,47	A-2-A	EJE	1.264.130	20	85.157
TOTAL	24.129,57					

3. Antecedentes

Nuestro cliente es una subsidiaria de una importante empresa petrolera. Como parte de nuestra auditoría interina, el equipo de trabajo desea realizar una circularización de las cuentas a cobrar. A las circulares se adjuntará un resumen de cuenta por deudor circularizado. Además, se desea realizar indagaciones específicas con respecto a los saldos de cuentas a cobrar para generar informes tales como análisis de antigüedad.

En años anteriores la tarea de localizar y copiar los resúmenes de cuenta para los deudores, a ser enviados con las circulares, requirió muchas horas de trabajo. Una posible solución a este problema consistía en transferir los detalles de los resúmenes al microcomputador y luego, generar los resúmenes y las circulares.

Originalmente, se consideró transferir los datos al microcomputador del cliente y luego, utilizar un software de base de datos para extraer una muestra de saldos que sería utilizada en el módulo de circularización de cuentas a cobrar del Software de Auditores Desafortunadamente, esto no fue posible por la falta de capacidad disponible en el disco rígido del microcomputador del cliente. Es por eso que se decidió que los auditores utilizaría su propio micro para preparar los informes requeridos. El cliente aceptó proporcionar una cinta magnética con los archivos requeridos.

4. Generalidades sobre el sistema

La información requerida es mantenida por un sistema on line. El mayor de ventas y los archivos de deudores son archivos de acceso directo que son actualizados en forma interactiva.. Existen copias de respaldo y archivos de datos históricos secuenciales asociados con el sistema. La cinta proporcionada por el cliente incluye dos archivos extraídos del mayor de ventas y del archivo de deudores. En el sistema existen aproximadamente 6.000 cuentas de deudores, pero no todas son activas. Las cuentas inactivas cuyo saldo es cero tienen el status "4"

5. De qué forma se cumplió el requerimiento

El primer paso consistió en utilizar utilitarios estándar para observar la estructura de los archivos de datos y confirmar la exactitud de las descripciones de los archivos. Luego se utilizó el módulo de downloading de transferencia de cintas del " para convertir los datos de la cinta magnética al formato ASCII Software de Auditores. Como el equipo de trabajo

solicitó un acceso especial a los datos, los archivos ASCII fueron posteriormente convertidos a DBASE 111 Plus.

Se escribió una serie de programas en Easytrieve Plus PC fin de leer los archivos ASCII y generar los informes planificados.

Luego se extractó un archivo con los datos de los 80 saldos más altos, todos los saldos acreedores y las cuentas inactivas que tuvieran un saldo que no fuera cero. Al mismo tiempo, se calculó el saldo total del mayor de ventas junto con el total de cuentas incluidas en el mismo, los que fueron utilizados como totales de control para determinar la integridad de los datos proporcionados por el cliente.

La muestra extraída anteriormente fue comparada con el archivo de transacciones detalladas para generar los estados. Dichos estados fueron clasificados por número de cuenta a fin de que el personal de auditoría pudiera compararlos con las circulares. También se imprimió un listado de todas las cuentas a circularizar. El archivo extraído fue convertido al formato de circularización de cuentas a cobrar del Software de Aplicación.

6. Conclusiones

La técnica de downloading para analizar los archivos del cliente tiene varias ventajas. Por lo general, resulta menos costosa que escribir los programas de recuperación y análisis y procesarlos en un servicio externo. También puede resultar más sencillo utilizar los microcomputadores de Los Auditores que aprender a manejar el software de consulta del cliente.

Una vez que los datos han sido transferidos al microcomputador, se podrán agregar los requerimientos de consulta específicos que sean necesarios. Esto representa un beneficio adicional de la técnica del downloading.

IX. Utilización del Software del Auditor

1. Recuperación y Análisis de Datos

1.1 Utilización del Downloading

a) Antecedentes

Nuestro cliente es una subsidiaria de una importante empresa petrolera. Como parte de nuestra auditoría interina, el equipo de trabajo desea realizar una circularización de las cuentas a cobrar. A las circulares se adjuntará un resumen de cuenta por deudor circularizado. Además, se desea realizar indagaciones específicas con respecto a los saldos de cuentas a cobrar para generar informes tales como análisis de antigüedad.

En años anteriores la tarea de localizar y copiar los resúmenes de cuenta para los deudores, a ser enviados con las circulares, requirió muchas horas de trabajo. Una posible solución a este problema consistía en transferir los detalles de los resúmenes al microcomputador y luego, generar los resúmenes y las circulares.

Originalmente, se consideró transferir los datos al microcomputador del cliente y luego, utilizar un software de base de datos para extraer una muestra de saldos que sería utilizada en el módulo de circularización de cuentas a cobrar del Software de auditoria. Desafortunadamente, ésto no fue posible por la falta de capacidad disponible en el disco rígido del microcomputador del cliente. Es por eso que se decidió que los auditores utilizaría su propio micro para preparar los informes requeridos. El cliente aceptó proporcionar una cinta magnética con los archivos requeridos.

b) Generalidades sobre el sistema

La información requerida es mantenida por un sistema on line. El mayor de ventas y los archivos de deudores son archivos de acceso directo que son actualizados en forma interactiva. Existen copias de respaldo y archivos de datos históricos secuenciales asociados con el sistema. La cinta proporcionada por el cliente incluye dos archivos extraídos del mayor de ventas y del archivo de deudores. En el sistema existen aproximadamente 6.000 cuentas de deudores, pero no todas son activas. Las cuentas inactivas cuyo saldo es cero tienen el status "4"

c) De qué forma se cumplió el requerimiento

El primer paso consistió en utilizar utilitarios estándar para observar la estructura de los archivos de datos y confirmar la exactitud de las descripciones de los archivos. Luego se utilizó el módulo de downloading de transferencia de cintas del Software de auditores para convertir los datos de la cinta magnética al formato ASCII software de auditores. Como el equipo de trabajo solicitó un acceso especial a los datos, los archivos ASCII fueron posteriormente convertidos a DBASE III Plus.

Se escribió una serie de programas en Easytrieve Plus PC a fin de leer los archivos ASCII y generar los informes planificados.

Luego se extracto un archivo con los datos de los 80 saldos más altos, todos los saldos acreedores y las cuentas inactivas que tuvieran un saldo que no fuera cero. Al mismo tiempo, se calculó el saldo total del mayor de ventas junto con el total de cuentas incluidas en el mismo, los que fueron utilizados como totales de control para determinar la integridad de los datos proporcionados por el cliente.

La muestra extraída anteriormente fue comparada con el archivo de transacciones detalladas para generar los estados. Dichos estados fueron clasificados por número de cuenta a fin de que el personal de auditoría pudiera compararlos con las circulares. También se imprimió un listado de todas las cuentas a circularizar. El archivo extraído fue convertido al formato de circularización de cuentas a cobrar del software de auditoria.

d) Conclusiones

La técnica de downloading para analizar los archivos del cliente tiene varias ventajas. Por lo general, resulta menos costosa que escribir los programas de recuperación y análisis y procesarlos en un servicio externo. También puede resultar más sencillo utilizar los microcomputadores de los auditores que aprender a manejar el software de consulta del cliente.

Una vez que los datos han sido transferidos al microcomputador, se podrán agregar los requerimientos de consulta específicos que sean necesarios. Esto representa un beneficio adicional de la técnica del downloading.

1.2 Utilización del Software de Auditoria

a) Antecedentes

El cliente posee una cadena de grandes almacenes que venden una variada gama de artículos no perecederos. Todos los items del inventario que se encuentran en las estanterías están marcados con etiquetas que pueden ser descifradas con dispositivos magnéticos, utilizándose este sistema para registrar tanto la venta en las cajas registradoras como el movimiento de existencias.

Todas las existencias son mantenidas al precio de venta y se utiliza un sistema computadorizado para calcular el porcentaje de utilidad bruta (relación entre el precio de compra y el precio de venta). Este sistema no produce un rastro de auditoría impreso y maneja semanalmente un gran volumen de transacciones.

El archivo de utilidad bruta generado por el sistema contiene detalles de las existencias con los precios de venta y de costo. El costo de cada ítem es calculado considerando las compras acumuladas, transferencias, ajustes, mermas y dividiendo el total resultante por la cantidad. El porcentaje de utilidad bruta así calculado se utiliza para deflacionar el precio de venta al costo de compra.

Rutina de actualización de archivo:

El archivo de utilidad bruta es actualizado semanalmente por dos archivos.

- Datos de entrada válidos de otros sistemas incluyendo compras, transferencias, mermas, rebajas (reducciones del precio de venta) y ajustes del precio de venta.
- Otros ajustes

b) Requerimiento

El requerimiento específico de auditoría es recalcular el valor de las existencias (precio de venta - % de utilidad bruta = costo).(Valores sin I.V.A.).

c) De qué forma se cumplió el requerimiento

Se utilizó el software de los auditores para alcanzar el requerimiento mediante los siguientes pasos:

- Recalcular la determinación del porcentaje de utilidad bruta en los archivos de una semana para asegurarnos de que se calcula el porcentaje correcto.
- Reproducir los procedimientos semanales de actualización para asegurarnos de que la posición inicial más la actualización semanal de datos de ingreso y ajustes validados equivale a la posición de cierre.
- Calcular la utilidad bruta global por departamento, ya que el nivel al cual se lleva a cabo el trabajo de auditoría es por departamento.
- Seleccionar muestras al azar de los datos de entrada a los cuales se les aplicaron procedimientos de actualización para ser comparadas con los datos autorizados, incluyendo:
    - Compras
    - Transferencias
    - Mermas
    - Ajustes
- Preparar informes de excepción abarcando, por ejemplo:
    - Almacenes con porcentajes de utilidad bruta significativamente distintos
    - de los porcentajes globales de la Compañía.
    - Porcentajes de utilidad bruta con grandes variaciones con respecto a los
    - archivos de la semana anterior.
    - Porcentajes de aumento pequeños.
- Listar todos los porcentajes de utilidad bruta para su comparación con los listados finales utilizados para los cálculos de las existencias.

1.3 Preparación de un Programa de Recuperación y Análisis a Medida

a) Antecedentes

El cliente es un gran operador de turismo, que cuenta con un sistema de reservas y control on line. Durante los primeros diez meses de 1984 el cliente no logró conciliar los saldos de cuentas a cobrar del sistema on line que se utiliza para preparar los estados de cuenta con los archivos off line derivados del sistema y que se utilizan para contabilización

y control de créditos. El cliente opinó que la diferencia de la conciliación, la cual se está incrementando, puede causar dificultades en la auditoría de cierre del período y solicitó nuestra asistencia.

b) Generalidades sobre el sistema

El sistema on line mantiene un archivo de reservas en el cual se registran los saldos adeudados por cada reserva. Este archivo es utilizado para imprimir estados de cuenta de reservas hechas a través de cada agencia de viajes en los cuales constan los saldos pendientes. El último estado de cuenta del año es un estado simulado con totales generales, impreso con el objeto de utilizarlo para control.

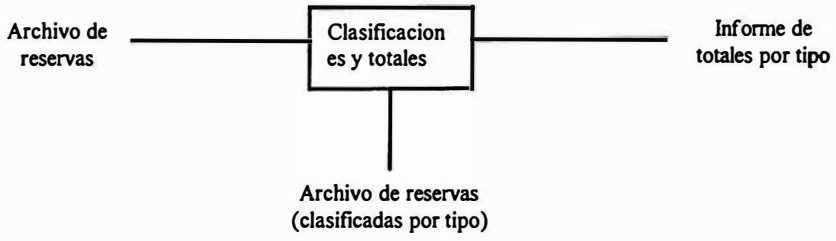
Los detalles de las reservas son transferidos de la base de datos en producción a un archivo denominado Archivo de Vacaciones Acumuladas (CHF - Cumulative Holiday File) con propósitos de control y estadística. Este es utilizado para generar un informe de control de crédito que indica el recálculo del total de las cuentas a cobrar por tipo de reserva, incluyendo un análisis de antigüedad. El saldo total de las cuentas a cobrar de este informe debería ser conciliaba con el valor total de los estados de cuenta mensuales.

El requerimiento para el programa de recuperación y análisis es identificar la composición y origen de las partidas conciliatorias entre el sistema que genera los estados de cuenta y el sistema de control de créditos.

c) De qué forma se cumplió el requerimiento

Se adoptó un enfoque de dos etapas con el propósito de verificar la sospecha de que el problema se limitaba únicamente a cierto tipo de reservas. La primera etapa consistió en analizar el archivo de reservas en producción y obtener totales por tipo de reservas

El programa que generó los informes con los totales por tipo fue escrito en Filetab y generó (como, subproducto) una versión del archivo de reservas con la misma secuencia del CHF.



Al efectuarse la corrida de la primera etapa del programa confirmamos que 10 de los 19 tipos de reservas estaban conciliados, situación que el sistema del cliente no fue capaz de revelar. Estábamos en condiciones de concentrarnos en los 9 tipos restantes.

