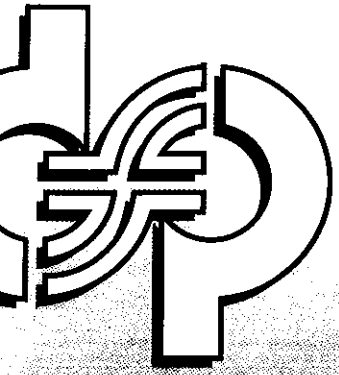

Federación Argentina
de Consejos Profesionales
de Ciencias Económicas

TRO DE ESTUDIOS CIENTÍFICOS Y TÉCNICOS (CECyT)

INFORME N° 15

ÁREA AUDITORÍA

AUDITORÍA EN AMBIENTES COMPUTARIZADOS

Autores
Leopoldo Cansler - Luis Elissondo
Luis A. Godoy - Ricardo Rivas

FEDERACIÓN ARGENTINA DE CONSEJOS
PROFESIONALES DE CIENCIAS ECONÓMICAS
(FACPCE)

CENTRO DE ESTUDIOS CIENTÍFICOS Y TÉCNICOS
(CECYT)

INFORME Nº 15
ÁREA AUDITORÍA

AUDITORÍA EN AMBIENTES COMPUTARIZADOS

AUTORES

Leopoldo Cansler
Luis Elissondo
Luis A. Godoy
Ricardo Rivas

Informe Nº 15: Area Auditoría - 1ª ed. - Buenos Aires
Fed. Argentina de Consejos Profesionales de Ciencias Económicas, 2007.
64p.; 22x16 cm.

ISBN 978-987-1346-02-8

1. Auditoría Contable
CDD 657

Fecha de catalogación: 25/04/2007

PRÓLOGO

El trabajo desarrollado por los Investigadores del CECYT viene a remplazar el Informe Nº 6 del Área de Auditoría denominado "Pautas para el examen de estados contables en un contexto computadorizado" que fuera realizado muchos años atrás, por un numeroso grupo de profesionales especializados en Sistemas y en Auditoria de Estados contables y del que tuve el honor de formar parte.

Aquel informe pudo cumplir acabadamente su cometido llenando un vacío doctrinario en un área particularmente sensible pero como ocurre a menudo, con el correr de los tiempos quedó parcialmente desactualizado.

Por tal motivo, se solicitó a los colegas Cansler, Elissondo, Rivas y Godoy "aggiornar" aquel trabajo incorporando los nuevos conceptos y desarrollos reconociendo la importancia creciente de la tecnología de la información. Así entonces, el Informe COSO (Committee of Sponsoring Organizations of the Treadway Commission), COBIT (*Control Objectives for Information and related Technology), SAC (Systems Auditability and Control Report), las normas y declaraciones internacionales de auditoría y mucho otro material* han sido tenidos en cuenta para preparar el presente trabajo.

Este informe tiene como objetivo ayudar al Contador en su trabajo de auditoría en entes con sistemas de información por computadora sin que se requiera para ello ser un especialista en sistemas. Se trata, entonces, de una obra corta, de fácil lectura y rápida comprensión que contiene lo esencial, lo importante, lo significativo.

Desde que un ambiente como el señalado puede afectar los procedimientos seguidos por el auditor para obtener una comprensión suficiente de los sistemas de contabilidad y control interno, la consideración del riesgo inherente y del riesgo de control a través de la cual el auditor llega a la evaluación del riesgo y el

diseño y desarrollo de pruebas de control y procedimientos sustantivos para cumplir con el objetivo de la auditoría, el presente Informe lo ayudará a obtener el conocimiento necesario para diseñar el plan de auditoría, dirigirlo o ejecutarlo y finalmente evaluar el trabajo desarrollado emitiendo las respectivas conclusiones.

Dr. Cayetano A. V. Mora
Ex Director del Área de Auditoría del CECyT

ÍNDICE

AUDITORÍA EN AMBIENTES COMPUTARIZADOS

1. Introducción

1.1. Objetivo y alcance

El presente Informe se emite para facilitar la comprensión de los procedimientos de auditoría que se deben aplicar en ambientes computarizados, con el propósito de realizar las comprobaciones pertinentes y obtener evidencias válidas y suficientes respecto de las afirmaciones contenidas y la información expuesta en los Estados Contables.

El objetivo de una auditoría de estados contables es hacer posible que el auditor exprese una opinión, acerca de la correspondencia de la preparación de los Estados, en todo lo significativo, con el conjunto de normas que lo regulan.

Puede afirmarse que el objetivo y alcances globales de una auditoría no cambia bajo un ambiente de Sistemas de Información Computarizada (SIC). Sin embargo, el uso de computadoras puede, y efectivamente produce cambios significativos en el ingreso, procesamiento, almacenamiento y comunicación de la información contable y, por tal razón, tener efecto sobre los sistemas de contabilidad y control interno, empleados por el ente.

Un ambiente SIC puede afectar:

- Los procedimientos seguidos por el auditor para obtener una comprensión suficiente de los sistemas de contabilidad y control interno.
- La consideración del riesgo inherente y del riesgo de control a través de la cual el auditor llega a la evaluación del riesgo, y
- El diseño y desarrollo de pruebas de control y procedimientos sustantivos apropiados para cumplir con el objetivo de la auditoría.

El auditor debería obtener suficiente conocimiento del SIC, para estar en condiciones de:

- diseñar el plan de auditoría,
- dirigirlo o ejecutarlo, y
- finalmente evaluar el trabajo desarrollado, habiendo considerado en su oportunidad si cuenta con los conocimientos específicos para la realización del trabajo.

1.2. Descripción del ambiente de sistemas de información computarizada (SIC)

Como ya se ha mencionado, debe tenerse presente que el objetivo y alcance generales de la auditoría, no cambian en un entorno SIC. Sin embargo, el uso de un computador produce cambios de distinta naturaleza y magnitud en el ingreso, procesamiento, conservación o almacenamiento de la información contable y en su comunicación posterior.
Por ello, puede afectar la organización y los procedimientos empleados por el ente para lograr un adecuado control interno. Cuando la información contable es procesada, total o parcialmente, por computadora deberá entenderse que el ámbito donde se realiza la auditoría es computarizado.

1.2.1. Elementos que componen el ambiente SIC

A continuación se describen los principales elementos que componen el ambiente SIC:

- **Planificación y Organización del Área de Sistemas**:
  Comprende la planificación estratégica de los sistemas de información, estructura y funciones del área sistemas y la existencia de políticas y procedimientos relacionados.

  - Planificación
    - Existencia de un plan de sistemas a corto y largo plazo debidamente formalizado y aprobado.
    - El plan de sistemas debe encontrarse adecuadamente integrado con los objetivos del negocio.

    - El plan de sistemas debe ser revisado y actualizado periódicamente, según los cambios que se produzcan en prioridades, requerimientos u objetivos del negocio, o nuevas demandas de naturaleza fiscal o legal que requieran ajustes en el SIC para que la organización pueda cumplimentarlas.
    - Es necesario que existan procedimientos formales establecidos para el proceso de planificación
    - El plan es adecuadamente comunicado a todos los involucrados.

  - Organización del área de sistemas
    - Existencia de una estructura claramente establecida y formalizada
    - Descripción de puestos y funciones que fije una adecuada segregación de funciones a través del establecimiento de los roles y responsabilidades respecto de las actividades de: desarrollo de software, adquisición, mantenimiento en particular, y aspectos de seguridad involucrados en la ejecución de las demás actividades funcionales en general.
    - Existencia de personal competente para cada una de los roles establecidos, que al mismo tiempo posea un adecuado grado de conciencia sobre las actividades de control involucradas

  - Definición de políticas y procedimientos
    - Un grado adecuado de formalización de las políticas y procedimientos relacionados con el ambiente SIC.
    - Revisión y actualización periódica de las políticas y procedimientos.
    - Comunicación de las políticas y procedimientos a los miembros de la organización alcanzados por las mismas.

- **Datos**
  Es el elemento básico de los sistemas de información.
  De su adecuado tratamiento depende la calidad de la información que luego se genere.

  - Debe encontrarse claramente establecida la responsabilidad por el ingreso de los datos. Sobre este punto hay que tener presente que el ingreso de los datos puede ser realizado desde distintas fuentes:
    - Por empleados de la organización que deben tener la autorización (el perfil de seguridad) requerida para realizar dichas tareas.
    - Por terceros ajenos a la organización: clientes o proveedores que realizan operaciones a través de internet, u otros dispositivos destinados a tal fin, tales como, entre otros: cajeros automáticos, terminales de autoconsulta, etc.
    - A través del intercambio de datos con otras organizaciones. (Intercambio electrónico de datos - EDI). Por medios magnéticos que contengan información para ser incorporada a los sistemas de información (SIC) de la organización.

  - **Documentación de Respaldo**: la información ingresada debe encontrarse sustentada en transacciones debidamente acreditadas, con los comprobantes respectivos, o a través de medios de efecto equivalente (en el caso de transacciones electrónicas).

  - **Control en el ingreso de los datos**: Los sistemas tienen que contemplar controles (validaciones y consistencias) que permitan asegurar la calidad de la información que se esta ingresando.

  - **Procesamiento de los datos:** El procesamiento comprende el tratamiento que los sistemas de información realizan de los datos ingresados. Son elementos indicativos de ello:
    - Los archivos maestros son adecuadamente actualizados por la información ingresada.
    - Las funciones de procesamiento son realizadas por las personas autorizadas a ello.
    - Existe un registro y se realiza el seguimiento de las transacciones rechazadas.
    - Se efectúa un adecuado registro del seguimiento de los errores que se producen.
    - Existe un registro o log de las transacciones críticas que se realizan y el mismo es revisado periódicamente.
    - Se depuran los datos para evitar la permanencia de aquellos erróneos o sin valor que puedan afectar el mismo procesamiento o la calidad de la información generada.

- **Sistemas de Aplicación**:
Comprende el desarrollo, adquisición, mantenimiento, soporte e implantación de sistemas de información computarizados. Es necesario que:
  - Exista una metodología para el desarrollo de aplicaciones y esta sea aplicada efectivamente en su totalidad.
  - Se hayan determinado métodos que permitan evaluar la adecuada calidad de las aplicaciones que se implementan.
  - Existan pautas o procedimientos específicos establecidos para la solicitud e instrumentación de cambios en las aplicaciones.
  - La puesta en marcha de nuevas aplicaciones o modificaciones a las existentes se encuentren adecuadamente autorizadas, como condición previa a su instalación.
  - Se disponga de mecanismos adecuados para dar soporte a los usuarios y se lleve un registro estadístico de los requerimientos realizados.

- Exista una política y procedimientos predefinidos para el caso en que las aplicaciones sean contratadas a terceros.

- **Infraestructura Tecnológica**:
Comprende el hardware (equipos de computación), dispositivos de comunicaciones, sistemas operativos, sistemas de bases de datos, instalaciones, y demás componentes necesarios para poder llevar a cabo el procesamiento de los sistemas de información (SIC) .Es necesario que:
  - Exista una planificación de los recursos tecnológicos utilizados por la organización, que se encuentre coordinada con los requerimientos del Plan de Sistemas de la misma.
  - El equipamiento que se utiliza cumpla con los estándares establecidos por la organización.
  - El software de base en uso se encuentre debidamente actualizado.
  - Las instalaciones sean adecuadas para el desempeño de las actividades y se respeten las medidas de seguridad establecidas.
  - Se desarrolle una actividad de monitoreo de la oferta tecnológica, de manera tal que permita establecer el rumbo a seguir por la organización en este campo, tomando en cuenta aspectos de operatividad, economicidad y productividad.

