



Especialización en Contabilidad Superior y Auditoría.

TRABAJO FINAL

PROCEDIMIENTOS DE AUDITORÍA EXTERNA ANTE CONTROLES INTERNOS INFORMÁTICOS

AUTOR:

Cielo, Daniel Alejandro

TUTOR:

Castello, Ricardo Justo

CO-TUTOR:

Morales, Héctor Rubén

Córdoba, 30 de Junio de 2016



PROCEDIMIENTOS DE AUDITORÍA EXTERNA ANTE CONTROLES INTERNOS INFORMÁTICOS por Cielo, Daniel Alejandro se distribuye bajo una [Licencia Creative Commons Atribución-CompartirIgual 4.0 Internacional](https://creativecommons.org/licenses/by-sa/4.0/).

AGRADECIMIENTOS

A todos los integrantes docentes y no docentes de la Escuela de Graduados en Ciencias Económicas por todos los conocimientos compartidos y el apoyo brindado.

A mi director de tesis, quien me ha guiado en este trabajo. También agradezco a mi co-director que estuvo cuando lo necesité.

A mis compañeros de especialidad, con quienes hemos trabajado juntos y apoyado a lo largo de la carrera.

DEDICATORIA

A mi familia, que ha entendido y acompañado durante el tiempo dedicado a la elaboración del presente trabajo y cursado de la especialidad. En especial a mis padres por haberme transmitido la vocación de estudiar y aprender.

A amigos y compañeros, que siempre alentaron en esta etapa de mi vida.

RESÚMEN

El objetivo del presente trabajo es analizar los procedimientos de auditoría externa necesarios ante controles internos basados en sistemas informáticas. Para ello, en primer lugar, se considera cómo las nuevas tecnologías modifican el entorno en el que se desarrolla la auditoría y la manera en que el auditor valida la información bajo estas condiciones. Se deben destacar las pruebas de control de que dispone, así como el efecto principal que provoca sobre el desarrollo de su labor profesional: su evaluación debe estar enfocada en depositar confianza sobre los controles internos. En segundo lugar, se realiza un desarrollo de los puntos principales informe COSO y de la importancia que brinda a la tarea del auditor para el adecuado relevamiento del sistema de control interno. Asimismo se avanza sobre otros factores que incrementan los riesgos y tienen impacto sobre las actividades e información contable de las empresas. Finalmente se completa con la tarea tradicional del auditor, tratando el enfoque según el riesgo detectado y las consideraciones reguladas en las normas profesionales. Los aspectos a tener en cuenta respecto de las pruebas de controles en conjunto con las técnicas tradicionales disponibles son desarrollados como parte de los procedimientos de auditoría externa necesarios. Esto último y la revisión de los controles internos, principalmente en entornos informatizados, forman las opciones de que dispone el auditor para su revisión y formación de opinión ante una nueva realidad en la que las tecnologías de información avanzan y son cada vez más frecuentes en las empresas.

Palabras clave: riesgo, pruebas de control, informe COSO, tecnologías de información.

ABSTRACT

The aim of this paper is to analyze the external audit procedures required to internal controls based on computer systems. To do this, first, it is considered how new technologies changed the environment in which audit and how the auditor validates the information developed under these conditions. It should be highlighted control tests available and the main effect that causes the development of their work: their evaluation should be focused on placing confidence on internal controls. Second, development of the COSO report main points and the importance for the proper survey of the system of internal control is performed. It is also progressing on other factors that increase the risks and have an impact on activities and accounting information of companies. Finally completed with the traditional task of the auditor to focus according to identified risk and considerations governed by professional standards. Aspects to consider regarding tests of controls in conjunction with traditional techniques available are developed as part of the external audit procedures required. The latter and the review of internal controls, particularly in computerized environments, are the options available to the auditor for review and opinion formation to a new reality in which information technologies are advancing and are becoming more frequent in the business.

Key words: risk, control tests, COSO report, information technologies.

ÍNDICE

| | |
|--|----|
| INTRODUCCIÓN..... | 1 |
| METODOLOGÍA..... | 5 |
| RESULTADO Y DISCUSIÓN..... | 7 |
| 1. ESTUDIO EXPLORATORIO SOBRE LA DETECCIÓN Y ANÁLISIS DEL SISTEMA INFORMÁTICO PARA EL CONTROL INTERNO..... | 7 |
| El sistema informático en el sistema contable..... | 7 |
| El auditor ante sistemas contables computarizados..... | 9 |
| Tipos de controles programados..... | 11 |
| Tarea del auditor adaptadas..... | 13 |
| 2. ESTUDIO EXPLORATORIO DE LA EVALUACIÓN DEL RIESGO DEL CONTROL INTERNO Y DE AUDITORÍA..... | 17 |
| Control Interno..... | 17 |
| Componentes del Control Interno..... | 18 |
| Consideraciones del Control Interno en la Auditoría..... | 21 |
| Consideraciones de Riesgos Internos y Externos en la Auditoría..... | 23 |
| Consideraciones de Otros Riesgos en la Auditoría..... | 23 |
| Análisis de Riesgos para Auditoría..... | 25 |
| Consideración del Efecto de Auditoría Interna sobre el Auditor..... | 25 |
| 3. ESTUDIO EXPLORATORIO SOBRE LOS PROCEDIMIENTOS DE AUDITORÍA EXTERNA DE ACUERDO A CONTROLES INTERNOS..... | 27 |
| Enfoque de auditoría..... | 27 |
| Consideraciones normativas sobre la tarea del auditor..... | 28 |
| Consideraciones para el auditor sobre las pruebas de los controles..... | 29 |
| Pruebas de los controles - Desarrollo de técnicas..... | 32 |
| Aspectos a destacar sobre los controles del auditor..... | 37 |
| CONCLUSIONES..... | 40 |
| BIBLIOGRAFÍA..... | 42 |

INTRODUCCIÓN

El objetivo del presente trabajo es realizar un análisis de la relación existente entre el proceso de la auditoría externa y los controles informáticos internos de una organización. Trabajo que comprende tanto aspectos de Auditoría Externa e Interna, y de Auditoría en sistemas computarizados.

El auditor debe emitir un informe en el que comunica su opinión acerca de si los estados contables reflejan razonablemente la situación de la empresa (FACPCE, 2004).

Para ello debe validar la información con la realidad de la empresa. Puede hacerlo mediante la aplicación de pruebas que cotejan las cifras expresadas en los estados contables con documentación respaldatoria. O bien, puede hacerlo mediante la validación de los procesos internos que posee la empresa para controlar las registraciones efectuadas.

No todas las empresas tienen normalizado un sistema de control interno, por razones de política de la Dirección o por razones de tamaño. En las pequeñas empresas la estructura operativa no permite la implementación de un proceso de control integrado. En consecuencia el conocimiento del sistema de control interno va a permitir desarrollar procedimientos de comprobación de información más eficientes en empresas que no tiene implementado un sistema de control interno (Malica y Abdelnur, 2012).

En las empresas que tienen implementado un sistema de control interno, para que sea de utilidad para la auditoría externa de estados contables, es necesario que el auditor deposite confianza en los controles que realiza la empresa. Para que el auditor decida depositar confianza, deberá evaluar el nivel de desarrollo y si funciona eficientemente. Es una tarea que constituye la “Evaluación de las actividades de control” (Malica y Abdelnur, 2012).

Este control interno es uno de los aspectos que más interesa en la evaluación de los sistemas de información. Se refiere a los métodos, políticas y procedimientos adoptados dentro de una organización para asegurar la salvaguarda de los activos, la exactitud y confiabilidad de la información gerencial y los registros financieros, la promoción de eficiencia administrativa y la adherencia a los estándares de la gerencia (Yann, 1994).

La bibliografía y las prácticas actuales conciben que una auditoría basada en riesgos requiere que el auditor entienda primero la entidad y luego identifique y evalúe los riesgos de declaración distorsionada significativa contenida en los estados financieros (Nannini y otros, 2011).