Para encarar este problema se utilizó una segunda etapa del programa escrito también en Filetab. Este programa leyó el archivo en producción clasificado, producido en la etapa anterior, y lo cotejó con los detalles de las reservas del CHF. Para cada reserva en particular se pudieron comparar los saldos incluidos en el estado de cuenta total con el saldo de cuentas a cobrar calculado por el informe de control de crédito. Cuando el programa indicaba diferencias, se incluían en el informe detalles de las cuentas individuales mostrando el saldo pendiente.

Este segundo informe permitió agrupar en siete categorías, cientos de reservas con diferencias entre los sistemas. La más significativa representaba el 80% de la diferencia original en la conciliación. Nuestra investigación determinó que esta situación estaba relacionada con un cambio menor que se realizó en el sistema, el cual no había sido incluido en el programa de control de créditos, lo que originaba que el sistema agregara un campo de descuento especial en lugar de restarlo.

d) Resultados

En este caso el programa de recuperación y análisis no solamente contribuyó a alcanzar nuestros requerimientos de auditoría sino que también se brindó un servicio adicional al cliente asistiéndolo en los procedimientos de conciliación y mejorando sus controles.

1.4 Utilización de Programas Utilitarios

a) Antecedentes

Strategist S.A. es una distribuidora de repuestos con existencias en diez unidades diferentes. Los antecedentes de auditoría son casi idénticos a los descriptos en la Sección anterior para UAI. La principal diferencia es que STRATEGIST S.A. no posee su propio software de auditoría o generador de informes.

b) Circunstancias de auditoría

Al realizar pruebas de los registros permanentes de una unidad, detectamos en el archivo de existencias un monto negativo importante para el repuesto número 0374890 y

otro monto negativo para el repuesto número 0229238. Existía la posibilidad de que en otras unidades de STRATEGIST S.A. existieran otros montos negativos que no hubieran sido identificados.

Las alternativas para extender el alcance de auditoría aparentemente eran:

- Revisión manual del archivo de existencias completo de todas las unidades para listar las cantidades negativas y los valores unitarios.
- Preparar un programa especial para extraer todos los montos negativos.

Se decidió seguir la segunda alternativa, ya que la primera podía requerir mucho personal de auditoría y tiempo del cliente y existía el riesgo de que no se detectaran la totalidad de los montos negativos al revisar los varios cientos de páginas con datos de las existencias.

c) Desarrollo de la aplicación

El encargado de auditoría tuvo que reunirse con el gerente de procesamiento de datos para intercambiar opiniones, ya que constató que no sería necesario realizar una programación especial porque se disponía de un utilitario obtenido a través de un proveedor de hardware. Dicho utilitario puede ser utilizado para imprimir los campos seleccionados y para sumar todas las existencias del archivo de existencias a fin de que los programas se autoprueben.

El encargado de auditoría proporcionó al gerente de procesamiento de datos los criterios de selección y presenció la ejecución del utilitario esa misma tarde. Además requirió que se imprimieran los mismos campos para aquellos ítems con valor superior a $700.000 para verificar un informe gerencial que era utilizado para llevar a cabo recuentos cíclicos de los ítems más significativos.

Los datos del programa utilitario han sido incluidos en la Tabla siguiente, El encargado de auditoría observó que los ítems negativos previamente identificados estaban en el listado y que el informe de recuentos cíclicos era exacto. Los encabezamientos de los campos impresos fueron agregados por la encargada de auditoría, utilizando el diseño del archivo de existencias, ya que no pudieron ser impresos por el programa utilitario.

TABLA

DATOS DEL PROGRAMA UTILITARIO
ITEMS CON VALOR NEGATIVO 0 SIGNIFICATIVO

Repuesto Nº	Descripción	Unidad	Cantidad	Valor unitario	Valor total de las existencias
0374890	TIRANTES, 7 x 9 x 9 PIES	7	26.774	32,00	856.768,00
0229238	CAJA DE CAMBIOS, SUPERIOR	7	2	00	00
0187445	TIRANTES, 7 x 9 x 9 PIES	9	13.387	16,00	214.192,00
0114619	CAJA DE CAMBIOS, SUPERIOR	7	1	00	00
0093722	TIRANTES, 7 x 9 x 9 PIES	10	6.693	8,00	53.544,00
0021986	REGULADORES, REPARADOS	7	2	00	00
0020840	SEPARADORES, AIRE ACON	7	8	83,00	664,00
0020228	MOTOR, LIMPIAPARABRISAS	7	6	83,58	501,48
0010993	REGULADORES, REPARADOS	4	1	00	00
0010420	SEPARADORES, AIRE ACON	3	4	41,50	166,00
0010114	MOTOR, LIMPIAPARABRISAS	1	3-	41,79	125.37
0005210	SEPARADORES, AIRE ACON	3	2	20,75	41,50
0005057	MOTOR, LIMPIAPARABRISAS	1	1	20,89	20,89
0280858	RIELES, CHATARRA (TONELADAS)	7	59.006	124,00	7.316.744,00
0326110	ACEITE	7	957.102	5,39	5.158.779,78
0064658	RIELES RECTOS, 132 Libras	7	4.980	604,86	3.012.702,80
0280336	RIELES, RELE (TONELADAS)	7	22.902	124,00	2.839.848,00
0237974	ALMOHADILLAS MF-275-1	7	5.480	351,12	1.924.137,60
0140429	RIELES, CHATARRA (TONELADAS)	8	29.503	62,00	1.924.137,60
0163055	ACEITE	8	998.551	1,29	1.288.130,79
0032329	RIELES RECTOS, 132 Libras	7	2.490	302,43	753.050,70
0140168	RIELES, RELE (TONELADAS)	8	11.451	62,00	709.962,00

d) Resultados

Los programas utilitarios resultaron una herramienta de auditoría efectiva en STRATEGIST S.A.. Después de la experiencia favorable de utilizar este programa, la encargada de auditoría detectó otros utilitarios en el departamento CIS para:

- Clasificar o resecuenciar archivos de datos.
- Fusionar varios archivos de datos en uno.
- Copiar una muestra de registros de un archivo a otro o copiar un archivo de un medio a otro (cinta o disco).

El encargado de auditoría obtuvo el manual del usuario provisto por el proveedor del hardware y se sorprendió al comprobar que, a pesar de sus conocimientos limitados sobre los aspectos técnicos de CIS, era de fácil comprensión. La necesidad de encontrar una técnica más eficiente para satisfacer el requerimiento de auditoría condujo a la encargada a obtener mayores conocimientos que dieron lugar al desarrollo de aplicaciones adicionales utilizando programas utilitarios. La gerencia tomó conciencia del valor de las técnicas de auditoría computadorizadas como control y como herramienta de auditoría y adquirió un importante paquete de software de recuperación para ser utilizado por personal de auditoría interna, del departamento de procesamiento de datos y algunos gerentes capacitados especialmente.

X. Transacciones de Prueba

1. Utilización de Datos de Prueba

a) Antecedentes

Se trata de una compañía matriz del Reino Unido con más de 400 subsidiarias distribuidas dentro y fuera del Reino Unido las actividades Internacionales del grupo son manejadas a través de dos subgrupos. El subgrupo europeo depende de la oficina de Londres y el norteamericano de la oficina de Nueva York.

El cliente tenía problemas con el proceso manual de consolidación debido a la cantidad de compañías/divisiones del grupo, Adquirió entonces un paquete de consolidación para automatizar el proceso y nos han solicitado que revisemos y documentemos nuestra comprensión del sistema antes de la preparación de los estados consolidados al cierre del período.

b) Generalidades sobre el sistema

El paquete básico de consolidación está formado por una serie de módulos. El cliente ha implantado todos los módulos y con la ayuda de los proveedores del sistema ha adaptado dicho paquete para cubrir sus propias necesidades.

Los módulos básicos son los siguientes:

- Formularios estándar (SAF).
- Ingreso y validación.
- Traducción de monedas extranjeras.
- Procesamiento de ajustes de consolidación.
- Transacciones inter-compañias.
- Procesamiento de consolidación

- Informes sobre los resultados de la consolidación.

- Control y supervisión del proceso de consolidación.

Las principales modificaciones que el cliente introdujo en el paquete son las siguientes:

Implantación de dos jerarquías Independientes de consolidación con el propósito de obtener Información para los estados legales y para la gerencia. Se requiere que estas dos jerarquías balanceen en todo momento para asegurar que los estados para la gerencia concilian con los legales. El sistertia fue modificado para incluir totales de control para ambas jerarquías después de cada etapa del procesamiento.

- Operación multiusuario para permitir que hasta ocho usuarios puedan acceder al sistema simultáneamente. El acceso a los datos financieros de una compañía es otorgado a un usuario por vez, pero existe la posibilidad de que ocho usuarios accedan al sistema simultáneamente.
- Informes multi-períodicos que permiten mantener en el sistema información histórica resumida.

c) Antecedentes de auditoría

En el pasado, la consolidación se realizaba manualmente. El cliente intentaba ahora confiar en el paquete de consolidación. Como nosotros estábamos preocupados por la pérdida de rastro de auditoría durante el procesamiento de acumulación de los datos financieros de las subsidiarias, llevamos a cabo los siguientes procedimientos de auditoría:

Trabajo realizado previo a la consolidación

- Obtuvimos una comprensión de los controles de procesamiento y funciones de procesamiento computadorizadas destinadas a asegurar la integridad y exactitud del procesamiento por el sistema de consolidación.
- Conjuntamente con nuestros especialistas en auditoría CIS, obtuvimos una comprensión de los controles existentes a fin de evitar el acceso no autorizado a los datos y programas (El cliente ha implantado el software de control de acceso).

Trabajo realizado durante el período de consolidación

Una vez confirmado que los controles y funciones de procesamiento computadorizadas identificadas proporcionan una seguridad razonable de que los datos son procesados en forma completa y precisa y de que el acceso está adecuadamente restringido, probamos la existencia y funcionamiento de los controles y funciones de procesamiento computadorizadas potencialmente clave de la siguiente manera:

- Se desarrollaron datos de prueba para confirmar que los controles de procesamiento y las funciones de procesamiento computadorizadas funcionaban satisfactoriamente.
- Con la ayuda de nuestros especialistas en auditoría CIS, revisamos los perfiles de seguridad, el sistema de registración y los informes disponibles por medio para asegurarnos que los controles de acceso a los datos de consolidación y archivos del programa estuvieran adecuadamente implantados.

Nuestro principal requerimiento consistía en determinar si el sistema de consolidación procesaba adecuadamente los datos de las subsidiarias y divisiones para generar subconsolidaciones de los subgrupos europeo y norteamericano, y la consolidación general del grupo.

d) De qué forma se cumplió el requerimiento

Esta prueba incluyó el ingreso de tres juegos de datos de la compañía a una copia de los sistemas en producción de las subsidiarias controlantes del Reino Unido y de los Estados Unidos, realizado de la siguiente manera:

- Se obtuvo una copia del sistema de consolidación de las subsidiarias del Reino Unido y de los Estados Unidos.
- Se procesaron nuestros datos de prueba en cada uno de los sistemas antes de utilizarlos para la consolidación real del cierre del período.
- Los resultados del ejercicio fueron comparados con los resultados calculados manualmente, lo cual confirmó la integridad y exactitud de la consolidación.

Los datos de prueba ingresados incluyeron:

- Datos con saldos de cuenta no razonables para determinar si eran rechazados por el sistema (por ej., saldo deudor para capital accionarlo y saldo negativo para existencias).

- Datos con errores obvios para determinar si eran rechazados (por ej., activos y pasivos no balanceados).
- Datos inusuales para determinar si los programas de procesamiento funcionaron adecuadamente (por ej., balances cuyo total de activos era cero, balances con total de activos de monto negativo significativo y estados de resultados con saldos significativamente mayores que los que normalmente se ingresarían al sistema).
- Asientos de ajustes de consolidación cuyo total de débitos difería del total de créditos, para determinar si los datos serían rechazados.

Además, se ingresaron datos que se ajustaban a los requerimientos del grupo. Los estados financieros consolidados (del grupo y de los dos subgrupos), generados por el sistema fueron comparados con las consolidaciones preparadas manualmente, con resultados satisfactorios.

También obtuvimos y documentamos nuestra comprensión de los controles del departamento CIS del cliente para asegurarnos de que nuestra confianza en la prueba fue justificada. Se probaron los controles clave del departamento CIS con resultados satisfactorios.

CAPITULO III
SOFTWARE

I. Introducción

1. Enfoque de auditoría

El software es un conjunto de instrucciones que le indican al computador cómo procesar y almacenar los datos. Generalmente se clasifica en software de sistemas y software de aplicación.