- **Seguridad y Continuidad de las operaciones**:
Comprende la seguridad física y lógica y el plan de "continuidad del negocio" (cobertura de contingencias que puedan afectar, total o parcialmente, las operaciones de la organización). La actividad a prever tiende a preservar el concepto de "Empresa en Marcha consagrado por las normas profesionales vigentes y por las normas internacionales de auditoría, las que se encuentran actualmente en proceso de adaptación para su adopción, de acuerdo a lo resuelto por la Junta de Gobierno de la FACPCE.

Uno de los objetivos del plan es brindar a la organización la habilidad para continuar las operaciones críticas, administrando la disponibilidad de los recursos y datos de los sistemas de información, en la eventualidad de una interrupción del procesamiento, lo cual requiere de un cuidadoso y detallado desarrollo de procedimientos de back-up y recupero de desastres.

Se requiere que:

- Existan políticas de seguridad física y lógica establecidas formalmente.
- Las políticas de seguridad sean comunicadas a todos los involucrados.
- Se genere un plan de "continuidad del negocio" que permita asegurar de manera razonable la continuidad en las operaciones esenciales de la organización sustentadas en sistemas de información computarizados.
- El plan de continuidad se encuentre actualizado, haya sido comunicado a todos los involucrados, y se realicen pruebas periódicas (simulacros totales o parciales) para comprobar su funcionamiento y efectividad.

- **Actividades de Monitoreo de los Sistemas de Información**
Comprende las actividades realizadas por la organización para determinar el grado en que se satisfacen los objetivos establecidos para el área. Es recomendable que:
  - Exista un área que se encargue de monitorear las actividades realizadas en el ambiente SIC.
  - Los hallazgos sean comunicados oportunamente a los niveles directivos.
  - Se realice un seguimiento adecuado y oportuno de las medidas correctivas que la organización haya instrumentado.

1.2.2. Elementos que determinan el grado de impacto del ambiente SIC

La importancia y complejidad del procesamiento realizado por medio de computadoras, tiene que ver con la significación de las afirmaciones de los estados contables que se encuentran vinculados al referido proceso y el grado de complejidad, tiene que ver con cuestiones como las que se detallan a continuación. Ambas circunstancias determinan el impacto que produce este ambiente.

- Alto porcentaje de procesos computarizados sustanciales de la organización que generan información para los estados contables.
- Alto volumen de transacciones que impide la adecuada identificación y control de los errores de procesamiento a través de aplicación de técnicas tradicionales.
- Elevada proporción de transacciones generadas automáticamente hacia otras aplicaciones o recibidas automáticamente desde otras aplicaciones.
- Existencia de áreas de desarrollo de nuevos sistemas y mantenimiento de los existentes.
- Cambios continuos en los sistemas de información, esencialmente originados en nuevas demandas de los distintos sectores de la organización.
- Aplicación extendida de la modalidad de "intercambio electrónico" de transacciones con otras organizaciones (EDI)
- Operaciones de negocio implementadas a través del uso de aplicaciones vía WEB (por Internet o por redes privadas -Intranet/extranet-), que implican una fuerte interacción con clientes y proveedores.
- Utilización intensiva de sistemas de información computarizados (SIC) para asistir la toma de decisiones (sistemas de información gerenciales, sistemas de soporte a las decisiones, herramientas de análisis de datos para la revisión de la toma de decisiones u otros

programas de estas características).

- Grado de descentralización importante de las actividades de SIC.
- Alta proporción de procesos sustanciales de la organización que se encuentran tercerizados.

1.2.3. Efectos sobre el trabajo del auditor

Para establecer el grado de confianza del auditor en el ambiente SIC es conveniente que se analice, por un lado el impacto y por otro lado, la situación en la que se encuentra cada uno de los componentes de dicho ambiente. Estos elementos determinarán el grado de confianza en el mismo y, por lo tanto, el alcance, naturaleza y oportunidad de los procedimientos de auditoría que el auditor deba desarrollar.

1.3. Impacto sobre la estructura de control de las organizaciones

El desarrollo de la Tecnología Informática y sus aplicativos, orientados a la gestión de las diferentes metodologías implementadas en campos de la administración y de la contabilidad, tienen un importante efecto sobre las actividades de control establecidas en las organizaciones.

La utilización de las herramientas tecnológicas y su permanente evolución, con la aparición de nuevos desarrollos, produce efectos significativos en las estructuras de controles, que hacen necesario introducir cambios sobre ellas.

La precitada evolución incluye la generación de herramientas de desarrollos informáticos, la incorporación de la imagen al proceso y el intercambio electrónico de datos.

Como consecuencia de esa permanente evolución tecnológica, los sistemas expertos, en un futuro no lejano, se encontrarán incorporados a muchas aplicaciones, de sistemas de información, oportunidad en la que sobre aquellos utilizados por las empresas que se audite, se deberán aplicar procedimientos que permitan un adecuado control de su funcionamiento.

En este sentido y tal como se menciona en el Informe COSO (Committee of Sponsoring Organizations)[1] el control se efectuaría de la misma manera que antes, es decir, a través de "actividades de control adaptadas a los objetivos".
Para asegurar los controles adecuados sobre las aplicaciones utilizadas, es necesario establecer políticas y procedimientos acordes al nivel de complejidad y desarrollo alcanzado.
Las transformaciones producidas sobre ambientes tienen que ver con:

- la información globalizada, intercambiada sin limitaciones de tiempo,
- la dependencia con la información y con los sistemas que la proveen,
- el aumento de la vulnerabilidad de las estructuras y la amplitud de las amenazas,
- el costo de las inversiones en sistemas de información, y
- la manera en que las tecnologías influyen sobre las organizaciones.

Ante este panorama es necesario comprender y manejar las técnicas para la identificación y evaluación de los riesgos que surgen como consecuencia de los cambios tecnológicos.
Con respecto a los recursos, se debe optimizar el uso de aquellos que las organizaciones disponen, incluyendo las personas, instalaciones, tecnología, sistemas de aplicación y datos. Para el logro de este objetivo, es necesario establecer un sistema adecuado de control interno, el que debe brindar soporte a los procesos de negocio, definiendo cómo cada actividad de control afecta a los recursos y satisface los requerimientos de información.
Se aprecia una creciente necesidad de garantizar a los usuarios y a las organizaciones, que existen seguridad y control adecuados. La tarea del auditor, como siempre, está comprometida con la evaluación

[1] Committee of Sponsoring Organizations of the Treadway Commission. Los nuevos conceptos del control interno. Ediciones Díaz de Santos. Madrid. 1997.

y propuestas de mejoramiento de las estructuras de control, que la empresa y sus operadores deben implementar y mantener.
Se puede reseñar, como causas de incidencias sobre las estructuras de controles y en la tarea del auditor a las siguientes:

- Los avances tecnológicos pueden influir en la naturaleza y la evolución de los trabajos en producción, administración, investigación y desarrollo, o provocar cambios respecto a los suministros.
- En el proceso de información: se deben incorporar una serie de controles, adaptados a la naturaleza informática del proceso, para comprobar la exactitud, totalidad, autorización y pertinencia de las transacciones.
- Funciones contables tales como cálculo, resumen y clasificación, o también controles, son llevados a cabo a través de programas de computación.
- El almacenamiento de información soportado en medios magnéticos tales como disquetes, casetes, cintas, discos, CD, microfilme u otros dispositivos, no son legibles a simple vista.
- Puede existir concentración de funciones e información, en base a las facilidades que provee la mencionada tecnología, hecho que en determinados casos, puede entrar en abierta colisión con premisas básicas de control.
- Pueden efectuarse transmisiones de datos por medio de las telecomunicaciones, eliminando la barrera de las distancias y facilitando la interconexión o interrelación directa entre distintas áreas de una misma organización o con otras organizaciones diferentes distribuidas geográficamente. Esta posibilidad trae aparejado riesgos, en cuanto a la seguridad de las comunicaciones, a la integridad de los datos y aún a las relaciones internacionales en orden al cumplimiento de las normativas vigentes en cada país.
- Puede existir encadenamiento de los sistemas de información, de tal modo que un acto administrativo genera registros subsecuentes hasta llegar a los estados contables,

sin la existencia de documentos intermedios visibles que respalden la operación, tal como, por ejemplo, la liquidación de remuneraciones al personal, donde el asiento contable se genera y registra automáticamente, en función de la información analítica procesada que cuenta con la correspondiente imputación a cuentas contables.

- Puede haber procesamiento de transacciones, sin la existencia visible de documento fuente, como por ejemplo, el caso de las operaciones por medio de cajeros automáticos, o los pagos por transferencias electrónicas de datos utilizando las facilidades de sistemas de información computarizados específicos (de uso estándar o provistos por las mismas entidades financieras).

Los hechos señalados anteriormente pueden producir los siguientes efectos

- Las fallas en los sistemas de información computarizados pueden perjudicar significativamente las operaciones del ente.
- Los cambios en la separación de funciones y en la oposición de intereses tradicionales en el desarrollo de las tareas administrativas y contables son capaces de debilitar el control interno.
- Mayor vulnerabilidad de la organización como resultado de la concentración de la información.
- Posibilidad de disponer de mayor información en menor tiempo y con diferentes ordenamientos.
- Aumento de las posibilidades de ejercer controles, a través de su automatización.
- Posibilidad de efectuar procedimientos de auditoría con mayor alcance y rapidez, como resultado de la automatización de las operaciones y el uso de herramientas computarizadas.
- Cambios en el comportamiento administrativo y en el modo de ejecutar los procesos.
- Posibilidad de limitar, por medio del uso de los recursos y

facilidades disponibles, el acceso a la modificación y/o lectura de datos e información almacenada o procesada (uso de "perfiles de usuarios" y posibilidad de acotar su acceso, y alcances, a recursos físicos y lógicos y su preservación a través de "claves de acceso"). Estas utilidades permiten a la empresa implementar controles en el primer nivel de aplicación y a la auditoría verificar el cumplimiento.

- Cambios en las pistas o rastros tradicionales que necesita el auditor para su examen.

2. El ambiente de riesgos y controles

El control interno se define[2] como un proceso efectuado por la dirección, la gerencia y otros miembros de una organización, destinado a proporcionar una seguridad razonable, en cuanto al logro de objetivos, en los siguientes aspectos:

- efectividad y eficiencia de las operaciones,
- confiabilidad de la información administrativa y contable, y
- cumplimiento de las leyes y normas aplicables.

Está conformado por cinco componentes interrelacionados e integrados en el proceso de gestión gerencial de la organización. Dichos componentes son:

- **Ambiente de Control**
- **Evaluación de Riesgos**
- **Actividades de Control**
- **Información y Comunicación, y**
- **Monitoreo**.

Para eliminar o disminuir el riesgo de ocurrencia o bien limitar las consecuencias de una contingencia una vez ocurrida, es necesario instrumentar distintos tipos de controles.

El riesgo es cuantificable y dependiendo del procedimiento que lo controla, su incidencia en los resultados no es absoluta.