De la evaluación de riesgos que efectúe el auditor en las instancias previas al desarrollo del plan dependerá el enfoque que dará a su trabajo, es decir, su respuesta a los riesgos potenciales identificados. Decidir el enfoque de auditoría implica entonces poner sobre el tapete cuestiones disímiles que tienen que ver con la consideración del riesgo desde diversas aristas. Por un lado, deberán segregarse aquellos riesgos que comprometen a la organización desde una perspectiva global, y por otro, deberán considerarse aquellos riesgos que afecten en forma exclusiva a determinadas partidas, y que, por ello resulten susceptibles de ser desagregadas para su consideración singular (Nannini y otros, 2011).

En caso de que la tarea de evaluación de las actividades de control concluya en un resultado no satisfactorio, se aplicarán procedimientos para lograr validar la información incluida en los estados contables y así poder emitir una opinión.

El auditor independiente debe determinar los procedimientos de auditoría que podrá dejar de aplicar depositando confianza sobre los controles internos. Del mismo modo planificará los procedimientos a aplicar para suplir la ausencia de este tipo de controles.

Los procedimientos a aplicar inciden directamente en el programa de auditoría. Este último sirve como un conjunto de instrucciones para el equipo de trabajo y como un medio para el control y registro de la ejecución apropiada del trabajo. El Programa de Auditoría puede también contener los objetivos de la auditoría para cada área y un presupuesto de tiempo con las horas estimadas para las diversas áreas o procedimientos de auditoría.

Ahora bien, el desarrollo de los sistemas informáticos ha cambiado la forma en que operan las organizaciones. Una gran parte de estos controles internos se encuentran estrechamente vinculados al uso de estas tecnologías. Por eso, en la actualidad, analizar el control interno implica sumergirse en un análisis de cómo los sistemas informáticos funcionan.

Pérez Gómez (1987) afirma que el ordenador no afecta los objetivos del trabajo del auditor, pero sí afecta al sistema de control interno de la empresa, así como a las técnicas de comprobación o rastreo. Aconseja examinar y comprender la circulación de los datos económico-financieros de una empresa, desde su aparición, continuando con las transformaciones realizadas hasta su registro como información de salida.

Es decir, los objetivos del trabajo siguen manteniéndose, el cambio respecto a la auditoría tradicional es el entorno. Por ello, los auditores insisten en privilegiar la revisión del sistema de control interno: satisfechos con las medidas de control interno implementadas, dan por buenos los datos que genera el sistema de información económico-financiero (Castello, 2008).

Como acabamos de mencionar, los sistemas computarizados tienen efectos sobre el control interno. Es por esta razón que el auditor debe ser capaz de analizar las medidas utilizadas en este tipo de sistemas.

Por todo lo expuesto, la tarea del auditor independiente de formarse una opinión acerca de la razonabilidad de la información de los estados contables está estrechamente ligada al control interno. Y hoy cada vez se vuelve más evidente que estos controles internos se respaldan en recursos informáticos.

En este desarrollo se abordará la forma en que el contador auditor debe observar los sistemas informáticos, a fin de lograr el desarrollo de una auditoría más segura y eficiente. Constituye un planteamiento teórico que analiza la bibliografía existente respecto de esta temática. El objetivo ha sido analizar los procedimientos de auditoría externa necesarios ante controles internos basados en herramientas informáticas.

METODOLOGÍA

Estudio exploratorio de carácter bibliográfico sobre los siguientes ejes temáticos:

1) Estudio exploratorio sobre la detección y análisis del sistema informático aplicado por una empresa para el control interno

Se analizaron las particularidades que existen en los controles internos que las empresas aplican a sus operaciones dando prioridad a la utilización de herramientas informáticas siguiendo los lineamientos desarrollados por:

- ⇒ Castello Ricardo (2008).
- ⇒ López, Albanese, y Durán (2013).
- ⇒ Astiz Fernández y Sole Bardía (2008).
- ⇒ Pérez Gomez (1987).
- ⇒ Mancuso (1997).
- ⇒ Rezaee y Reinstein (1998).
- ⇒ Instituto Americano de Contadores Públicos Certificados (1997).

2) Estudio exploratorio de la evaluación del riesgo del control interno y de auditoría

A través de la metodología que proponen los siguientes autores, se abordó el nivel de riesgo que plantean los distintos procesos de la organización, así como también su grado de eficacia y eficiencia:

- ⇒ Cooper y Lybrand (1997).
- ⇒ Nannini, y otros (2011).
- ⇒ Castello Ricardo (2008).

- ⇒ Cuellar M. (2009).
- ⇒ Yann Derrien (1994).
- ⇒ Barreira Sans (1980).
- ⇒ Comité Internacional de Prácticas de Auditoría (2009), puntualmente NIA 315.
- ⇒ Malica y Abdelnur (2012).
- ⇒ Casal (2009).
- ⇒ Arens y Loebbecke (1996).

3) Estudio exploratorio sobre los procedimientos de auditoría externa de acuerdo a las características de controles internos

Se analizaron aquellas pruebas que un auditor puede aplicar para depositar confianza en los controles internos aplicados por las empresas y las pruebas que son requeridas para una auditoría tradicional. Se utilizó el marco brindado por:

- ⇒ RT Nro 37 de la FACPCE (2013).
- ⇒ FACPCE-CECYT (2004) Informe Nro. 5.
- ⇒ Malica y Abdelnur (2012).
- ⇒ Nannini, y otros (2011).
- ⇒ Cuellar M. (2009).

RESULTADO Y DISCUSIÓN

1. Estudio exploratorio sobre la detección y análisis del sistema informático aplicado por una empresa para el control interno

El sistema contable es, dentro de los sistemas de información, el que tiene mayor desarrollo y difusión. Comenzó, en una primera instancia, siendo para trabajar en un entorno manual como libros contables, comprobantes y otra documentación escrita. Con este formato permaneció durante varios siglos. Pero fue en las últimas décadas del siglo XX cuando fue transformado por la implementación de tecnologías, desde máquinas de registro inicial hasta el posterior uso de las computadoras (Castello, 2008).

Los sistemas informáticos, que, tal como se ha mencionado en el párrafo anterior, han sido incorporados en el último tiempo, establecieron una nueva realidad para el auditor. El mismo se encuentra con dificultades como el que la información está registrada de un modo no es accesible al ojo humano. Por tal razón, el auditor depende de especialistas en informática para el acceso a la información. Además, hay una facilidad para modificar los datos sin dejar rastros. Y también existen controles que se delegan al sistema informático (Castello, 2008).

En igual sentido se expresan Rezaee y Reinstein (1998) al decir que la evidencia de la auditoría tradicional fue reemplazada por la prueba electrónica. Esta última, según el Instituto Americano de Contadores Públicos Certificados (1997), es información transmitida,

procesada, mantenida o consultada por medios electrónicos. Y, agrega, es la que el auditor utiliza para evaluar las aseveraciones de los estados financieros.

Debido a que no puede ser observada, se van a requerir el uso técnicas de auditoría informática con el fin de poder llevar a cabo las pruebas de auditoría sobre la prueba electrónica (Mancuso, 1997).

López y otros (2013) también sostienen que a partir de la incorporación de tecnologías de información se produce una evolución de las evidencias de auditoría. Su utilización convierte en digitales casi la totalidad de las evidencias, careciéndose del acceso tradicional a la documentación de referencia. Agregan que es posible que esta documentación se encuentre disponible solo por un período limitado de tiempo. Destacan la necesidad del auditor de mejorar sus competencias para adaptarse a estos entornos y permitir la obtención de evidencias.

A partir de las distintas posturas citadas, se observa entre los distintos autores una marcada coincidencia. En común afirman que el uso de sistemas informatizados limita el acceso físico a las pruebas sobre las cuales puede apoyar el auditor sus aseveraciones.

Continuando con la temática en desarrollo, se resalta que la introducción de la computadora no ha afectado los objetivos del trabajo del auditor. En cambio, sí afecta al sistema de control interno de la empresa, así como también a las técnicas de comprobación o rastreo. Ante esta situación se recomienda examinar y comprender la circulación de los datos económico-financieros de una empresa, desde su aparición, continuando con las transformaciones realizadas hasta su registro como información de salida. Por último se deben identificar las fuentes de información elemental, las distintas combinaciones que sufre esa

información elemental a lo largo del proceso, las pistas de auditoría, y los controles, tanto manuales como informáticos existentes (Pérez Gomez, 1987).

