UNIVERSIDAD DE LA REPÚBLICA

ORIENTAL DEL URUGUAY

Facultad de Ciencias Económicas y de Administración

♦ Enfoque de la Auditoría de Estados Contables en entornos computarizados.

♦ Alcance específico de procedimientos a aplicar sobre controles generales y de aplicación según las circunstancias de la empresa auditada.

♦ Situación en la cual existen controles generales inefectivos.

♦ Posibilidad de rotación de controles en auditorías recurrentes.

Cátedra: *Auditoría*
Tutor: *Cr. Claudio Muzi*

Integrantes:
Soledad Bazzino
Sandra Lemes
Silvana Olivieri

Trabajo de Investigación Monográfico presentado para la obtención del título de Contador Público

Agosto, 2010

"El trabajo monográfico presentado y las opiniones vertidas en él son de responsabilidad de los autores.
El coordinador / tutor ha cumplido un rol de orientación del grupo de estudiantes en aspectos metodológicos y académicos generales, sin que esa actuación implique compartir en todo o en parte el contenido final de la investigación desarrollada".

Agradecimientos:

A todos nuestros familiares y amigos que nos acompañaron e incentivaron a lo largo de nuestra carrera.

A nuestro tutor Cr. Claudio Muzi

A los profesionales que dedicaron su tiempo para las entrevistas:

Ing. Pablo Romero, PMP, CISA, CISM
Ing. Jose Luis Mauro Vera, CISA, CobiT-FC
Ing. Fernando Richly, CISA, CISM
Cra. María A. Marmolejo

ÍNDICE

Abstract

El objetivo de la presente monografía consiste en realizar una investigación en el área de auditoría de estados contables en entornos computarizados, con el objetivo de extraer conclusiones sobre distintos aspectos de la misma, tales como enfoque, alcance de procedimientos a aplicar sobre controles generales y de aplicación, situaciones en las cuales puedan existir controles generales inefectivos y rotación de controles en auditorías recurrentes. Dada la complejidad del entorno surge como tema fundamental la figura del experto en sistemas, en quien debe apoyarse el auditor para poder realizar la auditoría en este tipo de entornos.

Para llevar a cabo nuestro trabajo, realizamos una primera aproximación al tema a través del análisis de la información recabada en lo que refiere a normas de auditoría y más específicamente en lo que respecta a auditorías en entornos computarizados. Luego de avanzar en los conceptos teóricos, realizamos una serie de entrevistas a expertos en sistemas, contactándonos con gerentes del departamento de tecnología de la información, pertenecientes a tres reconocidas firmas internacionales de auditoría que actúan en el mercado local.

De esta forma presentamos nuestro trabajo dividido en distintas secciones, donde partimos del capítulo 1 que consta de una breve introducción, para luego pasar a desarrollar un marco teórico en los capítulos 2, 3 y 4 y a partir del capítulo 5 introducir la presentación de la información recabada en las entrevistas y de esta forma llegar al final del trabajo en el capítulo 8 a desarrollar las conclusiones a las que arribamos con la investigación realizada.

Capítulo 1

1 - INTRODUCCIÓN

1.1 - Conceptualización de entornos computarizados

La siguiente frase: "***hoy en día la información es uno de los activos más valiosos de las organizaciones***", es repetida con mucha frecuencia. Esto se debe al gran desarrollo de los sistemas informáticos, que con la diversidad y gran avance de la Tecnología de la Información (TI) en el entorno actual, la operativa de cualquier empresa depende cada vez más del buen funcionamiento de sus sistemas así como de su relacionamiento con el medio en que interactúa.

Desde hace unos años el entorno que rodea a las organizaciones se caracteriza por el ritmo acelerado del cambio continuo y por el proceso de globalización de los mercados. El cambio constante ha hecho que las organizaciones se tengan que adaptar a las nuevas situaciones reaccionando con rapidez a las exigencias de dicho entorno. El proceso de globalización obliga a las empresas ha estar continuamente actualizadas con respecto a las nuevas tecnologías de información.

Daniel Bell, en su libro *Hacia una Sociedad Postindustrial* nos dice:

> "***El punto crucial de toda sociedad postindustrial lo constituye el hecho de que el conocimiento y la información llegan a convertirse en recursos estratégicos***

> ***y transformadores de esa sociedad, igual que el capital y el trabajo lo han sido en la sociedad industrial***." [1]

Las computadoras han facilitado la recopilación, ordenamiento y almacenamiento de la información, grandes cantidades de documentos pueden ser fácilmente digitalizados y almacenados en espacios muy pequeños. Esta utilidad no solo se limita al manejo de datos, también sirve de soporte para la realización de las distintas tareas dentro de la organización. En el área contable y administrativa para llevar a cabo casi la totalidad de las tareas se requiere el uso de algún software.

Si un sistema informático no está bien diseñado puede llevar a errores que ocasionen peligrosos daños en la operativa normal de cualquier empresa, dado que el software elegido realiza los procesos que han sido configurados por el programador. Los controles sobre el funcionamiento del software utilizado, son fundamentales para asegurar que las decisiones tomadas por los directivos a partir de la información procesada, no se desvíen de los objetivos de la organización. El auditor deberá evaluar si esos controles se realizan y si funcionan de manera correcta.

> ***"El nivel técnico del auditor es a veces insuficiente, dada la gran complejidad de los sistemas, unido a los plazos demasiados breves de los que a menudo dispone para realizar su tarea…"*** [2]

El auditor de estados contables deberá hacer el relevamiento del sistema informático en su conjunto y así determinará si se ve obligado a recurrir al apoyo de especialistas en esta área, dependiendo tanto del tamaño de la empresa como

[1] BELL, Daniel, *La revolución tecnológica de las comunicaciones y sus consecuencias*, Harvard-Deusto Business Review, primer trimestre de 1981, p.38.
[2] ACHA ITURMENDI, J. José, Auditoría Informática en la empresa, Edit. Paraninfo SA, Año 1994, p.15.

de los sistemas utilizados, en el caso de sistemas complejos será necesaria siempre la intervención del experto para que realice la evaluación de los controles correspondientes.

> ***"Entorno de sistemas de información por computadora (SIC) - Existe cuando la entidad utiliza una computadora de cualquier tipo o tamaño en el procesamiento de información financiera de importancia para la auditoría, ya sea que esa computadora sea operada por la entidad o por un tercero".*** [3]

Actualmente la gran mayoría de las empresas operan en entornos computarizados, ya sea empresas pequeñas que optan por desarrollar sistemas informáticos por razones de rapidez, comodidad, o las grandes empresas en las cuales es impensable que puedan registrar sus operaciones si no fuera por complejos sistemas informáticos.

> *"**Entorno de TI – Las políticas y los procedimientos que implementa la entidad y la infraestructura de TI (hardware, sistemas operativos, etc.) y el software de aplicación que utiliza como soporte de las operaciones comerciales y el logro de estrategias comerciales."*** [4]

El auditor debe conocer en forma suficiente el hardware y los sistemas de procesamiento para planificar el trabajo y comprender de qué manera afectan al estudio y a la evaluación del control interno y la aplicación de los procedimientos de auditoría, incluyendo técnicas asistidas por computadora.

[3] IFAC, *Normas Internacionales de Auditoría*, Glosario de términos de Auditoría, Edit .Papel Tinta, Año 2009, p.37.
[4] IFAC, Ob. Cit., p.37.

Las empresas no sólo dependen de sus propios sistemas informáticos, sino también de los sistemas que les brinda su medio tanto del sector público o privado. De esta forma la organización queda inmersa en un entono computarizado y dependiendo de las características de la misma podemos hablar de que esa dependencia podrá ser en menor o mayor grado.

1.2 - Breve reseña de la evolución de la contabilidad tradicional en las organizaciones hacia los sistemas complejos actuales

En el pasado, antes del desarrollo de las computadoras, las organizaciones registraban sus operaciones manualmente, esto implicaba una mayor cantidad de horas y esfuerzo dedicados a la tarea contable. Las registraciones contables se realizaban manualmente en libros, que ocupaban demasiado espacio y requerían mucho costo de personal para mantenerlos actualizados. Actualmente este trabajo se puede realizar en menos tiempo a través de complejos sistemas informáticos que sólo requieren una simple capacitación de los usuarios, de esta forma se han minimizado costos. Pero todo este avance en el área de tecnología de la información también acarrea nuevos problemas, la seguridad de la información es uno de ellos, por lo tanto han surgido nuevos riesgos que deberá evaluar el auditor para planificar los distintos procedimientos a llevar a cabo.

Con la aparición del computador, las grandes empresas comenzaron a utilizar estos recursos para reducir esfuerzos, ser más eficientes y tener la información con la oportunidad requerida.

Muchas son las razones que han llevado a la empresa a depender cada vez más de sus sistemas informáticos, los cuales se componen de hardware y software computacional, redes de telecomunicaciones, técnicas de administración de bases de datos computarizadas y otras formas de tecnología de información. Algunas de esas razones son:

- Rapidez en el ingreso de datos, por ejemplo lectores de barra en supermercados, los cuales generan asientos en la contabilidad.
- Posibilidad de procesar rápidamente grandes volúmenes de datos y almacenarlos de manera compacta.
- Posibilidad de ingresar datos en tiempo real y en forma remota a través de redes incluyendo vía Internet.
- Acceso a la información simultáneamente por distintos usuarios, como proveedores, clientes, etc., adecuándose a las exigencias del mercado en el que opera.
- Contar con la información en forma rápida y oportuna para la toma de decisiones de la empresa.
- Para ser más eficientes reduciendo esfuerzos innecesarios, tiempo, recursos y errores (mayor confiabilidad).
- Aumento de la capacidad del hardware, disminución de sus costos y gran desarrollo del software.
- Aumento de la comunicación de la empresa con su entorno (vía e-mail, intercambio electrónico de datos y sistema de transferencia electrónica de fondos).

La primera computadora comercial fabricada en Estados Unidos fue: UNIVAC I (*Computadora Automática Universal I*), desde entonces, varias generaciones de computadoras se han desarrollado. Cada generación representó un paso que fue

caracterizado por el hardware del tamaño disminuido y de capacidades crecientes.[5]

Los sistemas de procesamiento electrónico de datos (PED) sustituyeron los tradicionales procedimientos manuales por otros basados en computadora. La mayoría de las organizaciones comenzaron a utilizar el PED por lo menos hasta cierto punto, para procesar la información financiera y contable.

Dada la necesidad de información de las organizaciones actuales en ambientes globalizados, surgen sistemas de información cada vez más complejos para responder a esas necesidades y así poder alcanzar las metas y objetivos. Actualmente se dejó de hablar del PED para comenzar a referirse al concepto de Tecnología de la Información (TI), porque éste abarca un campo más amplio (básicamente informática y telecomunicaciones).

Las organizaciones trabajan con sistemas de información que pueden ser paquetes adquiridos o hechos a medida, o una combinación de los mismos. En el mercado puede encontrarse gran variedad de paquetes estándar que son fácilmente aplicables a diferentes tipos de actividad, o por el contrario la empresa puede optar por la utilización de software específicamente diseñado para su operativa.

En consecuencia el uso de las computadoras ya no está limitado a las grandes empresas, sino que las organizaciones cualquiera sea su tamaño y su rubro, tienen a su alcance el uso de tecnología de la información para el apoyo en su gestión.

[5] Fuente: Pág. Web: *http://es.wikipedia.org*

Capítulo 2

2 - COMPLEJIDAD DE LOS SISTEMAS DE PROCESAMIENTO ELECTRÓNICO DE DATOS Y SU IMPACTO EN LA AUDITORÍA DE ESTADOS CONTABLES

2.1 - Conceptos previos

2.1.1 - Normas de auditoría generalmente aceptadas (NAGA)

Establecen un marco de referencia para la actividad de auditoría. Contemplan diferentes aspectos referidos a la persona del auditor, al trabajo que realiza y al informe que emite. A nivel global se reconocen como pautas las Normas Internacionales de Auditoría (NIAs) emitidas por la Federación Internacional de Contadores (IFAC), a nivel de cada país pueden existir otras normas locales.

2.1.2 - Normas internacionales de auditoría (NIAs):

Contienen principios básicos y procedimientos esenciales que debe seguir o aplicar el profesional que se dedique a trabajos de auditoria de estados financieros. Las NIAs pretenden su aceptación y aplicación mundial, sin embargo no prevalecen sobre las reglamentaciones locales que rigen la auditoría de

información financiera en cada país. En Uruguay existen los lineamientos fijados por el Colegio de Contadores, Economistas y Administradores del Uruguay a través de sus pronunciamientos técnicos, en el pronunciamiento Nº 13 se declara de aplicación obligatoria las normas internacionales de auditoría – servicios relacionados y las declaraciones internacionales para la práctica de auditoría, salvo algunas excepciones. [6]

2.1.3 - Estados contables (EECC)

Son informes escritos utilizados por la empresa para suministrarle a terceros ajenos a la misma, información del patrimonio y su evolución en el tiempo. Deben proporcionar una serie de información básica para que los terceros puedan utilizarlos para evaluar la gestión de la empresa, evaluar su rentabilidad (ya sea con fines de inversión, otorgar créditos, cobrar impuestos, etc.).

2.1.4 - Auditoría de estados contables

> ***"La auditoría de estados contables es el examen de éstos por parte de un profesional independiente con el propósito de dictaminar si fueron preparados de acuerdo con ciertas normas contables (NC)"*** [7]

El trabajo del auditor es un examen objetivo, libre de opiniones personales. El producto final de la auditoría es un informe que va a aumentar el grado de confiabilidad de los EECC, ya que en él se establecerá que los mismos están preparados respecto de todo lo sustancial de acuerdo con un marco de referencia,

[6] Colegio de Contadores Economistas y Administradores del Uruguay, Pronunciamiento Nº 13, *Normas de Auditoría Generalmente Aceptadas en el Uruguay.* Vigencia julio 2000.
[7] FOWLER NEWTON, Enrique, *Auditoría* Aplicada, Tomo I, Ediciones Macchi, Año 1997, p.3.

permitiendo que los usuarios sean más eficientes a la hora de tomar decisiones. En nuestro país, el marco normativo de referencia son las normas contables adecuadas (NCA).