Los **SIC** (Sistemas de Información Computarizada) están

[2] Committee of Sponsoring of the Treadway Comisión (COSO). Los nuevos conceptos del control interno. Obra citada.

conformados por: equipos, programas que los hacen funcionar para obtener ciertos resultados, personas que los operan y programan y datos sobre los cuales actúan.
Los procedimientos de controles a instrumentar, en ambientes de SIC, pueden ser clasificados en Controles Generales y Controles de las Aplicaciones.
Los Controles Generales son aquellos que se ocupan de todo cuanto incide en la totalidad del ambiente y no es específico de las Aplicaciones (controles programados). Los Controles Generales proponen el establecimiento de estándares para controlar el diseño, seguridad y uso de los programas de cómputo y la seguridad de los archivos de datos en toda la institución.
Los Controles de Aplicación son controles específicos únicos para cada aplicación computarizada, como nómina, cuentas por cobrar y procesamientos de pedidos. Consisten en controles aplicados desde el área funcional de usuarios de un sistema en particular o de procedimientos previamente programados. Más concretamente aplicaciones que se refieran a las actividades propias del negocio donde se utilizan.
Estos controles se instrumentan a través de una serie de procedimientos, que se tratan en los puntos que se irán desarrollando seguidamente.

2.1 Consideraciones generales

Tomando las definiciones sobre control contenida en las normas internacionales de auditoría, las que coinciden en sus aspectos principales con las enunciadas en modelos de gran aceptación, como el mencionado Informe COSO y conceptos coincidentes adoptados por las normas argentinas vigentes, se desarrollan los puntos siguientes.

2.2 Evaluación de los procedimientos generales de control

Los objetivos de control son los que la Organización desea

cumplir para minimizar o eliminar los riesgos.
Si la organización no establece controles internos se expone a los siguientes riesgos:

Fraude
Pérdidas de beneficios. Daños a la imagen de la empresa.

Interrupción del negocio:
Pueden interrumpirse sus operaciones, perder beneficios y pérdida de competitividad y marketing.

Errores:
Puede resultar información errónea lo cual puede conducir a tomar decisiones equivocadas.

Clientes insatifechos:
Un entorno de control débil puede impactar en las habilidades de la empresa y perder clientes o no renovarlos.

Uso ineficiente de recursos:
Si no son usados en forma eficiente no satisfacen las necesidades del negocio y de los clientes.
Los objetivos de control se pueden clasificar en:

Validez (o utilidad) de la información:

Seguridad

Conformidad

a. **Validez de la información:** Los controles deben asegurar la integridad, confidencialidad y oportunidad de la información. El dato, que es el elemento de la información es categorizado, sumado, ordenado, procesado y manipulado para formar la información para la toma de decisiones. El auditor debe evaluar los controles sobre los datos, transacciones y programas.
b. **Seguridad:** Incluye seguridad del Hard del Soft y de los datos. La seguridad es responsabilidad de todos y el compromiso de la Dirección es crítico. Los controles deben estar instalados para evitar pérdidas o destrucción y poder detectarlos si es que ocurre.

c. **Conformidad:** La conformidad tiene un impacto muy importante, está dada por a adecuación a normas y regulaciones legales.

Objetivos de control básicos

A título de ejemplo, se detallan algunos objetivos de control que se pueden considerar básicos en un ambiente SIC.

Acceso general a datos y programas

- El acceso a los sistemas de producción (programas, comandos de procesamiento, archivos de datos, etc.) debe estar debidamente controlado.
- El acceso físico al equipamiento de procesamiento de datos debe estar controlado.
- El uso y la administración de métodos de encriptación y autenticación debe estar controlado apropiadamente.
- Existe una función independiente y efectiva de seguridad de datos, la que es responsable de todos los aspectos de la seguridad de datos.
- Se controla el acceso al software de base y a los utilitarios sensitivos.
- Se monitorea el acceso y otras actividades de los usuarios.

Cambios a los programas

- Existen controles y procedimientos apropiados para la transferencia de programas de las bibliotecas de prueba a las bibliotecas de producción.
- Existen controles y procedimientos apropiados respecto de los cambios de emergencia a programas y sistemas.
- Las modificaciones a los sistemas son adecuadamente solicitadas aprobadas, especificadas, codificadas y documentadas.
- Los cambios a los programas se prueban adecuadamente antes de ser aceptados en producción.

CIS-Organización y Operaciones

- Existen controles diarios apropiados a las operaciones del computador.
- Existen controles para asegurarse de que se usan las versiones correctas de los archivos de datos y de los programas de producción durante el procesamiento.
- Existen procedimientos adecuados para enfrentar cualquier interrupción temporaria del procesamiento.
- La administración de redes y las funciones de transmisión aseguran que los datos transmitidos se reciben de manera completa y exacta.
- La función de gestión de base de datos está organizada apropiadamente.
- Las actividades del departamento de Sistemas están organizadas de manera tal que brindan una adecuada segregación de tareas.

Desarrollo de sistemas

- Las especificaciones de los paquetes de software adquiridos a proveedores externos coincide con las necesidades de la organización.
- Se controla adecuadamente la implementación de nuevas aplicaciones.
- Se emplean procedimientos y metodologías de desarrollo de sistemas apropiados para todas las nuevas aplicaciones.
- Se usan estándares de documentación adecuados.

Microcomputadores

- Existen controles adecuados sobre el uso de microcomputadoras.
- Existen controles adecuados sobre los microcomputadores usados como terminales.
- Los microcomputadores usados en aplicaciones comerciales críticas están sujetos a controles adicionales.

Recuperación de desastres

- Existe adecuada cobertura de seguros para cubrir los costos de implementación del plan de contingencias.
- Se ha desarrollado un amplio plan de contingencias conteniendo los procedimientos a ser adoptados en caso de que ocurriera un desastre.
- Se han hecho preparativos adecuados para asegurarse de la continuidad del procesamiento en caso de que ocurriera un desastre.

2.2.1 Sobre las operaciones del área de Sistemas de Información Computarizada (SIC). Organización y Planificación (actividades estratégicas y tácticas)

Los procedimientos de control se aplican uniformemente sobre la totalidad de las actividades desarrolladas por los SIC y pueden, a su vez subdividirse, por los objetivos que persiguen, relacionados con:

a. La asignación de responsabilidades con oposición de intereses

Se debe evaluar la segregación de funciones en las organizaciones, las que quedan reflejadas en los organigramas que corresponden a las áreas del SIC, por una parte, en relación con las restantes áreas de los entes, y por otra, con la atribución de responsabilidades internas dentro del propio SIC.

Esta distinción busca, en todo momento, disminuir la concentración de autoridad en una función, sin la incorporación de los controles adecuados.

En todos los casos, será necesario analizar la posibilidad de aplicar el principio de "**oposición de intereses**", respetando una adecuada separación de funciones.

Se tendrá especialmente en cuenta que el área del SIC no tenga dependencia con ninguna de las áreas usuarias de sus servicios, cuidando muy particularmente, que no pueda iniciar transacciones, realizar conciliaciones, ni custodiar otra clase de activos físicos, que los puestos expresamente bajo su responsabilidad.

En lo que respecta a su organización interna, habrá que evaluar la asignación de responsabilidades para el manejo independiente de los procedimientos, manuales, o incorporados a los programas de las aplicaciones, con relación al acceso a los datos de los distintos sistemas aplicativos.

b. La existencia de un Comité de Sistemas

Conformado por las más altas autoridades de las áreas del Ente.

c. Planes estratégicos y tácticos de Sistemas

Con vigencia en el tiempo (resulta aconsejable a más de 2 años y 1 año respectivamente), serán especialmente considerados como técnicas adecuadas de organización, para el ejercicio de un Control Gerencial efectivo.

Las operaciones del área de SIC, que involucren las tareas de planeamiento, programación, ejecución de trabajos (operación propiamente dicha) deben estar organizadas de modo que faciliten la tarea de controlar la gestión, disponibilidad y confiabilidad de los procedimientos.

Deben entenderse comprendidos los controles tanto sobre la finalización normal y correcta de las operaciones, como la anormal de los procesos y su recuperación (Restauración de las aplicaciones).

2.2.2. Sobre el software

Para la revisión de controles relacionados con el software, se toman en consideración las **Operaciones del área de SIC,** que involucren las tareas de planeamiento, programación, ejecución de trabajos (operación propiamente dicha) que faciliten el control de la gestión, disponibilidad y confiabilidad de los procedimientos.

En la consideración de estos controles, adquiere gran importancia, la confección y documentación de políticas y procedimientos que permitan tener en todo momento un marco de referencia adecuado para la gestión, adquisición y desarrollo de software.

2.2.3. La estandarización de los procedimientos

Comprende la elaboración de normas y procedimientos

uniformes para el análisis, diseño, programación, implementación y operación de los sistemas, de tal modo que:

- Se encuentren claramente definidas las misiones y funciones de cada uno de los puestos de trabajo existentes en el área del SIC.
- Se disponga de procedimientos formales y estándares para la ejecución de las actividades específicas de las distintas funciones del área.
- Se generen, o adopten y apliquen, metodologías específicas y apropiadas para el desarrollo y mantenimiento de las aplicaciones, y/o la adquisición de productos de software.
- Se disponga de normas uniformes para la ejecución de las operaciones del sistema.
- Se formalicen normativas precisas sobre el formato y contenidos de la documentación respaldatoria a elaborar en la construcción de aplicaciones, y sobre aquella a ser requerida a los proveedores, en el caso de productos de software aplicativo adquiridos, o desarrollados por terceros.
- Se disponga de normas uniformes que establezcan los formatos y contenidos mínimos necesarios de las instrucciones de funcionamiento (manuales funcionales o para usuarios finales) de cada una de las aplicaciones en uso en la organización.

Relacionados con los aspectos señalados, a los fines de constituir un sistema de controles adecuados, el ente debería incluir normas y procedimientos estándar que contemplen las actividades de investigación, admisión, prueba, autorización e instalación de las nuevas versiones de software de base y de apoyo a la gestión operativa de los sistemas (tal el caso, a modo de meros ejemplos, de: software para administración de bases de datos, telecomunicaciones, seguridad, demás productos auxiliares y utilitarios).

El auditor al evaluar los sistemas de control, apreciará estas inclusiones a los fines de su evaluación. En estos casos, en

particular, deberán estar contempladas las posibilidades de su "vuelta atrás", es decir, el retorno a las versiones previas, de modo de poder garantizar al ente la continuidad en la ejecución de sus operaciones normales.

Se incluyen también, en el caso de las relaciones con proveedores externos, las normas que han de regir los mecanismos de contratación y los instrumentos formales que la respaldarán, donde consten los respectivos derechos y responsabilidades de cada una de las partes y además, se garantice el respeto de las normas legales y reglamentarias del contexto, a las cuales debe someterse el ente.

En el caso indicado, debe contemplarse la posibilidad de acceso de funcionarios de la organización con idoneidad suficiente, a sus medios y contenidos que resulten necesarios, como para permitirles la realización de revisiones técnicas que, hagan viable la supervisión efectiva de las actividades del proveedor.

También cabe contemplar la inclusión de cláusulas específicas de salvaguarda que, en su caso, por la modalidad adoptada de contratación, garanticen la plena disponibilidad por parte del ente de los productos adquiridos, ante una eventual desaparición o interrupción de actividades del proveedor con el cual se contrate, (especialmente en el caso de un contrato de "licencia de uso", donde el ente no tiene acceso a los programas fuente que componen el software aplicativo).

2.2.4. Sobre la seguridad de acceso: Políticas y Actividades de prevención, detección y corrección

Las **restricciones de acceso a los recursos del sistema**, deben realizarse restringiendo la autorización, solamente para las personas que lo necesiten en el desempeño de su función específica, teniendo en cuenta, la aplicación de políticas de prevención, detección y corrección de acciones.

