ALBERTO R. LARDENT
UNIVERSIDAD ARGENTINA DE LA EMPRESA

SISTEMAS DE INFORMACIÓN PARA LA GESTIÓN EMPRESARIA

Procedimientos, Seguridad y Auditoría

COPY.AR
Fotocopias - Impresiones - Anillados
French 414 - UTN - 1°Piso

CAPÍTULO 20

Auditoría de Sistemas de Información

INTRODUCCIÓN A LA FUNCIÓN DE AUDITORÍA

La primera consideración que deseamos introducir al tratar este tema consiste en aclarar que no debe conceptuarse, visualizarse ni aplicarse la Auditoría de Sistemas como una disciplina independiente de la Auditoría General. Por el contrario, la Auditoría de Sistemas de Información es una parte componente de la Auditoría General, y sus funciones integran el plan y los esfuerzos de la misma.

La Auditoría General comprende a la Auditoría Contable y a la Auditoría Operativa. El propósito de la Auditoría Contable es evaluar la exactitud de los estados o registros contables. El mismo se expresa por medio de un informe en el que se manifiesta que el examen ha sido realizado en conformidad con las normas de auditoría generalmente aceptadas, y que los estados financieros examinados responden a principios de contabilidad generalmente aceptados y aplicados de modo consistente a lo largo del tiempo. Una auditoría contable incluirá pruebas sustantivas[1].

Por lo general, estas auditorías son desarrolladas por auditores externos, por eso se la suele denominar "auditoría externa". Los auditores de sistemas de información participan en este tipo de auditoría aplicando procedimientos asistidos por computadora para respaldar a los auditores contables.

La Auditoría Operativa o Auditoría de Gestión tiene el propósito de evaluar la estructura de control interno en un área determinada. Mide y evalúa la eficacia de otros controles. Por lo general, son los auditores internos quienes las ejecutan, y el acento está puesto en los procesos. Se aplican técnicas de cumplimiento. La Auditoría de Sistemas de Información tiene naturaleza operativa (revisiones de controles de aplicaciones o de sistemas lógicos de seguridad).

El objetivo de la auditoría interna es ayudar a la gerencia a ejecutar sus funciones con efectividad. Este objetivo implica las siguientes actividades:

[1] Pruebas sustantivas son las que sirven de apoyo para sostener la adecuación de los controles existentes y para proteger a la organización de la actividad fraudulenta.

- Revisión o evaluación de la adecuación, profundidad y aplicación de los controles contables, financieros y otros operativos ejercitados a un costo razonable. En el cumplimiento de sus funciones, el auditor interno no tiene responsabilidad directa ni autoridad sobre las actividades examinadas. Por lo tanto, su apreciación no desliga de responsabilidad al resto del personal afectado por el examen.
- Determinación del cumplimiento de las políticas, planes y procedimientos establecidos. Las responsabilidades del auditor interno deben formar parte de las políticas corporativas.
- Verificación de la adecuada registración de los activos de la empresa y de su reguardo frente a pérdidas. El auditor interno debe estar autorizado al acceso de los registros de la empresa, de documentación y del personal.
- Recomendación de mejoramiento operativo.

La tarea de la auditoría interna exige una absoluta independencia de criterio por parte del auditor. Esta exigencia tiene una significativa repercusión con respecto a la preparación del auditor actual en el manejo de la tecnología informática, eje central de este capítulo. Esta independencia se logra por medio de la estructura organizacional y de la objetividad. La organización debe estar estructurada de tal manera que la función de auditoría interna dependa de un funcionario que posea suficiente autoridad como para tomar acción sobre el personal de línea, frente a recomendaciones o hallazgos del auditor. La objetividad se manifiesta mediante la imposibilidad de que el auditor se involucre en el desarrollo e instalación de procedimientos que deberán luego ser motivo de examen y revisión por el mismo implementador. No obstante, se discutirá más adelante, en este texto, la necesidad de participación del auditor en la determinación de aquellos puntos de control que deben estar incorporados en todo sistema de información y que, desde luego, deben ser definidos al igual que las pistas de auditoría en los momentos de desarrollo del sistema.

Una auditoría global comprende tanto aspectos de auditoría contable como operativa. El planeamiento de una auditoría global debe combinar acciones de auditoría de sistemas de información como acciones de auditoría contable y operativa.

En la etapa de planificación de la Auditoría General deberá establecerse la relación entre la actividad de los auditores externos y la de los internos. Aunque los externos han de presentar una visión independiente de la empresa, es probable que quieran evitar duplicaciones inútiles de esfuerzos y desperdiciar recursos. La coordinación de ambos grupos puede alcanzar una cobertura de auditoría más completa. Los planes de auditoría tendrán en consideración la calidad de los controles de los sistemas de aplicación y los organizativos y de procedimientos que se hayan examinado en revisiones anteriores. Si los controles y procedimientos son buenos, se hará más hincapié en las pruebas de cumplimiento. Si por el contrario, la percepción es que los controles son débiles o inexistentes, se insistirá más en las pruebas sustantivas.

IMPACTO DE LA TECNOLOGÍA INFORMÁTICA SOBRE LA AUDITORÍA

Las computadoras, y sus mecanismos asociados, han pasado a formar parte integrante de los sistemas contables y administrativos en la mayoría de las empresas, sin distinción ya de la dimensión de las mismas. El grado de automatización de la actividad contable variará de una situación a otra, pero es indudable que en la mayoría es considerable. Los controles, antes reservados a la responsabilidad de personas físicas, se han incorporado definitivamente a los sistemas mismos.

Al comenzar el siglo XXI, la globalización de la economía mundial y, en nuestro caso particular, la apertura de la economía argentina, generaron una creciente necesidad, en las empresas que operan en nuestro medio, de optimizar sus operaciones a fin de competir ventajosamente en el mercado local y mundial mediante diversas metodologías y estrategias de *management*, las cuales permitan lograr una utilización más eficaz y segura de la tecnología disponible. La aplicación de técnicas *just-in-time*, operaciones *on-line*, la utilización de bases de datos, los sistemas operativos avanzados, la incursión en Internet, la EFT, y otras tecnologías emergentes de la informática, tales como la orientación a objetos, las herramientas CASE (*Computer-Aided System Engineer*, Ingeniería de sistemas asistida por computadora), *total quality*, arquitectura "cliente/servidor", sistemas LAN (*Local Area Network*, Red de área local) y distribuidos, el procesamiento de imágenes y la multimedia, crean un desafío a las empresas y a los profesionales, quienes sólo podrán subsistir y competir a través de capacitación y aplicación de estrategias adecuadas.

La utilización de computadoras modifica la naturaleza del control de los datos con relación a las atareas de control de los procedimientos administrativos manuales. El procesamiento electrónico minimiza la participación de personas en la gestión administrativa, volviendo más difícil el cumplimiento del clásico principio de separación de funciones. Los programas de computación, aunque deben ser probados antes de su puesta en marcha en operaciones de ejecución normal, pueden contener errores u omitir la consideración de alguna condición de posible aparición. Por lo tanto, su revisión es imprescindible.

Un conjunto de programas puede procesar una actividad completa. Si los controles incorporados al sistema son completos y adecuados, el sistema computarizado puede resultar más seguro y confiable que un mecanismo de verificación manual. Por el contrario, si los controles automáticos son débiles o insuficientes, esto puede llevar a la empresa a que aplique esos sistemas a situaciones de riesgo de una magnitud impredecible

Si bien es fundamental la existencia de guías y principios relativos a la documentación y pistas de auditoría y controles para la construcción de sistemas, la calificación final de tales sistemas no será posible hasta que se efectúe una revisión independientemente de los resultados de los mismos.

Muchos sistemas han sido diseñados por especialistas en informática competentes, pero carentes de los conocimientos necesarios en prácticas y procedimientos contables. Por el contrario, aquellos entendidos en políticas y procedimientos organizacionales encuentran limitaciones en el ámbito de desarrollo de sistemas. La revisión independiente, actividad de la auditoría, es el proceso de comparar resultados producidos por el sistema con los requerimientos determinados en el sistema. Si bien esta actividad es conducida por profesionales que no participaron en la implementación u operación del sistema, es imprescindible para estos profesionales tener el conocimiento de cada uno de los pasos que integran el proceso. Este conocimiento puede ser adquirido únicamente por medio del análisis de la documentación; por eso la importancia que reviste una adecuada documentación de sistemas, a efectos de posteriores auditorías.

El enfoque de la Auditoría de Sistemas

Con respecto al concepto de Auditoría de Sistemas, el *Manual de Auditoría*[2] recoge el enfoque del dr. López Santiso (figura 20-1).

"La Auditoría de Sistemas ha sido definida como la revisión sistemática organizada de los sistemas en funcionamiento para ver si en ellos se verifican las propiedades de:

- Vigencia de los objetivos planteados como base del diseño original (entendiendo por diseño el arreglo o coordinación de las partes o detalles del sistema).
- Concordancia del sistema con los objetivos (efectividad).
- Permanencia del diseño por no haber sufrido alteraciones que lo degradaran operativamente.
- Eficiencia del sistema".

Figura 20-1. Definición de Auditoría de Sistemas.

Pero la Auditoría de Sistemas avanzó sobre otras aristas del desarrollo de sistemas, sobre las cuales nos referiremos más adelante.

Diversos factores han influido para que aquellos métodos de auditoría que fueron efectivos en ambientes no computarizados, dejaran de serlo en un entorno de procesamiento automatizado. Mencionaremos algunos de ellos:

- Procesos automatizados en vez de manuales: para una persona no entrenada, puede significar una dificultad la comprensión de la lógica de esta forma de procesamiento.
- Riesgos y controles: las amenazas contra la seguridad de los sistemas electrónicos son nuevas con relación a las que podrían preocupar en un ambiente de procesos manuales; por ende, los controles y medidas contrapuestos a esas amenazas son distintos de los tradicionales.
- Evidencias: el auditor necesita en su trabajo apoyarse sobre evidencias; las evidencias no son visibles al ojo humano cuando su continente es magnético o electrónico.
- Herramientas y técnicas: las utilizadas en procesos electrónicos son descriptas con una terminología de difícil comprensión para el no iniciado.

La Auditoría de Sistemas de Información concentra sus esfuerzos en los aspectos relacionados con el control de sistemas. Obviamente, la función de auditoría no se limita al segmento de procesamiento electrónico de datos de un sistema, debido a que abarca el entorno total de una aplicación desde el momento en que ocurre una transacción hasta que esta es registrada y produce un informe final. En consecuencia, la auditoría debe asegurar, con respecto a los sistemas, lo siguiente:

- La existencia de pistas de auditoría, de modo que las operaciones puedan ser rastreadas a través de todo el sistema.
- La existencia de controles adecuados con respecto a la entrada de datos y al mantenimiento de la integridad de los mismos, así como también de las transacciones que se efectúan con ellos a través del segmento computarizado del sistema.
- El manejo adecuado de las excepciones y de los rechazos originados por los controles de entrada de datos, y el aseguramiento de su incorporación al sistema en los casos que corresponda.
- El aseguramiento de que las políticas corporativas y el cumplimiento de reglamentos gubernamentales hayan sido incorporados al sistema.
- La verificación de que los sistemas se comporten conforme fueron definidos.
- El control de que las modificaciones que se operen sobre los sistemas sean debidamente autorizadas por el nivel jerárquico que corresponda.
- La existencia de condiciones y procedimientos de seguridad que protejan los datos de la organización
- El aseguramiento de la adecuada interconexión entre los diversos sistemas.

Para la ejecución de una Auditoría de Sistemas de Información se debe entender con claridad cómo los objetivos generales de auditoría se deben traducir en objetivos específicos de auditoría de sistemas. Por ejemplo, en una Auditoría Contable, un objetivo de control interno puede ser garantizar que las operaciones sean imputadas correctamente para mantener su correlación con la realidad; pero en la Auditoría de Sistemas de Información el objetivo se extendería hasta abarcar la seguridad de que las funciones de edición detectarán errores en la codificación de las transacciones.

Tendencias de la Auditoría de Sistemas: el auditor del futuro

Es sensato pensar que la evolución de los métodos y técnicas de auditoría de sistemas acompañará, paso a paso, la evolución del avance de la tecnología informática. Simultáneamente, la capacitación de auditores deberá orientarse en esa dirección. Es deseable que no se produzca una brecha significativa en el tiempo que signifique una demora prolongada en alcanzar el grado satisfactorio de capacitación por parte de los auditores.

Lo concreto es que, con el correr del tiempo, los auditores se encontrarán cada vez más involucrados en las operaciones del procesamiento electrónico de datos y en los resultados que

[2] *Manual de Auditoría*, Centro de Estudios Científicos y Técnicos (CECYT), Federación Argentina de Consejos Profesionales de Ciencias Económicas, pág. 42.

surgen de las mismas. Por otra parte, será cada vez más intensa la participación de los auditores especializados en el desarrollo de los pasos que integran al ciclo de vida de sistemas de información, particularmente en lo referente a inserción de puntos de control en los procesos que integran los sistemas.

Las tendencias en materia de Auditoría de Sistemas de Información se pueden sintetizar en los siguientes puntos:

- Se profundizará y generalizará la transferencia electrónica (y tal vez por otros medios que aparezcan en el futuro) de datos e información. La comunicación entre sectores remotos continuará extendiéndose, por cuanto la ciencia de la computación y la ciencia de las telecomunicaciones deberán aunar esfuerzos y conocimientos en procura de una integración que constituya una unidad conceptual (de hecho, el desarrollo de Internet y las aplicaciones derivadas de la red de redes ya han integrado buena parte de los elementos técnicos que convierte en realidad esta manifestación de tendencia).
- Los auditores deberán prestar especial atención al "fraude informático". El incremento en la utilización de tecnología sofisticada produce mayor necesidad de implantar controles más rigurosos y específicos.
- La difusión de las técnicas de computación promueven el entusiasmo de desarrollar sistemas de información de usuario final. Se asegura que no se trata de un fenómeno pasajero sino de una tendencia en constante crecimiento. Las razones deben buscarse en los beneficios que presenta la técnica de "aplicaciones desarrolladas por usuarios finales".
- Mayor productividad: surge del uso de nuevos lenguajes de programación (lenguajes de cuarta generación) y del desarrollo de prototipos como alternativa frente al método de ciclo de vida. Los lenguajes de cuarta generación permiten al usuario concretarse en la información que desean, en vez de cómo producirla.
- Mayor participación de los usuarios: cubren el tiempo que no disponen los analistas para atender las solicitudes de trabajos de computación.
- Los departamentos de informática estructurados con modernos criterios de organización cuentan con un Centro de Información para cómputo orientado al usuario final. Estos centros asesoran al usuario en la utilización de herramientas que procesan, recuperan o transmitan información. Estas nuevas técnicas y posibilidades producen la necesidad de que el auditor examine los riesgos potenciales que emergen de su aplicación, que pueden ser:
  - Utilización de un software no confiable.
  - Análisis incorrecto de requerimientos por falta de experiencia.
  - Aplicación de modelos inadecuados.
  - Uso de información desactualizada o incompleta.
  - Inexistencia o deficiencia de controles.
  - Concentración de información en un único sujeto. Ausencia de control por oposición.
  - Poca o ninguna documentación.
  - Falta de constancia de pruebas.

- El uso de microcomputadoras, en las áreas de usuarios finales que no están conectadas a una red local, pueden generar multiplicidad de archivos referidos a una misma entidad, que a su vez puede significar falta de homogeneidad en el tratamiento de una misma información.
- Se desarrollarán con más rigurosidad estándares de proceso en los equipos de computación, y la Gerencia deberá asegurar su utilización.
- Una gran cantidad de aplicaciones se adquirirá a terceras partes, incluyendo el software de auditoría.
- La alta gerencia aprobará la provisión de fondos para proyectos informáticos en la medida que estos ayuden al logro de ventajas competitivas en la organización que los desarrolle.
- Surgirán técnicas de auditoría más sofisticadas, permitiendo al auditor una utilización más frecuente de la computadora en sus procesos de revisión.

Para el futuro se pretende una completa integración entre la hoy denominada auditoría de procesamiento electrónico de datos y la auditoría financiera. El conocimiento del moderno procesamiento de datos y de los procedimientos avanzados en materia de seguridad, control y auditoría, deberá ser patrimonio del auditor y no del "especialista" en determinado tipo de auditoría.

Actualmente, es frecuente encontrar una fuerte separación entre grupos de auditores de computación, por un lado, y auditores tradicionales, aún denominados financieros u operativos, por el otro. Incluso, algunas importantes firmas consultoras en auditoría y organización mantienen esta separación de especialidades. Los auditores "financieros" u "operativos" tradicionales no han logrado, en algunos casos, alcanzar el nivel de conocimientos y habilidad necesarios para comprender el modelo operativo en un ambiente moderno de administración por computación.

Sin embargo, la proliferación de microcomputadoras en oficinas, la computación de usuario final y la aplicación de prototipos en el desarrollo habitual del trabajo administrativo y contable, hacen difícil auditar en forma separada los aspectos de procesamiento manual o de decisión humana y los aspectos automatizados de un mismo sistema de aplicación. Además, esta separación de roles limita la capacidad de desarrollar un programa integral de auditoría utilizando técnicas de avanzada y a un costo razonable. Lo ideal sería que un mismo auditor pueda evaluar los controles aplicados en el procesamiento electrónico de datos junto con la aplicación de los procedimientos tradicionales de auditoría financiera/operativa. Recordemos que lo que cambia son las herramientas y la tecnología, no los objetivos básicos de control.

El enfoque anterior es una reflexión que mira hacia el futuro. No obstante, el debate está abierto debido a que existen diferentes alternativas con relación al tema, en virtud de la existencia de ventajas y desventajas acerca de la integración de las funciones de auditoría. Entre las ventajas de la integración se mencionan las siguientes:

1. El avance acelerado de la tecnología informática no afectó solamente a los procesos administrativo-contables sino que puso en manos de los auditores la posibilidad de utilizar herramientas (la computadora, las telecomunicaciones, el software adecuado) que le permitirán mejorar la productividad y calidad de sus funciones de revisión. Es decir, la actividad de auditoría debería avanzar tecnológicamente en paralelo con el desarrollo de

los procesos por ella controlados. En este sentido, la auditoría transforma sus actividades en tareas que profundizan cada vez más su automatización: la auditoría asistida por computadora facilita y agiliza los procesos de prueba y revisión de aplicaciones, como también la generación de papeles de trabajo y documentación, propia de la actividad de "auditar". Mediante el uso de estas herramientas y de nueva tecnología, los auditores tradicionales ingresan en el ambiente de computación y, paralelamente, los auditores especializados en procesamiento electrónico de información incrementan sus habilidades al interpretar las técnicas de los auditores financieros.

2. El incremento en la utilización de computación de usuario final vuelve difícil separar las funciones operativas o financieras de los aspectos vinculados con procesamiento electrónico de esa misma información.
3. La aplicación de tecnologías informáticas modernas provoca el cambio de la naturaleza de la evidencia de auditoría. Existe una tendencia en las organizaciones a eliminar (o disminuir) el uso de papeles como medio de documentación. Esto obliga al auditor a comprender qué controles incorporados a los sistemas avanzados reemplazan a los tradicionales, asentados en papeles. La integración de técnicas parecería ser la estrategia más conveniente.

A pesar de las ventajas señaladas en el comentario anterior, debemos reconocer los argumentos de quienes no coinciden con el enfoque de integración. Entre estos argumentos podemos rescatar los siguientes:

1. Existe una marcada diferenciación entre la formación profesional de las disciplinas correspondientes a las ciencias económicas y las específicas de tecnología informática. Se trata de una diferenciación cultural que se traduce en la distinta manera de capacitación y entrenamiento que suministran las instituciones culturales proveedoras de educación. En la Argentina, algunos planes de estudio de nivel terciario que han sido modernizados incluyen un propósito de integración de técnicas de auditoría mediante asignaturas específicas. Tales son, por ejemplo "Auditoría de Sistemas". Este enfoque es muy reciente y, por el momento, los profesionales deben efectuar un esfuerzo adicional en sus estudios de grado para adquirir conocimientos que les permitan satisfacer las exigencias modernas de la profesión. Es importante destacar, en este sentido, la importancia de la participación de los Consejos Profesionales y Colegios de Graduados en el ofrecimiento de cursos, seminarios y talleres de trabajo de indudable beneficio para los profesionales, frente a la necesidad de complementar la capacitación.
2. Dentro del enfoque de la integración, el auditor generalista invertiría mucho tiempo en alcanzar una capacitación y entrenamiento adecuado en ciertos aspectos específicos y complejos de la disciplina informática, como pueden ser, por ejemplo, el tema de las telecomunicaciones, la administración de base de datos, o la revisión del funcionamiento de un sistema operativo. En estos casos, el auditor suele recurrir a la experiencia de un especialista ya entrenado para que lo apoye en el momento de emitir su opinión sobre la bondad de un sistema en particular o la calidad (razonabilidad) de determinados estados contables. (Queda latente la discusión, en este caso, del requerimiento de "independencia de criterio" –criterio personal– que se exige al auditor independiente).

El auditor de hoy debe reflexionar (más allá de la opinión del autor de este texto) acerca de la posibilidad de que en un futuro muy cercano se encuentre ante la necesidad de auditar un sistema de información que actúe en un ambiente de procesamiento distribuido con varios procesos clave, localizados en las áreas de los usuarios finales y utilizando lenguajes de cuarta generación.

Desde el punto de vista normativo, Estados Unidos de Norteamérica es uno de los países en donde se encuentra la mayor literatura referida a temas de auditoría de sistemas informáticos, y se ha observado una tendencia hacia una mayor integración entre las funciones de la auditoría financiera (en nuestro país la llamaríamos "externa") y las funciones de auditoría de computación. Hasta el año 1984 (y desde mediados de la década de 1970), los auditores externos cumplían sus funciones de revisión de control del procesamiento electrónico de datos observando lo establecido en la norma SAS Nº 3 (*Statement on Auditing Standards*) proveniente del AICPA (American Institute of Certified Public Accountants, Instituto Americano de Contadores Públicos), que se denomina "Efectos del procesamiento electrónico de datos sobre el examen del auditor y evaluación del control interno". De acuerdo con esta norma, los auditores externos debían ejercer la revisión de los sistemas contables, que incluían controles de procesamiento electrónico de datos sin tener la necesidad de responsabilizarse por estos controles. Esto provocó que algunas firmas de auditorías hicieran recaer la responsabilidad por la revisión de los controles del procesamiento electrónico de datos en otras personas especialistas en informática pero no en auditoría, o bien, en grupos de consultores especializados en computación.

En el año 1984, la norma Nº 3 fue reemplazada por la Nº 48 (SAS Nº 48), titulada "Efectos del procesamiento de computación sobre el examen de estados financieros". Esta norma exige a los auditores externos que consideren a los controles de procesamiento de datos como parte del entorno del control interno global. Esto significa que los objetivos específicos de auditoría no cambian más allá de que la información contable sea procesada manualmente o por computadora. La norma SAS Nº 48 establece que el auditor debe considerar si será necesaria, con respecto a un examen particular, la participación de un auditor especializado en computación que asesore sobre el flujo de datos en los procesos computarizados, y que además ayude en la formulación de procedimientos de control en las aplicaciones informáticas. No obstante esta posibilidad, la norma SAS Nº 48 establece que el auditor responsable de una tarea de auditoría debe tener suficiente conocimiento sobre computación, de modo que resulte hábil para:

- Comunicar los objetivos de la tarea a otros profesionales.
- Evaluar si los procedimientos específicos alcanzarán los objetivos del auditor.
- Evaluar los resultados de los procedimientos aplicados con relación a la naturaleza, momento y extensión de otros procedimientos de auditoría planeados.

Con relación a las funciones de auditoría interna, en Estados Unidos de Norteamérica, los auditores siguen las normas emanadas de sus organizaciones profesionales, principalmente del IIA (Institute of Internal Auditors, Instituto de Auditores Internos) y de la EDPAA (Electronic Data Processing Auditors Association, Asociación de Auditores de Procesamiento Electrónico de Datos). Las normas de IIA (Statements on Internal Auditing Standards) son generales, y se aplican tanto a la auditoría financiera/operativa como a la auditoría de computación. Sin embargo, este Instituto edita publicacio-

nes y dicta conferencias específicas para temas de auditoría de computación. Con respecto a EDPAA, ésta se orienta a promover la auditoría de computación como una disciplina de especialización.

En la Argentina, la Federación Argentina de Consejos Profesionales de Ciencias Económicas, a través del CECYT (Centro de Estudios Científicos y Técnicos), emitió el *Manual de Auditoría* (Informe Nº 5 del área auditoría), el cual constituye un cuerpo orgánico analítico cuyo propósito, manifestado en su prólogo, es servir como "guía práctica que facilite el examen de los estados contables" (de hecho ha logrado su propósito en razón de la calidad y profundidad de su contenido). Dicho Manual contiene en su capítulo 21 las "Pautas para el examen de estados contables en un contexto computarizado", donde se describe qué se entiende pro "ámbito computarizado", se comentan las formas y metodologías de evaluación de las actividades de control interno en ese ámbito y también la determinación de la naturaleza, alcance y oportunidad de los procedimientos a aplicar para la obtención de los elementos de juicio válidos y suficientes.

Este manual, especialmente a través de este capítulo, constituye una comprensión sobre la necesidad de actualización profesional en función del impacto de la computación en las actividades de control y, también, sobre su repercusión en el futuro.

IMPACTO DE LAS NUEVAS TECNOLOGÍAS SOBRE LA FUNCIÓN DE AUDITORÍA

Los conceptos básicos de control interno no han cambiado mucho a lo largo del tiempo. Sin embargo, el rápido avance de la tecnología obliga al auditor a reflexionar acerca de los modos de aplicar esos controles. Existen diversas tendencias que continuarán impactando sobre la tecnología del procesamiento de datos. Algunas son nuevas, mientras otras están en desarrollo y no han alcanzado aún difusión comercial. Una de esas nuevas tecnologías es la que se conoce como "inteligencia artificial". La misma es una nueva faceta de los sistemas de información, que intenta enseñar a la computadora a efectuar tareas de una manera que pudiera considerarse inteligente. La inteligencia artificial modificará la actividad rutinaria. Tendrá influencia sobre los métodos que utilizan los usuarios para interactuar con los sistemas de información. Es en la interfaz Usuarios y Sistemas de Información donde la inteligencia artificial será mejor aprovechada. Esto ocurrirá cuando una persona pueda enunciar un problema o un requerimiento en lenguaje común (lenguaje natural); entonces, por medio de la inteligencia artificial el sistema de computación puede decidir la solución o el curso de acción.

En la actualidad existen algunas aplicaciones de lenguaje natural. A medida que se incremente su utilización, el auditor se encontrará con situaciones a controlar muy diferentes de las actuales: verá desaparecer las evidencias documentadas (por medio del papel) a las que está acostumbrado. Por ejemplo, ¿qué evidencia encontrará en el caso de autorizaciones verbales dictadas a un sistema de información por medio de un micrófono incorporado a una terminal de computación? ¿Dónde quedan las pistas de auditoría?

Otra de las facetas de la inteligencia artificial está constituida por los denominados sistemas expertos. Se espera que la aplicación de los sistemas expertos afecte en el corto plazo la actividad de la auditoría. (*Véase* figura 20-2, pág. 263.)

Un sistema experto es un programa de computación que utiliza datos almacenados y reglas que, aplicadas, imitan el accionar de un experto humano. Un experto humano tiene, fundamentalmente, la capacidad para determinar la probabilidad de un resultado concreto en circunstancias rodeadas de un alto grado de incertidumbre. Esa capacidad está dada por condiciones de experiencia y criterio.

Figura 20-2. Descripción del concepto de sistema experto.

El fundamento de un sistema experto consiste en la posibilidad de capturar el conocimiento de un experto humano e introducirlo en un sistema de computación a fin de que otros usuarios puedan acceder a este sistema y aprovechar esa experiencia para la toma de decisiones basadas en las reglas almacenadas.

La figura 20-3 ilustra acerca de los componentes de un sistema experto.

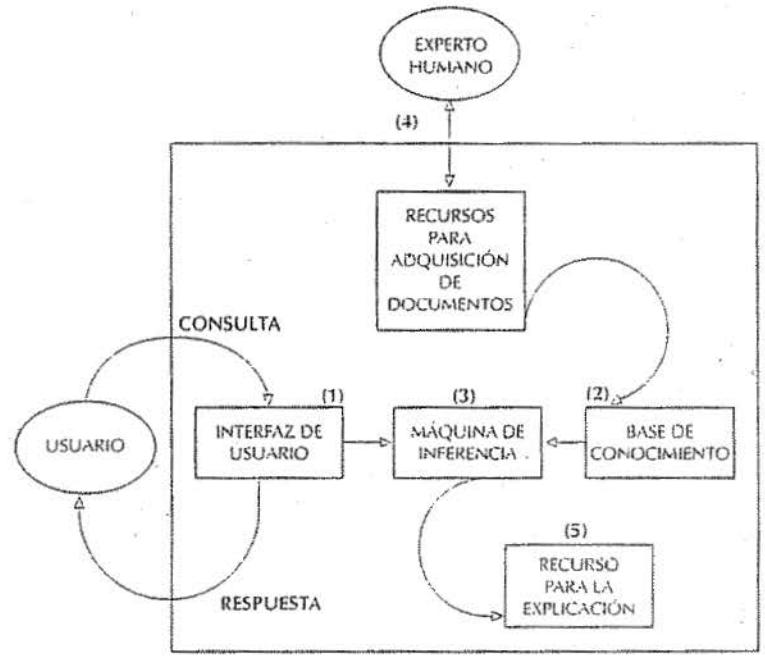

Figura 20-3. Componentes de un sistema experto.

Las referencias que explican el sentido del diagrama que se muestra en la figura 20-3 se indican a continuación.

1. Interfaz de usuario: este es el componente que permite la comunicación entre el usuario y el sistema.
2. Base de conocimiento: contiene información específica referente a un área de conocimiento. Esta información está integrada por datos y reglas que utilizan esos datos en la toma de una decisión. Ocupan un lugar de almacenamiento independiente de los métodos para el procesamiento del software. Los sistemas expertos pueden estar basados en reglas o en estructura. Cuando están basados en reglas, el conocimiento con respecto a una situación dada se presenta por medio de un conjunto de condiciones contra las que se confrontarán los hechos que están sometidos a una evaluación. Estas condiciones se presentan bajo los postulados *if-then* (si entonces), que son el medio por el cual se construye la base de conocimiento. El auditor puede emplear este tipo de reglas para obtener conclusiones sobre una determinada situación bajo examen. Un ejemplo sencillo de aplicación es el siguiente:

   Si el auditor debe evaluar las condiciones de seguridad física de un Centro de Cómputos de gran dimensión, un conjunto limitado de reglas será:

   - Si el equipo de computación se encuentra ubicado en un recinto cerrado.
   - Si dicho recinto contiene aberturas provistas de sistemas de bloqueo de accesos adecuados.
   - Si el local está provisto del sistema detector de fuego.
   - Si el local se encuentra sobre una plataforma que asegura la imposibilidad de ser afectado por inundación.
   - Si sólo el personal autorizado puede desbloquear el acceso.
   - Entonces, es razonable concluir que el equipo de computación se encuentra razonablemente protegido en cuanto a seguridad física.

   Los sistemas expertos también pueden estar basados en estructuras. Cada estructura constituye una red de nodos, donde cada nodo incluye datos y procedimientos para procesar datos. Los nodos superiores de la estructura representan los conceptos generales, y los de la parte inferior se refieren a partes específicas de esos conceptos. Existe una relación de jerarquía en el sentido de que, durante un proceso, se consideran en primer lugar las condiciones más importantes.
3. Máquinas de inferencia: "inferir" significa "deducir una cosa de otra". "Inferencia" es el paso de una proposición a otra, llamada "conclusión". Las máquinas de inferencia pueden desarrollar relaciones desde la base de conocimiento. Son programas de computación que consultan la base de conocimiento a efectos de estructurar una solución al requerimiento planteado.
4. Recursos de adquisición del conocimiento: la investigación procura encontrar herramientas que faciliten la labor del experto en el desarrollo o mantenimiento del sistema, para crear y mantener la base de conocimiento. Las personas "expertas" deben analizar la lógica de su proceso de decisión por medio de la heurística, es decir, mediante el arte de descubrir hechos valiéndose de hipótesis o principios que, aun no siendo verdaderos, estimulan la investigación.
5. Recurso para la explicación: el usuario final necesita conocer qué pasos se siguieron en el proceso de inferencia. Es decir, cuál fue la secuencia del razonamiento que se siguió para desarrollar una decisión o llegar a un resultado. La solución formulada podría no ser la adecuada si el razonamiento seguido por el sistema no es aplicable a las situaciones planteadas.

El auditor debe estar preparado para que en un futuro se encuentre ante la necesidad de efectuar revisiones de los controles de sistemas expertos. Deberá tener en cuenta que estos sistemas serán desarrollados e implementados con metodologías distintas de las aplicadas en los sistemas de información convencionales. Algunas situaciones podrán ser las siguientes:

- Se encontrará con reglas heurísticas (*if-then*) incorporadas a estos sistemas, que deberá comprender, interpretar, analizar y probar.
- Deberá considerar que, frente a una situación que debe resolver, puede haber más de una respuesta o resultado correcto.
- La metodología convencional para el desarrollo de sistemas de información comienza con la determinación de requerimientos concretos: en los sistemas expertos, las reglas de las bases de conocimiento se modifican, se agregan o se eliminan hasta que el sistema quede definitivamente ajustado. Lo mismo ocurre con las relaciones en la máquina de inferencia.
- En un sistema experto, las reglas aplicables conforme a la modalidad *if-then* se encuentran encadenadas: el auditor debe estar prevenido de que una pequeña modificación en una parte del sistema puede provocar resultados no esperados en cualquier otra parte del mismo.
- Una de las observaciones típicas de los auditores, en el análisis de sistemas convencionales, se refiere a los controles de acceso a datos y programas. Estos tipos de controles pueden no existir en el caso de sistemas expertos.
- Los métodos estándar que utilizan los auditores para probar y validar datos en los sistemas de procesamiento convencionales no son apropiados para su aplicación en sistemas expertos. Los resultados surgidos de la ejecución de sistemas expertos no pueden ser probados por comparación, es decir, confrontándolos con los surgidos por otro medio de ejecución.
- Cuando en el futuro se generalice el uso de sistemas expertos, existirá un riesgo adicional: no se debe esperar que estos sistemas siempre ofrezcan la mejor respuesta o solución a una consulta o problema, aunque sí lo harán en la mayoría de los casos. O sea, puede ocurrir que el usuario actúe en alguna situación guiado por una respuesta que no sea la correcta para esta situación. Debido a que por la modalidad de los sistemas expertos sus diseñadores y su usuarios introducen frecuentes cambios en los mismos, el auditor deberá verificar la ejecución de pruebas adecuadas cada vez que esos cambios se produzcan. Por otro lado, los sistemas expertos servirán como herramientas importantes para el futuro desarrollo de la función de auditoría. Podrán ser aplicados en determinadas áreas que requieran

alta especialización; por ejemplo, en la revisión de los controles de "*system programming*" (programación de sistemas). También podrán ser utilizados para evaluar el nivel de riesgo de auditoría asociado con decisiones de auditoría: servirán para ayudar al auditor a seleccionar aplicaciones que deberían ser auditadas prioritariamente dentro de un conjunto numeroso de sistemas.

En otro orden de ideas, la tendencia (y la realidad actual) muestra que las microcomputadoras van a ocupar varias de las funciones que tradicionalmente ejecutaban las *mainframes* (computadoras de porte grande). Ello se debe al aumento en la capacidad de memoria y del disco fijo, y al incremento del poder de los sistema operativos. Estas modificaciones en el hardware alterarán el futuro diseño de aplicaciones informáticas y la estructura de los departamentos de procesamiento de datos. En consecuencia, será necesario desarrollar un proceso de reingeniería de software para reemplazar versiones obsoletas de programas y encausarlas hacia las modalidades de la nueva configuración de equipos. El auditor deberá participar acompañando ese proceso de reingeniería, para verificar la actualización de la documentación para auditoría y el mantenimiento o modificación de los controles que formaban parte del sistema reemplazado.

Otro avance tecnológico trascendente lo constituye el procesamiento de imágenes. Esta técnica utiliza exploradores (lectores) ópticos (*scanners*) que pueden leer documentos tales como formularios e imágenes, y grabar su contenido en discos de tipo WORM (*Write Once/Read Many*, Escribir una vez/Leer muchas veces) (no se pueden regrabar). Esas imágenes o documentos pueden después ser recuperados, e incluso sus datos transportados a otra base de datos. Esta tecnología implica para el auditor un cambio, debido a que desaparecen los papeles y documentos que tradicionalmente formaban parte de las pistas de auditoría. El auditor del futuro deberá asegurarse de la existencia y aplicación de herramientas de software capaces de efectuar una rápida y confiable recuperación de la información almacenada en esas bases de datos, toda vez que sea necesario.

Hasta ahora las computadoras han trabajado de modo serial: esto significa que deben ejecutar una instrucción antes de ejecutar la siguiente. Los especialistas pronostican que las computadoras llegarán a efectuar procesos en paralelo (procesar varias instrucciones simultáneamente) que implicarán mayor productividad y capacidad para la resolución de problemas más complejos. Esta modificación del hardware generará cambios en los esquemas de programación y tendrá implicancias en la función del auditor en cuanto a disposición de evidencias y pruebas de auditoría.

EL CONTROL INTERNO

Entre las diversas definiciones que hemos analizado con relación al concepto de control interno, seleccionamos la que menciona Schuster[3], quien considera al control interno como un sistema (*véase* figura 20-4, pág. 267).

[3] Schuster, José A., *Control interno*, Ediciones Macchi, 1992, pág. 2.

"El sistema de control interno comprende el plan de organización y todos los métodos coordinados y medidas adoptadas dentro de una empresa con el fin de salvaguardar sus activos, verificar la confiabilidad y corrección de los datos contables, promover la eficiencia operativa y fomentar la adhesión a las políticas administrativas prescriptas."[3]

Figura 20-4. Descripción del concepto de control interno.

La evaluación de control interno es necesario para determinar el alcance de las pruebas a las cuales deben restringirse los procedimientos de auditoría.

En la definición señalada en la figura 20-4, están comprendidos los tipos de controles que constituyen los componentes de un sistema de control interno, que son los siguientes:

- Controles contables internos: conciernen a la salvaguardia de los activos y a la confiabilidad de los registros contables (confianza que requiere la información financiera). En un ambiente de procesamiento electrónico de información los controles contables son aquellos cuyo objeto consiste en asegurar que el procesamiento sea efectuado sin errores que no puedan ser detectados; por ejemplo, asegurar que la información de entrada sea correcta y que no haya pérdida u omisiones por falta de procesamiento de datos: que el programa emplee los archivos adecuados, que el procesamiento sea correcto y que la información de salida sea distribuida a las personas autorizadas para recibirla.
- Controles operativos: inherentes a las operaciones, funciones y actividades diarias. Garantizan que las operaciones satisfagan los objetivos del negocio.
- Controles administrativos: destinados a controlar la eficacia en un área funcional, el cumplimiento de las políticas gerenciales y su adhesión a las normas de la administración.

De las definiciones anteriores surgen los objetivos de control:

- Resguardo de activos.
- Cumplimiento de políticas corporativas y exigencias legales.
- Verificación de la exactitud e integridad de las transacciones.
- Aseguramiento de la confiabilidad de los procesos.
- Control de la eficacia y economía de las operaciones.

Un ejemplo aclarará las diferencias entre control interno contable y control interno administrativo. Un procedimiento de Compras Mayores exigirá cumplimentar determinada secuencia de pasos. Uno de esos pasos será "solicitar cotizaciones a cierto número de proveedores potenciales". La revisión de la forma en cuanto a cómo se cumplió con ese requisito apunta a determinar el grado de eficiencia aplicado en la operación. Se trata, en este caso, de un control de tipo administrativo que no apunta a verificar la corrección o no de los registros que sur-

jen de la operación. Por el contrario, un control interno contable verificará si se efectúa correctamente la registración de la entrada del material adquirido en el registro específico, y si se efectúan periódicamente recuentos físicos del material en depósito a efectos de su comparación con los mencionados registros. El control interno contable incluye también el análisis de eventuales diferencias de inventario y su correspondiente ajuste. No se ocupa de analizar la eficiencia de la gestión de Compra.

Los objetivos de control interno son válidos para todos los sistemas, cualquiera sea su grado de automatización. Sin embargo, en un ambiente computarizado se deben traducir los objetivos de control interno generales en procedimientos específicos de Auditoría de Sistemas de Información.

Algunos ejemplos de objetivos de control de información en un ambiente de procesamiento electrónico son los siguientes:

- Se mantiene control sobre accesos de datos incorrectos.
- La información se mantiene actualizada.
- Los datos de entrada rechazados por incorrectos o incompletos se informan al usuario y se verifica su destino final.
- Se mantienen copias de respaldo de los archivos de información a fin de lograr su recuperación en casos de desastre.
- Las modificaciones en los programas de computación de aplicaciones son aprobadas por la autoridad correspondiente y se efectúan las pruebas de calidad de los programas.

Todo sistema de control interno tiene limitaciones. Por eso puede brindar sólo una seguridad "razonable" en el logro de sus objetivos. Estas limitaciones surgen de las siguientes circunstancias:

- El control se ejerce principalmente hacia las operaciones repetitivas. Puede ocurrir que escapen de este control las excepciones.
- Ejercer control implica un costo. El control deberá encontrar su justificación en la medida en que su costo no supere el valor de aquello que se desea controlar. Por lo tanto, pueden quedar sin controlar aquellos hechos o cosas cuyo valor no justifique la aplicación de un sistema de control.
- Siempre estará latente la posibilidad de burlar el control que se apoya en la separación de funciones. Si se viola el control por oposición de intereses, porque dos o más personas que deben aplicarlo no lo cumplen, obviamente el control desaparece.

Las operaciones que realizan las organizaciones comerciales se conocen en la terminología como intercambios. Un intercambio es la operación por la cual una empresa entrega a un tercero, o recibe de él, un factor económico a cambio de otro factor económico contrapuesto. Un factor económico puede ser expresado en dinero, bienes, servicios, obligaciones, etc. Ejemplos de intercambios pueden ser la compra o venta de bienes de cambio o de

uso, contratación de servicios, cobranzas a clientes, pagos a proveedores, pago de remuneraciones, etcétera.

Para disponer de estados contables correctos, el procesamiento de datos contables debe capturar la totalidad de los intercambios y registrar sus atributos (fecha de formalización, partes intervinientes, identificación del bien o servicio, cantidad y precio) en forma exacta.

Los controles de captura de los datos asociados a los intercambios tienen una vital importancia para el sistema de control interno. Puede ocurrir como hipótesis de error que no se deje evidencia documental o magnética (en el futuro agregaríamos "óptica") de un intercambio producido (ausencia de rastro), o bien, que habiéndose registrado los atributos del intercambio, en un paso posterior del procesamiento contable, esa evidencia se pierda o modifique sin razón valedera.

Todo error no detectado, evitado o no corregido en la captura y procesamiento de datos inherentes a los atributos de los intercambios, implica un riesgo potencial de errores en la información contenida en los estados contables o en otro tipo de informe emitido por la organización. Por lo tanto, preocupa a la función de auditoría verificar que: los intercambios estén autorizados y registrados en el período contable correcto; que sean reales; que el activo recibido pertenezca realmente al ente receptor; que la otra parte del intercambio también sea la que corresponda; que se registre la operación por los pasivos; que sea correcta la especificación de la operación, lo mismo que la cantidad y precio.

Deben agregarse a las condiciones señaladas más arriba (existencia, exactitud, integridad, propiedad), las de valuación y exposición, ajustadas estas últimas también a las prescripciones de las normas contables.

En la Argentina, en la Tercera Convención Nacional de Auditores Internos, celebrada en 1982, se formularon normas relativas al alcance del trabajo del auditor interno, quienes atribuían una importancia sustancial a la confiabilidad en el sistema de información y de control interno. Dichas normas expresaban que es una función de auditoría interna efectuar el relevamiento y evaluación del sistema de control interno de la organización, a fin de determinar el nivel de efectividad del mismo en todas las etapas del proceso administrativo, produciendo su optimización a través de recomendaciones de los cambios necesarios.

Con relación a la tarea del auditor externo, la resolución técnica Nº 7 de la Federación Argentina de Consejos Profesionales de Ciencias Económicas, especifica que el profesional debe "obtener elementos de juicio válidos y suficientes que le permitan emitir su opinión o abstenerse de ella sobre los estados contables de un ente". Esos elementos de juicio válidos y suficientes deberán respaldar su informe mediante la evaluación de las actividades de control interno de los sistemas que son inherentes a su revisión (siempre que, con relación a su tarea, el auditor decida depositar su confianza en tales actividades, para determinar su naturaleza, alcance y oportunidad de las pruebas de auditoría a aplicar).

La referencia que se hace en el párrafo anterior al control interno es importante, porque ello significa que cuanto más efectivos sean los controles internos de una organización para cumplir sus objetivos, menor será el esfuerzo de realización de procedimientos sustantivos para asegurar la razonabilidad de los valores de los estados contables auditados.

Categorías de controles

Los controles se pueden clasificar en tres categorías:

DENOMINACIÓN	DESCRIPCIÓN	EJEMPLO
Preventivo	Diseñados para evitar que se produzca un error, omisión o acto doloso	Control de acceso lógico y aplicación de software de control de acceso en virtud del cual sólo personas autorizadas y desde lugares autorizados puedan acceder a archivos de información sensible.
Correctivo	Corrige errores, omisiones o actos maliciosos.	Software que asigna como valor por omisión (*default*) la fecha de corrida de la aplicación para el campo de fecha de un registro de entrada de datos, en el que la misma es errónea o está omitida.
De detección	Detectan que se ha producido un error, omisión o acto malicioso, e informan de su aparición.	Software de seguridad de acceso a través del cual quedan registradas intenciones de violación de acceso no autorizado.

Tipos de pruebas

En Auditoría se distinguen dos categorías de pruebas: las pruebas de cumplimiento y las pruebas sustantivas. El auditor de sistemas de información debe comprender las diferencias entre ambas.

Una prueba de cumplimiento tiene por objeto determinar si los controles se ajustan a las políticas y procedimientos de la organización, y si se aplican conforme a la descripción de la documentación de los programas de computación.

Es decir, intenta determinar si un control funciona efectivamente y si logra sus objetivos. Se diseñan pruebas de cumplimiento para reunir evidencias del funcionamiento efectivo de los controles internos generales y específicos. El diseño de estas pruebas debe contemplar estos objetivos:

- Que los procedimientos previstos fueron ejecutados.
- Que se ejecutaron adecuadamente.
- Que fueron ejecutados por alguien que cumple con los principios de separación de funciones.

Por ejemplo, una prueba de cumplimiento en el Departamento de Cuentas a Pagar, con respecto a la operación de Liquidación y Pago a Proveedores, abarcará:

a) Verificación de la existencia de la inicial del empleado de Cuentas a Pagar, quien es el responsable de verificar facturas de proveedores en las respectivas facturas.
b) Verificación de coincidencia de datos, comparados con los contenidos en la factura del proveedor y el remito correspondiente a la misma operación.
c) Verificación de la exactitud aritmética de los datos contenidos en la factura del proveedor.

Un ejemplo para el caso específico de sistemas de información es el siguiente: el auditor que desee verificar si los controles de la biblioteca de programas cumplen sus objetivos, deberá tomar una muestra de programas para determinar si las versiones fuente y objeto son iguales.

Las pruebas de cumplimiento se clasifican en pruebas de detalles y pruebas que emplean técnicas de indagación y observación.

Las pruebas de detalles requieren la revisión de documentos: por ejemplo, la verificación de la constancia de un control efectuado por el responsable con relación a los atributos (fecha, cantidad, precio, etc.) contenidos en un documento o soporte magnético,mediante la confrontación de esos atributos con los de otros documentos.

Una prueba de cumplimiento que emplee técnicas de indagación y observación puede aplicarse en el siguiente caso, que presentaremos a modo de ejemplo.

Supongamos una auditoría de un sistema de liquidación de jornales en el que los datos (legajo del trabajador, código de tarea, tiempo trabajado) ingresan desde una terminal. La auditoría consistiría en verificar la corrección e integridad de la liquidación. Las pruebas de cumplimiento, en este caso, radicarían en:

- Formular y aplicar un programa de computación con fines de auditoría que revise los archivos de datos e intente detectar errores que deberían haber sido descubiertos en las rutinas de edición.
- Indagar al personal responsable sobre qué acciones correctivas se toman en cuenta con respecto a situaciones de excepción que se detectan en el procesamiento habitual.
- Incorporar al sistema datos de situaciones simuladas con la intención de generar errores, y observar cómo reaccionan los programas rutinarios de edición.