- El software de sistemas es un conjunto de programas que permite que el software de aplicación procese los datos utilizando el computador. Esto se realiza mediante funciones estándar tales como traducción al lenguaje del computador, supervisión de comunicaciones de datos, instrucciones de tareas, secuencias de entrada/salida, administración del acceso a los archivos de datos, clasificación y control de acceso. De todas las funciones que desempeña el software de sistemas, la más importante para los auditores es la de control de acceso.
- El software de aplicación es un conjunto de programas que realizan tareas específicas para usuarios finales.

A continuación se resumen los aspectos más importantes de los controles de acceso y de otro tipo relacionados con el software, los que posteriormente, serán anatiza7dos en forma más detallada.

- Los controles de acceso pueden ser incluidos en diversos tipos de software de sistemas; no obstante, un software de control de acceso específico es, por lo general, el medio principal para la protección de datos y programas.

- La alteración de programas que sólo se mantienen en lenguaje de máquina es técnicamente difícil y no presenta un riesgo significativo de auditoría. La alteración de programas escritos en lenguajes de tercera o cuarta generación es más sencilla, pero frecuentemente requiere el acceso a un compilador para que las modificaciones sean efectivas.

- El software de administración de bibliotecas puede registrar las modificaciones efectuadas a los programas de aplicación.

- El empleo de programas intérpretes redunda en la pérdida de un importante punto de control, ya que no es necesario el proceso de compilación de lenguaje fuente a lenguaje objeto para efectuar cambios a un programa.

- Los controles de balanceo normalmente están incluidos en el software de aplicación pero son más difíciles de diseñar para las bases de datos, pudiendo no existir en sistemas de ese tipo.

- Algunos lenguajes de cuarta generación sólo permiten al usuario leer los datos sin posibilidad de modificarlos, mientras que otros permiten su modificación.

Ciertos utilitarios (p. ej.: ZAP y SUPERZAP) permiten realizar modificaciones a los datos y/o a los programas sin dejar una evidencia fácilmente identificable de dicha modificación.

II. Software de Sistemas

El software de sistemas generalmente es escrito y mantenido en lenguaje de máquina o en lenguaje ensamblador, mientras que para el software de aplicación se utilizan, por lo general, lenguajes de tercera o cuarta generación. Sin embargo, es habitual que los paquetes de software de aplicación adquiridos a proveedores externos sean suministrados únicamente en lenguaje de máquina para reducir la posibilidad de que el usuario efectúe modificaciones y para proteger la inversión del proveedor en el desarrollo del programa.

En esta sección se describen en términos generales los principales componentes del software de sistemas con relevancia para la auditoría de un ambiente CIS. Ellos son:

- Sistemas operativos.
- Software de control de acceso
- Administradores de acceso a archivos.
- Sistemas de administración de base de datos (DBMS).
- Editores on line.

Para cada uno de estos componentes se incluye una descripción general de las funciones que lleva a cabo el software. Además, se ha incluido información sobre cada categoría de software de sistemas bajo los siguientes títulos:

- Importancia para la auditoría.
- Implantación.
- Controles de acceso.
- Evidencia de auditoría.
- Aspectos a considerar relativos al acceso.

1. Sistemas Operativos

El sistema operativo puede ser definido como una serie de programas que sirven como una interface entre un software de aplicación y el hardware del sistema. Administra y controla la ejecución de los programas de aplicación y suministra los servicios que estos programas requieren, por ejemplo:

- Comunicación con el operador del computador o con el usuario final por medio de mensajes estándar.

- Ordenamiento de trabajos (por ejemplo, carga y ordenamiento de trabajos con prioridades de procesamiento).

- Administración del uso de discos y cintas.

- Registración de tareas (registración, análisis, costeo, facturación, etc. del uso del computador).

- Administración de las actividades de entrada y salida (por ej., asignar el uso de los dispositivos físicos).

- Administración de la memoria (asigna los programas a posiciones específicas de la memoria principal y la libera una vez completados los trabajos).

- Protección de los datos en caso de producirse una falla en el software o en el hardware.

- Compilación, prueba e identificación de errores (debugging) en los programas.

- Control del procesamiento de más de un programa a la vez (multiprogramación).

El "corazón" del sistema operativo es el programa supervisor, también denominado monitor o ejecutor. Este programa coordina todas las funciones del sistema operativo, incluyendo su interacción con los programas de control de tareas y la activación de los canales de transmisión de datos.

Importancia para la auditoría

Los sistemas operativos controlan las actividades de las aplicaciones que se procesan en el sistema. Esto implica un riesgo considerable, ya que si un usuario no autorizado logra acceder al sistema operativo puede alterar el flujo normal de procesamiento del sistema, incluyendo la lectura y modificación de archivos de datos, rastros de transacciones, etc.. Algunos sistemas operativos incluyen métodos para restringir los accesos no autorizados.

A causa de la autoridad que puede tener un sistema operativo, puede ser utilizado para eludir los dispositivos de seguridad y acceder a recursos confidenciales. Ello puede afectar el uso de software de control de acceso, (como por ejemplo RACF o ACF 2, en un ambiente de mainframes IBM). Otros componentes de software de sistemas operan al mismo nivel que el sistema operativo ("nivel supervisor") y también puede afectar la efectividad del software de control de acceso. Estos programas deben estar conectados con el sistema operativo y su uso debe ser controlado.

Implantación

Los sistemas operativos permiten la implantación de un dispositivo opcional de seguridad cuando el sistema es generado inicialmente. Algunos sistemas operativos (por ej., VMS para DEC) tienen sus propios dispositivos de seguridad, los cuales pueden ser implantados cuando se instala el sistema operativo. Otros sistemas operativos, tales como los productos IBM, no incluyen funciones de seguridad muy amplias. En este último caso, es aconsejable integrar al sistema operativo un software de control de acceso, como RACF o ACF 2, a fin de brindar mayor protección a los recursos.

Al instalarse el sistema operativo, los usuarios tienen la oportunidad de decidir no sólo qué tipo de software de seguridad utilizar, sino también cualquier otro tipo de software de sistemas requerido. Monitores de teleprocesamiento, editores on line y sistemas de administración de cintas y discos pueden ser instalados en este momento. Es importante

determinar qué tipos de aplicaciones serán ejecutadas, antes de seleccionar el tipo de software de sistemas requerido .

Controles de acceso

Normalmente, los sistemas operativos utilizan contraseñas e identificaciones del usuario para evitar que usuarios no autorizados logren acceder a las funciones del sistema operativo y a los utilitarios. Las contraseñas e identificaciones del usuario son definidas en tablas del sistema o archivos de datos que son activados cuando se genera el sistema.

Los sistemas operativos varían con respecto a sus controles de acceso. Algunos sistemas permiten contar con una instalación que establezca las restricciones de acceso mediante un perfil del usuario. Dicho perfil define las funciones que cada usuario puede realizar. A través de este proceso, los sistemas operativos controlan a qué usuario se le otorga acceso y a qué recursos. A otros sistemas operativos se les debe integrar un software de control de acceso para poder obtener este nivel de control.

Algunos sistemas operativos incluyen un dispositivo que limita el número de intentos de acceso infructuosos de los usuarios a un recurso protegido. Si ese número es excedido se bloquea el acceso del usuario a dicho recurso. Este dispositivo también puede ser utilizado cuando una persona no autorizada intenta obtener acceso al sistema operativo. En este caso, se bloquea la terminal.

Evidencia de auditoría

También existen sistemas operativos que incluyen un dispositivo que puede generar informes o "rastros de auditoría" de los hechos. Dichos rastros pueden ser utilizados para identificar violaciones de seguridad e intentos de acceso no autorizados. Otros sistemas necesitan un software de control de acceso para poder identificar estos casos.

Aspectos a considerar relativos al acceso

El uso de sistemas operativos requiere la consideración de los siguientes aspectos relativos al acceso:

- Los sistemas operativos pueden ser utilizados para burlar dispositivos de control de acceso incluidos en otros componentes de software, tales como un software de control de acceso.

- La actividad de programación de sistemas debe ser cuidadosamente supervisada. Los sistemas operativos consisten en una serie de programas. Los programadores de sistemas pueden obtener acceso a los mismos y alterar el procesamiento normal del sistema.

- Las contraseñas e identificaciones del usuario deben ser confidenciales. Las personas no autorizadas que puedan acceder al sistema podrán realizar cambios no autorizados en los programas y datos.

- Los Administradores de sistemas y de seguridad de datos deben ser cuidadosamente seleccionados y supervisados ya que tienen las atribuciones necesarias para modificar las funciones del sistema, incluyendo procedimientos de generación de sistemas y perfiles de los usuarios.

- Los sistemas operativos incluyen utilitarios que permiten realizar modificaciones no autorizadas a los recursos del sistema.

- Los generadores de sistemas y los IPL deben ser supervisados ya que una generación no autorizada puede dar lugar a un procesamiento no autorizado, en tanto que los IPL pueden cambiar las opciones que controlan la ejecución del programa.

- La forma en que los software de sistemas opcionales (como por ej., TSO, CICS, etc.) han sido integrados con el sistema operativo puede afectar la efectividad de los controles de acceso basados en dichos software. Los controles de acceso incluidos en estos productos se verán afectados si no están adecuadamente integrados.

- Los informes de intentos de acceso no autorizados deben ser revisados por supervisores en forma regular a fin de identificar y realizar un seguimiento de dichos intentos de acceso.

2. Software de control de acceso

El software de control de acceso es un componente del software de sistemas diseñado para proteger los recursos contra distintas vías de acceso. Los recursos que pueden ser protegidos de esta manera incluyen las bibliotecas de aplicación y de programas del sistema, archivos de datos, diccionarios de datos, directorios de terminales y bibliotecas de sentencias de control de tareas. El software de control de acceso también puede restringir el uso de dispositivos específicos (por ej., Terminales y volúmenes de dispositivos de almacenamiento de acceso directo) y el acceso a las funciones de procesamiento de transacciones de los programas de aplicación. Además de evitar el acceso no autorizado, el software de seguridad incluye frecuentemente dispositivos que mantienen rastro de auditoría de los intentos de acceso infructuosos, como también los accesos efectuados a recursos protegidos.

Importancia para la auditoría

El software de control de acceso puede ser utilizado para limitar el acceso a los recursos sensitivos. Por ejemplo, puede ser utilizado para asegurarse de que:

- El acceso a las funciones de procesamiento del software de aplicación es controlado de manera tal que permite a los usuarios autorizados acceder sólo para llevar a cabo las tareas que se les han asignado e impide que personal no autorizado acceda al sistema.

- El departamento CIS está organizado y opera de manera tal que no permite a sus empleados llevar a cabo funciones incompatibles.

- Se establecen procedimientos para prohibir a los programadores realizar modificaciones no autorizadas a los programas.

- El acceso a los recursos del sistema está restringido a individuos autorizados.

Normalmente, el software de control de acceso es el medio principal para la protección de datos, programas de aplicación y otros recursos CIS contra accesos no autorizados.

Implantación

Cuando el software de control de acceso es instalado, se le deben definir e identificar los recursos que se desean proteger y los usuarios autorizados. Esto puede lograrse a través de la creación de perfiles o tablas de seguridad. La mayoría de los software de control de acceso incluyen funciones que permiten codificar estos perfiles o tablas. Se pueden crear perfiles de seguridad para definir: grupos de usuarios con las mismas limitaciones de acceso, un usuario individual con autorización específica de acceso o un recurso protegido (por ejemplo, un archivo) y los usuarios con acceso a dicho recurso. Los perfiles de seguridad también pueden incluir restricciones a usuarios o recursos utilizadas para controlar el acceso a funciones de procesamiento específicas o a archivos de datos (por ej., para restringir los momentos del día en que se puede utilizar un determinado recurso).

Controles de acceso

Los software de control de acceso difieren en cuanto a los recursos que pueden proteger, las vías de acceso que pueden restringir, el método de implantación y el grado de integración con otro software de sistemas.

La mayoría de los software de control de acceso restringen el acceso a las bibliotecas de programas y archivos de datos. También pueden limitar el uso de una terminal en particular o restringir el acceso a algunas bases de datos. Los productos de control de acceso también pueden variar en los niveles de seguridad para los archivos de datos. En algunos, la seguridad puede estar basada en el tipo de acceso; por ejemplo, usuarios autorizados a agregar registros a un archivo mientras que a otros sólo se les permite leer los registros de ese archivo. El control sobre el acceso a las funciones de procesamiento de los programas de aplicación puede obtenerse a través de la integración del software con un monitor de teleprocesamiento. Los monitores de teleprocesamiento restringen el acceso a los programas de aplicación pero no pueden restringir el acceso a las funciones contenidas en dichos programas.

La mayor ventaja del software de control de acceso es que puede ser usado para proteger los recursos del acceso a través de diversas vías a los datos. Algunos ejemplos de estas vías de acceso son:

- Procesamiento con actualización inmediata a través de programas de aplicación utilizando un monitor de teleprocesamiento.