Otros autores coinciden en que la tecnología informática no ha modificado el objetivo de la auditoría, pero sí los procesos de registro, almacenamiento y comunicación de las organizaciones. Es decir, ha cambiado la forma en la que se operan los negocios. Ante esto, la auditoría debe adaptarse por ejemplo a la existencia de transacciones no escritas, autorizaciones virtuales y registros electrónicos (López y otros, 2013).

Astiz Fernández y Sole Bardia (2008) han sido más enfáticos al considerar cómo las tecnologías han afectado el trabajo del auditor. Sostienen que sin un conocimiento de los sistemas de control interno informático no se estaría en posición de determinar la integridad y exactitud de los datos contables. La tendencia hacia un enfoque de auditoría basado en la confianza sobre los controles debe ser un proceso natural, en especial cuando aumenta la complejidad de la organización.

En otras palabras, los auditores necesitan darle prioridad a la revisión del control interno. Si las medidas de control interno utilizadas son adecuadas, pueden dar por buenos los datos que genera el sistema de información (Castello, 2008).

Como consecuencia, la auditoría de información contable que ha sido procesada a través de sistemas informáticos recae principalmente en el conocimiento que se forma sobre el control interno. Los auditores deben dirigir sus esfuerzos en analizarlo para lograr la mayor eficiencia.

Cuando el auditor se encuentra delante de sistemas que incluyen tecnología computarizada deben estudiar el control interno, agrupándolo en dos grandes categorías. La

primera de esas categorías son los controles de entorno, y la segunda, los controles programados o de aplicación (Castello, 2008).

En la categoría de controles de entorno se debe realizar un análisis de las actividades que se producen “alrededor” de la aplicación. El auditor observa los elementos relacionados a la estructura. Dentro de ellos se incluyen el control de las actividades relacionadas con la operación de los sistemas, la construcción y mantenimiento de las aplicaciones, la puesta en marcha y uso de los programas, la seguridad de operación y resguardo de los archivos de datos o el control de acceso al sistema (Castello, 2008).

Los controles del entorno pueden estar orientados a:

- Las operaciones del computador, en las que se aseguran la consistencia de los procedimientos. Por ejemplo, implementar procedimientos y asignar responsabilidades para las tareas de back up, mantenimiento de perfiles de usuario, etc.
- La seguridad sobre archivos de datos, tarea en la que se procura impedir el acceso no autorizados o cambios no deseados a los datos. La configuración de perfiles de acceso a archivos y directorios es un ejemplo.
- El mantenimiento de los programas, el cual comprende controles y autorizaciones para poner en producción nuevos programas o aquellos modificados. Por ejemplo el uso de metodologías para el desarrollo y procedimientos para gestionar las modificaciones.
- Los productos de software utilizados, para evitar el uso incorrecto e indebido de software que pueda afectar la información sensible de la empresa. Se puede mencionar el requisito de usar solo versiones licenciadas de los productos, estandarizando las herramientas de productividad que pueden utilizar los usuarios (Castello, 2008).

La otra categoría de los controles que realiza el auditor ante entornos informáticos, es decir, los controles programados o de aplicación, se relacionan con los procedimientos operativos. Aquí se trata de los procedimientos automatizados de verificación y validación ejecutados por los programas de una aplicación que se ejecutan en forma autónoma (Castello, 2008).

Tipos de controles programados

Controles de entrada

A decir de Castello (2008) son los mecanismos de control que operan sobre los datos que ingresan al sistema. Así, los datos serán solo los debidamente autorizados y aquellos que cumplan los requisitos de integridad, exactitud y validez. Estas pruebas automáticas realizan validaciones, acumulación de totales, reconciliaciones, identificación e informe de datos incorrectos, excepcionales o faltantes, etc.

Para clarificar este tipo de controles el autor ya mencionado, Castello (2008), los agrupa en categorías:

- ❖ de formato: validan los datos de entrada en función de la “naturaleza” del campo, ejemplo: numérico, alfabético, fecha.
- ❖ de secuencia: verifican que las operaciones entren en el sistema en su totalidad y en el orden correspondiente.
- ❖ de comparación con datos preexistentes: impiden la aceptación de un dato si éste no satisface las condiciones previamente establecidas por otro dato.
- ❖ por límites: rechazan o advierten que los datos de entrada que no estén comprendidos dentro de determinados parámetros.

- ❖ por lotes: toma como elemento de control el resultado del procesamiento de un dato correspondiente a un lote de entrada. Por ejemplo, total de venta correspondiente a un día determinado en una sucursal no puede ser negativo.

Controles de procesamiento

Una vez que una transacción ingresa al sistema operan sobre ella transformaciones con el fin de obtener nueva información. Los controles de procesamiento están destinados a ese tipo de transformación. Tienden a mejorar la seguridad y confiabilidad en el procesamiento de datos, evitar que se produzcan fraudes o errores y a que la información obtenida sea correcta (Castello, 2008)

Castello distingue dentro de estos controles los siguientes tipos:

- control de límite, rechazan o advierten que los datos de entrada que no estén comprendidos dentro de determinados parámetros.
- prueba de sumas cruzadas, las cuales suman el mismo ítem desde varias fuentes.
- prueba de balanceo cero, en la que se asegura que los créditos son iguales a los débitos.
- control de procesamiento duplicado, estos controles aseguran que una transacción no se procese dos veces.
- control de ítems en suspenso, es decir de aquellas operaciones que no han satisfecho alguno de los requisitos de entrada y han quedado en un archivo especial. Cuando sean cumplidos los mencionados requisitos podrán ser procesadas.

Controles de salida

Estos controles deben proteger que la información que genera el sistema sea susceptible de errores o irregularidades cuando llegue a su usuario. Los mecanismos que garantizan la exactitud de la información son de especial importancia en este punto (Castello, 2008).

Controles sobre los archivos

Aquí se opera tanto sobre datos permanentes del sistema, grabados en archivos maestros, como datos transitorios. Este control protege los archivos grabados en soporte digital. Intervienen el departamento de sistemas y también los usuarios.

Dentro de este tipo de controles el autor menciona, respecto de las modificaciones efectuadas a los datos de los archivos maestros:

- número de registros dados de alta, baja o modificados.
- número de registros existentes en los archivos antes y después de las modificaciones.
- sumatoria del contenido de campos significativos que se deseen controlar (Castello, 2008).

Si bien la responsabilidad de los datos de un sistema recae sobre los usuarios finales, debe considerarse que el área de sistemas brinda un apoyo importante. El mismo debe procurar que no se produzcan modificaciones sobre datos críticos que no se encuentren amparados con sus respectivas autorizaciones (Castello, 2008).

Cada una de los tipos de controles programados explicitados se encuentran a disposición del auditor para el análisis del control interno. A mayor cantidad de controles, mayor es la probabilidad de que el sistema contenga información correcta.

Avanzando, ahora, sobre la tarea del auditor López y otros (2013) proponen que al momento de definir las tareas de auditoría se tenga en cuenta la particularidad de que se trabaja dentro de un entorno informático. En un principio, al planificar, se debe profundizar el conocimiento del negocio del cliente e industria. Cuando se analicen los riesgos, los derivados del uso sistemas informáticos cobran relevancia. El plan de auditoría debe ser confeccionado en función de la eficiencia y la eficacia de los controles internos por sobre las pruebas sustantivas de los documentos y transacciones electrónicas.

Luego, en la ejecución, el auditor debe resaltar la tarea de evaluar la validación de los controles internos informáticos cuando se utilice el enfoque de cumplimiento. En caso de optar por un enfoque sustantivo, las técnicas de auditoría asistidas por computador deben ser las dominantes (López y otros, 2013).

Finalmente, en el reporte, estos autores sugieren al auditor incluir recomendaciones sobre el control interno, así como observaciones relacionadas al uso de tecnologías de información (López y otros, 2013).

Se destaca entonces que los aspectos informáticos deben ser tenidos en cuenta por el auditor. Esta consideración debe ser realizada especialmente cuando desee determinar la forma en que se logra el conocimiento, comprensión y evaluación de los sistemas de contabilidad y control interno. Además, cuando requiera evaluar las consideraciones de los riesgos inherentes y de control, ya que de esta forma el auditor llega a la evaluación del riesgo de auditoría. Y también para analizar el diseño y aplicación de pruebas de control y procedimientos sustantivos apropiados para cumplir con el objetivo de la auditoría (López y otros, 2013).