En tal sentido, las acciones de todas las personas, autorizadas o no, deberán ser igualmente registradas, para contar con un respaldo formal suficiente que asegure que se desempeñan dentro

de los límites de sus autorizaciones, utilizando medios y procedimientos hábiles y efectivos de investigación que, al mismo tiempo que funcionan como "filtro" para los accesos, aseguren que su comportamiento es correcto.
Un aspecto que debe contemplarse en forma particular, son las protecciones a los medios del SIC relacionados con las comunicaciones, sean estas realizadas a través de las redes públicas o privadas, propias o ajenas. El objetivo es la búsqueda de medidas que aseguren su integridad, confiabilidad, disponibilidad y autenticidad, incorporando procedimientos idóneos a tal efecto, como ser: uso de firma digital (para garantizar la autoría y la integridad de los contenidos trasmitidos) o la encriptación de contenidos. El auditor deberá verificar que estas medidas de control sean tomadas y funcionen con efectividad.

2.2.5. Para preservar la continuidad del negocio. Planes y Actividades de recuperación y manejo de contingencias

La continuidad de las operaciones del negocio requieren de acciones que permitan garantizarla. Estas incluyen, planes y actividades de recuperación y manejo de contingencias, que contemplen la disponibilidad de las descripciones de los procedimientos necesarios, para que el sistema pueda ser difundido y exista la posibilidad de capacitar a todos los miembros de la organización que resulten involucrados, directa o indirectamente con las aplicaciones de sistemas de información (SIC).
Por extensión, dichos instrumentos también deben ser suficientes como para permitir la realización de tareas de comprobación periódica (simulacros) de modo que pueda experimentarse y demostrarse prácticamente la efectiva recuperación, con el menor daño y en el menor tiempo posible, ante hechos imprevistos y/o situaciones de desastre. Esta constituye una importante actividad de control, por lo que el auditor en los casos en que su adopción esté justificada por la naturaleza y envergadura del ente, debe constatar su existencia o recomendar su adopción.

2.3. Evaluación de los procedimientos de control incorporados en las aplicaciones

Este segundo cuerpo de controles comprende aquellos que inciden única y exclusivamente en forma directa, sobre objetivos afectados por los procesos específicos del SIC en las organizaciones (sistemas aplicativos tales como: liquidación de remuneraciones, contabilidad, facturación, compras, cuentas por pagar y otros).
Estos controles tienen, como propósito básico, asegurar que la información cumpla requisitos de calidad, a partir de la captura desde la realidad del contexto operativo dentro del cual se desenvuelve el ente y perdure a lo largo de toda su existencia dentro del sistema.
Conforme con el marco conceptual descripto, los sistemas aplicativos deberán contar con controles del tipo que se indican a continuación y el auditor debe verificar su existencia:

2.3.1. Criterios de totalidad y exactitud

La totalidad y exactitud de los datos de un aplicativo se satisfacen a través de la incorporación de totales de control, realizados sobre las transacciones agrupadas en "lotes" homogéneos.
A éstos lotes es factible calcularle los valores correspondientes en forma previa al proceso, si sus transacciones se acumulan operativamente y finalmente se vuelcan al sistema agrupados (lotes).
En cambio, el cálculo por el sistema de esos totales de control deberá ser en diferido, (para procesos en línea y tiempo real), cuando las transacciones se incorporan al proceso simultáneamente con su ocurrencia operativa.
Estos totales deberán ser determinados o confirmados, según corresponda, por los usuarios del sistema.
Otros controles adicionales sobre la totalidad y exactitud que pueden aplicarse son aquellos destinados a verificar secuencias numéricas, duplicaciones, faltantes y rechazos.

2.3.2. Criterios sobre validez, pertinencia y autorización

Estos criterios se satisfacen con validaciones lógicas respecto

de los contenidos de datos incorporados, así como de la identidad de quienes lo realizan, con lo cual se otorgará seguridad sobre su correspondencia con el procedimiento al que se pretenden incorporar.
Se introducen a los sistemas de información, según corresponda, luego de superar los mecanismos de verificación del nivel de atribución de quien tiene a cargo esa tarea.
De esta manera, se evita la incorporación de datos e informaciones al sistema que luego pueden llegar a provocar fallas o interrupciones en el procesamiento y pérdida de calidad en la información editada (en forma impresa o en pantalla).
A todo lo expuesto, debe adicionarse la eliminación de riesgos por la realización de transacciones no autorizadas.

2.3.3. Criterios para el control de las actualizaciones, acumulación y almacenamiento de información

El procesamiento de la información ingresada debe estar sometido a controles que aseguren una correcta actualización, acumulación y almacenamiento de datos en los soportes lógicos y físicos del sistema, tales como archivos maestros y de transacciones.
De esta manera será posible, en todo momento, afirmar que se mantiene la integridad, disponibilidad y confiabilidad de la información almacenada.
Por otra parte, debe impedirse el acceso y/o modificación sobre la información que se encuentre almacenada, mediante el empleo de herramientas de procesamiento (habitualmente lenguajes de alto nivel), que se utilicen al margen de los programas específicos de las aplicaciones, que constituyen la única vía legítima y autorizada para ello. Esta es una condición básica de control.
En todo momento debe mantenerse la coherencia entre los archivos pertenecientes a una misma aplicación y aquellos que están incorporados a otras aplicaciones relacionadas.

2.3.4. Criterios para el control de la información relacionada con otras aplicaciones

Cuando se trate de aplicaciones que se encuentren poco integradas

o que no lo estén, deberán instrumentarse controles adicionales con respecto a las informaciones procesadas en los distintos sistemas que puedan estar relacionadas.
Aplicaciones poco integradas requieren y, al mismo tiempo, brindan, mejores posibilidades en cuanto a establecer controles cruzados.
La conciliación de cifras que surge de los mencionados controles cruzados deberá realizarse en períodos razonablemente acotados, teniendo en consideración que los sistemas aplicativos pueden estar emitiendo informaciones diarias o periódicas que, arrojen valores disímiles, que necesariamente requieren ser conciliados, para comprobar la validez, o no, de tales diferencias.

3. Actividades de auditoría de sistemas

3.1. Pruebas de cumplimiento de los controles

3.1.1. Definición de objetivos y alcances

El propósito de este punto es establecer reglas y suministrar criterios en la obtención del necesario conocimiento de los sistemas contable y de control interno.
El auditor debe obtener el conocimiento suficiente de los sistemas contables y de control interno, que le permita una adecuada planificación de la auditoría y el correcto desarrollo de sus distintas etapas. Debe, asimismo, utilizar su criterio profesional para evaluar el riesgo en la auditoría y para diseñar los procedimientos de necesarios para asegurarse que los riesgos han sido reducidos a un nivel aceptablemente bajo.
El **"riesgo en la auditoría"** es la posibilidad que el auditor formule una opinión no adecuada cuando existan en los estados contables errores o irregularidades significativas.
Por "sistema contable" se entiende el conjunto de operaciones y registros del ente mediante los que se procesan y reflejan sus transacciones en la contabilidad. Tal sistema identifica, recopila, analiza, calcula, clasifica, registra, agrega e informa de las transacciones y otros hechos vinculados a ellas.

La definición de "control interno", según la Norma Internacional de Auditoría 400, implica el conjunto de políticas y procedimientos (controles internos) adoptados por la dirección del ente, con la finalidad de asegurar, en la medida de lo posible, la consecución de los objetivos gerenciales relativos a la adecuada y eficiente realización de la actividad de la misma, incluido el cumplimiento de las políticas de la dirección, la adecuada custodia de los activos, la prevención y detección de fraudes y errores, la precisión e integridad de los registros contables y la oportuna preparación de la información financiera.
Los "Procedimientos de control", incluyen políticas y procedimientos adicionales a los relativos al entorno del control, establecidos por la dirección para el cumplimiento de sus objetivos específicos.
En los ambientes informáticos, como se señala en puntos anteriores, los procedimientos de control pueden agruparse en:

- Control de las aplicaciones y de los sistemas de información computarizados, estableciendo para ello, controles, por ejemplo, sobre:
  - cambios en los programas de los sistemas de información.
  - el acceso a los archivos de datos.
  - Controles Generales

En cuanto a los objetivos del control, son los enunciados en este punto, contenidos en la definición de control de la NIA 400, los que también coinciden con el definido en el punto 2, tomado de la definición del Informe COSO.

3.1.1.1. Comprensión de los sistemas contable y de control interno
Cuando, con el propósito de planificar su trabajo, el auditor se disponga a obtener la adecuada comprensión de los sistemas contable y de control interno, debe alcanzar suficiente conocimiento de su diseño, así como de la manera en que funcionan. Por ejemplo, mediante pruebas aleatorias sobre algunas transacciones del sistema contable.

Este procedimiento debe ser tratado como parte integrante de las pruebas de control cuando las transacciones seleccionadas sean ajenas al sistema habitual.
La naturaleza y alcance de las pruebas aleatorias aplicadas por el auditor no permite que por sí solas suministren evidencia de auditoría suficiente y adecuada como para apoyar una evaluación del riesgo de control a un nivel diferente del alto.
La naturaleza, oportunidad y alcance de los procedimientos aplicados por el auditor para obtener la comprensión de los sistemas contable y de control interno varían en función de circunstancias tales como:

- Tamaño y complejidad del ente y de sus sistemas de información.
- Consideraciones sobre el principio de importancia relativa.
- Tipo de controles internos aplicables a cada situación.
- Naturaleza de la documentación que el ente disponga sobre controles internos específicos.
- Evaluación que realice el auditor del riego inherente.

Sistema contable
El auditor debe lograr el conocimiento y comprensión del sistema contable suficientes, para que le permitan identificar y entender:

a) los principales tipos de transacciones de las operaciones de la entidad;

b) la manera en que se inician dichas transacciones;

c) los registros contables significativos, los soportes documentales de los mismos y los saldos específicos de los estados contables; y

d) el proceso contable y de elaboración y presentación de la información contable, desde el comienzo de las transacciones significativas y otros hechos hasta su inserción en los estados contables.

3.1.1.2 Sistema Contable. Sus controles internos
Los controles internos relativos al sistema contable se orientan a alcanzar objetivos tales como los siguientes:

- que las transacciones se realicen de acuerdo a la autorización,

general o específica, de la dirección;

- que todas las transacciones y hechos se registren con prontitud por el importe correcto, en la cuenta adecuada y en el período en que han tenido lugar, de modo que sea posible la preparación de los estados contables en el marco de un conjunto completo de principios contables generalmente aceptados y adecuadamente identificados;
- que el acceso a los activos y registros sólo se permita con autorización de la dirección, utilizando para ello los recursos de hardware y de software disponibles de la forma más adecuada, y
- que los saldos de los activos se comparen con la existencia real de los mismos a intervalos razonables, y se tomen las medidas oportunas cuando se detecten diferencias.

3.1.1.3 Procedimientos de control

El auditor debe obtener el conocimiento necesario en relación con los procedimientos de control para desarrollar el plan de auditoría.

Constatar la presencia o ausencia de procedimientos de control, a través del examen del contexto del control y del sistema contable, le resultará de utilidad para determinar si es necesario algún conocimiento adicional de los procedimientos de control con el objeto de planificar su trabajo.

3.1.1.4 Pruebas de control

Las pruebas de control se aplican para obtener evidencia de auditoría sobre la eficacia:

a) del diseño de los sistemas contable y de control interno, es decir, si han sido concebidos adecuadamente para prevenir o detectar y corregir las irregularidades significativas; y

b) del funcionamiento de los controles internos en el período bajo evaluación.

Las pruebas de control pueden incluir:

- Inspección de los soportes documentales de las transacciones y de otros hechos, para obtener evidencia de que los controles han actuado adecuadamente, por ejemplo, verificando que las transacciones han sido debidamente autorizadas.
- Indagaciones y observación de controles que no dejan rastros en la auditoría, como por ejemplo, determinar quién realiza actualmente cada función y no meramente considerar como válida la información proporcionada por quien se supone que la realiza.
- Repetición de controles internos, por ejemplo, reconciliaciones de los saldos bancarios, para asegurarse que son realizadas en forma adecuada por el ente.