- Procesamiento con actualización diferida a través de programas de aplicación. Acceso a través de editores on line.

- Acceso a través de programas utilitarios.

- Acceso a una base de datos a través de un DBMS.

Los software de control de acceso más comúnmente utilizados (por ej., RACF, ACF 2 y TOP SECRET) pueden limitar automáticamente el acceso a los recursos del sistema con excepción de casos en los que la autorización se concede en forma explícita. Si esta posibilidad es utilizada adecuadamente, el acceso a recursos tales como los archivos de datos queda restringido al creador del archivo, a menos que se permita específicamente un acceso adicional. Estos dispositivos de protección automática permiten resguardar todos los recursos, todos los archivos de datos o sólo aquellos creados por determinados usuarios.

Algunos software de control de acceso pueden ser implantados de manera que el acceso no esté restringido en forma automática. En estos casos, habrá que decidir qué recursos serán protegidos en el momento de la instalación del software.

Los software de control de acceso también difieren en cuanto al ambiente en el cual pueden ser utilizados. Estas restricciones pueden estar referidas al hardware, al sistema operativo o a otro software de sistemas. Por ejemplo, un software de control de acceso puede ser integrado con un DBMS o un administrador de acceso a archivos para restringir el acceso a las bases de datos o a los archivos de datos. Otros software de control de acceso pueden ser conectados con editores on line o monitores de teieprocesamiento para restringir el acceso a los recursos por esas vías.

El software de control de acceso responde de diferentes formas a los intentos de violación de seguridad. Entre ellas se incluyen la finalización del procesamiento, el apagado automático de las terminales, la emisión de mensajes de error o la impresión de registros de intentos de acceso.

Evidencia de auditoría

El tipo de rastro de auditoría a mantener debe ser seleccionado durante la - implantación. Por ejemplo, se puede elegir entre la opción de registrar solamente los

accesos infructuosos o registrar además todos los accesos válidos a los recursos protegidos. También puede existir la opción de seleccionar los datos específicos que se incluirán en el rastro de auditoría. Estos datos pueden ser las identificaciones de los usuarios, recursos a los que se accede, fecha, hora, localización de la terminal y datos modificados.

Aspectos a considerar relativos al acceso

El uso de un software de control de acceso requiere la consideración de los siguientes aspectos relativos al acceso:

- Los cambios a los perfiles y tablas de seguridad sólo pueden ser efectuados por el personal apropiado (por ejemplo, un funcionario de seguridad de datos).

- Los perfiles y tablas de seguridad, como así también el software de control de acceso en sí mismo, debe ser protegido de los accesos no autorizados.

- Debe llevarse un registro de todos los cambios efectuados a los perfiles y tablas de seguridad.

- Las posibilidades de eludir los perfiles de seguridad deben ser restringidas.

- Los rastros de auditoría de violaciones a la seguridad y de accesos a los recursos deben ser protegidos de modificaciones no autorizadas.

- Algunos software de control de acceso sólo pueden restringir la posibilidad de lectura o actualización de un archivo completo, pero no de datos específicos o campos dentro de un archivo. Si este tipo de restricción fuese necesario, el software de control de acceso debe ser utilizado, cuando sea apropiado, en conjunto con los controles de acceso de un DBMS.

3. Administradores de acceso a archivos

Los administradores de acceso a archivos están diseñados para proporcionar un método para la centralización y control de los datos y el acceso a los mismos. Brindan a los usuarios la posibilidad de organizar los datos en forma lógica. Algunos de ellos ofrecen múltiples técnicas de acceso a los datos. Por ejemplo, éstos pueden ser almacenados en un archivo en forma secuencial y luego ser recuperado en orden secuencial o al azar mediante

el uso de claves o índices. La mayoría de los administradores de acceso a archivos pueden ser integrados con un software de control de acceso y monitores de teieprocesamiento, lo que permite establecer un nivel adicional de seguridad para proteger datos confidenciales contra accesos no autorizados. El administrador de acceso a archivos más comúnmente utilizado en ambientes de computadores IBM es el VSAM (Virtual Storage Access Method).

Los administradores de acceso a archivos suelen también denominarse sistemas de archivo "plano" (flat file). Se puede acceder a los datos en forma secuencial o en forma directa (también denominada al azar) dependiendo de:

- El medio de almacenamiento: sólo se puede acceder a los archivos almacenados en cintas magnéticas en forma secuencial; en cambio, a los archivos almacenados en dispositivos de acceso directo (DASD) se puede acceder en forma secuencias o directa.

- El método de acceso al archivo: sólo se puede acceder en forma directa a un archivo si se utiliza un método directo de acceso tal como el VSAM.

- La estructura del archivo: para el acceso directo, cada registro del archivo debe incluir un atributo particular denominado "clave". Por ejemplo: la clave de un archivo de nombres y domicilios de clientes puede ser el número de cliente, mientras que la clave de un archivo del mayor general puede ser el número de cuenta. El software que controla y maneja el acceso directo a los archivos generalmente mantiene un índice de las ubicaciones físicas de los registros con claves específicas, el cual es empleado para localizar los registros.

Importancia para la aurora

Los administradores de acceso a archivos tienen generalmente algunos dispositivos de seguridad que pueden ser usados para restringir el acceso de usuarios no autorizados a datos confidenciales. Estos dispositivos pueden controlar el tipo de acceso permitido a cada usuario. El control del tipo de acceso que cada usuario o grupo de usuarios tiene permitido facilita la implantación de una adecuada segregación de tareas. Estos controles se basan en la utilización de identificaciones del usuario y contraseñas, pero en la práctica no son muy utilizados. En su lugar, la mayoría de las organizaciones confían en el software de control de acceso. Otro aspecto de importancia para la auditoría es que algunos administradores de accesoaarchivossonmásflexiblesqueotrospararecuperardatosparaaplicaciones de auditoría.

No obstante, los DBMSs (ver Sección D2.24) son generalmente superiores en este sentido, aun comparándolos con los administradores de acceso a archivos más flexibles.

Implantación

El administrador de acceso a archivos es seleccionado al inicio del desarrollo de la aplicación. Es necesario considerar todas las características de una aplicación a efectos de decidir cuál es el tipo de administrador de archivos más conveniente. Una vez tomada la decisión, se crean los archivos de datos con un programa de servicio o a través de un lenguaje de control.

Controles de acceso

Los administradores de acceso a archivos protegen a los datos de accesos no autorizados principalmente a través de identificaciones del usuario y contraseñas. Las contraseñas son definidas cuando los archivos de datos son creados, ya sea a través de un lenguaje de control o de programas utilitarios, como por ejemplo el IDCAMS de un ambiente le mainframe IBM, Estas contraseñas del,3n ser especificadas cuando se solicita el acceso.

Evidencia de auditoría

En el ambiente de un sistema operativo IBM MVS, los archivos del SMF (System Management Facilities) pueden ser empleados para registrar los intentos de acceso a los archivos de datos. Muchos otros sistemas operativos (aunque no todos) tienen dispositivos similares. Este tipo de archivos no está directamente disponible en un formato de fácil lectura y probablemente sea necesario utilizar un programa generador de informes que permita manejar los registros más fácilmente.

Aspectos a considerar relativos al acceso

El uso de administradores de acceso a archivos requiere la consideración de los siguientes aspectos relativos al acceso:

- El uso de dispositivos de actualización y consulta debe permitirse solamente a personal autorizado.

- Las contraseñas deben ser mantenidas en forma confidencial.

- Los procedimientos de copias de respaldo deben ser regulares a fin de que la organización reconstruya los datos computadorizados con la menor perturbación posible en el caso de pérdida o destrucción.

- Los archivos de datos deben ser protegidos de actualizaciones concurrentes.

4. Sistemas de administración de base de datos

Un Sistema de Administración de Base de Datos (DBMS - Data Base Management System) es un software diseñado para centralizar, organizar y manejar datos y proveer múltiples vías de acceso al contenido de una base de datos. Un DBMS nos permite acceder a datos integrados que traspasan límites operacionales, funcionales y de la organización. Los sistemas de administración de datos utilizados comúnmente en ambientes de grandes computadores IBM son ADABAS, DATACOM/DB, DB2, IDMS, IMS/DB y TOTAL. Un DBMS satisface la necesidad de contar con información oportuna (actualización inmediata) y de versatilidad en la recuperación de información (múltiples visiones lógicas de los datos). Los DBMS también suelen ofrecer controles sobre el acceso a vistas y campos lógicos de datos específicos.

Vistas de datos

Una vista lógica de datos es el conjunto de campos al que se puede acceder para una determinada aplicación. Una vista lógica de datos puede representar un archivo físico de datos, parte de un archivo físico de datos o una combinación de campos de múltiples archivos físicos de datos. Las diferentes vistas de datos son posibles a raíz de las relaciones entre los datos de la base de datos. El DBMS utiliza indicadores físicos internos (pointers) y/o índices que proporcionan el enlace necesario pafa,organizar el conjunto de campos que comprende cada vista lógica.

La vista lógica proporciona los datos requeridos para cada propósito específico de la aplicación. Por ejemplo, un empleado del departamento de Liquidación de Remuneraciones responsable del ingreso de datos para las hojas de trabajo puede requerir una vista lógica de los campos que contengan el número de empleado, fecha de pago y horas trabajadas. El empleado que confecciona los cheques para el pago de las remuneraciones puede requerir

una vista lógica de los campos que contengan el número de empleado, nombre y apellido, domicilio, fecha de pago, monto bruto, impuestos, otras deducciones y monto neto.

La vista lógica de datos también define la secuencia particular en que se presentan los datos. Por ejemplo, los mismos datos pueden ser requeridos para dos aplicaciones distintas, pero con un orden diferente. Una aplicación puede requerir los datos en el siguiente orden: fecha de la nómina, departamento, cargo ocupado y nombre; en tanto que el orden requerido por otra aplicación puede ser: cargo ocupado, fecha de la nómina, departamento y nombre.

La vista lógica de datos describe también las acciones que se pueden llevar a cabo sobre cada dato que la integra. Por ejemplo: el empleado que confecciona los cheques para el pago de los sueldos puede estar definido en la vista lógica sólo para leer las deducciones por impuestos. El empleado a cargo de calcular las deducciones por impuestos, a través de una vista lógica diferente, puede estar definido como para leer, cambiar o eliminar la información relativa a dichas deducciones.

Todos los datos existentes en una base de datos y las relaciones físicas bajo las cuales son almacenados se conocen como vistas físicas de datos. La vista lógica de datos presenta la vista de los datos específicos de la base de datos con independencia de su almacenamiento físico. Para acceder a los datos tal como están almacenados físicamente, el DBMS utiliza indicadores (pointers). Un indicador es la identificación de la ubicación física de los datos. Los indicadores le permiten al DBMS localizar, acceder y reunir los datos físicos incluidos en una vista lógica de datos. Por ejemplo: la vista lógica de datos que contiene número de factura, fecha, número de cliente, número de ítem y monto, puede acceder a los distintos elementos de datos desde diversas ubicaciones de la base de datos.

El software DBMS se usa para reflejar la relación lógica que existe entre los datos y su interacción con los programas de aplicación. Debido a que los datos almacenados por el DBMS son independientes de los programas de aplicación que los utilizan, tanto los programas como los datos pueden ser modificados afectándose mínimamente entre sí. Un DBMS permite que los datos requeridos por múltiples usuarios puedan ser compartidos, con lo que se elimina la necesidad de duplicar datos en archivos diferentes.

La disposición física de los datos almacenados en los archivos de bases de datos es generalmente distinta a la que se observa en los tradicionales archivos "planos", que son archivos separados de datos, cada uno de ellos organizado en base a un solo campo clave.

Existen diversas formas para acceder a una base de datos porque puede contener indicadores para varias claves distintas, lo cual proporciona gran flexibilidad para llevar a cabo modificaciones a los sistemas. Además, el acceso a través de un DBMS puede proporcionar mayor nivel de seguridad de datos, ya que las vías de acceso pueden ser mejor controladas.

Si bien un DBMS tiene características que pueden ser utilizadas para estructurar los archivos de la base de datos a fin de evitar la duplicación de datos y mejorar la independencia de los mismos, una organización puede decidir no utilizar dichas características, Los archivos resultantes (si bien se accede a los mismos por medio de un DBMS) serán muy similares a archivos "pianos".

Los distintos DBMS tienen estructuras lógicas diferentes para reflejar las relaciones existentes entre los datos. Estas estructuras más comunes son la jerárquica, de red y de relaciones. Estas estructuras inciden sobre el orden y método de acceso a los datos. La estructura de relaciones facilita la recuperación "ad hoc" de información para propósitos de auditoría u otros fines.

Importancia para la auditoría

Los dispositivos de control de acceso del DBMS pueden ser utilizados para restringir el acceso de usuarios específicos a determinadas aplicaciones del programa o a ciertas vistas lógicas. Esta característica puede ser usada para asegurar que el acceso esté controlado de manera tal que sólo permita accesos autorizados.