Finalmente Castello (2008) propone que, al momento de programar la auditoría, se realice un relevamiento del sistema de control interno. El mencionado relevamiento del control interno que aplica tecnologías informáticas, recomienda conste de tres fases: estudio preliminar, estudio del sistema de control interno y prueba de los controles de los sistemas de información.

Estudio preliminar

Es la tarea previa al análisis detallado. Tiene como objetivo determinar las aplicaciones y sistemas que se auditan, así como también sus efectos sobre la información. Otro objetivo de su realización es llegar a conocer el equipamiento y sus características. El último fin es definir los efectos que los sistemas computarizados producen en la información de la empresa.

Estudio del sistema de control interno

Este estudio adquiere importante relevancia cuando se ha identificado previamente que intervienen sistemas informáticos para el procesamiento de la información de la empresa. El autor califica la tarea como obligatoria en estos casos.

Los objetivos del estudio del sistema de control interno son, por un lado, evaluar la estructura organizacional del área de sistemas y los controles bajo los que opera ese sector. Y por otro lado, conocer las características de las aplicaciones, el grado de intervención en la transformación de datos y la cantidad de operaciones que dependen del sistema. Se debe determinar si es necesario aplicar pruebas de cumplimiento a los controles que realiza el ambiente de procesamiento de datos.

Prueba de los controles del sistema de información

Se define como una actividad necesaria en aquellos casos en los que existe una importante cantidad de información proveniente de los sistemas. El auditor, de esta forma, puede considerar válida y suficiente la información emitida por los mismos.

Sintetizando lo desarrollado en esta metodología, podemos concluir que la adopción de nuevas tecnologías para el procesamiento de datos ha producido un cambio en la auditoría tradicional. No en el objetivo que la misma tiene, el cual es recolectar los elementos de juicio válidos y suficientes para emitir un dictamen sobre la veracidad de la información contenida en los estados contables. Sino más bien, en el enfoque que debe darle a su tarea profesional basándolo principalmente en depositar confianza en los controles internos que se están aplicando.

La información que las empresas incluyen en sus estados contable proviene de sus sistemas informáticos. Siendo de este modo, el auditor para lograr formarse una opinión acerca de la veracidad, exactitud, integridad de esa información cuenta con un conjunto de técnicas que le permiten validar cómo es el flujo de datos bajo estas nuevas tecnologías.

Finalmente, ante esta nueva realidad, es altamente recomendable la utilización de estas nuevas técnicas para lograr un trabajo eficiente y eficaz. La falta de consideración de las mismas pueden incluso llegar a imposibilitar la formación de una opinión respecto de la información contenida en los estados contables auditados.

2. Estudio exploratorio de la evaluación del riesgo del control interno y de auditoría

Según el Informe COSO de Coopers y Lybrand (1997) el control interno es un proceso efectuado por el Consejo de Administración, la Dirección y el resto del personal de la entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:

- Eficacia y eficiencia de las operaciones,
- Fiabilidad de la información financiera,
- Cumplimiento de leyes y normas aplicables.

Otros autores se refieren al control interno como los métodos, políticas y procedimientos adoptados dentro de una organización. El objetivo de los mismos es asegurar la salvaguarda de los activos, la exactitud y confiabilidad de la información gerencial y los registros financieros, la promoción de eficiencia administrativa y la adherencia a los estándares de la gerencia (Yann, 1994).

Al concepto dado de control interno, Castello (2008) agrega que, a su criterio, las definiciones reflejan ciertos conceptos fundamentales. Primero, Cuando se habla de control interno, se está hablando de un proceso, entendido como un medio para lograr un fin, y nunca un fin en sí mismo. Segundo, es una tarea llevada a cabo por las personas, por lo que debe evitarse que quede solamente en un conjunto de manuales y políticas impresas. Tercero, el control interno procura alcanzar un nivel razonable de seguridad, y no la seguridad total, para

la Dirección de la entidad. Por último, está pensado para facilitar el logro de los objetivos propios de cada entidad.

Avanzando con el informe COSO, se aclara que el control interno consta de cinco componentes. Todos ellos están relacionados entre sí. Y existe una derivación de cada uno de acuerdo al estilo de dirección de cada organización. Asimismo, los componentes, se integran al proceso de gestión de una entidad (Castello, 2008).

A pesar de que estos componentes están presentes en todas las entidades, las pequeñas y medianas compañías pueden implementarlos en forma diferente a como lo hacen las grandes. Sus controles pueden ser menos formales y menos estructurados pero, con todo, una compañía pequeña puede tener un eficaz control interno (Cuellar M., 2009).

Los componentes que conforman el sistema de control interno mencionados por Coopers y Lybrand (1997) en el Informe COSO son:

- Ambiente de Control
- Evaluación de Riesgos
- Actividades de Control
- Información y Comunicación
- Supervisión

Ambiente de control

El entorno de control establece el tono de una organización, influyendo la conciencia de control de su gente. Es la base para todos los otros componentes del control interno, proporcionando disciplina y estructura (Cuellar M., 2009).

Para evaluar el ambiente de control el auditor debe observar una serie de factores para determinar si el ambiente es positivo. Las características que posea determinan la conducta del personal en su conjunto (Castello, 2008).

Cuellar (2009) agrega que el corazón de cualquier negocio es su gente - sus atributos individuales, incluyendo integridad, valores éticos y competencia - y el ambiente en el cual se trabaja. Es el motor que impulsa a una entidad y la base sobre la que todo descansa.

Evaluación de riesgos

La entidad debe estar al tanto y manejar los riesgos a los que se enfrenta. Debe establecer objetivos, integrados con las actividades de ventas, producción, de mercado, actividades financieras y otras, a efectos de que la organización opere en forma concertada. También debe establecer mecanismos para identificar, analizar y manejar los riesgos relacionados (Cuellar M., 2009).

El control interno es esencial para limitar los riesgos que afectan las actividades de toda organización. El auditor, a través de la investigación y análisis de los riesgos relevantes y el punto hasta el cual el control los neutraliza, puede evaluar la vulnerabilidad del sistema. Requiere para tal apreciación, un conocimiento práctico de la entidad y sus componentes, de manera de identificar los puntos débiles. Debe abarcar tanto riesgos a nivel de organización, como a nivel de actividad (Castello, 2008).

Actividades de control

Deben establecerse y ejecutarse políticas y procedimientos de control para ayudar a asegurar que las acciones de la entidad sean eficazmente llevadas a cabo. Las acciones a las

que se encuentran dirigidos los controles son aquellas identificadas por la Dirección como necesarias para encarar los riesgos asociados al logro de los objetivos (Cuellar M., 2009).

Este tipo de actividad se desarrolla en todos los niveles de la organización con el fin de asegurar que se lleven a cabo las instrucciones de la Dirección, es decir, que se cumplan los objetivos fijados. Conociendo los riesgos, se deben evaluar los controles para determinar si son útiles y suficientes a los fines de evitarlos o minimizarlos (Castello, 2008).

El auditor debe observar las actividades de control bajo el contexto de objetivos fijados por la Dirección. Para ello tiene en cuenta si las actividades de control están relacionadas con el proceso de evaluación de riesgo y si son apropiadas para asegurar que las instrucciones se cumplan. Dicha evaluación se efectuará para cada actividad importante, incluidos los controles generales de los sistemas informáticos. Además, deberá tener en cuenta no solamente si las actividades de control empleadas son relevantes en base al proceso de evaluación de riesgos realizado, sino también si se aplican de manera correcta (Castello, 2008).

Información y comunicación

Debe haber una comunicación eficaz en un sentido amplio, que fluya en todas las direcciones a través de todos los ámbitos de la organización, de arriba hacia abajo y a la inversa. Las responsabilidades de control han de tomarse en serio. Los empleados tienen que comprender cuál es su papel en el sistema de Control Interno y cómo las actividades individuales están relacionadas con el trabajo de los demás. Asimismo, tiene que haber una comunicación eficaz con terceros como clientes, proveedores, organismos de control y accionistas (Castello, 2008).