La auditoría es un proceso dentro del cual se distinguen tres etapas:

- **Planeamiento:** en esta etapa básicamente debe realizarse un conocimiento del negocio, una revisión analítica preliminar, una evaluación del control interno y de los riesgos de auditoría. El auditor elaborará los programas de trabajo en los cuales establecerá los procedimientos que realizará en la siguiente etapa.
- **Ejecución:** donde se realizarán los procedimientos que fueron previamente establecidos en los programas de trabajo y se obtendrán las evidencias que respalden el trabajo del auditor.
- **Conclusión:** se realizarán las tareas finales y la elaboración del informe. [8]

De acuerdo con lo establecido en las NIAs, el proceso de auditoría también incluye otras actividades que se llevan a cabo durante todo el desarrollo del trabajo, por ejemplo la supervisión del equipo de colaboradores y el control de calidad del trabajo realizado.

2.1.4.1 - Requisitos éticos para auditar estados financieros

> ***"Los requisitos éticos relacionados con los compromisos de auditoría normalmente comprenden las partes A y B del Código IFAC y los requisitos nacionales más estrictos.***

[8] Fuente: GUBBA H. y otros, *Auditoría: Guía para su planificación y ejecución*, Edit. Central de Impresiones, Año 2007, p. 27 y sgtes.

El Código IFAC establece los principios fundamentales de la ética profesional que incluyen los siguientes:

a) Integridad;
b) Objetividad;
c) Capacidad profesional y diligencia debida;
d) Confidencialidad; y
e) Conducta profesional." [9]

La parte B del código IFAC incluye un enfoque conceptual acerca de la independencia del profesional.

En Uruguay el requisito de capacidad profesional comprende que el auditor debe poseer el título de contador público (o equivalente).

2.1.4.2 - Obligación de ciertas entidades a presentar estados contables auditados

- Fiscalmente en Uruguay para la presentación de EECC se exige un informe de auditoría sólo para el grupo grandes contribuyentes y un informe de revisión limitada para los contribuyentes de CEDE, esto último sólo si el activo contable es superior a 6.000 UR. El informe de revisión limitada es de menor alcance que el informe de auditoría, está regulado en Uruguay por el pronunciamiento Nº 5 del Colegio de Contadores, Economistas y Administradores del Uruguay.[10]

[9] IFAC, Ob. Cit., NIA 220, p.127.
[10] DGI, Resolución 1093/005 y modificaciones 480/009.

- Para presentar EECC ante el sistema financiero uruguayo existe una disposición del Banco Central del Uruguay que determina el tipo de informe que acompañará a dichos estados, esto dependerá del endeudamiento de la empresa con respecto a la responsabilidad patrimonial básica para bancos (RPBB), cuyo valor es fijado en forma trimestral por el BCU, el monto de la RPBB corresponde al valor de 130.000.000 de unidades indexadas,[11] (valor actual aproximado en dólares americanos: U$S 13.000.000).

  Si el endeudamiento de la empresa es:

  a) Inferior al 5% del valor de la RPBB, los EECC deberán ir acompañados con un informe de compilación el que deberá realizarse conforme a lo establecido en el pronunciamiento Nº 7 del Colegio de Contadores, Economistas y Administradores del Uruguay.

  b) Igual o superior al 5% de la RPBB, los EECC deberán ir acompañados con un informe de revisión limitada, realizado por un profesional independiente y conforme a lo establecido en el pronunciamiento Nº 5 del Colegio de Contadores, Economistas y Administradores del Uruguay. Según dicho pronunciamiento el profesional no tiene el requisito de la independencia, lo cual difiere con la normativa internacional, pues en la norma 2400 del IFAC se habla del carácter de independencia que tiene que tener el profesional para realizar la revisión limitada, pero en este caso en particular la circular del BCU habla de profesional independiente. [12]

  c) Igual o superior al 15% de la RPBB, los EECC deberán ir acompañados con un informe de auditoría emitido por

[11] BCU, Circular Nº 1938 de fecha 30/08/2005.
[12] IFAC, Ob. Cit., NICR 2400, p.781.

profesionales independientes y de acuerdo a las normas de auditoría generalmente aceptadas. [13]

2.1.5 - Tecnología de la información (TI)

Según lo definido por la asociación de la Tecnología de información de América (ITAA) es:

> *"**el estudio, diseño, desarrollo, implementación, soporte o dirección de los sistemas de información computarizados, en particular de software de aplicación y hardware de computadoras."*** [14]

La TI es un término general que describe cualquier tecnología que ayuda a producir, manipular, almacenar, comunicar, y/o esparcir información. Los profesionales de TI realizan una variedad de tareas que van desde instalar aplicaciones a diseñar complejas redes de computación y bases de datos. Algunas de las tareas incluyen administración de datos, redes, ingeniería de hardware, diseño de programas y bases de datos, así como la administración y dirección de los sistemas completos.

2.1.5.1 – ISACA

Surgió por la necesidad de los auditores que vieron que los controles de auditoría en los sistemas computarizados se estaban haciendo cada vez más críticos para las operaciones de sus organizaciones respectivas. ISACA es una organización

[13] BCU, Circular 1879 del 2/10/03.
[14] Fuente Pág. Web: *http://es.wikipedia.org*

global que desarrolla estándares internacionales de auditoría y control de sistemas de información, que son marcos referenciales, por ejemplo COBIT.[15]

2.1.5.2 - COBIT (Objetivos de control para la información y tecnologías relacionadas)

Es una guía que sirve de apoyo a los auditores para respaldar sus evaluaciones y opiniones sobre el diseño y funcionamiento de los controles internos y de los sistemas de información. COBIT cita expresamente su compatibilidad con el informe COSO. En Uruguay el BCU establece que el sistema de gestión a adoptar por las áreas de tecnología informática de las instituciones de intermediación financiera, deben considerar como guía los principios establecidos en el marco de referencia COBIT.[16]

2.1.5.3 - Auditoría en ambientes de TI

Esta expresión hace referencia a los desafíos que la TI plantea al auditor, a los potenciales riesgos de control que introduce y a las medidas de control que pueden mitigarlo, así como a los posibles usos de técnicas de auditoría apoyadas en computadora (TAAC).[17]

[15] ISACA, Pág. Web*: www.isaca.org*
[16] BCU, Comunicación 2003/179. (12.09.03), *Requisitos para la Administración de las Áreas de Tecnología Informática.*
[17] Fuente: GUBBA H. y otros, Ob. Cit., p.396.

2.2 - Cómo impacta el entorno computarizado en la auditoría de los estados contables

A medida que las empresas se fueron informatizando cada vez más y fueron automatizando la mayoría de sus procesos, los auditores comenzaron a preocuparse por los avances de la TI, ya que todos estos cambios ocurrían a gran velocidad y su utilización se expandía rápidamente a gran cantidad de empresas. Los auditores vieron en esta tecnología oportunidades de mejora y comenzaron a asistir su trabajo con el uso de computadoras, pero también estaba la preocupación de adaptarse para hacer frente a los nuevos riesgos que estaban surgiendo con el uso de esta nueva tecnología.

2.2.1 – Efectos de la informatización de los procesos en las organizaciones

Los autores Arens y Loebbecke, describen los efectos de los avances del procesamiento electrónico de datos sobre las organizaciones y los resumen en tres grandes grupos: cambios organizacionales, la visibilidad de la información y el potencial de comisión de errores.

2.2.1.1 – Cambios organizacionales

Instalaciones:

Para las empresas que utilizan minicomputadoras o microcomputadoras no hubo grandes cambios en sus instalaciones, ya que éstos son operados en un ambiente normal de oficina. Pero con respecto a las grandes entidades que usan sistemas complejos, donde el hardware tiene gran tamaño, sus grandes equipos necesitan

de un ambiente de computación especial, con controles especiales (temperatura, humedad, protección contra incendios, dispositivos de cierre de puertas, etc.)

Personal:

Cuando la entidad utiliza pequeños sistemas generalmente adquiere el software y el hardware conjuntamente y no requiere de profesionales ó técnicos para operar los programas, sólo una cierta capacitación para su personal normal. Mientras que en un sistema a gran escala, a menudo las funciones requieren de programadores, operadores, empleados para el control de datos y jefes de departamento informático.

Centralización de datos y separación de responsabilidades

El alto uso de la tecnología informática en una organización, por lo general hace que se integren las actividades de recopilación y acumulación de datos de diferentes partes de la organización en un sólo departamento. Esto tiene la ventaja de centralizar datos y realizar controles de mayor calidad, pero por otro lado tiene como desventaja la eliminación de controles, que antes proporcionaba la división de responsabilidades de personas independientes, que realizaban funciones relacionadas y luego comparaban sus resultados. En sistemas complejos los empleados pueden capturar pedidos de los clientes con el uso de teclados desde sitios remotos, de esta forma las facturas de ventas, el diario de ventas y el archivo de cuentas por cobrar se preparan o actualizan al mismo tiempo, por lo tanto tenemos la ventaja de la reducción de errores al reducirse el registro de los datos, pero a su vez cuando se produce un error de registro, éste se produce en muchas partes. Esta centralización de datos en sistemas complejos hace cambiar la custodia de conservación de registros, ahora se le asigna esta responsabilidad al departamento informático.

2.2.1.2 – Visibilidad de la información

Cuando los sistemas no son complejos existen documentos en apoyo de cada transacción y la mayor parte de los resultados del procesamiento se imprimen. Entonces pueden hacerse visibles las entradas, salidas y también parte del procesamiento, pero cuando los volúmenes de datos son mayores en sistemas complejos dejan de ser visibles para el usuario o para el auditor.

Visibilidad de los datos de entrada

Cuando las transacciones son capturadas directamente en la computadora por diversas terminales, los datos que se ingresan al sistema no son visibles para el auditor. Los mismos están en forma legible para la máquina, accesible para la computadora, lo que exige que el auditor tenga que dar pasos especiales para recuperarlos.

Visibilidad de procesamiento

Algunas transacciones se inician con un programa y se procesan sin evidencia visible. Los procesos de computación más importantes son internos y no son directamente observables.

Visibilidad del rastro de la transacción

Al ingresar un dato a sistemas de módulos integrados se pueden obtener diferentes informes con índices, estadísticos y la información puede utilizarse desde los distintos módulos que han procesado esos datos. Debido a esta integración de funciones, los informes se obtienen mediante una computadora sin que exista un rastro visible de la transacción que pueda relacionarse con las que fueron ejecutadas individualmente. Es importante que las compañías conserven algún rastro de las transacciones para tener una buena administración, atención al cliente y una auditoría efectiva.

2.2.1.3 – Potencial para la comisión de errores importantes

Como consecuencia del alto uso de sistemas complejos en las entidades, tenemos la aparición de nuevos riesgos, encontramos factores que incrementan la probabilidad de cometer errores importantes en los estados financieros.

Reducción de la participación humana

En procesos manuales o de sistemas no complejos, el personal ingresa datos y observa los resultados de forma que pueda detectar errores oportunamente, mientras que en sistemas complejos, las personas que intervienen en el inicio de la transacción nunca ven los resultados finales. Esto permite que los errores fluyan a través del ciclo y del sistema de contabilidad y de esta forma pueden permanecer sin ser detectados hasta los estados financieros.

Uniformidad de procesamiento

Esta es una característica de los sistemas informáticos, de tal forma que los datos ingresados se procesan consistentemente con la información anterior y la posterior, por lo tanto el sistema va a procesar un tipo dado de transacción de manera correcta o incorrecta, pero consistente. En consecuencia de esto, cuando el sistema no está diseñado para reconocer transacciones poco usuales, que requieren un manejo especial y es inadecuado el rastreo de la transacción, el auditor deberá poner énfasis a la comprobación de estas transacciones y a los cambios realizados en el sistema en el curso del tiempo, más que en la comprobación de una muestra grande de transacciones similares.

Acceso no autorizado

El alto grado de procesamiento electrónico de las transacciones ha introducido riesgos de errores potenciales en los estados financieros y riesgo de fraude, éstos surgen cuando los sistemas permiten un fácil acceso y uso de los datos, por

ejemplo si no existen los controles necesarios que eviten realizar una transacción no autorizada, cambiar programas, registros y obtener información confidencial.

Pérdida de datos

La gran dependencia de los sistemas informáticos y la centralización de los datos, hace imprescindible contar con la seguridad física adecuada, no sólo respaldos sino también tener cubierto el riesgo de la rotura de un equipo o falla física, de tal forma que el reemplazo no retrase las operaciones normales de la empresa.

Estos cambios, entre otros, han llevado al auditor ha modificar su forma de trabajo, surgiendo así la necesidad de verificar el funcionamiento de los sistemas informáticos de la empresa y del control interno ya que con respecto a éste ahora deberá chequear nuevas formas de seguridad: accesos, claves, cantidad de usuarios, restricciones, niveles de autorización, etc. Un sistema puede no producir un rastro visible de auditoría que nos proporcione certeza sobre la totalidad y exactitud de las transacciones procesadas, aparecen entonces nuevas formas de recopilación de evidencias de auditoría. [18]

Los nuevos riesgos que se introducen con el uso de sistemas cada vez más complejos, pueden ser minimizados con los controles adecuados, de esta forma las ventajas que ha proporcionado la TI han beneficiado enormemente a las entidades.

[18] Fuente: ARENS, Alvin A. y LOEBBECKE, James K., *Auditoría un enfoque integral,* 6ª Edición, Editorial Prentice Hall, p.569 y sgtes.

2.2.2 – Formas en que el auditor utiliza la computadora

Arens y Loebbecke nos dicen que existen tres formas en que el auditor utiliza la computadora:

- ***"El enfoque de datos de prueba, que involucra el procesamiento de datos de prueba del auditor en el sistema de cómputos del cliente como parte de la verificación de controles.***

- ***El enfoque de programa de computadora del auditor, que involucra la verificación de los registros permanentes en la computadora y los estados financieros del cliente.***

- ***La auditoría auxiliada por microcomputadora, que involucra el uso de la computadora para desempeñar tareas de auditoría independiente de los registros del cliente."*** [19]

Con respecto al enfoque de datos de prueba, lo que realiza el auditor es verificar la efectividad de los controles internos, probando el buen funcionamiento del software utilizado por el cliente. Incluye pruebas incorporando transacciones ficticias en el mismo, con diferentes datos, probando con operaciones no válidas para determinar si el sistema tiene los controles necesarios como para impedir el procesamiento cuando los datos son erróneos y sin que necesariamente alguien más que el auditor conozca que la prueba se está realizando. También para poner

[19] Ibídem, p.578 y sgtes.

a prueba controles específicos en programas de computadora, tales como controles en línea de contraseñas y acceso a datos.