Las bases de datos pueden ser utilizadas para sistemas que respaldan la toma de decisiones pero que no tienen impacto directo sobre los estados financieros. Por ejemplo, una organización puede procesar ventas, compras y transacciones de liquidación de remuneraciones con un sistema convencional de archivos "piano" y luego ingresar la información desde los archivos del sistema de procesamiento de transacciones al sistema de la base de datos. El sistema de base de datos permite el acceso específico de los gerentes de la organización a información a utilizar en la toma de decisiones sobre comercialización, compras, alquiler o de otro tipo. La base de datos no puede ser utilizada para agregar, eliminar o modificar la información contenida en el sistema de archivos "pianos". Las decisiones tomadas por la gerencia, que dan lugar a transacciones que son incluidas en los estados financieros, serán reflejadas en el sistema de procesamiento de transacciones. Aunque existe el riesgo de que se tome una decisión basándose en información inexacta, la

confiabilidad de los estados financieros (incluyendo los efectos de las decisiones erróneas) preparados por el sistema de procesamiento de transacciones w afectada por el sistema de la base de datos.

Diccionarios y archivos de datos

Frecuentemente, cuando se instala un sistema de base de datos sofisticado se requiere la designación de un administrador de base de datos (DBA - Data Base Administrador), quien es responsable del diseño global y mantenimiento de la base de datos y del enlace con los departamentos usuarios que comparten el sistema. Las responsabilidades del DBA incluyen el mantenimiento de un diccionario de datos. El diccionario de datos es una descripción de los datos contenidos en la base de datos incluyendo el nombre, tipo, uso, tamaño del campo y fuente de los datos, así como también de los programas de aplicación autorizados a utilizar dichos datos.

Un diccionario activo puede tener significatividad de auditoría ya que puede controlar y también describir los programas de aplicación y las funciones de programa autorizadas a acceder a diversos elementos de los datos. También puede ser utilizado para determinar el efecto de un cambio en algún componente de los datos sobre los estados financieros, ya que identifica las relaciones entre los elementos de los datos y los programas de aplicación, incluyendo aquellos que afectan los estados financieros, Un diccionario de datos pasivo no es tan útil ya que puede estar desactualizado. Ambos tipos de diccionarios son descriptos a continuación.

Los diccionarios de datos también facilitan el desarrollo de programas de consulta de auditoría, los cuales en general, son más complejos que en el caso de archivos "planos" convencionales, en los cuales se utilizan paquetes estándar de recuperación como fuente de los programas de consulta. Sin embargo, se pueden realizar consultas simples a los archivos de la base de datos utilizando las facilidades de consulta provistas por el mismo DBMS.

Un diccionario de datos activo permite incluir el formato de datos y los perfiles de los usuarios en los programas de aplicación. Si se utiliza un compilador o un ensamblador para traducir los programas fuente a lenguaje de máquina, las modificaciones al diccionario de datos se reflejarán en los programas de aplicación cuando estos sean recompilados o reensamblados. Los programas que se ejecuten sin recompilación o reensamblado no reflejarán las modificaciones. Si se utiliza un programa intérprete, las modificaciones al diccionario de datos sé efectivizan de inmediato. Un diccionario de datos activo también

puede generar en forma automática las definiciones de la base de datos (incluyendo perfiles de acceso) con ingreso de datos similares al idioma inglés.

Los diccionarios de datos pasivos son utilizados para proporcionar documentación a los programadores Estos diccionarios no están conectados directamente con el programa de aplicación y, por lo tanto, se requieren controles manuales para asegurar que todas las modificaciones al diccionario de datos se reflejan en los correspondientes programas de aplicación. Si bien la mayoría de los DBMS actualmente en uso sólo cuentan con diccionario pasivo, se espera que el uso de diccionarios activos aumente. Un diccionario activo es más útil que un diccionario pasivo porque puede asegurar que las definiciones actuales incluidas en el mismo son coherentes con el acceso a los datos del programa de aplicación.

Implantación

Una "sesión" DBMS se inicia habitualmente al comienzo del día y continúa en ejecución durante el resto del mismo a fin de que la información esté a disposición de los usuarios. En muchas instalaciones se asegura el uso de los DBMS durante las 24 horas del día. En el sistema operativo se adjudica una alta prioridad al DBMS con el objetivo de permitir una actualización inmediata de la base de datos. La mayoría de los DBMS mantienen registros diarios de las modificaciones realizadas para una eventual recuperación de datos. En caso de destrucción de la base de datos, sólo se deberán reprocesar los registros modificados desde que se realizó la última copia completa de. respaldo. En un ambiente bien controlado, las copias de respaldo de las bases de datos se realizan en forma regular.

Puede accederse a los datos a través del DBMS en la modalidad de actualización inmediata con programas de aplicación (utilizando una interfase con un Lenguaje de Manipulación de Datos (DML - Data Manipulation Language), con dispositivos de consulta o con un lenguaje de cuarta generación (similar al idioma inglés). El DML es un lenguaje de alto nivel que permite que los usuarios de bases de datos tengan acceso a dicha base a través del DBMS. En la modalidad de actualización diferida, se puede acceder a los datos a través del DBMS utilizando programas de aplicación (a través de un DML) o mediante programas generadores de informes.

Los utilitarios de la base de datos, utilizados por el grupo de Administración de la base de datos, proporcionan funciones de mantenimiento de la base de datos, tales como

copias de respaldo y restauración de la base de datos, reorganización de datos, estadísticas sobre la base de datos y revisión de las relaciones internas de los indicadores físicos e índices. Estos utilitarios también pueden ser utilizados para agregar o eliminar datos en forma masiva.

Cuando un usuario solicita inicialmente el uso del DBMS, se establece la identificación de dicho usuario. En la modalidad de actualización inmediata, el usuario es identificado por su identificación de usuario, identificación de la terminal y por aplicación o función. En la modalidad de actualización diferida el usuario es identificado por el nombre del trabajo y por aplicación o función. Todos los accesos a los archivos de datos a través del DBMS son "rastreados" por medio de los datos de identificación del usuario.

Controles de acceso

Los controles de acceso pueden ser establecidos de dos maneras. En primer lugar, se puede usar un sistema de identificaciones del usuario/contraseñas para permitir el acceso a terminales, archivos, campos, programas (o porciones de éstos) a cualquier usuario luego de haber ingresado la contraseña correcta. En segundo lugar, se pueden emplear perfiles del usuario, en cuyo caso el usuario ingresa al programa de aplicación un código que lo identifica y que le permitirá tener acceso a las vistas lógicas de datos autorizados.

Mediante el uso de identificaciones de usuario y contraseñas, se pueden restringir las consultas o actualizaciones de datos a los niveles de vistas lógicas de datos, campo o valores de campos. La seguridad a nivel de campo está relacionada con la sensibilidad de ciertos campos, como en el caso de los salarios. La seguridad a nivel de valor de campo se relaciona con el contenido del campo. Por ejemplo, a un empleado del área de liquidación de remuneraciones se le pueden restringir las actualizaciones de campos de remuneraciones superiores a $50.000 a fin de mantener la confidencialidad de las remuneraciones de la gerencia superior. Normalmente, se requiere una contraseña diferente para cada nivel de seguridad. Aun el grupo de administración de datos debe suministrar la clave apropiada para utilizar un utilitario de la base de datos contra datos protegidos por contraseñas. Los datos extremadamente sensitivos pueden ser "mezclados" cuando son almacenados físicamente mediante técnicas de codificación. En esta circunstancia, aun si la clave de seguridad fuera quebrantada o eludida, se debe tener conocimiento de la rutina de descodificación y utilizarla para leer los datos.

Debe señalarse que el software DBMS puede restringir el acceso a las vistas lógicas de datos a los cuales se ha accedido a través del DBMS pero no puede restringir el acceso a los datos por otras vías de acceso, como por ejemplo, software de sistemas sensitivos como los editores on line. Por consiguiente, el software DBMS debe estar integrado con un software de control de acceso para proporcionar un nivel de control efectivo sobre el acceso no autorizado.

Los perfiles de los usuarios pueden ser mantenidos por el Diccionario/Directorio de datos (DD/DS Data Dictionary/Directory System). El DDIDS proporciona una vista de datos específica o un conjunto de vistas para cada aplicación. Cada vista de datos especifica si el usuario está habilitado para consultar o actualizar cada uno de los campos dentro de la vista. A través de este método de seguridad, cualquier sistema cuya interfase con el DBMS se haga a través del DDIDS, puede ser controlado. Estos sistemas incluyen generalmente una función de consulta, lenguajes de cuarta generación, programas generadores de informes y posiblemente un lenguaje de manipulación de datos.

Evidencia de auditoría

Los rastros de auditoría que existen en la mayoría de los DBMS se utilizan principalmente para recuperación de datos. Como los DBMS facilitan el acceso a los datos para diversas aplicaciones, es importante que posean los medios para restaurar todas las modificaciones efectuadas a una base de datos en el caso de una falla en la base de datos o en otro lugar del sistema. Por lo tanto, el DBMS debe registrar todas las modificaciones; este registro, a su vez, constituye un rastro de auditoría de las actividades realizadas en la base de datos.

En muchos DBMS existen tres tipos de registros de recuperación en lenguaje de máquina: imágenes anteriores, imágenes posteriores y un registro diario de transacciones. Las imágenes anteriores, como el término indica, incluyen el contenido del registro de la base de datos (o la parte afectada del mismo) antes de la actualización. Se utilizan si, en caso de una recuperación, es necesario reversar una actualización errónea, Por el contrario, las imágenes posteriores (el contenido de un registro de base de datos inmediatamente después de la actualización) se utilizan para recuperar las actualizaciones completadas exitosamente en el caso de que el sistema falle. Aunque las imágenes anteriores y posteriores constituyen un rastro de auditoría detallado, debemos comprender que, dado que han sido creadas específicamente para recuperación de datos, generalmente no están en un formato preciso y de fácil lectura para que el auditor pueda utilizarlas. Para reconstruir una

serie de actualizaciones se requiere un software especial y la salida de datos requerirá un considerable análisis.

El registro diario de transacciones es un rastro de auditoría más tradicional, ya que detalla todas las funciones de aplicación específicas que causaron la actualización.

Es un registro de todas las "causas" de las actualizaciones, mientras que las imágenes posteriores son un registro de sus "efectos". En algunos DBMS se mantiene un registro de todos los accesos a la base de datos, no sólo de las actualizaciones; en estos casos el registro es conocido como un registro de acceso. En muchos casos, las imágenes anteriores y posteriores, como también los ingresos al registro diario de transacciones, están mezclados en el mismo archivo físico. También en este caso se requiere un software especial para leer dichos archivos.

Procedimientos de copias de respaldo (backup), reenganche y recuperación

□

□

La integridad de los datos está protegida a través de funciones de auto-retroceso y auto-reenganche del DBMS.

Si una actualización inmediata o diferida de una transacción termina anormalmente, el DBMS automáticamente retrocede las actualizaciones inconclusas hasta el final de la última transacción lógica. En la modalidad de actualización inmediata, el final de una transacción lógica usualmente se relaciona con una pantalla de ingreso o una serie de pantallas. Por ejemplo: el final de una transacción lógica de ingreso de datos a un registro de personal recién incorporado puede incluir la información básica (nombre, domicilio, etc.) en la primera pantalla. El final de una segunda transacción lógica puede ser la información sobre deducciones (por impuesto, aportes jubilatorios, etc.) ingresada en la próxima pantalla. Por lo tanto, si la terminación fuera anormal durante el ingreso de datos en la segunda pantalla, la información ingresada en la primera no se perdería.

El reenganche automático funciona cuando el sistema operativo termina su actividad en forma anormal mientras los usuarios están actualizando datos a través del DBMS. Cuando el sistema operativo entra en funciones nuevamente, el DBMS actualiza cualquier operación que haya alcanzado el final de su transacción lógica y retrocede en los casos en

que las transacciones no hubieran llegado al final de su transacción lógica. No obstante, cuando existe un daño físico a la base de datos, los datos en el área dañada deben ser reemplazados a partir de la última copia de dicha área. Las actualizaciones posteriores deben ser regeneradas de los registros de rastros de auditorías gerenciales que mantiene el DBMS.

Aspectos a considerar relativos al acceso

El uso de un DBMS requiere la consideración de los siguientes aspectos relativos al acceso:

- El uso de las posibilidades de consulta y actualización desde los programas de aplicación, los dispositivos de interfaces del DBMS y los utilitarios del DBMS de6e estar restringido únicamente al personal apropiado.

- Las funciones de seguridad implantadas en el DBMS son efectivas únicamente cuando el acceso a la base de datos se efectúa a través de l DBMS. Por ejemplo, un programador de sistemas puede acceder a los datos de ventas dentro de la base de datos utilizando un editor on line o un utilitario en vez de hacerlo a través de l DBMS. Por lo tanto, también puede necesitarse un software de control de acceso para prevenir accesos no autorizados a los programas y datos.