Cuellar (2009) lo resume diciendo que los sistemas de información y comunicación permiten a los integrantes de la entidad obtener e intercambiar la información necesaria para conducir, manejar y controlar sus operaciones.

Supervisión

El proceso completo de control debe estar supervisado o monitoreado y deben efectuarse las modificaciones necesarias. De esta forma, el sistema puede reaccionar dinámicamente, cambiando cuando las condiciones lo justifiquen (Cuellar M., 2009).

Los sistemas de Control Interno requieren supervisión, es decir, un proceso que compruebe que se mantiene el adecuado funcionamiento del sistema a lo largo del tiempo. Esto se consigue mediante actividades de supervisión continua, evaluaciones periódicas o una combinación de ambas cosas (Castello, 2008).

La anteriormente desarrollada división en cinco componentes provee un marco útil para que los auditores consideren la manera en que los diferentes aspectos del control interno de una entidad pueden afectar la auditoría. Del examen del control interno de su cliente, el auditor puede identificar riesgos de auditoría y determinar el alcance de los procedimientos de auditoría (Nannini, y otros, 2011).

Para Nannini y otros (2011) es conveniente comenzar clasificando conceptualmente el “*riesgo de auditoría*”. De esta forma encontramos:

- Riesgo inherente: riesgo de que ocurran errores significativos en la información contable, sin perjuicio de la existencia o no de sistemas de control.

- Riesgo de control: riesgo de que el control interno de la entidad no prevenga ni detecte los errores.
- Riesgo de no detección: riesgo de que errores remanentes importantes no sean detectados por el auditor.

Cuando se menciona el término “riesgo de auditoría” hay un elemento estrechamente relacionado que es fundamental tener en cuenta. Este elemento es el control interno (Nannini, y otros, 2011).

Según el Comité Internacional de Prácticas de Auditoría (2009) en su NIA 315, la división de control interno en cinco componentes, como la propuesta por el Informe COSO, provee un marco útil para los auditores. A partir del mismo pueden considerar la manera en que los diferentes aspectos del control interno de una entidad llegan a afectar la auditoría. La consideración primaria del auditor es si (y cómo) un control específico previene o detecta y corrige errores significativos en clases de transacciones, cuentas del balance o informaciones complementarias y sus respectivas aserciones.

De los factores mencionados precedentemente encontramos algunos que pueden influir en el sistema contable y otros que no. Es por ello que el auditor no debe dejar de reconocer ni perder de vista los casos que producen efectos contables (Nannini, y otros, 2011).

La evaluación final de los controles tiene por objetivo la obtención de información para identificar los riesgos individuales de auditoría que se considerarán al preparar el programa de Auditoría (Nannini, y otros, 2011).

Esta evaluación debe considerarse provisoria, mientras continúe el examen de los estados contables, porque cualquiera de las pruebas de validación de saldos puede poner en

evidencia defectos de control. Existe el riesgo de considerar aceptable algo que no lo es, debido a que el funcionamiento de los controles se prueba por muestreo y con posterioridad al examen podrían producirse cambios en los sistemas desconocidos por el auditor. Si se evidencia su existencia deben revisarse las anotaciones sobre el funcionamiento del control interno (Nannini, y otros, 2011).

Otra cuestión a considerar, es la realidad de que las entidades enfrentan una serie de riesgos tanto de origen interno como externo que deben ser evaluados. El método recomendado consiste en identificar y analizar aquellos factores que puedan llegar a influir en la consecución de los objetivos. Este análisis también contribuye para determinar qué riesgos deben ser estudiados (Castello, 2008).

Se recomienda, en forma complementaria, identificar los objetivos globales y por actividad de una entidad. Y aunque no éstos no forman parte del control interno, su fijación permite identificar los riesgos para alcanzarlos. La empresa puede tener los objetivos expresamente declarados, o bien pueden estar implícitos (Castello, 2008). El auditor debe reconstruirlos cuando los mismos sean informales.

No solo los riesgos a nivel empresa deben ser identificados. Luego de ese procedimiento corresponde que se realice lo mismo a nivel de cada actividad. Esto ayuda a reconocer riesgos de las unidades o funciones más importantes del negocio, y contribuye a mantener un nivel de riesgo aceptable para toda la entidad (Castello, 2008).

Finalmente, existen otros riesgos que pueden producir una re-evaluación del control interno, y que el auditor debe tener en cuenta su posibilidad de ocurrencia. Son el riesgo de fraude, el relativo de auditoría, el del negocio, el residual, el de independencia, el de servicio

al cliente, el operacional y el impacto del riesgo empresarial en el riesgo aceptable de auditoría (Nannini, y otros, 2011).

El riesgo de fraude es un acto intencional que genera una declaración equivocada material. Hay dos tipos de declaraciones equivocadas intencionales, las que surgen de información contable fraudulenta y las que surgen del uso indebido de los activos (Malica y Abdelnur, 2012). Para estos autores además de un riesgo adicional, debe ser considerado un riesgo propio de la auditoría.

Riesgo relativo de auditoría significa que, en el caso de determinados entes el riesgo puede ser mayor que para otros. También puede suceder para ciertos componentes o sistemas, rubros y/o cuentas de los estados contables financieros y de sus objetivos de auditoría (Casal, 2009).

Riesgo del negocio se refiere al riesgo de que los objetivos del negocio del ente no se alcancen como resultado de los factores, presiones y fuerzas (internas y externas) que lo afecten. Incluye el riesgo relacionado con la supervivencia del ente y la rentabilidad (Casal, 2009).

El riesgo residual es el remanente después de considerar la influencia mitigante de los controles del negocio del ente (Casal, 2009).

Riesgo de independencia. La independencia es la condición básica para el ejercicio de la auditoría. Cuando es vulnerada tiene posibles efectos para el auditor y la auditoría (Casal, 2009).

Riesgo de servicio al cliente es el riesgo de no cubrir las expectativas depositadas por el cliente en el trabajo del auditor (Casal, 2009).

Riesgo operacional hace mención al riesgo de pérdida provocado por la falla o insuficiencia de los procesos, personas y sistemas internos o por eventos externos a la entidad (Casal, 2009).

El riesgo empresarial es el riesgo que el auditor o el despacho de auditoría sufrirá un daño debido a una relación con el cliente, aunque el informe de auditoría presentado para el cliente estuviese correcto (Arens y Loebbecke, 1996).

Una vez culminado el proceso de identificación de riesgos se debe realizar el análisis de riesgo. Esto implica, en primer lugar, efectuar una estimación de la importancia del riesgo. En segundo lugar, una evaluación de la probabilidad o frecuencia de que se materialice el riesgo. Luego, realizar una cuantificación de la pérdida probable. Y por último, determinar las medidas que deben adoptarse para mitigarlo (Castello, 2008).

Complementando lo referido a análisis, un riesgo que no tiene un efecto significativo sobre la entidad y que tiene una baja probabilidad de ocurrencia generalmente no merece una consideración demasiado exhaustiva. Un riesgo significativo con una alta probabilidad de ocurrencia, en cambio, generalmente demanda atención considerable. Aquellos casos que estén entre estos extremos generalmente requerirán juicios difíciles. Es muy importante que se realice un cuidadoso y racional análisis (Cuellar M., 2009).

Sin embargo, así como existen cuestiones que incrementan los riesgos de una auditoría, hay otras que lo disminuyen. El funcionamiento de una Auditoría Interna influye notablemente en el ambiente de control y la cultura de la organización. Se puede observar

que inciden en la eficacia del control interno su independencia respecto de la Dirección, la experiencia y calidad de sus miembros, el grado de implicancia y vigilancia, y el acierto de sus acciones (Castello, 2008).

Al decir de Barreira Sans (1980) la estructura jerárquica existente en algunas organizaciones, la auditoría interna, ejecuta funciones de control. Se encuentran entre sus tareas el tener conocimiento de la gestión de la empresa; contrastar su funcionamiento de acuerdo a lo que se ha previsto. También examina la rectitud, suficiencia y aplicación de criterios contables, financieros y operacionales; comprueba que la información responde a la realidad; verifica que la división funcional del trabajo sea acorde al control interno. Además juzga la aceptabilidad de los planes y presupuestos; y asimismo controla la integridad y exactitud del activo de la empresa. Finalmente comprueba que se recogen todas las obligaciones existentes frente a terceros, así como los riesgos latentes; y recomienda mejoras operacionales si en su control detecta deficiencias.