El auditor debe obtener evidencia de auditoría a partir de las correspondientes pruebas de control, para apoyar cualquier evaluación del riesgo de control a nivel inferior al elevado. Cuanto más baja sea la evaluación del control del riesgo, mayor apoyo debe obtener el auditor del correcto diseño y funcionamiento de los sistemas contable y de control interno.

En un contexto computarizado, los objetivos de las pruebas de control no difieren de las relativas a entornos no informatizados. Sin embargo, algunos procedimientos de auditoría pueden cambiar. Puede resultar necesario o preferible para el auditor la utilización de técnicas de auditoría asistidas por computador.

La utilización de tales técnicas, como ser, por ejemplo, programas de comprobación de archivos o pruebas de datos de auditoría, puede resultar adecuada cuando los sistemas contable y de control interno no suministren evidencia visible que documente el comportamiento de los controles internos programados en un sistema contable informatizado.

Apoyándose en los resultados de las pruebas de control, el auditor evaluará si los controles internos están diseñados y operan de la manera prevista en la evaluación preliminar del riesgo de control.

El análisis y la ponderación de las desviaciones detectadas, puede llevar al auditor a concluir que es necesario revisar su evaluación del nivel de riesgo de control. En este caso, debe modificar la

naturaleza, oportunidad y alcance de los procedimientos de auditoría previstos.

3.1.2. Técnicas de verificación y herramientas aplicables Verificaciones. Pruebas de cumplimiento

La obtención de evidencias deberá dividirse según los tipos de controles que se probarán. Esto es,

- Sobre los controles generales y
- Sobre los controles incorporados en las aplicaciones.

3.1.2.1 Para los controles generales

Se recomienda la confección de una planilla al efecto, donde se haga constar una especie de inventario de los distintos Objetivos de Control, conteniendo además las pruebas a realizar. **En general éstas se desarrollan sin el empleo del computador.**

Son mecanismos válidos y habituales:

- **Inspección visual**, con la observación de los espacios físicos, la disposición de los equipamientos, pasillos, cubiertas de equipos, estado y comportamiento del personal, archivo y custodia de la documentación utilizada, las condiciones generales de orden y limpieza y otros.
- **Lectura de documentación** como ser memorandos, organigramas, Manuales de Procedimientos o bien procedimientos formalizados por escrito sin la creación de un Manual, Planes de Trabajo, Actas transcriptas en libros o no, planos de las instalaciones y de las redes y otros.

  La documentación de los procedimientos suele encontrarse informatizada en algunos entes, en cuyo caso es conveniente obtener un prospecto instructivo que ilustre sobre el modo de su utilización y en su caso, solicitar la autorización a los niveles superiores del ente, para poder acceder a ella también por esa misma vía cuando ello sea requerido por necesidades de la revisión que ha de llevarse a cabo.
- **Lectura de Manuales Técnicos** entre los que deberán

incluirse aquellos que se refieren a los productos instalados que hacen a los Controles Generales, tales como los software de "Seguridad y Administración, tanto para el Sistema, como para los perfiles de Usuarios", software de "Administración de Bases de Datos" y otros.

Deben considerarse las definiciones de las funciones más importantes, asignadas a operadores, que se comportarán como "administradores del sistema" y además las **"funciones utilitarias", o de soporte** que poseen y que permiten efectuar una definición de objetivos de control más específicos, que como tales, involucrarán más actividades para la revisión.

Estas "funciones utilitarias" proveen a los sistemas operativos de una potencialidad muy alta, justificada para su empleo sólo en casos excepcionales, pero con terminantes recaudos de seguridad y control del uso.

Cabe destacar que en la actualidad la mayor parte de la documentación se obtiene de medios electrónicos y aun de páginas web. Ello no obstante, cierta documentación de uso frecuente o crítico debiera encontrarse también en forma impresa y resguardada.

En este grupo documental, también se requerirán los **respaldos formales de los sistemas aplicativos que se dispongan.**

Luego esta documentación será analizada más en profundidad en los casos en que deban evaluarse puntualmente las aplicaciones. Para los **Controles Generales**, solo interesará la impresión global del cumplimiento de las **Normas y Procedimientos de Desarrollo y Mantenimiento de Sistemas.**

- **Entrevistas** con funcionarios responsables del sector auditado, provistos en todos los casos, con los check-list correspondientes.

  Con los resultados de estas entrevistas, será conveniente **formalizar lo actuado en documentos**, tales como Actas

o correos electrónicos, notas, memorándum de los temas abordados y las conclusiones obtenidas.

- **Informes técnicos específicos.** Para algunos aspectos, tales por ejemplo como los derivados de la seguridad, podrán aplicarse procedimientos específicos y si es necesario acudir al auxilio de expertos en la materia (por ejemplo las cuestiones relacionadas con el cableado).
  En la seguridad física, deberá evaluarse la capacidad de los sistemas de energía ininterrumpida respecto de los tiempos de mutación de la electricidad al UPS (dispositivo de energía ininterrumpida) o bien la iniciación del ciclo y entrada en régimen de un motogenerador. También será conveniente la realización de un simulacro.
  Iguales consideraciones revisten los aspectos para el control de accesos, los dispositivos antiincendios y de control de temperatura y humedad y otros similares.
  En estas cuestiones, es importante obtener copias de los trabajos que al respecto suelen cumplir los funcionarios encargados del mantenimiento, que dejan constancias de sus intervenciones correctivas o de inspección. Dichas personas podrán pertenecer a la organización o no, pero en todos los casos será conveniente que sean formalizadas las constancias de sus actividades.
  Respecto a las evaluaciones de las **comunicaciones**, podrá apelarse a contar con copias de los elementos que el personal encargado de la administración de la red suele obtener, como medida de su propio control. Esto es, estadísticas de tráfico, disponibilidad de dispositivos, cantidad y tiempo empleado en los procesos de recuperación ante caídas, etc.

Los procedimientos detallados, permitirán evaluar la calidad de los controles, brindando al auditor elementos para decidir si depositar confianza en ellos o no. Todos los procedimientos deberán ser documentados.
En la revisión de los **Controles Generales**, podrá ser requerido

el empleo del computador, en la obtención de las informaciones que suministran las "prestaciones utilitarias" de los productos instalados y también para acceder a revisiones de Seguridad Lógica. En este caso el auditor podrá funcionar como un "usuario" con determinados privilegios.
Es probable que el auditor necesite que se le asigne un determinado perfil de usuario a efectos de comprobar el comportamiento del sistema ante la variedad de pruebas que ha previsto realizar. También podrá apelar a contrastar y analizar archivos de ingreso y acciones de los usuarios, si es que este importante medio de registración y control se encuentra instalado.

3.1.2.2. Para los controles de las aplicaciones

La revisión de los controles de las aplicaciones, resulta de mayor complejidad.
Dando por superada la etapa de la Programación de actividades, donde se han seleccionado ya el o los sistemas aplicativos que habrán de ser comprobados, deberá profundizarse en su conocimiento, con la finalidad de orientarse respecto de las herramientas existentes que utilizará en su verificación. (O bien para definir la creación de herramientas nuevas).
Será menester interpretar cuáles son sus módulos de procesamiento en una forma más detallada que la expuesta en la Planilla (Matriz de análisis de riesgos) recomendada para los Controles Generales, siguiendo los objetivos de control introducidos en las aplicaciones. En determinadas circunstancias podrá obviarse confeccionar esta matriz de riesgos como parte de la metodología, en la medida que sea posible distinguir los programas específicos de los aplicativos que serán objeto de la revisión. Toda aplicación suele incluir programas "polifuncionales" que cumplen más de una función, donde se concentra, por lo común una cantidad significativa de actividades. A pesar de las metodologías de programación existentes, la construcción de sistemas de información computarizados sigue teniendo su cuota

de "artesanía" y por ello, en cada sistema se podrán detectar programas del tipo señalado.
En ciertos casos, la construcción de un cursograma de las actividades, (por su calidad de vinculador de los sectores de la organización intervinientes) puede contribuir a definir con mejor precisión los núcleos del problema donde se producen las fuentes de riesgo a investigar.
En consecuencia, el orden de las herramientas a emplear dependerá del caso concreto que deba ser analizado.
Superadas las instancias anteriores, deberán distinguirse para el o los sistemas objeto, sus entradas, las validaciones, si posee mecanismos de autorización específicos de la aplicación, cuáles son sus almacenamientos y las formas de actualizarlos, el tratamiento que se le dispensa a las transacciones que se rechazan por inconsistentes, etc.
Para profundizar el análisis, la fuente más eficaz proviene de una buena documentación del sistema, sobre todo técnica.
En caso que la documentación no exista o sea parcial, es posible contar con algunos papeles de trabajo o anotaciones que hayan desarrollado los analistas o programadores que intervinieron en la construcción de la aplicación en cuestión.
Cuando estas formalidades no se logren, habrá que ver de qué manera se obtiene ese conocimiento imprescindible para estructurar la prueba.
El principal problema que se enfrenta es, si aún a través de todos estos elementos parciales e imperfectos, no se llega a comprender el funcionamiento del sistema aplicativo a revisar, ni identificar los puntos de riesgo. Los elementos que es más probable que existan, seguramente, son:

- Diagrama de los procesos:
  Si éste funciona en modalidad de lote, existirán una serie de gráficos o bien un listado de sentencias con los distintos pasos de la ejecución. De ellos se obtendrán los archivos que ingresan a cada proceso y cuáles archivos son su salida.
  Si el sistema funciona en forma interactiva, habrá que

identificar la pantalla principal y luego sus esquemas de navegación entre los distintos menúes de menor nivel que se derivan y vinculan al menú principal.
Otra prestación importante de los diagramas, es la posibilidad de identificar el o los programas de mayor significación, de acuerdo a los objetivos que se proponga probar el auditor.
Difícil será conocer qué hace "el" programa importante, si no está documentada su función. Podrá obtenerse información a través de una entrevista con el analista a cargo del mismo a quien se solicitará una explicación que luego podrá ser corroborada con la lectura del programa en el lenguaje de computación que se emplee.
Esta última situación, complica la tarea del auditor tanto en cuanto a su capacidad para llegar a entenderlo por cuanto puede conocer el lenguaje de programación en que está elaborado o no. Aún cuando conozca el lenguaje empleado, habrá que ver la metodología que utilizó quien lo construyó, que quizá no sea el funcionario que ahora se encuentra a su cargo. Es probable que en estas circunstancias, el auditor deba evaluar la necesidad de recurrir a la colaboración de un experto, a fin de asistirlo.

- Diseño de los archivos empleados. Al respecto, tiene especial importancia el lenguaje de computación que se utilice. De emplearse procedimientos gráficos, tipo Visual Basic, Access, SQL-server, DB2, etc. en los diseños de los archivos (o tablas) se podrán obtener cuáles son las validaciones de atributos (campos) que se realizan. De acuerdo al tipo de campo que se trate, del análisis de sus propiedades se pueden visualizar (y hasta documentarlo a través del propio software) cuáles son las consistencias que realiza y cuáles son las acciones que toma en caso de detectar errores.
  En general, las formas modernas de programación con orientación a objetos, son adecuadas para las demandas del auditor.