Las pruebas sustantivas intentan verificar la adecuación de los controles existentes para proteger a la organización de actividades fraudulentas. Una Auditoría Contable aplicaría este tipo de pruebas para probar errores monetarios que puedan afectar los saldos de los estados contables. Una Auditoría de Sistemas de Información aplicaría una prueba sustantiva para determinar, por ejemplo, si el inventario de la biblioteca de cintas está registrado adecuadamente.

Áreas de la auditoría de sistemas de información

Los temas o aspectos que deben ser objeto de revisión por la auditoría de sistemas de información se pueden agrupar en los siguientes módulos:

I) Revisión de controles generales

Los controles generales se refieren a los que afectan a la estructura de la organización, a las políticas y procedimientos y al ambiente de control de los sistemas de información.

II) Revisión de las operaciones de procesamiento de información

Se refiere no sólo a las operaciones que se ejecutan dentro del denominado Centro de Procesamiento de Información, sino además a aquellas que se realicen en el entorno informático.

III) Revisión de seguridad

Abarca la revisión de la calidad del acceso lógico, del acceso físico y de los controles del ambiente informático.

IV) Revisión del software del sistema operativo

Se relaciona con la revisión de las políticas y procedimientos de desarrollo y con la adquisición y mantenimiento del software del sistema operativo.

V) Revisión de la metodología para el desarrollo de sistemas de información

Abarca la revisión de la metodología empleada, las normas y los procedimientos para el desarrollo, adquisición y mantenimiento del software dentro de ciclo de vida del desarrollo de sistemas u otras estrategias que se adopten (aplicación de prototipos, desarrollo a través de usuarios finales, etcétera).

VI) Revisión de los controles del software de aplicación

Comprende la revisión y evaluación de las fortalezas y debilidades de los puntos de control y procedimientos de control que deben permanecer insertos en los sistemas de aplicación de la organización.

VII) Plan de contingencias

Consiste en verificar la existencia y aplicación de políticas y procedimientos referentes a recuperación de información y continuidad de operaciones en caso de presentación de desastres.

Pasos para la ejecución de una auditoría de sistemas de información

La ejecución de una auditoría de este tipo exige el cumplimiento de diversos pasos. El cuadro de la figura 20-5 muestra su secuencia.

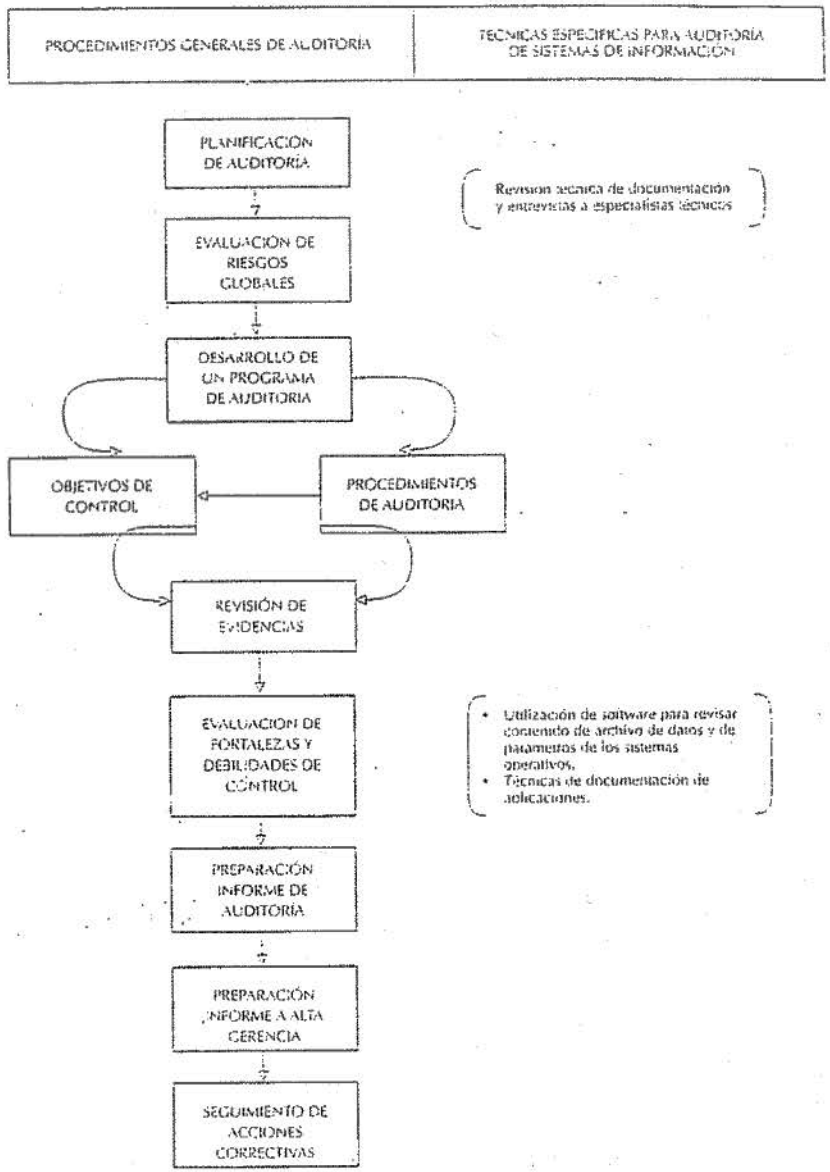

Figura 20-5. Desarrollo de una Auditoría de Sistemas de Información.

Planificación de la auditoría

Como ocurre con todo proyecto, el primer paso que debe integrar un proceso de Auditoría de Sistemas de Información es una planificación adecuada. Por supuesto que para que la planificación resulte adecuada debe conocerse con precisión el perfil de los objetivos que se persiguen con dicha auditoría y los objetivos de control.

Ya hemos explicado que los objetivos de control interno son válidos tanto para los sistemas manuales como para los computarizados. También explicamos que lo que puede diferir entre ambos tipos de sistemas son las funciones de control, y que por lo tanto el auditor de sistemas debe efectuar un proceso de conversión de objetivos de control interno a procedimientos específicos de auditoría de sistemas de información.

Debemos recordar que el marco dentro del cual el auditor debe planificar su actividad no se limita a la revisión de una aplicación que sea procesada por medio de la computación, sino que además abarca los controles operativos y administrativos del Centro de Procesamiento de Información y de su entorno, la seguridad de la infraestructura informática de los datos y programas, el resguardo de archivos, la protección de los objetivos y los demás ítems mencionados en esta sección.

Entre los aspectos que debe considerar el auditor de sistemas de información en el momento de la planificación, figuran los siguientes:

1. **Conocimiento del negocio y de su ambiente**

   Conocer el negocio significa saber qué es lo que se va a revisar y sobre qué se va a opinar. Si bien la utilización de la computación por parte de la organización que será auditada no afectará el alcance del conocimiento del negocio, en lo que se refiere a las políticas de registración y a la razonabilidad de los estados financieros, sin embargo sí puede afectar el alcance de los conocimientos del negocio relacionado con:

   - La identificación de posibles problemas relacionados con la obtención de evidencias de auditoría.
   - La identificación de posibles problemas del negocio relacionados con el procesamiento electrónico de datos.
   - La identificación de áreas que requieran personal con experiencia especial.

   El auditor de sistemas de información debe conocer también el ambiente normativo en el que opera el negocio. Por ejemplo, el entorno normativo no será el mismo con respecto a una institución financiera que con respecto a una organización comercial.

   La información relativa al conocimiento del negocio, relacionada con el procesamiento electrónico de datos, se obtiene recorriendo las instalaciones de la organización, manteniendo entrevistas con los gerentes usuarios de la información, con personal gerencial del Departamento de Sistemas y con gerentes claves del área Comercial, además de la lectura de informes financieros y de planes estratégicos a largo plazo y de todo el material que reúna antecedentes de la organización.

2. **Evidencia de auditoría y auditabilidad**

   La actividad de Auditoría de Sistemas de Información debe contar con la existencia de fuentes verificables de evidencia de auditoría, que son necesarias para probar los controles o para realizar procedimientos de pruebas de sustanciación.

   Pero pueden presentarse situaciones relacionadas con el procesamiento electrónico de la información que originen problemas de auditabilidad, los cuales deben considerarse al formular un plan de auditoría. Algunas de esas situaciones son las siguientes:

   - Entrada de datos sólo legibles por elementos de la máquina.
   - Información legible por la máquina que sólo se retiene por un período limitado.
   - Ausencia de documentos de entrada que dan comienzo al flujo de transacciones (existe mayor complicación cuando el procesamiento es en línea).
   - Controles de edición dentro de la computadora que no producen evidencia visible de auditoría.
   - Transacciones contables originadas por un proceso computarizado en el que no quedan evidencias en un documento o informe impreso.
   - Procesamientos internos efectuados por la computadora que involucran cálculos y desarrollos lógicos que no están bien documentados y no son bien explicados por el usuario.
   - Sistemas de computación que no presentan evidencias de que su puesta en marcha fue precedida de pruebas de programas y de controles sobre las conversiones de los archivos de datos.
   - Salidas con importes resumidos formados por la sumatoria de varios importes parciales, sin pistas visibles de auditoría que las relacionen con las transacciones individuales.

   Las revisiones relacionadas con la existencia de fuentes de evidencia deben llevarse a cabo para determinar:

   - Si las aplicaciones implementadas de sistemas de información afectan la disponibilidad y naturaleza de las fuentes de evidencia.
   - Si se han previsto los controles necesarios a incorporar en los nuevos sistemas que se encuentran en desarrollo, y lo mismo con respecto a los nuevos controles planeados para la conversión de los sistemas en vigencia.
   - Si se han planeado modificaciones a los sistemas de información vigentes.
   - Si se han planeado cambios de equipos o de programas.

FACTORES QUE AFECTAN LA COMPLEJIDAD DE UNA AUDITORÍA DE SISTEMAS DE INFORMACIÓN	
FACTORES	**CONDICIONES QUE IMPLICAN UN AUMENTO DE COMPLEJIDAD**
Objetivos de la auditoría de sistemas de información	Situaciones en que las expectativas respecto de los resultados de la autoridad exceden los requerimientos para detectar errores relevantes, tales como un análisis de la eficiencia del procedimiento de la información.
Evidencia de auditoría	La ausencia de salidas impresas con detalle de las transacciones o la falta de homogeneidad y frecuencia en la aplicación de controles.
Características de las aplicaciones de computación	Lógica de procesamiento compleja, incluso de fórmulas o cálculos no explicados con claridad, generación interna de datos que ingresan automáticamente sin evidencias a otra fase del proceso, datos que provienen de otras fases sin una clara determinación de su lógica de generación.
Confiabilidad en los controles	Ausencia o debilidad de los controles requeridos por los sistemas en cuanto a responsabilidad del usuario como a los que deberían estar incorporados a los sistemas.
Estabilidad de los sistemas de información	La ejecución frecuente de modificaciones a los sistemas en vigencia o introducción de nuevos.
Grado de complejidad de los recursos informáticos	Utilización de tecnología sofisticada (hardware y software).
Descentralización extendida	Transferencia de datos entre múltiples puntos. Falta de normalización de los procedimientos.
Técnicas de auditoría	Necesidad de aplicar técnicas de auditoría que incluyan el uso de la computadora.

Figura 20-6. Condiciones de complejidad en la auditoría de sistemas de información

Selección del área o aplicación a auditar

Al planificar una Auditoría de Sistemas de Información, el auditor se puede enfrentar ante la disyuntiva de tener que seleccionar o establecer prioridades con respecto a qué área de la auditoría, o cuál o cuáles aplicaciones comenzar a auditar. El auditor no puede auditar todos los sistemas al mismo tiempo. Se deben establecer criterios que faciliten ese ordenamiento. Algunos de esos criterios de selección se explican a continuación:

- Nivel de los activos controlados por el sistema

  Se refiere a la proporción de los activos totales controlados por la aplicación; por ejemplo, cuentas bancarias, inventarios, bienes de uso.

- Dimensión de la aplicación

  El tiempo de uso de la máquina, la magnitud de la entrada de datos a procesar y de la programación, son también factores a considerar.

- Impacto sobre la toma de decisiones

  Se relaciona con las decisiones que se basan en información suministrada por los sistemas. Debe considerarse también, dentro de la estructura organizacional, el nivel que ocupa el decisor que se apoya en esa información.

- Expectativa de vida de la aplicación

  En el caso de que en una aplicación se haya tomado la decisión de reemplazarla por otra a corto plazo, ello significará que la misma no estará contemplada prioritariamente en los planes de auditoría.

- Sensitividad de la información

  Se refiere fundamentalmente a datos de entrada, o bien, a salida de información que debe ser tratada confidencialmente. Es el caso, por ejemplo, de información gerencial o de mercadeo. En estas situaciones, la incidencia de la aplicación de este criterio incrementa las posibilidades de otorgar prioridad a la auditoría de esos procesamientos.

Riesgo y materialidad de auditoría

El concepto de riesgos de auditoría debe entenderse como la posibilidad de que la información financiera pueda contener errores materiales, o bien, que el auditor de sistemas de información pueda no detectar un error que ha ocurrido.

El término "material" se refiere a un error de carácter significativo desde el punto de vista de la auditoría. En una Auditoría Contable un error material es aquel que afecta a los estados contables en su conjunto. En una Auditoría de Sistemas de Información, la determinación de riesgo material depende del tamaño o importancia del ente auditado, como también de otros factores. Los riesgos de auditoría pueden clasificarse de la siguiente manera:

- Riesgo inherente

  Ocurre cuando un error se convierte en material (significativo); es decir, cuando se combina con otros errores encontrados durante la auditoría y no existen controles compensatorios relacionados.

– Riesgo de control

Se denomina así cuando un error material no puede ser evitado o detectado a tiempo por el sistema de control interno.

– Riesgo de detección

Es el riesgo que se corre cuando el auditor realiza pruebas exitosas a partir de un procedimiento de prueba inadecuado. Por lo tanto, se puede llegar a la conclusión de que aparentemente no existen errores materiales cuando en realidad los hay.

Es importante considerar la existencia de estos riesgos de auditoría en el momento de planificación. Un objetivo de auditoría de sistemas de información consiste en acortar el riesgo del área o aplicación que se someterá a revisión, de modo que el riesgo global se limite a un nivel bajo. La manera de minimizar este riesgo, es decir, la probabilidad de no detectarlo, es por medio de una muestra suficientemente grande o mediante la utilización de técnicas estadísticas adecuadas.

El concepto de materialidad es de más difícil comprensión para el auditor de sistemas de información que para el auditor contable. Este último basa su medición en términos monetarios. En cambio, el auditor de sistemas de información considera la materialidad en términos del impacto potencial para el conjunto de la organización. Por ejemplo, un error material puede consistir en el hecho de que un programador pueda acceder, sin autorización, a modificar la codificación de los programas de una aplicación.

PROCEDIMIENTOS DE CONTROL

Dentro de la actividad de Auditoría General se aplican los denominados **procedimientos generales de control**, que deben ser traducidos a **procedimientos particulares de control de sistemas de información** en el momento de la planificación de una auditoría. El cuadro de la figura 20-7 resume esta situación.

PROCEDIMIENTOS GENERALES DE CONTROL	PROCEDIMIENTOS DE CONTROL DE SISTEMAS DE INFORMACIÓN
• Para garantizar la adecuada autorización de transacciones y actividades. • Para la utilización de documentos y registros que garanticen la correcta registración de las transacciones. • Para salvaguardar el acceso a los activos e instalaciones.	• Para control de organización general. • Para acceso lógico y físico a datos y programas. • Para aplicación de metodologías para el desarrollo de sistemas. • Para las funciones del procesamiento de información. • Para el control de calidad del procesamiento de datos.

Figura 20-7. Interpretación de los procedimientos generales de control en procedimientos de control de sistemas de información.

CARTA DE AUDITORÍA

El trabajo de auditoría exige el pleno apoyo de los niveles más altos de la organización. El mismo se traduce mediante dos tipos de documentos, que en esta actividad se denominan "Carta Fundamental" y "Carta Fundamental del Proyecto". La Carta Fundamental define el grado de autoridad, el alcance y responsabilidad de la función de auditoría. La Carta Fundamental del Proyecto determina los objetivos de auditoría de cada área o aplicación a auditar. Incluye el cronograma de actividades, los recursos y áreas que abarca el trabajo e informes a formular.

DESARROLLO DEL PROGRAMA DE AUDITORÍA

Una vez finalizada la planificación, previa a la ejecución de la auditoría, quedará definido el tema y área a auditar, el objetivo de la auditoría, su alcance (uno o varios sistemas o un espacio de tiempo determinado), las habilidades técnicas y recursos necesarios y la identificación de las fuentes de información para ejecución de pruebas y revisiones. La figura 20-8 indica los siguientes pasos a desarrollar.

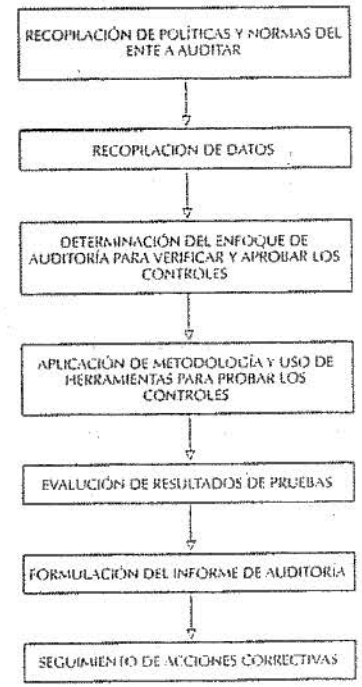

Figura 20-8. Desarrollo del programa de auditoría de sistemas de información.

La evidencia en auditoría

El concepto de "evidencia" es definido como el conjunto de información que ha reunido y que dispone el auditor de sistemas de información para determinar si el ente o los datos auditados han cumplido con los criterios u objetivos de auditoría. "Durante la realización de la auditoría, el auditor de sistemas de información ha de obtener evidencias que, por su naturaleza y suficiencia, respalden los hallazgos y conclusiones informadas"[4]. Las fuentes de la evidencia de auditoría pueden ser los resultados de las pruebas de auditoría efectuadas o de las entrevistas con responsables de área, la documentación examinada u observaciones propias del auditor.

La evidencia debe reunir condiciones de calidad y cantidad. La evidencia tiene características de calidad cuando es "competente", es decir, válida y relevante. Además, en materia de cantidad, la evidencia debe ser "suficiente", aspecto que se determina a través de un juicio de auditoría.

El auditor de sistemas de información debe considerar el grado de confiabilidad de las evidencias en que se apoya. Existen varios factores que influyen en la determinación del grado de confiabilidad:

- Evidencia de fuentes externas: cuando la evidencia proviene de fuentes externas a la organización se la considera más confiable que cuando es suministrada dentro de la organización. De ahí surge el proceso de circularización de saldos de clientes, al que recurren siempre los auditores externos.
- Objetividad de la evidencia: una evidencia objetiva será preferible a aquella que exige un juicio de valor.
- Calidad de la fuente de evidencia: la calificación de la evidencia de auditoría dependerá también de la confiabilidad de quien provee la información para formar evidencia.

Existen diversas técnicas para recopilación de evidencia de auditoría, algunas de las cuales se explican a continuación.

1. Revisión de estructuras organizacionales

   El auditor de sistemas de información debe verificar el cumplimiento de los criterios referidos a segregación de funciones dentro del esquema funcional del procesamiento de información.

2. Revisión de documentación de sistemas de información

   La documentación es un elemento fundamental para evitar malos entendidos, producir mejores sistemas de información y facilitar la auditoría. Lo que se documenta es el resultado de los pasos que integran la metodología del desarrollo de sistemas. Los usuarios documentan sus requerimientos y los diseñadores documentan el diseño de los procesos.

[4] Norma Nº 6 (*Exigencia de Evidencia*) de las Normas Generales de la EDPAF sobre Auditorías de Sistemas de Información.

   Toda organización debe contar con estándares de documentación. El auditor de sistemas deberá analizar las normas vigentes sobre este tema y estar en condiciones de verificar el cumplimiento de las mismas.

   Una documentación mínima deberá contener:

   - Instrumentos que avalen la autorización para desarrollar el proyecto (bajo requerimiento y condiciones preestablecidas).
   - Descripción del diseño funcional.
   - Registro de toda modificación al sistema y su autorización.
   - Documentación del usuario.

   El auditor moderno de sistemas de información debe estar preparado para encontrarse con nueva documentación –sin papeles–, distinta de la tradicional. Deberá tener habilidad para comprender especificaciones de bases de datos y analizar programas autodocumentados, al igual que conocer las aplicaciones de herramientas CASE y manejo de prototipos.

   Las tradicionales pistas de auditoría –basadas en documentos de papel– que los auditores financieros han utilizado para rastrear y validar transacciones se reducirán o eliminarán en los modernos sistemas de computación. En éstos, la nueva tecnología procesará las transacciones a través del procesamiento digital de imágenes, lo cual incrementará el uso de software de auditoría generalizado.

   Asimismo, el auditor moderno podrá encontrarse con sistemas que utilizan pistas de auditoría muy limitadas en un ambiente de microcomputación. Por ejemplo, el caso de ventas a través de representantes viajeros que ingresan sus pedidos desde microcomputadoras portables o *laptop* para su transmisión al procesador central.

3. Aplicación de técnicas de muestreo

   Las técnicas de muestreo se aplican para inferir las características de un universo, utilizando los resultados del examen de una porción del mismo, denominada muestra. Es decir, la muestra es una parte del universo, pero es útil en la medida en que sea fielmente representativa del mismo. El muestreo se aplica con el propósito de reducir el tiempo y el costo de una actividad de auditoría.

   El muestreo de auditoría puede ser estadístico o no estadístico. El muestreo estadístico es un método objetivo para determinar el tamaño de la muestra y los criterios de selección; permite evaluar el grado de precisión de la muestra y el nivel de confianza. Cada miembro del universo debe tener la misma oportunidad de ser escogido. En el muestreo no estadístico, el auditor debe aplicar su criterio para definir el método, el tamaño de la muestra y qué ítems se seleccionarán.

Técnicas de auditoría asistida por computadora

Con el propósito de cumplir con uno de los principales objetivos de la auditoría, como es el de obtener evidencias de la validez de la registración de las transacciones y evaluar la posibilidad de erro-

res potenciales, se han desarrollado técnicas de auditoría que se basan en la aplicación de métodos y programas que utilizan a la computadora para obtener evidencias por medio de los resultados de las pruebas que incluyen.

Tradicionalmente se han distinguido dos enfoques para el desarrollo de auditoría de sistemas de información:

a) Técnicas de auditoría alrededor de la computadora

Es la más antigua de las técnicas. Las formas que admiten estas técnicas son:

- Verificación de totales y de operaciones aritméticas: consiste en la revisión manual por parte del auditor de las mismas operaciones que, rutinariamente, efectúa en forma automática la computadora.
- Seguimiento manual de transacciones que procesa la computadora: para su desarrollo, el auditor selecciona algunos ítems reales de ingreso de datos y revisa los informes de salida para obtener evidencias de la corrección o no en el tratamiento de esas transacciones por los programas intervinientes.
- Revisión de código fuente: en este caso, el auditor debe tener conocimiento suficiente del lenguaje en que se desarrollaron los programas, como también saber interpretar los diagramas de flujo y la organización de archivos asociados con esos programas.

b) Técnicas de auditoría a través de la computadora

Estas técnicas comprenden tanto aquellas pruebas que se realizan en un solo momento, como las que surgen de los procedimientos de auditoría asistidos por computadora, como los procedimientos continuos de auditoría construidos dentro de una aplicación. Los procedimientos continuos son particularmente utilizados cuando existe un interés permanente en observar transacciones que puedan presentar condiciones de excepción en sistemas de cierta complejidad.

La aplicación de técnicas de auditoría asistida por computadora presenta algunas ventajas que se enuncian a continuación.

- El universo de aplicación es más amplio.
- Se detecta mayor cantidad de excepciones.
- Se logra mayor coherencia en el tratamiento de los ítems auditados.
- Se reduce el nivel de riesgo de auditoría.
- Se reduce el tiempo invertido en las revisiones.
- Se toma una muestra más amplia y mejor tratada.
- Se detectan con mayor facilidad las debilidades de control interno.
- Se obtienen más rápidamente los resultados de las pruebas.
- Se obtiene mejor documentación de evidencias.
- La auditoría es más objetiva.

Algunas de las técnicas de auditoría asistida por computadora son las siguientes:

- Programas específicos que verifican la integridad y corrección de cambios a programas.
- Generador de datos de prueba: facilita la creación de lotes de prueba para revisar la lógica de los programas de aplicación.
- Software generalizado de auditoría. Permite a los auditores ejecutar funciones de auditoría mediante la definición de parámetros de entrada. Estos parámetros constituyen entradas a los programas de auditoría que, en su momento, generarán programas objeto ejecutores de las funciones deseadas. Algunas de estas funciones son:
  - Análisis de archivos de datos.
  - Comparación de archivos.
  - Costeo, totalización (o subtotalización) de valores almacenados en archivos.
  - Selección de registros que contengan determinados atributos (ejemplo, pagos que superen determinados valores).
  - Validación de cálculos aritméticos.
  - Circularización de saldos de clientes.
  - Muestreo.

Las técnicas de auditoría asistida por computadora deben desarrollarse siguiendo los siguientes pasos:

1. Definir el objetivo de la prueba de auditoría

   Los objetivos pueden incluir:
   - Evaluación de controles automáticos.
   - Suministro de asesoramiento a los auditores financieros en la evaluación y certificación de estados contables.
   - Revisión y evaluación del diseño de sistemas y programas con respecto a controles, pistas de auditoría y eficiencia.
   - Determinación del grado de cumplimiento de las políticas corporativas.
   - Suministro de pruebas sustantivas sobre los detalles de las transacciones.
   - Establecimiento de la confiabilidad de los datos.
   - Detección de fraude informático.

2. Analizar los elementos de la aplicación que se intenta auditar: diagramas de flujo, organización de archivos; y seleccionar los datos adecuados para la ejecución de pruebas.

3. Diseñar la lógica general del programa de revisión y el formato de los informes de salida.

4. Codificar el programa de revisión y preparar las pruebas sobre un universo reducido de datos. Los resultados deben ser analizados desde el punto de vista de la corrección del procesamiento y del cumplimiento de los objetivos de auditoría.

5. Ejecutar la auditoría asistida por computadora. Este paso requiere una estrecha cooperación entre el auditor y el personal encargado de operaciones de computación, a fin de coordinar la forma y el momento de acceso a los archivos de datos. Debe preverse que ese acceso sea de lectura solamente (*read-only*) y que el auditor trabaje sobre copias de los archivos de operaciones de modo de evitar que los datos de producción queden expuestos a manipulación no autorizada. Es importante recordar la necesidad de documentación del proceso de auditoría y de sus resultados (verificación de cumplimiento y de objetivos de auditoría).

Con respecto a la selección de las técnicas de auditoría aplicables a cada situación en particular, el auditor deberá considerar estos factores:

- Requerimientos de capacitación y conocimiento de lenguajes de programación y procesamiento de datos (complejidad de codificación y mantenimiento).
- Requisitos de instalación de la técnica.
- Tiempo disponible para finalizar la auditoría (si se encuentran problemas el tiempo puede prolongarse en exceso, ocupando espacios necesarios para la producción normal de información).
- Influencia del método de procesamiento: si el sistema utiliza entrada remota de datos y el auditor está asignado a la computadora central, no podrá examinar simultáneamente la terminal desde donde se envían los datos.
- Esfuerzo necesario para proveer de información a la técnica que se aplique.
- Flexibilidad para la adecuación a distintas situaciones.

Los informes de auditoría

El trabajo de auditoría debe concluir en un informe y en su posterior seguimiento, y también con los cursos de acción que debieran surgir como consecuencia de las recomendaciones contenidas en el informe.

Dicho informe debe reflejar las conclusiones a las cuales arribó el auditor luego de desarrollar su programa y recopilar las evidencias de auditoría.

El informe deberá contener una opinión (aunque luego veremos que pueden existir informes sin opinión). Por lo tanto, el auditor deberá evaluar la información recopilada y determinar las fortalezas y debilidades de la auditoría.

Para la determinación de debilidades puede utilizarse una planilla que constituya una matriz de control, en la que se registren, sobre el eje vertical, los errores que puedan presentarse y, sobre el horizontal, los controles a través de los cuales se pueden detectar o corregir esos errores.

La identificación de controles fuertes y controles débiles tiene importancia a causa de determinar la existencia de controles compensatorios y controles redundantes. Un control fuerte puede compensar un control débil: se tratan entonces de controles compensatorios. Si en una situación se presentaron dos controles fuertes para un mismo procedimiento, nos encontramos con que uno de ellos es redundante. Por ejemplo, si el auditor de sistemas detecta debilidades en el control de ingreso de transacciones a un proceso computarizado, pero simultáneamente existe un fuerte control en una revisión manual detallada de ese proceso, pueden llegar a compensarse las debilidades señaladas. Si por el contrario el auditor encontrase que el control de ingreso de transacciones es fuerte y además se efectúa una revisión manual, podría tratarse este último de un control redundante.

El auditor de sistemas de información deberá apelar a su juicio profesional en el momento de decidir cuáles de las evidencias detectadas incorporará en su informe de auditoría. Para ello evaluará el grado de materialidad de los hallazgos, teniendo en cuenta el nivel de la estructura empresaria que se verá afectado por las observaciones y recomendaciones.

Tal como se expresó al comienzo de esta sección, los informes de auditoría constituyen uno de los productos finales del trabajo del auditor de sistemas de información. Es el elemento de comunicación entre el auditor y la alta gerencia, como también, el elemento de transmisión de observaciones y recomendaciones.

Los informes de auditoría tienen, por lo general, una determinada estructura y un determinado contenido. La figura 20-9 muestra una propuesta de estructura de ese informe.

INFORME DE AUDITORÍA

I) **Introducción**
Debe incluir los objetivos de auditoría, el área o funciones abarcadas, el período que cubrió la revisión y el alcance o extensión de los procedimientos de auditoría utilizados.

II) **Descripción de hallazgos y formulación de recomendaciones**
Se incluirán las fuentes de las evidencias.

III) **Detalles de las acciones correctivas a desarrollar**

IV) **Expresión de la opinión del auditor sobre la situación encontrada**
Se refiere a la adecuación de los controles, grado de cumplimiento de los mismos y conclusión sobre los procedimientos que fueron sujetos a revisión. La opinión del auditor debe quedar respaldada en el informe a través de las evidencias recopiladas durante la ejecución de la revisión.

V) **Anexos**
Tienen el propósito de mencionar información más detallada a la que el lector podrá recurrir o no de acuerdo a su interés o predisposición. Se trata de detalles que podrán ser importantes, pero cuya inclusión en el texto principal puede provocar en el lector la desviación de su atención del tema básico hacia detalles secundarios. Cuando el informe incluye anexos en el texto del mismo deberá hacerse referencia a la información ampliatoria o aclaratoria.

Figura 20-9. Contenido de la estructura de un informe de auditoría de sistemas de información.

Cuando el informe es elaborado y presentado por un auditor independiente, existen cuatro posibilidades en cuanto a tipos de informes:

1. Informe sin salvedades
   Significa que la revisión de auditoría no encontró problemas materiales o controles débiles no compensados. En este caso, la opinión expresa que los estados contables de la empresa "están de acuerdo con principios de contabilidad generalmente aceptados".

2. Informe con salvedades
   En este tipo de informe, el auditor manifiesta que si bien los estados contables de la empresa cumplen con las normas de contabilidad generalmente aceptadas, se presenta alguna condición de excepción que debe ser expresamente expuesta. Esta condición debe tener una importancia relativa, de modo que signifique un riesgo para el resguardo patrimonial de la empresa.

3. Informe con opinión adversa
   Esta posibilidad no es de frecuente aparición, pero igualmente debe ser contemplada. Puede presentarse cuando los estados contables auditados fueron expuestos sin cumplir las normas contables generalmente aceptadas o cuando se han detectado debilidades significativas en los procedimientos de control.

4. Informe sin opinión
   Un informe sin opinión se emite en los casos en que el alcance de la auditoría es limitado o bien cuando la situación financiera de la organización auditada permite pensar en una posible disolución.
   En cuanto a la terminología empleada en los informes, debe tenerse en cuenta que los destinatarios no son expertos en técnicas avanzadas de computación, por lo que la misma deberá poder ser comprendida por ejecutivos de distinta naturaleza profesional, y solamente los anexos podrán contener detalles de desarrollo técnico.

CAPÍTULO 21

Auditoría de Organización y Administración del Ambiente Informático

INTRODUCCIÓN

El objetivo de este capítulo es examinar y evaluar las políticas, administración, estructura organizativa y aplicación de controles en un ambiente informático.

Entendemos por ambiente informático no sólo el correspondiente a un Departamento de Procesamiento de Información, sino también a todos aquellos sectores de la organización que estén asociados con aquél, ya sea porque son proveedores de datos a procesar o porque son usuarios de información procesada o que procesan información localmente y proveen de datos resumen al procesador central.

Las funciones específicas del auditor de sistemas de información, con respecto a este objetivo, deben incluir:

- Tener una comprensión precisa del ambiente informático de la organización por medio de la identificación de las áreas funcionales que procesan información; también, por sus asignaciones y responsabilidades.
- En función de esa comprensión, evaluar la estructura organizacional del ambiente informático y verificar su adecuación a las políticas institucionales.
- Evaluar el ambiente de control de la organización para verificar si se cumplen los objetivos de control que otorgan confiabilidad al procesamiento de información.
- Efectuar pruebas de controles y evaluar sus resultados.
- Detectar las debilidades que puedan existir desde el punto de vista de la gestión y del impacto que producen sobre los procedimientos de auditoría. Las debilidades serán una indicación de la necesidad de efectuar más esfuerzos de auditoría en ciertas áreas.

La auditoría de organización propone los siguientes propósitos:

- Verificar que la estructura organizativa asegure una adecuada separación de funciones para cumplir con principios de control interno.
- Asegurar la protección de archivos (de datos y de programas) para mantener la continuidad de las operaciones bajo condiciones normales de procesamiento.
- Verificar la presencia de un buen diseño de control interno a causa de acotar las deficiencias y riesgos de procesamiento.
- Verificar que se mantenga un control eficaz en los niveles de autorización de datos y de procedimientos.
- Examinar si existen estándares de actuación y evaluar su adecuación y vigencia.
- Examinar la documentación existente y evaluar su contenido y nivel de actualización.
- Analizar el nivel de formación del personal y evaluar si por medio del mismo se alcanzan los estándares diseñados.

Plan de organización

Un Sistema de Procesamiento de Información debe ser organizado y administrado con los mismos métodos que han demostrado su efectividad en otros segmentos de la organización. Debe existir un plan de organización y una clara asignación de responsabilidades. Para la administración de las operaciones debe haber documentación de los procedimientos y normas previstas con las cuales poder comparar los resultados.

Para establecer responsabilidades se deben preparar la descripción de trabajos a efectuar para todos los participantes en el procesamiento de información, e incluso para los usuarios y proveedores de datos.

En la mayoría de las organizaciones, la actividad de procesamiento de la información es particular en cuanto a la variedad de sus funciones, responsabilidades, aptitudes y características. Un plan de organización adecuado, con la consiguiente división de labores, es importante en razón de la concentración de la actividad de procesamiento de información en un reducido número de personas, menor del que requerirían esas actividades si fueran procesadas a través de métodos manuales. El menor número de participantes y el alto grado de automatización exponen al sistema a posibles manipulaciones y riesgos de fraudes, si una sola persona tiene tanto el conocimiento operacional como fácil acceso a los procedimientos y programas en todos los niveles.

Las responsabilidades y funciones básicas de un Departamento de Procesamiento de Información se prestan a un agrupamiento natural dentro de la organización. Reconocer estos grupos naturales, y proporcionar la correspondiente estructura organizacional, ayudan al logro de efectividad y control dentro de un departamento de esta naturaleza.

Las actividades de estos grupos funcionales se reconocen tradicionalmente como:

I) Funciones de proyectos.
II) Funciones de procesamiento de información (operaciones).

III) Funciones de servicios técnicos.
IV) Funciones de control.

A estas funciones tradicionales se agregan las recientemente surgidas como consecuencia del desarrollo tecnológico y del avance en la tecnología de telecomunicaciones. Es así como aparecen áreas de responsabilidad asociadas a la tecnología de Internet (Intranet y Extranet) y los centros de información o Infocentros que ayudan (asesoran, estos últimos) al desarrollo de sistemas por parte de usuarios finales, despejando la carga de trabajo (siempre abundante) de los analistas/programadores, que pueden dedicarse, así, al desarrollo de los grandes proyectos informáticos de carácter institucional.

Las funciones de proyectos comprenden las siguientes responsabilidades:

- Desarrollo de sistemas

  Es la más importante en cuanto a incidencia presupuestaria y atención de la Gerencia. Incluye el análisis de los sistemas existentes, la atención de los requerimientos de los usuarios y el diseño de nuevos o mejores métodos.

- Documentación

  Abarca la responsabilidad de crear y mantener manuales de procedimientos y ayudas a través de instrucciones incorporadas internamente en los programas de aplicación (que deben ser consultados a través de mensajes desplegados en pantalla).

- Análisis cuantitativos

  Consiste en aplicar técnicas de lógica y modelos matemáticos a las tareas apropiadas de las operaciones y planeamiento de la organización.

A diferencia de las actividades de procesamiento de información, las funciones relativas a proyectos de sistema son poco repetitivas. Estas últimas tienen una duración prolongada, y su repetición sólo se medirá en términos de meses, y no de días u horas. En consecuencia, sus resultados son menos visibles. No obstante, cuando se aplican técnicas de secuencia estructurada en las actividades de desarrollo de sistemas, es más factible obtener resultados intermedios visibles. La característica de las funciones de proyectos radica en que sirven de enlace entre los problemas del negocio y las soluciones informáticas.

Las funciones de procesamiento de información tienen características que pueden asimilarse a las que son comunes en una operación de fabricación. Entre ellas, las siguientes:

- Sin funciones altamente repetitivas.
- Pueden planificarse: definir su desarrollo en el tiempo.
- Las cargas de máquina son programables.
- Se aplican normas de instrucción para la ejecución de operaciones.
- Se aplican elementos de medición a las operaciones, de modo que se la compare con los estándares.

- Se ejerce estrecha supervisión sobre las operaciones repetitivas.
- Se utilizan equipos que requieren una inversión.
- Existe alta rotación de personal.

Las funciones básicas del procesamiento de información son las siguientes:

- Captura de datos: los datos surgen de documentos fuente provenientes de los Departamentos Usuarios, y se captan a través de digitación en teclado o bien directamente por medio de un lector de código de barras u otras formas modernas de captación. Los datos también pueden provenir de fuentes remotas e ingresarse a los archivos en procesamiento en línea.
- Operación de la computadora y de los equipos asociados: comprende el manejo de consola y equipos periféricos y auxiliares.
- Operaciones de biblioteca: consisten en el mantenimiento del almacenamiento y en la responsabilidad por la custodia de programas y datos.

La responsabilidad por la ejecución de estas operaciones se enfoca hacia:

- Obtención de productos (información) variados.
- Eficiencia y exactitud en la ejecución de las operaciones.
- Mantenimiento de calidad.
- Cumplimiento de los plazos de entrega comprometidos.

Las funciones de servicios técnicos requieren, por parte de quienes las ejercen, un cierto grado de especialización. Estas funciones asumen cada vez más una mayor importancia como consecuencia del avance de la tecnología informática y de la creciente dependencia del resto de la organización con respecto a la misma. Actualmente, se tiene una clara idea del impacto real y potencial de los servicios técnicos en el mejoramiento de la eficacia operativa y la reducción de costos.

La variedad de funciones técnicas o de apoyo incluyen:

- Análisis de configuración de equipo, incluyendo redes y técnicas de comunicación, a fin de comparar el existente en la organización con las propuestas que ofrecen constantemente los proveedores.
- Selección de los programas de operación y actualización de sus versiones.
- Desarrollo de normas aplicables para el desarrollo de proyectos y para el procesamiento de información.
- Mantenimiento del control de calidad con respecto al grupo de servicio técnico.
- Desarrollo de instrucciones de codificación.

- Administración de bases de datos.
- Administración de redes y enlaces.
- Mantenimiento de programas de aplicaciones en vigencia.
- Administración de seguridad.

Las funciones de control comienzan desde el momento en que los datos intentan ingresar en un proceso (se inicia la producción), y continúan a lo largo de los trabajos conforme avancen a través de la instalación. Además del control de entrada de los datos, los resultados intermedios y finales del procesamiento se asientan en registros cronológicos (*logs*) para comparar las cifras de control con los importes obtenidos de los datos procesados.

ADMINISTRACIÓN DEL PROCESAMIENTO DE INFORMACIÓN

Los principios de administración que se aplican a la administración en general son aplicables también al procesamiento de información. No obstante, en vista de la permanente evolución que ocurre en la tecnología informática, las técnicas para un control administrativo efectivo están también en permanente evolución. A medida que los gerentes y otros miembros de las organizaciones van familiarizándose con las modernas formas de procesamiento de la información, se han ido desarrollando técnicas efectivas de buena administración.

Los principios y las técnicas se han plasmado en los Manuales de sistema y procedimientos y, actualmente, también se han incorporado instrucciones de operaciones en los programas de aplicación, que pueden ser consultadas, a modo de ayuda o auxilio, a través de funciones que despliegan mensajes en pantalla.

El contenido de este cuerpo orgánico de normas abarca los siguientes tópicos:

a) Convencionalismos y procedimientos estándar de programación.
b) Procedimientos estándar de operación.
c) Procedimientos de control.
d) Organización y recursos humanos.

a) Los convencionalismos y procedimientos estándar comprenden la definición acerca de qué metodología se desarrollará con respecto a: la diagramación del análisis y diseño de sistemas de información; simbología a aplicar; tablas de decisiones; convencionalismos de codificación; integración del diccionario de datos; glosario estándar; prohibición de abreviaturas no estándar; desarrollo de técnicas estándar de programación (confección de rutinas para efectuar operaciones específicas de la computadora, comunes a varios programas); procedimientos de depuración de fallas de programas; ejecución de "pruebas de escritorio", para la comprobación de la ruta que siguen los datos a través del programa para verificar si su lógica es satisfactoria; especificaciones para documentación de programas y de sistemas.

b) Los procedimientos estándar de operación intentan asegurar que se empleen técnicas uniformes en todos los equipos de la instalación, estableciendo tiempos estándar para

los procesos, estándares para carga de programas, calendario de operaciones, definición de tiempo de retención de archivos, registros de tiempos de uso de la computadora (con indicación de la aplicación ejecutada), planes y procedimientos para emergencias.

c) Los procedimientos de control serán coherentes con los controles especificados en la documentación de cada aplicación. Incluirán las siguientes responsabilidades: registro de los datos de entrada, conciliación de datos de entrada con información de salida, cumplimiento del cronograma de operaciones, controles de acceso físico y lógico, verificación de corrección de errores.

d) Organización y recursos humanos: todos los técnicos intervinientes en el procesamiento de información deben conocer qué se espera de su intervención, cuál es su papel en el procesamiento de información y de qué manera será calificada su actuación. Generalmente, las tareas de procesamiento de información se ejecutan en etapas o pasos separados: el personal debe estar preparado para cubrir cada fase en el lapso asignado y así evitar demoras en el tiempo total del trabajo. Deben existir informes periódicos sobre el avance de las tareas. Los operadores deberán informar las razones de desviaciones en el plan de trabajo, si las hubiera. Al igual que en otro tipo de tareas productivas, debe aplicarse el criterio de rotación periódica de operadores a fin de evitar la permanente asignación de responsabilidad de una operación siempre a la misma persona.

Auditoría del ambiente de procesamiento de información

El ambiente de procesamiento de información puede calificarse como centralizado o descentralizado según sea la ubicación física de los elementos que lo componen y de las políticas y procedimientos que rijan sus operaciones.

El procesamiento centralizado se identifica por la presencia de una computadora central en la que se efectuarán operaciones de almacenamiento, procesamiento y actualización de datos que son transmitidos a terminales bobas (inhabilitadas para efectuar procesamiento) o recibidos desde ellas.

El ambiente de procesamiento descentralizado consiste en la existencia de varios centros de procesamiento de información locales que envían y reciben datos a través de conexiones vía módem. Este ambiente se apoya en una moderna tecnología de redes de telecomunicaciones que incluye redes de conmutación de datos, canales de microondas y satélites.

Desde el punto de vista de la Auditoría de Sistemas de Información, es importante destacar las diferencias que se presentan confrontando un ambiente con otro. Los controles organizativos y los que ejerce la gerencia están más concentrados en un ambiente centralizado: son más rigurosos: se nota más su presencia. En un ambiente descentralizado surgen riesgos que son consecuencia de controles que se hallan más dispersos. En este tipo de ambiente, donde no existe un único punto hacia el cual dirigir la atención, puede ocurrir que la Gerencia aplique criterios de tipo subjetivo que puedan llegar a ser inconsistentes entre los diversos centros de procesamiento.

En estos casos, la auditoría deberá analizar la existencia de políticas que deberían provenir de la más alta gerencia, y verificar si las mismas tienden a preservar la uniformidad en materia de aplicación de controles y su grado de cumplimiento. Además, en un ambiente descentralizado se puede mejorar el nivel de control si se centralizan ciertas funciones, tales como desarrollo de sistemas, control de calidad y administración de accesos.

El avance de la tecnología informática ha provocado, por un lado, la proliferación del uso de microcomputadoras y de LAN, y por el otro, el uso del software se encuentra cada vez más cerca del usuario. Estas circunstancias han dado origen a lo que se denominó "computación de usuario final". Esta técnica puede crear en el auditor la misma preocupación que la que surge de las aplicaciones en una computadora central. En consecuencia, la computación de usuario final debe ser formalizada en la organización. Debe evitarse que existan archivos paralelos sobre un mismo tema, cada uno en distintos departamentos, que pueden no coincidir entre sí con respecto al contenido de la operación, en razón de sus distintos momento de actualización. Un comité *ad hoc* decidirá sobre temas tales como:

- Políticas y normas referentes al cumplimiento de leyes de *copyright* y utilización no autorizada de datos y programas.
- Vinculación con el Centro de Procesamiento de Información. Se denomina *downloading* al proceso que consiste en el envío de datos desde una central a una PC (o terminal); el *uploading* es el proceso inverso. Esta integración entre computadora central y PC permite el diálogo entre distintos tipos de arquitecturas.
- Estudios de factibilidad para adquisición de hardware y software.
- Responsabilidad en la confección de programas.
- Técnicas de prueba y condiciones mínimas de documentación.
- Condiciones y técnicas de seguridad de datos y programas.

Otro tema que interesará al auditor de sistemas, con relación al ambiente de procesamiento de información, es el referido a telecomunicaciones y redes. El control en el área de telecomunicaciones constituye un factor crítico. En general, la responsabilidad por la definición de instalación y el monitoreo de las redes de telecomunicaciones corresponde al sector de programación de sistemas. Las redes permiten la comunicación y la posibilidad de compartir datos y recursos de computación con dos o más computadoras. Una LAN enlaza entre sí microcomputadoras localizadas dentro de un ambiente restringido. Cuando la comunicación conecta redes remotas constituye una red de área amplia (WAN, *Wide Area Network*, Red de área amplia).

El auditor de sistemas verificará la aplicación, en la organización, de un software de seguridad que controle el acceso a los sistemas a través de contraseñas y tablas de autorización. Este software de seguridad deberá registrarse en un *log* (registro histórico) en todos los intentos de acceso, incluyendo aquellos provenientes de líneas telefónicas de acceso directo (*dial-up*). Las funciones de la auditoría de sistemas, relacionadas con las redes y telecomunicaciones, se vinculan con:

- Revisión de las condiciones de seguridad física de equipos e información.
- Previsión de protección de los datos de naturaleza crítica.
- Verificación de existencia y aplicación de políticas y normas de administración de redes.
- Verificación del cumplimiento de exigencias empresariales y gubernamentales.

Otro tipo de ambiente de procesamiento de información, con el que se puede enfrentar el auditor, es el brindado a través de servicios de terceros bajo la forma de procesamiento en tiempo compartido (*time-sharing*) o bajo un servicio específico (*outsourcing*).

Por medio del tiempo compartido, los centros ofrecen sus servicios con computadoras y archivos de gran capacidad e impresoras rápidas, y también recursos de teleprocesamiento a través de terminales. Las exigencias mínimas de seguridad con respecto a estos centros no deben ser inferiores a las que se requieren para la empresa que los contrató. El auditor de sistemas de información revisará, si se presenta un ambiente de esta naturaleza, las condiciones establecidas en el contrato referidas a los compromisos a cumplir por el proveedor, condiciones y garantías de seguridad de programas y datos, formas de establecer los cargos por el servicio, acciones en caso de incumplimiento por parte del proveedor, métodos del suministro de los datos a procesar por parte del cliente.