Cuando el auditor elige dichas pruebas debe abarcar todas las transacciones relevantes, es decir que él debe verificar que el software esté realizando los controles básicos para el buen funcionamiento. Por lo general se requiere del apoyo de un especialista en TI según la complejidad del sistema.

Es recomendable que la ejecución de la prueba se realice en un ambiente especialmente previsto para ese fin, con el objetivo de no crear problemas a los datos reales que procesan los mismos programas.

Cuando se procesan los datos de prueba el auditor se asegura de que éstos sean eliminados posteriormente de los registros contables de la entidad, estas tareas adicionales requieren más tiempo, por lo cual esta técnica se emplea en situaciones en que es relevante la auditoría continua del funcionamiento de controles, es decir es más aprovechable por auditores internos.

Con respecto al enfoque de programa de computadora del auditor, éste consiste en que el auditor corra su propio programa de manera controlada, realizando muchas clases de pruebas con el fin de verificar los datos del cliente registrados en lenguaje de máquina. Puede usar programas específicos o software de auditoría general (SAG).

Los programas escritos para un propósito desempeñan tareas de auditoría en circunstancias específicas. Estos programas pueden ser desarrollados por el auditor, por la entidad que está siendo auditada o por un programador externo contratado por el auditor. En algunos casos el auditor puede usar los programas existentes de una entidad en su estado original o modificados, ya que de esta

forma puede ser más eficiente que si desarrolla uno nuevo. Los programas generalizados de computadora son 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.

2.3 - Enfoque de auditoría

2.3.1 - Conceptos Previos

Evidencia de auditoría

Evidencia es cualquier información que utiliza el auditor para determinar si la información cuantificable que se está auditando se presenta de acuerdo con los criterios establecidos. La evidencia puede ser de muchas formas: testimonios del auditado, comunicaciones por escrito con personas externas, observaciones que hace el auditor, etc. Es importante conseguir una calidad y cantidad suficiente de evidencia, éstas constituyen un respaldo que el auditor deberá conservar, ya que forman parte de sus papeles de trabajo y sustentan su opinión.

Pruebas de controles o de cumplimiento

El auditor debe verificar si los controles declarados en realidad existen, si se llevan a cabo y si realmente funcionan de acuerdo a los objetivos para los cuales fueron diseñados. Las pruebas pueden estar orientadas a verificar el cumplimiento de controles generales o de controles específicos. La NIA 330 nos dice que son procedimientos de auditoría diseñados para evaluar la eficacia operativa de los controles para prevenir o detectar y corregir distorsiones significativas en las aseveraciones.

Pruebas sustantivas

En este tipo de pruebas se debe ahondar en la verificación de los saldos contables al cierre del ejercicio auditado o también se pueden realizar cierres interinos siempre y cuando se confíe en el control interno de la empresa. Según la NIA 330 las pruebas sustantivas pueden dividirse en procedimientos analíticos sustantivos y pruebas de detalle, admitiendo estas últimas una subdivisión adicional sobre clases de operaciones, saldos de cuentas e informaciones.

Enfoque de cumplimiento o de confiabilidad

En este enfoque el auditor se basa en la información emanada del sistema de control interno y de sistemas contables, es decir que va a desarrollar su trabajo partiendo de la base de que confía en el control interno de la empresa.

En una organización en la que el auditor compruebe que los sistemas de control interno existen, están vigentes y son eficientes, podrá trabajar bajo un enfoque de cumplimiento.

Enfoque sustantivo

En este enfoque el auditor se basa en la obtención de evidencias sobre los EECC, ya que no es posible apoyarse en el sistema de control interno debido a que dicho sistema no es confiable, de esta forma el auditor va a desarrollar pruebas en mayor número y alcance que bajo un enfoque de confiabilidad. Si no es posible basarse en un enfoque sustantivo, el auditor no acepta el trabajo.

Siempre aplico pruebas sustantivas pero si el enfoque del auditor es de cumplimiento, éstas tendrán menor alcance que en un enfoque sustantivo.

2.3.2 - Enfoque a aplicar

Cuando el auditor realiza una auditoría tiene que decidir si va a aplicar un enfoque de confianza o un enfoque sustantivo. El enfoque a aplicar dependerá no sólo del sistema de control interno, sino también de los sistemas contables utilizados por la empresa, ya que el auditor puede encontrarse con paquetes de software estándar reconocidos en el mercado, que ya ha sido probado su buen funcionamiento por la firma de auditores para la cual se desempeña o por el contrario puede enfrentarse a un software desconocido y entonces deberá evaluar su funcionamiento, teniendo en cuenta si necesita el apoyo de un experto en sistemas.

De acuerdo a la NIA 315, el auditor para poder planear la auditoría y desarrollar un enfoque de auditoría efectivo deberá obtener una comprensión suficiente de los sistemas de contabilidad y de control interno de la entidad auditada.

De esta forma vemos que el enfoque a aplicar dependerá de las características de la entidad y del grado de desarrollo de los sistemas de TI que utilice la misma.

Para aquellos ambientes altamente computarizados, en donde la dependencia de TI es un factor muy importante, existen muchos controles automatizados sobre todo en empresas con gran volumen de transacciones, por lo tanto el auditor va a aplicar un enfoque de confianza realizando para ello una evaluación de los controles existentes en el área informática.

Capítulo 3

3 - ALCANCE DE PROCEDIMIENTOS A APLICAR SOBRE LOS CONTROLES GENERALES Y DE APLICACIÓN SEGÚN LAS CIRCUNSTANCIAS DE LA EMPRESA AUDITADA

3.1 - El control interno

3.1.1 - Conceptos previos

3.1.1.1 - Informe COSO (Committee Of Sponsoring Organizations):

Surgió como una respuesta a las inquietudes que planteaban la diversidad de conceptos, definiciones e interpretaciones existentes en torno al control interno. Fue publicado en EEUU en 1992. Este informe logra definir un marco conceptual común y se constituye en una visión integradora del control interno. El informe COSO define el control interno como:

> ***"un proceso, efectuado por el directorio, la dirección y el resto de los integrantes de una organización, destinado a proveer razonable seguridad en relación al logro de objetivos en las siguientes categorías:***
>
> - ***Eficacia y eficiencia de las operaciones***

· ***Confiabilidad en la elaboración de información contable***

· ***Cumplimiento con las leyes y regulaciones aplicables."***

El control interno comprende cinco componentes interrelacionados:

- **Ambiente de control**

  El corazón de cualquier negocio es su gente (sus atributos individuales: integridad, valores éticos y competencia) y el ambiente en el cual se trabaja.

- **Apreciación de riesgos**

  La entidad debe estar al tanto y manejar los riesgos a los que se enfrenta. También debe establecer mecanismos para identificar, analizar y manejar los riesgos relacionados.

- **Actividades de control**

  Deben establecerse y ejecutarse políticas y procedimientos de control para ayudar a asegurar que las acciones identificadas por la dirección, como necesarias para encarar los riesgos asociados al logro de los objetivos de una entidad, sean eficazmente llevadas a cabo.

- **Información y comunicación**

  Rodeando estas actividades están los sistemas de información y comunicación. Estos permiten a los integrantes de la entidad obtener e intercambiar la información necesaria para conducir, manejar y controlar sus operaciones.

- **Monitoreo**

  El proceso completo debe estar monitoreado y deben efectuarse las modificaciones necesarias. De esta forma, el sistema puede reaccionar dinámicamente, cambiando cuando las condiciones lo justifiquen.

3.1.1.2 - Concepto de control interno utilizado por las NIAs

La NIA 315 (Identificación y análisis de los riesgos de distorsiones significativas mediante la comprensión de la entidad y de su entorno) utiliza los mismos conceptos de control interno y sus componentes definidos en el informe COSO. En su párrafo 4 define el control interno como:

> ***"El proceso diseñado, implementado y mantenido por quienes tienen a su cargo la dirección, la gerencia y otro personal con el fin de brindar una seguridad razonable sobre el logro de los objetivos de la entidad en relación con la confiabilidad de la información financiera, la eficacia y la eficiencia de las operaciones y el cumplimiento de las leyes y normativa aplicables. El término "controles" se refiere a cualquier aspecto de uno o más de los componentes del control interno."*** [20]

En dicha NIA se establece que el auditor deberá comprender el control interno relevante para la auditoría, recurriendo a su criterio profesional para determinar si un control, en forma individual o en combinación con otros, es relevante o no.

No importa lo bien diseñado y operado que esté el sistema de control interno de una entidad, independientemente de ello, sólo puede brindar una seguridad razonable sobre el logro de los objetivos de información financiera. La probabilidad de logro está afectada por las limitaciones inherentes al control interno, ya que pueden producirse errores en el diseño de un control o estando bien diseñado pueden producirse fallas en su aplicación. Además los controles pueden ser evadidos por colusión de dos o más personas o debido a que la

[20] IFAC, Ob. Cit. NIA 315, p.309.

gerencia hace caso omiso de los controles inherentes. Por ejemplo los controles de edición en un programa de software que están diseñados para identificar e informar sobre operaciones que excedan límites de crédito específicos, pueden ser evadidos o desactivados intencionalmente.

Es importante el conocimiento del control interno tanto para la eficacia como para la eficiencia del trabajo del auditor y es obligatorio ese conocimiento por la NIA 315.

3.1.2 - El control interno en ambientes computarizados

La NIA 315 nos dice que el auditor para entender el control interno de una entidad deberá comprender la manera en que la misma ha dado respuesta a los riesgos informáticos. También en dicha norma se enumera el uso de la TI, dentro de las cuestiones a considerar por el auditor que pueden dar origen a riesgos de distorsiones significativas en los estados financieros, por ejemplo si los sistemas y los procesos resultasen incompatibles. El auditor deberá considerar el ambiente de TI al diseñar los procedimientos y de esta manera poder reducir el riesgo de auditoría a un nivel aceptablemente bajo.

El auditor se enfocará en los procedimientos relativos a los sistemas de contabilidad y control interno relevantes para su trabajo, basado en la información que surge de los mismos. De esta forma el análisis que realizará el auditor con respecto al control interno, va a abarcar un campo más específico que el realizado por la empresa.

En toda entidad existen controles manuales y controles automatizados. Los controles en sistemas informáticos consisten en una combinación de ambos.

Dicha combinación varía con la naturaleza y complejidad del uso de la informática en cada entidad.

Los controles automatizados son más confiables que los manuales porque no se pueden omitir, ignorar o evadir con facilidad y son menos propensos a errores y equivocaciones simples. Este tipo de controles es más adecuado en operaciones de gran volumen o recurrentes, o en las situaciones en que se puedan impedir o detectar y corregir los errores que sean predecibles mediante parámetros de control automatizados, también en aquellas actividades de control en las que se puedan diseñar y automatizar adecuadamente los pasos específicos para realizar el control. En otros casos, como en transacciones grandes, inusuales o no recurrentes y en aquellas circunstancias donde los errores sean difíciles de definir anticipar o predecir, son más adecuados los controles manuales.

El auditor deberá considerar si la entidad responde de manera adecuada a los riesgos que se originan por el uso de TI, si se establecieron controles y si fueron efectivos, para así poder evaluar el sistema de control interno de la entidad. Los recursos tecnológicos deben ser regularmente testeados a los efectos de lograr cumplir con los requisitos del sistema de información.

3.1.2.1 - Beneficios de la informática al control interno

El alto uso de la informática en una entidad ha traído beneficios sobre el sistema de control interno, algunos de los cuales son:

- Procesamiento de grandes volúmenes de transacciones o datos realizando cálculos complejos.

- Mejora de la oportunidad, disponibilidad y exactitud de la información.
- Facilita el análisis adicional de información.
- Amplía la capacidad de monitorear el desempeño de las actividades de la entidad y sus políticas y procedimientos.
- Reduce el riesgo de que se burlen los controles.
- Aumenta la capacidad de lograr una efectiva segregación de funciones al implementar controles de seguridad en aplicaciones, bases de datos y sistemas de operación.

3.2 - Aplicación y alcance de los procedimientos según las circunstancias de la empresa

3.2.1 - Procedimientos de auditoría

Durante el proceso de la auditoría, el profesional actuante aplica una serie de procedimientos con el fin de obtener evidencia válida, suficiente y relevante para poder llegar a las conclusiones de su trabajo. Estas evidencias le permitirán fundamentar sus opiniones y conclusiones para elaborar su dictamen.

Procedimientos y técnicas de auditoría:

- **Indagaciones:**

Reuniones con la gerencia, con determinados funcionarios y con terceros que tengan relación con las operaciones de ésta para recabar información útil para el desarrollo de su trabajo (evidencias testimoniales). Si de estas entrevistas surgen

datos relevantes para la auditoría, el auditor solicitará a los mismos que documenten dichas afirmaciones como evidencia.

- **Solicitud de documentos:**

Tales como: actas de Directorio y Asamblea de Accionistas, contratos de la empresa con terceros (por ej. contratos de representación, exclusividad, distribución, de royalties, de servicios contratados, etc.), también si la empresa posee manuales, reglamentos, instructivos, contratos especiales con empleados, es decir toda aquella documentación que le aporte datos de interés para el conocimiento del negocio (evidencias documentales).

- **Lectura y análisis de leyes, decretos, resoluciones y otros:**

El auditor debe tomar conocimiento acerca del marco legal en el que está inmersa la entidad para poder corroborar que se esté cumpliendo con el mismo.

- **Encuestas y cuestionarios:**

Formulación de preguntas para conocer la realidad de los hechos, situaciones u operaciones. Deben estar debidamente intervenidas por los involucrados (evidencias documentales, testimoniales).