Cuellar M., (2009) expone sobre la auditoría interna, que sus integrantes juegan un rol importante al evaluar la eficacia de los sistemas de control y contribuyen a una eficacia continua. Debido a la posición organizacional y a la autoridad en una entidad, una función de auditoría interna a menudo juega un rol significativo en el monitoreo.

De todas formas la creación de un departamento de auditoría interna no siempre es recomendada. Hay empresas que por su tamaño no lo precisan, son casos en los que la Dirección debe y puede llevar el control por sí misma. En otros casos corresponde determinar el costo-beneficio, ya que es posible que los beneficios no superen los costos de su funcionamiento, en cuyo caso su creación tampoco es recomendable (Barreira Sans, 1980).

Concluyendo lo desarrollado en esta metodología, se destaca que el informe COSO constituye una importante herramienta de la cual puede disponer el auditor para evaluar el riesgo. Ésta le permite realizar un relevamiento del control interno de una entidad y observar si un control específico previene o detecta y corrige errores significativos. Las posibles desviaciones que el control interno no resuelva son los que representan el mayor riesgo. La mirada del auditor debe enfocarse hacia estas cuestiones en las que no están dadas las garantías de certeza, veracidad e integridad; puesto que son las características que debe reunir la información contable.

Asimismo, es posible notar que una entidad que posee una unidad de Auditoría Interna se encuentra continuamente desarrollando revisiones de los procesos de control interno. Por lo tanto, la eficiencia y eficacia del mismo estaría mejor lograda. El auditor puede analizar las características de la Auditoría Interna para tener una aproximación del nivel en el que se ubican los controles internos de la organización.

3. Estudio exploratorio sobre los procedimientos de auditoría externa de acuerdo a las características de controles internos

El enfoque de auditoría (determinación de la naturaleza, oportunidad y alcance de los procedimientos de auditoría a aplicar) está relacionado estrechamente con la evaluación del riesgo que realiza el auditor, e implica buscar la combinación adecuada entre pruebas de

cumplimiento y pruebas de validación o sustantivas a fin de obtener evidencias de auditoría con la menor cantidad de horas insumidas (Nannini, y otros, 2011).

De la evaluación de riesgos que efectúe el auditor en las instancias previas al desarrollo del plan depende el enfoque que da a su trabajo, es decir, su respuesta a los riesgos potenciales identificados. Decidir el enfoque de auditoría implica entonces poner sobre el tapete cuestiones disímiles que tienen que ver con la consideración del riesgo desde diversas aristas. Por un lado, deben segregarse aquellos riesgos que comprometen a la organización desde una perspectiva global, y por otro, deben considerarse aquellos riesgos que afecten en forma exclusiva a determinadas partidas, y que, por ello resulten susceptibles de ser desagregadas para su consideración singular (Nannini, y otros, 2011).

La Resolución Técnica N° 37 emitida por la FACPCE (2013) establece que el auditor debe reunir los elementos de juicio válidos y suficientes que permitan emitir su informe a través de la aplicación de procedimientos de auditoría.

Uno de esos procedimientos es la evaluación del control interno pertinente a la valoración del riesgo, siempre que, con relación a su tarea, el contador decida depositar confianza en el control interno del ente. Esta evaluación es conveniente que se desarrolle en la primera etapa porque sirve de base para perfeccionar la planificación en cuanto a la naturaleza, extensión y oportunidad de las pruebas de auditoría a aplicar. Si el ente utilizase una organización de servicios, es necesaria la obtención de conocimiento sobre ella, incluido el control interno relevante para la auditoría, que sea suficiente para identificar y valorar los riesgos de incorrección material, así como para diseñar y aplicar procedimientos de auditoría que respondan a dichos riesgos (FACPCE, 2013).

Para la RT 37 FACPCE (2013) el procedimiento de evaluación de control interno implica, en primer lugar, relevar las actividades formales de control interno que son pertinentes a su revisión. En segundo lugar, comprobar que esas actividades formales de control interno se aplican en la práctica. Luego, evaluar las actividades reales de control interno, comparándolas con las que se consideren razonables en las circunstancias. Y finalmente, determinar el efecto de la evaluación mencionada sobre la planificación, de modo de replantear, en su caso, la naturaleza, extensión y oportunidad de los procedimientos de auditoría seleccionados previamente.

Cuando el auditor decide depositar confianza en el control interno de la empresa, debe probar su funcionamiento, para ello aplica las “Pruebas de los controles” (Malica y Abdelnur, 2012).

Las pruebas de los controles deben ser diseñadas para obtener evidencia de auditoría. Se aplican respecto de si los controles identificados funcionaron adecuadamente durante el período bajo examen. Si durante ese periodo hubo en algún período parcial aplicación de otros controles, cada sistema de control interno debe ser considerado por separado. Además se aplican respecto de la consistencia con la cual se aplicaron los controles internos, y por quién y por qué medios fueron aplicados los controles (Malica y Abdelnur, 2012).

Los procedimientos a aplicar para probar la efectividad de la operatoria pueden consistir en indagación al personal, inspección de la documentación relevante, observación de las operaciones de la compañía o volver a realizar la operación del control (Malica y Abdelnur, 2012).

Se debe determinar qué constituye una desviación de control. Cuando se diseñan las pruebas de los controles, debe dedicarse tiempo para definir exactamente qué constituye un error o una excepción a la prueba (Malica y Abdelnur, 2012).

Hay algunos casos en que las actividades de control son realizadas por el computador y no existe documentación de respaldo. En estos casos el auditor tiene que volver a realizar el control para asegurarse que los controles de la aplicación del software están funcionando tal y como fueron diseñados (Malica y Abdelnur, 2012).

Otro enfoque es usar lo que se denomina “Técnicas de auditoría asistidas por computadoras o CAATs”, por ejemplo: importar el archivo de datos de la entidad y luego probarlos, tales programas a menudo ofrecen evidencias de auditoría que se necesita (Malica y Abdelnur, 2012).

El objetivo de la prueba es obtener evidencia de auditoría suficiente y apropiada de que el control interno operó efectivamente durante el período de confianza.

Cuando se diseñan los procedimientos de auditoría, puede ser útil considerar dos niveles de confianza a alcanzar a partir de las pruebas de los controles:

- Un nivel alto de confianza (nivel bajo del riesgo que permanece); y
- Un nivel moderado de confianza (nivel moderado del riesgo que permanece).

Si la evidencia primaria viene de la prueba de los controles, entonces se requiere un nivel alto de confianza. Si se combinan las pruebas de los controles con procedimientos sustantivos, un nivel bajo de confianza (moderado), puede ser todo lo que se requiera (Malica y Abdelnur, 2012).

Como una guía para definir la extensión de las pruebas, el manual de la IFAC considera que deben tenerse en cuenta los siguientes puntos:

Cuando el muestreo estadístico es usado para evaluar la efectividad del control interno, el tamaño de la muestra no debe variar en proporción al crecimiento del tamaño de la población. Una muestra al azar, tan pequeña como de 30 ítems, que no presente ninguna desviación, puede proveer un alto nivel de confianza de que el control interno está operando efectivamente (Comité Internacional de Auditoría, 2009).

Los procedimientos sustantivos son usados para obtener evidencia con relación a toda clase de transacciones, saldos de cuentas y revelaciones que sean materiales. Existen dos tipos de procedimientos sustantivos, las pruebas de detalle y los procedimientos sustantivos analíticos (Comité Internacional de Auditoría, 2009).

La extensión de los procedimientos sustantivos que se requieren es mayor cuando los procesos que contador audita presentan importantes riesgos de declaración equivocada material. Así también es mayor su extensión cuando se evalúa el control interno y se decide no confiar en el mismo (Malica y Abdelnur, 2012).

Luego de la terminación de la auditoria, se requiere que el auditor use los procedimientos analíticos para ayudar a evaluar la presentación general del estado financiero. Esto permite determinar si los estados contables tomados en su conjunto son consistentes con el entendimiento que el auditor tiene respecto de la entidad (Malica y Abdelnur, 2012).