Si el servicio de procesamiento se efectúa mediante un acuerdo de *outsourcing*, el cliente paga un canon y el proveedor se hace cargo del control de esa parte o del total de las funciones de procesamiento de información; o sea que provee los recursos y los conocimientos técnicos para desarrollar las tareas.

En un ambiente surgido de un acuerdo de *outsourcing*, el auditor debe enfocar su tarea considerando que en esta situación la empresa cliente pierde el control de sus sistemas de información, pasando a la órbita del proveedor del servicio: el control de acceso y la administración de Seguridad quedan en manos del proveedor; la generación de informes de violación son controlados por el proveedor y las modificaciones a programas son efectuadas y probadas por el proveedor. El auditor deberá determinar:

a) De qué manera podrá desarrollar sus funciones en un ambiente de esta naturaleza: qué protección ofrece el contrato en estas circunstancias.
b) De qué manera se asegurará la integridad, confidencialidad y disponibilidad de los datos de propiedad de la empresa.

SEGREGACIÓN DE FUNCIONES

Cuando una empresa establece una organización de procesamiento de información debe darle una adecuada consideración al control interno. Un elemento importante del control interno se logra por medio de la separación de funciones.

La separación de funciones debe aplicarse tanto en lo referente a ciertas tareas que se ejecutan dentro del ámbito de procesamiento de información, como en lo referente a la separación de funciones entre el ambiente de procesamiento de información y otros ambientes de la organización.

El control interno se verá fortalecido si se cumple con este criterio. Esta separación también dará por resultado una mayor eficiencia a causa de los diferentes niveles de habilidad y entrenamiento que requiere cada función.

Un plan de organización que prevea la división de labores es importante a causa de la alta concentración de la actividad de procesamiento de información en un menor número de personas, contrariamente a lo que se requiere en un procesamiento manual. Si una sola persona tuviera el conocimiento operacional completo de un Centro de Cómputos, y la posibilidad de ejercer todas las operaciones involucradas, el riesgo de fraude sería mayor. Cuando las funciones están segregadas entre varias personas se reduce la posibilidad de daño que podría causar la actuación de una sola persona.

En Estados Unidos de Norteamérica, la norma SAS N° 1 de AICPA define qué se entiende por funciones incompatibles, considerando aquellas tareas que no estén debidamente separadas, lo cual resulta una disminución del control.

Según esa norma, funciones incompatibles para propósitos de control contable son aquellas que ubican a una persona en una posición que le permite cometer, y al mismo tiempo ocultar, errores o irregularidades en el curso normal de sus obligaciones. Los errores no son intencionales, mientras que las irregularidades son consideradas intenciones de desfalco. Todo aquél que registra transacciones o tiene regularmente acceso a los activos está en condiciones de cometer errores o irregularidades. Por consiguiente, el control contable depende necesariamente de la eliminación de oportunidades de ocultamiento.

La norma SAS N° 3 de AICPA se refiere específicamente al ámbito del procesamiento electrónico de datos en los siguientes términos: frecuentemente funciones que podrían ser consideradas incompatibles, si fueran ejecutadas por una sola persona en una actividad manual, son ejecutadas mediante el uso de programas de computación. Una persona que tenga la oportunidad de efectuar cambios no autorizados en esos programas, ejecuta funciones incompatibles con relación a la actividad del procesamiento electrónico de datos.

La norma SAS N° 3 agrega que una persona que puede ejecutar cambios no autorizados en los programas supervisores tiene la oportunidad de iniciar transacciones no autorizadas, similares a las de aquella persona que puede efectuar modificaciones no aprobadas en los programas de aplicación o en los archivos de datos. En consecuencia, el programador de sistemas y el administrador de Base de Datos se encuentran en situación de ejecutar funciones incompatibles.

Además de lo estipulado en las normas SAS de AICPA, en Estados Unidos de Norteamérica, el Foreign Corrupt Practices Act de 1977 exige que todas las empresas registradas en el Security and Exchange Commission mantengan un sistema de controles internos. Estos controles deben asegurar que las transacciones sean debidamente autorizadas y registradas, y que los activos de la empresa se encuentren resguardados.

Anteriormente, en este mismo capítulo, hemos identificado cuatro grupos funcionales actuantes en un ambiente de procesamiento de información: proyectos, operaciones, servicios técnicos y control. Dentro de estos grupos, también existen funciones que deben estar separadas. Es lógico pensar que en ambientes de procesamiento reducidos se haga difícil (costoso) mantener un nivel de segregación estricto. Sin embargo, el plan de organización debe intentar compatibilizar al máximo con los costos del principio de separación. Llevando esta afirmación a un extremo, y pensan-

do en un ambiente sumamente reducido en el que exista una microcomputadora donde se ejecuten todos los procesos, el esquema organizativo podría ser el que muestra la figura 21-1.

Figura 21-1. Esquema organizativo en una empresa de reducida dimensión.

La supervisión de los procesos estaría a cargo del gerente administrativo (no habría un jefe del Centro de Cómputos): la programación sería efectuada por servicio externo; la operación (separada de la programación) sería ejercida por los usuarios. En una situación así, la Auditoría de Sistemas de Información deberá aplicar controles compensatorios, tales como revisión periódica y sorpresiva de los programas en uso (verificación de que son los originales aprobados) y la verificación de la ejecución de conciliaciones y su registro por parte de los usuarios finales de los informes de control.

En ambientes de procesamiento más amplios, existirán las áreas funcionales que se describen a continuación. El auditor de sistemas verificará que la división de funciones, existente entre las distintas secciones del Centro de Procesamiento de Información, proporciona un control interno adecuado, y que las funciones de control se encuentran en una posición que les permite ejercerlo con suficiente independencia y autoridad.

Funciones de proyectos

1. Sector Desarrollo de Proyectos

El desarrollo de proyectos comprende:

a) Dirección del desarrollo: se refiere a los métodos para iniciar, planificar y controlar los proyectos en sus etapas de análisis, diseño e implementación.
b) Análisis de sistemas: se refiere a las actividades necesarias para interpretar los requerimientos del usuario y formular un diagnóstico.

Al estudiar la dirección de los proyectos, los auditores analizarán los siguientes aspectos:

- Si se ha formulado realmente un grupo de dirección.
- Si la información que se dispone para controlar un proyecto de desarrollo es confiable.
- Si el nivel de supervisión del diseño mantiene a los proyectos dentro de límites de costo y tiempo.
- Si se prepara un buen plan de control de implantación del proyecto.
- Si los cambios que se producen con el transcurso del tiempo no afectan negativamente la consistencia del proyecto durante su desarrollo.
- Si se ha previsto, como parte de la política de la dirección del proyecto, la incorporación de módulos de programas de auditoría.

Con relación a la función de análisis de sistemas, el auditor verificará que ese sector se mantenga independiente de los demás. Es particularmente importante que la función de desarrollo de proyectos, llevada a cabo por los analistas de sistemas, sea independiente de las actividades de operación. Los aspectos que el auditor de sistemas deberá considerar, al analizar el sector de desarrollo, se indican a continuación.

- Los analistas de sistemas no deberán tener acceso a los datos operativos.
- Los trabajos se realizan sobre la base de estándares de métodos, procedimientos y documentación.
- Las actividades de los analistas de sistemas son sometidas a pruebas de calidad antes de que el desarrollo de los proyectos pase a fases más avanzadas en el ciclo de vida.
- La sección de análisis recibe asesoramiento de auditoría en los aspectos específicos referidos a control.
- Los usuarios son informados de los avances del análisis del proyecto y tienen oportunidad de opinar sobre sus resultados.

2. Sector Programación de Aplicaciones

Si bien la función de programación forma parte del desarrollo de sistemas en algunas organizaciones, al igual que la función de análisis de sistemas, el auditor debe efectuar un examen específico de las tareas de programación. En razón de la necesidad de separación de funciones, los programadores de aplicaciones no deben tener acceso a las bibliotecas de programas de sistemas; tampoco deben alterar el sistema operativo, el DBMS y los controladores de comunicaciones.

Los aspectos que el auditor de sistemas deberá examinar, con respecto a la función de programación, se indican a continuación.

- Si las actividades de programación se desarrollan conforme a normas preestablecidas. Si se aplican criterios de programación modular o estructurado. Si existe control de calidad de la programación y si se emplean métricas adecuadas de control.

- Si las pruebas de los programas se efectúan independientemente de las pruebas de los sistemas.
- Si se controla que los programadores no utilicen datos ni tengan acceso a la computadora en modo operativo.
- Si los nuevos programas, mientras están en desarrollo, se mantienen en una librería especial y si se envían a operaciones luego de haber sido probados y autorizados.
- Si se mantiene actualizada la documentación de los programas.

3. Sector mantenimiento de Programas

El mantenimiento de programas es una tarea vinculada con el desarrollo, pero en instalaciones grandes, es conveniente que se mantenga separada por razones de seguridad. El mantenimiento se refiere a modificaciones menores de los programas que se encuentran en operación, pero que no implican un reemplazo total de las funciones que cumplen esos programas.

El auditor de sistemas deberá examinar los siguientes aspectos con relación a modificaciones:

- Si las modificaciones de los programas que se encuentran operativos son autorizadas del mismo modo que se autorizan nuevos programas (métodos de solicitud y de autorización de correcciones).
- Si las modificaciones no afectan negativamente otras partes del programa que no deben ser modificadas.
- Si se mantiene un registro de las modificaciones solicitadas con indicación de fecha de solicitud y fecha de entrada en vigencia, solicitante, en conformidad con este último.
- Si durante las pruebas de las modificaciones no se utilizan los archivos en explotación.

Funciones de procesamiento de información

1. Sector Captura de Datos

La captura o ingreso de datos (*data entry*) puede efectuarse por diversos métodos. Existen distintos equipos de captación de datos, los cuales crean diversos problemas a los auditores. En algunos casos, es necesario realizar doble operación: entrada y verificación. Entre los diversos métodos de ingreso de datos se aplican: el ingreso en línea (*on line*); el ingreso por lotes (*batch*); la utilización de un dispositivo magnético intermedio; la lectura de caracteres ópticos.

a) Entrada en línea

En un ambiente "en línea", las tareas de entrada son realizadas desde los departamentos usuarios, quienes deben controlar que los datos sean exactos, íntegros y estén autorizados. Un sistema en línea incluye diversas pantallas de edición para realizar la verificación básica del ingreso de datos: controles alfanuméricos, controles de rangos, controles de límites. También debe preverse un adecuado control de los datos rechazados por errores u omisiones, como también, un control de que reingresen corregidos. El personal de entrada de datos en línea no debe estar autorizado para actualizar instrucciones de programas (separación de funciones). Deben mantenerse registros adecuados de los datos con problemas y de sus formas de solución.

b) Entrada por lotes

En un ambiente de entrada "por lotes" el ingreso de los datos se opera dentro del Centro de Procesamiento de información, donde existirá un área de control de datos, cuyas funciones serán las siguientes:

- Desde los departamentos usuarios, recepción de documentos de origen y conservación de los mismos hasta finalizar su procesamiento y retorno a su origen.
- Agrupamiento de los documentos fuentes en lotes, en cantidades manejables, acompañando cada lote con totales de control. Es preferible que los totales de control provengan calculados desde su origen.
- Verificación, conciliación y registración de la salida, y su despacho al departamento de destino.

c) Utilización de dispositivos magnéticos intermedios

La entrada de datos puede provenir desde teclados de varias terminales y almacenarse en un dispositivo magnético intermedio y, desde allí, transmitir los registros a la computadora central. Cuando se utiliza este procedimiento, el auditor de sistemas debe examinar:

- Si el control de calidad e integridad de datos, que se efectúa parte en la terminal y parte en la computadora central, se coordina a la perfección.
- Si en ambas posiciones se corrigen los errores y se reingresan los datos correctos.
- Si los datos que ingresan a proceso se encuentran totalmente verificados.
- Si se controla que no se omitan lotes de datos a ingresar o que no dupliquen lotes.

d) Entrada por lectura de caracteres ópticos

Las lectoras de caracteres ópticos suelen funcionar fuera de línea; leen caracteres ópticos desde los documentos y graban los datos leídos sobre algún medio magnético que luego se conecta con la computadora. Estas lectoras no controlan la calidad de los datos, pero verifican si los caracteres son válidos. Los documentos aceptados durante la lectura se depositan en un casillero, y los rechazados en otro casillero. Esto significa que los registros erróneos no ingresan al proceso. En estos casos, el auditor deberá examinar qué tratamiento seguir para concretar el reingreso de los datos rechazados al proceso, o bien, qué grado de seguridad brinda ese mecanismo.

También interesará al auditor el examen de los siguientes aspectos:

- Agrupamiento de los documentos en lotes manejables, acompañados de carátulas de identificación y totales de control.
- Identificación de los rechazos con relación a la proveniencia de los lotes.

2. Sector Operaciones de Computadora

Debido a la alta concentración de operaciones que se realizan en este sector, será de gran interés para el auditor conocer los procedimientos y, en consecuencia, examinar y evaluar sus condiciones de seguridad. Debe preverse la ejecución de tareas en varios turnos, por lo cual el examen abarcará alternativamente todos ellos.

El examen del auditor de sistemas abarcará los siguientes aspectos:

- Si el área se encuentra resguardada y si sólo el personal autorizado tiene acceso a la misma.
- Si existe una planificación real de las tareas a efectuar.
- Si existe una adecuada separación de funciones dentro del sector Control de Datos, biblioteca de Archivos, control de impresos, montaje de trabajos.
- Si se dispone de estándares operativos adecuados que otorguen seguridad a los procedimientos y métodos de operación.
- Si se mantiene identificación de los trabajos que se refieren a operación de aplicaciones en vigencia, operación de desarrollo de sistemas, desarrollo de software o de recuperación.
- Si se dispone de normas a seguir en caso de interrupción del proceso y actitudes en situaciones de emergencia.
- Si se mantienen registros de las operaciones, en los que se deberán incluir los siguientes datos (con indicación de fecha y hora): programas ejecutados, archivos utilizados, situaciones de interrupción de procesos, mensajes generados por los programas. En los equipos modernos, estos registros son grabados por medio de programas en archivos magnéticos.
- Si se mantienen registros impresos u otras formas de registración de la situación "antes" y "después" de aquellos archivos sobre los cuales se regraba información.
- Si se efectúa el mantenimiento preventivo regular de los equipos.

El auditor de sistemas pondrá especial atención en el examen del ejercicio de los controles gerenciales en el ámbito de Operaciones, con respecto a tres categorías de controles:

a) Seguridad física: destinada a proteger a la organización de los riesgos por pérdida de capacidad de procesamiento, a causa de siniestros o contingencias negativas.

b) Seguridad de datos: se refiere a la cobertura necesaria para proteger los datos frente al riesgo de su destrucción accidental o intencional, como también frente a su modificación o divulgación indebida.

c) Seguridad de procesamiento: se refiere al ejercicio de controles que garantizan un procesamiento de datos correcto, íntegro y oportuno. Deben existir controles de procesamiento con respecto a:

- Asegurar que se procesen todos los datos necesarios para que la información que se obtenga como salida (para cada aplicación) sea completa y confiable.

- Asegurar que los procesos se efectúen en función de una adecuada asignación de tareas y administración de medios magnéticos.
- Asegurar que los operadores conozcan perfectamente los pasos de ejecución de tareas y que existan maneras de verificar su cumplimiento.

A causa de la separación de funciones, el operador no debe tener acceso a totales de control y no debe ingresar datos en los archivos mediante entrada por consola.

3. Sector Distribución

El usuario dispondrá de información impresa a partir del momento en que la reciba. Es por eso que en organizaciones de gran dimensión y con diversidad de aplicaciones (caso de existencia de sucursales), la distribución de la salida de información puede requerir controles especiales, de modo de evitar efectos no deseados tales como: retrasos en las entregas, envíos a destinos equivocados, incumplimiento de prioridades.

Cuando se presente esta situación, el auditor de sistemas deberá examinar los siguientes aspectos:

- Si existe clara definición de prioridades.
- Si se han definido y aplican estándares de distribución.
- Si se mantiene confidencialidad con respecto al manipuleo de informes reservados.
- Si existe una verificación previa del sector Control de Datos antes de disponerse la distribución.

Funciones de servicios de apoyo técnico

1. Administración de seguridad

Las funciones de administración de seguridad deben estar contenidas dentro de la política formulada (sobre el tema) por la gerencia superior. La persona encargada de la administración de Seguridad debe, fundamentalmente, verificar que sean cumplidas las reglas y procedimientos que surgen de esa política previamente definida. Esas reglas comprenden:

- Autorización de acceso a archivos, datos y recursos.
- Acciones correctivas que corresponde emprender en casos de detectarse intentos de violación contra la seguridad.
- Mantenimiento de seguridad con respecto a la reserva sobre el conocimiento de códigos de identificación y contraseñas y sus periódicas modificaciones.
- Aseguramiento de que los datos almacenados se encuentran encriptados según sea necesario.

El auditor de sistemas de información deberá examinar la manera en que se desarrolla esa actividad, asociando la misma a la dimensión y nivel de complejidad del centro de información donde se la aplique, a fin de determinar si esa función se encuentra adecuadamente cubierta o si existe debilidad en cuanto a su cumplimiento.

2. Administración de Base de Datos

Una "base de datos" es un conjunto de datos que son utilizados por varias aplicaciones o programas, que actualizan esos datos de una sola vez y que facilitan el acceso y recuperación de información independiente. Los datos de la base, que pueden ser localizados en distintos registros, son independientes de los programas que los utilizan.

La incorporación del software denominado DBMS reemplaza a una serie de archivos convencionales de datos que debían ser actualizados cada uno en forma independiente. Sin duda, las bases de datos han significado un adelanto de modernización trascendente para las empresas que lo aplican. Pero, paralelamente, estos sistemas presentan situaciones de mayor riesgo desde el punto de vista de su control. En efecto:

- Al estar concentrados todos los datos de una empresa en una única base, aumenta la vulnerabilidad de la empresa y la posibilidad de que los datos de la base se contaminen (si los datos estuviesen distribuidos en distintos archivos la contaminación se limitaría a algunos de ellos, no a todos en una misma oportunidad).
- Las bases de datos alojan elementos de datos que son utilizados por distintos sectores de la empresa. Si no se aplican bases de datos, cada sector dispondría de sus archivos propios y cada uno actualizaría sus datos de manera independiente de los demás sectores. En una base, al existir datos comunes a varios y distintos usuarios, podría ocurrir, por ejemplo, que el Departamento de Ventas decidiera cancelar la cuenta de un cliente y ordenara borrar sus datos del archivo. Sin embargo, el Departamento de Contabilidad necesitará aún disponer de algunos de esos datos, debido a que pueden quedar saldos pendientes de cancelar, cuyo seguimiento deberá continuarse.

El ejemplo anterior pone en evidencia la necesidad de rodear de una adecuada coordinación a los actos que impliquen una manipulación de los datos contenidos en la base: su creación, su modificación o su eliminación.

Por lo tanto, el advenimiento de las bases de datos en lo sistemas de procesamiento de información de las empresas, introdujo una nueva función en el ámbito informático: el administrador de la Base de Datos. Quien detente esta función es responsable de la calidad, seguridad y clasificación de los datos que integran la base. Para ello, debe actuar como nexo entre los distintos usuarios que comparten datos y definir cuál de ellos será el autorizado a modificarlos o anularlos. Además, debe desarrollar, mantener y controlar el diccionario de datos, elemento fundamental en una gestión de base de datos.

El auditor de sistemas de información deberá participar en el proceso de adquisición de un sistema de administración de base de datos en razón de la magnitud del desembolso financiero que ello significa y, además, para verificar que el paquete seleccionado reúna características de seguridad y control satisfactorios. Principalmente, el auditor examinará las condiciones de acceso del sistema seleccionado y la doble protección que ofrece la posibilidad de dos intentos simultáneos de acceso a la base de datos.

3. Programación de sistemas (*System Programmer*)

La función de programación de sistemas comprende la responsabilidad del mantenimiento del hardware y software de sistemas, incluyendo el sistema operativo. Se trata de un función que requiere la posibilidad de acceder a todo el sistema, por lo cual toda intervención deberá quedar asentada en registros históricos; pero en principio, el programador de sistemas no debe operar los programas de aplicación y no debe efectuar corridas de programas utilizando archivos de datos activos.

4. Administración de redes y sistemas distribuidos

La tendencia moderna apunta a adoptar redes y sistemas distribuidos como soluciones informáticas para las empresas. Las ventajas de estos sistemas son:

a) El costo de procesamiento puede resultar más económico que la utilización de una gran instalación central.
b) La descentralización permite una mejor respuesta del sistema de procesamiento de información a las necesidades locales.

Los sistemas distribuidos utilizan computadoras separadas físicamente pero comunicadas entre sí. En estos sistemas, los datos se ingresan y utilizan en diversos puntos geográficos (en los que se realiza algún tipo de proceso local). Por lo general, de los procesos locales surgen datos que, en forma resumida, se transmiten a un organismo central. Esta modalidad de procesamiento debe interesar al auditor de sistemas de información debido a que las operaciones que surgen de un sistema distribuido resultan en su conjunto más complejas que aquellas que son de aplicación en un sistema informático centralizado. Con relación a este tema, el auditor de sistemas de información deberá examinar:

a) Si la función del administrador de red es desempeñada de manera independiente del resto de las funciones informáticas. El administrador de red debería depender directamente del responsable máximo del Departamento de Procesamiento de Información. Por razones de separación de funciones, el administrador de red no debería ejercer funciones de programación de aplicaciones.
b) Si las computadoras locales son compatibles entre sí y también con la que se ubica en el organismo central.
c) Si los programas de aplicación se diseñan y se prueban siguiendo estándares comunes a todos.

d) Si existen procedimientos definidos que aseguren que toda modificación a programas locales tenga su correspondiente aprobación (previa a su ejecución) con expresa indicación de las consecuencias sobre el resto de la instalación.

e) Si existen controles adecuados con respecto a los datos que se transfieren desde un punto local a otro punto local, o desde éstos al organismo central.

f) Si existen controles adecuados referidos al acceso a los programas fuente y a los compiladores. (Los programas fuente no deben estar disponibles para su acceso en los puntos locales debido a que no se permite el desarrollo de proyectos informáticos.)

g) Si todo el sistema provee elementos que permiten disponer de una evidencia auditable adecuada.

Funciones de control

1. Mesa de Control

Las funciones de la Mesa de Control (o sección Control de Datos) debe ser independiente del resto de las funciones de los sectores informáticos, particularmente de aquellas del sector al que están controlando. Este sector de Control de Datos concierne particular interés al auditor de sistemas de información a causa de que por el mismo pasan prácticamente todos los datos que circulan por la empresa y que resultan clave para ejercer pruebas y control interno.

El auditor de sistemas de información examinará, en particular, los siguientes aspectos:

a) Si las funciones de control se ejercen con total independencia de las funciones de operaciones y de programación.

b) Si los usuarios mantienen registros de los datos que envían a procesamiento, de modo que sirvan como elementos para cotejar con aquellos que se registran como entrada en la Mesa de Control.

c) Si el control de los datos que ingresan se ejerce en el nivel de autoridad adecuado y en la etapa del procesamiento lo más adelantada posible.

d) Si se ejerce un control de salida de datos que permita su cotejo con los correspondientes datos de entrada, de modo de verificar el resultado final del procesamiento.

e) Si existen procedimientos definidos con respecto al trámite a seguir en el caso de detección de errores, de su registración, de su informe al usuario, y, finalmente, de su corrección e introducción del dato corregido al proceso.

2. Encargado de biblioteca (de archivos magnéticos u ópticos)

Se incluyen las funciones de resguardo de archivos de datos y de programas, como también de movimiento de entrega y recepción al del área de operaciones dentro de la categoría de funciones de control, a causa de la importancia que significa disponer de elementos esenciales para la continuidad y eficacia de las operaciones trascendentes para la empresa. Esta función debe ser ejercida en forma independiente del resto de las funciones de procesamiento, de modo de respetar el ejercicio del principio de separación de funciones.

Con respecto a las funciones que corresponden al encargado de biblioteca, el auditor de sistemas de información examinará los siguientes aspectos:

a) Si existen estándares definidos que aseguren un almacenamiento adecuado de los archivos de datos y programas contenidos en la biblioteca.

b) Si existen registros de los movimientos (entrega y recepción) de archivos. En algunas organizaciones existe un sistema automático de administración de archivos para facilitar la actualización del inventario y registro de los movimientos de archivo.

c) Si se ejerce un control del inventario de archivos.

3. Control de Calidad (*Quality Assurance*)

Debe ser una función totalmente separada de las funciones de programación. El grupo o persona encargada del control de calidad debe cerciorarse de que los programas, los cambios a los programas y la respectiva documentación cumplan con los estándares antes de ser trasladados al sector de operaciones para su utilización rutinaria.

4. Control de formularios impresos

Se trata de una función que existe en organizaciones amplias, en donde la cantidad y diversidad de formularios es importante. Reviste particular significación en el caso de formularios que, por motivos de control interno, deben contener numeración secuencial correlativa preimpresa. Se encuentran en esta situación los formularios de cheques, facturas, recibos, etc., preparados para ser impresos por procedimientos de computación.

El auditor de sistemas de información deberá examinar los siguientes aspectos:

a) Si existen estándares que reglamenten la manipulación de formularios y el control de su existencia.

b) Si se mantienen registros de los movimientos de entrada y salida (y de su destino) de formularios.

c) Si el control de los movimientos es independiente (separación de funciones) de aquellos sectores que utilizan los formularios.

d) Cómo se dispone de formularios cuando el depósito de los mismos (por razones de turnos) se encuentra cerrado.

Segregación de funciones entre el ambiente de procesamiento de información y el resto de la organización

El principio de separación de funciones rige también con respecto a los límites entre el centro/ambiente de procesamiento de información y otras funciones de la organización, es decir, las correspondientes a usuarios.

En primer lugar, las transacciones relativas a las aplicaciones deben ser autorizadas por el responsable del Departamento Usuario, antes de ser ingresadas al procesamiento. La política de seguridad de la empresa determinará los niveles de autorización que se necesitan para cumplir con ese objetivo. El administrador de Seguridad debe participar en la tarea de asegurar el cumplimiento de las normas que responden a este principio. El auditor de sistema de información, por su parte, debe efectuar controles periódicos de cumplimiento para evitar el ingreso no autorizado de transacciones. Todo lo anterior es válido más allá de que la captura de los datos se realice dentro del recinto del Centro de Cómputos como a través de terminales instaladas en lugares remotos.

El usuario debe participar en la conciliación de datos que ingresan al proceso, y de la misma manera, respecto de la información que egresa. Por su parte, el grupo de control de datos registrará totales de control en planillas de balanceo (podrá utilizar herramientas informáticas para ejecutar este control). Pero la conciliación se efectuará cotejando totales emitidos por el usuario con totales obtenidos por el Centro de Cómputos y revisados por el grupo de control. Los datos rechazados en un proceso deberán ser informados al usuario y deberán ser considerados también como elementos de conciliación.

Elementos y técnicas que ayudan a delimitar funciones

Cuando las funciones están delimitadas se reduce el riesgo potencial de acciones de personas que puedan dañar los activos de la empresa enmarcados en el ambiente informático: datos, programas, sistema operativo, documentación de sistemas, dispositivos físicos.

Existen elementos y técnicas que ayudan a delimitar y separar funciones, algunas de las cuales son las siguientes.

1. Controles en el ambiente físico

   Se refieren a la necesidad de evitar el acceso de personas no autorizadas a los dispositivos que integran el hardware, ubicados tanto en el Centro de Procesamiento de Información como en las áreas usuarias. El propósito de estos controles es evitar que, a través del acceso a los dispositivos, se acceda indebidamente a los datos.

2. Utilización de tablas de autorización

   Estas tablas definen, a través de contraseñas, qué persona está autorizada a acceder a los datos y, en este caso, cuál es nivel de autorización; esto es, acceso a consultas, actualización, modificación o borrado (ya sea de todo el archivo, una transacción o sólo un campo). A su vez, las tablas de autorización de contraseñas deben estar también protegidas de accesos no autorizados: ello se logra a través de un proceso de encriptación de datos o de una protección adicional de contraseña. Además, debe existir un registro histórico de control en el que queden registrados todos los intentos de acceso, como también el resultado positivo o negativo de esa intención.

3. Tratamiento de excepciones

   Las excepciones pueden llegar a constituir puertas de entrada a accesos no autorizados. Deben existir, por lo tanto, informes de excepciones, y el ingreso de los datos contenidos en los mismos debe ser específicamente autorizado.

4. Registros de firmas

   El acceso de usuarios a los sistemas debe quedar evidenciado mediante formularios que lleven firmas autorizadas. En empresas que dispongan de sedes remotas, desde las cuales se provea y se soliciten datos a través de formularios, debe existir un procedimiento de registro de firmas que permita verificar, por medio de cotejo, la autenticidad de los intentos de acceso.

El análisis costo-beneficio de la segregación de funciones

Es indudable que el cumplimiento estricto del principio de separación de funciones significa un peso importante en el rubro Remuneraciones y Cargas Sociales, debido a la necesidad de contar con mayor número en la dotación de personal. Pero también es cierto que existe un costo oculto en aquellas situaciones que, por motivos de economía en la nómina de personal, no se cubren adecuadamente las funciones que evitarían los riesgos de combinar funciones incompatibles entre sí. En estos casos (inadecuada o inexistente separación de funciones), se genera la posibilidad de una pérdida, resultante de la combinación de funciones incompatibles entre sí.

Este costo puede ser estimado, aunque en forma aproximada, mediante el "análisis de riesgo", cuyo concepto se compone con la siguiente variable:

$$\text{Pérdida esperada} = \left[\text{Error no detectado} \times \text{Probabilidad de presentación}\right] + \left[\text{Irregularidad} \times \text{Probabilidad de presentación}\right]$$

Una vez asignado los valores a estas variables, se puede obtener el costo estimado esperado por cada aplicación que resulta de operar sin contar con controles adecuados. La suma de los costos esperados de todas las aplicaciones de la empresa determinará el costo total esperado para la empresa, como resultante de la deficiencia de controles. Desde luego, la adecuación de controles no asegura la

absoluta eliminación del riesgo de errores o irregularidades, pero sí disminuye significativamente sus valores y la probabilidad de presentación.

Cuando el auditor de sistemas se encuentra evaluando el cumplimiento del principio de separación de funciones, debe considerar:

a) La dimensión de la operación y la cantidad de personas involucradas en la misma (cuanto menor sea la dotación más difícil será lograr la separación de funciones).
b) El costo adicional que resulta (en Remuneraciones y Cargas Sociales) de la segregación de funciones.
c) El riesgo emergente de la no separación de funciones .
d) La posibilidad de aplicar técnicas alternativas para alcanzar propósitos similares (supervisión muy estrecha, cuidadosa revisión de las entradas de datos y de la salida de información, registros –*logs*– de toda participación de operadores en los procesos, programas de validación de datos y de rangos muy severos, listados de excepción, etcétera).

Capítulo 22

Controles de accesos lógicos y físicos

Introducción

El objetivo de este capítulo es brindar al auditor de sistemas de información el conocimiento necesario para efectuar la revisión y evaluación de los controles diseñados para resguardar la instalación computarizada de intentos indebidos de acceso lógico y de acceso físico. Incluye también la revisión de los controles ambientales.

Las exposiciones ambientales a riesgos se producen por fenómenos naturales (incendios, inundaciones, problemas de suministro eléctrico). Los intentos indebidos, tanto de acceso lógico como físico, constituyen amenazas (humanas) accidentales o intencionales.

Las funciones básicas del auditor de sistemas de información, con relación a estos controles, son:

1. Verificar la existencia de políticas de seguridad formuladas por la alta autoridad.
2. Evaluar el ambiente de seguridad para verificar su compatibilidad con la política de seguridad.
3. Verificar que los controles y procedimientos guarden vigencia con relación a la política, y controlar que estén en actividad.

Existen temas claves que interesan a la Auditoría de Sistemas de Información; entre ellos, se destacan los que se señalan en el cuadro de la figura 22-1 (*véase* pág. 310).

TAREAS DEL AUDITOR DE SISTEMAS DE INFORMACIÓN CON RESPECTO A:

TEMA	ACCESO LÓGICO	ACCESO FÍSICO
Evaluación de controles	Sobre las potenciales rutas de acceso al sistema.	De la seguridad física del recinto en que se encuentren ubicados los dispositivos involucrados en el procesamiento y almacenamiento de información.
Prueba de controles	Sobre las rutas de acceso para determinar su eficacia.	De la seguridad física, para determinar su eficacia.
Evaluación del ambiente	De control de acceso para analizar resultados de pruebas y evidencias de auditoría y determinar el cumplimiento de los objetivos de control.	De seguridad física para analizar resultados de pruebas y evidencias de auditoría, para determinar el cumplimiento de los objetivos de control.

Figura 22-1. Temas claves para el auditor de sistemas de información.

Política de seguridad

Un elemento clave para cumplir con éxito todo propósito de seguridad, es la formulación de una política que defina con claridad el marco de la seguridad y el establecimiento de responsabilidades.

Esta política exige los siguientes requisitos:

1. Conscientización formal de la importancia de la seguridad por parte de la alta gerencia.
2. Percepción de esa importancia por parte de la dotación de personal en sus distintos niveles.
3. Entrenamiento de seguridad.

La política no debe limitarse a un conjunto de intenciones documentadas por escrito: se debe comunicar y verificar el compromiso por parte de todos los involucrados.

Uno de los elementos trascendentes de la política es el referido a la protección de la información y, por lo tanto, a la autorización de acceso a la misma. La posibilidad de acceso responde a la siguiente filosofía: "Podrá acceder aquél que tenga 'necesidad de saber' o 'necesidad de hacer' en el cumplimiento de su trabajo".

El acceso a la información estará protegido por medio de una técnica de utilización de códigos y contraseñas –que serán mantenidos en secreto–, y el resguardo físico se apoyará en la protección de los recintos que alberguen los dispositivos de procesamiento y transmisión de datos.

Una cuestión que debe quedar dilucidada, es el tema de reconocer quién es el propietario de los datos en una organización y quiénes son los usuarios de los datos. Los propietarios son aquellos miembros que generan informes o que toman decisiones a partir de esos datos. Pero también existen otros usuarios que utilizan datos, en la medida en que disponen de autorización de acceso otorgada por sus propietarios. Asimismo, las políticas de seguridad deben definir la responsabilidad de quienes son custodios de los datos: el personal de procesamiento de información.

Todo lo anterior, referido a políticas de seguridad, debe ser canalizado por quien detenta una función muy específica dentro del Departamento de Procesamiento de Información: el administrador de Seguridad. Es el responsable de verificar el cumplimiento de las normas y políticas de seguridad. También es responsable de participar en el programa de entrenamiento que asegura la percepción del concepto de seguridad por parte del personal.

En empresas de gran magnitud, es común la existencia de un Comité de Seguridad, integrado por representantes de todos los sectores (debido a que la seguridad abarca a toda la organización). En definitiva, dicho Comité será quien asesore sobre los aspectos que deben abarcar las normas de seguridad.

Rutas de acceso lógico

El acceso lógico de la información contenida en archivos magnéticos puede efectuarse por distinta rutas. Debido a que los dispositivos de acceso también pueden variar, y los motivos de acceso también pueden ser diferentes, será necesario analizar las distintas exposiciones a riesgos y los métodos de protección que para cada caso corresponda.

Las instalaciones pueden adoptar las siguientes formas:

1. Computadora instalada en sede central

   Es la computadora principal de la empresa. Procesa grandes volúmenes de datos. El ingreso de datos puede efectuarse "en línea" o por procesamiento diferido.

2. Red de procesamiento distribuido

   Dentro de este ambiente existen computadoras descentralizadas o remotas que cumplen algunas funciones, tales como entrada y edición de datos, y procesamiento de transacciones y generación de informes. La computadora central queda reservada para otras funciones, tales como actualización de archivos maestros y desarrollo de software. La computadora central y las computadoras remotas se conectan a través de líneas de comunicación y comparten datos y procesamiento.

3. Conectividad entre microcomputadoras y redes

   En la actualidad, las redes constituyen elementos de gran desarrollo bajo la forma de descentralización de procesamiento de datos. Las denominadas LAN enlazan a varios usuarios dentro de un área geográfica limitada. Las WAN cubren distancias lejanas. Pueden conectarse microcomputadoras con el procesador central o con una red, beneficiándose al compartir datos y software. Es una variante de una red de procesamiento distribuido.

4. Terminales para entrada remota de trabajos (*Remote Job Entry*)

   En este ambiente, las terminales se ubican en sedes remotas, cerca de los usuarios. Las terminales están conectadas por líneas de comunicación con la computadora central, lo cual les permite enviarle datos sobre transacciones y aprovechar la capacidad de ésta.

5. Otros dispositivos

   Además de los dispositivos de procesamiento, existen otros que se utilizan específicamente para comunicación y transmisión de datos. Entre estos últimos se encuentran los denominados módem (modulador-demodulador), cuya utilización se debe a la necesidad de compatibilizar las señales analógicas que utilizan las líneas telefónicas, con las señales digitales que utilizan las computadoras. Otros dispositivos son los controladores de comunicaciones entre las terminales y la computadora central.

Teniendo en consideración los dispositivos que se emplean, el auditor de sistemas de información deberá interesarse en conocer las distintas modalidades o vías de acceso lógico a la información.

Los usuarios u operadores podrán ingresar datos en la modalidad "en línea" o por "procesamiento diferido". En el procesamiento en línea, los datos se ingresan desde una terminal con pantalla (*video display terminal*); se aceptan o rechazan los datos de inmediato, y aquellos que son aceptados pueden provocar inmediatamente –si así corresponde por definición del sistema la actualización de archivos– la incorporación de nuevos datos o el borrado de algunos, o bien simplemente una consulta y respuesta a/de archivos. El procesamiento diferido o por lotes se realiza agrupando datos y transmitiéndolos (electrónica o físicamente) en grupo en determinados momentos, a intervalos predefinidos o luego de acumular cantidades fijas de datos.

Nos interesará analizar cuáles son las funciones del auditor de sistemas de información con respecto a la revisión de controles en los casos de procesamiento en línea y en procesamiento diferido.

Procesamiento en línea: modalidades

La modalidad de procesamiento en línea es una de las que más preocupa al auditor de sistemas, a causa del alto grado de vulnerabilidad de la misma. Exige que se ejerzan los mejores métodos de control y seguridad. El uso de terminales ha colocado a los usuarios cerca del lugar de generación y uso de los datos, y también cerca del lugar de procesamiento. Ha permitido a los usuarios tener un contacto más directo con los sistemas computarizados. Pero todo esto ha provocado un cambio en el grado de responsabilidad de los operadores del sistema: el manipuleo de datos ya no se efectúa exclusivamente dentro del Centro de Cómputos; puede efectuarse desde cualquier lugar técnicamente habilitado.

Los diferentes tipos de ambientes de procesamiento electrónico de datos tienen similitudes (características generales) y diferencias (características especiales). Entre las características generales se observan:

- Las funciones que realizan los sistemas computarizados son similares en todos los ambientes.
- Todos los sistemas computarizados están expuestos a errores potenciales similares.
- Todos los sistemas computarizados pueden ser controlados por tipos de controles similares.

Sin embargo, existen factores que diferencian las necesidades de procesamiento de datos en distintos ambientes:

- La frecuencia y magnitud de los errores potenciales.
- La naturaleza y extensión de los controles.
- La naturaleza y extensión de las pistas de auditoría.
- La complejidad de la tecnología de procesamiento electrónico de datos aplicada.
- El costo y esfuerzo de los controles.

El cuadro de la figura 22-2 resume las principales características de los sistemas en línea y sus efectos sobre los controles y la auditoría.

EFECTOS DE LOS SISTEMAS EN LÍNEA SOBRE LOS CONTROLES Y LA AUDITORÍA

CARACTERÍSTICAS DE LOS SISTEMAS EN LÍNEA	EFECTOS SOBRE LOS CONTROLES Y LA AUDITORÍA
1. Multiplicidad de puntos de entrada de datos.	La implantación y aplicación de controles exige mayor esfuerzo, por lo cual es mayor el costo de evaluación y prueba de esos controles. Los datos ya no son agrupados en lotes y transportados físicamente al centro de procesamiento, sino que son enviados al azar por línea telefónica a medida que van ocurriendo.
2. Los documentos de entrada de datos pueden quedar archivados en sedes remotas (locales) distantes del lugar donde se efectúa el procedimiento.	El acceso físico a los documentos de origen, para el auditor, puede ser dificultoso.
3. Los datos de entrada o de transacciones pueden tener distinta naturaleza entre sí y llegar a intervalos al azar.	Las transacciones en lotes tienden a desaparecer. Muchas personas pueden tener acceso directo a los sistemas, sus programas y archivos.
4. Una vez instalado un sistema en línea se hace difícil retornar a procedimientos manuales o artesanales. El tiempo de respuesta se vuelve muy rápido, casi instantáneo.	La concreción de muchos negocios se apoya en la información producida por los sistemas en línea. Tendría efectos desastrosos para la organización la ruptura del sistema ya que podría detener la operatoria del negocio. La confiabilidad y viabilidad del sistema de información adquiere características críticas.
5. Las transacciones en línea, generalmente, alimentan directamente a la computadora. Utilizan para ello una variedad de dispositivos de entrada, tales como *scanners* ópticos, terminales inteligentes, etcétera.	Las pistas de auditoría dejan de ser las convencionales. Los registros visibles (legibles) disminuyen. Se necesita, en consecuencia, aplicar procedimientos compensatorios de auditoría para suplir la ausencia parcial de evidencias escritas.

6. En los sistemas en lotes, los pasos de procesamiento son generalmente fijos y repetitivos. En los sistemas en línea, la cantidad de pasos de procesamiento y su secuencia pueden ser diferentes para distintos tipos de transacciones, en razón del ingreso al azar.	En los sistemas en línea, los controles están orientados técnicamente, al contrario de los controles de los procedimientos en lote (orientados a tareas manuales de los usuarios).
7. El dinamismo que impone el procesamiento en línea provoca que los errores tiendan a ser más complejos y difíciles de detectar.	El diseño de los sistemas debe incorporar rutas para rastrear transacciones sobre una base más dinámica y frecuente que los controles periódicos ocasionales.
8. La detección y corrección de errores, en muchos casos, sólo puede efectuarse después de que las transacciones tratadas individualmente fueron procesadas, dado que el ciclo de procesamiento se ha vuelto más compacto.	El diseño de los sistemas debe prever la posibilidad de corregir errores después de finalizado el procesamiento en línea. Como medida de precaución esta capacidad de acceder a archivos en línea para efectuar corrección de errores, debe quedar restringida a muy pocas personas y perfectamente identificadas.
9. Multiplicidad de rutas posibles en el ambiente de procesamiento en línea (procesamiento "orientado a transacciones", opuesto a "procesamiento orientado a lotes").	Crea la posibilidad de que surjan nuevas oportunidades de fraudes potenciales. Provoca la necesidad de aplicar técnicas de "auditoría de procesos" en lugar de "auditoría de resultados" (después de los hechos).
10. Los sistemas en línea se orientan al multiusuario, lo que provoca la necesidad de compartir dispositivos y archivos.	El diseño de los sistemas debe prever la inclusión de capacidades de identificación, autenticación y control de acceso. También, el hecho de compartir archivos, hace necesario establecer mecanismos de protección de privacidad y confidencialidad de la información.
11. Algunas transacciones pueden generarse electrónicamente durante el procesamiento (por ejemplo, cálculo de intereses) sin intervención humana y sin preparación de documentación escrita.	Existe el peligro de que estas transacciones (o parte de ellas) no puedan ser visibles directamente por el auditor. Por lo tanto, si se modificara intencional o indebidamente un registro, puede ocurrir que el auditor no logre rastrear y ubicar la fuente del cambio. El diseño del sistema debería prever alguna forma de documentación (y de acceso a la misma) de registros que se generen automáticamente.
12. Cuando se procesan sistemas en lotes, los archivos son utilizados solamente cuando se opera una aplicación determinada. Los archivos de los sistemas en línea se encuentran permanentemente en línea y disponibles.	El usuario puede acceder instantáneamente a los datos almacenados sin necesidad de esperar un procesamiento en lote. Pero esto obliga a la segregación de datos y estrictos controles para evitar accesos no autorizados o que no correspondan.
13. Los sistemas en línea avanzados pueden consistir en un conjunto de varios subsistemas desarrollados por distintas personas.	Las pruebas de esos sistemas resultan más complejas para el auditor. Este debe determinar qué interfases son prioritarias desde el punto de vista de las pruebas de auditoría.
14. Los sistemas en línea orientados a bases de datos tienden a forzar la integración de los datos que surgen de operaciones de negocios, con la simultánea captura, registración y actualización de datos operativos y financieros (fundamento de la contabilidad).	Los datos contables pueden ser, en consecuencia, un subproducto de otros datos. Se necesitan, entonces, nuevos criterios y nuevos enfoques para auditoría, control y seguridad.

15. Los sistemas en línea tienden a operar con bases de datos. Uno de los objetivos de los mecanismos de las bases de datos es la reducción de la redondancia de elementos de datos.	La reducción o eliminación de la redundancia provoca la debilitación de la capacidad de control que surge de disponer de duplicación de elementos de datos. Se origina, así, la necesidad de aplicar controles complementarios, desde el punto de vista de auditoría.
16. Los sistemas en línea avanzados pueden requerir el ensamble de varios componentes de hardware y software provenientes de distintos proveedores.	En el caso de fallas del sistema se complica la detección de la causa. Algunos programas pueden carecer de capacidad de auditoría.
17. En algunos sistemas avanzados, el alcance de las rutas de información pueden trascender los límites de la organización (ingreso y egreso de datos). Tal es el caso de los sistemas de punto de venta y transferencia de fondos.	El auditor de sistemas debe enfocar nuevos problemas surgidos de la necesidad de controles o confirmaciones "computadora-a-computadora" entre compañías.

Figura 22-2. Efectos de los sistemas en línea sobre los controles y la auditoría.

En el procesamiento en línea se utilizan terminales. Estas pueden ser inteligentes (disponer de la posibilidad de ejecutar una cantidad limitada de funciones: validar datos, formatear mensajes, almacenar información en un dispositivo local) o no inteligentes (bobas): acepta los datos que se ingresan en la terminal sin análisis ni control. La figura 22-3 (*véase* pág. 317) muestra un modelo de procesamiento en línea.

Para analizar los problemas que afectan a la auditoría, el auditor de sistemas deberá interpretar las características de las diversas formas que puede presentar el procesamiento en línea. Esas modalidades son las siguientes:

1. Lotes remotos de transacciones

   Consiste en grabar lotes de datos de transacciones en archivos transitorios y transmitir esos lotes en momentos determinados a la computadora central. Este método no permite alterar lo datos que ya existen en los archivos de la computadora. La figura 22-4 (*véase* pág. 318) muestra un esquema de esa modalidad de procesamiento.

   Las causas de riesgo que surgen con las aplicaciones de lotes remotos son la pérdida parcial o completa de las transacciones durante la transmisión, como también, la alteración indebida de los datos de entrada a causa del ruido en los circuitos de transmisión (líneas telefónicas).

   El auditor de sistemas de información deberá verificar, con relación al procedimiento de introducción de datos en línea, los siguientes aspectos:

   – Si los controles de acceso son adecuados (se analiza este tema más adelante).
   – Si el Departamento Usuario está estructurado con sectores separados en los que se preparen los datos y se efectúen las verificaciones previas a la entrada; autorización de las transacciones; asientos en registros y control de los totales de los datos que ingresan (sector Control de Datos), a causa de evitar omisiones o duplicaciones de datos de entrada); captura y transmisión de datos (sector Ingreso de Datos). Los totales de control deben ana-

lizarse desde tres puntos de vista: a) totales por cada sede de origen de datos; b) totales por cada tipo de transacción, y c) totales que afecten a cada archivo maestro de Datos.

- Si existen elementos suficientes –a modo de pistas de auditoría– que permitan hacer el seguimiento de las operaciones desde su registración en los documentos originales hasta su almacenamiento en archivos.
- Si los errores que se detectan, como consecuencia de aplicar procedimientos de validación, son tratados adecuadamente a través de correcciones oportunas.
- Si en situaciones de emergencia, frente a caídas del sistema de comunicaciones en momentos en que se introducen datos, existen formas de determinar cuál ha sido la primera operación de la serie que se ha perdido. De tal manera, en el momento de reiniciar el proceso no se producirán omisiones ni duplicaciones en la transmisión de transacciones. Si la duración de la interrupción es muy prolongada, deberán aplicarse planes de emergencia para los cuales deberán estar disponibles equipos supletorios, formularios adecuados y normas de procedimientos para la preparación, control y transferencia de lotes de datos.