- **Observaciones:**

Consiste en la verificación ocular de operaciones y procedimientos durante la ejecución de las actividades de la entidad y de los controles realizados por los funcionarios de la empresa (evidencias físicas).

- **Revisión analítica – comparaciones:**

Se realiza un análisis y se relacionan los datos para efectuar comparaciones, tanto de información real y presupuestada como de los saldos contables de estados financieros de diferentes períodos, de esta forma se pueden calcular diferentes

índices, identificando y analizando sus variaciones. Se define una cifra denominada materialidad preliminar, los rubros que la superen serán analizados y los demás serán descartados con excepción de rubros que a pesar de que no superen dicha cifra son relevantes, por ejemplo disponibilidades (evidencias analíticas).

- **Rastreo:**

Consiste en el seguimiento de una operación a través de la documentación respectiva, a fin de conocer y evaluar su ejecución (evidencias analíticas).

- **Revisión de cálculos matemáticos:**

Consiste en la verificación de la exactitud aritmética de las operaciones contenidas en documentos, procurando establecer la razonabilidad de los saldos contables. Algunos ejemplos de esto es el recálculo de la depreciación de bienes de uso, de previsiones, etc. (evidencias analíticas).

- **Inspección de documentación respaldante**:

Consiste en la confrontación de información de transacciones contenida en registros contables contra el soporte documental para confirmar la veracidad, exactitud, existencia, legalidad y legitimidad de las operaciones realizadas (evidencias analíticas y documentales).

- **Conciliaciones:**

Consiste en el examen de la información emanada de diferentes fuentes con respecto a una misma operación (evidencias analíticas).

- **Circularización:**

Consiste en la confirmación de saldos contables a terceros (empresas o personas), que interactúan habitualmente con la entidad auditada para obtener información

directa y por escrito de un sujeto externo a la misma. Siempre que pueda solicitar a alguien externo que confirme un saldo entonces lo aplico, ya que es el más eficiente de los procedimientos (evidencias testimoniales).

- **Análisis de soportes informáticos:**

Consiste en la evaluación de los elementos lógicos, programas y aplicaciones utilizados por el auditado. El auditor comienza por tomar conocimiento de los sistemas informáticos utilizados y analizar las medidas adoptadas por la empresa con respecto a la seguridad física y lógica de los mismos y luego realiza las pruebas correspondientes para verificar que funcionen correctamente (evidencias informáticas). En el caso de entornos altamente computarizados, el auditor solicitará la intervención del experto en sistemas informáticos para así poder llevar a cabo este tipo de procedimiento.

- **Comprobaciones físicas:**

Consiste en inspeccionar los activos tangibles, realizando el examen físico y ocular de los mismos, para ello el auditor deberá realizar indagaciones en la entidad, hacer observaciones de los activos, realizar el rastreo de algunas transacciones y de esta forma poder realizar las comprobaciones necesarias, por ejemplo: arqueo de dinero y valores, participación en inventarios, verificación física de bienes de uso, etc. (evidencias físicas).

- **Evaluaciones de los criterios contables aplicados:**

El auditor deberá llegar a una conclusión sobre los EECC, opinando si los mismos están elaborados razonablemente sobre el marco normativo aplicado, por lo tanto uno de los procedimientos a aplicar es tomar conocimiento de cuáles fueron los criterios contables que la entidad aplicó para la realización de los mismos.

- **Cartas solicitando información a terceros:**

El auditor solicita información relevante a escribanos, abogados y a otros terceros que estén relacionados con la entidad para tomar conocimiento sobre situaciones como juicios, demandas, embargos y cualquier otra información relevante para su trabajo. Con respecto a la respuesta del abogado si existen litigios él deberá hacer una referencia a su naturaleza, cuantía y eventual desenlace (probabilidad de ocurrencia). Toda la información de los referidos profesionales se solicita en la etapa de las tareas finales, ya que el auditor necesita tener conocimiento de los hechos que surjan también en el período comprendido entre la fecha de los EECC y la de emisión de los informes por parte del auditor. [21]

Los procedimientos detallados no constituyen una lista taxativa, el auditor en base a su experiencia y a las características de la empresa auditada podrá llevar a cabo otros. Luego de seleccionar aquellos que crea convenientes, los incluirá en su programa de trabajo.

3.2.2 - Alcance de una auditoría de estados financieros

> ***"El término "alcance de una auditoría" se refiere a los procedimientos de auditoría que, a juicio del auditor y sobre la base de las NIAs, se consideran adecuados en determinadas circunstancias para lograr el objetivo de la auditoría".*** [22]

El alcance es la intensidad y profundidad con que se aplican los procedimientos de auditoría en la práctica, el cual depende del tipo de empresa y de sus

[21] Fuente: Pág. Web, *Auditoría Interna de la Nación (www.ain.gub.uy)*. GUBBA H. y otros, Ob. Cit. p.22 y 23, IFAC, Ob. Cit., NIA 315.
[22] IFAC, Ob. cit., NIA 200, párrafo 10, p. 98

particularidades operativas. Se relaciona con la oportunidad, que es el momento en que deben aplicarse los procedimientos.

La NIA 330 dice:

> ***"El alcance de un procedimiento de auditoría que se juzgue necesario se establece luego de considerar la significación, el riesgo analizado y el grado de seguridad que el auditor se propone obtener… En general, el alcance de los procedimientos de auditoría se incrementa a medida que aumenta el riesgo de distorsiones significativas. "*** [23]

El auditor para establecer el alcance de los procedimientos a aplicar, va a tener en cuenta además de las características de la empresa, el funcionamiento de su control interno y el riesgo de auditoría, el cual intentará minimizar. Para lograr esto, aumentará el alcance de las pruebas de control, por ejemplo dado un procedimiento si el auditor quiere trabajar con un riesgo de auditoría inferior, deberá aplicarse un tamaño de muestra más grande para llevar a cabo las pruebas. Siempre que el auditor llegue a la conclusión de que no puede reducirse el riesgo de control, deberá ampliar la verificación sustantiva.

Según la NIA 330 la utilización de las técnicas de auditoría asistidas por computadora, TAACs, permite la realización de pruebas más exhaustivas que pueden ser útiles cuando el auditor decide modificar el alcance de las mismas. Dichas técnicas pueden seleccionar una muestra de operaciones de los archivos electrónicos clave, para detectar operaciones con características especiales o para analizar una población entera en lugar de una muestra.

[23] IFAC, Ob. cit., NIA 330, párrafo 15, p. 384

En cada auditoría de acuerdo al resultado de la evaluación del sistema de control interno, el auditor al planificar su trabajo determinará la naturaleza de los procedimientos, su alcance y su oportunidad según los riesgos y otras circunstancias con el objetivo de obtener la evidencia necesaria y la suficiente certeza para sustentar sus conclusiones y opiniones de manera objetiva, no descuidando la relación costo-beneficio entre los insumos necesarios y la utilidad de los resultados esperados.

La NIA 330 también nos dice que debido a la consistencia que caracteriza al procesamiento informático, cuando tenemos un control automatizado no va a ser necesario incrementar el alcance de las pruebas sobre dicho control, pues se espera que el control automatizado funcione de manera uniforme, salvo aquellos casos en que el programa se cambie. Un auditor puede evaluar que un control automatizado funciona de manera efectiva y de esta forma posteriormente sólo alcanzará con realizar pruebas para establecer que continúa funcionando de dicha manera.

Por lo tanto en entornos altamente computarizados el auditor no va a aumentar el alcance de las pruebas sobre los controles, ya que el control automatizado funcionará en forma consistente tanto para una o miles de transacciones.

3.3 - Controles de interés para el auditor

En auditorías desarrolladas en ambientes de TI es imprescindible evaluar los controles presentes en el área informática. Para empresas que utilizan sistemas complejos, el ambiente de control es mucho más determinante que para aquellas que utilizan sistemas simples, porque hay mayor posibilidad de ocurrencia de

error, por lo tanto si se quiere obtener información confiable de sus sistemas contables, se deberá contar con un sólido ambiente de control.

A consecuencia de esto, los procedimientos de control en una entidad de este tipo deberán diseñarse con más cuidado y ser evaluados de manera más frecuente, de tal forma que en la mayoría de ellas existe un departamento de auditores internos en el área informática. Los controles sobre la suficiencia y razonabilidad de la información suministrada por la entidad pueden ser relevantes para la auditoría si el auditor tiene intención de utilizar dicha información para diseñar y llevar a cabo posteriores procedimientos. Los controles que la empresa realiza sobre operaciones y objetivos de cumplimiento también pueden ser relevantes para la auditoría si se relacionan con datos que el auditor evalúa o utiliza al aplicar procedimientos de auditoría.

El auditor no realiza la evaluación de todos los controles, sino que se limita a aquellos que afectan a la confiabilidad de la presentación de la información financiera.

Las actividades de control son uno de los cinco elementos del control interno. Estas actividades tanto en sistemas manuales como informáticos se aplican con diversos objetivos y en diferentes funciones. Al auditor le interesarán las actividades de control que se relacionan con los siguientes aspectos fundamentales de control interno:

- Autorización de las operaciones.
- Contabilización de las operaciones.
- Acceso restringido a los activos.
- Comprobaciones físicas.

El auditor pondrá énfasis en identificar y comprender las actividades de control que estén relacionadas con las áreas donde el auditor considera que los riesgos de distorsiones significativas son mayores.

La implementación de las actividades de control va a verse afectada por el uso de la informática. Los controles de los sistemas en este entorno van a ser eficaces para el auditor siempre y cuando:

- Mantengan la integridad de la información.
- Mantengan la seguridad de los datos.
- Contengan controles informáticos correspondientes.

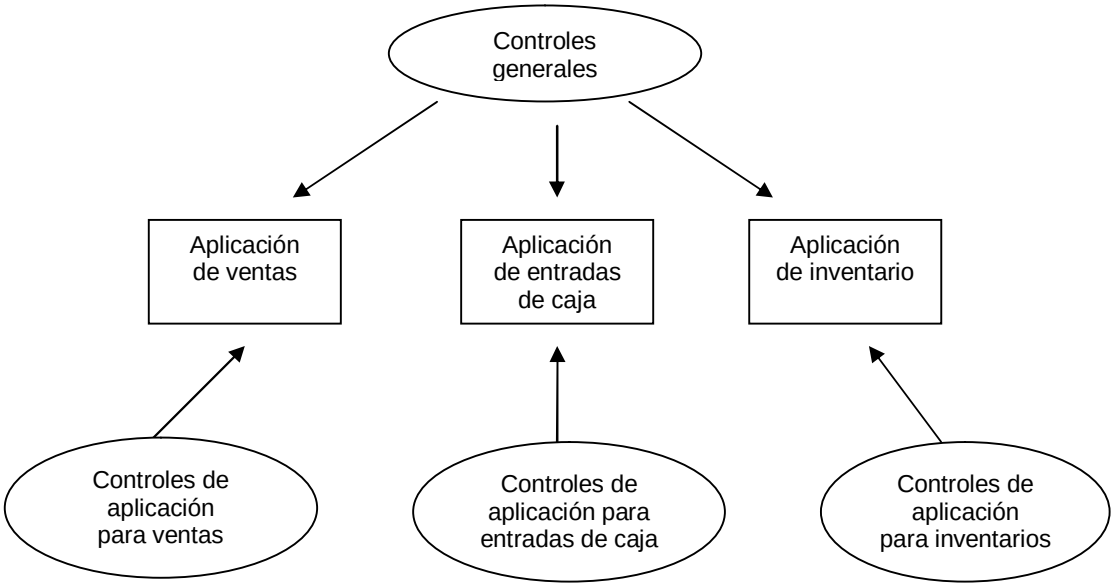
Con respecto a los controles informáticos, se clasifican en controles generales y controles de aplicación.

Según Arens y Loebbecke:

> **"Un control general se relaciona con todas las partes del PED, y, por tanto debe ser evaluado en las primeras etapas de la auditoría. Los controles de aplicación se relacionan con un uso específico dentro del sistema, como el procesamiento de ventas o entradas de efectivo, y debe evaluarse específicamente para cada área de auditoría en que el cliente utiliza la computadora, donde el auditor planea reducir el riesgo del control determinado". [24]**

[24] ARENS y LOEBBECKE, Ob. Cit., p. 573 y sgtes.

Dichos autores muestran la relación de los dos tipos de controles con las distintas aplicaciones en el siguiente esquema:



3.3.1 - Controles generales

Según la NIA 315 los controles generales informáticos son políticas y procedimientos que sirven de apoyo para el funcionamiento y la eficacia de los controles de aplicaciones, ya que ayudan a asegurar el funcionamiento continuo y apropiado de los sistemas de información.

Ejemplos de controles generales informáticos:

- Controles de cambios de programas.
- Controles que restringen el acceso a programas o datos.
- Controles de implementación de nuevas versiones de aplicaciones de paquetes de software.

- Controles sobre el software del sistema que restringe el acceso o que monitorea el uso de los utilitarios del sistema que pueden llegar a realizar modificaciones en los datos o en los registros contables sin dejar ningún tipo de referencia de auditoría.

Según la NIA 330, los cambios producidos en un sistema, como por ejemplo que la entidad pueda emitir nuevos informes a través de los mismos, probablemente no afecten la relevancia de los elementos de juicio de auditoría obtenidas en auditorías previas, sin embargo un cambio que cause que los datos se acumulen o que se calculen de manera diferente si la afecten.

Según Arens y Loebbecke dentro de los controles generales se pueden distinguir cuatro categorías:

- **Plan de organización**

  Dentro de esta primera categoría encontramos la segregación de funciones, por ejemplo la división de tareas que debería existir entre el programador y los operadores de la computadora. Es mucho más probable que encontremos esta separación en organizaciones de gran tamaño y que cuentan con sistemas complejos. En la etapa inicial donde se realiza el conocimiento del negocio, pueden obtenerse organigramas, cursogramas, flujogramas si la empresa cuenta con ellos puede determinarse rápidamente si hay falta de segregación de funciones en el área informática para detectar debilidades de control.