Si se tratara de lenguajes no visuales (por ejemplo Cobol), el problema es más complejo por cuanto normalmente, las condiciones de validación están incluidas en el cuerpo de los programas. Aún sus diseños (descripción detallada de sus campos de datos) pueden existir en forma externa al programa (para que así todos los programas que emplean el diseño lo tomen de su repositorio) o bien formen parte del programa (no por copia, sino incluido específicamente).
Estas informaciones, también podrían estar contenidas en diccionarios de datos, que consisten en un depósito de uso general, donde se describen para cada uno de los archivos sus diseños y el uso que se hace de sus contenidos.

- Tablas y árboles de decisiones. Esta es una posibilidad más remota, que dependerá del grado de profesionalidad que se hubiera empleado en la construcción de la aplicación. Una tabla de decisiones consiste en una tabla que contiene en sus encabezamientos distintas entradas de condición que, de acuerdo a los análisis de la realidad que se presentan, se incluirán la parte inferior de la tabla, cuál deberá ser el tratamiento que el sistema seguirá.

3.1.2.3. Pasos para realizar las pruebas de las aplicaciones

Para concretar las pruebas de las aplicaciones, deberá avanzarse a partir de los contenidos que se han volcado sobre la Matriz, en la etapa de relevamiento para el Análisis de los Controles de las Aplicaciones.
Dada la necesidad de emplear técnicas a ser ejecutadas con el auxilio del computador, se requiere cumplir con los siguientes pasos:
Ubicación del Sistema Objeto en la Organización. Esto es, dilucidar la duda de si, el aplicativo a verificar cumple funciones que colaboran con los objetivos del negocio y soportan las actividades de varios sectores del ente.
Para establecerlo se deberá utilizar herramientas gráficas, tales como Organigramas y Cursogramas.

Desde los Cursogramas es posible detectar algunas debilidades generales y otras específicas con relación al sistema a probar.
Los pasos a seguir, en un sentido genérico, son los siguientes:

- Desarrollo y formalización de listas de control (check-list). Esta herramienta, puede completar eficazmente los aspectos relevados, orientándolos en forma específica hacia los aplicativos y módulos donde se detecte la mayor cantidad de riesgos o inconvenientes.
- Identificación de los módulos en que se encuentra subdividido el aplicativo. Esto es, cuáles son las variables ambientales que lo estimulan y condicionan para las actividades que tiene previstas. Para el cumplimiento de estos objetivos, también se cuenta con herramientas gráficas, pero orientadas con mayor énfasis, hacia el procesamiento de datos computarizados, tales como los Diagramas de Flujo de Datos.
  A través de ellas es posible distinguir para los módulos existentes, cuáles son los más trascendentes a los fines de la revisión a realizar, sus vínculos con las entradas y salidas de información y también, los archivos que emplea.
  Identificados los módulos a comprobar, se considerará en conjunto con el área de sistemas del ente, cuál sería la mejor forma de comprobar su adecuado comportamiento.
- Seleccionar la técnica a emplear. Esto surgirá de la entrevista con el personal del área de Sistemas, lo cual dependerá en alto grado de las condiciones que se disponga para poder efectivizarla. Lo más aconsejable sería ejecutar un lote de prueba, y, en especial, disponer de un dispositivo de prueba integrado (minicompañía) o bien proceder a realizar un cruce de archivos de datos reales (simulación en paralelo).

3.1.2.4. La prueba de las aplicaciones

Seleccionada la técnica a aplicar, es necesario establecer los pasos a seguir para la concreción efectiva de una prueba de cumplimiento sobre un aplicativo, en su totalidad, o sobre algunas

funciones de ellos.
Este procedimiento dependerá de la forma cómo se realizará la prueba. Esto es,

- empleando transacciones simuladas sobre el sistema real (Lote de Prueba o Caso Base o Minicompañía), o bien
- seleccionando transacciones existentes del sistema real y emulando el comportamiento del sistema (Simulación en Paralelo o Minicompañía).
- Si los anteriores procedimientos no son viables, hay que considerar la posibilidad de observar la realización de una operatoria real y tomar evidencias de su comportamiento, como prueba de cumplimiento.
- Como método menos ortodoxo, podría utilizarse la revisión de los procedimientos a través de la selección (por mecanismos de muestreo estadístico) y extraer transacciones de la realidad. Con ellas, se podrá revisar la situación real en el sistema real y analizar con criterio crítico cómo el sistema ha tratado las transacciones seleccionadas. En operatorias complejas, donde algunas herramientas de las expuestas no pueden ser aplicadas por problemas prácticos, es un método alternativo que puede permitir avanzar en revisiones y documentarlas.

Para preparar las transacciones a simular, deben cubrirse las siguientes etapas:

- Identificar qué controles comprobar. Para entender su alcance se mencionan algunos ejemplos: verificar si al intentar dar de alta nuevamente un cliente existente el sistema lo rechaza, como debiera, o bien lo admite; comprobar cómo suma el sistema para emitir los totales finales del ingreso de datos; revisar la determinación de impuestos por parte del sistema de facturación, entre otros.
- Aislar las transacciones a través de las cuales es posible comprobar tales controles. Por ejemplo: qué transacción permite darle de alta a un cliente en el archivo de clientes.

- Obtener del sistema los elementos que permitirán elaborar dichas transacciones de prueba. Por ejemplo seleccionar un cliente, del cual se toma un dato identificatorio que podría ser el No. de CUIT y agregar otro creado para la prueba, con el mismo Nº de identificación tributaria, verificar la forma de generar la factura para clientes que mantengan diferentes condiciones ante el IVA, etc.
- Elaborar un documento donde se vuelque el contenido de todos los datos de las transacciones que se ingresarán a la comprobación.
- Predeterminación de los resultados esperados.
- Ejecución de la prueba y comprobación de los resultados reales.
- Completar la Matriz de la Prueba en la columna Observaciones donde se incluirá la calificación del resultado como exitoso o fallido.

Para simular el procedimiento empleando transacciones existentes, se cubrirán las siguientes etapas:

- Identificar los controles a comprobar, de igual manera que en el procedimiento anterior.
- Elaborar un diagrama sintético que posibilite graficar qué archivos sería necesario seleccionar. Por ejemplo para el cliente que se duplique, se comprobará su inexistencia en el archivo principal, para comprobar la aplicación del IVA, se tomarán las facturas y se verificará el valor del impuesto determinado, en base a lo cual, se verificará la condición del cliente en el archivo principal a fin de verificar la correcta aplicación en función de su calificación ante el impuesto. Para comprobar las sumas de control, se tomaría el archivo final del proceso de un día, se sumarían algebraicamente las transacciones del día siguiente y sus resultados, deberían coincidir con las contenidas en el archivo final del proceso de este último día.
- El documento conteniendo los resultados predeterminados podrá existir según sea el método de la prueba. Por ejemplo

si el método es verificar facturas podrá conocer por contraste con la situación general de los clientes ante el IVA. Pero si se trata de verificar el Valor del archivo, más/menos (+/-) las transacciones, el valor nuevo deberá coincidir pero con posterioridad al proceso.

- Ejecución de la prueba y comprobación de los resultados reales.
- Completar la Matriz de la Prueba en la columna Observaciones donde se incluirá la calificación del resultado como exitoso o fallido.

Para **observar la ejecución** de un procedimiento real, no se requiere una habilidad técnica especial. Sólo habrá que tomar precauciones respecto de cómo documentar los distintos momentos de la ejecución, de manera de emplearlos como respaldo de una prueba de cumplimiento.

3.1.3. Herramientas aplicables. Pruebas de cumplimiento

El objetivo de estas pruebas es determinar si el sistema (como sistema en sí) y más precisamente respecto de los controles relevados, se comporta en la práctica de acuerdo a como se espera que lo haga.

Debe aclararse que "control" no sólo se refiere a las llamadas genéricamente validaciones sobre la información, sino que también deben incluirse las decisiones que se toman dentro de los sistemas (consecuencia de controles que poseen los programas aplicativos), tal el ejemplo de aplicar descuentos por pago dentro del vencimiento de una factura, o no aplicarlos o reclamar cláusulas punitorias.

Por otra parte vale la pena recordar que del resultado de la evaluación del control interno dependerán el alcance, extensión y oportunidad de los procedimientos de auditoría que se seleccionarán para formar el plan de auditoría.

a) La presentación de las herramientas se hace clasificándolas de acuerdo al ambiente en el cual se pueden desarrollar.

Ambiente de la prueba	Fuera del ámbito operativo (*)		Dentro del ámbito operativo
Transacciones a utilizar	Desarrolladas especialmente para la prueba (simuladas).	Aprovechando las transacciones reales procesadas en el sistema (una copia de ellas).	Es posible aplicar una mezcla de las transacciones a emplear.
Sistema empleado	Sistema real (copia)	Sistema simulado (construido)	Sistema real
Técnicas aplicables	• Lote de prueba • Caso base	• Simulación en paralelo	• Minicompañía • Técnicas concurrentes. • Observación

(*) Ello no implica qué computador se empleará, sino que puede ser el que se emplea en la operación diaria, pero en un área del ambiente adecuadamente separado.

Entre las técnicas que complementan a las anteriores, deberemos citar:

- Software de comparación de versiones de programas.
- Pista de seguimiento de transacciones.

Tal como se muestra en el cuadro anterior, entre las técnicas aplicables tenemos:

- Lote de prueba
- Caso base
- Simulación en paralelo
- Minicompañía
- Técnicas concurrentes
- Observación

a.1. Lote de prueba

Sintéticamente propone que el auditor genere transacciones, a efectos de poner en evidencia qué relación existe cuando esas transacciones se ejecuten en el sistema (sistema real), con respecto a los resultados que se espera produzcan. Según sean los objetivos de control a probar, habrá que seleccionar las transacciones que posibilitarán probarlos (que son aquéllas que impactan sobre esos objetivos de control) y de tales transacciones, crear datos para sus contenidos de manera que logren el efecto deseado.

Para más claridad, con una transacción que ingresa una Nota de Pedido se desea verificar que si el cliente se encuentra excedido en el crédito autorizado, la reacción del sistema sea (porque así está previsto) rechazarla o enviar un comunicado al área de Créditos para tramitar su autorización.

a.2 Caso base

Es una extensión del lote de prueba luego de su primera utilización. Toda la documentación y soportes magnéticos, pueden ser mantenidos (y mejorados) tanto con sus transacciones simuladas como con sus datos "maestros", posibilitando que en una circunstancia futura, se puedan ejecutar con el empleo de una copia del sistema real y volver a obtener los resultados a comparar con los esperados.

Un logro importante, sería encontrar en el propio sistema que se está auditando, los datos de prueba conservados por sus responsables como elemento respaldatorio del trabajo desarrollado por el área de sistemas de la organización. Esto aliviaría sobremanera la labor del auditor que, luego de evaluar la calidad y profundidad de los componentes de la prueba, quizá solo quiera ejecutarla nuevamente o bien agregar sólo algunos casos especiales.

a.3. La simulación en paralelo

Consiste en desarrollar un programa (o sistema de programas) con el cual, se analicen las transacciones de un período transcurrido, a efectos de hallar qué reacciones, excepcionales o no, han debido provocar en el sistema que se está auditando.

La prueba se completa con la revisión en el sistema real, ubicando la transacción real y verificando los resultados producidos por ese proceso real.

Al construir otro sistema y procesar las transacciones reales, se puede evaluar si los resultados reales coinciden correctamente con los esperados. Esto es, si los datos grabados en los archivos coinciden con lo esperado, puesto que en caso contrario, se demostraría que los archivos son alterados por fuera de la operación de las aplicaciones (apelando a programas utilitarios

y/o comandos del software de base o de base de datos).

a.4. La minicompañía

Consiste en la incorporación, dentro de los archivos normales de la institución, de registros especialmente ingresados (dados de alta) para finalidades de auditoría.