2. RJE (*Remote Job Entry*, Entrada remota de trabajos)

La terminal de RJE se compone de un medio de introducción de gran volumen de datos y de la salida correspondiente. El proceso y el almacenamiento de los registros se efectúa en la sede central.

Normalmente, este método actúa en modalidad por lotes; se preparan en la sede remota los lotes de entrada y las instrucciones de control del trabajo; luego, en momentos determinados, se envían a la sede central. El proceso se realiza en el ordenador central y el resultado (salida) se devuelve a la sede remota. La responsabilidad del proceso recae en el usuario, pues es quien controla los datos a través del proceso.

Los riesgos en esta modalidad de procesamiento son similares a los anotados con respecto a los lotes remotos de transacciones, a los cuales se agregan los relacionados con el acceso limitado y el abuso del uso de la computadora.

Desde el punto de vista de auditoría, el auditor de sistemas de información deberá considerar el dispositivo terminal de RJE como si fuera un sistema de computación común, en modalidad por lotes; pero debido a que la computadora y los archivos se encuentran a distancia, se plantean una serie de problemas adicionales.

El usuario deberá disponer de una estructura que comprenda una función de preparación de datos, otra de control de datos y otra de control de impresos. El sistema deberá prever las medidas de emergencia que se aplicarán en caso de interrupción de comunicaciones por causa de la alta dependencia de la sede local y del procesamiento que se efectúa en la sede central.

3. Consultas en tiempo real

Permiten a los usuarios acceder a los datos de los archivos de la computadora y obtener una respuesta inmediata a las solicitudes de información desde una terminal. Esta modalidad no permite introducir datos o alterar la información contenida en el archivo. En algunas situaciones puede mantenerse un registro de las consultas. La figura 22-5 (*véase* pág. 318) muestra un esquema de esta modalidad.

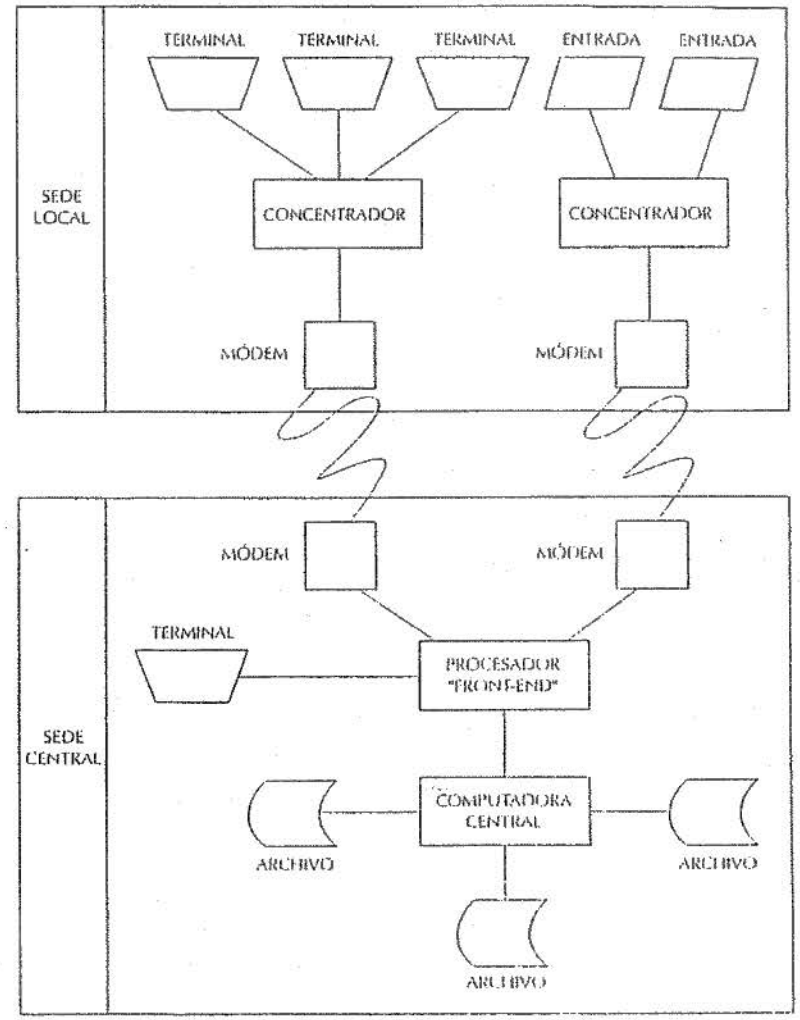

Figura 22-3. Diagrama de modelo de procesamiento en línea.

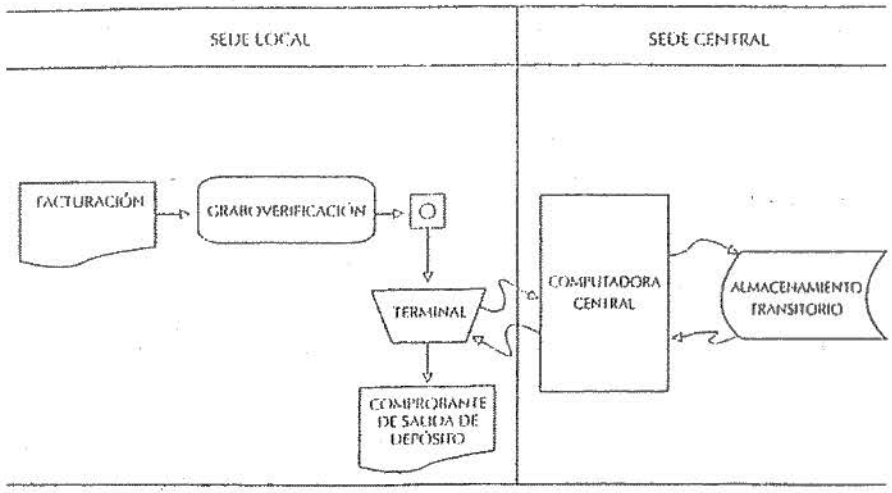

Figura 22-4. Esquema de procesamiento a través de lotes remotos de transacciones.

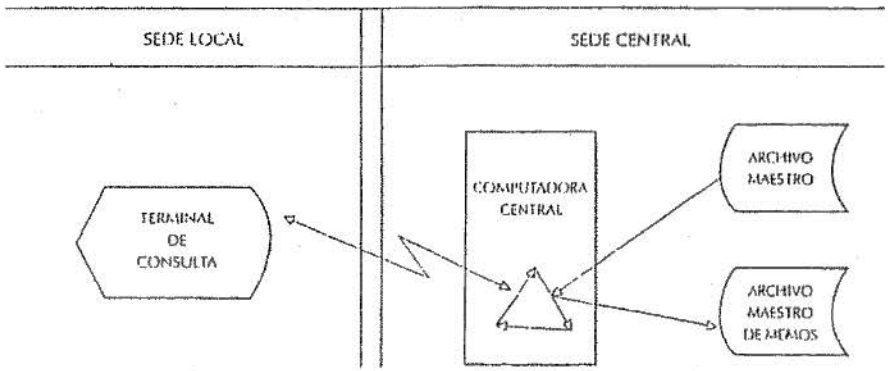

Figura 22-5. Esquema de consulta en tiempo real.

Las causas de riesgo que implica esta modalidad son las siguientes:

- **Invasión a la privacidad**
  El acceso ilimitado permite obtener conocimiento de información que no tiene que ser difundida. Esto puede dar lugar a sanciones legales.
- **Respuestas con información desactualizada**
  Puede ocurrir que un archivo sea actualizado periódicamente a través de procesamiento en lotes. Si se efectúa una consulta en línea a ese archivo se obtendrá una respuesta inmediata, pero que no reflejará las transacciones comprendidas entre el momento de la última actualización y el momento en que se efectúa la consulta.
- **Suministro de información errónea**
  Surge como consecuencia de las mismas causas que pueden afectar distorsivamente las transmisiones electrónicas.
  El auditor de sistemas de información verificará, con respecto al procedimiento de consultas en línea, los siguientes aspectos:
  - Si los controles de acceso son adecuados (se analiza este tema más adelante).
  - Si el usuario accede a información en forma de consulta respecto de la cual tiene "necesidad de conocer", es decir, si la consulta es justificada.
  - Si en el caso de distintos tipos de consultas se respetan las prioridades definidas.
  - Si los tiempos de respuesta son oportunos y si la forma de expresión de la respuesta es la más adecuada: representación visual en pantalla, auditiva o impresa.

4. **Actualización en línea**

Este procedimiento permite que los archivos maestros sean alterados mediante transacciones de entrada, de actualización, de mantenimiento o de corrección de errores originados en las terminales. La figura 22-6 muestra un esquema de este tipo de procesamiento.

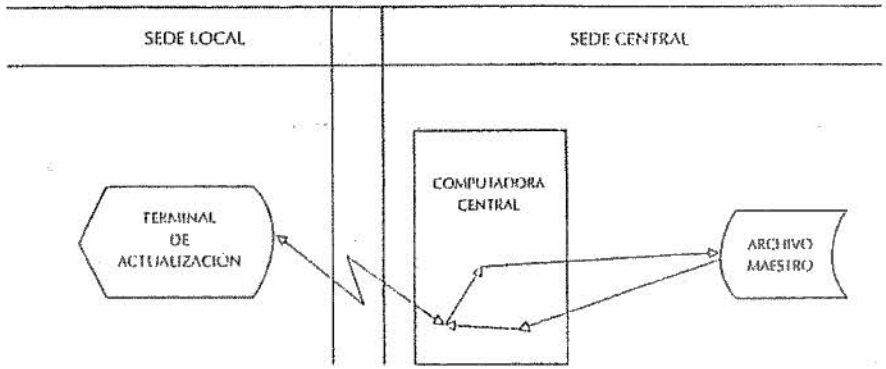

Figura 22-6. Esquema de actualización en línea.

Las causas del riesgo que implica la actualización en línea son las siguientes:

- Acceso ilimitado
  Este problema es similar al que se presenta en el caso de consulta en tiempo real, aunque agravado por el hecho de que las transacciones no autorizadas pueden tener consecuencias más graves que la violación contra la confidencialidad.
- Fallas del equipo de computación o de los programas de operación
  El operador que ejecuta una transacción desde una sede remota puede ignorar si la transacción se procesó completamente; en este caso, la operación puede perderse o repetirse indebidamente. Además, los archivos pueden alterarse sin que queden registros de la transacción que originó el cambio. Puede ocurrir, así, la ausencia de una pista de la transacción que impida acciones correctivas o la imposibilidad de corroborar resultados.
- Incremento en la comisión de errores
  Cuando la entrada de datos puede provenir de un gran número de usuarios que acceden a las terminales, se incrementa la probabilidad de ejecución de errores. El auditor de sistemas de información verificará, con respecto al procedimiento de actualización en línea, los siguientes pasos:
  - Si los controles de acceso son adecuados (se analiza este tema más adelante).
  - Si se aplican procesos de validación de los datos de los registros de entrada.
  - Si se efectúan controles de conciliación entre totales de datos de entrada, como también la incidencia sobre los totales de los datos del archivo afectado una vez realizado el proceso de actualización.
  - Si se efectúan las correcciones que corresponden (y en tiempo oportuno) como consecuencia de errores detectados en el momento de validación. Cómo se soluciona la situación de respuestas sobre datos que no fueron actualizados en su momento (en los casos de consultas) como consecuencia de rechazos por errores de entrada.
  - Si existe alguna manera de determinar (registrar) el contenido de los registros del archivo actualizado antes de la actualización y después de la modificación.

La figura 22-7 (*véase* pág. 321) muestra un esquema de programación en línea. Los programas así conducidos pueden ser utilizados para acceder a un archivo en sede central y modificar sus registros.

Las causas de riesgos deben interpretarse del mismo modo que si una persona ubicada dentro de la sede central pudiera manejar y controlar personalmente el equipo.

El auditor de sistemas de información verificará, con respecto al procedimiento de programación en línea, los siguientes aspectos:

- Si los controles de acceso verifican que solamente los programadores autorizados puedan introducir programas o modificaciones en los programas existentes.
- Si existe documentación que evidencie la necesidad y la correspondiente justificación y autorización de cada programa que se incorpore al sistema, como también de cada modificación (mantenimiento) que se ejecute.
- Si el tiempo de utilización del hardware es eficaz mediante este método de programación o si existen razones para revertir su desarrollo.
- Si las pruebas de los programas y de las modificaciones se efectúan en forma independiente de quien los elaboró.

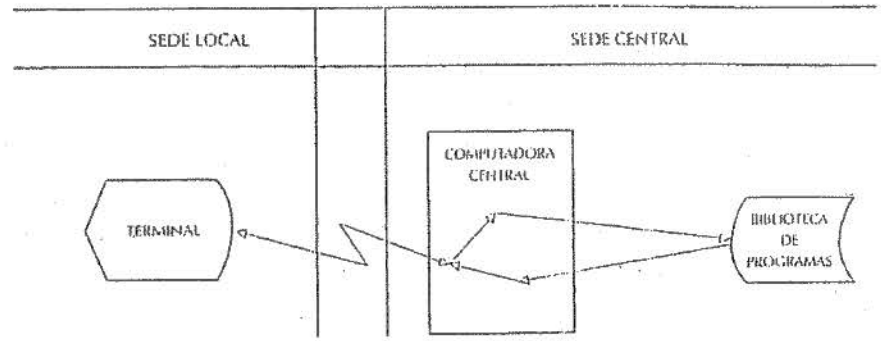

Figura 22-7. Esquema de programación en línea.

REVISIÓN DE AUDITORÍA DEL ACCESO EN LÍNEA

El objetivo principal de la Auditoría de Sistemas, con relación a la protección del acceso en línea, es evitar que algún usuario no autorizado pueda acceder a datos o programas a los que no debiera, y permitir que sólo efectúe procesos para los cuales está autorizado.

Los temas específicos que deberá abordar el auditor de sistemas de información se detallan a continuación.

1. Uso de contraseñas

   Uno de los modos para reducir el riesgo de un "acceso ilimitado" consiste en la utilización de una clave denominada "contraseña". Las contraseñas intentan conocer o verificar algo, que puede ser:

   - Verificar "quién" intenta el acceso; cómo se llama; qué puesto ocupa, etcétera.
   - Verificar si el usuario expresa "algo que debe saber": clave especial, información peculiar que sólo el usuario sabe (una fecha, etcétera).
   - Verificar "desde dónde" se intenta el acceso: es el reconocimiento de la ubicación del dispositivo desde donde se intenta acceder.
   - Verificación de algo que el usuario "debe tener": habitualmente se refiere a alguna tarjeta plástica magnetizada que, ante el intento de acceso, debe insertarse en un dispositivo lector.

   Para que los controles de contraseñas sean efectivos deben combinarse algunos de los enfoques anteriores. Los sistemas de software suelen disponer de una protección de acceso. El auditor de sistemas deberá verificar el alcance de esa protección.

   El auditor de sistemas también verificará el nivel de acceso que permite la contraseña en cada caso: acceso limitado a archivos, a programas, a registros, a campos. Además, las contraseñas podrán habilitar al usuario al acceso a archivos, de modo que se efectúen sólo

consultas; o bien, actualizar datos, borrar datos, crear registros, copiar. Los usuarios deben mantener reserva de la contraseña asignada: no deberá quedar registrada ni ser mostrada por pantalla.
Las contraseñas son asignadas por el administrador de Seguridad. Las mismas deben cambiarse periódicamente (el paso del tiempo deteriora su condición de reserva). Es preferible que el sistema computarizado exija su cambio periódico.
Existe un método de encriptación de las contraseñas: los métodos criptográficos son mecanismos de codificación que reducen el riesgo de que se conozca la clave y se la utilice indebidamente.
Las contraseñas deben respetar cierto formato y cumplir cierta reglas: su longitud mínima debe ser de cuatro caracteres; los mismos deben resultar de una combinación de caracteres alfabéticos y numéricos.
El administrador de Seguridad (o el sistema automáticamente) debe desactivar los códigos de identificación que no sean utilizados durante un lapso prolongado. Una vez que se operó el acceso, tras haber cumplido con las condiciones de accesibilidad, el sistema automáticamente debe desactivar la conexión si es que registra inactividad durante un lapso prolongado, por ejemplo, una hora.
En consecuencia, el auditor de sistemas de información efectuará una evaluación sobre la utilización de contraseñas y códigos de identificación de los usuarios. Para probar el grado de seguridad en el manejo de contraseñas, el auditor de sistemas intentará vulnerar los accesos tratando de descubrir alguna, ya sea por adivinanza o por búsqueda del código en el recinto de trabajo de los responsables. Si logra acceder a la tabla donde figuran almacenadas las contraseñas, deberá verificar si éstas son ilegibles (por estar encriptadas). Además, verificará personalmente que al ingresar una contraseña ésta no sea exhibida. También revisará la documentación de autorizaciones y comprobará si las mismas responden al principio de "necesidad de saber". Con relación a la permanencia en las tablas de contraseñas inactivas, el auditor de sistemas debe revisar que todas ellas pertenezcan a personas que continúan en funciones dentro de la organización. También deberá intentar vulnerar las condiciones sintácticas de las mismas a través de formatos inválidos, observando cómo reacciona el sistema. Con relación a la desconexión automática de una terminal, hará la prueba de iniciar un proceso de ingreso de datos de transacciones, para luego suspenderlo durante un intervalo predefinido y esperar hasta que se produzca la desconexión automática de la terminal al término del intervalo. También el auditor probará que se cumpla la condición de desconexión automática de una terminal, provocando varios intentos de acceso infructuosos.

2. Registro de tiempo de uso de cada sistema y de accesos a la computadora

Debe aplicarse un método que registre, en un *log*, el uso y las tareas de las terminales, así como también los intentos de violación. En los sistemas de mucha actividad de procesamiento, el controlador de teleproceso vigilará, a través de una terminal, las incidencias que se produzcan. Si se intenta ingresar en forma continua una contraseña errónea, el sistema de seguridad debe desactivar automáticamente el ingreso. Los departamentos usuarios deben ser informados de la cantidad de tiempo que se invierte en el procesamiento de sus sistemas. A su vez, deben informar sobre los casos en que esos tiempos no sean adecuados con relación a los trabajos recibidos.
El administrador de Seguridad debe revisar periódicamente los informes que surjan del *log*. Por su parte, el auditor de sistemas de información debe realizar un seguimiento de las violaciones y analizar tendencias que indiquen los reiterados intentos de violación contra las reglas de acceso (determinar si son accidentales o intencionales).

3. Criterios de autorización

En el párrafo anterior se explicaron los diversos niveles de acceso que pueden tener los usuarios con relación al alcance de la información. El criterio general que rige para la autorización de accesos es la "necesidad de saber" y la "necesidad de hacer". La alta gerencia formulará la política general en materia de autorizaciones, y el administrador de Seguridad será quien la implemente y vigile.
Los criterios de autorización formalizados indicarán que los usuarios son autorizados para ingresar únicamente a aquellas transacciones que sean compatibles con sus funciones. Dentro de éstas, algunos sólo podrán consultar datos, otros podrán ingresar y actualizar archivos y otros podrán efectuar corrección de errores. Además, cada usuario estará autorizado a acceder únicamente a aplicaciones y archivos asociados a sistemas consistentes con sus funciones. La figura 22-8 ilustra una tabla de esta naturaleza, incorporada a un software de protección.

CLAVE DE ID. LÓGICA	ARCHIVO			
CLAVE DE ID. LÓGICA	ARCHIVO	CÓDIGO DE TRANSACCIÓN		
CLAVE DE ID. LÓGICA	ARCHIVO	CÓDIGO DE TRANSACCIÓN	LÍMITE MONETARIO	
CLAVE DE ID. LÓGICA	ARCHIVO	CÓDIGO DE TRANSACCIÓN	LÍMITE MONETARIO	FECHA HABILITADA

Figura 22-8. Modelo de tabla de autorizaciones.

4. Reglas de protocolo en línea

La mayoría de las transacciones en línea se efectúan por medio de líneas telefónicas convencionales. Las condiciones de seguridad exigen que se cumplan ciertas reglas de protocolo, entre las que se encuentran las siguientes:

- Clave de identificación de la terminal.
- Número de control consecutivo para identificar la transmisión.
- Número de mensaje.
- Fecha y hora.
- Clave de acción.
- Indicador de fin de mensaje.

5. Confirmación de llamada

Cuando el acceso se efectúa mediante líneas telefónicas de discado común, debe aplicarse un procedimiento de devolución de la llamada (*dial-back*) para confirmar el origen válido de la llamada inicial. Esta confirmación puede hacerse automáticamente si se dispone de sistemas de comunicación adecuados: la computadora rastrea en una tabla electrónica la validez del número telefónico de origen; si la devolución del llamado no logra conexión con un teléfono autorizado, se traba el acceso a la computadora.

6. *By-pass* (desvío) de seguridad

En general, los programadores de software de sistemas pueden tener la necesidad de ejercer ciertas funciones no permitidas, como por ejemplo las que otorgan acceso a archivos sin leer la etiqueta (*by-pass* de procesamiento de etiqueta). También puede ocurrir que ciertos códigos de protección de programas enlatados sean los mismos para todos aquellos suministrados por el mismo proveedor. En estos casos, el auditor de sistemas de información deberá asegurar que queden registros de las intervenciones de los programadores cuando se acceda a archivos sin respetar el procesamiento de etiquetas, y que la contraseña de los programas adquiridos sean cambiadas en el momento de la instalación.

7. Verificación de redundancia

Es un método aplicado por la unidad de control de comunicaciones, el cual verifica la transmisión de los caracteres de información, ya sea en un sentido vertical o longitudinal (similar al de verificación de paridad). Su propósito es detectar distorsiones que se produzcan sobre la información en el momento de la transmisión.

8. Registro cronológico de transacciones

Si bien este método es usado específicamente en los DBMS (algunos de estos sistemas acompañan la gestión con esta finalidad en forma automática), el auditor de sistemas de información debe verificar la presencia de un registro de este tipo, debido a que el mismo constituye la fuente principal en los intentos de recuperación de información de archivos dañados o borrados. La figura 22-9 ilustra este procedimiento de seguridad.

9. Sensibilidad de archivos

La alta gerencia debe definir los niveles de sensibilidad de los distintos archivos de datos. Habrá archivos que contendrán datos más sensibles que otros, lo cual hace necesario determinar los diferentes niveles de la misma (alta, media, baja) a causa de adecuar el peso (y costo) del control que ejerce sobre ellos, según el riesgo que implique la posibilidad de su manipulación.

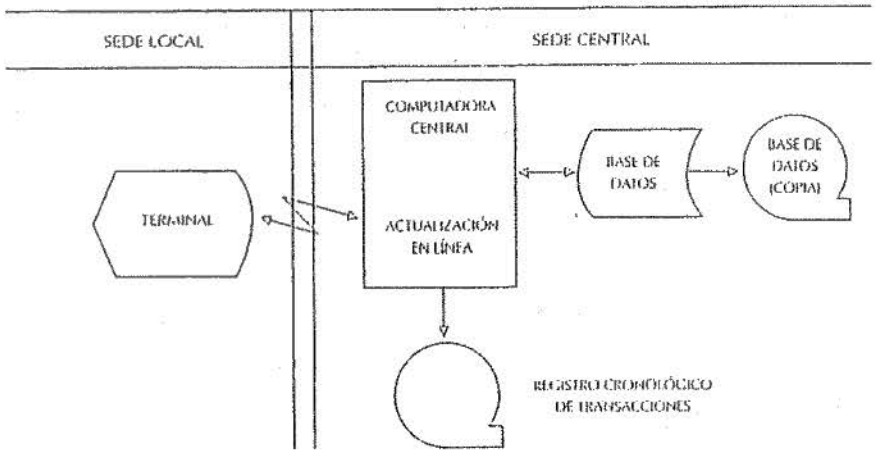

Figura 22-9. Procedimiento de seguridad a través de un registro cronológico de transacciones.

BENEFICIOS DE LA INTEGRACIÓN DE CONTROLES EN LOS SISTEMAS EN LÍNEA

Los objetivos generales de control que requieren las organizaciones se apoyan en los siguientes tipos de controles:

- Controles de exactitud.
- Controles de privacidad y seguridad.
- Controles de continuidad.
- Controles de condiciones ambientales o entorno.

Cuanto mejor sea la integración de estos principales tipos de control, mayor será el alcance de los objetivos generales del mismo. El concepto de integridad de los sistemas en línea se alcanza a través de la especificación de controles internos que caen dentro de las cuatro categorías de controles indicados más arriba.

La figura 22-10 muestra gráficamente el sentido de integridad de sistemas en línea. Se podría expresar que, si el nivel o extensión de los controles para cada una de las categorías mostradas es bajo, la magnitud del resultado de la integración (nivel de cumplimiento de los objetivos generales de control) será consecuentemente bajo. Por el contrario, si la política de la organización se orienta a elevar el nivel de controles, la integridad del sistema de control se elevará. La "ganancia" en integridad del sistema representa una medida de "retorno de inversión" en controles, y el costo de los controles representa la inversión en alcanzar la integridad esperada.

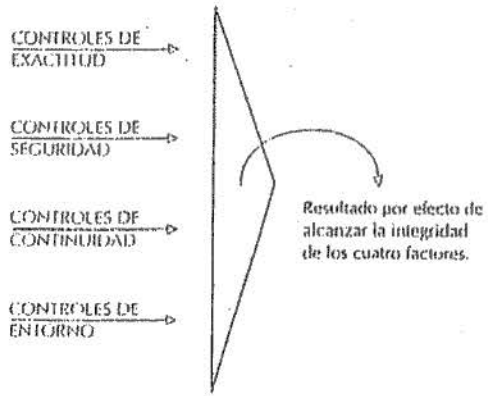

Figura 22-10. Representación gráfica del concepto de "integridad de los sistemas".

Por lo tanto, los sistemas en línea son particularmente dinámicos: no basta entonces con alcanzar una integridad estática. En consecuencia, debemos incorporar el ingrediente dinámico a la integridad de los sistemas en línea para asegurar que ésta se mantenga ante condiciones de cambio. Entonces, el diseñador de sistemas y el auditor de sistemas deberán trabajar juntos y construir los elementos para dotar a los sistemas de una quinta condición o categoría de control: la capacidad de "auditabilidad". Esto implica la capacidad de permiso para cumplir funciones de auditoría. Asimismo, esta condición acrecentará el nivel de integridad de los sistemas en línea. La figura 22-11 (*véase* pág. 327) muestra gráficamente la manera en que se eleva ese nivel.

La "ganancia", a causa de la integración de los controles de los sistemas, puede verse como la imagen inversa de la reducción de la exposición al riesgo.

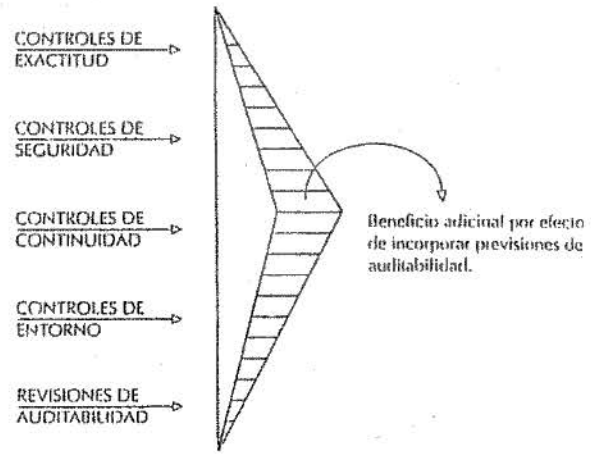

Figura 22-11. La incorporación de la capacidad de auditabilidad eleva el concepto de integridad de los sistemas.

Las condiciones de integridad mencionadas, con la incorporación de las previsiones de auditabilidad, toman en consideración no sólo las necesidades específicas de auditoría de sistemas sino también las funciones de administración de bases de datos, administración de seguridad y de aseguramiento de calidad. Dentro del concepto de integridad con auditabilidad se encuentran los temas asociados con la capacidad de los sistemas para informar sus situaciones anormales con respecto a la manera en que se comportan los controles internos, comparados con lo que se espera de ellos, con la existencia de pistas de auditoría, evidencias para auditoría y ciclos de retención de datos.

Controles internos en los sistemas en línea

En la sección anterior nos hemos referido al concepto de integridad de sistemas en línea. Uno de los métodos utilizados para medir el beneficio de la integridad consiste en fijar el grado de reducción de exposición al riesgo que puede surgir de la provisión de controles internos. En un ambiente de sistemas en línea, el propósito final de los controles internos es reducir la exposición al riesgo (o incrementar el nivel de integridad) a niveles aceptables para la organización, conforme a lo determinado por el análisis económico costo-efectividad.

En este sentido, el costo de implementar y aplicar controles internos representa una inversión y, por lo tanto, es de esperar un retorno de esa inversión si se aplican conforme a claras reglas de economía.

En el análisis que efectúe el auditor de sistemas se deben considerar las tres porciones en que se dividen los sistemas en línea. La figura 22-12 describe esta situación. Ese análisis contemplará las siguientes nuevas condiciones:

- La porción manual se ha ido reduciendo significativamente.
- La cantidad y naturaleza de evidencias ha cambiado.
- La porción no visible ha aumentado y las pistas de auditoría de transacciones y actualización de archivos no se manifiestan con facilidad.
- Los usuarios están localizados en lugares remotos y comparten la utilización de datos de la base de datos.
- La continuidad del sistema, sin interrupciones, se ha vuelto una vital importancia.

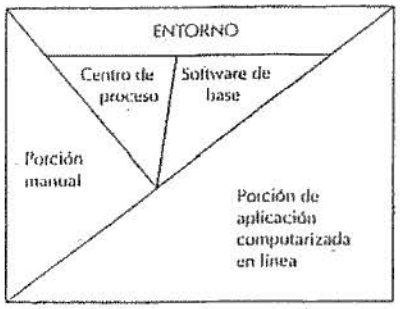

Figura 22-12. Porciones en que se dividen los sistemas en línea.

El diseño de controles internos se lleva a cabo mediante un proceso que pasa por varias etapas. Cada una de esas etapas debe satisfacer determinados requerimientos o responder a un determinado cuestionario. La primera etapa de este proceso consiste en identificar las amenazas potenciales a las que está expuesta la organización. Debe responderse a la pregunta: ¿Qué puede pasar?

La segunda etapa consiste en cuantificar el riesgo, es decir, estimar la frecuencia con que ocurre de la amenaza. Se debe contestar a la pregunta: ¿Con qué frecuencia?

La tercera etapa consiste en una estimación de tipo económico. La misma intenta cuantificar el costo o pérdida económica de la exposición al riesgo que puede derivarse como consecuencia de la materialización de la amenaza. La pregunta que debe responderse en este caso es: ¿Cuánto se podría perder si se concreta la amenaza?

La cuarta etapa se dirige hacia la definición de los objetivos de control. Las definiciones logradas en las fases anteriores sirven de base para el diseño de objetivos de control, los cuales orientarán a su vez la determinación de las técnicas que satisfacen esos objetivos. La pregunta en esta fase será: ¿Qué es lo que se debe satisfacer?

La quinta etapa cubre la fase de diseño y la selección de las técnicas de control que satisfacerán los objetivos ya determinados. La pregunta que corresponde a esta fase es: ¿Qué controles satisfacen los objetivos?

La sexta etapa, al igual que la tercera, también es de carácter económico. Cubre el análisis de la relación costo-eficacia y justificación. Significa que además de la justificación técnica debe encararse la evaluación económica de la aplicación de los controles diseñados y seleccionados. La pregunta pertinente es: ¿Podemos soportar los costos de los controles definidos?

AUDITORÍA DE VÍAS DE ACCESO LÓGICO

La figura 22-13 muestra los componentes de hardware y software que atraviesan la ruta lógica, mediante la cual un usuario puede acceder a una información en la medida en que los sucesivos controles se seguridad permitan ese acceso.

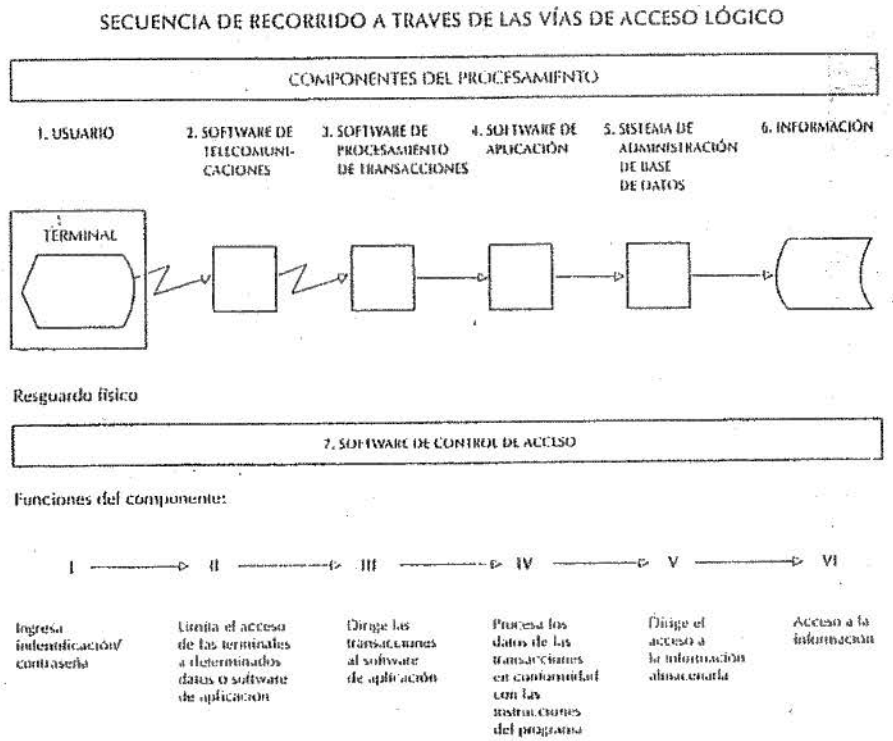

Figura 22-13. Secuencia de recorrido de los datos a través de las vías de acceso lógico.

El análisis de esta ruta es importante para el auditor de sistemas de información debido a la revisión del grado de seguridad que envuelve al procedimiento de acceso desde una terminal hasta la información almacenada.

En el cuadro de la figura 22-14 se analizan los principales aspectos que interesan al auditor con relación a cada una de las funciones señaladas en el cuadro de la figura 22-13.

COMPONENTE	INTERÉS DEL AUDITOR
1. Terminal	• Verificar la situación de seguridad física del dispositivo (ubicación en local aislado). Verificar que se cumplan las condiciones que deben satisfacer los códigos de identificación.
2. Software de telecomunicaciones	• Verificar que la Gerencia haya definido, para cada aplicación, las condiciones de accesibilidad con respecto a este software.
3. Software de procesamiento de transacciones	• Verificar el sistema de seguridad de identificación del usuario y del esquema (a través de tablas) de autorización de acceso a cada una de las aplicaciones.
4. Software de aplicación	• Verificar que las instrucciones de los programas de aplicación respondan a los objetivos del sistema.
5. Sistema de administración de base de datos	• Verificar que todos los elementos de datos que se procesen estén sujetos al sistema de seguridad de acceso lógico.

Figura 22-14. Aspectos de interés del auditor con respecto a las funciones de cada componente de un equipamiento para procesamiento y transmisión de datos.

El software de control de acceso cumple las siguientes funciones: identificación del usuario, restricciones de acceso lógico y registración en un *log* y emisión de un informe de accesos e intentos de acceso (con indicación de terminal, fecha, hora y archivo al cual se intentó acceder). Esta información sirve al auditor de sistemas para una revisión de seguridad.

Debido a que los controles de acceso se apoyan fundamentalmente en tablas de seguridad, el auditor de sistemas de información verificará, también, que el único que pueda tener acceso a las tablas sea el administrador de Seguridad.

DISEÑO DE CONTROLES INTERNOS EN LOS SISTEMAS EN LÍNEA

Con el objetivo de diseñar y relacionar los controles internos en los sistemas en línea, el diseñador debe detectar, para cada situación particular, la técnica específica de control que mejor se adecue a esa situación en especial. Pero para llegar a la determinación del control más adecuado se deben pasar por un conjunto de definiciones previas, que irán orientando sucesivamente al diseñador en su determinación.

En primer lugar, el diseñador de controles debe tener en cuenta que el propósito principal de los controles internos en los sistemas en línea es, como ya se explicó, reducir la probabilidad de exposición al riesgo.

En segundo lugar, el diseñador puede subdividir el sistema total en áreas de controles generales. Un área de control es un lugar físico, una entidad, un sujeto, una función o un objeto, respecto de los cuales pueden existir amenazas que causen exposición a riesgos y vulnerabilidad, las cuales deben ser sometidas a control para reducir la magnitud de la exposición potencial.

En los tradicionales sistemas de escaso procesamiento computarizado, en la modalidad en lote, las áreas de control se dividían en áreas de control de entrada, de procesamiento y de salida. En los sistemas en línea, más complejos, surge una mayor cantidad de áreas de control. El gráfico de la figura 22-13 muestra algunas de las áreas de control principales: entrada de datos (desde una terminal), telecomunicaciones, procesamiento de aplicaciones en línea, DBMS, software de control de accesos. Estas son las áreas en las que las amenazas y la exposición a riesgos tienen mayor probabilidad de ocurrir.

Dentro de cada área de control existen elementos de definición más específicos, en niveles de mayor precisión, a los cuales se denomina **Puntos de Control**. El diseño, selección y aplicación de controles debe efectuarse al nivel de **Puntos de Control**. Los Puntos de Control son elementos integrantes de las áreas de control, los cuales pueden sufrir varios tipos de amenazas, y cuyos controles a aplicar tienen alta probabilidad de satisfacer objetivos específicos de control y reducir, por lo tanto, la exposición a riesgos.

Obsérvese que las amenazas nos permiten conocer "qué es lo que puede ocurrir", y los Puntos de Control nos indican "dónde pueden hacerse efectivas". Sobre la base de ese conocimiento, es posible definir los objetivos de control, esto es: qué necesidades deben ser satisfechas. Debe tenerse particularmente en cuenta, por parte del diseñador de controles y luego por el auditor como revisor de esos controles (su calidad y su aplicación), que la determinación de qué es lo que se intenta satisfacer debe ser previa a la selección o prescripción de la batería de controles de posible aplicación.

RELACIONES ENTRE POLITICA, OBJETIVOS, ÁREAS, PUNTOS Y TÉCNICAS DE CONTROL

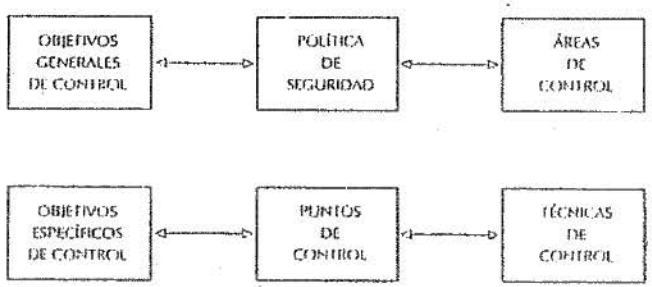

Figura 22-15. Relaciones entre política, objetivos, áreas, puntos y técnicas de control.

Con el propósito de definir la técnica de control más apropiada para cada situación, será necesario profundizar en la determinación de objetivos específicos de control, debido a que los objetivos generales no son lo suficientemente precisos como para cumplimentar los requerimientos de seguridad y confiabilidad de la organización.

La figura 22-15 (*véase* pág. 331) muestra las relaciones entre los conceptos arriba mencionados.

La distinción que se ha efectuado con respecto a estos conceptos, y a través de su definición, obedece a la necesidad de precisar su sentido y su ubicación dentro de los Manuales de instrucción de normas de control. El ejemplo que se incluye en el cuadro de la figura 22-16 ilustra los conceptos analizados en esta sección.

ESPECIFICACIÓN DE CONTROLES

Sistema: Pedidos de Ventas y Facturación
Área de control: Entrada de datos
Punto de control: Transacciones en línea
Objetivos generales de control:
Proveer y mantener exactitud, seguridad y pistas de auditoría para reducir las exposiciones derivadas de las siguientes amenazas: ingreso de transacciones erróneas o no autorizadas, pérdidas potenciales de transacciones, degradación de la base de datos, malas prácticas de corrección de errores.

OBJETIVOS ESPECÍFICOS DE CONTROL	TÉCNICAS DE CONTROL
• Cerciorarse de que únicamente sean admitidas las transacciones autorizadas en las operaciones en línea.	• Catalogar todos los tipos de transacciones que el sistema está autorizado a aceptar. Revisar que estas transacciones sean aprobadas por autoridad pertinente. • Catalogar las transacciones aprobadas contra la identificación de los operadores autorizados para ingresarlas.
• Asegurar la razonabilidad de cada transacción.	• Comparar los valores de los datos con una tabla que contenga valores normales.
• Asegurar la consistencia interna de los datos de cada transacción.	• Analizar si los datos son alfabéticos, cuando corresponda, y numéricos, cuando deban serlo. • Revisar anomalías en la estructura de los datos.

Figura 22-16. Modelo de especificación de controles (Sistema de Pedido de Venta y Facturación).

Seguridad en el área de control de transmisión de datos

En la sección anterior hemos explicado los conceptos de áreas de control, punto de control, objetivos generales de control, objetivos específicos de control y técnicas de control. También se analizaron las relaciones entre los mismos. Por otro lado, en la figura 22-13 se mostró esquemáticamente la secuencia de recorrido de datos a través de las vías de comunicación, y se señalaron las áreas de control.

En la presente sección se abordará específicamente el área de control "Transmisión de Datos" (telecomunicaciones). Los datos ingresan en el área de control "Transmisión de Datos" provenientes del área "Entrada de Datos" (dispositivo de *data entry* o terminal) y avanzan hasta que los datos transmitidos ingresan en la siguiente área de control: "Procesamiento de Transacciones". La figura 22-17 muestra gráficamente los puntos de control del área "Transmisión de Datos". Los objetivos generales de control dentro de esta área se muestran a continuación (figura 22-18)

PUNTOS DE CONTROL DEL ÁREA TRANSMISIÓN DE DATOS

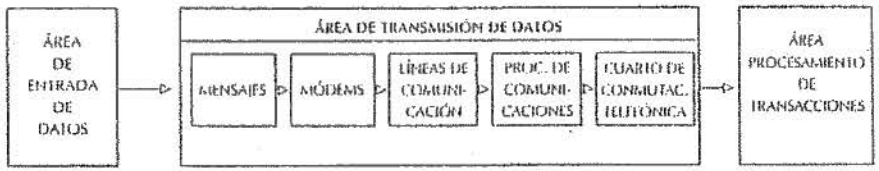

Figura 22-17. Esquema de puntos de control del área transmisión de datos.

ÁREA DE TRANSMISIÓN DE DATOS

PUNTO DE CONTROL	OBJETIVOS GENERALES DE CONTROL
• Transmisión de mensajes	• Asegurar exactitud, integridad y efectividad en la transmisión de datos. • Manejar de manera eficaz la corrección de errores en los mensajes.
• Módems	• Proveer continuidad de las operaciones.
• Líneas de comunicación	• Proveer seguridad y privacidad en la comunicación de datos. • Minimizar el riesgo de intromisiones indebidas en las líneas. • Mantener la continuidad de la línea y minimizar las interrupciones.
• Procesador de comunicaciones	• Proveer condiciones ambientales adecuadas y controles para asegurar las operaciones.
• Cuarto de conmutación de comunicaciones telefónicas.	• Restringir el acceso al conmutador telefónico.

Figura 22-18. Modelo de objetivos generales de control (área transmisión de datos).

Los objetivos generales de control deben traducirse en objetivos específicos de control, debido a que sus técnicas se aplican a nivel de objetivos específicos. Por tal motivo, se analizarán estos últimos en los párrafos siguientes (*véanse* figuras 22-19 a 22-23 respectivamente).

TÉCNICAS DE CONTROL APLICABLES AL PUNTO DE CONTROL

Transmisión de mensajes

Objetivos específicos

1) Asegurar que cada mensaje sea transmitido una sola vez y que su transmisión sea completa y exacta.
2) Confirmar la recepción de los mensajes por parte del destinatario conforme a la intención de su emisor.
3) Confirmar la recepción de una cantidad de mensajes que sea igual a la cantidad de mensajes emitidos.

Técnicas de control

1) Aplicar un criterio de numeración consecutiva de mensajes o transacciones. Asignar un número tanto a los mensajes que ingresan como a los que egresan.
2) Asegurarse de que en ambas sedes (de emisión y de destino) se efectúan controles de secuencia de mensajes transmitidos. Identificar y analizar errores de secuencia.
3) Verificar que, en caso de caída del sistema (interrupción), se controle que los mensajes no sufran solapamiento o queden truncados.
4) Colocar en fila de espera un mensaje únicamente después de recibir la señal de "fin de mensaje" o "fin de transmisión". Utilizar estos indicadores.
5) Registrar fecha y hora de los mensajes, a fin de facilitar un posterior rastreo.
6) Utilizar mecanismos de control para detectar errores, tales como bit de paridad.
7) Utilizar "encabezamiento" de mensajes y aplicar programas de computación para determinar su aceptabilidad.
8) Aplicar la verificación de recepción completa de mensajes a través de *Echo-checks*: significa que una parte del mensaje se devuelve a su origen, lo cual supone que el mensaje se recibió completo.
9) Conciliar la cantidad total de transacciones, por terminal y por día, a través de totales de control basados en valores (pesos, dólar, etc.), conteo de mensajes, etc. Estos valores se mantendrán en el área de origen y luego se cotejarán a través de controles propios del sistema.

Figura 22-19. Modelo de objetivos específicos de control (Punto de control: transmisión de mensajes).

TÉCNICAS DE CONTROL APLICABLES AL PUNTO DE CONTROL

Módems

Objetivos específicos

1) Minimizar las posibilidades de interrupción de las comunicaciones motivadas por fallas en los módems.
2) Garantizar la correcta utilización de los módems.

Técnicas de control

1) Utilizar módems con capacidad para detectar el mal funcionamiento.
2) Disponer de módems de reserva en áreas clave de la red.
3) Evitar la divulgación de los números telefónicos anexados a los módems. Cambiar periódicamente los números de líneas conectadas a módems.

Figura 22-20. Modelo de objetivos específicos de control (Punto de Control: módem).

TÉCNICAS DE CONTROL APLICABLES AL PUNTO DE CONTROL

Líneas de comunicación

Objetivos específicos

1) Neutralizar el riesgo de intercepción de líneas, a fin de evitar:
   - La inserción, a través de la línea, de transacciones falsas.
   - La captación electromagnética de señales de mensajes transmitidos.
   - La captación de información confidencial.
   - El conocimiento indebido de contraseñas o del código de identificación personal para ser usado indebidamente.
   - La grabación magnética del *sign-on* (señal de comienzo de una transmisión) para utilizar posteriormente esta grabación a fin de ingresar en el sistema y efectuar transmisiones simulando al legítimo usuario (esta técnica se denomina *spooling*).
2) Frustrar el uso de contraseñas falsas.
3) Minimizar la posibilidad de acceso indebido. Asegurar la autenticidad del usuario.
4) Asegurar la continuidad de la línea. Evitar discontinuidad por fallas o roturas provenientes de insuficiencia de mantenimiento.
5) Proveer la grabación de mensajes.
6) Asegurar, desde la terminal, el control sobre las operaciones del software de comunicaciones.
7) Documentar las actividades y proveer pistas de auditoría.

Técnicas de control

1) Encriptar los códigos de identificación personal.
2) Evitar el acceso a la computadora a través de llamada telefónica directa; utilizar el mecanismo de devolución de llamadas (*call-back*) cuando la comunicación proviene de una terminal.
3) Utilizar contraseñas algorítmicas en ocasiones en que el sistema transmite datos al azar. (Estas contraseñas se cotejan con la respuesta producida por la computadora, dado que el algoritmo no viaja a través de la línea, por lo tanto no puede ser interceptado). Un ejemplo de contraseña algorítmica puede ser el siguiente:

   El sistema envía al usuario tres dígitos seleccionados al azar, que aparecen en la pantalla, por ejemplo:

A	B	C
6	4	2

   El algoritmo, solo conocido por el usuario es:

$$X = A - B + C$$

   Entonces:

$$X = 6 - 4 + 2 = 4$$

   El usuario responde (digita): 4

   El programa computarizado aplica la misma operación y compara la respuesta. Debido a que que los dígitos son seleccionados al azar, la contraseña es siempre diferente y no se relaciona directamente con los registros anteriores.
4) Si los dispositivos lo permiten, efectuar conmutación de mensajes de una terminal a otra, en caso de caída de líneas de una de las terminales.
5) Asegurar que exista suficiente documentación acerca del sistema de comunicación y de su software, y que la misma sea compatible con la instalación en uso.
6) Analizar la posibilidad de fragmentar mensajes en partes, durante una transmisión sensible, y proceder luego a la integración del mensaje total.
7) Insertar los cables vulnerables dentro de paredes o contenedores blindados.
8) Mantener registros de transacciones (*logging*) para verificar si todos los mensajes son bien recibidos o si algunos se pierden. En caso de detectar errores de transmisión, registrar la identificación de la terminal de origen, el código de operador, fecha y hora. Registrar, también, el comienzo y fin de programas, mensajes de fallas de hardware, señales de comienzo y fin de programas, inconsistencia de encabezamientos de mensajes. Analizar las inconsistencias registradas.
9) Separar las funciones de administración de las redes de comunicación de las funciones de operación de la computadora terminal.
10) Desalentar las intenciones de interceptar mensajes durante la transmisión enviándolos en forma "distrazada", dificultando, así, su reconstrucción por parte del interceptor. O bien, codificar porciones clave del mensaje, con el mismo propósito.
11) Verificar la identidad del usuario en el caso de transmisiones sensibles, haciéndole una pregunta de tipo personal; por ejemplo, fecha de nacimiento de su hijo mayor. De esta manera sólo él podrá responder. Si esta reautenticación del usuario no se cumple, ello hace pensar que un impostor ha interceptado la línea, reemplazando al operador legítimo.
12) Mantener reserva acerca de los números de líneas telefónicas utilizadas para la transmisión de datos. Cambiar periódicamente esos números.
13) Asegurarse que, en caso de interrupción del servicio por corte de energía, existan reservas para el mantenimiento en actividad del procesador de comunicaciones y concentradores remotos.