- **Procedimientos para documentar, revisar y aprobar los sistemas y programas**

  Uno de los controles aquí consistiría en verificar que el cliente controla los programas de computación y la documentación relacionada. Un

programa adecuado corre instrucciones para operar la computadora. Los controles primarios en esta área se incluyen en el diseño y uso de los manuales de sistemas.

- **Controles de hardware**
  Estos controles son diseñados por el fabricante del equipo y se utilizan para detectar fallas en el mismo. Son construidos dentro del sistema con el objetivo de que descubran y reporten todas las fallas de la máquina. De esta forma cuando se produce una falla, aparecen mensajes de error en el computador.

- **Controles sobre el acceso al equipo, programas y archivos de datos**
  Estos controles físicos son muy importantes para proteger el equipo y los registros de PED. En estos casos se requiere una clave autorizada para que funcione la terminal de computadora**.**

Por lo general, antes de evaluar la efectividad de los controles de aplicación se realiza una evaluación de los controles generales, ya que si éstos últimos son inefectivos podría haber errores en cada aplicación de contabilidad basada en computadora, como ejemplo de esto, si existe una inadecuada separación de responsabilidades de modo que los operadores de computadora sean también programadores y tengan acceso a los programas de computación y a los archivos de datos, entonces el auditor se va a preocupar por las potenciales transacciones ficticias o los datos no autorizados y las omisiones en cuentas como ventas, compras y nóminas, llegando a la conclusión que existe un riesgo importante de pérdida de datos porque los controles generales afectan a cada aplicación**.**[25]

[25] ARENS y LOEBBECKE, Ob. Cit., p. 573

3.3.2 - Controles de aplicación

Según la NIA 315 son procedimientos manuales o automatizados, que se aplican en los procesos de una empresa para el procesamiento de aplicaciones individuales. El objetivo de los mismos es asegurar la integridad de los registros contables. Pueden ser:

- Controles de aplicación preventivos.
- Controles de aplicación con fines de detección.

Estos controles ayudan a asegurar que las operaciones fueron autorizadas, registradas y procesadas en su totalidad y de manera exacta (objetivos de integridad y exactitud).

Ejemplos de controles de aplicación:

- Controles de la verificación de la razonabilidad aritmética de los registros.
- Controles del mantenimiento y la revisión de cuentas y de balances de comprobación de sumas y saldos.
- Controles de edición de los datos de entrada.
- Controles de secuencia numérica.
- Seguimiento manual de los informes de excepciones o enmiendas al momento del ingreso de datos.

Según Arens y Loebbecke estos controles se aplican a las entradas, procesamiento y salidas de una aplicación de los sistemas informáticos:

- **Controles de entrada**

Estos controles se utilizan para corroborar que la información procesada por la computadora sea válida, completa y precisa. Estos controles son muy importantes, ya que gran parte de los errores en los sistemas de cómputo ocurren por errores en la entrada. Como ejemplo de controles que reducen este tipo de errores encontramos entre otros: la existencia de una adecuada autorización previa de las transacciones, documentos adecuados, verificación en el teclado y dígitos de verificación.

- **Controles de procesamiento**

  Estos aseguran que la entrada de datos al sistema se procesa correctamente, es decir que todos los datos que ingresan a la computadora se procesan solo una vez y de forma correcta. La mayor parte de estos controles son también controles programados, donde la computadora se programa para realizar esta verificación. Un ejemplo sería la prueba de razonabilidad de precio unitario en una transacción.

- **Controles de salida**

  Estos controles están diseñados para comprobar que los datos que genera la computadora son válidos, precisos, completos y que se distribuyen solo a las personas autorizadas. El más importante dentro de esta área es la revisión de la razonabilidad de los datos por alguien que conoce cómo debe ser la salida.

Generalmente existe la necesidad de un mayor número de procedimientos de control interno en un sistema complejo. Muchos controles son necesarios debido a que el rastro de la transacción es invisible, entonces se requiere de un experto para su evaluación. De esta forma cuando el cliente posee un sistema complejo, los auditores necesitan del apoyo de especialistas para evaluar la estructura del control interno y para comprender esta estructura se debe obtener información

preliminar observando flujogramas, cuestionarios del área informática y un estudio de la lista de errores generados por el sistema.

Luego de que el auditor comprende la estructura del control interno de los sistemas informáticos decide hasta qué grado se reduce el riesgo de control. [26]

[26] ARENS y LOEBBECKE, Ob. Cit., p. 574

Capítulo 4

4 - HERRAMIENTAS Y TÉCNICAS PARA LA EVALUACIÓN DE CONTROLES

4.1 - Técnicas de auditoría asistidas por computadora (TAACs)

> ***"Técnicas de auditoría asistidas por computadora – Aplicación de procedimientos de auditoría utilizando la computadora como herramienta de auditoría (también conocidas como TAAC)."*** [27]

Son aplicaciones especiales, útiles para la evaluación de los controles internos y la recolección de evidencia de carácter sustantivo.

Las TAACs son programas de computadora que el auditor usa como parte de los procedimientos de auditoría para procesar datos importantes para su trabajo, contenidos en los sistemas de información de una entidad.

Los datos pueden ser de transacciones, sobre los que el auditor desea realizar pruebas de controles o procedimientos sustantivos, o pueden ser de otro tipo. El auditor puede usar TAACs para revisar archivos para obtener evidencia de la

[27] IFAC, Ob. Cit., Glosario de términos de Auditoría , p. 50

existencia y operación de controles. Las TAACs pueden consistir en programas de paquete, programas escritos para un propósito, programas de utilería o programas de administración del sistema. Independientemente del origen de los programas, el auditor ratifica que sean apropiados y su validez para fines de auditoría antes de usarlos.

Pueden mejorar la efectividad y eficiencia de los procedimientos de auditoría, proporcionar pruebas de control efectivas y permitir realizar 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, usando la computadora como una herramienta de auditoría.

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

- Pruebas de detalle 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 el uso de software de comparación de códigos, para verificar que la versión del programa en uso es la versión aprobada por la administración.
- Muestreo de programas para extraer datos para pruebas de auditoría.
- Pruebas de controles de aplicación, por ejemplo pruebas del funcionamiento de un control programado.
- Rehacer cálculos realizados por los sistemas de contabilidad de la entidad.

El auditor al planificar su trabajo puede considerar una combinación apropiada de técnicas de auditoría manuales o automatizadas. Al evaluar el uso de TAACs los factores a considerar incluyen:

- El conocimiento, pericia y experiencia del equipo de auditoría del ambiente de TI.
- La disponibilidad de TAACs e instalaciones y datos adecuados de computación.
- La imposibilidad de realizar pruebas manuales.
- La efectividad y eficiencia.
- La oportunidad.

En ambientes de TI la mayoría de los procesos están computarizados y los rubros de los EECC surgen de datos ingresados en sistemas informáticos, entonces el auditor debe considerar cómo afecta a la auditoría un ambiente de sistemas y cuándo utilizar el trabajo de terceros expertos en el área pero no comprometidos con la organización auditada.

Los objetivos y alcance global de una auditoría no cambian cuando se conduce una auditoría en un ambiente de TI. Sin embargo la aplicación de procedimientos de auditoría puede requerir que el auditor considere las TAACs porque este tipo de ambiente puede afectar:

- Los procedimientos seguidos por un auditor para obtener una comprensión suficiente de los sistemas de contabilidad y de 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.

- El diseño y desarrollo de pruebas de control y procedimientos sustantivos apropiados para cumplir con el objetivo de la auditoría.

La etapa de la auditoría en que es más necesario o conveniente el empleo de TAACs, es en la de obtención de evidencia válida y suficiente, cuando se ejecutan las pruebas de cumplimiento y sustantivas, llegando a ser imprescindible el uso de TAACs en auditorías en ambientes altamente computarizados.

Existen rutinas de auditoría incorporadas a veces por la entidad, que están integradas en un sistema de computadoras para proporcionar datos que serán usados posteriormente por el auditor.

Las organizaciones deberán ser concientes de la necesidad de emplear parte de sus recursos al desarrollo de la TI, para aprovechar las oportunidades que ésta le presenta y minimizar el impacto de los nuevos riesgos que introduce. Una inadecuada administración de la TI, sin los debidos controles de seguridad y de funcionamiento impactará directamente en el resultado de la auditoría.

4.2 – Herramientas para la evaluación de controles

En las auditorías en ambientes altamente computarizados el auditor se ve forzado a la utilización de herramientas para la evaluación de los controles sobre los sistemas informáticos.

Según Jorge R. Nardelli, las herramientas utilizadas para la evaluación de los controles en el área informática se pueden clasificar en cuatro categorías:

i. Programa especial de auditoría desarrollado por o bajo la supervisión del auditor.

ii. Software de aplicación de la entidad auditada. El auditor puede realizar un reprocesamiento total o parcial con una copia de este software y eventualmente en el microcomputador de su propio estudio (totalmente compatible).

iii. Software especial para auditoría. Son paquetes para preparar papeles de trabajo de auditoría en un entorno de microcomputadores y ofrecen ciertas ventajas como flexibilidad del formato, almacenamiento de papeles de trabajo para reutilizar al siguiente año y facilitan al auditor el desarrollo de los papeles de trabajo.

iv. Software generalizado para auditoría. Consiste en un programa o una serie de programas desarrollados para llevar a cabo ciertas funciones, con el fin de procesar la información que surge de los sistemas informáticos del cliente, para ser utilizada en la auditoría de estados contables, dichas funciones incluyen: lectura de la información contenida en medios magnéticos, selección de datos, realización de cálculos e impresión de listados de acuerdo con las especificaciones del auditor. Nos nombra como ejemplo cuatro paquetes:

- **ACL PLUS** (ACL Services Ltd. – Canadá)
- **APPLAUD** (Premier International – Chicago, EUA)
- **PANAUDIT PLUS** Workstation (Pansophic Systems – Illinois, EUA)
- **IDEA** (Desarrollado por el Instituto de Contadores de Canadá (CICA) y comercializado también por el AICPA por convenio especial con la entidad anterior). [28]

[28] Fuente: NARDELLI, Jorge R., *Auditoría y seguridad de los sistemas de computación,* p. 383 y sgtes. Edit. Cangallo, Año 1992.

Arens y Loebbecke con respecto al uso de software nos dicen que aunque es posible que los auditores escriban programas específicos o que utilicen programas del cliente ya existente, el enfoque más común es utilizar software de auditoría general (SAG). También aclaran que el uso de SAG tiene dos ventajas importantes: la facilidad en el uso y la amplia variedad de tareas que pueden desarrollarse con él, lo que evita incurrir en costos de desarrollo de programas específicos. Es común que este software general se utilice ampliamente en las firmas de auditoría. [29]

Algunos recursos de TI utilizados en auditoría:

- Información disponible en Internet.
- Información disponible en Intranet.
- Soporte de seguridad del sistema operativo y/o del resto del software.
- Planillas de cálculo electrónicas.
- Procesadores de texto.
- Manejadores de bases de datos.
- Plantillas patentadas de software comercial de uso general. Utilizando hojas de cálculo electrónicas y procesadores de texto, pueden crearse formatos prediseñados para papeles de trabajo, cartas y otros, estos formatos se llaman plantillas.
- Datawarehouse o almacén de datos, es una técnica de modelado, extracción y almacenamiento de datos para su posterior empleo para obtener información a demanda. Esta herramienta permite emitir reportes fácilmente a través del análisis de la información ingresada y almacenada en cada aplicación de la entidad, es útil para aquellos reportes que no estén configurados en las aplicaciones. Esta herramienta no genera datos,

[29] Fuente: ARENS y LOEBBECKE, Ob. Cit., p. 582.

solamente toma los datos del sistema y permite analizarlos muy fácilmente. Quien posee esta herramienta no es el auditor sino el cliente, para el auditor es muy útil utilizarla en caso de que el cliente cuente con ella.

- Bases de datos y los propios programas de aplicación del cliente, incluyendo datawarehouse si lo hubiera.
- Herramientas OLAP (análisis automáticos de procesos en línea), se trata de un software que permite analizar, administrar y ejecutar acciones sobre una amplia variedad de posibles vistas de la información, que en el datawarehouse han sido transformadas en filas de datos a través de accesos rápidos e interactivos. El auditor puede recurrir a ellos si la entidad dispone de estos recursos.
- Programas específicos preparados por la auditoría o para ella.
- Paquete de software especializado en auditoría de uso generalizado. Los clientes utilizan diferentes tipos de aplicaciones para su operativa, entonces el auditor utiliza esta herramienta ya que le permite recopilar, comparar y analizar información aunque ésta provenga de bases de datos y archivos de distintas plataformas tecnológicas. Es sumamente útil porque le permite al auditor identificar tendencias, excepciones, situaciones con errores o irregularidades, áreas con debilidades de control, etc.
- Paquetes de software especializado en la evaluación de riesgos y controles. En general proveen análisis detallados sobre objetivos, riesgos, e indicadores de riesgo por unidad de negocio o proceso, permiten jerarquizar riesgos a partir de ponderaciones por probabilidad de ocurrencia e impacto, etc.
- Software especializado en la auditoría de industrias particulares. Ej. software específico para compañías de seguros, para instituciones financieras, etc.

- Paquetes de software especializado en apoyar la administración de la auditoría. El auditor traza un plan de desarrollo e implementación de la auditoría, dividido en etapas e indicando el tiempo y recursos necesarios para cada una permitiendo la administración del personal disponible. [30]

[30] Fuente: D' OLIVO, Ma. Fernanda, MANGUIAN, Jennifer y SAULEDA, Luis A., *Una propuesta de profundización de la enseñanza del aporte de la Tecnología de la Información a la labor de auditoría* - Año 2002

Capítulo 5

5 - EMPLEO DE ESPECIALISTAS

5.1 - Conceptos previos

5.1.1 – Experto

Para la NIA 620 experto es aquella persona (física o jurídica) que posee ciertas habilidades, conocimientos o experiencia en determinadas áreas específicas aparte de la contabilidad y de la auditoría. El auditor podrá recurrir a un experto perteneciente a la misma firma que él integra, o contratar a un tercero, en este último caso el auditor deberá evaluar la competencia profesional del mismo. [31]

5.1.2 – Necesidad del uso del trabajo del experto

El trabajo del experto es necesario en aquellos casos en que el auditor no posee determinadas habilidades, experiencia o conocimientos especiales sobre temas de importancia significativa para la auditoría. La NIA 620 indica que en tales casos el auditor deberá fundamentar que la intervención del experto es necesaria para cumplir con los objetivos de su trabajo. La NIA 300 nos dice que esta necesidad de recurrir a expertos en determinadas materias debe establecerse en el plan general de auditoría. [32]

[31] Fuente: IFAC, Ob. Cit., NIA 620, p. 517.
[32] Ídem, NIA 300, p.243.