Regresando al método con el que el auditor obtiene los elementos de juicio válidos y suficientes que permitan emitir su informe, la RT 37 (2013) continúa con los pasos, más allá de los relacionados con la verificación de las actividades de control interno. Establece como parte de la tarea del auditor, cotejo de los estados contables con los registros contables, inspecciones oculares, obtención de confirmación directa de terceros. Además, la revisión de la correlación entre registros contables, y entre éstos y la correspondiente documentación comprobatoria. También incluye comprobaciones matemáticas, revisiones conceptuales, comprobación de información relacionada, comprobaciones globales de razonabilidad, examen de documentos importantes. Por último, preguntas a funcionarios y empleados del ente; en particular, preguntas a la Dirección para identificar si existen dudas sustanciales sobre la capacidad del ente para continuar como una empresa en funcionamiento, y obtención de una confirmación escrita de la Dirección del ente de las explicaciones e informaciones suministradas.

El Informe 5 de la FACPCE-CECYT (2004) desarrolla un conjunto de pruebas de las que puede valerse el auditor, y que son comúnmente utilizadas para cumplir lo establecido en la resolución técnica del párrafo anterior.

Pruebas Analíticas o Sustantivas

Los procedimientos de revisión analítica o sustantivos, mencionadas anteriormente, consisten en pruebas que se aplican sobre información contable y que comprenden el estudio y la comparación de relaciones entre datos. La premisa básica subyacente en la aplicación de los procedimientos de este tipo es que ciertas relaciones pueden razonablemente esperarse que existan y continúen en el tiempo a falta de condiciones que indiquen lo contrario.

Son de suma importancia para el auditor pues le permiten formarse una opinión sobre la consistencia lógica de la información contable e indagar sobre las relaciones inusuales que encuentra en estas pruebas. Esto, en cualquiera de las etapas que los aplique e independientemente de los objetivos que persigue en cada una de ellas. Justo es destacar que perfeccionan el conocimiento del auditor sobre las operaciones del ente, permitiéndole interpretar si a la luz de esas operaciones de su cliente los estados contables tienen sentido (FACPCE-CECYT, 2004).

Toda revisión analítica implica la comparación de una partida con otra y la comparación procura establecer una relación que pueda ser considerada lógica. Ahora bien, si se ha de validar una partida (variable dependiente) por su relación con otra (variable independiente), el auditor debe satisfacerse que esta última sea confiable y que la relación funcional sea válida (FACPCE-CECYT, 2004).

Puede tratarse de análisis comparativo de estados contables de períodos sucesivos, en valores absolutos y en porcentajes. Otro caso es el análisis de tendencias respecto de un año base. También se encuentran la comparación de datos reales con presupuestados. Análisis de cocientes o ratios importantes y comparación con los ejercicios anteriores y los típicos del ramo del negocio, como una alternativa adicional. Finalmente, se puede optar por las relaciones lógicas entre ciertas cifras de los estados contables (FACPCE-CECYT, 2004).

Algunas de las pruebas de revisión analítica que el auditor puede aplicar son:

- Prueba de amortizaciones.
- Prueba de ingresos.
- Análisis de los márgenes de utilidad.

- Relaciones entre cuentas contables que deben seguir un parámetro lógico (comisiones/ventas; ingresos brutos/ventas; cargas sociales/remuneraciones; débito fiscal IVA/ventas; devoluciones/ventas).
- Análisis de la evolución de los sueldos y jornales.
- Índices de rotación de créditos; de bienes de cambio, de cuentas a pagar.

Estos ejemplos de pruebas de revisión analítica dan cuenta de las posibilidades de que dispone el auditor al momento de desarrollar su tarea. Como se observa, son combinaciones de valores presentes en todo sistema de información contable.

Observación de Actividades

Siguiendo también a FACPCE-CECYT (2004), existen las pruebas de observación de las actividades de la organización para verificar si responden a los controles preestablecidos. Un ejemplo podría ser observar un determinado circuito de procesamiento de datos con el propósito de determinar si los discos están debidamente protegidos y los programadores no operan desde el computador en producción. Del mismo modo, otro caso sería observar si la persona que maneja los fondos en efectivo tiene vedado el acceso a los registros contables. Asimismo, también es válida para verificar la existencia de ciertos activos como efectivo, valores, bienes de cambio y/o de uso.

Otra forma de observación son las denominadas “pruebas circulares”. Éstas consisten en una revisión de la disposición efectiva de los controles de la empresa en un determinado momento con el propósito de ratificar el relevamiento efectuado por el auditor. A tal efecto, debe tomar en cada subsistema de la empresa, cuatro o cinco operaciones y seguir el movimiento de la documentación a través de todo el sistema. Por ejemplo, en el subsistema de

ventas, toma la nota de pedido, el remito y la factura y verifica las autorizaciones, controles, el débito de la cuenta del cliente, el registro en libros principales. Es decir, todas las operaciones que dan lugar a esos comprobantes. Del mismo modo procede con las compras, ingresos, egresos, almacenes, sueldos y jornales, u otros que desee verificar (FACPCE-CECYT, 2004).

Cuatro o cinco operaciones en cada área son suficientes para este tipo de “pruebas circulares”. El objetivo de las mismas no tiende a medir el funcionamiento de las actividades de control durante todo el ejercicio examinado, sino que simplemente apuntan a confirmar el conocimiento del sistema. De esta forma el auditor releva y evalúa preliminarmente los controles, y está en condiciones de comprobar su funcionamiento durante todo el período objeto del examen (FACPCE-CECYT, 2004).

Este tipo de prueba pone en evidencia la asiduidad o frecuencia de los errores producidos por la falta o insuficiencia de controles.

Por lo expresado, la observación puede ser tanto parte de una prueba de cumplimiento de controles como de una prueba sustantiva.

Prueba de transacciones o de Cumplimiento

Las pruebas de transacciones son pruebas detalladas de operaciones y de los comprobantes a que dan origen esas operaciones y tienen dos propósitos. Por un lado, tienden a verificar la efectividad de los controles de los sistemas, y por otro, dan información al auditor para corroborar los saldos de los estados contables (FACPCE-CECYT, 2004).

Estas pruebas comprenden la aplicación de procedimientos de auditoría al registro contable de las operaciones. Se selecciona una muestra de operaciones, por ejemplo compras, y el auditor verifica para cada una de ellas el respaldo documental pertinente. Entre el respaldo se observa la nota de pedido, cotizaciones, orden de compra, remitos del proveedor, nota de recepción, factura del proveedor. Todos ellos a través de procedimientos de auditoría tales como recómputo, comprobación de cotejo, etc. y la adecuada imputación y registro contable de la transacción (FACPCE-CECYT, 2004).

Pruebas directas de saldos contables

El saldo de muchas de las cuentas de los estados contables, es comprobado verificando selectivamente la razonabilidad de los saldos individuales que la componen (FACPCE-CECYT, 2004).

Ello se produce a través de la aplicación de procedimientos de auditoría tales como confirmación, inspección ocular, recálculo. Estos procedimientos se aplican a las cuentas por cobrar y pagar, existencias de bienes de cambio, cuentas bancarias, obligaciones por pagar, y restantes grupos de cuentas (FACPCE-CECYT, 2004).

Constituyen pruebas sustantivas toda vez que tienden primariamente a comprobar la razonabilidad de los importes registrados.

Sin embargo, cuando a través de esos procedimientos se detecta un error en un saldo, existe evidencia de que un cierto control operó ineficientemente o decididamente no existió. Esto hace que el auditor investigue las causas del error y detecte la falla, configurándose, entonces, también una prueba de cumplimiento (FACPCE-CECYT, 2004).

Pruebas de incremento y disminuciones de los saldos contables

Otro modo de revisar el saldo de una cuenta, es a través de la verificación de las partidas debitadas y acreditadas con la documentación de base. Generalmente, este procedimiento se aplica a cuentas que no tienen un número muy significativo de transacciones tales como cuentas de bienes de uso, activos intangibles, gastos anticipados y similares (FACPCE-CECYT, 2004).

Estas pruebas son similares a las pruebas de transacciones en cuanto que la evidencia es la misma aunque su objeto es distinto. En efecto, éstas tienden a verificar, básicamente, el saldo de una cuenta, en tanto que las pruebas de transacciones se proponen primariamente evaluar los sistemas de control (FACPCE-CECYT, 2004).