Figura 22-21. Modelo de objetivos específicos de control
(Punto de Control: líneas de comunicación).

TÉCNICAS DE CONTROL APLICABLES AL PUNTO DE CONTROL

Procesador de comunicaciones

Objetivos específicos

1) Impedir el acceso a personas no habilitadas al área del procesador de comunicaciones.
2) Minimizar la posibilidad de que se exponga al software de comunicación a modificaciones fraudulentas.
3) Proteger los equipos del peligro de siniestros que puedan afectar su integridad.

Técnicas de control

1) Mantener cerrada el área del procesador de comunicaciones con cerraduras adecuadas. Aplicar mecanismos de autorización de acceso.
2) Mantener permanentemente actualizada la lista del personal autorizado a acceder (en forma permanente) al área del procesador de comunicaciones. Llevar registros del personal que transitoriamente ingresa o egresa del área (técnicos de mantenimiento, proveedores, etc.).
3) Aplicar las técnicas de Auditoría de Sistemas durante el ciclo de desarrollo de sistemas. Establecer mecanismos de autorización para los requerimientos de modificaciones de los programas.
4) Verificar que en todos los casos se apliquen los programas versión "objeto" derivados de los correspondientes programas versión "fuente" legítimos.
5) Instalar dispositivos de protección (detección de humo, mecanismos de corte automático de energía, etc.).
6) Prever planes de recuperación en caso de emergencias.

Figura 22-22. Modelo de objetivos específicos de control
(Punto de control: procesador de comunicaciones).

TÉCNICAS DE CONTROL APLICABLES AL PUNTO DE CONTROL

Procesador de comunicaciones

Objetivos específicos

1) Limitar el acceso al conmutador telefónico.

Técnicas de control

1) Destinar un lugar físico para cumplir exclusivamente la función de conmutación.
2) Exigir identificación de acceso y permitir el mismo solamente al personal autorizado.
3) Mantener los registros de códigos de comunicaciones en lugares reservados, sólo accesibles al personal autorizado.

Figura 22-23. Modelo de objetivos específicos de control
(Punto de control: cuarto de conmutación).

Causantes de violaciones contra el acceso lógico: el delito informático

En abril de 1994, una noticia publicada en diferentes periódicos causó gran conmoción en los habitantes de todo el país y, en particular, en los de la Ciudad de Buenos Aires. La misma daba cuenta del siguiente hecho: "Según se informó oficialmente, superaría los $ 300.000 la suma sustraída a bancos oficiales y privados por medio de microcomputadoras"[5].

La estafa, sin precedentes en el país, se concretó a través de los accesos que los bancos asignan a sus clientes para manejar las cuentas corrientes. La maniobra delictiva se perpetuó de la siguiente manera:

1. Mediante computadoras personales conectadas por módem a líneas telefónicas, los delincuentes ingresaron en el sistema informático del Banco Central.
2. A través de claves, procedimientos operativos y rutas de acceso, suministradas por un entregador, llegaban hasta los registros que manejan el *clearing* de todo el país.
3. Monitoreando por esa vía los registros, transferían electrónicamente, a diferentes cuentas de otras importantes firmas locales, valores de varias empresas depositados en bancos de nuestro país, evitando que las abultadas cifras en juego despertaran sospechas.
4. Luego, esos fondos eran girados a cuentas particulares en Estados Unidos de Norteamérica y Europa, donde quedaban disponibles para su retiro.

Como se observa de la relación anterior, la maniobra debe contar con la complicidad de alguien del banco damnificado. No es suficiente contar con la clave; son varios los pasos a seguir para llegar al corazón de la red. El caso relatado ha sido uno dentro una larga serie de delitos informáticos perpetrados desde hace muchos años en todo el mundo.

El auditor de sistemas de información deberá conocer en profundidad las posibles causas de exposiciones a riesgos de acceso lógico y las causantes de las violaciones. Entre estos últimos, existen los siguientes:

- *Hackers*: son piratas informáticos que desean demostrar su habilidad para burlar los controles y acceder a información reservada. Su propósito no es, por lo general, destruir la información, pero el resultado puede ser ése.
- *Crackers*: son piratas informáticos contratados por un tercero.
- *Phrackers*: son piratas informáticos que intentan ingresar en el sistema de comunicaciones.
- Personal de sistemas de información: las buenas medidas de prevención aconsejan la separación de funciones para evitar que una sola persona conozca la totalidad de los elementos que integran un proceso.
- Ex empleados que conozcan claves y rutas de acceso.

[5] *Diario La Nación*, 29 de abril de 1994, pág. 20.

Las técnicas más usuales para cometer delitos mediante el uso de computadoras son las siguientes:

- Alteración de datos: se realiza antes de que se active el sistema de protección de datos. Es la modificación de datos antes o durante su ingreso en las computadoras: cualquier persona que intervenga en los procesos de creación, grabación, traslado, codificación, revisión y transformación puede alterar los datos.
- *Superzapping*: es un procedimiento que contiene un programa que puede burlar todos los controles y acceder, así, a información almacenada en equipos de computación para modificarla.
- Caballos de Troya: consiste en el ingreso, en forma encubierta, dentro de un programa autorizado de un grupo de instrucciones con fines maliciosos. Tales instrucciones ocultas –no autorizadas– se ejecutarán cuando se ejecute el programa autorizado. Un ejemplo sería incluir, en un programa de liquidación de sueldos, una rutina que se ocupe de quitar pequeñas sumas de dinero al resultado de cada liquidación correcta, y acreditarla en una cuenta que beneficie indebidamente a un tercero.
- Técnica del salame: consiste en retirar pequeñas cantidades de los importes de las transacciones o cuentas computarizadas en forma automatizada.
- Redondeo por defecto: consiste en aplicar una rutina computarizada que redondea importes hacia abajo y envía los mismos a una cuenta no autorizada.
- Virus informáticos: son programas que se desplazan de computadora a computadora, es decir, se autoduplican, y pueden hacer desaparecer los datos almacenados o dañarlos seriamente. El desplazamiento de programas puede realizarse mediante el traspaso de *diskettes* entre varias computadoras, o también por medio de la transmisión a través de líneas de telecomunicaciones. A veces un virus puede permanecer inactivo durante un tiempo hasta que un determinado acontecimiento (una fecha) active su poder destructivo.
- Gusanos: son similares a los virus –destruyen datos u ocupan recursos de computación– pero no se duplican como los virus.
- Puertas traseras: son instrucciones insertas maliciosamente en un programa autorizado con la intención de permitir la introducción de rutinas no autorizadas.
- Ataque asincrónico: las líneas de telecomunicaciones por donde viajan los datos son asincrónicas (en una sola dirección por vez). De ahí que algunas transmisiones deban esperar (antes de ser transmitidas) que la línea esté libre para que los datos fluyan en la dirección adecuada. Los datos que están en espera de su transmisión quedan expuestos al delito denominado "ataque asincrónico": son susceptibles a accesos no autorizados.
- Ingreso a caballito de otro (*Piggy-backing*): consiste en conectar una línea de comunicaciones a la computadora autorizada para interceptar los datos de la transmisión, y así alterarlos.
- Fuga de datos: consiste en extraer información del equipo de computación.

Controles de accesos físicos

Además de la revisión de la seguridad de accesos lógicos, el auditor de sistemas de información deberá analizar las rutas de ingreso físico para establecer el grado de exposición a riesgos, como también el nivel de protección de los controles diseñados y aplicados.

El auditor de sistemas debe considerar que la protección debe alcanzar a toda la organización: a la sede de la computadora central, a las redes remotas y también a los centros y procedimientos sujetos a regímenes de alquiler (*leasing* o compartidos). Los elementos de control físico que debe analizar el auditor son los siguientes:

- Cerraduras: la utilización de llaves metálicas constituye el medio más sencillo para proteger bienes. Sin embargo, la tecnología ha posibilitado el desarrollo de recursos más sofisticados para limitar los accesos físicos, creando dispositivos, tales como el teclado numérico, que exigen el conocimiento de una clave para liberar el paso. En el primer caso, el auditor verificará la existencia o no de llaves duplicadas y también en poder de quién se encuentran las mismas. En el segundo caso, verificará que las claves sean modificadas periódicamente y que se mantenga reserva de las mismas. La tecnología más moderna utiliza tarjetas magnéticas como elemento que permite el acceso físico a través de la operación de pasar la tarjeta por un sensor electrónico que activa el mecanismo de cerradura de puerta. Esta tecnología más sofisticada permite incorporar a la tarjeta diferentes alternativas: identificar a la persona, restringir el acceso a determinadas puertas o en determinados horarios, desactivar el permiso de entrada si fuera necesario. El auditor deberá revisar la gestión administrativa que se persigue con respecto al otorgamiento y mantenimiento activo de estas tarjetas. Para la protección de locales que contengan elementos de extrema confidencialidad pueden utilizarse cerraduras biométricas de puertas: actúan tras la verificación de características corporales tales como huellas dactilares, mapa de retina y voz.

Capítulo 23

Seguridad en los sistemas de base de datos

Introducción

El concepto de base de datos ha sido utilizado generalmente para describir la disponibilidad de un gran volumen de datos.

En su acepción más moderna de tecnología informática, la "base de datos" es descripta como un gran archivo de datos que se enlazan, interrelacionan y se controlan por medio de un software específico denominado DBMS. La figura 23-1 (*véase* pág. 342) muestra el mecanismo de funcionamiento de un DBMS y sus relaciones con la entrada y la salida de los mismos.

En la práctica, este software, que actúa como controlador de programas de operación, establece una referencia cruzada, a fin de que, mediante el conocimiento de una clave de identificación común, un programa de aplicación pueda acceder a cualquier registro almacenado en la base de datos, independientemente del archivo en que se encuentre. La figura 23-2 (*véase* pág. 343) otorga una idea acerca del funcionamiento de esta técnica.

La aplicación de sistemas de bases de datos presenta ventajas indiscutibles con respecto a la gestión de datos a través de archivos convencionales, pero también trae aparejadas nuevas causas de riesgo.

Entre las ventajas, pueden citarse las siguientes:

1. Cada elemento de dato se ingresa y almacena una sola vez; por lo tanto, las necesidades de capacidad de almacenamiento pueden ser menores.
2. Al no existir redundancia de datos (éstos se registran una única vez), la información es consistente para toda la empresa, más allá del sector que consulte el dato y del objetivo que se persiga con el mismo.
3. El proceso de actualización de los elementos de datos se efectúa una sola vez. Esto también ayuda a preservar la consistencia de la información.
4. Las aplicaciones pueden ser relativamente independientes de los datos, de manera que la programación no necesita conocer la estrategia física de los mismos. Esa estructura

puede cambiarse o añadirse sin tener que modificarse todos los programas involucrados. Por lo tanto, se reduce el costo de mantenimiento.

5. Debido a que existe mayor verificación y control, mayor es la integridad de los datos.
6. Se obtiene una mejor definición en cuanto a responsabilidad y posesión de los datos (en algunos casos recaen en el administrador de la Base de Datos).

ESQUEMA DEL SISTEMA DE GESTIÓN DE BASE DE DATOS

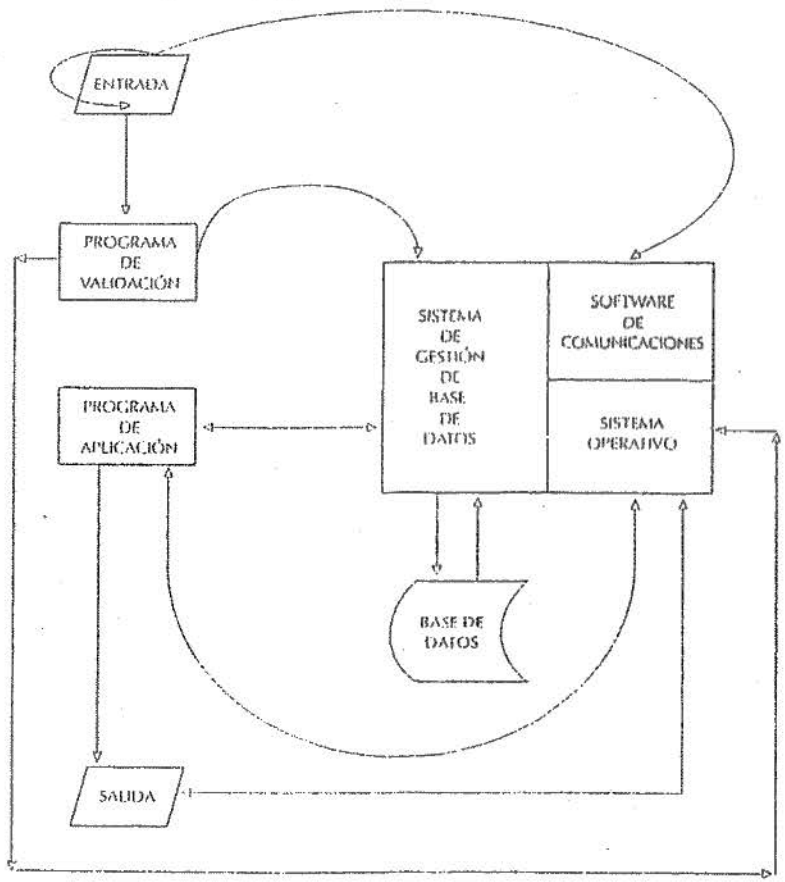

Figura 23-1. Esquema de un sistema de gestión de Base de Datos.

ESQUEMA DE FUNCIONAMIENTO DE UNA BASE DE DATOS

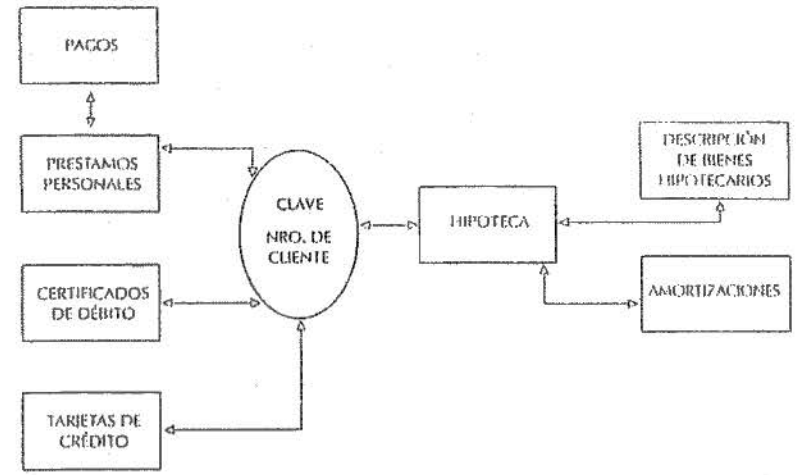

Figura 23-2. Esquema de funcionamiento de un sistema de Base de Datos.

A pesar de las ventajas señaladas más arriba, las bases de datos presentan problemas que afectan la seguridad y el control en el procesamiento de la información (tema que interesará a los diseñadores y, particularmente, a los auditores de sistemas de información). Algunas de las desventajas se analizan a continuación:

1. Al mantener almacenado en una base de datos centralizada un volumen importante de la información de la empresa, aumenta la vulnerabilidad de la misma. Las operaciones de la empresa pasan a depender en mayor medida de su base de datos (concentración de información), en vez de hacerlo de archivos aislados e independientes en los cuales la misma información podría encontrarse repetida varias veces.
2. Si no existiera la base de datos, un programa de aplicación podría acceder únicamente a la información almacenada en los archivos específicos involucrados en esa aplicación, pero el riesgo sobre acceso indebido sería menor. El sistema de base de datos no cuenta con los "controles de biblioteca" sobre los archivos, pero sí permite (si no se le incorporan otros controles) el acceso ilimitado a cualquier archivo en cualquier momento.
3. La existencia de sistemas de bases de datos complica el desarrollo de archivos adecuados de respaldo con el propósito de recuperación. El medio en el que se mantiene la base de

datos no permite un procedimiento fácil de respaldo tipo "abuelo-padre-hijo" tradicional. Las operaciones de respaldo son más costosas.

4. Por causa de la utilización del software de gestión de base de datos, la empresa sufre el agregado de otros programas, además de los que componen el sistema operativo. Estos nuevos programas también quedan sujetos a la posibilidad de que se produzcan nuevos tipos de violaciones por parte de usuarios y programadores.
5. Debido a que diferentes sectores de una organización pueden utilizar los mismos datos de la base, surge el problema de tener que definir qué usuario será el responsable de su mantenimiento y actualización (suele asignarse esa responsabilidad a la función de administrador de Base de Datos).
6. El DBMS se sitúa entre el sistema operativo y el programa de aplicación. Este añade un paso más de trabajo previo que requiere tiempo de ejecución y una mayor ocupación del área de memoria. O sea que se presenta un problema de lentitud de respuesta que puede afectar la capacidad productiva de la computadora. Los registros requeridos por una aplicación específica pueden encontrarse físicamente ubicados en zonas muy distantes dentro de los archivos. No obstante, frente al avance de la tecnología, las actuales velocidades de procesamiento pueden llegar a relativizar este problema.
7. Pueden presentarse situaciones de operación en las que se generen errores que surjan de dos intentos simultáneos de acceso a la base de datos.

EL CONCEPTO DE ESQUEMA Y SUBESQUEMA

Para comprender cómo funciona un DBMS es necesario comprender el concepto de esquema y subesquema. En primer lugar, recordemos que un DBMS no elimina la necesidad de los programas de aplicación. El DBMS es un puente entre el programa de aplicación (que determina qué datos procesará) y el sistema operativo (cuya función es ubicar esos datos en los dispositivos de almacenamiento).

Un esquema define y describe una base de datos incluyendo el enunciado de las características de los datos y las relaciones entre los diferentes elementos de los mismos. Un subesquema define la porción de la base de datos que utilizará un programa específico. Consta de nombres y descripciones de los datos y se constituye como un subconjunto del esquema.

Para cada base de datos existe un único esquema, pero también pueden existir varios subesquemas. Cada aplicación de sistemas de información que utilice la base de datos puede tener un subesquema diferente. La figura 23-3 proporciona una explicación del funcionamiento del DBMS.

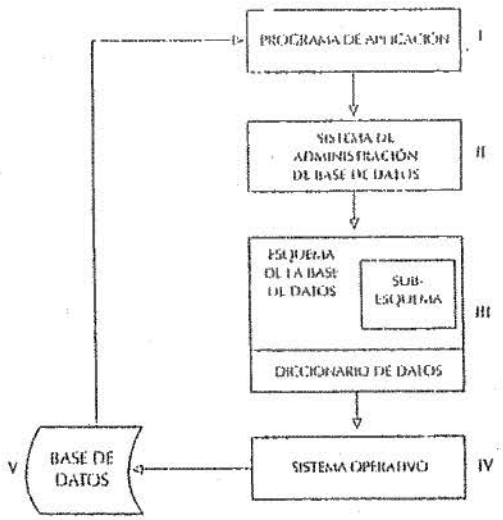

Figura 23-3. Descripción gráfica de un esquema y subesquema de un DBMS.

Acompañaremos la explicación con una descripción de la función de cada módulo.

1. El programa de aplicación define qué datos necesitará para procesar; luego, lo comunicará al DBMS.
2. El DBMS verifica la consistencia de los datos determinados con los contenidos en el esquema. Los datos solicitados se definen en el subesquema.
3. El DBMS instruye al sistema operativo para que éste ubique y recupere los datos de la localización específica de los medios de almacenamiento (normalmente discos).
4. El sistema transmite una imagen de los datos a los programas de aplicación para que éstos ejecuten el procesamiento.

DIFERENCIA ENTRE CONTROLES APLICABLES A SISTEMAS DE ARCHIVOS INDIVIDUALES Y SISTEMAS DE BASE DE DATOS

El auditor de sistemas de información debe observar que, si bien existen procedimientos de control que son aplicables a ambos métodos de tratamiento de archivos, también existen diferencias que deben ser consideradas. En los párrafos siguientes se explicarán algunas de las diferencias.

1. Controles generales sobre desarrollo y mantenimiento de programas

Algunos controles básicos, tales como aprobación de solicitudes de modificaciones, revisión de documentación y procedimientos de prueba y revisión de copias de resguardo y recuperación, se aplican a ambos métodos. Sin embargo, un sistema de base de datos requiere de controles adicionales. En sistemas de archivos individuales, los cambios en programas son generalmente dirigidos a la revisión de las operaciones lógicas ejecutadas sobre el archivo; por ejemplo, reestructurando el programa para incrementar su efectividad o corrigiendo un error de lógica no previsto con anterioridad. Los datos a los que puede tener acceso ese programa generalmente no cambian, porque el archivo está lógica y físicamente dedicado al programa.

Una revisión en el programa de liquidación de remuneraciones no cambiará los datos contenidos en el archivo de remuneraciones al cual accede ese programa, a menos que el archivo también sea reestructurado y modificado.

En un sistema de base de datos el programa opera sobre la base de datos, en vez de hacerlo sobre el archivo. El programa de aplicación contiene especificaciones que son procesadas a través del DBMS, para luego acceder a los datos requeridos. Una modificación en el programa de aplicación puede provocar un cambio en las operaciones lógicas ejecutadas sobre los datos, un cambio en los ítems de datos accedidos, o bien, ambas cosas. En consecuencia, los controles generales sobre los procedimientos de mantenimiento de programas, en un ambiente de base de datos, debe asegurar que cualquier cambio en las especificaciones de los programas de aplicación sea necesario y debidamente autorizado.

2. Efecto "cascada" de la modificación de un programa de aplicación

La posibilidad de acceder a diferentes ítems de datos, por parte de un programa de aplicación, puede causar un efecto cascada, puesto que un elemento de dato de la base de datos es probable que pueda ser accedido por varios programas de aplicación diferentes. Por ejemplo, un programa que actualiza datos del personal para empleados contratados, y cuyo término ha vencido, puede ser modificado para eliminar los números de empleados (legajos) que no permanecen más en la empresa. Este procedimiento puede ser usado para controlar la emisión de órdenes de pago de remuneraciones (o cheques) que pertenezcan a empleados que ya no son parte de la firma, o bien, para conservar datos históricos. Sin embargo, esta modificación puede causar también la destrucción de la relación lógica en la base de datos, entre "número de empleado" y "remuneraciones liquidadas en el año y hasta la fecha" a ese empleado, afectando, en consecuencia, otros programas de aplicación.

Por tales motivos, los controles generales sobre desarrollo y mantenimiento de programas son más críticos en un ambiente de base de datos que en un ambiente de archivos individuales. Como control adicional, las modificaciones de programas deben ser revisadas por el administrador de Base de Datos, debido a que se encuentra más familiarizado con todos los programas de aplicación.

3. Controles sobre el acceso a los datos

En un entorno de archivos individuales, los archivos dedicados a un programa de aplicación determinado necesitan estar en línea sólo cuando el programa se encuentra procesando esos archivos. Por lo tanto, los controles de acceso a datos en un sistema de archivos son, mayormente, de tipo organizacional. Por lo general, los archivos se encuentran almacenados en la biblioteca, y su utilización se realiza una vez que se ha ya programado (en el plan de corridas) que el respectivo programa de aplicación debe ser ejecutado. De manera que el acceso físico al archivo es controlado por el encargado de biblioteca –que es el depositario del archivo. Se trata de un control organizacional.

En un sistema de base de datos, el control sobre el acceso de datos es más dificultoso de alcanzar a través de medios físicos. La base de datos contiene datos para apoyar a varios programas de aplicación, el cual debe estar disponible en la computadora durante el procesamiento de todos los programas.

El control sobre el acceso a los datos, en un sistema de base de datos, se centraliza en la biblioteca del DBMS, cuando este sistema se encuentra en operación. El DBMS contiene información de seguridad con respecto a qué elementos de datos pueden ser accedidos por cada programa de aplicación.

Mientras el software del DBMS se está ejecutando, todo acceso a la base de datos se controla por medio de ese software. Sin embargo, el DBMS, como todo software, requiere mantenimiento, el cual puede ser programado o no programado. Cuando el software del DBMS se encuentra no operable (caído), la base de datos se mantiene en el sistema. Puede ser accedida, copiada o eliminada de la misma manera que cualquier otro dato, mientras el software del sistema se encuentra no operable. De manera que deben establecerse controles para prevenir todo acceso no autorizado a la base de datos cuando ésta no esté protegida bajo el control del DBMS.

4. Controles generales sobre organización y operaciones

Los controles, tales como las instrucciones de operación para cada programa, mantenimiento y revisión regular de un *log* (registro) del sistema y controles de acceso al sistema, son necesarios en ambas configuraciones (bases de datos y archivos individuales). Sin embargo, en un sistema de base de datos son necesarios controles adicionales. Todo cambio en la biblioteca del DBMS debe ser controlado por un responsable: el administrador de Base de Datos. Para acceder a la biblioteca, debe controlarse la utilización de programas utilitarios suministrados por el proveedor del sistema. Tales programas pueden ser utilizados para obtener conocimiento de la estructura física y de la visión lógica de la base de datos, mediante el análisis de la especificación de programas y de la descripción de la base de datos contenida en la biblioteca. Además, el *log* de la biblioteca del DBMS debe ser mantenido y revisado periódicamente por el administrador de Base de Datos. El *log* debe contener todos los agregados y cambios en la biblioteca del DBMS. Los procedimientos de control deben asegurar que los programas de aplicación accedan solamente a los elementos de datos respecto de

los cuales tienen autorización de acceso, y que todo cambio en la biblioteca sea debidamente autorizado.

CONTROLES RECOMENDABLES EN UN AMBIENTE DE BASE DE DATOS

Si bien se han explicado algunos conceptos básicos sobre los controles aplicables, a continuación se comentarán, de manera más metódica y detallada, las técnicas para su aplicación.

Los procedimientos de control en el diseño y aplicación de sistemas de base de datos pueden agruparse en las siguientes categorías:

1. Separación de responsabilidades.
2. Acceso a los datos.
3. Operaciones.
4. Programas de aplicación.
5. Selección del DBMS.

A continuación analizaremos las características de estos grupos.

1. Separación de responsabilidades

La necesidad de segregación de funciones entre programadores de aplicación, analistas de sistemas y operadores se mantiene equivalente a la que existe respecto de sistemas de archivos individuales. Pero deben agregarse algunos controles de organización adicionales. Un administrador de Base de Datos debe ser responsable de la definición, organización, protección, eficiencia y control de la base de datos. El administrador de Base de Datos cumple esas funciones asesorando a la Gerencia en la selección del hardware y software, planificando la estructura de la base de datos, documentando su contenido, consultando con los usuarios sobre la organización y métodos de recupero, estableciendo procedimientos de seguridad y procedimientos de recuperación ante la eventual destrucción de la base de datos y monitoreando el uso de la misma.

Los controles de organización que surgen cuando existe el administrador de Base de Datos, incluyen:

a) El administrador de Base de Datos podrá tener acceso a la sala de computación únicamente con autorización de la supervisión; no estará autorizado a operar el equipo. Ya que el administrador de Base de Datos es la única persona que tiene completo conocimiento del contenido de la biblioteca del DBMS y de todos los programas de aplicación, éste podría, con facilidad, obtener acceso y manipular cualquier elemento de dato en la base de datos.
b) Solamente el administrador de Base de Datos debe tener la autorización para efectuar cambios en la biblioteca del DBMS.

c) El administrador de Base de Datos no debe estar habilitado para iniciar transacciones (ingresar datos de transacciones) sin la aprobación del usuario. Tampoco podrá ejercer control de decisión sobre los activos de la empresa.
d) El programador de aplicaciones debe conocer únicamente la información de la especificación del programa que esté relacionada con los programas de los cuales es el responsable. Un programador de aplicaciones no tiene necesidad de conocer ningún dato de la base que no esté directamente relacionado con su aplicación. Este tipo de control es necesario tanto en los sistemas de archivos individuales como en los sistemas de bases de datos, pero es más crítico en este último debido a que el control físico sobre los datos es más difícil de alcanzar.

A efectos de la aplicación del principio de separación de funciones, la preparación de los datos que componen los subesquemas, al igual que su mantenimiento, no debe corresponder al programador de la aplicación sino al administrador de la Base de Datos. De la misma manera, las limitaciones a las actividades que pueden realizar los programas deben ser especificadas por el administrador de Base de Datos y no por el programador de aplicaciones.

2. Acceso a los datos

A causa de que los controles físicos y organizacionales sobre el acceso a los datos es menos factible en un ambiente de base de datos, se vuelve necesario contar con controles adicionales, entre los que se sugieren los siguientes:

a) Debe verificarse que los DBMS permitan que un programa acceda solamente a determinadas áreas de la base de datos. Estas áreas se definen en un subesquema para cada programa. Además, estos sistemas deben limitar la acción de los programas a una o más de las siguientes operaciones (niveles de restricción): dar altas a elementos de datos, dar bajas, actualizar, o sólo leer.
b) El acceso de programas utilitarios (son aquellos que realizan funciones básicas de procesamiento, independientemente de los programas de aplicación) a la biblioteca del DBMS, debe ser adecuadamente controlado a través del administrador de Base de Datos. Un programa utilitario puede, por ejemplo, listar la descripción de la base de datos, accediendo indebidamente a la divulgación de información que puede ser reservada. El administrador de Base de Datos debe controlar el uso de los programas utilitarios. (Por ejemplo, el programa de carga inicial de la base de datos y el de compresión de elementos de datos eliminados de la base.) Esto es así porque el administrador de Base de Datos es quien tiene pleno conocimiento de la estructura de la base. Este control asegura que el mantenimiento de la base de datos sea apropiado y autorizado.
c) Deben existir procedimientos adecuados para prevenir el acceso a la base de datos en momentos en que la misma no se encuentre bajo control del software del DBMS. Mientras este software se mantiene no operable, la base de datos física aún existe en el sistema y debe ser protegida.

d) El *log* del sistema operativo y el DBMS debe ser revisado por el administrador de Base de Datos. Esta revisión debe determinar si la base de datos fue accedida sólo bajo el control del DBMS, si los programas han sido autorizados, y si se ha actuado conforme a un plan de tareas. Esta revisión será posible únicamente si es apoyada por un software que resuma estos *logs*.

e) La base de datos activa (la que se utiliza regular y habitualmente) debe ser separada de la base de datos utilizada para prueba de programas. Este control asegura que la base activa no corra riesgo de ser contaminada durante esas pruebas.

f) Protección contra actualizaciones duplicadas. En los sistemas que utilizan bases de datos puede ocurrir que, en un mismo momento, dos o más programas intenten acceder a la vez a la misma serie de datos. Para evitar las dificultades que esta situación pudiera provocar, el DBMS debe prever la asignación de un orden de prioridades con respecto a los programas y a los usuarios. De esta manera, habría programas y usuarios de alta y baja prioridad. El sistema debería prever la situación que se presentaría cuando el intento de acceso corresponda a dos usuarios que tengan la misma prioridad.

3. Operaciones

Varios de los controles aplicables a los sistemas de archivos individuales son también aplicables a los sistemas de base de datos. Sin embargo, existen otros controles adicionales aplicables en un ambiente de base de datos, de modo que se asegure el control sobre las operaciones. Los mismos se explican a continuación.

a) Mecanismos de respaldo y recuperación. Las bases de datos significan una gran concentración de datos. La posibilidad de destrucción o pérdida de la misma implicaría un gran riesgo para la organización. Además, a causa de la variedad de información que contienen, una cantidad importante de programas de aplicación acceden a las bases, de manera que las probabilidades de generar errores sobre las mismas se multiplican. Para resguardar esa información existen diversos métodos, los cuales se mencionan a continuación.

- Registración contable: los datos de cada transacción se registran simultáneamente en dos dispositivos de almacenamiento; las modificaciones que se producen, a causa de actualizaciones, se ejecutan en ambas copias de los archivos. Si llegara a ocurrir una falla en uno de ellos siempre queda el otro dispositivo con el cual continuar el procesamiento. Obviamente es una solución costosa y deberá evaluarse en cada situación la conveniencia económica de su aplicación.
- Volcado de la base de datos o de parte de ella: consiste en copiar con cierta periodicidad la base de datos y conservar la copia. A esto debe agregarse un registro de todas las transacciones procesadas desde una copia a la siguiente. De manera que si se pierden datos del archivo original, la base de datos se puede restaurar aplicando esas transacciones de transición sobre la última copia de respaldo ejecutada.

- Lista de cambios o tira de auditoría: consiste en efectuar una copia de cada registro que será procesado antes y después de su actualización. Se la acompaña con una lista detallada de las transacciones que producen esa actualización (tira de auditoría), la cual se genera a medida que los datos ingresan en el sistema. Por lo tanto, si se produjera una falla en el sistema, con estos elementos se podría reconstruir la base procesando la cinta de transacciones (copiadas) y aplicándola sobre los registros copiados antes de la actualización original.

b) El administrador de Base de Datos debe aprobar y registrar todos los cambios en la biblioteca del DBMS. Este control es necesario para asegurar que únicamente los elementos de datos necesarios sean accedidos por medio de un programa de aplicación.

c) El administrador de Base de Datos deberá efectuar una revisión periódica de las bibliotecas del sistema. El propósito de esta revisión es asegurar que no se efectúen cambios no autorizados.

d) El administrador de Base de Datos deberá también efectuar una revisión periódica del *log* de programas ejecutados y de la información de especificación del programa utilizado por el programa. Este control permite asegurar que sólo se utilice información de especificación de programa autorizada para acceder a los datos. Además, este control revelará todo cambio temporario efectuado en la biblioteca del DBMS; por ejemplo, detectará una entrada no aprobada de información de especificación de programa ejecutada para una corrida de programa, y luego removida.

e) El administrador de Base de Datos debe aprobar toda modificación extra que se realice al software del DBMS. A efectos de su conocimiento técnico, es el único que puede detectar el impacto que puede significar una modificación sobre la integridad de los datos.

f) Revisión del diccionario de datos. Si bien los diccionarios de datos pueden utilizarse con los sistemas de archivos convencionales, es habitual que integren necesariamente un DBMS. Los diccionarios de datos proporcionan homogeneidad y disciplina sobre los datos que manipulan los programas, sobre todo si se tiene en cuenta el hecho de que varios usuarios pueden utilizar los mismos datos. Los mismos mejoran la documentación y ayudan en el diseño de sistemas. Asimismo, brindan a los analistas información muy útil para el desempeño de sus funciones: indican el nombre de cada campo, su sinónimo (alias), tamaño y formato del campo, orígenes de los datos, qué programa pueden leer, ingresar, borrar, actualizar o validar campos, las reglas de validación, las relaciones con otros datos y la identificación de usuarios o personas a las que se permite acceder a los datos. De acuerdo con lo señalado, los diccionarios de datos representan una porción importante de la documentación del sistema informático. Además, contienen importantes elementos de control. Desde este punto de vista, interesarán a la auditoría de sistemas de información las siguientes consideraciones:

- Análisis de las normas de validación de datos. Las mismas sirven como base para el diseño de pruebas de cumplimiento.
- Modificaciones que operen sobre el contenido de un diccionario de datos. Estas modificaciones deberán estar sometidas a controles similares como los que se utilizan para modificaciones de programas.
- Vigilancia y control de acceso a la información contenida en el diccionario. Se trata de información que puede revestir el carácter de confidencial. Deberá impedirse el acceso a personas no autorizadas.

g) Generación de Puntos de Control. La posibilidad de que la base de datos se actualice simultáneamente desde programas que provienen de varias sedes remotas (terminales) implica que deba preverse, en el procesamiento, la generación de Puntos de Control. Se trata de registros específicos que se generan en determinados momentos del procesamiento y que expresan la situación del sistema en esos momentos precisos. La información contenida en estos registros (Puntos de Control) servirá para recuperar el sistema en los casos necesarios, como por ejemplo, la identificación de archivos afectados, cuenta de registros, identificación de los programas activos en el momento de la registración y de las terminales actuantes.

4. Programas de aplicación

Varios de los controles que se ejercen sobre programas de aplicación, en un ambiente de base de datos, tienen atributos comunes con los sistemas de archivos individuales. Tales son los que se refieren a estándares de documentación, estándares de programación, estándares de pruebas y procedimientos de resguardo y recuperación –los cuales son necesarios todos en ambos sistemas. Sin embargo, existen procedimientos de control adicionales para los que se sugiere que su desarrollo se realice sobre los mismos programas de aplicación que actúan en un ambiente de base de datos. Esos procedimientos se estudiarán a continuación.

- Deben existir estándares de documentación para todos los programas de aplicación; la documentación debe ser revisada y aprobada por el administrador de Base de Datos antes de que el programa sea puesto en producción. La documentación es más crítica en un sistema de base de datos, debido a que una base de datos común es accedida por múltiples programas. El administrador de Base de Datos debe tener la habilidad para determinar el impacto que puede causar la introducción de nuevos programas o la alteración de programas existentes sobre el resto de los programas de aplicación.
- Deben existir estándares para pruebas de programas que especifiquen los criterios para generar datos de prueba, revisar los resultados de las pruebas y mantener la documentación de esos datos y resultados. Estos controles son más importantes en un ambiente de base de datos debido al "efecto cascada" de errores, ya explicado anteriormente.
- Los procedimientos de resguardo y de recupero deben ser probados previamente a su implementación, con el propósito de asegurar que cumplan adecuadamente sus funciones. Las pruebas son más críticas en un ambiente de base de datos debido a que una falla en un programa de aplicación puede alterar la efectividad de cualquier otro programa de aplicación que acceda al dato involucrado.

5. Selección del DBMS

El control del funcionamiento de un DBMS debe comenzar por la decisión acerca de qué sistema adquirir e incorporar. El auditor de sistemas de información debe participar en el proceso de selección a fin de verificar la presencia de condiciones de seguridad y control satisfactorias, conforme con las consideraciones planteadas en el presente capítulo.

COPY.AR
Fotocopias - Impresiones - Anillados
French 414 - UTN - 1°Piso

CAPÍTULO 24

Seguridad de redes y sistemas distribuidos

INTRODUCCIÓN

En sus comienzos, el procesamiento electrónico de datos se efectuó dentro de un recinto cerrado (denominado "sala de cómputos") al cual había que enviarle papeles con datos impresos; esos datos eran procesados por medio de una computadora con los programas correspondientes. De ese recinto cerrado salían otros papeles impresos, los cuales eran portadores de información obtenida a partir de los datos procesados.

Con el transcurso del tiempo, la tecnología de comunicación de datos se desarrolló significativamente y, en la actualidad, es frecuente encontrar sistemas que incluyan en su diseño la transmisión de datos entre instalaciones ubicadas en lugares distantes. Esto significa que el dato puede generarse y captarse en lugares remotos y alejados de aquél en que se lo procesa: el usuario del dato puede beneficiarse de la información producida a través de transmisiones por canales de distinta conformación.

Esta tecnología de comunicación sirvió como base para la aparición de una nueva solución informática que se apoya en los sistemas distribuidos y en la utilización de redes.

Los sistemas distribuidos utilizan computadoras separadas físicamente pero conectadas entre sí. En la mayoría de los casos, los sistemas distribuidos ingresan datos para un proceso en las sedes locales (remotas) y efectúan algún tipo de procesamiento local del que surgirá información detallada para su uso local, como también información resumida que se transmitirá a la computadora central (para control de gestión). Los lugares desde donde se capturan y procesan datos (sedes locales) reciben el nombre de nodos.

Los sistemas distribuidos requieren la disposición de redes para el procesamiento y transmisión de información. En algunos casos, las redes constan de un computadora central a la cual están conectadas varias computadoras locales. Éstas ejecutan determinadas funciones utilizando archivos locales, y transfieren datos a la computadora central para actualizar los datos del archivo central. Este tipo de sistemas distribuido se denomina grupo jerárquico o grupo radial. En otros casos, pueden existir solamente varias computadoras locales que pueden efectuar los mis-

mos tipos de procesos y contar con la capacidad de transmitir datos entre ellas. Este tipo de sistema distribuido se denomina grupo de iguales.

Razones para el diseño de sistemas distribuidos

Las razones que se señalan son las siguientes:

- A nivel mundial existe una marcada tendencia hacia la instalación local de microcomputadoras que se debe, en parte, a la disminución de los costos de hardware y al mejoramiento de los medios de comunicación. Esto favorece el procesamiento local en todo lo que sea posible. Si todo el procesamiento de los datos capturados en sedes remotas tuviera que efectuarse en la computadora central, y a través de comunicación en línea, es probable que el costo total (procesamiento y transmisión) fuera mayor.
- El hecho de que el procesamiento de los datos se efectúe en el mismo lugar en que se produce la generación de los mismos mejora la eficiencia administrativa, debido a que el usuario se encuentra cerca del proceso y cerca de la información originada. Las consecuencias son: mayor rapidez o mejor apoyo a las decisiones, y mayor facilidad para detectar y tratar errores u omisiones en datos de entrada.
- Permite equilibrar la carga de trabajo cuando ésta es dispar entre varios nodos: un nodo puede transportar datos hacia otro nodo cuando el primero esté sobrecargado y el segundo desarrolle poca actividad. Los datos se procesan en este último; los resultados se almacenan en la instalación remota y son trasladados a la instalación de origen cuando ésta tenga el sistema disponible.
- Permite compartir software. Desde una sede remota se pueden capturar y luego transmitir datos a otra sede remota para ser procesados en esta última. De este modo se puede aprovechar el software ahí instalado y retransmitir los resultados a la sede que originó los datos.
- El sistema es diseñado para que la empresa no tenga que depender de un solo centro de procesamiento.

Auditoría de sistemas distribuidos

En la modalidad de sistemas distribuidos, las transacciones totales de la empresa y los archivos maestros pueden estar fragmentados, es decir, que cada porción puede hallarse en sedes remotas distintas. Esta circunstancia crea condiciones particulares de control debido a que los datos que se originan en una sede pueden afectar archivos ubicados en otra. En este caso, el auditor de sistemas deberá participar, con su asesoramiento, en el momento del diseño del sistema de control. Éste recomendará, por ejemplo, los mecanismos mediante los cuales se mantendrán archivos de respaldo en la sede central y cómo se actualizarán éstos al actualizarse los archivos remotos.

Con respecto a las funciones de análisis y programación, el auditor de sistemas deberá revisar lo siguiente:

- Si la programación, para todas las sedes remotas, se efectúa en forma centralizada o si se efectúa en cada una de éstas, según sus propias necesidades. En este último caso, el auditor verificará la compatibilidad de estos programas cuando en su aplicación se afecten computadoras ubicadas en distintas sedes.
- El auditor revisará si existen controles adecuados ante la posibilidad de que se acceda a los programas fuente. Particularmente, debe controlar que las personas no autorizadas a efectuar desarrollos y modificaciones no puedan acceder a los programas fuente y a los compiladores. En el caso de sistemas que funcionan con intérprete, debe controlar que los programas fuente no puedan modificarse durante su ejecución. Una buena práctica es desarrollando programas y probándolos en la sede central, como también manteniendo el código fuente en sede central y enviar a las sedes locales sólo los programas en código objeto. Esta modalidad permite mantener un control sobre las modificaciones a los programas, evitando que se apliquen en algunas sedes y en otras no.
- El auditor verificará que los programas tengan incorporadas rutinas que permitan encontrar pistas de auditoría en revisiones futuras. El auditor especificará los parámetros que se incorporarán a esas rutinas para las pruebas de auditoría y selección de datos; por ejemplo, selección de valores mínimos de saldos deudores morosos para análisis individual. El auditor debe determinar cómo analizar estos casos en archivos ubicados en sedes remotas: se podrá transferir el archivo de consulta a la computadora central para procesarlo allí, o bien efectuar la selección en el archivo de la sede local y enviar el resultado a la sede central.
- El auditor debe estar informado de todos los desarrollos que se efectúen en la diversas sedes, con el propósito de analizar los efectos que los mismos podrían acarrear sobre los sistemas ya en curso.

En cuanto al hardware:

- El auditor recomendará que las computadoras distribuidas y los archivos sean compatibles entre sí y con la computadora central. Cuando los dispositivos son incomparibles se producen problemas de adaptación, con el consecuente riesgo de pérdida de información.
- El auditor revisará si existen planes para casos de emergencias, de manera que se permita la transferencia de trabajos de una máquina no operable a otra del sistema que sí lo esté. En estos casos debe preverse la identificación de la sede que cubra la emergencia y, además, que ésta mantenga vigentes los controles diseñados para la sede de origen.

Redes de comunicaciones

Las redes de comunicaciones interconectan las computadoras y componentes de un sistema de cómputo dentro de áreas geográficas que puedan cubrir diferentes distancias, según los requeri-

mientos de la organización y el sistema de información. En función de las distancias, se realiza la siguiente clasificación:

1. Internacionales (entre países).
2. Nacionales (dentro de un país).
3. En instalaciones locales (dentro de un edificio o conjunto de edificios cercanos).

Las redes internacionales y las nacionales reciben el nombre de redes de cobertura amplia. Las de instalaciones locales se denominan redes de área local.

Las redes deben ser diseñadas conforme a alguna de las topologías posibles. "Topología", es la disposición física o arreglo de los dispositivos de comunicación y rutas que deben transmitir los datos. Las más utilizadas son:

– Estrella

En la disposición estrella todos los nodos (dispositivos) se interconectan directamente con un punto central. Cada estación de trabajo o terminal puede comunicarse solamente con la instalación central y no con los demás nodos de la red (figura 24-1). Dentro de esta topología, toda comunicación entre nodos debe pasar necesariamente por el nodo central, que es el que envía los datos al nodo destino. Esta configuración presenta la ventaja de poder agregar o quitar con facilidad dispositivos a la red. Pero la confiabilidad y velocidad del servidor central de la red es crítica.

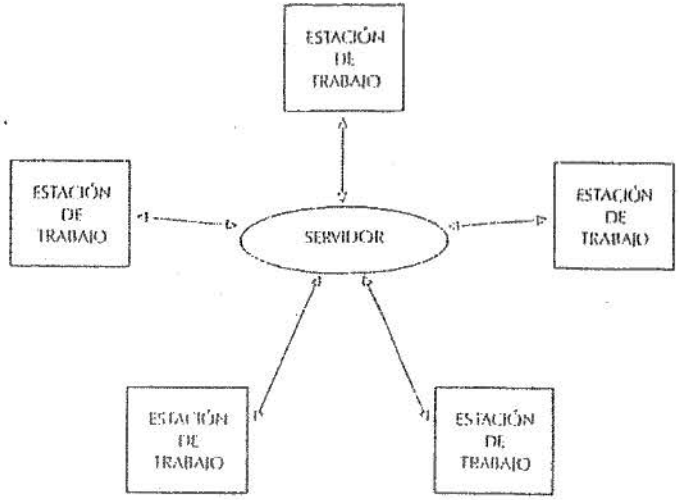

Figura 24-1. Disposición de red estrella.

– Anillo

En la disposición anillo o red cíclica cada dispositivo está conectado al que tiene por vecino, hasta que las conexiones se hagan a todos los dispositivos (figura 24-2). No existe una instalación central que maneje los datos que se transmiten de nodo a otro. Esta disposición es fácil de expandir debido a que se pueden conectar nuevos dispositivos al anillo. La red en anillo es vulnerable a las fallas (en el caso de que fallara uno de los dispositivos).