En una auditoría de estados contables en ambientes altamente computarizados, el auditor financiero para evaluar determinados aspectos sobre los sistemas informáticos en los cuales él no posee el conocimiento necesario, deberá recurrir a expertos en sistemas. Debido a esta necesidad las firmas de auditoría cuentan con un departamento de tecnología de la información a cargo de profesionales expertos en el área informática.

Para la presente monografía hemos entrevistado a tres profesionales que poseen el título de Ingeniero en Sistemas y pertenecen a tres firmas internacionales de auditoría. A lo largo del presente capítulo y en los siguientes iremos presentando la información recabada en las entrevistas sobre los temas correspondientes.

5.2 - Empleo de especialistas: cuándo involucrarlos

El auditor luego de evaluar la importancia que tienen los sistemas dentro de la entidad, de determinar el grado de automatización de los procesos y de definir el enfoque a aplicar, deberá decidir si solicita o no el apoyo de especialistas del área informática.

> ***"...es un reto la dificultad de aunar la función auditoría y la función informática. En efecto, existen excelentes auditores y excelentes informáticos, pero no es habitual la simbiosis necesaria de ambos. La razón de tal escasez se halla seguramente en la relativa juventud de esta***

> ***profesión y en la experiencia informática previa que el auditor ha de poseer. "*** [33]

El auditor debe obtener suficiente conocimiento del ambiente de TI para planear, dirigir, supervisar y revisar el trabajo desarrollado. Si el auditor considera que debe requerir el apoyo de un profesional en TI, debe dejar evidencia de que dicho trabajo es adecuado para los fines de la auditoría de acuerdo con las NIAs en lo que refiere al uso del trabajo de un experto.

Los tres profesionales entrevistados poseen conocimientos contables para poder llevar a cabo sus tareas, recibiendo la capacitación de las firmas para las cuales trabajan a través de cursos, de libros y de la experiencia que han adquirido. Este conocimiento también es básico para la comunicación con el auditor financiero. Han tenido que capacitarse, ya que según lo respondido por ellos en la facultad de ingeniería no vieron temas contables, o si los vieron no fue con la profundidad requerida para su trabajo actual, así como también los auditores deberán tener nociones sobre informática para poder tener un entendimiento de qué tipo de pruebas podrá solicitarle al experto.

El auditor deberá necesariamente convocar a un experto de sistemas para todos los casos de entornos computarizados complejos, ya que el especialista deberá realizar la evaluación de los controles generales para soportar el entendimiento de riesgos y así poder diseñar las pruebas adecuadas.

En muchas empresas sería muy difícil hacer pruebas sustantivas para todas las transacciones debido a la alta dependencia de TI y a que poseen una gran cantidad de movimientos en sus cuentas significativas, por lo cual no sería viable.

[33] ITURMENDI ACHA, José, Ob. Cit., p.13

Para estos casos está prevista la participación de expertos en sistemas para poder llevar a cabo la auditoría bajo un enfoque de confianza en los controles.

Con respecto al trabajo en sí, dichos profesionales concurren a la entidad auditada en dos instancias, primero en lo que se denomina la visita interina que se realiza previo al cierre del ejercicio y puede ser unos meses antes del cierre y en una segunda instancia visitan al cliente luego de la fecha de balance. En la visita interina realizan en su mayoría pruebas de controles generales y después del cierre concurren para obtener evidencia suficiente de que dichos controles estuvieron vigentes durante todo el ejercicio y además realizarán las pruebas de los controles de aplicación.

5.3 - Necesidad de evaluar los controles generales y de aplicación de los sistemas informáticos de la entidad

Cuando el auditor va a realizar la auditoría bajo un enfoque de confianza, entonces tiene que corroborar si la información emanada de los sistemas informáticos es confiable. Para ello deberá evaluar los controles sobre los mismos, es decir realizar una evaluación de controles generales y de aplicación de los sistemas informáticos, para obtener evidencia válida y suficiente de que la información relevante que se presenta en los estados contables y que surge de los mismos, representa razonablemente la realidad de las transacciones. Es en este caso entonces que intervienen los expertos en sistemas dada la necesidad de evaluar los controles.

5.4 - Objetivo del trabajo del especialista

El auditor solicita al experto que realice una evaluación de los controles generales y los de aplicación de los sistemas informáticos para las auditorías de aquellas empresas que tienen todos o casi todos sus procesos automatizados, en especial aquellos de los cuales se deriva la información relevante que se plasma luego en los estados contables. Los controles a evaluar no son todos, son los relevantes para la auditoría y los define el auditor financiero, más allá de que luego el experto indique la necesidad de la evaluación de algún otro control, ya que el trabajo se realiza en forma coordinada. Con respecto a esto último en la evaluación de los controles generales hay más independencia, se sigue una metodología básica determinada en cada una de las firmas y luego a nivel de lo que son los controles de aplicación se trabaja en forma más conjunta con los auditores.

Los expertos no realizarán una evaluación de los sistemas informáticos utilizados por la entidad, sino que el alcance de su trabajo se limitará a evaluar los controles que le indique el auditor y tampoco brindarán certeza sobre las funcionalidades de los sistemas, sino que su opinión se limitará a establecer si las mismas funcionan eficazmente para los fines de la auditoría.

En resumen, la evaluación de los controles generales y de aplicación de los sistemas informáticos de la entidad auditada, será entonces el trabajo a desarrollar por el experto con el objetivo de llegar a una conclusión sobre si los mismos son efectivos o inefectivos y esto es esencial para una auditoría con enfoque de confianza en los sistemas informáticos, sobre todo en aquellos casos de alta dependencia de TI con respecto a sus procesos relevantes que puedan impactar en los estados contables.

5.5 - Desarrollo del trabajo del especialista

El trabajo a realizar por el especialista también implica una serie de etapas, como planificación, ejecución de los procedimientos a desarrollar y tareas finales donde realizará la evaluación de los resultados obtenidos, estas grandes etapas no varían según las características de la empresa auditada. El especialista deberá documentar todo lo realizado en las distintas etapas del proceso: recopilación y evaluación de la información, resultados obtenidos, etc. en papeles de trabajo que serán entregados al auditor.

5.5.1 – Planificación

El experto obtendrá primero un conocimiento del negocio, el cual en primera instancia es proporcionado por los auditores contables que son los que realizan el primer contacto con el cliente y luego es complementado con la información que recaban ellos a través de Internet, Intranet y de entrevistas con el personal del área informática de la empresa auditada. No sólo recaban información del cliente en particular, sino también todo lo que tiene que ver con la industria a la que pertenece, por ejemplo todo lo relativo a normas o regulaciones específicas que puedan existir.

Planifican las entrevistas que realizarán al personal de la empresa auditada, fijándose un objetivo, siguiendo un programa de trabajo y utilizando el conocimiento del negocio que tengan hasta ese momento, de manera que nunca concurren a un cliente sin saber nada sobre él ni tener nada planificado. Los especialistas cuando concurren a la empresa en primera instancia solicitarán información inicial, incluyendo organigramas, cursogramas o flujogramas, porque si la empresa los posee serán de utilidad, pudiendo minimizar el tiempo

de las entrevistas, mientras que si no cuenta con los mismos, no se le solicitará a la empresa que los genere, sino que será el experto quien se encargará de realizarlos, por lo menos hasta el nivel que necesiten. Esta documentación básica, de ser proporcionada por la empresa, permite tener una primera aproximación para ir detectando deficiencias y así establecer puntos donde se deberá poner énfasis en el desarrollo del trabajo.

Si se trata de una auditoría recurrente, el experto observa qué es lo que cambió en la empresa con respecto al ejercicio anterior, qué sistemas implementó, cuáles dejó de usar y luego dependiendo de este conocimiento inicial va a realizar la planificación de su trabajo.

Los expertos solicitan solamente la información necesaria tratando de definirla claramente en forma previa, dependiendo de cada cliente. Solicitan niveles conceptuales de información tratando de no incomodar al cliente con averiguaciones de detalles específicos que no sean necesarios. Generalmente el cliente le brinda fragmentos o extracciones de temas puntuales y le otorga usuarios de consulta, nunca un usuario con atributos de administrador.

En conclusión para realizar una buena planificación, deberán hacer una investigación preliminar y algunas entrevistas previas así podrán desarrollar su programa de trabajo. Cada auditoría será planificada, pero siempre deben realizar procedimientos estándares y respetar normas locales e internacionales, así como guiarse por la metodología definida en su firma. En la planificación se establece cuándo realizarán la evaluación de los controles generales, cuándo la de los de aplicación, qué persona va a ir a hacer el trabajo, quién lo va a revisar, el tiempo estimado necesario para realizarlo y cuál es la fecha para entregar el resultado a los auditores.

5.5.2 – Ejecución

Los expertos siguen una metodología para llevar a cabo sus tareas, incluso utilizan software que los guían en la planificación, ejecución y en el llenado de los papeles de trabajo estándar.

Las tareas no sólo pueden ser realizadas dentro de la entidad auditada, sino también fuera de ésta, en las oficinas de la firma auditora si así lo permite el cliente, ya que existe un acuerdo de confidencialidad de la información en el cual el cliente puede establecer que la información no sea "llevada" fuera de la empresa, en este caso se trabajará sólo en las instalaciones de la misma. Cuando se trabaja fuera de la entidad los expertos encriptan la información que llevan en sus notebook para tenerla protegida. Lo ideal es desarrollar las tareas dentro de la empresa auditada para tener las respuestas a sus dudas en forma inmediata.

En la visita interina los expertos prueban los controles generales, evalúan el riesgo inherente y el riesgo de control para poder definir su estrategia, estableciendo el alcance de los procedimientos que llevarán a cabo luego en la visita final.

Los controles generales y de aplicación son distintos, pero no se puede hablar de que unos son más importantes que otros, la importancia siempre va en relación a los riesgos, no hay una única respuesta. El auditor comenzará siempre su trabajo evaluando los controles generales porque las aplicaciones se sustentan en una plataforma informática donde éstos deben estar siempre presentes, luego seguirá con su trabajo realizando la evaluación de los controles de aplicación.

En general la forma de proceder de los expertos es la siguiente: ellos solicitan los datos, o sea que no se conectan directamente a los registros de la empresa, sino que le piden al cliente que le baje los archivos. Prácticamente todos los

programas que usan las empresas pueden exportar la información a muchos formatos y entonces los expertos piden el formato que más le convenga, que puede ser Excel, un archivo de texto o una base de datos, de esta forma cargan los archivos en esas herramientas y los procesan de forma independiente, incluso trabajan en sus notebook y no en el equipo del cliente, por un tema de comodidad para ellos y más seguridad para la empresa auditada. Normalmente el cliente les otorga un usuario de consulta para poder ver lo que necesiten, por ejemplo si les interesa ver una factura en particular pueden hacerlo en cualquier momento.

5.5.2.1. – Evaluación de controles generales

Con respecto a la evaluación de los controles generales podemos identificar grandes áreas donde el experto realizará el desarrollo de su trabajo:

- Seguridad lógica.
- Seguridad física.
- Control de cambios e implementación de nuevos sistemas
- Control de operaciones.

Seguridad lógica

Algunos de los controles que serán objeto de evaluación dentro de esta área son:

- Evaluar cómo se realizan los procedimientos de creación y eliminación de usuarios, por ejemplo controlar que no existan usuarios en el sistema que correspondan a funcionarios que ya no integran la nómina de la empresa. Debe estar bien definido el o los responsables para estas tareas de creación y eliminación y deben ser los únicos autorizados a tal efecto.

- Verificar que los privilegios que posee cada empleado estén bien definidos, que sean razonables de acuerdo al cargo, que estén asignados a las personas correctas y por las personas autorizadas.
- Verificar que se lleve a cabo el monitoreo del trabajo realizado por los usuarios del sistema de la empresa, es decir corroborar la existencia de controles que servirán como pistas de auditoría que puedan ser revisadas luego.
- Verificar que no cualquiera pueda modificar los datos y que quien lo haga sea la persona autorizada.
- Verificar la existencia de parámetros que se configuran en las aplicaciones, para poder implementar controles que impidan el acceso a la información a personas no autorizadas.

Seguridad física

Con respecto a la seguridad física, se deberá evaluar:

- Que el centro de cómputos se encuentre cerrado, que presente buenas condiciones ambientales, tales como aire acondicionado, una correcta instalación eléctrica, detectores de fuego, extintores, etc.
- La existencia de un plan de contingencias.

Control de cambios e implementación de nuevos sistemas

Dentro de esta área el experto deberá corroborar la existencia de los controles que deben hacerse antes de realizar una modificación en un sistema actual o para incorporar sistemas nuevos:

- Comprobar que los cambios sean aprobados por las personas responsables.
- Corroborar que las modificaciones o nuevos programas hayan sido probados antes de su implementación, deberán verificar que se hicieron las pruebas y se documentaron.
- Verificar que hayan ambientes separados, uno donde estén los sistemas funcionando y otro donde se hace el desarrollo y la prueba.
- Corroborar la segregación de funciones en el proceso, es decir comprobar que quién hizo ese pasaje de producción, no sea la misma persona que pone a funcionar los sistemas, que los usuarios no autorizados no puedan realizar modificaciones y viceversa que quien realiza las modificaciones no sea luego un usuario que ingrese transacciones.
- Comprobar la existencia de monitoreo sobre los cambios efectuados.

Control de operaciones

Con respecto a las operaciones, deberán hacer hincapié en controlar:

- Los procedimientos de respaldos.
- La existencia de programas antivirus.
- Los procesos que se ejecutan, procesos que consoliden información, por ejemplo ver cómo se controla que todas las sucursales transmitieron toda la información, que las transacciones sean íntegras y que no exista duplicidad de las mismas.