- Los procedimientos de copia de respaldo y de reenganche y recuperación de l DBMS deben ser adecuados para asegurar la integridad de los datos.

- Los procedimientos de mantenimiento de los perfiles de seguridad en el DDIDS y las tablas de seguridad de l DBMS deben evitar los accesos no autorizados a información sensitiva.

Comparación entre el DBMS y el software
de administración de acceso a archivos

□

Las ventajas del DBMS en relación con el software de administración de acceso a archivos son:

□

- Los datos son compartidos entre los usuarios para reducir duplicaciones y falta de uniformidad.

- El acceso a los datos es controlado por medio de contraseñas y perfiles de l usuario.

- Se logra una mayor independencia de los datos con respecto a las aplicaciones que los usan, lo cual proporciona una mayor flexibilidad para el desarrollo y modificación de los programas de aplicación.

- Se mejora el poder de recuperación de los datos incluyendo procedimientos de reenganche y recuperación. (La mayoría de los administradores de acceso a archivos no cuentan con estas posibilidades, las cuales pueden ser implantadas mediante el uso de otro software de sistemas).

Las desventajas potenciales de un DBMS en relación con el software de administración de acceso a archivos son:

- A menudo se requiere el uso de software y hardware más caro y complejo.

- Puede requerirse un largo proceso de conversión.

- El personal puede mostrarse reticente a adoptar los cambios que se produjeron en el sistema computadorizado.

- Si no existen controles de acceso adecuados, puede ser más fácil efectuar cambios no autorizados a los datos.

Una interrupción imprevista en el procesamiento de l DBMS puede afectar adversamente la integridad de los datos, afectando potencialmente todas las aplicaciones y/o programas que utilizan el DBMS.

5. Editores on line

Los editores on line son utilizados para controlar la creación y modificación de programas de aplicación, registros de trabajos realizados y archivos de datos. Proporcionan capacidades de actualización inmediata que facilitan el desarrollo de aplicaciones e incrementan la productividad de los programadores. Muchos de los editores on line ofrecen procedimientos sistemáticos para la organización de bibliotecas de programas. Algunos de ellos incluyen dispositivos que permiten la ejecución de aplicaciones bajo su control. Los editores on fine más comúnmente utilizados en ambientes de computadores grandes IBM son TSOIISPF, ICCF, WYLBUR, CMS y ADS/O.

Importancia para la auditoría

El uso de editores on line implica un riesgo porque proporcionan los medios para acceder a programas y datos sensitivos. Dan a los usuarios la posibilidad de modificar programas y registros de control de trabajos que afectan los estados financieros y los informes gerenciales. Algunos editores on line permiten a los usuarios ejecutar trabajos de actualización diferida por su intermedio, lo que origina un riesgo ya que los trabajos usados para actualizar datos confidenciales podrían ser ejecutados sin el conocimiento de la gerencia.

Los editores on line incluyen utilitarios para el mantenimiento de bibliotecas de programas y de control de trabajos, los cuales pueden ser utilizados para eliminar o copiar bibliotecas enteras o partes de las mismas. Esto origina un riesgo porque los programas o los registros de trabajos utilizados para actualizar datos usados en la preparación de estados financieros o informes gerenciales pueden ser alterados o destruidos. Algunos editores on line no dejan un rastro de auditoría que detalle los intentos de accesos autorizados y no autorizados.

Muchos de los editores on line proporcionan los medios adecuados para controlar estos riesgos. Por ejemplo, pueden restringir los accesos de actualización a determinadas bibliotecas de programas. Esta posibilidad puede ser utilizada para implantar una adecuada segregación de funciones. También se pueden implantar otras alternativas, tales como las que restringen el uso de las opciones de l editor a usuarios autorizados.

Implantación

La mayoría de los editores on line incluyen medios de seguridad opcionales, los cuales son implantados en el momento de su instalación. Existen tablas de control en donde se incluyen los perfiles de los usuarios con datos sobre el personal autorizado a usar el editor, las opciones disponibles para cada usuario y la identificación y contraseña de cada usuario. Las bibliotecas de programas y los controles de acceso a estas bibliotecas pueden ser implantados en este momento. Las bibliotecas pueden ser creadas en cualquier momento después de la instalación del editor on line.

Controles de acceso

Los editores on line difieren en cuanto al tipo de acceso que pueden controlar, el tipo de protección de recursos que proporcionan, la capacidad de someter y procesar trabajos a través de l editor y los utilitarios provistos para la manipulación y control de las bibliotecas de programas. Algunos editores on line pueden restringir ciertos tipos de acceso a determinados usuarios. Por ejemplo, los programadores de l departamento de liquidación de remuneraciones pueden tener acceso de lectura y actualización a los programas de la biblioteca de liquidación de remuneraciones, mientras que pueden tener acceso restringido (de lectura únicamente) a la biblioteca de programas de cuentas a pagar.

Diferentes editores on line disponen de distintos tipos de protección de recursos. Algunos de ellos protegen los recursos estableciendo niveles de autorización para cada recurso protegido. Por ejemplo, si al intentar acceder a una biblioteca, el nivel de autorización de l usuario es inferior al nivel de autorización asignado a la biblioteca, el acceso será denegado. Otros editores on line emplean identificaciones de l usuario/contraseñas para evitar los accesos no autorizados. Después de un número predeterminado de intentos de acceso con una contraseña incorrecta, el sistema emite'un mensaje de error y el acceso es denegado.

La mayoría de los editores on line permite la ejecución de trabajos de actualización diferida directamente desde una termina l. Algunos brindan la posibilidad de procesar las aplicaciones bajo el control de l editor. El ISPF, por ejemplo, incluye un dispositivo denominado administración de diálogo (dialog management) que permite que las aplicaciones sean diseñadas y procesadas directamente bajo el control de l editor a través de l uso de pantallas o paneles de l ISPF.

Los editores on line pueden ser utilizados para controlar bibliotecas de programas, de registros de trabajos realizados y otras. Algunos editores on line, por ejemplo, permiten a los usuarios autorizados crear, eliminar y copiar bibliotecas directamente desde la termina l. Otros editores on line controlan los movimientos entre bibliotecas. Por ejemplo, un editor on line puede ser utilizado para movilizar un programa de una biblioteca de prueba a una biblioteca de producción.

Los editores on line pueden ser integrados con un software de control de acceso o un monitor de teieprocesamiento para brindar un segundo nivel de seguridad para la ejecución de trabajos y protección de los archivos.

Evidencia de aurora

Algunos editores on line proporcionan rastros de auditoría detallados de las actividades sobre datos, bibliotecas y otros recursos protegidos. Estos rastros de auditoría generalmente brindan información tal como la identificación del usuario, fecha y hora de acceso, y recurso al que se accede. Constituyen un registro de hechos, incluyendo las violaciones de seguridad y accesos autorizados.

Aspectos a considerar relativos al acceso

El uso de editores on line requiere la consideración de los siguientes aspectos relativos al acceso:

- Los dispositivos opcionales de seguridad deben ser utilizados apropiadamente.

- Se deben tomar precauciones para asegurar que la ejecución de trabajos de actualización diferida está restringida al personal autorizado.

- Se deben tomar precauciones para asegurar que los utilitarios que permiten la manipulación de bibliotecas (por ejemplo, eliminar, copiar) están protegidos de usos no autorizados.

- Se deben tomar precauciones para asegurar que sólo el personal autorizado tenga acceso a las aplicaciones que se ejecutan bajo el control de un editor on line.

- Se deben tomar precauciones para asegurar que sólo usuarios autorizados pueden actualizar las bibliotecas de producción o partes de las mismas.

- Los rastros de auditoría producidos por los editores on line deben ser cuidadosamente revisados para identificar posibles violaciones de seguridad.

III. Software de Aplicación

Introducción

El software de aplicación consiste en programas escritos para llevar a cabo tareas especificas para los usuarios finales. Estos programas pueden ser desarrollados internamente o comprados a proveedores de software. Los paquetes de software comprados se utilizan a menudo para funciones estándar de contabilidad tales como mayor general, pago de remuneraciones, cuentas a cobrar y cuentas a pagar.

Los paquetes de software se pueden comprar en código fuente o en código objeto, si bien, por lo general, los proveedores prefieren suministrar únicamente las versiones en código objeto ya que son más difíciles de modificar. Muchos proveedores ofrecen versiones en código objeto que incluyen "user exits" que permiten que el comprador del paquete pueda adaptar partes de los programas a sus necesidades especificas.

Frecuentemente, el software de aplicación debe ser modificado para ser adaptado a las necesidades de los usuarios. Es importante controlar dichas modificaciones para asegurarnos de que sólo se efectúan cambios autorizados a los programas que procesan datos significativos.

1. Desarrollo de sistemas

Es obvia la importancia que tienen los sistemas de aplicación en la registración, procesamiento e información de los datos de una organización. El proceso de desarrollo de sistemas suele tener gran importancia para nuestros clientes y también puede ser de importancia para nosotros. La gerencia debe asegurarse de que los sistemas hayan sido adecuadamente diseñados, probados e implantados y de que se han incluido los controles adecuados. Como auditores, nos interesa que una vez que los sistemas que procesan información significativa para los estados financieros han sido instalados, incluyan controles adecuados que funcionen de la manera esperada.

Debido al alto costo del desarrollo de los sistemas computarizados y a la incidencia cad vez mayor que tiene sobre la eficiencia y competitividad de una organización, la gerencia superior suele estar muy involucrada en esta área. La comprensión del proceso de desarrollo de sistemas facilita la comunicación del auditor con la alta gerencia, a la que podrá aportar sus conocimientos sobre el tema.

El proceso de desarrollo puede ser descrito de la siguiente manera :

- Se identifica una necesidad.
- El usuario junto con el analista, determina qué debe hacerse para satisfacer dicha necesidad.
- Los analistas determinan de qué forma se hará.
- Los programadores desarrollan el software que lo hará.
- Los programadores prueban el software y los analistas y los usuarios prueban el sistema.
- Las gerencias del Departamento de procesamiento de datos y del Departamento usuario aprueban el sistema.
- El sector de Operaciones implanta el sistema.

Obviamente, esta es una simplificación de los pasos de este proceso. Sin embargo, brinda una visión global del proceso típico que debe seguir una organización cuando desarrolla internamente un sistema de información computadorizado. Existen paquetes de software que pueden satisfacer las necesidades del usuario más eficientemente que los sistemas desarrollados internamente. En estos casos, los pasos tercero, cuarto y quinto serán reemplazados por la evaluación e implantación del software.

En este proceso resulta fundamental el trabajo en conjunto de usuarios y personal del Departamento de procesamiento de datos. Si los usuarios no participan activamente en el proceso, existe una alta probabilidad de que los proyectos de desarrollo de sistemas fracasen. Algunas organizaciones intentan solucionar este problema estableciendo un Comité de Dirección (Steering Committee) en las etapas iniciales de un proyecto de desarrollo de sistemas. Por lo general, estos comités incluyen representantes de los grupos usuarios, del Departamento CIS, de auditoría interna y de niveles gerenciales. El comité supervisa cada etapa del proceso de desarrollo, y del proceso de implantación.

Hay muchas metodologías aceptables en uso para el desarrollo de sistemas. El enfoque SMM se usa aquí como ej., no sólo por tratarse del enfoque de los auditores, sino porque es una buena referencia para comprender el proceso de desarrollo de sistemas.

A continuación se enumeran las etapas generales de la plicación del enfoque SMM en el desarrollo de sistemas :

- Análisis.
- Diseño.
- Construcción
- Implantación.
- Apoyo.

IV. Intercambio Electrónico de Datos

1. Visión general

El Intercambio Electrónico de Datos (EDI - Electronic Data Interchange) representa un cambio fundamental en la forma en que las compañías conducen sus operaciones con sus clientes, proveedores, distribuidores, concesionarios, bancos, transportistas y con los organismos gubernamentales. Los métodos tradicionales de comunicación empresaria incluyen el envío de documentos como por ejemplo cheques, órdenes de compra, órdenes de pedido, facturas, etc. enviadas a través de servicios postales regulares o especiales; comunicaciones telefónicas o por facsímil. Es usual que los datos de dichas comunicaciones sean digitados una y otra vez en series de distintos sistemas a lo largo del ciclo operativo. El EDI permite reemplazar estas actividades relativamente engorrosas y que insumen tiempo por comunicaciones de información más veloces y precisas de computador a computador, libres de papeles que entorpecen la tarea. A medida que aumente la difusión del EDI, se espera que cada vez más compañías establezcan una comunicación electrónica con otras compañías para transmitir grandes volúmenes de información crítica, de computador a computador, sin intervención humana.