El auditor debe seleccionar, del conjunto de pruebas detalladas precedentemente, aquella o aquellas que estime conveniente. Está claro que, a mayor número de pruebas utilizadas, mayor será verificación y validación que obtiene como resultado. Sin embargo si la cantidad de pruebas es demasiado excesiva, requiere mayor tiempo, lo que se traduce en un mayor costo.

Cuellar M. (2009) empieza a acercarse a la solución cuando dice que la mayoría de las entidades, incluyendo pequeñas compañías o unidades de empresas más grandes, utilizan computadoras para el procesamiento de información. Se trata de sistemas de información que incluyen elementos tanto manuales como computarizados. Para aquellos que son estrictamente manuales, pueden aplicarse diferentes controles; tales controles a pesar de ser diferentes, estarían basados en los mismos conceptos subyacentes de control.

Los controles que Cuellar M. (2009) plantea que pueden usarse, se dividen en dos grandes grupos. El primero comprende los controles generales, los que se aplican a muchos sino a todos los sistemas de aplicación, y que ayudan a asegurar su operación continua y apropiada. La segunda categoría comprende los controles de aplicación, que incluyen los pasos computarizados dentro del programa de la aplicación y los procedimientos manuales relacionados para controlar el procesamiento de diversos tipos de transacciones. En conjunto estos controles sirven para asegurar la integridad, exactitud y validez de la información contable y de otra índole dentro del sistema (Cuellar M., 2009).

Un aspecto no menos válido es el tamaño de la empresa cuyos estados contables son objeto de auditoría, ya que el mismo influye en la elección de un determinado enfoque. Por lo general, mientras más grande y compleja sea la entidad, resulta probablemente más eficiente aplicar una estrategia de confianza en controles en lugar de usar una estrategia que comprenda únicamente pruebas sustantivas. Para entidades más pequeñas, y especialmente para negocios administrados por su propietario, es menos probable que se adopte una estrategia de confianza en controles debido a que con frecuencia solamente hay un pequeño número de actividades de control en las que el auditor puede confiar (Nannini, y otros, 2011).

Las posibilidades de declaración incorrecta en las afirmaciones, observaciones o declaraciones de los estados financieros, se analizan mediante la consideración específica del riesgo inherente, riesgo de control y riesgo de detección. En base a la consideración que el auditor haga de estos factores de riesgo, establece su estrategia de auditoría y el alcance de las pruebas que realiza para lograr el grado de seguridad deseado. Es decir, en base a las afirmaciones de los estados financieros y considerando los ciclos de negocios se establecen

los objetivos generales y específicos de cada tipo de operación y del saldo final en la cuenta relacionada (Nannini, y otros, 2011).

De los análisis precedentes se concluye que el auditor tiene dos opciones al momento de encarar un trabajo de auditoría. Puede enfocarse en la revisión de los controles internos, para lo cual aplica los procedimientos y pruebas específicos, y luego descansa en los mismos. O también puede aplicar pruebas sustantivas a toda aquella información que crea conveniente verificar. Finalmente tiene la posibilidad de aplicar una combinación entre ambas opciones. Cualquiera de los caminos que elija debe lograr la combinación adecuada entre pruebas de cumplimiento y pruebas de validación o sustantivas a fin de obtener evidencias de auditoría en el menor tiempo.

CONCLUSIONES

- La adopción de nuevas tecnologías para el procesamiento de datos ha producido un cambio en la auditoría tradicional. No en el objetivo que la misma tiene, el cual es recolectar los elementos de juicio válidos y suficientes para emitir un dictamen sobre la veracidad de la información contenida en los estados contables. Sino más bien, en el enfoque que debe darle a su tarea profesional basándolo principalmente en depositar confianza en los controles internos que se están aplicando.
- Es altamente recomendable la utilización de técnicas de auditoría adaptadas a entornos informáticos para lograr un trabajo eficiente y eficaz. La falta de consideración de las mismas pueden, incluso, llegar a imposibilitar la formación de una opinión del profesional respecto de la información contenida en los estados contables.
- El informe COSO constituye una importante herramienta de la cual puede disponer el auditor. Le permite realizar un relevamiento del control interno de una entidad y observar si un control específico previene o detecta y corrige errores significativos. Las posibles desviaciones que el control interno no resuelva son los que representan el mayor riesgo. La mirada del auditor debe enfocarse hacia estas cuestiones en las que no están dadas las garantías de certeza, veracidad e integridad; puesto que son las características que debe reunir la información contable.
- El auditor tiene dos opciones al momento de encarar un trabajo de auditoría. Puede enfocarse en la revisión de los controles internos, para lo cual aplica los procedimientos y pruebas específicos, depositando confianza en los mismos. O también puede aplicar pruebas sustantivas a toda aquella información que crea conveniente verificar. Finalmente

tiene la posibilidad de aplicar una combinación entre ambas opciones. Cualquiera de los caminos que elija debe lograr la combinación adecuada entre pruebas de cumplimiento y pruebas de validación o sustantivas a fin de obtener evidencias de auditoría en el menor tiempo.

BIBLIOGRAFÍA

- Arens, A. A., y Loebbecke, J. K. (1996). *Auditoría: Un enfoque integral* (11ª ed.). Prentice Hall.
- Astiz Fernández, F. J., y Sole Bardia, M. (2008). La Auditoría de Cuentas Anuales en Entornos Informátizados. *Partida Doble* (202), 70-81.
- Comité Internacional de Prácticas de Auditoría (International Auditing and Assurance Standards Board - IAASB). (2009). Normas Internacionales de Auditoría. *NIA 315 Identificación y Evaluación de los Riesgos de Error*.
- Barreira Sans, J. (1980). La Auditoría Interna. *Revista Española de Financiación y Contabilidad*, Vol IX N°31, 139-150.
- Casal, A. M. (2009). *Tratado de informes de auditoría, revisión, otros aseguramientos* (1ª ed.). Buenos Aires: Errepar.
- Castello, R. J. (2008). *Auditoría de Sistemas y Tecnologías de Información*. (3ª ed.) Córdoba: ACFCE.
- Coopers & Lybrand (1997). *Los Nuevos Conceptos del Control Interno (Informe COSO)*. España: Ed. Díaz Santos.
- Cuellar M., G. A. (2009). *Informe Ejecutivo COSO*. México: Universidad del Cauca Facultad de Ciencias Contables, Económicas y Administrativas.
- FACPCE - CECYT. (2004). *Informe N° 5 Manual de Auditoría*. Avellaneda.

FACPCE. (2013). Resolución Técnica N° 37. *Normas de auditoría, revisión, otros encargos de aseguramiento y servicios relacionados*. Santa Fe, Argentina.

Instituto Americano de Contadores Públicos Certificados (American Institute of Certified Public Accountants). (1997). Auditing procedure study. *Evidential matter in the electronic environment*.

López, M. D., Albanese, D. E., y Durán, R. (2013). Auditoría Financiera en Entornos de Computación en la Nube: Revisión del Estado del Arte. *Escritos Contables y de Administración*, vol 4 N° 1, 109 a 147.

Malica, D. O., y Abdelnur, G. D. (2012). Trabajo de investigación. *El sistema de control interno y su importancia en auditoría*. Argentina: FACPCE-CECYT - Área Auditoría.

Mancuso, A. (1997). Auditing Standard Board issues SAS No. 80. *The CPA Journal*, vol 67, p.74.

Nannini, M. S., Español, G., González, S., Giménez, M., Puyó, V., Padovan, A., y otros. (2011). Trabajo de investigación. *El enfoque de riesgo de la auditoría*. Rosario, Santa Fe, Argentina: Instituto de Investigaciones Teóricas y Aplicadas, Escuela de Contabilidad.

Pérez Gomez, J. M. (1987). Auditoría Informática de las Organizaciones. *Centro Regional del IBI para la Enseñanza de la Informática*. Madrid, España.

Rezaee, Z. y Reinstein, A. (1998). The impact of emerging information technology on auditing. *Managerial Auditing Journal*, Vol. 13 N° 8, 465-471.

Yann, D. (1994). Técnicas de la auditoría informática. España: Marcombo.