Los controles detallados dentro de cada una de estas grandes áreas, son solo algunos ejemplos, el experto luego de realizar los procedimientos sobre los controles que crea conveniente, realizará una evaluación de si éstos son efectivos o inefectivos en función de los controles generales existentes y de los riesgos que

estén involucrados tratando de ver si existe un nivel de riesgo razonable, o sea que no hayan deficiencias significativas que puedan llegar a impactar en la integridad de los datos.

5.5.2.2. – Evaluación de controles de aplicación

Dentro de los controles de aplicación también podemos identificar diferentes tipos: controles de entrada, de procesamiento y de salida.

El experto en general se enfoca en los controles de procesamiento, por ejemplo verificación del funcionamiento de los sistemas por medio de recálculos, como lo es recalcular la diferencia de cambio, la previsión por incobrabilidad, la previsión por obsolescencia, etc. y de esta forma comparar con los saldos emitidos por el sistema contable de la empresa, para ello los expertos solicitan los datos al cliente y hacen el cálculo por su cuenta. Otro ejemplo es probar las interfases de los sistemas integrados realizando la verificación de la integridad de la información.

En el caso particular de los controles de aplicación el auditor intenta definir lo más detallado posible qué es lo que quiere probar, por lo tanto se trabaja más en conjunto con los expertos ya que no todas las empresas son iguales y no todas utilizan los mismos sistemas, de forma tal que deben definirse para cada caso las pruebas a realizar. Los controles de aplicación se realizan básicamente para aquellas transacciones rutinarias y de gran volumen. Los procedimientos de auditoría más utilizados por el experto para llevar a cabo su trabajo son la observación, la indagación y el recálculo.

Luego de llevar a cabo las pruebas sobre los controles de aplicación el experto comunicará sus conclusiones al auditor y éste evaluará si las pruebas realizadas le

permiten tener evidencia suficiente para poder determinar la efectividad de los controles, en caso contrario puede solicitarle pruebas adicionales al experto, ya que es el auditor quien decide si las pruebas fueron suficientes o no para la auditoría.

Conclusiones sobre la evaluación de los controles

El fin último del trabajo del experto es llegar a una conclusión de si los controles son efectivos o inefectivos, que en definitiva es la información que le fue solicitada por el auditor. Llegado a este punto podemos encontrar diversas situaciones, como por ejemplo tener efectividad en ambos tipos de controles o efectividad en una de las categorías e inefectividad de controles en la otra.

El hecho de evaluar primero los controles generales hace que se minimicen los tiempos, ya que una conclusión de efectividad de estos controles hará reducir luego las pruebas sustantivas sobre los controles de aplicación.

Dada la característica de uniformidad de los programas que procesan consistentemente la información, si se prueba que un control general es efectivo, por ejemplo que en el año la posibilidad de que los datos sean modificados sin autorización o la posibilidad de que un programa esté fallando sea baja, entonces se podrá reducir la cantidad o el alcance de las pruebas sobre los controles de aplicación.

Si se tiene un procedimiento de aplicación de cambios donde éstos fueron probados, los usuarios finales los validaron, se documentaron y fueron autorizados por el negocio, es muy poco probable que exista un cambio que se haya introducido en un programa que tenga posibilidad de fraude o de error operativo que genere un impacto en la contabilidad.

Tener confianza en los controles generales implica darle un grado mayor de confianza a la información, para evitar la posibilidad de hacer más procedimientos de integridad, por ejemplo en un auxiliar de ventas en vez de hacer pruebas de integridad como tomar las facturas manuales y ver si todas están en el reporte, ese paso se podrá llegar a omitir por tener confianza en los controles generales, entonces lo que se logra es hacer más eficiente el trabajo tratando de insumir la mínima cantidad de horas y de mantener controlado el riesgo de auditoría.

En resumen, durante la etapa de ejecución los expertos evaluarán en primer lugar los controles generales y luego los de aplicación y a medida que vayan llegando a conclusiones de efectividad o inefectividad de un control, irán comunicando estos resultados al auditor junto con toda otra información recabada por ellos que consideren relevante para la auditoría. Es muy importante la oportunidad de la información, debido a ello el trabajo del experto se desarrolla en forma coordinada con el auditor contable.

5.5.3 - Uso del informe del especialista

El resultado de su trabajo debe ser comunicado a los auditores en la medida que vayan evaluando los controles, más allá de la realización de un informe y de tener la obligación de ir dejando plasmado el desarrollo de sus procedimientos en papeles de trabajo. Cuando detectan algún riesgo y ven que no existen controles suficientes, informan cuanto antes al auditor para que él pueda definir una estrategia adecuada y no avisar sobre el final de la auditoría que un control era inefectivo, porque se podría llegar a la conclusión de que el alcance de los procedimientos realizados fue inadecuado, lo que puede implicar más trabajo

para el auditor. Pero más allá de esto, el experto de todas formas tiene que cumplir con las formalidades de la documentación de su trabajo y de su informe. Saber oportunamente si el control es efectivo o no, es muy importante para la auditoría. Si los controles generales que se evalúan primero llegasen a ser evaluados como ineficaces, entonces tampoco se podrá confiar en los controles de aplicación. La idea es tratar de que la comunicación sea fluida pero evitar que sea inestable, por lo tanto deben informar con cautela sobre los avances obtenidos.

Más allá de todo esto existen ciertas normas de documentación que están definidas internamente en cada firma y los expertos tienen que cumplir con la parte formal de documentar su trabajo que va a depender de las exigencias particulares de cada una, pero sí es claro que ese informe no lo dejan para el final sino que existe una continua comunicación e interacción entre auditor contable y especialista en sistemas y los resultados obtenidos los van dejando documentados en papeles de trabajo que luego el auditor utilizará para dejar evidencia de las tareas realizadas. En la práctica existe una fluida comunicación entre auditor contable y especialista, coinciden todos en que esta interacción es muy importante para que el auditor obtenga en forma oportuna los resultados a los que va arribando el experto sobre los controles, ya que a partir de ahí va a definir alcances de procedimientos, enfoque, etc.

Como conclusión podemos decir que la elaboración de un informe final no es una etapa tan definida, ya que el trabajo lo van documentando en la medida que realizan los procedimientos.

5.5.4 – Otras consideraciones sobre el trabajo del especialista

Normativa a aplicar

Los expertos deben basar su trabajo en determinada normativa, como por ejemplo el COBIT, si bien no realizan una auditoría basada en COBIT directamente, si lo hacen en forma indirecta ya que las metodologías de las firmas a las que pertenecen toman todo lo referente a COBIT así como a otros marcos de referencia de nivel internacional. Sus programas de trabajo respetan normas locales y del exterior. Más allá de sus metodologías definidas, en la práctica realizan una adaptación a las exigencias de cada cliente, ya sean corporativas o de un ente regulador tanto local como externo.

Un caso particular en Uruguay es el sistema financiero, que tiene como ente regulador al BCU, quien exige que los bancos apliquen COBIT. También exige a los bancos que realicen una revisión trienal del control interno y que cumplan una serie de estándares mínimos sobre resguardos de información, procesamiento externo, generaciones de información del BCU, particularidades del sistema contable, etc.

En resumen los expertos pueden adaptar su trabajo en relación a determinados marcos de referencia internacionales indirectamente, ya que éstos están tomados en cuenta en la metodología de cada firma y a su vez se adaptan a las exigencias de cada cliente. Por lo tanto el experto estudia cada caso para definir la normativa que debe aplicar y las adaptaciones particulares que deba realizar a su programa de trabajo.

Tiempo insumido en el trabajo del experto

El tiempo requerido por los especialistas para el desarrollo de sus tareas es muy variable, se espera que su trabajo simplifique las tareas del auditor financiero y de

esta forma lograr una reducción significativa de horas en el total de la auditoría. El tiempo insumido depende de cada cliente, algunos de los factores que inciden son:

- Si es primera auditoría o es recurrente.
- El tamaño de la empresa y el grado de dependencia de TI de aquellos procesos que sean relevantes para la auditoría de estados contables.
- La existencia de controles particulares, lo cual depende del rubro de la empresa, ya que pueden existir normas específicas debido a algún ente regulador.
- El alcance de los procedimientos a realizar.
- De la evaluación de los controles realizada en años anteriores.
- El enfoque que vaya a realizar después el auditor.
- La evaluación del costo beneficio de aplicar un enfoque u otro.

La relación entre el tamaño de la entidad y el tiempo insumido no siempre es tan directa, el tamaño es un factor que debe observarse junto con el grado de dependencia de TI, ya que en las empresas grandes pero que tengan poca infraestructura de TI el tiempo insumido en la revisión de los controles puede ser inferior que en cualquier empresa de menor porte pero con alta dependencia de este tipo de tecnología.

Dos de los expertos estimaron que en una organización de computación dominante, la participación del personal de informática de la firma estaría entre un 10 y un 15% del tiempo total de la auditoría financiera.

Capítulo 6

6 - SITUACIONES CON CONTROLES GENERALES INEFECTIVOS

6.1- Problemática en los ambientes computarizados

Debido al uso de los sistemas informáticos han surgido riesgos específicos al control interno tales como:

- Dependencia de sistemas o programas mal diseñados.
- Acceso no autorizado a datos, esto puede provocar la pérdida de los mismos o cambios inapropiados, incluyendo el registro de transacciones no autorizadas o inexistentes, o registro inexacto de transacciones, por ejemplo si múltiples usuarios tienen acceso a una base común de datos.
- La posibilidad de que personal de sistemas obtenga privilegios de acceso más allá de los necesarios, fallando el principio de segregación de funciones.
- Cambios no autorizados a datos en los archivos maestros.
- Cambios no autorizados a sistemas o programas.
- Dejar de hacer los cambios necesarios a sistemas o programas.
- Intervención manual inapropiada.

- Potencial pérdida de datos o incapacidad de acceder a los datos cuando se los necesite. [34]

En una entidad donde sus procedimientos se encuentren altamente automatizados, abarcando casi todas las etapas de las diferentes transacciones (inicio, autorización, revisión, registro, proceso e informes), los registros en formato electrónico sustituyen documentos en papel por lo tanto han cambiado los procedimientos de control interno, surgiendo nuevos controles de seguridad para dichas transacciones y así el auditor ha tenido que cambiar también la forma de obtener la evidencia de auditoría.

Los procesos y controles automatizados pueden reducir el riesgo de error inadvertido pero no evitan el riesgo de que los usuarios puedan burlar estos procesos, por ejemplo pueden cambiar las cantidades que se pasan automáticamente al mayor general, entonces el auditor deberá hacer énfasis en verificar que no exista esta intervención manual cuando la información es transferida automáticamente en los sistemas informáticos.

Cuando la información contable de las entidades depende únicamente de los sistemas informáticos y más aún cuando no hay documentación de las transacciones, sino que éstas se realizan total o mayormente en forma electrónica, no hay otra salida más que establecer controles en los sistemas, ya que hay diversos factores de riesgo que podrían llegar a distorsionar la información, como los son:

- El riesgo de fraude por la intervención manual de algún miembro de la entidad en los sistemas informáticos.

[34] Fuente: IFAC, Ob. Cit., NIA 315, pág. 328.

- El riesgo de errores humanos con respecto a la entrada de datos o cambios no autorizados en los sistemas.
- El riesgo de que los sistemas no estén bien diseñados para los objetivos de la empresa y por lo tanto haya un procesamiento "erróneo" de la información.
- El abuso en la utilización de las computadoras.
- La posibilidad de pérdida de información.
- La necesidad de mantener la privacidad de la organización y de sus miembros ya que puede ocurrir un mal uso de la información.
- La toma de decisiones incorrectas.

Dentro de estos factores, el abuso en la utilización de las computadoras sería el principal disparador para el desarrollo de nuevos controles en los sistemas informáticos, mientras que los problemas que surgen de los errores, omisiones, o fraudes causan importantes pérdidas en una organización. [35]

6.2 - Controles generales inefectivos. Problemas detectados, fallas, causas

La efectividad o inefectividad de un control va a depender de ciertos factores entre los cuales podemos destacar los siguientes:

- el criterio que tenga el auditor,
- la situación en particular que estuvo presente durante el período auditado,
- el nivel de riesgo que se determine,

[35] Fuente: Echenique García, José Antonio, Auditoría en informática, Edit. McGraw Hill Interamericana, 2ª edición, año 2001, p.18.

- el peso que pueda tener cada control dentro de la organización y su impacto en la información relevante de los estados contables,
- la forma en que el auditor selecciona la muestra, el alcance de la misma y el grado de confianza que se desea tener,
- la existencia de otros controles que puedan mitigar las deficiencias del control evaluado,
- el peso de la suma de las deficiencias que pueda llegar a tener el control.

A la conclusión de efectividad o inefectividad de un control se llegará tomando en cuenta estos factores y evaluando cada control y su impacto. Un control puede estar funcionando con deficiencias, en tal caso nunca se califica como inefectivo sin antes evaluar de qué tipo de deficiencias se trata, si son relevantes o no, ya que los controles pueden funcionar con fallas, en una situación en la que se está ante un entorno en el cual hay deficiencias que son todas no significativas y cada una apunta a mitigar riesgos distintos de modo tal que la suma tenga un impacto no significativo, entonces se concluye al control como efectivo, mientras que en el caso contrario donde pueda tener deficiencias que a nivel individual son insignificantes pero que en la suma son significativas, entonces se concluyen como inefectivos, porque el impacto que pueda tener en los estados contables es un factor primordial a evaluar, ya que en definitiva se está trabajando en una auditoría contable.

Existen ciertos controles típicos que se encuentran implementados por lo general en todas las organizaciones, pero no existe una regla bajo la cual se catalogue a una categoría de controles como inefectiva, si se llega a comprobar que unos de esos controles no está funcionando, primero se deberá investigar si fue suplantado por otro control que mitigue los mismos riesgos, de lo contrario si el riesgo ha quedado descubierto, entonces si se podrá concluir sobre la inefectividad del control.