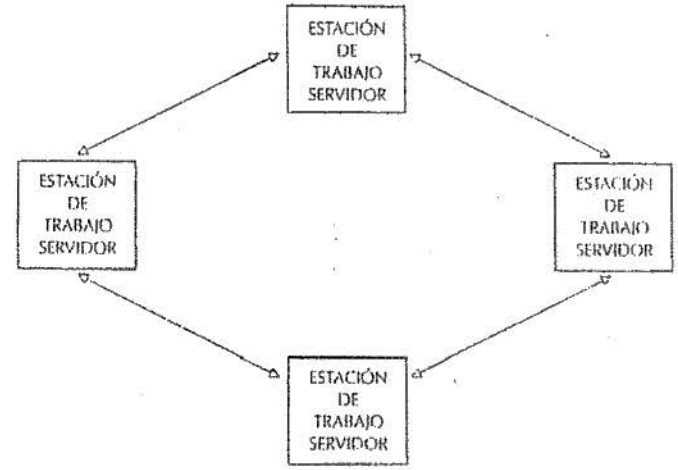

Figura 24-2. Disposición de red anillo.

– *Bus*

En esta configuración, todos los dispositivos están conectados a una línea continua de conexión (figura 24-3).

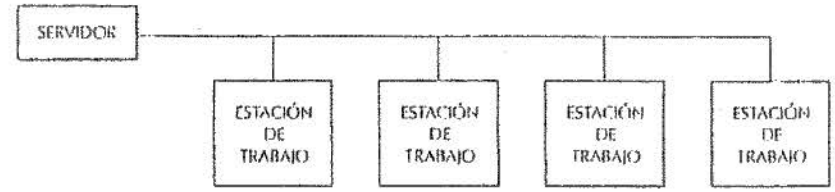

Figura 24-3. Disposición de red bus.

Redes de área local

La tendencia moderna en materia de tecnología informática se orienta hacia la instalación de las denominadas LAN. Esta modalidad, que se beneficia de la proliferación del uso de microcomputadoras, provee capacidad para intercambiar o compartir datos computarizados, software, almacenamiento, impresoras y equipo de telecomunicaciones.

En su origen, las LAN incluían el equipo y el software de comunicaciones necesario para conectar dispositivos de microcomputadoras cuya distancia máxima de separación no excediera aproximadamente los trescientos metros. Posteriormente, el equipamiento incluyó a los procesadores, software y servidores conectados a la LAN y, además, al dispositivo y software de comunicaciones. Los componentes principales de una LAN son:

- Dispositivos y software de transmisión.
- Terminales de usuarios.
- Periféricos compartidos.

La transmisión exige el cumplimiento de ciertas reglas denominadas protocolos. Estas reglas posibilitan el acceso compartido a los dispositivos en la red y evitan que un dispositivo la monopolice. Una señal, denominada *token*, designa al dispositivo que tiene el derecho de transmisión. El dispositivo que se necesita transmitir toma el *token* de la red y comienza la transmisión. Cuando finaliza la transmisión, el dispositivo que transmitía envía la señal *token* a la red.

La red puede utilizar dispositivos compartidos, tales como los siguientes:

- Servidores de red: contienen el software que se utiliza para administrar las transmisiones de red.
- Servidores de archivo: contienen el almacenamiento compartido da datos que utilizan los usuarios de la red.
- Servidores de impresión: administran el flujo de información que se transmite a las impresoras compartidas.
- Servidores de comunicaciones: administran las comunicaciones entre los usuarios.

Riesgos asociados a las LAN

En sus comienzos, el interés por la tecnología LAN estaba centrado en las capacidades y funcionalidades del sistema, y no tanto en la seguridad. Las capacidades surgen de la condición de procesamiento descentralizado que caracteriza a las LAN; brindan, por lo tanto, una mayor capacidad de respuesta. Pero se trata de una tecnología de aplicación relativamente reciente, donde las funciones administrativas y de control asociadas al software de red son limitadas.

Además, existen versiones nuevas de software que contemplan capacidades opcionales de autorización de acceso a lectura, registración y ejecución, con relación a archivos y programas. Pero no siempre incluyen elementos que sirvan de pistas de auditoría, tales como *logs* automáticos y declaración de actividades.

Si bien se ha intentado estandarizar las configuraciones de red, las necesidades que cubren son tan variadas que los componentes de las redes provienen de diversos proveedores, por lo que la mezcla de dispositivos y software (topología, técnicas de transmisión, protocolos, software de red) da por resultado que cada LAN tenga características particulares.

Los principales riesgos asociados a las LAN se sinterizan en los siguientes puntos:

1. Facilitan un acceso global a los datos, en lugar de asignar un acceso limitado, aplicando el criterio de "acceder por necesidad de saber".
2. Ejecución de cambios no autorizados a datos o programas.
3. Utilización de software no licenciado.

Auditoría de las LAN

La revisión, a cargo del auditor de sistemas, debe comenzar por comprender las funciones de la LAN; para ello, debe analizar y entender:

1. Topología y configuración de la red. Dispositivos integrados al sistema: repetidores (amplifican la señal de transmisión para que llegue a dispositivos distantes); ruteadores y *bridges* (puentes) (cumplen funciones de conmutación que permiten acceder a dispositivos alternos); *gateways* (permiten acceder a rutas extranjeras de acceso a redes).
2. Funciones que cumplen los responsables de actividades relacionadas con la red, principalmente las del administrador de red, además de las del administrador de Seguridad y de quien se encarga del diseño.
3. Modalidades de trabajo de los usuarios de la red.
4. Aplicaciones que utiliza la red.
5. Documentación que contenga normas y procedimientos relacionados con la red.

La auditoría de las LAN debe comprender aspectos de seguridad lógica, seguridad física y control ambiental. Los mismos se explican a continuación.

- Aspectos de seguridad lógica
  - Verificar la existencia de políticas organizacionales en materia de seguridad.
  - Verificar el conocimiento y percepción de los usuarios con respecto a la política de seguridad.
  - Verificar que los perfiles de acceso/seguridad de los usuarios sea acorde con las responsabilidades de cada uno de ellos.

- Verificar que las funciones del administrador de red tengan incorporadas normas de seguridad.
- Verificar que existan procedimientos concretos para otorgar autorizaciones de acceso a las LAN, basadas en el criterio de "necesidad de saber". Verificar que esos procedimientos incluyan formularios normalizados con el propósito de registrar las solicitudes y aprobaciones de: altas, bajas y modificaciones de acceso lógico a la LAN. Verificar que la restricción de acceso e identificación de usuarios se efectúe mediante un método automatizado. Verificar que se exija una contraseña a los usuarios de la LAN, y que sólo accedan los usuarios autorizados. Verificar que las contraseñas se cambien periódicamente y que se mantengan encriptadas internamente (que no sean visibles por pantalla).
- Verificar que se efectúe un seguimiento para los casos de intentos de acceso no autorizados.
- Verificar si la LAN se encuentra conectada a una fuente externa a través de un módem y de una red de línea telefónica. En caso afirmativo, controlar de qué manera se resguardan esas conexiones.
- Verificar si, ante una llamada telefónica que intente una conexión (*dial-up*), el sistema responde con una devolución de llamada (*dial-back*).
- Verificar si luego de una habilitación de la conexión (*log-on*) se efectúa automáticamente una desconexión (*log-off*) y si transcurre un determinado lapso predefinido de inactividad. Verificar si se produce la inhabilitación de las terminales de los usuarios luego de un predefinido número de intentos de *log-on* infructuosos y continuos.

– Aspectos de seguridad física
- Verificar que todos los componentes de la LAN (servidor de archivos, cuarto de cableado y conectores) y su documentación se encuentren ubicados en sedes protegidas. Solamente el administrador de red debe tener acceso al destrabe del teclado y a la contraseña de arranque.
- Verificar que se reduzcan los riesgos con respecto al retiro de componentes del servidor de archivos.
- Verificar que las llaves o elementos que permiten el acceso físico a los componentes se encuentren exclusivamente en poder del personal autorizado (personal de soporte).

- Aspectos de control ambiental
- Verificar las condiciones de protección de los equipos conforme a las especificaciones técnicas del proveedor, con respecto a efectos de la electricidad estática, estabilizadores de energía (protectores de picos de tensión), condiciones de las fuentes de energía, control de humedad.
- Verificar el estado de limpieza y ordenamiento de los elementos físicos.
- Verificar el estado de protección de los diskettes, cintas y otros dispositivos de respaldo, ante posibles riesgos de excesos de temperatura y efectos de campos magnéticos.

Capítulo 25

Auditoría del desarrollo de sistemas

Introducción

Los auditores de sistemas de información suelen, en su tarea de revisión, encontrarse con sistemas en los que se evidencia cierta carencia o insuficiencia de controles que podrían haberse incorporado en los mismos en el momento de su diseño. Esta falencia provoca que la actividad de auditoría se vea dificultada por no disponer de pistas de auditoría que posibiliten la revisión.

En los comienzos de la era de la computación, la auditoría tradicional comenzaba a actuar a partir del momento en que el sistema entraba en operación normal. Durante mucho tiempo, los auditores argumentaban que ellos no debían involucrarse en el desarrollo, porque ello significaba perder, en una posterior revisión, la independencia de criterio y objetividad –este principio ha sido muy defendido por los profesionales de auditoría.

El argumento que sustenta esta posición se basa en que, si el auditor participa en el diseño e implementación de un sistema y se satisface de los controles que él mismo hizo incorporar, quedaría inhabilitado para opinar, luego de la implementación, acerca de la falta de adecuación de esos mismos controles.

A pesar de la validez de este argumento, no es justificable sacrificar la calidad y la confiabilidad de un sistema a efectos de que el auditor mantenga su independencia. Una solución posible frente a este dilema, sería que la revisión en operación del sistema sea efectuada por un auditor distinto de aquél que participó en el diseño.

Objetivos de la auditoría de desarrollo de sistemas

El objetivo de este tipo de auditoría consiste en identificar, analizar y evaluar los requerimientos del usuario, así como también los riesgos, las exposiciones a riesgos y los controles que deben ser incorporados a los sistemas de aplicaciones durante las fases de desarrollo. Para ello, el auditor debe:

- Determinar los objetivos y requerimientos básicos de los usuarios del sistema e identificar las áreas afectadas por el mismo.
- Determinar y clasificar los riesgos y exposición a riesgos del sistema.
- Procurar la identificación de los controles necesarios con el propósito de minimizar los riesgos y exposiciones a riesgos del sistema.
- Asesorar a los miembros integrantes del proyecto de desarrollo del sistema respecto de la incorporación de controles en el diseño y de módulos de auditoría, que permita, una vez implementado el mismo, las revisiones de rutina a través de las pistas de auditoría.
- Asegurar que se sigan los pasos definidos en la metodología de desarrollo aplicada.

Debido a que que un programa de computación, ejecutado varias veces con las mismas condiciones, producirá siempre el mismos resultado, el auditor deberá prestar la mayor atención posible al análisis del sistema que maneja los datos. El análisis del sistema indicará al auditor los puntos fuertes y débiles que tendrá que tener en cuenta cuando planifique la auditoría de rutina.

Los Puntos de Control

Con relación a la premisa de que el auditor debe participar en el desarrollo de los sistemas, debemos destacar que el alcance de su participación debe enfocarse hacia la determinación de determinados puntos de control que deberán estar insertos en el cuerpo de los sistemas.

Estos puntos clave son aquellos que, incorporados a los sistemas, permiten al auditor definir la adecuación de los controles y el cumplimiento de las políticas y procedimientos de la organización. Cada uno de estos puntos permite al auditor cumplir con objetivos específicos de auditoría.

Es natural que estos puntos de control se desarrollen siguiendo muy de cerca las etapas que se cumplen durante el propio desarrollo del ciclo de vida de los sistemas de información. En consecuencia, se comentarán, a continuación, los puntos clave que deberá considerar el auditor en su participación en cada una de las etapas que componen el ciclo de vida de los sistemas.

Revisión del desarrollo del ciclo de vida de los sistemas de información

Hemos explicado anteriormente la necesidad de que la auditoría cumpla un papel activo a nivel consultoría en las fases del ciclo de vida de los sistemas de información. Ello contribuirá significativamente a la calidad y confiabilidad de los sistemas implementados.

Para efectuar la tarea de revisión, el auditor deberá disponer de la documentación elaborada en cada una de las fases, así como también, mantener periódicas reuniones con los miembros del proyecto a fin de participar en el momento en el cual su contribución sea más útil.

Durante el desarrollo del ciclo de vida, el auditor debe analizar los riesgos asociados y las exposiciones a riesgos que son inherentes a cada fase. Deberá asegurar, también, de que se hayan

previsto los mecanismos de control adecuados para minimizar esos riesgos. Deberá tener en cuenta que el costo de administrar los controles no sea mayor que el valor de los riesgos que intenta minimizar.

Desarrollo del Plan Maestro

Antes del concreto desarrollo de proyectos de sistemas de información, las organizaciones deben formular un Plan Maestro.

El Plan Maestro es un instrumento para estructurar sistemas. Este identifica aquellos proyectos específicos planeados para el futuro y también el orden de prioridades de los mismos; además, prevé los recursos necesarios para desarrollarlos.

Desde luego, ese plan debe ser acorde con el planeamiento estratégico formulado para esa organización, debido a que no sería posible desarrollar ni uno ni otros si no se logra su compatibilización. El interés del auditor en esta fase de definiciones deberá estar dirigido a la revisión de los siguientes aspectos:

1. Verificar que exista un Plan Maestro sistemático, que sea acorde con los objetivos corporativos formulados en el planeamiento estratégico.
2. Verificar que el plan esté estructurado de tal forma que, en el futuro, se pueda determinar en qué etapa del desarrollo se encuentra cada aplicación.
3. Verificar que en el plan no se incluyan aplicaciones que produzcan esfuerzos (y costos) duplicados.
4. Verificar que el plan tienda a la integración de aplicaciones actuales y de propuestas, de manera que los recursos asignados sean utilizados eficientemente.
5. Verificar que el plan sea lo suficientemente flexible, de manera que, de ser necesario, se pueda ajustar a nuevas prioridades.
6. Verificar que los sistemas propuestos sean realmente necesarios y que los usuarios hagan un uso provechoso de los mismos.

Evaluación de factibilidad

Una de las prioridades que debe alcanzarse en la determinación del desarrollo de un proyecto de sistemas de información tiene que ver con la factibilidad del sistema solicitado; es decir, con que sea posible y beneficioso su desarrollo.

Los resultados que se obtienen con un estudio de factibilidad son los siguientes:

- Definir los requerimientos básicos del sistema que se propone.
- Cuantificar, de manera aproximada, el costo del desarrollo del sistema que se presenta como solución al problema o al requerimiento del usuario.

- Verificar la disposición de los recursos financieros, técnicos y operativos necesarios para desarrollar el proyecto.
- Determinar si la solución propuesta es coherente y acorde con el planeamiento estratégico de negocios de la organización.
- Determinar un marco temporal dentro del cual se efectuará el desarrollo.
- Asegurar la conveniencia del desarrollo de un nuevo proyecto mediante el cumplimiento de las etapas del ciclo de vida de los sistemas de información, ante la posibilidad de recurrir a un producto ofrecido por un proveedor o a la utilización de un prototipo.
- Estimar los beneficios estratégicos que se alcanzarán a partir de la implementación del sistema, los cuales se reflejarán en ganancias de productividad y de ahorro en los costos futuros; determinar el período necesario para recuperar el monto de la inversión en el proyecto.

Las funciones que debe cumplir el auditor de sistemas, con relación a esta fase, son las siguientes:

- Revisar la documentación producida, de modo que se evalúe la razonabilidad de su contenido.
- Verificar que se haya efectuado el estudio de justificación económica del proyecto y que el mismo sea aprobado por la alta gerencia.
- Verificar que se haya definido una fecha a partir de la cual se estima que comenzarán a observarse los beneficios.
- Verificar si se mantiene la necesidad del negocio que dio origen al proyecto.
- Corroborar si se han contemplado soluciones alternativas y si las mismas se han cotejado. Verificar que la decisión tomada sea la más adecuada.

Fases del desarrollo del proyecto (aplicación)

Cuando se encara el desarrollo de una aplicación en particular se debe cumplir con una secuencia de fases, las cuales se analizan a continuación.

1. Definición y análisis de requerimientos

   Esta etapa se caracteriza por un activa participación de los usuarios en la definición de sus requerimientos. La claridad y precisión de requerimientos (en ese momento) será de vital importancia para evitar posteriores construcciones de sistemas erróneas o incompletas.

   Un requerimiento es una característica que debe incluirse en un nuevo sistema. La determinación de requerimientos consiste en el análisis de un sistema, el cual permita conocer cómo actúa y en qué parte del mismo es necesario llevar a cabo mejoras o innovaciones. En esta etapa de definición de requerimientos se intenta alcanzar lo siguiente:

   - Una comprensión del proceso básico de la empresa y de la finalidad de la actividad básica de la aplicación dentro de ese proceso.

   - Un detalle de la necesidades de información expresadas por los usuarios.
   - Una identificación de los datos que alimentan la aplicación y de la información generada por la misma.
   - Una estimación de volúmenes y frecuencia de procesamiento.
   - Identificación de debilidades y fortalezas de los controles necesarios en el sistema y necesidades de mejoramiento de controles.

   Las funciones que debe cumplir el auditor de sistemas, con relación a esta fase, consisten en:

   - Determinar quiénes son los miembros clave que intervendrán en el proyecto, como también a quiénes han expresado con precisión e integridad sus requerimientos los usuarios.
   - Revisar el diseño conceptual para cerciorarse de que cubra las necesidades del usuario y de que existe alta probabilidad de alcanzar los objetivos del sistema.
   - Verificar que la gerencia haya aprobado el proyecto, el presupuesto y los recursos asignados al mismo.
   - Verificar que en el análisis de requerimientos se hayan contemplado las necesidades que aseguran la preservación del control interno y la evidencias auditables del sistema, incluyendo las fases administrativas.
   - Determinar (si corresponde), en la aplicación bajo análisis, si se debe incorporar una rutina de auditoría para fines de revisión, luego de la implementación.
   - Determinar la efectividad del sistema verificando si los requerimientos del usuario contemplan la emisión de información de gestión.
   - Comprobar si la lista de requerimientos contempla la flexibilización y adaptabilidad del sistema necesarias para adaptarse a modificaciones y desarrollos futuros.
   - Verificar si se han incluido requisitos de calidad total en la gestión del desarrollo del proyecto, incluyendo la observación de estándares.

Diseño lógico del sistema

Para que el proyecto de sistemas pueda avanzar, las características de los requerimientos del usuario, ya definidas en la etapa anterior, deben convertirse en especificaciones de diseño.

El análisis de los requerimientos permite conocer qué necesita el usuario. El diseño expresa de qué manera (la mejor) se pueden satisfacer estos requerimientos.

El diseño de sistemas se formula en dos etapas:

a) Diseño lógico.
b) Diseño físico o construcción física del sistema (actualmente denominada ingeniería de software).

El diseño lógico se refiere a la construcción funcional del sistema. Contiene las especificaciones detalladas del nuevo sistema, o sea, aquellas que describen sus características: salidas de información, entradas de datos, archivos y bases de datos, procedimientos. Se denomina a este conjunto de características con el nombre de especificaciones de diseño del sistema.

En esta etapa se generan los diagramas de flujo de datos, los cuales ilustran cómo será el flujo de información dentro del sistema. También se incluyen los planes de conversión de datos que permiten pasar del anterior sistema al nuevo sistema.

Las principales funciones que debe cumplir la auditoría de sistemas, en la etapa de diseño lógico, se indican a continuación.

- El auditor deberá observar si los temas de auditoría se cubren satisfactoriamente. En caso contrario, deberá emitir un informe sobre ellos.
- Asegurarse de que el diseño se ajuste a las bases establecidas originariamente.
- El diseño deberá adaptarse a los estándares que se apliquen en la empresa.
- Verificar que se respeten los criterios de separación de funciones.

En el diseño del sistema se incluirán especificaciones administrativas no informáticas y otras estrictamente informáticas. Las especificaciones no informáticas tratarán sobre el origen de los datos de entrada, su captación, aprobación y preparación para la entrada, como también su destino en forma de salida. Con respecto a estas especificaciones, el auditor verificará que:

- El diseño de los formularios y su utilización garanticen contener los datos adecuados, debidamente aprobados.
- Los formularios contengan una numeración que facilite el control de su procesamiento.
- Las actividades administrativas sean desarrolladas por el personal correspondiente.
- Se hayan definido volúmenes de carga de trabajo compatibles con el tiempo disponible para su procesamiento.
- Se hayan definido las condiciones que permiten la aceptación de la calidad de los datos de entrada, como también las condiciones para el tratamiento de aquellos que sean rechazados. Asimismo, que se determinen las condiciones para el control de su corrección y reingreso al proceso.
- Existan adecuadas condiciones de control para el ingreso de datos *on-line*.
- La salida se presente de manera que cubra las necesidades de información del usuario sin que éste deba procesar o seleccionar manualmente la información que necesita.

Con respecto a las especificaciones de procedimientos automatizados, el auditor deberá disponer, a esta altura, de documentación que incluya las herramientas propias del análisis estructurado, tales como los diagramas de flujo de datos (en sus diferentes niveles), las tablas de decisiones o árboles de decisiones, especificaciones de archivos, etc. Respecto de estas especificaciones, el auditor deberá asegurar que:

a) En cuanto a controles:
   - En cada paso del proceso computarizado se generen totales de control que puedan ser cotejados con otros totales provenientes de otros cálculos obtenidos en forma independiente.
   - El sistema prevea la presencia de evidencias que faciliten la tarea de la auditoría.
   - Existan controles que protejan al sistema contra usos no autorizados.

b) En cuanto a entrada de datos:
   - Los controles de validación y consistencia sean adecuados y completos.
   - Los errores detectados en los datos que intentan ingresar al proceso sean comunicados al responsable que los originó, y que éste los corrija y reingrese en tiempo oportuno.
   - Cuando la entrada de datos sea *on-line* los controles impidan que los usuarios accedan a los programas utilitarios o que ingresen datos no autorizados.

c) En cuanto a archivos:
   - Los archivos de datos (archivos maestros y de transacciones) sean protegidos adecuadamente.
   - La organización, diseño y métodos de acceso a los archivos de datos sea el correspondiente a los procesos asociados al sistema, y que exista un diccionario de datos definido con precisión.

d) En cuanto a la salida de información:
   - La salida responda a las necesidades reales del usuario, en cuanto a contenido, formas, nivel de síntesis o de detalle y oportunidad.
   - La entrega de documentación de salida (o bien la disponibilidad de información en pantalla) sea precedida por controles de validación y de detección de errores.
   - Se tomen medidas de seguridad con respecto a información calificada como confidencial o reservada.

Desarrollo físico del sistema (Ingeniería de software)

El desarrollo o diseño físico, también denominado construcción física o (actualmente) ingeniería de software, se refiere a la etapa de elaboración de los programas de computación y de organización y carga de los archivos, todo ello asociado con el diseño lógico definido en la etapa anterior.

La principal actividad, en esta etapa, consiste en escribir los programas que integran el sistema y los programas necesarios para la conversión de datos del sistema vigente hacia el nuevo sistema. "Escribir programas" significa convertir las especificaciones en operaciones de computadora.

Es probable que en la etapa de diseño lógico los auditores hayan analizado las especificaciones y elaborado un recordatorio referente a recomendaciones o comentarios sobre verificaciones, que deberían incluir en los programas, tales como, por ejemplo, módulos específicos para prueba de auditoría. Es en ese momento cuando deben revisar si se cumplió con tal incorporación.

La etapa de desarrollo físico debe incluir las pruebas individuales de los programas. Estas pruebas son independientes (y previas) a las pruebas del sistema que se efectuarán en la etapa posterior. A medida que se terminan, se realizan pruebas de unidad para cada programa. Estas pruebas se denominan "pruebas alfa" (*alpha testing*).

Las tareas específicas de la auditoría de sistemas, en esta etapa de construcción física del sistema, se indican a continuación.

- Comprobar si se siguen procedimientos adecuados de gestión para controlar la calidad de los programas elaborados y asegurar que se efectúen pruebas completas de cada uno de ellos, las cuales cubran todas las alternativas y condiciones de posible presentación.
- Revisar los flujogramas de los programas para verificar su coherencia con el diseño general del sistema.
- Verificar que los controles de entrada/salida diseñados para cada programa sean los apropiados para cada situación.
- Revisar la exactitud de los procedimientos de cálculos aritméticos.
- Verificar que los programas que se encuentran en desarrollo se mantengan separados de los que ya son operativos, a fin de evitar su confusión.
- Evaluar los rastros de auditoría que se programan en el sistema para rastrear la información clave.
- Verificar que queden documentadas las modificaciones realizadas sobre el diseño general original que surjen durante la programación, y que dichas modificaciones sean aprobadas por las mismas personas que aprobaron aquel diseño.
- Revisar qué resultados arrojó el proceso de Aseguramiento de Calidad (Calidad Total) con respecto a los programas desarrollados durante esta fase.

Prueba del sistema

Luego de finalizadas las pruebas de cada programa (efectuadas en forma individual), y efectuadas las correcciones que correspondan, se procederá a la prueba del sistema. Los programas que integran el sistema deben entrelazarse y formar una secuencia, de modo que en el momento de su corrida (ejecución) en operaciones de producción normal se pueda verificar que el sistema cumpla su cometido: actualizar los archivos que correspondan, proveer las salidas definidas, etcétera.

Esta secuencia de programas debe ser probada en su conjunto. El entrelazamiento entre programas (la salida de uno de ellos puede ser la entrada del que le sigue en la secuencia) debe encajar de manera perfecta.

La prueba ocurrirá en un ambiente de prueba separado del ambiente de producción. Para ejecutar la prueba deberán prepararse datos de prueba. Estos datos deben reflejar todas las posibles variantes de presentación; se intentará violar el sistema con datos erróneos o incompletos, a fin de observar cómo reacciona el sistema ante estas situaciones. La prueba incluirá también una planificación de los resultados esperados con el propósito de compararlos con los obtenidos.

En sistemas complejos puede ocurrir que deban probarse distintas fases de un mismo sistema; esto es, verificarse resultados parciales antes de llegar al resultado final.

Para que la prueba sea confiable, los datos de prueba deben prepararse sobre la base de lo que se espera que el sistema haga, y no sobre la base de los flujogramas o especificaciones, ya que, en este caso, se estaría probando el diseño.

Si se efectúan modificaciones en algún módulo del sistema deberá verificarse que las mismas no afecten negativamente a otras rutinas ya verificadas. Las pruebas del sistema deben incluir pruebas de volumen, de modo que se evalúe el comportamiento del sistema en los picos de actividad.

El auditor debe controlar todo el operativo de comprobación. A continuación, se indican las tareas específicas del auditor en esta fase.

- Debe examinar que el plan de prueba sea completo (que contemple todas las posibilidades).
- Debe verificar los resultados de procesos cíclicos (procesos de cierre de mes, cierre de ejercicio, etcétera).
- Deben revisarse los informes de error y los mecanismos que se aplicarán para comunicar los mismos a los usuarios; luego, debe asegurar su corrección y reingreso al sistema.
- Deben revisarse las conciliaciones de totales de control.
- Deben intentarse accesos indebidos al sistema para verificar cómo funcionan las condiciones de seguridad.

Una vez finalizado el operativo de comprobación, deberá existir una aceptación formal del sistema por parte de la gerencia usuaria, de la gerencia de sistemas de información y del el sector de aseguramiento de calidad y auditoría.

Implantación

La implantación puede iniciarse sólo después de haber verificado el éxito de la etapa de prueba. El auditor de sistemas debe verificar que se haya cumplido con las aprobaciones del funcionamiento del sistema. Recién a partir de ese momento el nuevo sistema podrá migrar del ambiente de prueba al ambiente de producción. La fecha de la migración no debería afectar el procesamiento de las operaciones normales del negocio.

Un aspecto de particular atención para el auditor es la auditoría de la conversión de archivos. Es muy probable que haya necesidad de convertir todos los datos con que arrancará el nuevo sistema al formato del nuevo medio. Particularmente, con respecto a este tema, el auditor verificará que:

- Se haya planificado adecuadamente la conversión de archivos y que el proyecto provea procedimientos de control.
- Se hayan efectuado pruebas de buen funcionamiento de los programas que se encargan de la carga inicial de datos en los archivos. Estos programas contienen rutinas de control y validación de datos.
- El usuario sea el responsable de la calidad e integridad de los datos de carga.
- El personal responsable de suministrar los datos de carga inicial y el responsable de la carga hayan sido adecuadamente entrenados y que, además, conozcan los efectos que los errores de esa operación pueden provocar.

- Se mantenga una clara distinción entre los datos que integran la carga inicial y aquellos que todavía no han sido cargados.
- Se garantice que los errores detectados por los programas de control de calidad y validación hayan sido corregidos, y que luego se verifique su ingreso al archivo del nuevo sistema.
- Se haya previsto la disposición de un listado que contenga toda la información incorporada al archivo del nuevo sistema en el momento en que el mismo comenzaba a ser operativo.

La migración de un nuevo sistema, desde el comienzo de la prueba hasta el ambiente de producción, puede realizarse "en paralelo", es decir, comenzando con el nuevo sistema y manteniendo simultáneamente en operación el anterior; o bien, en forma "directa": comenzar con el nuevo y discontinuar el anterior.

Las corridas paralelas permitirán al auditor comparar los resultados del sistema anterior con los resultados que se obtienen del nuevo, durante el tiempo en que se mantengan. Si surgen diferencias de esa comparación, el auditor deberá analizar en detalle los motivos, verificando que se efectúen las correcciones pertinentes. También deberá comprobar que el paralelo se realice en un período en el que se presente la totalidad de condiciones que debe contemplar el nuevo sistema. Por ejemplo, aplicar la rutina de cálculo de importes de horas extraordinarias.

Cuando el traspaso al nuevo sistema se efectúe en forma directa, el auditor deberá enfatizar en la revisión de controles, debido a que no tendrá oportunidad de efectuar comparaciones como las que realizó con el método de paralelo.

Postinstalación (Mantenimiento)

La revisión de la postinstalación la realiza habitualmente el personal de sistemas que participó en el desarrollo del proyecto, en conjunto con los usuarios y bajo la responsabilidad del gerente de Sistemas de Información.

Pero la auditoría de sistemas de información debe cumplir también con sus planes de revisión. Los auditores que realicen este examen deben ser independientes de aquellos que actuaron en carácter de consultores en el proceso de desarrollo del sistema (para mantener la objetividad de su opinión).

A continuación se indican las funciones específicas de la auditoría de sistemas para esta etapa.

- Determinar si, luego de que el nuevo sistema ha operado durante un lapso prudente, éste cubre satisfactoriamente los requerimientos y objetivos definidos en las etapas iniciales del proyecto. Es imprescindible conocer, en este momento, la opinión de los usuarios (clientes internos).
- Verificar que existan elementos de medición que permitan identificar los beneficios proyectados en el estudio de factibilidad y analizar los resultados de la aplicación del nuevo sistema.
- Identificar las dificultades que pudieron presentarse durante la operación del nuevo sistema y verificar que los cambios que las mismas produzcan queden documentadas y no perjudiquen rutinas del mismo sistema.

- Examinar los controles para verificar si actúan conforme al diseño y a los requerimientos.
- Utilizar el módulo de auditoría (que debió haberse incorporado al sistema) para probar el comportamiento de las operaciones clave.
- Revisar los importes totales de control de entrada de datos y de salida para comprobar la corrección del procesamiento.
- Revisar los *logs* de error del operador para identificar los problemas asociados al sistema y efectuar un seguimiento de las soluciones.

Auditoría de la documentación de sistemas

Todo sistema que actúe en producción deberá quedar respaldado mediante una documentación elaborada en forma técnica, observándose los estándares definidos por la organización.

La documentación debe ser completa, debiendo abarcar todas las fases del ciclo de vida de los sistemas de información. Para cada fase se deben cubrir los siguientes aspectos:

- Objetivos que se persiguen en cada etapa.
- Resultados que se esperan producir en cada etapa y fechas de cumplimiento.
- Aprobaciones de cumplimiento por parte de la Gerencia de Sistemas y de las Gerencias usuarias.

La documentación específica de cada etapa debe comprender los elementos que se enuncian a continuación.

ETAPA	DOCUMENTOS
Plan Maestro	Planilla-detalle de proyectos a implementar, en secuencia según prioridad, aprobada por la alta gerencia.
Estudio de factibilidad	Cálculo económico de costo/beneficio, aprobado por la alta gerencia.
Definición y análisis de requerimientos	Detalle de las condiciones que debe reunir el sistema para cubrir las necesidades de los usuarios, con la aprobación de estos últimos.
Diseño lógico del sistema	Detalle de los elementos de datos (entrada), estructuras de datos (archivos), procesos y presentaciones de entrada/salida (pantallas, informes y archivos).
Desarrollo físico del sistema	Cada programa debe incluir los módulos de código fuente y objeto, como también las evidencias de aprobación y verificación.
Prueba del sistema	Resultados obtenidos aplicando los nuevos programas; evidencias de su corrección con aprobación de la gerencia usuaria.
Implantación	Plan de implantación que incluya fecha de puesta en marcha.
Postinstalación	Registración de los procedimientos de auditoría y de los resultados de las pruebas ejecutadas por los auditores de los sistemas de información.

El auditor de sistemas deberá revisar, también, la preparación de los manuales destinados a todos aquellos involucrados en el sistema:

- Personal que prepara datos.
- Personal que ejecuta entrada de datos *on-line*.
- Empleados administrativos de control.
- Operadores.
- Directivos.
- Administradores de Bases de Datos.
- Personal de distribución de salidas.
- Bibliotecarios.
- Administradores de redes.
- Administradores de Seguridad.
- Administradores de Control de Calidad.
- Usuarios de la información.

RIESGOS ASOCIADOS CON UNA METODOLOGÍA INADECUADA

Metodologías de desarrollo de sistemas débiles o incompletas pueden crear situaciones de riesgo. Por lo tanto, el auditor deberá analizar la calidad y adecuación de aquélla que se haya seleccionado. El desarrollo del método de ciclo de vida, o la aplicación de un prototipo, dependerá de las circunstancias específicas del momento en que se tome la decisión de perfeccionar un sistema, como también de otros factores (político-económicos, estabilidad o inestabilidad, plazo de vida útil del proyecto, etc.) que el auditor deberá considerar.

Estos riesgos pueden sintetizarse en los conceptos que se explican a continuación.

- El resultado final del proyecto no satisface las expectativas de los usuarios. Se observa una escasa participación de los usuarios en los momentos de definiciones.
- El sistema implementado no acompaña el desarrollo del negocio.
- El sistema es poco utilizado y se desaprovecha parte importante de la inversión. Se presupone que pronto se volverá obsoleto.
- Los controles no existen o son débiles. Es evidente la falta de consulta a la auditoría.
- Si la falta de controles no es advertida durante un largo tiempo, se facilita la posibilidad de acciones irregulares.
- Una metodología de desarrollo de sistemas inadecuada será un obstáculo para una buena administración del proyecto

PARTICIPANTES EN EL DESARROLLO DE SISTEMAS

Funciones de la Auditoría de Sistemas

Alta gerencia	• Planifica a mediano y largo plazo. • Aprueba proyectos y decide el orden de prioridades. • Asigna recursos para el desarrollo de los proyectos.
Gerencias usuarias	• Responsables de la definición de requerimientos. • Responsables de la revisión de las pruebas del sistema. • Responsables de la aprobación del producto entregado a producción. • Responsables de la capacitación de los usuarios.
Gerencia de Sistemas de Información	• Planifica su actividad en función del planeamiento estratégico de la corporación. También lo acompaña. • Actúa como soporte técnico con respecto al desarrollo, instalación y puesta en marcha del sistema aprobado. • Se responsabiliza del mantenimiento en operación del sistema durante su ciclo de vida. • Atiende y ejecuta las modificaciones aprobadas según los estándares definidos.
Líder del proyecto	• Monitorea cada proyecto que se le asigne. • Dirige al resto de los participantes en ese proyecto y efectúa la coordinación general. • Verifica el cumplimiento de estándares. • Coordina las tareas entre usuarios. • Efectúa un seguimiento del grado de avance del proyecto según el cronograma formulado.
Técnicos del proyecto	• Cada uno cumple la tarea asignada: análisis del sistema, diseño, programación, documentación.
Usuarios	• Definen requerimientos, cada uno en su nivel. • Revisan pruebas. • Informan resultados y desvíos en el avance del proyecto.
Aseguramiento de calidad	• Revisa y controla el cumplimiento de estándares de calidad en cada una de las etapas del desarrollo del sistema.
Responsable de Seguridad	• Verifica que la empresa disponga de políticas de seguridad. • Se cerciora de que el diseño del sistema responda a las políticas de seguridad. • Asesora con respecto a medidas de seguridad que deben incorporarse a los sistemas. • Verifica la seguridad de los sistemas antes de su implantación.
Auditoría de sistemas	• Cerciora si el sistema responde a las políticas y procedimientos administrativos y contables de la empresa, y si está dentro del marco del planeamiento estratégico. • Evalúa la razonabilidad de los resultados que surgen del estudio de factibilidad. • Verifica la presencia de controles en el diseño de sistemas. • Se asegura de que el sistema sea auditable y que contenga rastros de auditoría. • Formula las nuevas tareas de auditoría que surgen del nuevo sistema. • Verifica la ejecución de pruebas y revisa los resultados de las pruebas efectuadas.

Auditoría de la adquisición de software

Una de las soluciones informáticas de posible aplicación es la compra de software ya elaborado, en vez del desarrollo de aplicaciones a medida.

El auditor de sistemas deberá revisar la aplicación de criterios de evaluación, tales como los que se indican a continuación.

1. Solvencia e idoneidad del proveedor

   Aquellos proveedores de buena reputación que ofrezcan productos originales (no copias no autorizadas) serán más confiables y mostrarán evidencias de mayor solvencia y permanencia en el mercado de suministros. Deberá analizarse si el proveedor respalda el producto por medio de futuras versiones de tecnología actualizada o si, en el corto plazo, la tecnología que ofrece se volverá obsoleta. Deberá comprometerse la ayuda del proveedor hasta que el cliente se encuentre capacitado para la utilización del producto (compromiso del servicio). La antigüedad del proveedor debe valorarse.

2. Recupero del código fuente

   Ante la eventualidad de que el proveedor de software no continúe con su negocio, el contrato del producto debe prever una cláusula que permita adquirir el código fuente. Ante esta situación, debe existir un acuerdo de depósito por el cual un tercero conserve el software en depósito. El contrato de compra del producto debe asegurar que se incluyan, en el acuerdo de depósito del código fuente, los arreglos de programas y actualizaciones.

3. Documentación de respaldo del producto

   La adquisición del producto debe incluir la documentación lo más detallada posible como para que el usuario resuelva los problemas que se pudieran presentar en las operaciones.

4. Nivel de satisfacción de otros clientes

   Es importante observar el comportamiento del producto en un ambiente de producción y no solamente en uno de demostración.

5. Capacidad del proveedor para actualizar el producto

   Frente al desarrollo tecnológico del hardware, el software debe estar en condiciones de acompañar esa mejora. Esto implica el compromiso del vendedor de afrontar futuras actualizaciones de las versiones del producto.

   Respecto del contrato de adquisición, el auditor de sistemas debe examinar estos aspectos:

   - El contrato debe cubrir la descripción específica de los productos adquiridos, con indicación de la fecha de entrega.

   - El contrato debe especificar también el tipo de documentación que acompañará al producto, el compromiso de capacitación para su uso, la obligación de notificar sobre nuevas versiones y el reemplazo de la versión adquirida por la versión de última generación.
   - El contrato también indicará si el usuario podrá efectuar o no modificaciones a los programas y, en caso afirmativo, bajo qué condiciones.
   - Deberán incluirse cláusulas relativas al acuerdo de depósito del software, en un tercero, y relativas a los mecanismos de mantenimiento.
   - El contrato deberá prever mecanismos de solución para casos de recuperación de desastres (facilitar copias de software, etcétera).

Auditoría de modificaciones a programas

Los sistemas de información son dinámicos. Difícilmente un sistema se mantenga sin cambios a lo largo de su ciclo de vida. Los sistemas que se aplican deben acompañar las transformaciones de la organización que los utiliza. Por lo tanto, el cambio será una constante; para no perder el control sobre los sistemas será necesario seguir una metodología de ejecución, autorización y registro de las modificaciones a programas. Esta metodología debe incluir los siguientes aspectos:

1. Autorización de cambios

   De la misma manera en que es necesaria la autorización para desarrollar un nuevo sistema, también es necesaria la autorización para modificar parte de un sistema que ya se encuentra en producción. La autorización debe provenir de un usuario involucrado. Al igual que en el caso de desarrollo, los programas modificados deben pasar del ambiente de prueba al ambiente de producción, manteniéndose siempre la independencia entre esos dos ambientes para evitar todo tipo de confusiones. El auditor de sistemas deberá acentuar su tarea de control en aquellas situaciones de emergencia en las que suele obviarse (por esa misma razón de urgencia) el cumplimiento del compromiso de autorización.

2. Concordancia entre programas de código fuente y código objeto

   El auditor de sistemas debe cerciorarse de la perfecta concordancia entre ambos tipos de programas. La biblioteca de código fuente de producción debe contener exactamente las mismas versiones de programas que la biblioteca de código objeto de producción. El auditor debe asegurarse de que cada vez que se transfiera un programa a la biblioteca de código fuente de producción, el respectivo programa objeto ejecute exactamente las mismas funciones que aquél. Esto es muy importante para prevenir la ejecución de programas no autorizados.

3. Pistas de auditoría para seguimiento de cambios

   Todos los cambios de programas deben quedar registrados, de modo que se posibilite cualquier análisis posterior. Las pistas de auditoría sobre estos cambios se refieren a:

- Referencia de la solicitud de cambio y su correspondiente aprobación.
- Fecha y hora en que el programa modificado queda en producción.
- Identificación del personal actuante en la modificación.
- Instrucciones del programa antes y después de la modificación.

La registración de estos rastros de auditoría de cambios puede ser provista por los productos de software que se encargan de la administración de biblioteca.

4. Documentación de programas

Dentro de la documentación de programas deben existir evidencias de los cambios operados en los mismos, entre los que se incluyen:

- Solicitud del cambio.
- Motivos del cambio.
- Resultado del análisis costo/beneficio.
- Especificación del cambio.
- Resultados de las pruebas efectuadas.

5. Documentación de sistemas

Por supuesto que las modificaciones de programas pueden provocar cambios en la documentación del sistema del cual forman parte esos programas. El auditor de sistemas deberá verificar la concordancia entre una y otra documentación, especialmente en cuanto a:

- Diagramas de flujo del sistema.
- Descripción del proceso.
- Contenido del diccionario de datos.
- Descripción de corridas de programas.
- Documentación para usuario final.

Capítulo 26

Auditoría de sistemas de aplicación instalados

Introducción

Los componentes de los sistemas de aplicación instalados comprenden funciones de captura e ingreso de datos, funciones de procesamiento de esos datos, funciones de almacenamiento y funciones de salida de información.

El objetivo de este capítulo es identificar, analizar y evaluar las fortalezas, debilidades, eficacia y efectividad de las mismas.

Para ello es necesario activar controles sobre esas funciones. Los controles intentan asegurar que:

- En un sistema computarizado solamente se ingresen datos completos, exactos, válidos y autorizados (y por única vez).
- La actualización de esos datos se efectúe en los momentos en que realmente corresponda y bajo las mismas condiciones de seguridad arriba señaladas.
- El procesamiento se realice a tiempo y cumpliendo con el diseño aprobado del sistema, según sus objetivos.
- Los datos se mantengan protegidos y actualizados.
- Las salidas –resultados del procesamiento– cumplan las expectativas formuladas en el momento de definición del proyecto.

Estos controles pueden referirse a pruebas de validación de datos, conciliación de totales predeterminados, generación de informes sobre datos incorrectos, omisiones, o bien, sobre procesamientos de excepción o reingreso de datos oportunamente rechazados y luego corregidos.

Tareas del auditor de sistemas de aplicación ya instalados

Las tareas principales del auditor de sistemas de aplicación ya instalados se enuncian a continuación.

1. Obtener una comprensión profunda de cada aplicación a través del examen de la documentación y de la investigación, con el propósito de identificar los componentes significativos de la misma y el flujo de datos entre los mismos. De ese análisis surgirán las estrategias para el desarrollo de pruebas de auditoría.
2. Evaluar los controles incorporados a las aplicaciones para identificar sus fortalezas y, en el caso, sus debilidades; definir, en consecuencia, los objetivos de control.
3. Probar los controles existentes para evaluar su funcionalidad, utilizando adecuados procedimientos de auditoría.
4. Evaluar el ambiente de control para determinar si se han alcanzado los objetivos del mismo al analizar los resultados de las pruebas.
5. Analizar la eficiencia y eficacia de las operaciones que componen la aplicación, comparándolas con estándares de programación y considerando a la tecnología y procedimientos utilizados.
6. Verificar el grado de cumplimiento, a través de la aplicación, de los objetivos de la gerencia (formulados en el momento de definición del sistema).

Ambiente de sistemas de aplicación

Los sistemas de aplicaciones procesados por computación se desarrollan en distintos tipos de ambientes, lo cual crea condiciones y diferentes técnicas de aplicación de auditoría para cada tipo de situación: actualización instantánea de archivos, ausencia de evidencias o rastros de auditoría, etc. Los ambientes en que pueden residir los sistemas de aplicación son los siguientes:

1. Procesamiento general centralizado

   Es el método tradicional de procesamiento. La documentación con datos de entrada se recibe en el Centro de Procesamiento de Información, en donde se procesan y se obtienen las salidas, y desde donde se distribuye al usuario. Los esfuerzos de auditoría se concentran en esta sede central.

2. Sistemas de información para oficina

   La oficina moderna hace uso, cada vez con mayor frecuencia, de herramientas de computación que implican no solamente el procesador de texto y el correo electrónico, sino que a veces incluyen también formas de procesamiento de datos que enlazan microcomputadoras con acceso a la computadora central. Este es un ambiente que interesa al auditor en virtud de la diversidad de posibles accesos a información sensible (la tendencia actual es integrar la automatización de oficinas con el procesamiento de información a través de la computadora central).

3. Sistemas de procesamiento cooperativo

   En esta situación participan, en la resolución de problemas de información, diversos ambientes, debido a que el problema se divide en segmentos en el cual cada parte es procesada por diferentes dispositivos. El propósito es que se utilice el procesador más adecuado para el tratamiento de cada una de las unidades del sistema total, minimizando, así, la necesidad de comunicación entre los componentes (los que sólo comunican entre sí los resultados).

4. Sistemas integrados

   Los sistemas modernos automatizados procuran integrar las diversas operaciones que forman parte de los procedimientos administrativo-contables. La integración incluye desde las operaciones de compras de materias primas y pago a proveedores, hasta ventas, facturación y cuentas a cobrar; pasando por recepción, almacenamiento, trabajo en proceso, productos terminados, control de inventarios.

   En este caso, el auditor debe cubrir en su revisión áreas diversas y flujos de datos que atraviesan horizontalmente esas áreas; deberá, en tal ambiente, hacer hincapié en la revisión del control interno por oposición de intereses.

5. Sistemas de Punto de Venta

   Consisten en capturar y registrar datos en el lugar de la transacción y en el momento en que se ejecutan. La captura puede efectuarse en la terminal, a través de *scanners* (lectura óptica de código de barras) o por medio de tarjetas magnéticas (que actúan como tarjetas de crédito y, en algunos casos, como tarjetas de débito automático en cuenta del comprador). Estas terminales suelen estar conectadas con el procesador central a los efectos de actualización instantánea de inventarios y control financiero, o bien pueden consistir en microcomputadoras que registran las transacciones en el momento de su ejecución, y luego las acumulan, formando lotes, para su transmisión bajo esa modalidad a la computadora central.

6. Intercambio Electrónico de Datos*

7. Transferencia Electrónica de Fondos*

8. Cajeros automáticos*

* Véase Ludent, Alberto, *Sistemas de Información para la Gestión Empresaria: Planeamiento, Tecnología y Calidad*, Prentice Hall, Buenos Aires, 2001 (capítulos 11 y 13 respectivamente).

9. Conexión con archivos de clientes
   Es frecuente esta integración entre organizaciones bancarias y archivos de sus clientes. Consiste en almacenar datos sobre cuentas corrientes, cajas de ahorro, certificados de depósitos, préstamos, etcétera.

10. Redes

Procedimientos de control de entrada de datos

La mayoría de las transacciones de procesamiento electrónico de datos comienza con procedimientos de entrada de datos. En términos generales, cualquiera sea el ambiente en que se procesan los datos, se hace necesario efectuar el control de ingreso para asegurar que cada transacción a ser procesada cumpla con los siguientes requisitos:

- Se debe recibir y registrar con exactitud e íntegramente.
- Se deben procesar solamente datos válidos y autorizados.
- Se deben ingresar los datos una vez por cada transacción.