El EDI está relacionado tanto con el concepto general del uso de transmisiones electrónicas que reemplazan al papel, como con un conjunto de normas que grupos industriales están desarrollando en los Estados Unidos y en otros países para facilitar la implantación del concepto. Se han desarrollado normas EDI para elementos de datos y formatos de mensajes electrónicos para una amplia gama de transacciones, como por ejemplo, órdenes de compra, facturas, órdenes de pedido, notas de despacho, remitos, notas de pago, informes de discrepancia, acuses de recibo, conocimientos de embarque y otros documentos comerciales y de transporte. Las normas consideran tanto campos opcionales como necesarios para que las compañías puedan transmitir únicamente los datos necesarios para satisfacer sus propios requerimientos.

Las compañías que utilizan EDI obtienen muchos beneficios. La computadorización de las transacciones de rutina le han permitido a algunas compañías reducir sus gastos generales y existencias, intercambiar datos en forma más oportuna, mejorar el servicio a sus clientes, mejorar la administración de fondos, obtener descuentos, eliminar el ingreso de datos redundantes (y por consiguiente, disminuir los errores provocados por dicho ingreso de datos) y mejorar la planificación de recursos. Ajustándose a las normas existentes, las redes de cientos o miles de asociados (por ej., proveedores y clientes) pueden implantar velozmente un sistema EDI, utilizando paquetes de software proporcionados por proveedores y servicios de comunicaciones ofrecidos por redes de terceros. Además, una vez que una compañía ha implantado el sistema con un asociado, le resultará relativamente sencillo trabajar con otras compañías de la misma manera, aplicando las mismas normas.

El sistema EDI puede ser implantado sin alterar el manejo contable, de producción, de pedidos u otros sistemas de computación existentes. El concepto EDI clave que permite este uso es el "traductor". La información con que se cuenta en la mayoría de los sistemas, como por ejemplo, descripción, cantidad y monto de ciertas partidas es tomada de la aplicación existente y reformateada (traducida) al lenguaje estándar aplicado en el software EDI. Luego, será transmitida a través de una red de comunicaciones de datos a otra entidad e interpretada por el software EDI al llegar a su destino. Por lo tanto, la información transmitida estará inmediatamente disponible para ser utilizada por los sistemas existentes en la compañía receptora.

2. Ejemplos de EDI

El EDI puede ser aplicado en prácticamente cualquier departamento y sistema de la compañía. En realidad, los beneficios del sistema pueden ser mayores si se lo utiliza en departamentos vinculados y sistemas integrados entre sí, como se demuestra en los ejemplos que se incluyen a continuación.

3. Manejo de pedidos

Una compañía del sudeste de los Estados Unidos tiene un cliente importante en la Costa Oeste. En lugar de enviar una copia impresa de la orden de compra, el cliente transmite un lote de órdenes electrónicas. La transmisión se realiza en las primeras horas de la mañana de la Costa Oeste y llegan al comienzo de la jornada laboral en el Sudeste. Las órdenes de compra electrónicas quedan inmediatamente a disposición del sistema de manejo de órdenes de la compañía a fin de procesarlos y transmitirlas a la planta productora para su inclusión en el programa de producción.

4. Despacho

Muchas compañías solicitan a sus proveedores que despachen las mercaderías terminadas en una determinada secuencia (el orden en el que son utilizadas en el proceso de fabricación) y requieren una notificación inmediata del envío de los productos desde el lugar de despacho. La única forma práctica de lograrlo en un tiempo razonable es a través de medios electrónicos. Se transmite un aviso de despacho al mismo tiempo que un empleado del sector de despachos ingresa la confirmación de que el transportista ha aceptado y firmado el conocimiento de embarque. El aviso de despacho puede ser enviado inmediatamente o puede ser mantenido en un "buzón postal" electrónico hasta que sea recogido por el cliente.

5. Facturación

A la mayoría de las compañías les interesa facturar las mercaderías en el momento de despacho. La factura electrónica puede ser preparada y transmitida al mismo tiempo que se genera el aviso de despacho. Algunas compañías han avanzado aún más y utilizan el aviso de despacho en lugar de la factura, eliminándose de esta manera uno de los pasos del ciclo de facturación. La compañía que recibe las mercaderías considera al aviso de despacho como un informe de recepción, como una factura y como un ingreso al sistema de producción y de esta manera, puede pagar las mercaderías tan pronto como se completen los restantes requerimientos.

6. Cuentas a pagar

El volumen de facturas que una empresa de cierta magnitud recibe puede ser un problema en cuanto a su procesamiento oportuno si su comparación con las órdenes de compra o informes de recepción no está completamente automatizada. El sistema EDI permite recibir la información de facturación en forma electrónica. Este método elimina la necesidad de reingresar los datos de facturación al sistema de cuentas a pagar y facilita la conciliación automatizada de por lo menos una porción de las facturas recibidas.

7. Administración de fondos

El sistema EDI incluye una función de transferencia electrónica de fondos (EFT Electronic Funds Transfer). Muchas compañías se ven entorpecidas para cumplir con el programa de pagos por la combinación de esfuerzos manuales, automáticos y mecánicos que se requieren para procesar facturas, preparar cheques y sobres que luego deben ser enviados. Estos procedimientos pueden resultar tan engorrosos que existe el riesgo de que las facturas sean pagadas sin completar la revisión que el departamento de cuentas a pagar hubiera deseado, para cumplir con condiciones básicas, como por ejemplo pagos a 30 días. El EFT le permite a la compañía programar sus pagos basados en otros criterios, como por ejemplo descuentos por pagos inmediatos o consideraciones de administración de fondos. Sabiendo que los pagos son automáticos, se pueden elaborar políticas que permitan el pago a último momento según las condiciones establecidas con los proveedores, sin necesidad de tener fondos ociosos durante un tiempo indeterminado.

8. Costos de transporte

Los costos de transporte son manejados de diversas formas. Algunas compañías disponen que bancos u otras organizaciones controlen y paguen sus facturas por flete. Estos agentes de pago pueden utilizar sistemas EDI para recibir datos de quienes transportan mercaderías hacia o desde la compañía por vía terrestre, marítima o aérea. El EDI está ampliamente difundido en el área de transportes. De hecho, ha surgido de esta industria a principios de la década del 70. Muchos transportistas ofrecen acceso a los despachantes de mercaderías a sus sistemas de reservas y rastreo, que difieren de los verdaderos EDI sólo en que estos sistemas son de propiedad de una empresa en particular en lugar de estar destinados a los usuarios en general.

El amplio uso que los transportistas y agentes hacen de los sistemas automatizados y sistemas EDI permite al departamento de despacho de una compañía solicitar la recepción de los datos que considere necesarios. Por ejemplo, si una compañía opera con el extranjero y envía los pedidos directamente al cliente, podría no poder facturar las mercaderías en tránsito hasta que dichas mercaderías hayan ingresado al país. Una forma rápida y confiable de obtener los datos necesarios es recibir una copia electrónica de la orden de despacho a plaza emitida por el agente del transportista marítimo, lo cual indicará que los requerimientos del gobierno y del transportista correspondientes a dicho envío ya han sido completados.

9. Consideraciones de auditoría

El EDI se aparta un paso más de la documentación de transacciones con implicancias financieras. Esta tendencia cada vez mayor de confiar en los medios electrónicos ya se ha iniciado hace algún tiempo en la mayoría de las principales compañías, representada por la preponderancia de los sistemas computadorizados relacionados con remuneraciones, contabilidad e información financiera. El EDI es la prolongación de esta tendencia para interactuar con terceros. A medida que estos sistemas cubren las transacciones externas de una compañía, las relaciones entre los sistemas internos también tienden a ser más automatizados, ya que se eliminan las "conexiones de papel" (existe una conexión de papel cuando la copia impresa de un sistema es la base para el ingreso de datos a otro sistema).

El uso del EDI origina diversas implicancias de auditoría. Estas incluyen:

- El acceso de terceros a los sistemas computadorizados del cliente es una característica de los EDI. Cuando se otorga acceso a los sistemas, existe el riesgo de que se logre obtener acceso no autorizado a datos y programas. Además la presencia de vías de acceso para terceros puede aumentar el riesgo de acceso no autorizado (como por ej., el acceso de "hackers"). Por lo general, se requieren controles de acceso basados en software para otorgar acceso sólo a los terceros autorizados y para restringir su acceso a las funciones autorizadas.
- En un ambiente en el que las transacciones quedan documentadas, la gerencia podrá revisar y evaluar los cambios realizados en los datos para verificar su razonabilidad. Por ejemplo, los precios de venta especiales pueden ser investigados por el responsable de aprobar las facturas de venta. En un sistema EDI adecuadamente diseñado, la revisión de la gerencia puede ser lograda más eficientemente. Por ejemplo, el sistema puede registrar electrónicamente y señalar los cambios que se realizaron en las transacciones. Luego, emitirá informes de excepción sobre las transacciones que no reúnen criterios preestablecidos. En un sistema no bien diseñado, la posibilidad de la gerencia de evaluar la razonabilidad de los cambios será disminuida por la ausencia de un rastreo de las transacciones.
- El riesgo de que los datos sean modificados sin que los controles del cliente o los procedimientos de auditoría detecten el cambio puede ser mayor cuando los datos son transmitidos y almacenados en forma electrónica. Las alteraciones que se realizan en la copia original de un documento son difíciles de disimular. Sin embargo, se pueden alterar los datos almacenados electrónicamente sin dejar un rastro fácilmente

identificable de las modificaciones realizadas. La confianza gerencial y de auditoría generalmente es depositada en controles de acceso basados en software.

- La obtención de evidencia de auditoría de que las transacciones han sido autorizadas puede resultar más complicada que en un ambiente CIS convencional, Las transacciones EDI pueden ser autorizadas electrónicamente sin dejar evidencia escrita. Por ejemplo, las identificaciones del usuario/contraseñas que se asignan a individuos seleccionados le indican al sistema que estos individuos pueden autorizar transacciones específicas. También se pueden autorizar transacciones comparando datos transmitidos y almacenados electrónicamente sin participación humana y sin documentación escrita para evidenciar las transacciones subyacentes, Por ejemplo, la comparación electrónica de información de recepción, orden de compra y factura en un sistema de cuentas a pagar/compras puede proporcionar la "autorización" requerida para pagar una factura. En estas circunstancias será necesario que depositemos mayor confianza en las funciones de procesamiento y en los controles computadorizados.
- Uno de los objetivos de muchos sistemas EDI es proporcionar y mantener rastros de transacciones y documentos fuente en forma electrónica. En algunos sistemas EDI es probable que no existan los documentos que tradicionalmente han proporcionado importantes fuentes de evidencia de auditoría. Por ejemplo, como se comentó anteriormente, en algunos sistemas de compras/cuentas a pagar, la transmisión electrónica de avisos de despacho elimina la necesidad de obtener facturas de compra. La ausencia de documentación en los sistemas EDI obliga a poner mayor énfasis en el uso de las técnicas de auditoría computadorizadas como una forma de obtener evidencia de auditoría.

10. Resumen

Las herramientas más poderosas para controlar el acceso a los programas y datos y detectar cambios no autorizados a los mismos requieren el uso de software. Estas herramientas se han convertido en elementos especialmente importantes con el creciente uso de sistemas computadorizados descentralizados. Para muchos de nuestros clientes, el control de acceso no puede ser proporcionado únicamente por restricciones sobre el acceso físico a las instalaciones del computador.

Existen diferentes tipos de software de sistemas que proporcionan diversos grados de control. El control de prevención o detección proporcionado por algunos componentes de software puede ser vulnerado por otros (por ej., los dispositivos de control de acceso proporcionados por un sistema de administración de base de datos pueden ser vulnerados si el acceso a la base de datos se realiza a través de un editor on line en lugar de un DBMS).

Para comprender las capacidades y riesgos de un sistema computadorizado en su totalidad, debemos considerar la capacidad de los componentes de software individualmente, cuáles son las que se utilizan y la forma en que interactúan entre ellas.

V. Transmisión de Datos

1. Redes y Organizaciones de Servicios

a) Enfoque de auditoría

Como se mencionó anteriormente, las organizaciones que utilizan tecnología de transmisión de datos son potencialmente vulnerables a accesos no autorizados a los datos y programas y errores ocurridos durante la transmisión de los mensajes. En esta sección se analizan los principales métodos de transmisión de datos existentes y los distintos niveles de riesgo asociados con cada uno de ellos.

b) Visión global de la tecnología

Las redes de transmisión de datos son medios que proporcionan las conexiones necesarias para permitir la transferencia de datos entre componentes de un sistema de computación que necesitan comunicarse (tales como CPU y terminales). Las redes pueden ser clasificadas en cuatro grupos :

- Redes privadas
- Redes públicas
- Redes de valor agregado
- Redes locales (LAN - Local Area Networks)

Las tres primeras son redes de área amplia (es decir, que pueden cubrir grandes distancias y que usan dispositivos de transmisión de datos para la comunicación; líneas telefónicas, canales de microondas, canales de comunicación por satélite o métodos similares). Las LAN transmiten los datos por cable coaxial, cables de fibras ópticas o por otros medios similares y la distancia que pueden cubrir es limitada por lo general las redes de esta naturaleza no superan los tres kilómetros).