En tal situación, el auditor puede utilizar el método de crear transacciones (tal como para el lote de prueba), o bien seleccionar transacciones reales a las que, luego de duplicarlas, las lleve a impactar sobre los registros especiales de auditoría.

En esta técnica, las salidas del sistema deberán segregarse de las comunes (por el propio sistema, por realizar contraasientos contables o bien sin separarlas, ingresarlas por importes ínfimos de modo tal, que no alteren significativamente las cifras del sistema real).

Los resultados obtenidos del proceso de los registros de auditoría, permiten que el auditor exprese la inferencia válida que si la "minicompañía" tiene adecuadamente controlados sus procedimientos, la "compañía" auditada también los tiene.

El concepto de la minicompañía permite la realización de la auditoría, conjuntamente con el procesamiento normal, por lo cual y con posterioridad a su presentación, se adicionaron rutinas que se propuso incorporar a las aplicaciones.

a.5. Las técnicas concurrentes (que mantienen como técnica básica a la minicompañía)

Constituyen mecanismos muy hábiles de auditoría pero que comprometen al auditor con la operación del sistema.

Su aplicación conceptualmente es excelente, si bien no resulta así desde un aspecto práctico.

El objetivo de estas rutinas, disparadas automáticamente o a pedido del auditor, crean evidencias (obteniendo copias de áreas de la memoria antes y después de ejecutar una determinada rutina del programa o una transacción completa), quedando una pista de auditoría muy valiosa.

Esto se podrá realizar, incorporando datos a los propios registros del sistema a auditar (concepto del "registro extendido") o bien,

grabando un archivo de auditoría (tal el SCARF = System Control Audit Review File).

a.6. La observación

Constituye un mecanismo que podríamos indicar de última instancia, que no se encuentra citado en la bibliografía indicada para esta clase de comprobaciones.

Es un procedimiento habitual en la auditoría contable, pero que no es citado para Pruebas de Cumplimiento en este ambiente, más aun cuando alguna parte del control interno se encuentra introducido en los programas de las aplicaciones.

Sin embargo, es factible a través de él obtener evidencias del comportamiento del sistema, especialmente en las etapas del ingreso de datos para luego munirse de los documentos emitidos (fotocopiados) o del listado de las pantallas productos de la reacción prevista en el sistema.

Las pruebas son limitadas y aprovechables cuando no sea posible aplicar otros procedimientos como los descriptos o bien luego de aplicados, se los desee complementar.

Con las limitaciones mencionadas, es una alternativa para tomar en consideración.

De las técnicas complementarias más comunes, se pueden citar:

- Comparador de versiones de un mismo programa, el cual tiene por objeto conocer el nivel de autorización existente para los que se encuentran en el ambiente operativo.

  Se puede trabajar sobre los programas en su lenguaje fuente. En tal caso, la evaluación tiene por objeto *analizar en el tiempo*, si las modificaciones a los sistemas (actividad del área de Desarrollo y Mantenimiento de Aplicaciones) se realizan cumpliendo con las pautas de control establecidas, o no.

- Sobre los programas en su lenguaje ejecutable, permiten *evaluar en el momento*, si la versión que se encuentra operativa se corresponde con la autorizada, la cual a su vez se habrá evaluado en el servicio de Desarrollo y Mantenimiento, con el procedimiento anterior.

- Pistas para el seguimiento de transacciones. Esta tarea, que puede tener una aplicación más generalizada que lo que impresiona a primera vista, trata de emplear los registros que normalmente quedan en los procesos para el recupero de transacciones en caso de fallas.

Estos procesos reservan parte de las operaciones (transacciones), con sus imágenes anteriores y posteriores a la actualización de archivos para lograr su recuperación ante caídas del sistema. Sin embargo, son fértiles para el auditor.

Si su empleo se considera de utilidad, deberá convenirse con el área de Sistemas por la reserva de sus contenidos, por cuanto lo que resulta habitual es que con posterioridad al transcurso de un plazo prudencial, estos almacenes de datos se desechen, teniendo en cuenta que para la operación del sistema, no revisten más utilidad.

Comparación de las técnicas descriptas

Con respecto a las distintas técnicas descriptas, se debe concluir que no existe "una técnica" que se corresponda con lo que sería deseable obtener y por ello, aprender a emplearla y aplicarla para la totalidad de las situaciones, dando pautas al auditor de cómo organizar su tarea.

Todas ellas tienen ventajas y limitaciones, ya sea por el tiempo que demandan, por los beneficios que brindan, por las evidencias que ofrecen, por el grado de compromiso que asume un auditor en su aplicación, por el nivel de sencillez que implica su utilización y por la habilidad técnica necesaria para su elaboración.

En el cuadro sinóptico siguiente se presenta un resumen de lo hasta aquí expuesto en cuanto a ventajas y limitaciones de las técnicas, a lo que se debe agregar la absoluta necesidad de contar con la colaboración del personal del área de sistemas para poder llevarlas a cabo con éxito.

Técnica	Ventajas	Limitaciones
LOTE DE PRUEBA	• Demanda escasa habilidad técnica al auditor. • Permite probar el circuito computarizado y el administrativo. • Posibilita una prueba cuasi completa de todas las variantes que se deseen probar. • Produce una evidencia completa de los resultados.	• Exige mucho tiempo dedicado a su elaboración, al menos la primera vez. • La prueba completa de todas las alternativas previsibles combinadas, es prácticamente irrealizable. • Resulta difícil reproducir el ambiente operativo real. • Da una imagen del sistema en el momento de la prueba (idea de **fotografía**).
CASO BASE	• Las ventajas son idénticas a las expuestas para el tote de prueba. • Permite nuevas fotografías en instancias futuras, con el esfuerzo de la primera vez.	• Debe mantenerse el caso base, actualizado con las actividades de cambios en el sistema, al tener que crear nuevas transacciones para probar las nuevas rutinas y eliminar las retiradas.
SIMULACIÓN EN PARALELO	• Demuestra si los archivos son accedidos (y modificados) por fuera de los programas de las aplicaciones. • Si bien se la presenta para Pruebas de Cumplimiento, puede realizar conjuntamente Pruebas Sustantivas. • No se afecta el ambiente operativo, pues puede ejecutarse en una PC. • En procedimientos muy complejos, donde se cuenta con poca documentación, puede resultar de utilidad la técnica, **simulando qué debe hacer** el sistema, aún sin poder conocerlo.	• Demanda habilidad técnica del auditor, para programar el sistema, aunque también es posible efectuarla empleando soft específico de auditoría u otras herramientas. • Sólo se pueden probar, de las situaciones buscadas, aquéllas que se presenten en las transacciones analizadas. • Por el motivo anterior, requiere sea ejecutado en más de un período. • Es probable que ciertas situaciones que se desean controlar, no se presenten en absoluto. En esto queda la duda, si se desean probar situaciones demasiado fantasiosas o hay abierta una puerta que debiera encontrarse cerrada ?
MINICOMPAÑÍA	• Demanda escasa habilidad técnica al auditor. • La prueba es concurrente con la operación (en línea y en el mismo ambiente) y es ejecutable varias veces durante un ejercicio comercial, sin preparación previa (idea de **película**). • Aunque los registros especiales se conocen, el auditor cuenta con la sorpresa de su utilización. • Se prueban situaciones de cambio, que el sistema tiene previsto resolver, por el mero transcurso del tiempo	• El programa (siempre hay un programa principal), podría estar alterado para atender los requerimientos del auditor? Esta consideración parece poco probable. • Pueden existir limitaciones impositivas y de otras fuentes reglamentarias. • El auditor queda comprometido con el sistema (se requiere un logging muy adecuado para deslindar responsabilidades). • Se pierde integridad (aunque controlada) de la base de datos.
TÉCNICAS CONCURRENTES	• Posibilita un monitoreo excelente de las condiciones que el auditor desee. • De venir provisto en el soft adquirido (ERP), su aplicación se ve facilitada.	• Demanda alta habilidad técnica del auditor o de quien esto realice, con las consiguientes inversiones de dinero y tiempo. • El compromiso del auditor con las rutinas del sistema, es insoslayable.
OBSERVACIÓN	• Demanda escasa habilidad técnica al auditor y sólo un conocimiento funcional del sistema. • La prueba es concurrente con la operación (en línea y en el mismo ambiente), sin preparación previa, lo cual facilita el factor sorpresa.	• Resulta de aplicación limitada, para validar las interfaces del usuario en los ingresos de datos y consultas. • Puede dificultar el desenvolvimiento normal de los operadores.

3.2. Pruebas sustantivas

Tal como expresan las normas internacionales de auditoría, el auditor debe obtener un conocimiento apropiado del ente, de los sistemas contables y del control interno.

Asimismo debe evaluar el riesgo de auditoría y seleccionar los procedimientos adecuados para reducirlo a un nivel aceptablemente bajo.

Para conseguir esos objetivos debe planificar en forma adecuada el trabajo de auditoría, determinando la naturaleza, alcance y oportunidad de los procedimientos a aplicar para la obtención de elementos de juicio validos y suficientes, teniendo en cuenta el efecto de los puntos anteriormente mencionados, la finalidad del examen y el tipo de informe a emitir, de la misma manera que en un ambiente no computarizado.

En un ambiente computarizado se producen:

Cambios en la aplicación de los procedimientos de auditoría, incluido el uso de técnicas informáticas utilizadas en la auditoría, debido a cuestiones tales como:

- La necesidad de auditores con un mínimo de conocimientos técnicos sobre sistemas informáticos;
- La incidencia de los sistemas informáticos en los estados contables;
- El efecto de los sistemas informáticos en la planificación de los procedimientos de auditoría;
- La probable ausencia de rastros visibles (pistas de auditoría) de las transacciones procesadas

El auditor, debe tener en cuenta la necesidad de evaluar las pruebas con el personal adecuado del cliente, y además, obtener la aprobación necesaria con anterioridad a su aplicación, para así evitar la alteración involuntaria de los registros de los clientes.

El desarrollo de las pruebas sustantivas, entre otras metas, tendrán como finalidad:

- suministrar rastros de auditoría, habida cuenta de la probable inexistencia de pistas;

- comprobar la integridad de la información almacenada en las base de datos;
- obtener la información necesaria para la auditoría.

Las pruebas utilizadas tienen la característica de la generalidad de las pruebas utilizadas en auditoría, la dualidad de su aplicación, pueden ser orientadas a verificar el cumplimiento de los controles o ser utilizadas para validar saldos como pruebas sustantivas.

3.2.1. Definición de objetivos y alcances

Los objetivos y alcance global de una auditoría no cambian cuando se la conduce en un ambiente de sistemas de información computarizada, tal como se menciona en 1.1.

3.2.2. Técnicas de verificación y herramientas aplicables

La aplicación de procedimientos de auditoría puede requerir que el auditor considere técnicas conocidas como Técnicas de Auditoría con Ayuda de Computadora (TAACs).

Las TAACs pueden mejorar la efectividad y eficiencia de los procedimientos de auditoría. Pueden también proporcionar pruebas de control efectivas y procedimientos sustantivos cuando no haya documentos de entrada o un rastro visible de auditoría o cuando la población y tamaños de muestra sean muy grandes.