Si bien los datos de entrada no siempre provienen de transacciones remotas, pondremos mayor atención en el control que se ejerce en la entrada de datos transmitidos a distancia (en línea), debido a que esta modalidad abarca controles más sofisticados que los que comprenden a las modalidades de ingreso fuera de línea. Por otra parte, la tendencia moderna se orienta hacia la modalidad de transmisión en línea.

Control de entrada de datos transmitidos a distancia (en línea)

Esta sección abarca el análisis de los controles que deben existir desde el punto en que el usuario u operador de entrada de datos inicia una transacción o genera una actividad, hasta el punto en que la transacción en línea se introduce en el área de control siguiente (el área de comunicación de datos).

Los objetivos generales de control de entrada de datos se enuncian a continuación.

- Toda transacción que ingresa en un proceso de datos debe cumplir determinados requerimientos relacionados con el cumplimiento de las políticas de la organización, de las reglamentaciones vigentes y de las autorizaciones específicas.
- Todo el personal afectado al ingreso de datos debe estar expresamente autorizado a ingresar datos referidos únicamente a operaciones permitidas. Debe evitarse el acceso en el sistema de personas no autorizadas o de quienes intenten entrometerse indebidamente.

- Todos los medios utilizados para el ingreso de datos que representan transacciones o actividades (dispositivos de entrada de datos) deben ser reconocidos como tales por la organización y deben estar expresamente autorizados para enviar o recibir datos o información.
- Debe mantenerse la continuidad de las operaciones de ingreso de datos y evitar los riesgos de interrupciones.

Dentro del área de control de entrada de datos se localizan los siguientes Puntos de Control (figura 26-1):

1. Transacciones en línea.
2. Usuario u operador.
3. Terminal o dispositivo de entrada de datos.

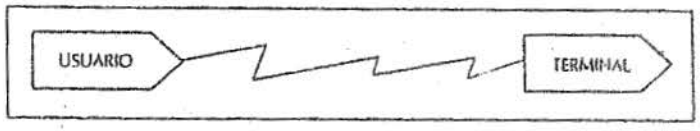

Figura 26-1. Área de control de entrada de datos.

Punto de Control: transacciones en línea

Los objetivos generales de este Punto de Control se apoyan en la necesidad de:

1. Disponer de mecanismos de control que minimicen la exposición a riesgos derivados de amenazas como las siguientes:
   - Ingreso de transacciones que no cumplan con lo establecido por las regulaciones vigentes.
   - Ingreso de transacciones erróneas o incompletas.
   - Ingreso de transacciones que no estén expresamente autorizadas por la organización o que no respondan a la política declarada por la misma.
   - Ajustes indebidos a transacciones.
   - Deterioros o degradación de la base de datos.
   - Aplicación incorrecta de mecanismos de corrección de errores.
   - Carencia de pistas de auditoría.
2. Asegurar la continuidad de las actividades mediante vías alternativas de entrada de datos.

Los objetivos generales mencionados más arriba deben traducirse en objetivos específicos. Los mismos se indican a continuación.

1. Asegurar la exactitud, razonabilidad y legalidad de las transacciones en línea.
2. Asegurar la consistencia de los datos de las transacciones. Verificar las aplicaciones de mecanismos adecuados de control de validación de datos de las transacciones, en cuanto a estructura, integridad, rango, fecha de ocurrencia.
3. Cerciorar que sólo las transacciones aprobadas sean admitidas en las operaciones en línea.
4. Asegurar que no exista posibilidad de perder la transmisión de transacciones. Verificar la aplicación de mecanismos de "control de totales" para cada terminal y para cada tipo de actividad por sesión de transmisión.
5. Asegurar la eficacia de los mecanismos de detección de errores y de las prácticas de corrección de los mismos. Minimizar los períodos de demoras en el reingreso de las transacciones previamente rechazadas y que luego fueron corregidas.
6. Asegurar que los mecanismos de transacciones en línea provean de pistas de auditoría para pruebas posteriores y que los mismos sirvan como medio de evidencia ante requerimientos legales o regulatorios.
7. Minimizar el riesgo de que se produzcan interrupciones durante la transmisión de transacciones.

Las técnicas de control aplicables a los objetivos indicados más arriba consisten en:

1. Identificar y registrar todos los tipos de transacciones aceptadas por el sistema.
2. Identificar y registrar a los operadores autorizados para ingresar las transacciones aprobadas.
3. Desplegar en pantalla formatos específicos para orientar al operador acerca de los datos que debe ingresar en cuanto a dimensión (cantidad de dígitos o caracteres), secuencia, rango o límites dentro de los cuales se deben mantener los valores a ingresar.
4. Exhibir rangos de validez de los datos de manera que sirvan de orientación también al operador. Por ejemplo, el código de artículo debe estar comprendido entre el número mil y el tres mil inclusive. Cualquier otro código fuera de ese rango debe ser rechazado por no ser válido. Verificar límites máximos y mínimos asociados a cada tipo de transacción. Los datos no deben superar un monto determinado. Por ejemplo, los importes de sueldos básicos no deben superar los cinco mil pesos. Si un sueldo supera ese monto, los datos serán rechazados y posteriormente investigados.
5. Aplicar diálogos interactivos de control. Por ejemplo, si el operador intenta ingresar un código de cuenta que se compone de dos partes, una general y otra específica, y existe incompatibilidad entre ambas a causa de la existencia de un error de transposición de números, el error se señalará en la pantalla. El mensaje sería como lo indica la figura 26-2.

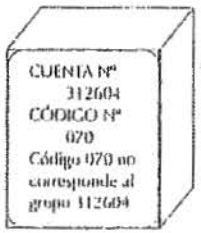

Figura 26-2. Mensaje desplegado en pantalla que indica de un error en el ingreso de datos.

6. Controlar la presencia de anomalías estructurales de datos; ejemplos: campos que deben integrarse solamente con dígitos o bien con caracteres alfabéticos; aplicación de dígitos verificadores en los campos críticos; omisión de datos en determinados campos. Con relación a este último caso (datos omitidos), los datos de transacciones deben clasificarse en exigibles u optativos: los exigibles son aquellos que no pueden faltar en el momento de ingreso a un proceso; los optativos, por su diseño, pueden omitirse, aunque los mensajes por pantalla deban señalar al operador dicha omisión.
7. Evitar el ingreso, como dato, de fechas inexistente. Por ejemplo, día superior a 31, mes superior a 12 o fechas legalmente no laborables.
8. En el caso de procesamiento en línea, modalidad en lote, puede crearse un archivo de datos de entrada sin verificárselos en una primera instancia. A continuación, otro operador distinto del que ingresó los datos en la instancia anterior, digita nuevamente los mismos datos tomados de los mismos documentos. Un programa de control provocaría que las discrepancias que surgen al cotejar lo digitado en la segunda instancia, con lo digitado en la primera, sean detectadas, informadas y corregidas para proceder, luego, a un nuevo intento de reingreso. Los datos aceptados conformarían un archivo da datos de entrada verificados.
9. En el caso de procesamiento en línea, modalidad en tiempo real, la verificación de datos de entrada que acceden al azar puede efectuarse por medio de una simulación de procesamiento en lote. Por ejemplo, pueden acumularse por programa importes provenientes de la suma de algún campo de determinadas transacciones –como el tipo de transacción y el intervalo de tiempo– y cotejarse dichos totales con otra sumatoria de esos mismos elementos, pero efectuada localmente y en forma independiente de la anterior. Luego se debe proceder al balanceo de ambas totalizaciones. También pueden mantenerse archivos independientes en los que se almacenen los datos provenientes de transacciones procesadas en línea y en tiempo real, para luego imprimir su detalle con propósitos legales o para proveer de evidencias, o bien, sumar los valores de las transacciones para su conciliación. Asimismo, en los casos en que sea técnicamente posible, utilizar grabación de voz durante el ingreso de transacciones. En estos casos, deberán

observarse y cumplirse las regulaciones que imponen las leyes respecto de temas tales como la privacidad y validez de estos registros. Por ejemplo, en algunos países existen prerrequisitos asociados con la necesidad de que el usuario manifieste fehacientemente su acuerdo para operar dentro de estos mecanismos.

10. Efectuar previsiones de control en los procedimientos de transacciones transmitidas en línea, bajo la modalidad en lote; por ejemplo, determinar una cantidad fija de transacciones a ser procesadas en lotes y conciliar la sumatoria de los valores de determinados campos con totales de esos mismos campos obtenidos por separado y registrados fuera del sistema. El control de lote puede basarse en el total de los montos (valores monetarios), en el total del ítem (verificar que el número total de los ítems incluidos en cada documento en el lote concuerde con el número total de ítems procesados), en el total de comprobantes (verificar que el número total de documentos en el lote sea igual al número total de documentos procesados), o en totales ciegos (verificar que la sumatoria de un campo numérico no monetario que existe en todos los documentos en un lote concuerde con la sumatoria de los números de ese campo de los documentos procesados). El balanceo del total por lote debe acompañarse de procedimientos de seguimiento, aclaración y corrección de diferencias, como también del ingreso de ítems rechazados y luego corregidos.
11. Mantener un conteo de transacciones ingresadas para conciliar el total de la cantidad de éstas con un total obtenido por vía separada. Aplicar un criterio similar para el caso de procesamiento en línea, en el que se refiere a cantidad de lotes ingresados.
12. Establecer procedimientos específicos para administrar la corrección de errores detectados en el ingreso de datos y para asegurar su reingreso al proceso. Mantener registros de datos rechazados y que están pendientes de corrección, e informar sobre los mismos a un tercero (para conocimiento de esta situación). Estos registros deberían mencionar: fecha y hora del rechazo, tipo e identificación de la transacción, causa del rechazo, antigüedad del dato rechazado y aún no corregido. La gestión de errores de ingreso de datos puede procesarse siguiendo distintos criterios:
    - Rechazando solamente las transacciones con errores; las transacciones correctas y válidas serán procesadas.
    - Rechazando todo el lote de transacciones; deberán ser corregidos los errores para intentar nuevamente el ingreso de datos del lote.
    - Aceptando el lote (aun conteniendo errores) y señalando las transacciones con errores. Estos últimos deberán ser luego corregidos.
    - Aceptando el lote (conteniendo algunos errores) en suspenso, el cual será así mantenido hasta que se realice la corrección. Todas las correcciones deberán ser aprobadas por el usuario.
13. Suministrar pistas de auditoría de actividad. Por ejemplo, mantener al final de cada archivo (cuyos valores se modifiquen por la registración de transacciones) importes de control en los que se registre lo siguiente: importe inicial (total del archivo antes de procesar una transacción); importe de la transacción (sumando o restando); importe total del archivo después de procesada la transacción. (Esto es, mantener una rutina de programación, almacenar un importe de control de apertura, sumarle los importes de transacciones procesadas en ese archivo y obtener un importe de control de cierre). Estos importes deberán ser balanceados con otros similares procesados independientemente de los anteriores. Por ejemplo, si los registros de un archivo de cuentas corrientes tienen un valor inicial de control de 200, y luego en un proceso posterior se ingresan datos cuya sumatoria da un valor neto de 80 (positivo), el valor de control de cierre para que balancee será 280. Si esto no es así, deberá ser investigado.

14. Mantener en las terminales *logs* que sirvan como pistas de auditoría para posibilitar la reconstrucción de transacciones desde todas las estaciones de usuarios.
15. Mantener registros de mensajes enviados y recibidos, identificados por un número de serie.
16. Prever la formulación de informes gerenciales diarios sobre tipos de transacciones desarrolladas, que incluyan totales de importes de determinados campos.
17. Mantener continuidad en el procesamiento en línea mediante la posible utilización de vías alternativas de procesamiento, de manera que se recurra a otra terminal en caso de inoperatividad de alguna de ellas. De no ser posible esta solución, prever mecanismos manuales o alternativos que incluyan el almacenamiento de las transacciones durante el procesamiento de emergencia, la generación de pistas de auditoría respecto de esas transacciones y la consiguiente incorporación de las mismas al reiniciarse la transmisión normal a la base de datos. Prever que no se produzcan omisiones ni duplicaciones de transacciones como consecuencia de la emergencia y de la restauración de los datos a los archivos o base de datos.
18. Verificar que en las transacciones contables los débitos balanceen con los créditos.
19. Prever la efectivización de un profundo entrenamiento por parte de los usuarios y operadores de los sistemas en línea y en tiempo real. Asegurar que los programas de entrenamiento no afecten los archivos de operación normal.

Punto de control: operador de entrada de datos

Los objetivos generales de este punto de control se apoyan en la necesidad de:

a) Minimizar la posibilidad de que se cometan errores humanos durante la transmisión de entrada de datos.
b) Asegurar que las funciones que ejecutan los operadores de entrada de datos sobre áreas reservadas se ajusten a las políticas y prácticas de control de la organización.

Los objetivos generales mencionados más arriba deben traducirse en objetivos específicos, tales como los que se indican a continuación.

a) Restringir la posibilidad de ingreso de datos, consulta y actualización de archivos a personas exclusivamente autorizadas e identificadas.

b) Desactivar la terminal desde la que se hayan intentado, frecuentemente, accesos no autorizados o erróneos, o bien, aquella que haya estado un determinado tiempo inactiva.

c) Mantener registros de los cambios efectuados en las autorizaciones de accesos.

d) Asegurar el mantenimiento confidencial de las claves de encriptación de datos o mensajes; hacer lo mismo con las contraseñas.

Las técnicas de control aplicables a los objetivos indicados más arriba consisten en:

a) Facilitar y simplificar la tarea del operador a través de:
   - El diseño de un formato o de una estructura de pantalla que oriente al operador.
   - El uso de un cursor que indique la posición en la que un mensaje debe ser ingresado.
   - El uso de códigos mnemotécnicos.
   - Ayudas (*helps*) al operador por medio de la aparición, en pantalla, de instrucciones en "ventanas" (ante su requerimiento).
   - La utilización de terminales inteligentes para editar y verificar/corregir errores con anterioridad a la transmisión de datos.
   - La utilización de lectores ópticos para la captura de datos que admitan esta modalidad.
   - El registro de la frecuencia con que se cometen errores, a efectos de motivar los mecanismos que los eviten y corrigen.
   - Cursos de entrenamiento.

b) Utilizar opciones limitadas entre las posibles de un menú conforme a las autorizaciones otorgadas a cada usuario por medio de tablas (es decir, que no todos los usuarios deberían acceder a todos los comandos posibles dentro de un procedimiento de captura y transmisión de datos de entrada). Asignar a cada usuario una contraseña basada en algún algoritmo. No utilizar el mismo algoritmo para todos los usuarios o grupos de usuarios. Evitar que las contraseñas se desplieguen en pantalla (evitar que se hagan visibles). Al remitir contraseñas para su distribución, distribuirlas en forma fraccionada y, cada parte, por separado, evitando así la posibilidad de que personas no autorizadas tengan conocimiento de las mismas. Evitar contraseñas que tengan menos de cinco caracteres (así es más difícil adivinarlas). Las contraseñas deberán ser periódicamente modificadas para que no se generalice su conocimiento con el transcurso del tiempo; deberían perder su validez si no cambian luego de un cierto período de utilización. Las tablas de contraseñas incorporadas al software deben ser conocidas por muy pocas personas. Deben existir procedimientos de aplicación muy estrictos con respecto a la utilización de tablas de autorización. Con la misma condición deben depurarse las tablas de autorización y las contraseñas obsoletas. Los tipos de autorización comprenden:
   - Utilización de documentos fuente estándar. Un documento fuente estándar puede consistir en un formulario de papel para registrar datos, o bien, en una imagen que se exhibe para el ingreso de datos en línea. Un documento fuente bien diseñado facilita la preparación de datos para su introducción en la máquina, por medio de dispositivos para reconocimiento de patrones o diseños y, además, aumenta la velocidad y exactitud con que pueden registrarse los datos.
   - Los documentos fuente deben ser formularios preimpresos con el propósito de que puedan ser conductivos (que orienten a quien deba cubrirlos) y prenumerados; si esto último no se cumple, se deberán establecer procedimientos para garantizar que todos los documentos fuente hayan sido ingresados.
   - Su diseño debe prever la incorporación de casilleros que definan la dimensión (cantidad de dígitos) de cada elemento de dato, agrupando los campos similares para facilitar el ingreso y conteniendo números de referencia cruzada para mejorar el control.
   - Antes de su utilización, los documentos fuente no deben estar bajo la custodia del personal que origina las transacciones que luego los utilizarán.
   - Los formularios de lotes deben estar firmados como evidencia de su emisión autorizada.

c) Introducir en el software rutinas de bloqueo que sólo puedan ser desafectadas por medio de contraseñas autorizadas.

d) Disponer de procedimientos específicos de seguridad para el caso de que se restauren operaciones ocurridas luego de un período de inactividad por fallas de una terminal. Ante esta situación, prever condiciones especiales de control en la actualización de la base de datos.

e) Desactivar terminales después de tres intentos fallidos de ingreso de datos. Mantener registros de intentos frustrados. Investigar las causas de estos intentos. También, desactivar las terminales al terminar la jornada de trabajo y bloquear el software desde la computadora central. En el caso de que haya necesidad de mantener activo el sistema fuera de las horas ordinarias, mantener registros de las transacciones operadas en esas circunstancias. Informar al administrador de Seguridad acerca de toda circunstancia que se encuentre por fuera de lo normal.

f) Efectuar control de duplicación. Por lo tanto, a medida que ingresen transacciones, se deben comparar éstas con las ya ingresadas, para detectar si se les dio entrada con anterioridad.

Punto de control: terminal

Los objetivos generales de este punto de control se sustentan en la necesidad de:

a) Asegurar, por medio de operadores autorizados y desde lugares autorizados, que el dispositivo terminal capture los datos con exactitud y procese transacciones autorizadas.

b) Asegurar la continuidad de los negocios (procesamiento de transacciones) aun en el caso de que se produzcan fallas en los dispositivos (terminales) que producen interrupciones.

c) Mantener la confidencialidad y privacidad de los datos capturados y transmitidos para su procesamiento dentro de un ambiente protegido.

Los objetivos generales mencionados más arriba deben traducirse en objetivos específicos. Los mismos se mencionan a continuación.

a) Resguardar físicamente el área destinada a terminales.
b) Asegurar que el dispositivo de entrada de datos (terminal) pueda ser identificado.
c) Asegurar que, antes de efectuar una conexión e iniciar una sesión de transmisión de datos, se verifique que la respectiva terminal sea auténtica. Evitar la posibilidad de establecer conexión con terminales falsas.
d) Asegurar la autenticidad y legitimidad del operador/usuario.
e) Verificar que el usuario opere en una terminal que envíe y reciba transacciones que están dentro de los límites de su autorización. Los datos muy sensibles sólo podrán transmitirse desde terminales específicas. Esto obliga a la segregación de datos y terminales, clasificándoselos como de "uso general" y de "uso restrictivo".
f) Asegurar que la terminal, por medio del software de la computadora central, tenga capacidad para aceptar o rechazar transacciones en conformidad con las reglas establecidas. La terminal estará dotada de esa capacidad localmente, en el caso de que se trate de una terminal inteligente.
g) Evitar, en la terminal, la exposición de códigos de encriptación.
h) Minimizar el riesgo de infidencias delimitando qué es lo que cada operador puede hacer y observar. Evitar que operadores no autorizados puedan obtener datos de manera subrepticia.
i) Evitar que personas extrañas quieran obtener conocimiento de información confidencial y puedan intentar "succionar" datos captando señales acústicas o electromagnéticas.

Las técnicas de control aplicables a los objetivos indicados más arriba, se indican a continuación.

a) Utilizar un software específico de protección que verifique:
   - Autenticidad de la terminal conforme a su localización.
   - Análisis del tipo de transacción. Programación de las aplicaciones de modo que las operaciones que se acepten queden restringidas a terminales específicas.
   - Inclusión de un encabezamiento de mensaje con identificación de la terminal, y activación del software para que lo controle y reconozca antes de efectuar su procesamiento.
   - Utilización del mecanismo (si el hardware instalado lo permite) por el cual un chip incorporado tiene la capacidad de enviar señales a la computadora principal, de manera que se garantice la autenticidad de la terminal.
   - Luego de que un usuario ha sido reconocido como auténtico, la computadora central debe efectuar un llamado al número de la respectiva terminal para asegurar que dicho usuario se encuentra conectado desde la terminal que corresponde. En caso contrario, la conexión no deberá efectivizarse, pues provendría de una terminal falsa.

b) Separar físicamente las terminales de "uso general" de las terminales de "uso restringido". Localizar estas últimas en áreas rodeadas de un entorno de seguridad (control perimetral).
c) Delimitar los menú (opciones de operación), de modo que cada operador pueda activar sólo aquellas opciones para las cuales está autorizado.
d) Evitar que personas ajenas al operador autorizado de la terminal puedan visualizar los datos que se ingresan. Evitar también que terceras personas no autorizadas conozcan y manejen el procedimiento de conexión y de acceso que va desde la terminal a la sede central.
e) Registrar los datos a transmitir, si es que la terminal tiene capacidad para ello, a efectos de futuros balanceos o conciliaciones.
f) En caso de falla o inactividad transitoria, establecer procedimientos alternativos para la utilización de terminales. Aplicar criterios de autorización, para envío/recepción de mensajes de la terminal reemplazante, similares a los definidos para la terminal reemplazada. Registrar la última transacción procesada antes de que se detecte la interrupción de transmisión (a efectos de posterior verificación y conciliación de operaciones transmitidas). Identificar las transacciones ingresadas por medio de la terminal reemplazante. Conciliar la transmisión de transacciones efectuadas bajo condiciones de emergencia. Controlar la seguridad en los mecanismos de regreso del proceso de transmisión a los procedimientos normales.
g) Establecer límites de tiempo para el mantenimiento de la conexión de terminales. Inhabilitar la terminal que se mantenga inactiva después de cierto período de tiempo.
h) Bloquear las terminales en intervalos heterogéneos y solicitar nueva autenticación (si la terminal fuera falsa –no habilitada– no podría reautenticarse por sí sola).
i) Asignar llaves funcionales especiales a los usuarios (particularmente en operaciones bancarias).
j) Utilizar cables blindados en las transmisiones a terminales y en las transmisiones desde terminales.
k) Asegurar que únicamente la persona autorizada (administrador de Seguridad) efectúe cambios en los códigos de encriptación. Establecer las responsabilidades correspondientes con respecto al manejo de los dispositivos de protección dentro de las terminales.
l) Verificar si todas las terminales quedan fuera de servicio al finalizar la jornada laboral.

Procedimientos de control sobre archivos de datos

Se ha manifestado repetidas veces que el valor de un archivo de computación es incalculable. Esto es válido tanto para un archivo de datos como para un archivo de programas. Obviamente, la protección de registros es absolutamente necesaria.

La protección de archivos que interesa al auditor, a efectos de su revisión, abarca los siguientes temas:

- Riesgos de destrucción.
- Prácticas indebidas por parte del operador.
- Mal funcionamiento de la máquina.
- Programas no probados suficientemente y que, en consecuencia, son destructivos.

Un ambiente destructivo puede provenir de la falta de protección sobre la variación excesiva de la temperatura, interrupción de energía eléctrica o amenazas de la naturaleza.

Las prácticas indebidas por un descuido del operador pueden provocar la pérdida de la información. Debido a que la mayoría de los medios de archivo pueden ser utilizados varias veces, es frecuente el borrado de los mismos; o bien, puede ocurrir que se utilice prematuramente un archivo antes de que venza el período de retención de la información. Una mala práctica puede ocurrir, también, cuando se usa un archivo por otro (cuando no se han tomado las precauciones adecuadas).

La mayoría de los dispositivos utilizados para el manejo de archivos operan a alta velocidad. Esto es beneficioso para la rapidez de procesamiento, pero a la vez representa un peligro para los medios de registro. Sin embargo, debemos aceptar que el avance de la tecnología ha vuelto menos vulnerables a los dispositivos frente a esta amenaza.

Los programas de computación que no cumplan estrictamente con los resultados que se esperan de ellos pueden provocar operaciones aritméticas erróneas o un flujo de datos que no responda a una lógica válida. Todo ello derivará en el almacenamiento de datos mal elaborados, inexactos o fuera de control.

Las prácticas de protección de archivos poco sólidas pueden conducir a problemas de operación e interferir con la auditoría al no proporcionarle una pista adecuada. Los procedimientos de retención de archivos también pueden proporcionar datos para las pruebas de auditoría. Aun cuando no ocurra una destrucción, un sistema de protección débil pone en peligro los registros y, en consecuencia, amenaza las operaciones y auditorías futuras de la empresa. Al auditor de sistemas le interesa particularmente el rastro para la auditoría. El rastro para la auditoría lo constituye un conjunto de archivos y referencias que permite comprobar o revisar las operaciones desde su inicio hasta su registro final o viceversa.

En materia de controles de procedimiento que involucran a los archivos, interesa revisar los aspectos que afectan a la actividad del operador y también otros que surgen de los programas de aplicación, como también aquellos cuyo análisis deberá afrontar el auditor.

Algunos de los métodos usuales de control sobre archivos de datos se explican a continuación.

1. Autorización para afectación de archivos

   La actualización y mantenimiento de archivos debe efectuarse dentro de un marco de protección, mediante restricciones de acceso que deben contener los programas de aplicación, además de las restricciones globales de acceso al sistema. Al auditor le interesa, además, verificar la existencia de rastros de auditoría con relación al mantenimiento de archivo.

2. Validación y edición de datos de actualización de archivos

   Los datos que intenta iniciar un proceso de actualización de archivos deben ser validados y editados lo más cerca posible del punto de origen. La estructuración de formatos adecuados al dato (predeterminados) facilita su correcta incorporación. Si por razones de operatividad y de urgencia se autoriza eludir esta condición, dichos datos deberán quedar asentados en registros automáticos, que luego serán revisados por personas ajenas al inicio de la operación.

3. Plan de preservación de la información

   Comprende las consideraciones legales y los requerimientos técnicos-operativos para la reconstrucción de archivos y para la referencia o comprobación de auditoría.

   - Conservación de documento fuente. Deben existir en la empresa políticas sobre retención de documento fuente. Estas políticas deben compatibilizar las obligaciones legales de conservación de documentos (tiempo de retención) con las necesidades de retención, a efectos de permitir, si se requiriese, la recuperación, reconstrucción o verificación de datos. Los documentos fuente, durante el período de retención, deben permanecer custodiados en el departamento emisor.
   - Preservación de registros almacenados en discos. Una característica del procesamiento de un archivo en disco es que, al actualizarse un registro de ese archivo, el registro anterior es destruido. La actualización de un archivo en disco significa que un registro sea leído –para introducirlo al almacenamiento primario (memoria interna)–, modificado (actualizado) y copiado nuevamente a la misma parte del archivo; por lo tanto, el registro anterior queda eliminado. Para obtener una copia de respaldo se debe llevar a cabo un registro específico. A diferencia del procesamiento en cinta magnética, el procesamiento del archivo en disco no produce automáticamente una copia en duplicado. En consecuencia, es aconsejable efectuar periódicamente una copia completa del archivo de datos (duplicación) y conservar los datos de las transacciones que se producen en los intervalos entre copia y copia (a efectos de reconstrucción) hasta que se compruebe la exactitud del último procesamiento de actualización. Los archivos duplicados, más los datos de operaciones posteriores, permiten la reconstrucción. La frecuencia de ejecución del procedimiento de duplicación depende del equilibrio que se espere alcanzar entre tiempo y gasto de duplicación, por un lado, y tiempo y gasto de reprocesamiento, en caso de ser éste necesario.
   - Preservación de registros almacenados en cintas magnéticas. A diferencia de lo que ocurre con el procesamiento de actualización de archivos en disco, la actualización en cinta magnética produce la creación de un nuevo archivo en cinta sin destruir el archivo anterior. Normalmente, la actualización de un archivo maestro grabado en cinta magnética se produce mediante un proceso de lectura del archivo maestro del período anterior, mediante modificaciones del mismo de acuerdo con las operacio-

nes (novedades) que estén siendo procesadas y por la grabación del nuevo archivo en una unidad física diferente de aquella que se leyó. El respaldo para archivos de cinta generalmente se logra mediante la aplicación del proceso denominado "hijo-padre-abuelo" (figura 26-3).

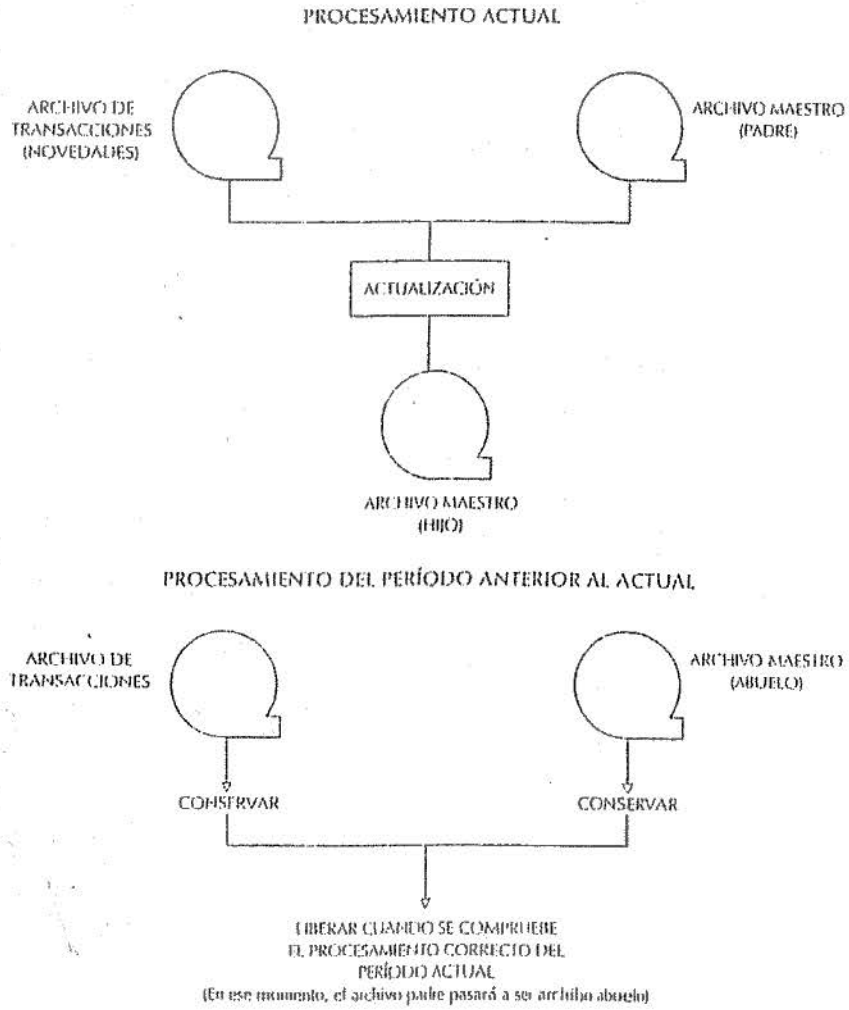

Figura 26-3. Procedimiento de preservación de registros almacenados en cintas magnéticas.

- Vaciado a otros medios. Un archivo puede ser retenido mediante el vaciado (reproducción) a otro medio de archivo. Los vaciados más frecuentes son los que provienen de archivos grabados en discos fijos que se vuelcan en cintas magnéticas –y actualmente también a diskette. La combinación de archivos de discos con respaldo de cintas vuelve muy confiable a un sistema de computación desde el punto de vista de control de archivos, pero aumenta el costo del sistema el agregado de la unidad de cinta y el control de ésta.

4. **Protección de límites entre archivos**

   La protección de límites consiste en proteger un archivo o programa con respecto a otro, cuando ambos estén almacenados en un medio común. En el almacenamiento en discos debe evitarse (mediante programación) que un archivo ingrese en el área de almacenamiento asignada a otro. Cuando varios archivos o tablas están almacenados en el mismo módulo, todos los programas que se leen o graban en los discos deben tener protección de límites.

5. **Etiquetas internas y externas**

   Las etiquetas internas aseguran que se utilice el archivo adecuado, ya que son pruebas programadas para proteger los archivos contra un uso indebido. Todo programa que intenta acceder a un archivo de datos debe efectuar previamente la prueba de etiqueta. La etiqueta de encabezamiento es un registro especial colocado al principio de un medio magnético, el cual lo identifica y le proporciona información para cerciorarse de que el archivo sea el requerido, o bien de que ha llegado la fecha en que debe ser desechado.
   Las etiquetas externas de las cintas permiten asegurar, básicamente, la correcta utilización del medio magnético que se carga para fines de procesamiento. Con todo, esta medida de protección básica no es suficiente y debe ser acompañada siempre de la aplicación de etiquetas internas. Una cinta sin etiquetar supone ser una cinta borrador que puede ser utilizada para grabar en ella nueva información. Las etiquetas externas indican la fecha en que fue preparada la etiqueta, el número de archivo, el nombre del archivo y la fecha en que fue terminada la cinta.

6. **Anillos de protección de archivos**

   Un anillo de plástico o de metal indica, con su presencia o ausencia, que se puede grabar o no sobre esa cinta. Se utiliza para evitar que se borre información antes de la fecha en que una cinta debe ser desechada. El método común consiste en insertar el anillo que permite grabar y en retirarlo cuando se quiera impedir la grabación.

7. **Biblioteca de cintas**

   Una manera de custodiar la información de los archivos consiste en mantener una adecuada administración del inventario de cintas magnéticas en uso. Las buenas prácticas de biblioteca deben ser observadas aun en instalaciones pequeñas, en las que podrá no existir una función específica y exclusiva de encargado de biblioteca. Con el propósito

de un buen ordenamiento, se deben distinguir ubicaciones separadas para cintas con archivos en uso y cintas que puedan ser reutilizadas con nueva información.

8. Administración de errores de actualización y de reingreso de datos

Los errores que surjan de los procesos de actualización de archivos deben quedar identificados y documentados, y el procedimiento debe incluir condiciones de seguridad de reingreso de esos datos una vez corregidos. Las correcciones de errores deben ser revisadas y autorizadas por personas distintas de las que iniciaron las transacciones, a causa de la necesidad de respetar la segregación de funciones de ejecución y control.

9. Registración de imagen previa y posterior a una actualización

Una manera de efectuar un seguimiento de transacciones (como pistas de auditoría) es registrándose los datos de un archivo antes y después de su actualización.

10. Control de totales de archivos

Para verificar que un archivo ha sido correcta e íntegramente actualizado, debe mantenerse un archivo de control independiente que concilie automáticamente los totales. Por ejemplo, supongamos un proceso de actualización de un archivo de cuentas corrientes a cobrar:

ARCHIVO DE CUENTAS CORRIENTES		ARCHIVO DE CONTROL
Saldo antes de la actualización (en débito)	1000	1000
Importe predeterminado que ingresa al archivo de control (en débito)		600
Transacciones de actualización:		
Nº 1 Factura (débito)	200	
Nº 2 Factura (débito)	300	
Nº 3 Cobranza (crédito)	150	
Nº 4 Nota de Débito (débito)	50	
Nº 5 Nota de Crédito (crédito)	20	
Nº 6 Factura (débito)	220	
Saldo después de actualización (en débito)	1600	1600

11. Verificación de cálculos

A efectos de verificar la exactitud de las operaciones de cálculos incluidas en los programas de actualización, deben tomarse muestras de algunas operaciones y recalcularlas por otros medios (no automáticos). La comparación entre ambos resultados determinará la calidad del proceso.

12. Controles de razonabilidad y de límites de importes calculados

Los programas de actualización que contengan operaciones de cálculos pueden incluir rutinas que comparen los resultados de los cálculos con límites o rangos predeterminados y que, además, denuncien los resultados que escapen a esos parámetros para su posterior investigación (informes de excepciones).

13. Control individual de los ítems procesados

Consiste en cotejar visualmente uno a uno los documentos fuente procesados con un listado detallado producido por el programa de computación que incorporó esos datos. Este control puede ser tedioso; depende de la calidad humana para asegurar su exactitud.

14. Datos de entrada preimpresos

Aquellos datos fijos (código de transacciones, direcciones postales, etc.) pueden estar preimpresos en formularios a cubrir con otros datos variables, para evitar errores de transcripción de aquéllos.

15. Registro automático de transacciones

El sistema de entrada de datos puede prever el almacenamiento de todos los datos de entrada en un *log*. Si posteriormente fuera necesario generar un rastro de auditoría se haría imprimir un listado de esos datos, en el que se incluya fecha y hora de la entrada, identificación y ubicación de la terminal y del usuario.

Procedimientos para el control del procesamiento

Si bien los programas de computación deben ser sometidos a pruebas antes de ser lanzados a producción rutinaria, y los datos de entrada también deben ser controlados antes de ingresar a un procesamiento, no obstante ello, el auditor debe revisar las condiciones bajo las cuales se realiza el procesamiento interno. Existen diversas razones para programar controles sobre el procesamiento; una de ellas es que un programa puede ser modificado indebidamente, ya sea en forma intencional o accidental, mientras los datos son procesados. El auditor no debe confiar en que una vez controlados los datos de entrada, controlados los archivos y probados los programas, no puedan ocurrir errores de procesamiento que den por resultado salidas incorrectas.

Los programas de computación pueden contener errores. A continuación analizaremos algunas de las fuentes principales de los mismos.

Fuentes de errores en los programas de aplicación

1. Errores de codificación

   Al escribir las instrucciones, el programador puede cometer errores de codificación, los cuales son detectados durante el proceso de compilación cuando el programa es traducido del lenguaje simbólico (humano) al lenguaje absoluto (de máquina). Por lo tanto, es difícil encontrar este tipo de errores cuando un programa pasa de la fase de prueba a la fase de producción (operación de rutina).

2. Errores u omisiones en el diseño lógico del procesamiento

   Un buen diseño debe contemplar la totalidad de condiciones de procesamiento que puedan presentarse. Sin embargo, en algunos casos se vuelve imposible probar con anticipación todos los juegos de combinaciones posibles dentro de un programa complejo, y con el paso del tiempo puede presentarse una situación no prevista.
   Por ejemplo, en un sistema de Control de Inventario es lógico suponer que el campo "existencia" no pueda ser nunca negativo; sin embargo, podría, a través de alguna combinación de eventos, adoptar un valor negativo. Como consecuencia, los resultados del procesamiento pueden ser incorrectos y cuando sea detectado el error provocaría informes inseguros y no confiables.
   Otro error de procesamiento que puede ocurrir sería cuando un programa de aplicación que efectúa operaciones aritméticas origine un resultado de dimensión mayor que la capacidad de almacenamiento asignada al resultado. El dígito que excede esa capacidad se perderá, salvo que el programa prevea esta situación y actúe para recuperarlo. Una alternativa sería prever una interrupción temporal programada cuando la capacidad sea excedida; entonces, el programa determinará la razón de la interrupción, efectuará los ajustes necesarios y el proceso regresará al punto en que fue interrumpido.

3. Modificaciones incorrectas al programa

   Toda modificación a un programa debe ser probada y aprobada. Sin embargo, en programas complejos, una modificación puede quedar incompleta si no se prevé el impacto que la misma puede ocasionar sobre otra parte del programa (por efecto de la interacción) o sobre otros programas asociados. Los cambios de poca importancia pueden provocar en el programa importantes errores en cadena.

Controles incluidos en los programas para detectar errores de procesamiento

Los programas de aplicación deben prever la posibilidad de detectar errores de procesamiento y, en ese caso, deben indicar el error a través de mensajes dirigidos, en primera instancia, al operador. Estos mensajes, o bien las instrucciones al operador contenidas en el Manual de operaciones o en las ayudas (*helps*) visibles en pantalla, deben especificar un procedimiento de corrección. Según el tipo de error, el procesamiento deberá ser interrumpido; si no, podrá continuar.

El diseño del programa debe prever que cuando el error ocurre en la etapa final de la corrida no requiere que se corra por completo nuevamente el programa. Para ello, deben incorporarse puntos de repetición de corrida en el programa; de esta manera los resultados intermedios obtenidos hasta cada punto de repetición se mantienen almacenados y no se pierden. Esto significa que si se produce una interrupción, y el error está subsanado, el procesamiento puede ser reiniciado desde el punto anterior al momento de la interrupción.

A continuación se analizarán algunos de los tipos de control que comprueban el procesamiento de la computadora.

1. Importe totales predeterminados

   Se trata de incluir en el procesamiento, al comienzo de la corrida, un importe total que deberá ser conciliado al final del procesamiento de todas las partidas procesadas. La conciliación puede ser efectuada automáticamente por el mismo programa; ello aseguraría que el procesamiento ha sido correcto y completo, al menos en cuanto a la cantidad de ítems procesados. Si la entrada comprende importes, tanto positivos como negativos, la conciliación deberá efectuarse con totales independientes por signo.

2. Controles de razonabilidad y de límites de importes calculados por programa

   Los programas deben comprobar la razonabilidad de un cálculo aritmético efectuado durante el procesamiento, comparando el resultado obtenido en cada operación con límites fijos o flexibles predeterminados. En operaciones de facturación de productos relativamente homogéneos, el programa puede prever un cálculo adicional que permita comprobar si el precio resultante queda dentro de un marco de referencia razonable o estándar. Si ese precio se aleja del porcentaje de un precio promedio, un mensaje de error deberá denunciar la excepción.
   El auditor de sistemas deberá controlar la efectividad de este método. Otra forma de comprobación es efectuando los mismos cálculos que ejecuta el programa pero fuera del sistema, tomando muestras de operaciones y comparando ambos resultados para determinar si el procesamiento realiza su función correctamente.

3. Prueba de sumas horizontales

   Se trata de un método de control cruzado. Consiste en llegar a un importe neto final por dos caminos diferentes. Si las cifras finales obtenidas a través de estas dos rutas no coinciden, se indicará algún error en el procesamiento. Imagínese, a modo de ejemplo, una corrida de computación para cálculo de nómina de empleados (remuneraciones). Para simplificar el ejemplo, supongamos el cálculo de tres sueldos netos a a los que se le aplicará el mismo tipo de deducciones, pero con diferentes importes:

a) Liquidación individual:

		EMPLEADO "A"	EMPLEADO "B"	EMPLEADO "C
Sueldo básico		1.000	1.200	2.000
Deducción "1"		100	120	200
Deducción "2"		30	30	30
Deducción "3"		50	20	40
Sueldo neto		820	1.030	1.730
Sumatoria de sueldos netos:	3.580			

b) Comprobación mediante sumas horizontales:

Sumatoria de sueldos básicos	4.200
Sumatoria deducción "1"	420
Sumatoria deducción "2"	90
Sumatoria deducción "3"	110
Sumatoria de sueldos netos:	3.580

Procedimientos para el control de las salidas

Anteriormente, la información de salida de un procesamiento computarizado se reflejaba en tados o tabulados impresos en papel o formularios continuos. El avance tecnológico ha introcido modificaciones en las tendencias de las modalidades de salidas, y los despliegues de mej jes en pantalla se han convertido en la forma más frecuente de expresión. De manera que a típicos controles de distribución de material impreso deben adicionarse los controles sobre usuarios que estarán autorizados a acceder a información por pantalla, como también, bajo circunstancias (normalmente será por la "necesidad de saber").

A continuación se explicarán algunos de los controles de salida más habituales.

1. Custodia de los formularios críticos o negociables

   Los formularios en blanco que serán destinados para ser impresos por computadora de estar protegidos adecuadamente contra robos o daños. También deberán mantenerse : cuados registros sobre la existencia y uso de los mismos, y cumplirse con planes de recu tos físicos periódicos.

2. Conciliación entre formularios salidos del inventario y aquellos procesados (impre

   Una persona ajena a quien genere la impresión deberá conciliar y fundamentar las r: nes de las diferencias por errores de impresión, mutilaciones, etc.

3. Conciliaciones de importes totales contenidos en las salidas

   A medida que los procesos lo permitan, el encargado de Mesa de Control o de la seci Control de Datos debe conciliar los importes totales de salida con los respectivos im tes totales de datos de entrada al proceso asociado con esa salida. Al auditor de sistem:

interesará verificar en el diseño del sistema la existencia de pistas de auditoría que permitan el rastreo del procesamiento de las transacciones en caso de ausencia de balanceo.

4. Control de distribución y verificación de recepción

   El control de distribución obedece a la necesidad de mantener la confidencialidad de la información reservada. Debido a que en la actualidad la mayoría del procesamiento de información pasa por procesos computarizados, es necesario diferenciar los informes confidenciales de los generales. Por otra parte, será necesario, en todos los casos, cerciorarse de la recepción de los mismos por parte de los usuarios.

5. Tiempo de retención de informes

   La política de retención deberá determinar los tiempos fijados desde el punto de vista legal y desde la normativa interna de la empresa.

6. Información de salida para corrección de errores

   Normalmente los programas prevén métodos de detección de errores, lo cual no implica necesariamente que los procesos se interrumpan por esa circunstancia. En estos casos, los errores se imprimen en un listado o bien se muestran por pantalla, pero lo importante es verificar que los mismos queden registrados en almacenamiento transitorio hasta tanto se verifique su corrección y reingreso al proceso (en cuyo caso se depurarán del archivo en suspenso). El auditor revisará el procedimiento que utiliza el usuario para corregir y retornar los datos al proceso.

CAPÍTULO 27

Técnicas de auditoría y evaluación

INTRODUCCIÓN

En el momento de planificar la auditoría de sistemas de información se le plantean al auditor distintas opciones o estrategias, cuya selección dependerá de diversos factores asociados con: el tipo de aplicación a auditar, objetivos de la auditoría, dimensión y complejidad de las operaciones involucradas, características del hardware y software utilizado en el procesamiento de la información, competencia técnica del auditor, y otros.

Frecuentemente, se efectúa una primera clasificación de las técnicas, separando aquellas que no utilizan la computadora para efectuar las pruebas de auditoría de aquellas otras que hacen uso expreso de la computadora para automatizar algunos procedimientos de auditoría. Sin embargo, aun cuando el auditor pueda no hacer uso de la computadora, igualmente debe considerar el marco general del control en el cual se efectúa el procesamiento electrónico de la información.

En todos los casos, el auditor debe evaluar los riesgos inherentes a una aplicación basándose en factores tales como:

- Complejidad de las operaciones involucradas y volumen de las transacciones.
- Modificaciones recientes operadas en la modalidad de las transacciones o de su entorno. Tiempo de vida de la aplicación.
- Consideración del valor de los bienes en riesgo.
- Calidad y profundidad en la aplicación de los criterios de control interno.

Al margen de la estrategia seleccionada para la revisión (con o sin computadora), el auditor de sistemas debe desarrollar actividades específicas de evaluación tales como las que se indican a continuación.

Verificación de la segregación de funciones

Tal como se ha explicado en otro capítulo de este texto, la aplicación del principio de separ de funciones ayuda a disminuir el riesgo de acciones indebidas, mal intencionadas o no aut das, ejecutadas por personas involucradas en el procesamiento de información.

De acuerdo con este criterio, ninguna persona debería estar autorizada a realizar más d de las siguientes tareas en el procesamiento de información:

- Generación de datos.
- Autorización.
- Modificación.
- Verificación.
- Distribución.

Los datos generados por efectos de transacciones ocurridas deben ser autorizados an su ingreso a un proceso. La evidencia de la autorización del ingreso (necesaria para el au puede manifestarse por medio de la inicialización de la documentación (documentación fí o a través de una contraseña única que exprese específicamente quién está ingresando los La revisión abarca también la verificación del cumplimiento de las reglas de acceso a la inf ción almacenada. También deben examinarse las condiciones de excepción autorizadas por pervisión (para verificar evidencias de revisión gerencial).

La auditoría de accesos a la información debe basarse en la descripción de funciones donde surgirán los niveles de autorización de accesos, que darán origen a tablas de control cesos incorporadas al software de seguridad. También aquí deberá hacerse cumplir el princi segregación de funciones.

También deberán revisarse los informes de actividades (que señalan usuario, actividad, tunidad de cada tarea ejecutada) a fin de determinar si las tareas fueron ejecutadas por qui bía hacerlo, sin penetrar en áreas reservadas a otras personas. El auditor deberá, además, busc dencias de intentos de violaciones (accesos no autorizados) a través de registros que indiquen hora, identificación de terminal, y efectuará un seguimiento de las acciones emprendidas Gerencia y el administrador de Seguridad en los casos de repeticiones sucesivas de las mism

El auditor debe buscar también evidencias de cumplimiento en la ejecución de bala entre los datos ingresados a un proceso y la salida de información correspondiente. Debe minar, asimismo, si la persona que ejecuta ese balanceo y la respectiva conciliación y corr de errores es otra distinta de quien tiene la responsabilidad de ingresar o procesar los datos

Con relación a la distribución de la información de salida, deberá verificar el cumpli to de normas de seguridad, oportunidad y confidencialidad (un listado de *mailing* de client tribuido en forma no autorizada significa información de mucho valor para la competenci perjuicio importante para la empresa defraudada).

Revisión de la documentación de sistemas

La documentación de una aplicación es un medio para mostrar los elementos esenciales del sistema de procesamiento de información: estructura de datos de entrada, descripción de los procedimientos para efectuar el procesamiento, descripción del contenido de archivos de datos, estructura de la información de salida, definición de controles aplicados.