A continuación se incluye una breve descripción de cada tipo de red :

1) Redes privadas

Las redes privadas (también denominadas líneas arrendadas o exclusivas) son dispositivos de transmisión obtenidos de un transportador común para uso exclusivo de la organización que las arrienda. Los transportadores son organizaciones autorizadas y controladas que suministran servicios de transmisión a terceros.

En una red privada, el sistema computadorizado de una organización está conectado directamente al transportador para la transmisión de datos, no siendo necesario discar para conectarse con las instalaciones del transportador. Además de líneas telefónicas, también suelen utilizarse instalaciones de microondas y satélite. La ventaja de la red privada es que la conexión siempre está disponible y que los datos pueden ser transmitidos en cualquier momento sin necesidad de esperar a establecer una conexión. En contraste, en una red de conmutador (discado), la conexión se establece cada vez que se requiere una transferencia de datos y además, la demanda para el uso de la red puede hacer imposible que se obtenga la conexión cuando se la necesita.

Las principales ventajas de las redes privadas respecto de las líneas públicas son :

- Las redes privadas generalmente permiten transmitir un mayor volumen de datos.
- Habitualmente, el usuario puede especificar las características de la línea que necesita para asegurar la calidad de la transmisión lo cual reduce los errores en los mensajes y aumenta la eficiencia.

Sin embargo, las redes privadas son generalmente más costosas.

Debido a que Ja conexión a la red no se efectúa a través de un dispositivo de discado, por lo general, resulta más difícil que terceros logren acceder a una red privada que a una red con computador. Sin embargo, son vulnerables a ser interceptas - as por dispositivos electrónicos, porque las líneas a través de las cuales se hacen las transmisiones son siempre las mismas y suelen estar claramente identificadas en el computador de la organización. En contraste, en una red de computador público o de discado directo, las líneas utilizadas varían. La comunicación de datos en base a la tecnología de transmisión por microondas o por satélite es particularmente vulnerable a la intercepción electrónica (eavesdropping). Si bien la posibilidad de interferencia no representa un riesgo de auditoría, el riesgo para el negocio puede ser significativo. Por tal razón, la gerencia debe considerar el uso de técnicas de codificación en los casos en que se transmita información sensitiva a través de una red de transmisión de datos.

2) Redes públicas

Estas redes emplean las instalaciones telefónicas públicas para la transmisión de los datos. Al utilizar este tipo de redes, se debe establecer una conexión por discado cada vez que desee llevarse a cabo una transmisión de datos entre dos puntos.

Este tipo de red suele ser la alternativa más eficiente cuando dos localidades deben intercambiar datos con poca frecuencia y no les afecta esperar hasta obtener una conexión. En algunas ocasiones, al intentar la conexión se obtiene una señal de ocupado, ya sea porque el otro punto está ya conectado con otro lugar o porque los circuitos de la red están sobrecargados. Otra desventaja de este tipo de red respecto de una red privada es que la calidad de la transmisión de datos es variable; en determinadas circunstancias la transmisión de datos se lleva a cabo con muy pocos o sin errores, mientras que en otras ocasiones pueden producirse un número importante de errores. Una de las razones de tal variabilidad puede ser el método de ruteo (una conexión entre dos puntos puede hacerse a través de rutas distintas cada vez y en algunas de éstas puede haber equipos que sean más propensos a errores que otros). Algunos equipos de transmisión son además muy sensibles a factores tales como los problemas meteorológicos (tormentas eléctricas, etc.), los que pueden originar errores de transmisión. Afortunadamente, existen técnicas de hardware y software efectivas para detectar y corregir errores en las líneas, con lo que se incremento la confiabilidad de las redes.

Las redes públicas son las más vulnerables a los accesos no autorizados. Cualquier persona que tenga a su disposición una terminal o un microcomputador equipado con los dispositivos de comunicación apropiados y el número de teléfono de un sistema de computación con facilidades de acceso por discado de "auto-respuesta" (es decir, que no se necesita de la intervención manual de un operador para conectar la llamada), puede llamar al computador. Dependiendo de los privilegios asignados al dispositivo al que accede el usuario no autorizado, éste puede acceder a funciones a nivel de sistema y/o aplicación. Es más, los microcomputadores pueden ser programados para intentar ingresar a un sistema protegido por contraseñas llamando reiteradamente al computador y probando una clave de acceso distinta cada vez,

El riesgo de acceso no autorizado puede ser reducido mediante la implantación de dispositivos de retro-discado. A la persona que accede al sistema por una red de computador público se le requiere su desconexión después del contacto inicial. El computador llama a la persona utilizando el número telefónico autorizado para la identificación del usuario/contraseña utilizada para hacer el contacto inicial. Sin embargo, la efectividad de este control puede ser reducida mediante técnicas como "transferencia de

llamadas" (cail forwarding), por la cual el computador llama a la persona al número autorizado pero la llamada es automáticamente transferida a un número no autorizado.

3) Redes de valor agregado

Las redes de valor agregado (VAN - Value Added Networks) son instalaciones públicas que se comparten de igual manera que las redes telefónicas, pero que sólo se utilizan para la transmisión de datos. Se las denomina de "valor agregado" debido a que las organizaciones que operan redes de este tipo obtienen las funciones básicas de transmisión de datos de otras organizaciones, les agregan valor (por ej.: proveen los computadores que interconectan la red) y luego revenden el servicio a sus clientes. Otro valor agregado es el servicio de detección y corrección automática de los errores de transmisión.

Hay dos clases de VAN. Una de ellas utiliza técnicas de transmisión en paquetes (packet switching) para transmitir los datos y la otra de transmisión por circuitos (circuit switching). En el primer tipo de red (la más habitual) los datos son enviados, a través de instalaciones telefónicas con conexión por discado, a una instalación local de la VAN. Esta separa los datos en "paquetes" de longitud fija (por lo general de 128 caracteres) y los transmite a alta velocidad hacia la instalación de la red más cercana al destino final de los datos. Los datos son reensamblados y transmitidos a destino, generalmente a través de una línea arrendada.

Debido a que los "paquetes" de distintos mensajes pueden ser entremezclados, y que los mensajes cortos (tales como transacciones) no necesitan esperar hasta que se completen mensajes largos (tales como trabajos o archivos), la segmentación de los mensajes en paquetes permite un uso bastante eficiente de las conexiones de la red. La red asegura que los datos son entregados en el destino correcto y que cualquier error de transmisión o problema que se presente es corregido o solucionado. La correcta entrega de los datos en cada destino es responsabilidad del operador de la red.

Las redes de transmisión por circuitos son muy similares a las redes públicas, con la diferencia de que sólo se las utiliza para la transmisión de datos. Estas redes proporcionan una conexión exclusiva durante la transmisión, sin compartirla con los demás usuarios de la red. Cuando finaliza la transferencia de los datos, uno de los participantes debe cortar la conexión mediante una notificación a la red VAN.

Ambas clases de VAN tienen distintas capacidades y ventajas. La transmisión en paquetes es una forma eficiente y de bajo costo para transmisiones de cantidades pequeñas de datos (por ej.: transacciones y respuestas) entre una gran cantidad de puntos receptores, en especial si el diagrama de conexiones entre éstos varía con frecuencia y es difícil de predecir, Por lo general, no son una buena alternativa para el envío de grandes volúmenes

de datos, en especial si los puntos receptores intercambian a su vez datos interactivos, tales como transacciones, La transmisión por circuitos, por el contrario, puede ser costosa cuando se usa para enviar transacciones y respuestas, a menos que ello ocurra continuamente y se necesite de un circuito exclusivo. (En tal caso, una red privada es usualmente la alternativa más conveniente). Establecer un circuito toma tiempo y el operador de la VAN usualmente efectúa un cargo cada vez que se establece y desconecta el circuito. Asimismo, el operador de la red usualmente efectúa un cargo por el tiempo durante el cual el circuito está en operación, por lo que puede ser bastante costoso mantener el circuito abierto cuando no se están transmitiendo datos, La transmisión por circuitos es muy apropiada para la transferencia de archivos, trabajos u otros flujos importantes de datos, ya que el costo de establecer el circuito para cada transmisión está justificado.

4) Redes locales (LAN)

Una red local (LAN - Local Area Network) es una instalación de comunicación utilizada por una organización para conectar entre sí dispositivos cercanos, tales como computadores, terminales y equipos de procesamiento de texto. Por lo general, estas redes están localizadas en su totalidad dentro de un edificio, aunque también se las utiliza para conectar dispositivos ubicados dentro de un complejo de edificios. La mayor parte de los dispositivos están conectados por cables coaxiales o de fibras ópticas, que permiten altas velocidades de transmisión y brindan una gran confiabilidad. Las LAN posibilitan el uso compartido de los datos entre los computadores de la organización y, asimismo, permiten compartir el uso de equipos periféricos de alto costo.

De todas las redes, la LAN es la que generalmente presenta menor riesgo de accesos no autorizados por terceros ajenos a la organización y de errores de transmisión. Sin embargo, en muchas redes locales se pueden interceptar las comunicaciones desde estaciones de trabajo que no son las del receptor autorizado. Además, como los archivos de datos son compartidos, son posibles los accesos no autorizados a los programas y archivos compartidos. Por ello, la gerencia debe analizar la conveniencia de usar técnicas de codificación y/o controles de seguridad de correo electrónico (empleando, por ejemplo, contraseñas) para proteger información sensitiva o confidencial durante la transmisión y el uso de controles de contraseñas para proteger archivos de datos y programas críticos.

Una vez que las redes de comunicación pasan a formar parte de los sistemas de información computadorizados de una organización, dichos sistemas se tornan vulnerables a los riesgos de accesos no autorizados y errores en la transmisión de mensajes. El grado de vulnerabilidad a los accesos no autorizados y la probabilidad de que se produzcan errores en los mensajes difieren según el tipo de red de comunicación que se utilice. La gerencia de

toda organización que use redes de comunicación de datos debe evaluar si son adecuados los controles de acceso, las técnicas de codificación y autenticación de datos, el hardware, el software y los demás procedimientos utilizados para identificar y corregir los errores que se pueden producir durante la transmisión de los mensajes.

CONCLUCION

El desarrollo de la informática a traído con sigo que mucho de los procesos manuales ahora Se hagan en forma automática lo que ha generado un nuevo escenario de trabajo para los auditores externos. Para hacer frente a éste cambio tecnológico en el mundo financiero, el auditor del presente debe estar capacitado para poder desarrollar un enfoque de auditoria que cubra todos los riesgos inherentes al procesamiento electrónico de datos para poder opinar acerca de la razonabilidad de los Estados Financieros; el cumplimiento de los principios de contabilidad generalmente aceptados y de la falta de uniformidad respecto del año anterior.

Los objetivos específicos de la Auditoria de Estados Financieros no cambian si la información contable es procesada manualmente o por computador. Sin embargo, los procedimientos de auditoría a través de los cuales se reúne la evidencia de auditoría necesaria pueden ser influenciados por el método de procesamiento de la información. El auditor puede usar procedimientos de auditoria manuales o técnicas de auditoria asistidas por computador y/o una combinación de ambos, para obtener suficiente y adecuada evidencia de auditoría. Sin embargo, en ciertos sistemas contables, por el particular uso del computador en el procesamiento de aplicaciones computarizadas contables significativas podría ser dificultoso o imposible para el auditor obtener información necesaria para su enfoque sin la asistencia del computador. En resumen, cuando los sistemas de información de significación para la Auditoria de Estados Financieros se procesan por un medio computarizado el auditor deberá llevar a cabo las pruebas necesarias para confirmar el razonable funcionamiento de esos sistemas computarizados.

BIBLIOGRAFIA

1. CARLOS A. SLOSSE, JUAN CARLOS GORI)ICZ, SILVIA P. GIORDANO, FEDERICO A. SERVIDO, DANIEL LOPEZ LADO, GUSTAVO F. DREISPIEL, CARLOS A. PACE/ DANIEL J. DE MARXO
   - "Auditoría un Nuevo Enfoque Empresarial"
   - Ediciones Macchi, Buenos Aires, 1990

2. PETER NORTONS
   - "Introducción a la Computación"
- McGraw-Hill México, 1995

3. OSCAR BARROS V.5 ANTONIO HOLGADO S. M., Y VICTOR PEREZ V.
   - Introducción a la Informática y los sistemas de Información administrativos.
   - Ediciones Universitarias, Santiago, 1987

4. OSCAR BARROS V., JOSÉ MANUEL ROBLES, PABLO SFRRA, ANDRÉS WEINTRAUB
   - REVISTA INGENERÍA DE SISTEMAS
   - Ediciones del Departamento de Ingeniería Industrial Universidad de Chile - Julio 1994