Las TAACs pueden usarse para desarrollar diversos procedimientos de auditoría, incluyendo los siguientes:

- **pruebas de detalles de transacciones y saldos**, por ejemplo, el uso de software de auditoría para recalcular los intereses o la extracción de facturas por encima de un cierto valor de los registros de computadora;
- **procedimientos analíticos**, por ejemplo, identificar inconsistencias o fluctuaciones importantes;
- **pruebas de controles generales**, por ejemplo, pruebas de la instalación o configuración del sistema operativo o procedimientos de acceso a las bibliotecas de programas o el uso de software de comparación de códigos para verificar

que la versión del programa en uso es la versión aprobada por la gerencia;

- **obtención de muestras sobre universos que complementen** las pruebas de auditoría; **reprocesar cálculos** realizados por los sistemas de contabilidad del ente.

El creciente poder, miniaturización e independencia de alimentación eléctrica de las microcomputadoras, incorpora otras herramientas para uso del auditor. En algunos casos, estas micros podrán estar conectadas a los sistemas de computación del auditor.

Ejemplos de estas técnicas incluyen:

- **sistemas expertos**, por ejemplo en el diseño de programas de auditoría y en la planificación de auditoría y evaluación de riesgos;
- **herramientas** para evaluar los procedimientos de un cliente para gerenciar riesgos;
- **papeles de trabajo electrónicos**, planeados para la extracción directa de datos de los registros de la computadora del cliente, por ejemplo: descargar el libro mayor para pruebas de auditoría; y
- **programas de modelaje corporativo y financiero** para usar como pruebas predecibles de auditoría.

Las TAACs son programas de computadora que el auditor usa como parte de los procedimientos de auditoría para procesar datos importantes para su tarea contenidos en los sistemas de información del ente. Los datos pueden ser de transacciones, sobre los que el auditor desea realizar procedimientos sustantivos, o pueden ser otros tipos de datos. También pueden consistir en programas en paquete, programas escritos para un propósito determinado, programas utilitarios o programas de administración del sistema.

Independientemente del origen de los programas, el auditor verifica que sean apropiados y su utilidad para los fines y objetivos

de la auditoría que lo ocupa antes de usarlos.
Los distintos tipos de programa a utilizar son entre otros:

- Programas en paquete
- Programas escritos para un propósito
- Programas utilitarios
- Programas de administración del sistema
- Rutinas de auditoría

- Los programas en paquete son programas generales de computadora, diseñados para desempeñar funciones de procesamiento de datos, tales como leer datos, seleccionar y analizar información, hacer cálculos, crear archivos de datos así como dar informes en un formato especificado por el auditor.
- Los programas escritos para un propósito deberían desempeñar tareas de auditoría en circunstancias específicas. Estos programas pueden desarrollarse por el auditor, por el ente que está siendo auditado o por un programador externo contratado por el auditor. En algunos casos el auditor puede usar los programas existentes de un ente en su estado original y aun emplearlos modificados, porque así puede ser más eficiente que desarrollar programas completamente independientes.
- Los programas utilitarios se usan por un ente para desempeñar funciones comunes de procesamiento de datos, tales como clasificación, creación e impresión de archivos. Estos programas generalmente no están diseñados para propósitos de auditoría pero pueden facilitar el cumplimiento de ciertas funcionalidades de evaluación sustantiva de la información del computador.
- Los programas de administración del sistema son herramientas de productividad mejorada que típicamente son parte de un ambiente complejo de sistemas operativos, por ejemplo, software de recuperación de datos o software de comparación de códigos. Como los programas utilitarios,

estas herramientas no están diseñadas específicamente para usarlos en auditoría, pero además su uso, requiere un cuidado adicional.

- También es factible incorporar rutinas de auditoría a los programas de computadoras de un ente, para proporcionar datos de uso posterior por el auditor. Ellas incluyen lo siguiente:
  - Imágenes instantáneas: Esta técnica implica obtener un impreso o grabado del contenido de una transacción mientras fluye por los sistemas de computadora en diferentes puntos de la lógica del procesamiento, con el objeto capturar imágenes de ella mientras avanza por las diversas etapas del procesamiento. Esta técnica permite al auditor rastrear los datos y evaluar los procesos de computadora aplicados a los datos. Esta técnica si bien brinda una importante pista de auditoría, en caso de no estar prevista en el diseño del sistema, puede producir errores no previsibles que comprometen al auditor.
  - Archivo de auditoría para la revisión del sistema. Este implica incorporar módulos de software de auditoría dentro de un sistema de aplicaciones para proporcionar monitoreo continuo de las transacciones del sistema. La información es reunida en un archivo especial de computadora que el auditor puede examinar, en línea o con posterioridad. Es una técnica equiparable a la anterior aunque puede representar menor riesgo.

3.2.3. Consideraciones en el uso de TAACs

Al planear una auditoría, el auditor puede considerar una combinación apropiada de técnicas de auditoría manuales y con ayuda de computadora.
Al evaluar el uso de TAACs, los factores a considerar incluyen:

- el conocimiento, pericia y experiencia del equipo de auditoría en ambientes de TI debe ser el suficiente, de acuerdo a la complejidad del ambiente y de los

procedimientos necesarios de aplicar;

- la importancia de la interacción del sistema computarizado con los estados contables y con el control interno;
- la disponibilidad de TAACs, instalaciones y datos adecuados de computación;
- la imposibilidad de aplicar pruebas manuales

3.2.4. Utilización de TAACs

Los pasos principales que debe tomar el auditor en la aplicación de una TAAC son:

- establecer el objetivo de aplicación de la TAAC;
- determinar el contenido y accesibilidad de los archivos del ente;
- identificar los archivos específicos o bases de datos que deben examinarse;
- entender el diseño y la relación entre las entidades de datos cuando deba examinarse una base de datos;
- definir las pruebas o procedimientos específicos, transacciones relacionadas y saldos afectados;
- definir los requerimientos de datos de salida;
- convenir con el usuario y departamentos de TI, si es apropiado, en las copias de los archivos relevantes o entidades de las bases de datos que deben hacerse, en la fecha y momento apropiado de su realización;
- identificar al personal que puede participar en el diseño y aplicación de la TAAC;
- precisar las estimaciones de costos y beneficios;
- asegurarse del control y documentación apropiados del uso de la TAAC;
- organizar las actividades administrativas, incluyendo los recursos humanos necesarios, así como las instalaciones de computación;
- conciliar los datos que deban usarse para la TAAC con

los registros contables;

- ejecutar la aplicación de la TAAC; y
- evaluar los resultados.

3.2.5. Control de la aplicación de la TAAC

Los procedimientos específicos necesarios para controlar el uso de una TAAC dependen de la aplicación particular. Al establecer el control, el auditor considera la necesidad de:

- aprobar especificaciones y conducir una revisión del trabajo que deba desarrollar la TAAC;
- revisar los controles generales de la entidad en cuanto contribuyan a la integridad de la TAAC, por ejemplo, controles sobre cambios a programas y acceso a archivos de computadora. Cuando dichos controles no son confiables para asegurar la integridad de la TAAC, el auditor debe considerar el proceso de la aplicación de la TAAC en otra instalación de computación adecuada; y
- asegurar la integración apropiada de los datos de salida dentro del proceso de auditoría por parte del auditor.

Los procedimientos llevados a cabo por el auditor para controlar las aplicaciones de la TAAC pueden incluir:

- participar en el diseño y pruebas de la TAAC;
- verificar, si es aplicable, la codificación del programa para asegurar que esté de acuerdo con las especificaciones detalladas del programa;
- solicitar al personal de computación del ente revisar las instrucciones del sistema operativo para asegurar que el software correrá en las instalaciones del ente;
- ejecutar el software de auditoría en pequeños archivos de prueba antes de ejecutarlo en los archivos principales de datos;
- verificar si se usaron los archivos correctos, por ejemplo, verificando la evidencia externa, así como totales de

control mantenidos por el usuario, que aseguren que dichos archivos estén completos.

- obtener evidencia de que el software de auditoría funcionó según lo planeado, por ejemplo, revisando los datos de salida y la información de control; y
- establecer medidas apropiadas de seguridad para salvaguardar la integridad y confidencialidad de los datos obtenidos en el procesamiento de la TAAC.

Cuando el auditor tiene la intención de desarrollar procedimientos de auditoría en forma concurrente con un procesamiento en línea, tiene que revisar dichos procedimientos con el personal apropiado del cliente y obtener su aprobación antes de conducir las pruebas para evitar la alteración inadvertida de los registros del cliente.
Para asegurar procedimientos de control apropiados, no se cree necesaria la presencia del auditor en la instalación de computación durante la ejecución de una TAAC. Sin embargo, esto puede proporcionar ventajas prácticas, como controlar la distribución de los datos de salida y asegurar la corrección oportuna de errores, por ejemplo, si se fuera a usar un archivo de entrada equivocado.
Los procedimientos de control respecto del uso de otros software que ayuden a la auditoría pueden incluir:

- verificar la totalidad, exactitud y disponibilidad de los datos relevantes, por ejemplo, pueden requerirse datos históricos para elaborar un modelo financiero;
- revisar la razonabilidad de los supuestos usados en la aplicación del conjunto de herramientas, particularmente cuando se usa software de modelaje;
- verificar la disponibilidad de recursos con habilidad en el uso y control de las herramientas seleccionadas; y
- confirmar lo adecuado del conjunto de herramientas para el objetivo de auditoría, por ejemplo, puede ser necesario el uso de sistemas específicos para la industria en el diseño de programas de auditoría para negocios con ciclos únicos.

3.2.6. Metodología de trabajo

Finalmente se puede afirmar que la metodología de trabajo a aplicar en un ambiente computarizado, es similar a la utilizable en un ambiente no computarizado.
El auditor deberá planear el trabajo de auditoría de modo que sea desempeñada de una manera efectiva.
En esta instancia deberá considerar el apropiado conocimiento del negocio, la comprensión de los sistemas de contabilidad y control interno, las secuencias de identificación de riesgos, su relación con controles asociados de cumplimiento efectivo, la medición de sus posibles impactos sobre la tarea de auditoría y la evaluación de actividades de control en general, el auditor, con el conocimiento derivado de los pasos señalados procederá a seleccionar los procedimientos de auditoría, definiendo su naturaleza, oportunidad y alcance.

4. Conclusión

Tal como se expresa en el punto 1. Introducción, el objetivo de una auditoría de estados contables es hacer posible que el auditor exprese una opinión, acerca de la correspondencia de la preparación de los estados, en todo lo significativo, con el conjunto de normas que lo regulan.
Si bien puede afirmarse que el objetivo y alcances globales de una auditoría no cambian bajo un ambiente de sistemas de información computarizada, los cambios significativos que la computación produce en el ingreso, procesamiento, almacenamiento y comunicación de la información contable pueden tener consecuencias de alto impacto sobre los estados contables.
Las Normas Internacionales de Auditoría, bajo revisión para ser adoptadas como normas vigentes en Argentina, requieren que el auditor obtenga suficiente conocimiento del SIC, para estar en condiciones de: diseñar el plan de auditoría, dirigirlo o ejecutarlo y finalmente evaluar el trabajo desarrollado, debiendo considerar si se necesitan conocimientos específicos para la realización del trabajo.

En el presente informe se han desarrollado procedimientos que permitirían evaluar el cumplimiento de los controles, la detección de riesgos y la validez de saldos en ambientes en los que se utilizan sistemas de información computarizados.
El propósito de la aplicación de estos procedimientos, tiene como fin primordial la obtención de evidencias válidas y suficientes, para sustentar la opinión del auditor de estados contables, en cuanto a la razonabilidad de sus expresiones y al cumplimiento de normas profesionales vigentes.

Se terminó de imprimir
en el mes de abril de 2007 en
Amalevi
Mendoza 1851/ 53 - Rosario - Santa Fe
Tel. (0341) 4213900 / 4242293 / 4218682
e-mail: amalevi@citynet.net.ar