La documentación es una fuente común de información, con respecto al sistema, para todos los participantes (usuarios y especialistas). Provee una explicación de cómo opera el sistema y qué funciones cumplen los procesos y algoritmos utilizados en él.

El estilo de documentación ha evolucionado en conjunto con la evolución de la tecnología informática. En otros tiempos, se notaba bastante descuido en cuanto a la calidad y nivel de actualización de la documentación de sistemas de computación. Con frecuencia la documentación era insuficiente y la mayoría de las veces no estaba actualizada, es decir, que algunas modificaciones efectuadas a los programas no figuraban incorporadas a su documentación. La tarea de mantenimiento de programas se efectuaba con dedicación y tiempo, cosa que no se hacía con el registro de los efectos de ese mantenimiento. Pero el avance de la tecnología informática ha ayudado a revertir esa situación. Las herramientas de documentación basadas en ayuda de computación constituyen un avance importante en el desarrollo de la documentación de sistemas. Si bien los mayores beneficios de estas herramientas se perciben en la determinación de requerimientos, a través de definición de diccionario y herramientas de diagramación cubren una buena parte del desarrollo de aplicaciones.

Las herramientas automatizadas reducen de manera importante el tiempo necesario para describir una aplicación. Estas otorgan importancia a la preparación exacta y coherente de la documentación. Sus informes validan las descripciones del sistema; previamente detectan, si ocurrieran, las relaciones inconsistentes entre datos y procesos o diagramas incompatibles. También permiten definir las contraseñas de los usuarios, los niveles de acceso y los procedimientos de respaldo. Permiten reunir, al terminar el desarrollo de una aplicación, los documentos gráficos, los informes que surgen del diccionario, la diagramación de la información de salida (informes impresos y pantallas) y también texto bajo la forma de narración. Los lenguajes de cuarta generación, producto del avance tecnológico en el área de software, son por lo general auto-documentados; por lo tanto, los propios programas se convierten en su propia documentación: la simple lectura del código explica qué hace el programa.

El auditor de sistemas deberá corroborar que la documentación de un sistema de aplicación, ya sea por la típica forma de Manuales, a través de procedimientos de ayuda en línea, diagramas descriptivos u otras herramientas (tablas de decisiones, árboles de decisiones, etc.), coincida con los mecanismos en los que funciona la aplicación. La no coincidencia entre lo documentado y lo actuado puede significar, en realidad, una amenaza potencial para el éxito del sistema.

El auditor utiliza la documentación del procesamiento de información para cumplir con dos funciones:

a) Revisión del control interno.
b) Planeamiento de la auditoría utilizando la computadora.

Para realizar la revisión del control interno, la documentación de cada programa es, con cuencia, la mejor fuente de información. La ausencia de una documentación adecuada indica falta de controles administrativos que puede influir en el plan de revisión del auditor. Cuand auditor decida emplear métodos de comprobación con uso de la computadora (métodos de tos de prueba, rutinas para auditar registros), la documentación resulta imprescindible: la est tura de los registros, organización de los datos, etc., deben ser conocidos para facilitar la elab ción de programas de auditoría o datos de prueba.

Un plan de documentación

La documentación es imprescindible para todos los involucrados en las aplicaciones informát (y obviamente para la empresa donde se aplican); estos son:

- Analistas/programadores.
- Operadores.
- Apoyo técnico.
- Usuarios.
- Auditor de sistemas.

La documentación estará incorporada a cuerpos orgánicos frecuentemente denomina Manuales, aunque, como ya se explicó, la tendencia moderna es encontrar "ayudas" o instruc nes de operación incorporadas a los propios programas, de manera que las mismas aparezcan pantalla) a la vista del operador/usuario en el momento en que se las solicite, por medio de mandos que cumplan con esa función.

Uno de los elementos básicos en el que se apoya la documentación es la "corrida de la c putadora". Pero dada la interrelación de las diversas corridas, se hace necesario una descripc general de la aplicación que explique cómo son utilizadas las mismas, y así disponer de una c prensión completa del sistema.

Otro de los elementos básicos de documentación es el conjunto de "instrucciones para el op dor", el cual podrá formar parte del "Manual de corrida de la computadora". Los usuarios tambien cesitan instrucciones y explicaciones. Los Manuales de usuarios son consultados por quienes inte túan con la computadora a nivel de programa de aplicación. Deben contener instrucciones detall explicativas de la utilización de las funciones y comandos que deben activarse para la ejecución coti na de operaciones con la computadora: procedimientos para autorización de las transacciones, m pulación de documentos, correcciones de errores e interpretación de informes impresos o por pant

El Manual de corrida puede expresarse de diversos modos. Sin embargo, debe compren un contenido mínimo que pasaremos a describir. Las secciones típicas serán las siguientes:

1. Definición del problema.
2. Descripción del sistema.
3. Descripción de los programas.
4. Configuración de registros, diccionario de datos, esquema de base de datos, pantallas e informes.
5. Instrucciones de operación.
6. Registros de aceptación.

En los párrafos siguientes se describen esas secciones.

1) Definición del problema

Es la fuente básica de información relativa al propósito del sistema. Contiene la descripción de las razones del proyecto (antecedentes), su ubicación en el Plan Maestro de Sistemas de Información y su aporte a los objetivos corporativos. Su contenido mínimo debe comprender:

1. Antecedentes del proyecto.
2. Solicitud del proyecto.
3. Definición del problema.
4. Aprobaciones de requerimientos y decisiones sobre el plan de trabajo.

La definición del problema servirá como respaldo del proyecto. Debe considerarse que la posterior descripción del sistema y la elaboración de programas constituyen la respuesta a solicitudes de futuros usuarios. Por lo tanto, deben ser aprobadas por éstos y por el gerente del Departamento de Sistemas de Información. La solicitud aprobada se convierte en parte de la documentación.

2) Descripción del sistema (análisis y diseño lógico)

Consiste en una descripción general del ambiente en el cual operará el sistema. Esta sección contendrá los DFD (con indicación de entidades intervinientes en el sistema, indicación de procesos y de almacenamiento de datos y señalización del flujo de datos entre los elementos mencionados), tablas o árboles de decisión y lenguaje estructurado.

Si se utiliza como herramienta de descripción el diagrama de flujo del sistema, el cual indicará:

1. Fuente y naturaleza de todos los datos de entrada.
2. Las operaciones de la computadora (indicadas globalmente).
3. La naturaleza y disposición de los datos de salida.

Por lo tanto, muestran cómo los datos de los documentos fuente fluyen a través de la co tadora hasta la distribución final a los usuarios. En este diagrama los programas son tratados "cajas negras" (se identifican globalmente sin incluir detalles). Los símbolos que se utilizan d ser los estándares aceptados internacionalmente. Este diagrama ayuda a elaborar las instruce detalladas de operación y control.

3) Descripción de los programas (diseño físico o ingeniería de software)

La descripción del sistema explica el proceso en su conjunto y trata a cada programa como si una caja negra. La descripción de los programas se refiere a detalles que documentan la po del sistema que representa cada uno de los programas involucrados.

La tecnología moderna en materia de ingeniería de software incluye diversos tipos de h mientas y técnicas que se utilizan para la elaboración y documentación de programas de co tación. Entre ellas, se incluyen las siguientes:

- Diagramas de flujo estructurado (denominados de Nassi-Schneiderman). Son h mientas gráficas que obligan al diseñador a estructurar software que sea modular y cendente.
- Diagramas de HIPO (*Hierarchical input-process-output*, Entrada-proceso-salida jerárq El propósito de este diagrama es entender, describir y documentar los módulos y su ración, de manera que se disponga del detalle suficiente, pero que al mismo tiemp pierda de vista el panorama general.
- Diagramas de Warnier/Orr. Identifican la salida y el resultado del procesamiento, opera hacia atrás para determinar los pasos y entradas necesarios para producirlos.

Otras técnicas, que se utilizaron anteriormente a las mencionadas más arriba, utilizab diagrama de flujo de programa (también denominado diagrama de bloques o diagrama ló como medio de documentación. Este tipo de diagrama es una representación gráfica de la l del programa de computación. Muestra la secuencia de instrucciones de un programa y a t de qué vías fluyen los datos. Los símbolos que se utilizan deben ser los estándares aceptade ternacionalmente.

Una copia del listado de cada programa (última versión) deberá ser parte de la docum ción. El listado sirve como respaldo; debe incluir fecha de emisión para evitar confusión de siones. Toda modificación de los programas debe ser específicamente autorizada por el mism vel que autorizó el programa original. La impresión de memoria después de que un progran sido cargado puede resultar importante para diagnosticar posibles errores del diagrama.

Interesará al auditor verificar que los programas que forman parte de las corridas r (código de máquina) sean la versión exacta de los programas (código fuente) que integr documentación.

4) Configuración de registros, diccionarios de datos, esquemas de bases de datos, pantallas e informes

El diseño de registros brinda información sobre el tipo de registro, su estructura y extensión y el tipo de datos que incluye. Los diseños de pantalla y los informes impresos por los programas especifican los resultados (salidas) que brinda el sistema y, en el caso de pantallas, también indican qué datos son necesarios para su ingreso.

El diccionario de datos es fundamental como herramienta complementaria de un diagrama de flujo de datos. Contiene la denominación de cada elemento de dato, su alias (si lo tuviera), tipo, estructura, rango de valores aceptables, origen y autorización para ser accedido. Indica también qué programas de aplicación utilizan esos datos.

Las bases de datos facilitan las relaciones entre datos que se encuentran en distintos archivos. Los "esquemas" son diagramas que informan cómo se organizan y relacionan esos datos.

La descripción de las áreas de almacenamiento es muy útil. Se almacenan resultados finales de un procesamiento o bien resultados intermedios durante las etapas de procesamiento. Será de utilidad conocer el tamaño de cada área de almacenamiento (cantidad de caracteres), estado inicial (cero, en blanco u otro), cómo fue totalizado (totales menores, intermedios, mayores o finales).

5) Instrucciones de operación

Constituyen la parte del Manual de corrida que contiene las instrucciones que requiere el operador de consola para correr cada programa, así como también la secuencia de éstos. La determinación de cuáles programas deberán correrse y en qué momento dependerá del plan (*schedule*) preparado por el planificador (*scheduler*).

El principio de separación de funciones en el procesamiento de información implica que el operador de la computadora no debe tener acceso a toda la documentación completa. El operador debe conocer exclusivamente las instrucciones necesarias para procesar. Sin la documentación completa del Manual de corridas sería difícil para el operador de la computadora alterar el programa para fines no autorizados. Dentro de las instrucciones para el operador deben incluirse las que definen la iniciación, corrida y finalización del programa. Se debe instruir al operador sobre todos los mensajes e interrupciones programadas contenidas en el programa.

6) Descripción de controles

En esta sección se describen los controles asociados a cada corrida de programa. Esta enunciación de controles es valiosa para el auditor a efectos de su revisión. Los controles a los que se hace referencia son:

- Controles que se efectúan fuera del Departamento de Sistemas de Información, que curan asegurar la exactitud de los datos de entrada.
- Controles que se practican dentro de Departamento de Sistemas de Información.
- Controles incorporados en los programas de aplicación para detección de errores.
- Controles de la información producida por el Departamento de Sistemas de Informa y efectuados (fuera de ese departamento) por los usuarios receptores de la informaci
- Controles de exactitud e integridad de los datos transmitidos a distancia.

7) Registro de aceptación

Todo sistema de computación, antes de entrar en producción, debe ser aprobado por el niv usuario correspondiente y por el gerente de Sistemas de Información. Obviamente, la aproba significa su previa comprobación en cuanto a cumplimiento de objetivos y en cuanto a veri ción de la exactitud de los procesos ejecutados por los programas que lo componen.

La documentación de esta sección comprende la descripción de la técnica, seguida p comprobación del correcto y completo funcionamiento de un programa y la verificación d ber contemplado la totalidad de posibilidades en cuanto a alternativas de entrada de datos ejemplo, pueden utilizarse datos de prueba como técnica de comprobación para detectar er en los programas. Las copias de los datos de pruebas de entrada y salida deberán ser conserv como parte de la documentación del programa. Cada vez que el programa sea modificado, d rá reprocesarse la comprobación para verificar el impacto de esas modificaciones sobre las sal Las modificaciones también deberán ser aprobadas, debiéndose mantener registros de la com bación y de la aprobación. Los registros incluirán: solicitud del cambio, fecha de solicitud conclusión, razones del cambio, aprobación del método de cambio y aceptación del progr modificado. De esta manera, se mantendrá actualizada la documentación.

Capítulo 28

Técnicas de auditoría asistidas por computadora

Introducción

Una manera de procesar una revisión de auditoría, en un ambiente de procesamiento electrónico de datos, consiste en tratar a la computadora como una "caja negra". Esto es efectuar una auditoría "alrededor de la computadora", sin utilizarla. Obviamente, esta modalidad no resulta ser la más eficiente, ya que produce importante desperdicio de recursos humanos y tecnológicos. Por otro lado, la auditoría con (o a través) la computadora permite al auditor aprovechar mucho mejor su inversión en el tiempo, y agregar alto grado de seguridad y mayor rendimiento en su actividad específica. Esto hace a la auditoría más atractiva y más segura, ya que permite un mejor desarrollo intelectual de la tarea y agiliza la obtención de resultados.

A continuación se analizarán varias de las técnicas que utilizan software específico, y que por lo tanto se aplican mediante el uso de la computadora para el ejercicio de la revisión de auditoría. Desde luego, el juicio profesional determinará la técnica, la oportunidad, el tiempo de dedicación y la extensión de cada procedimiento de posible aplicación.

ITF (*Integrated Test Facility*, Centros de pruebas integradas)

Es una técnica que también se la conoce como técnica de auditoría de la "minicompañía". Consiste en un procesamiento simultáneo de datos de prueba que representan operaciones ficticias en conjunto con datos de operaciones reales, durante una corrida de procesamiento real. Esto permite al auditor comparar los resultados del procesamiento de datos de prueba con importes previamente determinados. Si los resultados del procesamiento de los datos de prueba resultan conforme a lo esperado, es razonable suponer que el programa de computación procesa los datos reales tal como corresponde.

La aplicación de esta técnica implica el establecimiento de registros para prueba, f
o simulados, en la base de datos para auditoría. Los datos de prueba representan un con
to de entidades ficticias, tales como departamentos, clientes y productos o empleados
operaciones de prueba deben ser conocidas solamente por aquellos (auditores) que apli
esta técnica de revisión. Por lo tanto, los operadores de ingreso de datos al sistema suj
revisión no deberán estar en condiciones de diferenciar las transacciones de prueba de a
llas que son reales.

Las primeras aplicaciones sometidas a revisión por el auditor, a través de la técnica ITF,
por lo general: Compras, Liquidación y Pago de Remuneraciones, Cuentas a Cobrar y entra
pedidos de venta. Es aplicable tanto para procesamiento en lotes como para sistemas en lí
en tiempo real.

Debe observarse que esta técnica de auditoría no se propone revisar la validez de lo
tos de entrada sino que prueba la validez de los programas de computación que procesa
datos de entrada, a efectos de determinar si operan en conformidad con su diseño previa
te probado y aprobado.

Un ejemplo ilustrará el mecanismo de aplicación del ITF. Supongamos que se aplica est
nica sobre un sistema de Cuentas a Cobrar. Para ello se deberán crear algunas cuentas de cli
ficticios (sólo conocidas para el auditor). Supongamos también que uno de los controles i
porados en el programa a revisar consiste en emitir un mensaje de atención para el caso en q
saldo de cualquier cuenta corriente del cliente exceda el cupo crediticio (límite de crédito)
nido al mismo. Para revisar este control con el ITF, deberá generarse una transacción de vent
afecte una de esas cuentas ficticias, con un importe que produzca un exceso de saldo resul
sobre el límite del crédito disponible. Si como consecuencia de esta prueba no se obtiene el
rado mensaje de atención en forma automática, ello indicará al auditor la necesidad de profi
zar su investigación, debido a que tampoco funcionará correctamente el programa para el p
samiento de los casos reales.

Uno de los aspectos más difíciles de resolver en la instrumentación de esta técnica es
generar los datos de prueba. Para ello, el auditor deberá hacer uso de imaginación y creativ
Por ejemplo, a través de la misma, deberá revisar si se han efectuado cobranzas que ganaro
cuentos por pronto pago, habiendo sido efectuadas fuera de término; o si se han efectuado p
excedidos con relación a las deudas.

Debe observarse la necesidad de verificar la correcta aplicación de la técnica ITF, a
de que una falla en su implementación puede dar lugar a que se produzcan riesgos d
portancia sobre la alteración indebida de archivos reales o de información suministrada
de ellos. ITF debe diseñarse de forma tal que, luego de ser aplicado, las transacciones
cias deban ser retiradas y los archivos reales volver a su estado anterior al del momen
la prueba.

Por lo tanto, la aplicación de esta prueba debe efectuarse sin perturbar a los datos de
sacciones reales que sirven de base para la preparación de estados financieros e información
toma de decisiones. Los auditores deben asegurarse de que no queden efectos residuales
pruebas efectuadas.

Test deck

El enfoque denominado *test deck* es un método de prueba de cumplimiento en un entorno de procesamiento electrónico de información. Está integrado por una serie de transacciones falsas o simuladas. Estas transacciones contienen datos, en algunos casos válidos y en otros no. Éstos son procesados luego, y el auditor compara los resultados de los datos de prueba con resultados determinados previamente en forma independiente. Si se observan diferencias, ello indicará ausencia de controles, lo cual dará motivo para que el auditor investigue en profundidad las causas de esas diferencias. Algunos ejemplos de esta técnica se describen a continuación.

1. Intentos de procesar transacciones no autorizadas

   Intento de efectuar una liquidación de sueldos con respecto a un número de legajo que fue dado de baja algún tiempo atrás y que, por lo tanto, no corresponde efectivizar ese pago.

2. Pruebas de límites y de razonabilidad

   Si un programa prevé el rechazo de datos sobre horas trabajadas por un operario durante una semana (por ejemplo, más de cuarenta horas), el auditor incluirá un registro que exceda esa cantidad y verificará, luego del procesamiento, si efectivamente esa transacción ha sido rechazada.

3. Prueba de validez

   Si los códigos de clientes deben mantenerse, por ejemplo, entre los números 0001 y 5999, el auditor intentará ingresar al proceso una transacción identificada con el número de cliente 6000, a efectos de observar cómo reacciona el programa y si éste detecta el caso como no válido.

4. Prueba de signo

   Introducir datos con un campo con signo negativo y observar el resultado del procedimiento. Verificar si la rutina de cálculo respeta o ignora el signo de un importe.

5. Prueba de tipo de caracteres

   Probar, introduciendo caracteres de tipo distinto del aceptado (alfabético donde debe figurar numérico y viceversa), la reacción del programa. A los efectos de la preparación de los datos de prueba para la aplicación de esta técnica, el auditor deberá consultar la documentación del sistema y conocer el diseño de los registros (denominación de los campos, su dimensión, tipo de caracteres).

   La técnica *test deck* presenta algunas limitaciones. Una de ellas es la dificultad para que el auditor encuentre la totalidad de posibilidades de error que pueda presentar el programa a ser probado. Esto significa que la prueba no es absolutamente segura: pueden presentarse en el futuro casos de error que no fueron antes previstos.

Otra limitación es que la versión del programa a ser probado a través de esta técnica de no ser la misma que la que se utiliza durante las corridas regulares. O puede oc también que la documentación del programa bajo revisión no esté actualizada y q hayan producido modificaciones en el mismo, lo que provocaría inseguridad en lc sultados obtenidos como consecuencia de la prueba, pues los datos preparados pa revisión no se apoyaron en una base documental cierta.
Una manera de evitar estas incertidumbres es mediante la obtención de una copi programa a auditar que esté actualmente en uso, de las que luego se prepararán, sob base, las pruebas.

6) Pruebas de rebosamiento (*overflow*)

Incluir una cantidad de caracteres en un campo de modo que su procesamiento pr que condiciones de *overflow* (rebosamiento). Esto ocurre cuando, por ejemplo, el r tado numérico de una sumatoria de un conjunto de campos arroja una cantidad qu cede la capacidad de almacenamiento reservado en memoria para registrar ese resul En este caso, el dígito de extrema izquierda del resultado quedaría fuera de la pos dad de registrase, es decir, se perdería. El auditor observará si el programa de aplica prevé solucionar estos casos o si el dígito excedente se pierde luego del procesamie

Generadores de pruebas

La preparación de datos de prueba para la aplicación de la técnica *test deck* puede ser efect manualmente o bien a través de la ayuda de paquetes de software denominados generador datos de prueba. Estos programas generan transacciones y datos de acuerdo con criterios es ficos, los cuales son utilizados para facilitar la prueba de aplicaciones. Las transacciones de p ba son procesadas durante una corrida normal de la aplicación, y su salida debe compararse los resultados predefinidos.

PTF (*Parallel Test Facility*, Simulación paralela)

Existen dos modalidades de utilización de esta técnica:

a) Procesamiento paralelo (pruebas de cumplimiento).
b) Simulación paralela (pruebas sustantivas).

En el procesamiento paralelo debe efectuarse una copia, en un medio magnético, de los gramas de aplicación, de la base de datos y del sistema operativo. Con estos elementos se efec una corrida en otra computadora, distinta de la de uso habitual. El paso siguiente será compar resultados obtenidos en ambas instancias y evaluarlos. El propósito del procesamiento pa lo es determinar si el sistema operativo y los programas de aplicación actúan conforme

objetivos de su diseño oportunamente aprobados. La ventaja de esta modalidad es que su aplicación no afecta a la base de datos de transacciones reales, debido a que a ésta no se la involucra en el procedimiento de prueba. La figura 28-1 ilustra el funcionamiento de la técnica.

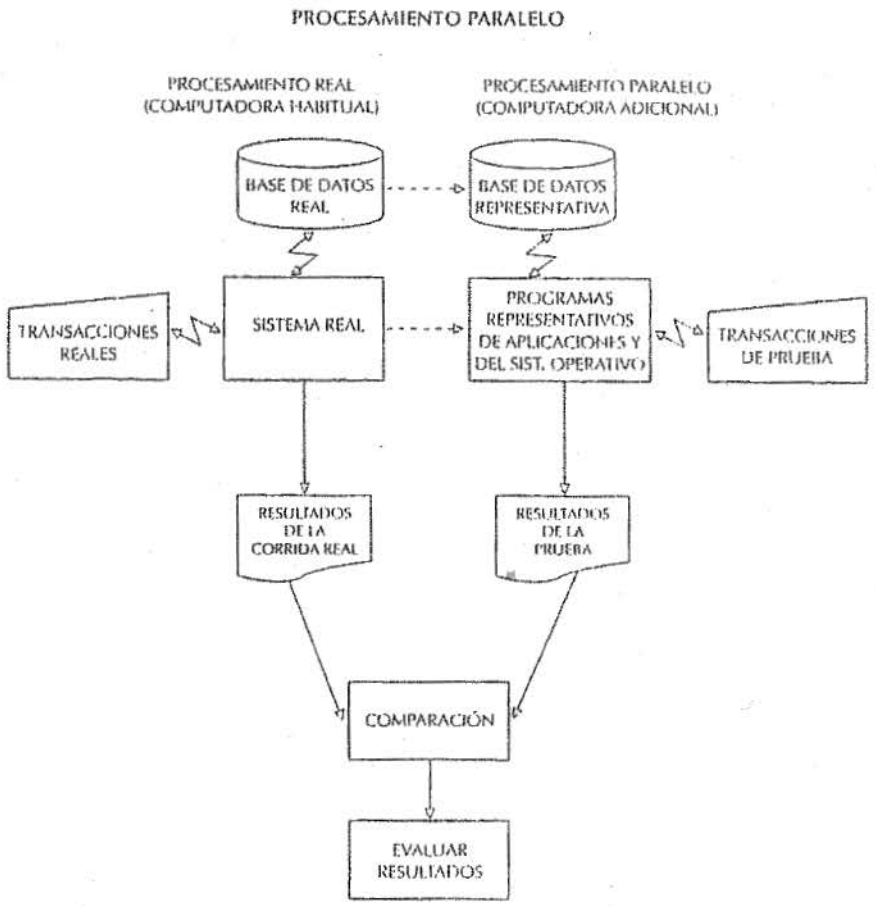

Figura 28-1. Ilustración gráfica del funcionamiento de la técnica de procesamiento paralelo.

Bajo el enfoque de simulación paralela no se trabaja con una copia de los programas de cación como en el enfoque anterior. En su lugar, se utilizan rutinas preparadas específicar para la auditoría, las cuales simulan total o parcialmente partes del sistema que interesan pa larmente a la revisión: cálculos complejos (intereses sobre depósito o sobre préstamos), bala de cuentas, eliminación automática de cuentas incobrables, etcétera.

Por consiguiente, estos programas especialmente elaborados ejecutan las mismas func que los programas regulares de aplicación, y además aceptan las mismas transacciones con tradas de datos aplicándolas sobre los registros de la base de datos real. Estos registros deber copiados en un dispositivo de almacenamiento de acceso directo a fin de evitar su modific por efectos de la prueba. El punto fundamental del enfoque de simulación paralela es la e ción de la comparación entre los resultados de dos sistemas diferentes que han recibido lo mos datos de entrada. La figura 28-2 ilustra acerca de la técnica de simulación paralela.

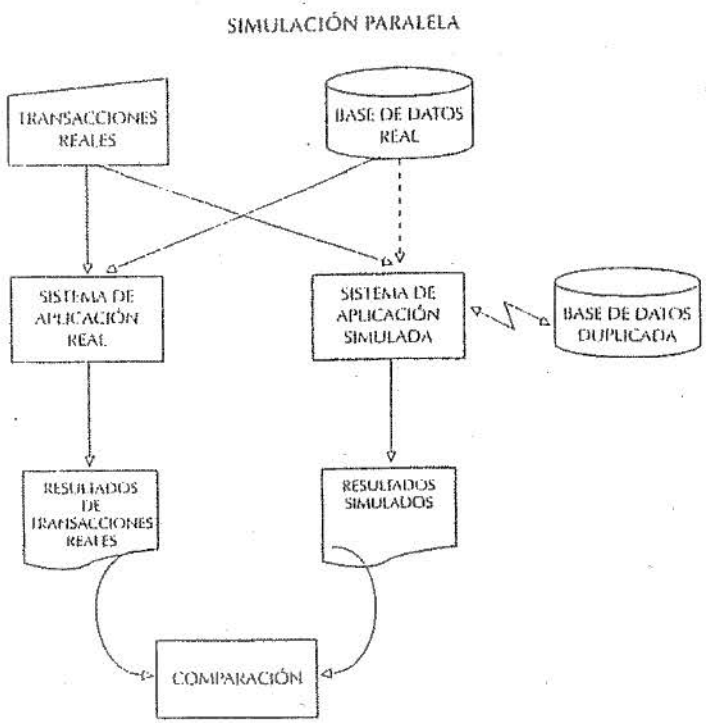

Figura 28-2. Ilustración gráfica del funcionamiento de la técnica de simulación paralela.

Tagging and tracing (Rotulación y rastreo)

Esta técnica se utiliza para auditar transacciones que son seleccionadas automáticamente en conformidad con la lógica del sistema y con el cumplimiento de determinados criterios establecidos por el auditor. Tiene las siguientes características.

1. Las transacciones seleccionadas deben ser marcadas por medio de una identificación. Existen dos maneras de marcar las transacciones. Una es reservar una posición en el registro elegido, a efectos de indicar que esa transacción ha sido señalada para su rastreo a través del sistema. La otra es utilizar un caracter dentro de un campo de un registro, que es el que indica esa situación.
2. El programa de aplicación debe contener instrucciones que reconozcan las transacciones identificadas.
3. Determinadas rutinas provocarán la impresión de la información relacionada con las transacciones seleccionadas; los módulos de selección y de reconocimiento deberán ser incorporados en la etapa de diseño del sistema. Esto implica la participación del auditor durante el desarrollo de la aplicación.

Las transacciones a seleccionar para el uso de esta técnica son, por lo general, aquellas que provienen de una operación que pueda dar lugar a una observación. Por ejemplo, estarían en esta situación aquellas compras efectuadas a proveedores no integrantes del archivo maestro de Proveedores, pagos efectuados en concepto de horas extraordinarias que excedan una cantidad máxima predeterminada, Notas de Crédito por devolución de mercaderías cuyo monto exceda una cantidad definida, etcétera.

Software de auditoría generalizado

El software de auditoría generalizado constituye un conjunto de programas de computación preelaborados que ejecutan, automáticamente, una variedad de tareas de auditoría. Evitan, de esta manera, efectuar tareas manuales en un proceso de revisión.

Debe destacarse que este software utiliza la computadora para ejecutar operaciones específicas sobre datos que ya están elaborados y disponibles para su lectura en lenguaje máquina. O sea que su objetivo no es evaluar programas de computación que procesen datos (como ocurre con el método *test deck* y con ITF). Su propósito es efectuar pruebas sobre los datos por sí solos. Se reconoce a esta técnica dentro de las denominadas pruebas sustantivas.

Si bien los programas ya están elaborados, es necesaria su adaptación a cada situación especial, a efectos de su aplicación. Por ejemplo, es necesario observar determinadas instrucciones relativas a características relevantes de los datos a revisar, tales como campos de interés, dimensión de cada campo, etc., que constituyen los denominados parámetros. Los parámetros,

junto con el software genérico de auditoría y los datos a auditar, serán sometidos al pro de revisión.

Los tipos de software de auditoría genérico incluyen las siguientes funciones:

1. Verificación de cálculos en archivos
   Se ejecutan rutinas que prueban la exactitud de operaciones aritméticas contenidas e archivos, así como también operaciones lógicas: determinación con respecto a si un n ro es mayor, igual o menor que otro. También pueden incluirse operaciones de cálcu porcentajes. La prueba puede ser realizada sobre una muestra o sobre todo el archivo. l gura 28-3 ilustra sobre el esquema de aplicación de software de auditoría generalizad

ESQUEMA DE APLICACIÓN DE SOFTWARE DE AUDITORIA GENERALIZADO

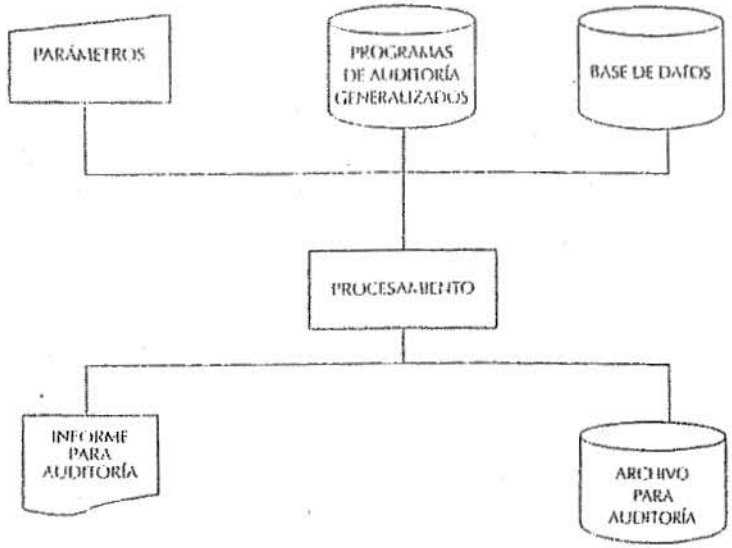

Figura 28-3. Ilustración gráfica del funcionamiento de software de auditoría generalizado (aplicación-verificación de cálculos en archivos).

2. Clasificación de registros
   En algunos casos, se facilita la revisión de los datos de un archivo si éstos se presenta un orden determinado que quizá no coincida con la secuencia en que se encuentra macenados. Por ejemplo, si se desean conocer fechas de cobranzas de un lote gran facturas, tal vez convenga ordenar las facturas por número de comprobante. Tam

   puede ser útil un ordenamiento determinado a efectos de una conciliación bancaria (comparación de extracto contra registración contable).

3. Comparación de datos
   Puede resultar necesario, a efectos de una revisión de auditoría, comparar datos de diferentes archivos para asegurar su sincronización.

4. Selección de muestras
   Un programa puede seleccionar una muestra de registros de un archivo conforme a especificaciones definidas por el auditor e ingresadas a través de parámetros. Este mecanismo permite un importante ahorro de tiempo al auditor en la ejecución de tareas rutinarias.

5. Investigar y recuperar
   Ciertas condiciones en la información almacenada, que no deberían presentarse, pueden investigarse (conforme a criterios especificados por el auditor) y dar lugar a la generación de informes de excepción. En esta situación se encontrarían, por ejemplo, ítems de inventario de escaso (o lento) movimiento, o saldos de cuentas a cobrar expresados en crédito.

6. Sumarización
   Puede ocurrir que el auditor necesite obtener totales o subtotales de importes contenidos en determinados campos de registros almacenados en archivos. Los programas de computación pueden agilizar significativamente estas operaciones.

7. Disposición de un archivo duplicado
   Puede ser útil para el auditor disponer de un archivo de Cuentas a Cobrar o a Pagar a efectos de gestionar confirmación de saldos de cuentas de clientes o de proveedores.

8. Impresiones específicas
   El auditor puede requerir un formato específico de impresión de informes para facilitar su labor de modo diferente del que resulta del programa de aplicación. De ahí la importancia de disponer de un programa de salida específica para auditoría.

El software de auditoría generalizado provee al auditor de un alto grado de independencia, particularmente respecto del personal de procesamiento de información.

TRANSFERENCIA DE INFORMACIÓN HACIA UN *MAINFRAME* (*UPLOADING*) Y DESDE UN *MAINFRAME* (*DOWNLOADING*)

A efectos de facilitar el análisis del auditor, puede convenir transferir datos desde una *mainframe* a una PC. Se tratará, en este caso, de transacciones seleccionadas. Luego del manejo de los datos

por parte del auditor, éstos deben ser transferidos desde la PC a la *mainframe*. Se requiere ur daloso manipuleo de información para evitar pérdida de su integridad.

Sistemas expertos

Para el futuro se prevé una creciente utilización de estas nuevas formas que surgen de la inve ción en inteligencia artificial, que consiste en la aplicación de reglas provistas por personas ex en el tema tratado. De manera que, luego de ingresados los datos de entrada, el sistema expert berá interpretar el problema y brindar las recomendaciones para su solución.

Capítulo 29

Recuperación de desastres: Continuidad de operaciones

Introducción

El desarrollo de sistemas de información procesada por computadora ha llevado a concentrar una cantidad significativa de datos de una organización en un área muy reducida, lo cual acrecienta la vulnerabilidad de las organizaciones en cuanto a la posibilidad de perder información, o bien debilitar su capacidad para procesar datos.

De ahí surge la importancia de analizar y evaluar las políticas y los procedimientos relativos a la planificación para la atención de contingencias, de modo de devolver a la organización su capacidad de respuesta para afrontar desastres o actuar ante situaciones de emergencia. Esta planificación es responsabilidad de la gerencia superior, a causa de que a ella se le ha confiado la salvaguardia y viabilidad de la empresa.

Dentro de estos aspectos, la tarea fundamental del auditor de sistemas de información es prever las acciones necesarias para asegurar la continuidad de operaciones, aun en situaciones de emergencia o ante la presentación de un desastre. La implantación de procedimientos rigurosos de seguridad reduce el riesgo, pero no lo elimina totalmente. Por eso es imprescindible para una organización que utilice procedimientos de procesamiento electrónico de información, y que formule y disponga de un adecuado plan de emergencia debidamente documentado y de aplicación práctica y efectiva.

Los temas que forman parte de la planificación de emergencias se enuncian a continuación.

1. Evaluación de riesgos.
2. Formulación de un plan de contingencias. Prueba y mantenimiento.
3. Alternativas de utilización de hardware, software y medios de almacenamiento.
4. Metodología para recuperación de desastres.
5. Contratación de seguros.
6. Técnicas de auditoría.

A continuación se describirán los temas indicados más arriba.

Evaluación de riesgos

Los riesgos que aquí interesan son los vinculados con la posibilidad de presentación de un c tre. Un desastre es todo suceso sujeto a un cierto grado de incertidumbre, en cuanto a su ocu cia, pero que cuando ocurre tiene potencial como para interrumpir o afectar seriamente l tión normal de un negocio.

Los desastres pueden provenir de hechos naturales (tales como incendios, inundacion rremotos) o bien de acciones malintencionadas (agresión física contra equipos, robo de inf ción, relaciones laborales).

Los riesgos deben ser clasificados, a efectos de priorizar las acciones, en conformidad c sensibilidad al tiempo (necesario para que se reanude el negocio luego de la ocurrencia de u sastre). La evaluación del riesgo debe considerar la tolerancia del sistema; esto es, la capacid enfrentar una interrupción de los sistemas. La tolerancia puede ser expresada como un valor netario. En función del grado de tolerancia, los sistemas pueden ordenarse según se muest el cuadro de la figura 29-1.

	CRÍTICOS	VITALES	SENSIBLES	NO CRÍTIC
Tolerancia a la interrupción	Muy baja (Costo de interrupción muy alto)	Moderada (Costo de interrupción ligeramente menor)	Flexible (costos tolerables)	Amplia (Costo esca o costo adicional m
Reemplazo de funciones	No pueden ser reemplazadas por métodos manuales	Puede ejecutarse manualmente por períodos breves	Pueden realizarse en forma manual por períodos relativamente largos. Exige mano de obra adicional	Pueden reemplazarse poco esfuer

Figura 29-1. Ordenamiento de los sistemas en función de su grado de tolerancia (capacidad para enfrentar una interrupción).

Las organizaciones que disponen de alto nivel de automatización están sometidas a ma riesgos que aquellas escasamente mecanizadas. Las primeras, en caso de emergencias, ter mayores dificultades para restaurar sus procedimientos, y además tendrán menor capa para procesar sus datos.

Las consecuencias de una interrupción de sistemas críticos o vitales pueden ser l guientes:

1. Imposibilidad de facturar a clientes.
2. Incapacidad para reclamar el pago de sus créditos.
3. Desconocimiento del nivel de existencia de materias primas y productos terminados.
4. Imposibilidad de programar y controlar la producción.
5. Incapacidad para liquidar correctamente las remuneraciones.

Formulación de un plan de contingencias

La empresa debe estar en condiciones de reconocer en qué nivel de emergencia se encuentra cuando se presenta una situación de interrupción de operaciones. Una clasificación puede determinar los siguientes niveles:

a) Catástrofe

Se trata de interrupciones en la capacidad de procesamiento provocadas por la destrucción de instalaciones y de los componentes físicos que las integran. En estos casos, se requiere acudir, transitoriamente, a otra instalación alternativa de configuración similar a la destruida. Simultáneamente, debe comenzarse a equipar una nueva instalación que, a muy corto plazo, tenga capacidad de procesamiento continuo del servicio de procesamiento de datos. Este reequipamiento incluye los dispositivos de conexión a telecomunicaciones.

b) Desastres

Se trata de interrupciones en la capacidad de procesamiento de información durante un período superior a un día, pero con altas posibilidades de reanudar las mismas en la instalación original luego de superados los inconvenientes causantes de la interrupción. Se deberá recurrir a una instalación de procesamiento alternativa utilizando copias de software y de archivos de datos conservados fuera de la sede original. La instalación alternativa deberá estar disponible todo el tiempo que dure la interrupción.

c) No desastres

Se trata de interrupciones breves (no mayores de un día). Son provocadas por mal funcionamiento de algún dispositivo o por fallas en el software no detectadas anteriormente y que requieren inmediata corrección.

Todo sistema, y con ello toda gestión empresaria, tiene un lapso crítico de recuperación. Este es el período o tiempo hasta donde puede extenderse una interrupción antes de que se presente el riesgo de incurrir en pérdidas. La naturaleza del negocio condiciona ese marco de tiempo o lapso crítico. Por ejemplo, las instituciones financieras en las que su "materia prima" es la información tienen un lapso crítico de recuperación menor que instituciones de otra naturaleza.

La formulación del plan de contingencias es responsabilidad de la gerencia superior. Esta debe asignar responsabilidades para el desarrollo e implementación, comprometer los recursos ne-

cesarios y fijar fechas de cumplimiento de objetivos. La participación del usuario también es vital para asegurar el éxito del plan: la capacitación del personal para identificar las aplicaciones críticas, conocer los mecanismos y sus tiempos de recuperación en caso de interrupción, debe ser constante y actualizada. El plan de contingencia contendrá lo siguiente:

1. Determinación del orden de prioridades en materia de recuperación de aplicaciones, software de base y archivos de datos. Ese ordenamiento estará en función del grado de tolerancia con respecto a la interrupción.
2. Formulación de un detalle del orden de procesamiento de tareas que lo requieran.
3. Mecanismos de acoplamiento a los sistemas manuales durante las interrupciones cortas.
4. El plan debe incluir no sólo las operaciones del *mainframe* sino también las que se realizan en sedes remotas. En este sentido, el usuario final deberá estar capacitado para participar en la identificación de funciones calificadas como críticas. Los resguardos de archivos de datos y del software de base y de aplicación (*back up*) deberá ser práctica de rutina para prever desastres.
5. Disponibilidad de hardware alternativo (*back up*). Deberá preverse dónde recurrir en caso de emergencia. Las alternativas posibles son:
   a) Centro de duplicado de procesamiento de información de propiedad de la misma empresa (para aplicaciones críticas). Es una solución eficaz (mayor facilidad de compatibilización y coordinación) pero costosa.
   b) Centros de procesamiento ubicados en otras sedes. En función del tiempo de activación y del costo, estos centros se clasifican en:
      - *Hot sites*:
        Son instalaciones completas, configuradas de manera similar a la sede primaria, y pueden activarse rápidamente.
      - *Warm sites*:
        Son instalaciones parcialmente configuradas en las que generalmente falta la unidad central de procesamiento. Dado que esta unidad es el dispositivo más costoso, esta alternativa es más económica.
      - *Cold sites*:
        Son lugares físicos que se encuentran en condiciones de recibir el equipamiento necesario, pero no dispone de instalaciones específicas.

   Los centros de procesamiento alternativo deben poseer las mismas condiciones de seguridad que la sede original. En el caso de los centros alternativos que no son propiedad de la empresa, ésta deberá documentar los arreglos que efectúe con los terceros. Los aspectos a cubrir en los contratos incluyen los siguientes temas: definición de la situación de emergencia; configuración disponible, incluyendo las comunicaciones; tiempo de respuesta (demora máxima en reiniciar las actividades); límite máximo de suscriptores por centro; lapso máximo de uso.
   Un modo contractual específico son los acuerdos de reciprocidad entre dos o más empresas; puede ocurrir en los casos de organizaciones con equipos o aplicaciones similares.

   Estos acuerdos reducen el costo, pero en la práctica pueden generar inconvenientes derivados de modificaciones no denunciadas, tanto en las configuraciones, condiciones de seguridad, tiempo disponible para operar, confidencialidad de los datos, etcétera.
6. Disponibilidad en la capacidad de telecomunicaciones para mantener activos los procesos críticos del negocio. Los componentes y métodos más utilizados con este propósito son los siguientes:
   a) Rutas alternativas (redes, circuitos, terminales). Se utilizan cuando se interrumpa la red normal.
   b) Rutas diversificadas: si un cableado de respaldo se encontrara en la misma cañería que aquél al que respalda, podría sufrir los mismos riesgos que este último. Para evitar esta exposición a riesgos, pueden duplicarse las instalaciones cuando se dispone de rutas diversificadas de entrada dual.
7. Disponibilidad de una sede alternativa para almacenamiento de medios magnéticos y documentación. Todo plan de recuperación debe tener como medida preventiva la disponibilidad de un lugar físico distinto del habitual para almacenamiento de los datos de *back up* del software (sistemas operativos, compiladores, utilitarios, programas de aplicación) y de la documentación. La periodicidad del proceso de *back up* de datos dependerá de la naturaleza de la aplicación. La programación de los *back up* puede efectivizarse a través de un sistema de administración automatizada de cintas y software de *job scheduling* (programación de tareas) automatizado. La documentación a resguardar incluye las carpetas descriptivas de los sistemas en aplicación, la descripción de los procedimientos operativos (corridas de aplicaciones, instrucciones para ejecución del plan de trabajos y operaciones de excepción), documentos fuente para entrada de datos y documentos de salida imprescindibles como fuentes de información.

Metodologías de recuperación

Un plan de contingencia debe apoyarse en una metodología que establezca los pasos a seguir en situaciones de emergencia (estrategias), así como también en los responsables de su ejecución y de su tiempo. Los pasos serán los siguientes:

1ª acción:	protección de la vida humana.
2ª acción:	evaluación de daños y estimación de tiempo necesario para la recuperación.
3ª acción:	coordinación de las actividades de recuperación; recuperar datos vitales y críticos y reconstruir la base de datos; instalar y probar el software en la sede alternativa, operar desde ésta y reorientar el tráfico de comunicaciones.
4ª acción:	restauración del software de base y de aplicación en la sede alternativa.
5ª acción:	recuperación de red; redireccionar el tráfico de comunicaciones.

6ª acción: preparación de datos y registros; supervisar los trabajos de obtención de datos fuente y de su carga y actualización de la base de datos.

7ª acción: almacenamiento en sede alternativa: formular un cronograma y vigilar el cumplimiento de las actividades a desarrollar en sede alternativa para el almacenamiento de la información inicial y de la que se vaya generando durante el proceso de recuperación.

8ª acción: administración de las acondiciones de seguridad.

9ª acción: provisión de apoyo administrativo; tareas de control y balanceo de datos ingresados, datos procesados e información que egrese.

10ª acción: gestión de aspectos legales derivados de la emergencia (demora en cumplimiento de obligaciones, incumplimiento de contratos), aspectos financieros (modificación del flujo de fondos) y, si fuera necesario, atención de las relaciones públicas o institucionales.

El plan de contingencia debe mantenerse actualizado. Diversos factores pueden alterar, en el tiempo, los mecanismos previstos para un plan determinado: modificación de la estrategia del negocio de la empresa, que puede alterar la calificación del grado de criticidad de las aplicaciones; evolución de los componentes de hardware y software, etcétera.

Técnicas de auditoría y funciones del auditor de sistemas de información

La revisión de la continuidad de operaciones exige del auditor de sistemas de información la ejecución de las tareas que se indican a continuación.

1. Evaluación del plan de contingencias: verificación de su adecuación y actualización y de su capacidad para permitir reiniciar el procesamiento de información luego de una interrupción imprevista. Verificación de que e plan considere desastres de diverso grado. Verificación de que contemple no sólo las aplicaciones desarrolladas para *miniframes* sino también para los sistemas basados en PC o desarrollados por usuarios finales. Verificación de que para cada aplicación se haya determinado su nivel de tolerancia en caso de desastre.
2. Examen del inventario detallado de los elementos almacenados en la sede alternativa: archivos de datos, software de sistemas y de aplicaciones, documentación actualizada de sistemas y de aplicaciones, insumos necesarios.
3. Evaluación del grado de capacitación del personal a efectos de poder enfrentar con éxito la aplicación del plan de contingencia: verificación de las precisiones con respecto a las responsabilidades asignadas a cada integrante de la dotación de personal
4. Verificación de que el plan contemple los mecanismos de fusión de los datos obtenidos o procesados durante el período de emergencia, con los existentes antes del desastre: análisis de los métodos de control de seguridad.

5. Evaluación de las condiciones de seguridad física de la instalación alternativa, en cuanto a controles de acceso.
6. Examen del contrato de procesamiento alternativo con el proveedor de la instalación: análisis de las cláusulas referentes a derechos y obligaciones de las partes (observar que su redacción pueda ser comprendida por un juez).
7. Evaluación de los resultados de pruebas anteriores (registrados como documentación histórica): determinación de los resultados esperados, si es que es necesario ajustar algunos mecanismos.
8. Análisis de la cobertura de seguros: verificar qué rubros son cubiertos por el seguro: seguros de los empleados ubicados en la sede alternativa; daño físico contra el Centro de Procesamiento de Información y contra sus instalaciones; costos de programación para reproducir los medios de almacenamiento dañados; costos de los esfuerzos extraordinarios de contingencia; pérdida de ganancias provocada por la suspensión de operaciones a causa de daños de los medios de procesamiento de información; responsabilidad legal por errores u omisiones cometidos por analistas o diseñadores de software, que puedan afectar financieramente a un cliente; cobertura de transporte de medios magnéticos (asegurarse si deben o no estar microfilmados antes de su transporte para que el seguro responda por su protección); cobertura de fidelidad frente a actos deshonestos. En el cálculo de la prima a cobrar, las compañías de seguros suelen observar los planes de emergencia y de seguridad que presentan sus clientes: si los consideran adecuados, las primas serán más reducidas.

COPY.AR
Fotocopias - Impresiones - Anillados
French 414 - UTN - 1°Piso