6.3 - Repercusiones de los problemas detectados

Cuando en una auditoría se llega a la conclusión de que un control general es inefectivo, lo que se está concluyendo en el fondo es que el cliente tiene un problema de control interno y a consecuencia de esto va a haber un impacto en el plan de auditoría definido por el auditor, ya que no podrá seguirse un enfoque de confianza en los controles, es decir que se está ante un problema tanto para el cliente como para la auditoría. El auditor deberá decidir qué hacer en consecuencia, ya que al tener controles generales evaluados como inefectivos, se deberá reforzar todo lo relacionado a la integridad y disponibilidad de la información. De esta forma se está ante una situación que impacta en la estrategia de los auditores de cómo seguir con la auditoria de EECC. Los profesionales de sistemas no se encuentran afectados en cuanto a esa ineficiencia de los controles, dado que quienes definen el alcance y los procedimientos que se realizan en la auditoría son en definitiva los auditores contables. Esta debilidad será incluida en la carta de comentarios a la gerencia, donde se informará la situación y se propondrá una recomendación.

6.4 - Posibles soluciones de controles inefectivos

El auditor financiero es quien deberá optar por las soluciones en los casos de controles generales evaluados como inefectivos, ya que esto impactará no solo sobre los controles que de alguna forma dependen de los controles generales, que son los controles de aplicación, sino también sobre los procedimientos de auditoría que se lleven a cabo, ya que se deberá reforzar las pruebas a realizar.

El auditor en consecuencia puede cambiar el enfoque de la auditoria pasando a realizar un enfoque sustantivo, ya que no podrá basarse en la confianza en los controles debido a la ineficacia de los mismos. Esto traería como consecuencia un mayor esfuerzo para la auditoría, ya que deberán realizarse mayor cantidad de pruebas sustantivas, también puede cambiar el alcance de los procedimientos, la desventaja de todo esto es el mayor costo de recursos insumidos en la auditoría.

Como conclusión a este punto podemos decir que el auditor ante una situación con controles generales inefectivos, deberá realizar pruebas sustantivas para intentar reunir evidencia suficiente sobre la razonabilidad de la información financiera que luego se vuelca en los estados contables, si con esto tampoco lo consigue, entonces el auditor deberá evaluar el impacto sobre los estados contables, de forma que podrá llegar a limitaciones en su opinión o en el caso extremo a una abstención de dictamen.

Capítulo 7

7 - ROTACIÓN DE CONTROLES EN AUDITORÍAS RECURRENTES

7.1 - Auditorías recurrentes en empresas

En general en nuestro país las auditorías son recurrentes, porque es práctica común del mercado de las auditorías externas que se negocie de esta forma con el cliente, uno de los motivos es que en el primer año el trabajo lleva mucha inversión en adquirir conocimiento de la entidad auditada, entonces lo típico es el caso de que las firmas de auditores cuenten con clientes a los que se concurre todos los años a realizar la auditoría.

7.2 - Necesidad de rotación de controles en la planificación de la auditoría recurrente

En las auditorías recurrentes en general lo primero que realiza el experto es ver qué cambios hubo en el área informática, deberán determinar si se implementó un sistema nuevo, si dejó de usar alguna aplicación, si siguen usando los mismos sistemas, entre otros aspectos a considerar y luego observan si los controles que

hicieron el año anterior siguen vigentes. Si se trata de un control que ya probaron, solicitan la información y la procesan porque ya cuentan con los programas para ello y tienen todo documentado y de esta forma es más fácil repetir las pruebas, ya saben qué hay qué pedir, saben cómo controlarlo, más allá que siempre hay que hacer alguna prueba adicional, sobre todo si se implementó un sistema nuevo hay que ver qué funcionalidades tiene, pero siempre las auditorías recurrentes son más fáciles de realizar, implican chequear que lo probado el año anterior continúe vigente. En general la auditoría finaliza con recomendaciones que el cliente después puede implementar o no, entonces en la auditoría del año siguiente se realiza un seguimiento de esas observaciones hechas anteriormente para ver si se corrigieron y en el caso de un cliente nuevo que fue auditado por otra firma, en general se piden los últimos informes de auditoría y se estudian las observaciones y se corrobora si se corrigieron.

En cada firma de auditoría poseen una metodología de trabajo definida, por lo tanto los auditores y los expertos deberán respetar los lineamientos especificados en ella, hay firmas que ya establecen que los controles no se rotan, definen una determinada categoría de controles básicos los cuales prueban siempre todos los años, mientras que en otras firmas se puede manejar la posibilidad de rotarlos.

El hecho de poder rotar los controles, podría tener la ventaja de no acostumbrar al cliente a probar siempre los mismos, de tal forma que se realiza una planificación en base a una rotación de controles, pero esta situación puede tener como desventaja el riesgo que se corre al dejar de probar un control básico, por lo tanto se debe ser muy cuidadoso en este punto, de tal forma que en la elección del nuevo control a probar se opte por otro que mitigue el mismo riesgo que el control que se deja de probar o por lo menos verificar que cubra un nivel de riesgo razonable.

Capítulo 8

8 - CONCLUSIONES FINALES

En la actualidad las empresas tienden a desarrollar la totalidad de sus procesos en entornos computarizados, aunque no todos son entornos complejos. En general éstos últimos se relacionan con empresas de grandes volúmenes de transacciones, por lo tanto cuando se lleva a cabo una auditoría de estados contables en esta situación, el auditor aplicará un enfoque de confianza ya que no es viable la aplicación de un enfoque sustantivo, lo cual determina que en estos casos siempre va a ser necesario realizar un análisis de los controles presentes en el área informática, en particular aquellos que estén relacionados con la fuente de la información relevante para la elaboración de los estados contables, por lo tanto deberá llevarse a cabo una evaluación de dichos controles para que el auditor pueda sustentar un enfoque de confianza.

Para realizar el análisis y la evaluación de los controles que la empresa efectúa sobre los sistemas informáticos, los auditores requieren el apoyo de especialistas en sistemas, debido a que ellos no poseen los conocimientos necesarios para llevar a cabo dicho análisis dada la complejidad del caso. De esta forma se podrá lograr un conocimiento adecuado de la entidad y su entorno para poder cumplir con la normativa vigente al respecto. Esto lleva a que hoy en día las firmas de auditoría cuenten con un departamento de tecnología de la información a cargo de especialistas en informática para auxiliar al auditor en el desarrollo de su trabajo.

En una empresa pueden estar funcionando un gran número de controles en el área informática, pero no todos serán objeto de estudio para la auditoría, sino que solo se evaluarán aquellos que le interesen al auditor, es decir aquellos que mitiguen riesgos importantes y que en el caso de llegar a ser inefectivos o directamente de no estar funcionando, causen un impacto relevante en la información presentada en los estados contables.

Los controles que el auditor solicita al especialista que evalúe, se dividen en dos grandes grupos: controles generales y controles de aplicación. Según la información recabada en las entrevistas podemos concluir que el especialista realiza la evaluación de los controles generales en forma más independiente con respecto a la forma en que evalúa los controles de aplicación, ya que cada firma cuenta con una serie de controles generales estándar, considerados fundamentales para la auditoría. Mientras que los controles de aplicación son más específicos de cada empresa ya que dependen de los sistemas utilizados por ésta, por lo tanto habrá una solicitud expresa del auditor en cuánto a cuáles serán los controles de aplicación que necesita que el experto analice.

La profundidad del análisis y el aprovechamiento del uso del experto dependerán de las características de la propia entidad que se está auditando y del criterio del auditor, ya que es él quien va a determinar el enfoque y el alcance de los procedimientos a aplicar, por lo tanto va a diferir según el cliente, la dependencia de TI que tenga, las aplicaciones que utilice, el funcionamiento del control interno y del riesgo de auditoría determinado. En entornos altamente computarizados, para aquellos controles automatizados que funcionan en forma consistente tanto para una o para miles de transacciones, no va a ser necesario incrementar el alcance de las pruebas sobre dichos controles, ya que éstos funcionan de forma uniforme. En esta situación, si el auditor llega a la

conclusión de que un control es efectivo, entonces posteriormente solo alcanzará con probar que continúa funcionando de esta manera.

Luego de que el auditor profundiza en el conocimiento del negocio, más específicamente en cuanto al área informática, es cuando va a determinar cuáles son los controles de aplicación que le interesa sean calificados como efectivos o inefectivos, para ello solicitará al experto la evaluación de los mismos y determinará qué controles se van a probar, cuál es el alcance y la oportunidad de las pruebas a realizar.

El experto a medida que vaya llegando a conclusiones de efectividad o inefectividad, comunica los resultados al auditor ya que el trabajo lo irán realizando en forma coordinada y manteniendo un continuo contacto, sobre todo en lo que respecta a los controles de aplicación, de todas formas el especialista deberá cumplir con aspectos formales de presentación de su informe.

Luego de conocer el resultado de las evaluaciones realizadas por el experto, el auditor deberá realizar un estudio de aquellos casos donde se está frente a un control inefectivo, de manera de poder buscar posibles soluciones ante este tipo de situaciones. El auditor tendrá que ver hasta qué punto existen controles compensatorios o determinar si es posible realizar pruebas sustantivas para soportar la opinión, o de lo contrario evaluar la falta de evidencia y ver cómo impacta en el informe, en el contexto global del proceso de formación de opinión. Concluimos de esta forma que el auditor ante la falta de evidencia de auditoría causada por la inefectividad de un control deberá buscar caminos alternativos, verificará si existe algún tipo de evidencia de controles compensatorios que mitiguen el mismo riesgo y ante la inexistencia de los mismos deberá determinar el impacto sobre la información contenida en los estados contables, si este no es material dicha situación no influirá en su opinión. Una vez realizado el análisis,

si el auditor concluye que no existe ninguna posible solución y que el impacto en dichos estados es material, tendrá que considerar la eventual limitación por tener falta de evidencia y probablemente llegue en la mayoría de los casos a una limitación, que en un caso extremo podría llegar a convertirse en una abstención.

Con respecto a la rotación de controles en auditorías recurrentes, podemos concluir que ésta es más frecuente en las pruebas de evaluación de los controles de aplicación que en las pruebas de controles generales, ya que las firmas poseen una lista de controles generales estándares los cuales llevan a cabo con regularidad, además el hecho de rotarlos puede tener más desventajas que ventajas, por lo tanto la decisión de no realizar un rotación de controles sería un criterio más conservador. También en este punto podemos agregar que este tema no está muy claro en la normativa vigente, por lo tanto dependerá del criterio del auditor y de la metodología de cada firma.

En este tipo de entorno cada entidad tiene definida una serie de controles generales, de esta forma el auditor seleccionará aquellos que considere importante evaluar y año a año el trabajo del experto en este punto consistirá en verificar que dichos controles continúen siendo efectivos, para que de esta manera el auditor pueda tener la evidencia necesaria y pueda confiar en los mismos.

La rotación de controles tiene la ventaja de no acostumbrar al cliente de lo que se va a probar, para evitar esto es conveniente agregar algún control más que rotarlos, ya que con la rotación se corre el riesgo de dejar de probar controles que realmente resultan de suma importancia para el auditor. En el caso de que las firmas de auditoría tomen la decisión de rotar alguno de los controles generales a evaluar, podría resultar en un riesgo de impacto relevante en la información contenida en los estados contables, ya que el control que se deje de probar puede

volverse inefectivo, lo cual provocaría un riesgo al auditor en cuanto a la opinión que pueda llegar a emitir.

Como conclusión a este tema podemos decir que si bien en algún caso se podría rotar algún control general, sería preferible o aconsejable no realizar la rotación ya que se puede incurrir en riesgos, si de todas formas el auditor decide cambiar la evaluación de un control por otro, deberá hacer hincapié en verificar que el nuevo control a evaluar mitigue los mismos riesgos.

Anexo 1

A.1 – Entrevistas realizadas a expertos en sistemas

1. ***Cuando un auditor solicita su apoyo para una auditoría, ¿cuál es el objetivo de su trabajo?***

Según las respuestas de los tres profesionales el trabajo consiste en probar los controles de los sistemas informáticos, ya sea de los generales como también de controles más específicos denominados controles de aplicación. Evalúan los controles haciendo el testeo de los mismos para llegar a la conclusión de si éstos son efectivos o no, que es en definitiva lo que le interesa al auditor. Hay controles que siempre se evalúan y otros que el auditor solicita específicamente que sean probados.

2. ***¿Realiza una evaluación del negocio o estos datos se los proporciona el auditor?***

Coinciden en que se dan las dos cosas, van a tener el conocimiento del negocio que les proporciona el auditor financiero y a realizar un relevamiento por su cuenta. En general parten de la base de lo que ya relevaron los auditores contables, que son quienes tienen el primer contacto con el cliente y luego a partir de ese conocimiento profundizan en aquellas áreas que son más críticas.

Además depende de cada cliente, del grado de dependencia de TI que ellos tengan. Para los clientes más dependientes donde aparece un riesgo informático importante, como por ejemplo los bancos, puede ser que se requiera su intervención en la etapa del conocimiento del negocio, incluso si ellos detectan consideraciones de la empresa que puedan llegar a

impactar en el control interno desde el punto de vista de los sistemas informáticos, lo deben comunicar de inmediato al auditor.

Uno de los expertos se extendió en explicarnos cómo consiguen la información, es decir aparte de lo que ya relevaron los auditores, en el caso de que sean clientes nuevos hay mucho lugar donde buscar información, sobre todo empiezan por Internet donde pueden conocer mucho sobre lo que expresa el propio cliente y además información de la industria a la que pertenece, también esta información pueden extraerla de la Intranet global con la que cuenta la firma, es decir bases de conocimiento a nivel internacional. Hay muchos temas que hay que conocer, no sólo la parte informática, ésta solo tiene sentido en función de todo lo demás, entonces el gerente de sistemas deberá tomar conocimiento de todo el entorno para saber dónde poner énfasis.

3. ***¿Es una exigencia poseer algún conocimiento contable para llevar adelante su trabajo? Si es así, ¿la firma para la cual trabaja lo ha capacitado en temas contables?***

Poseer un conocimiento contable es esencial para lograr la comunicación con el auditor financiero y para entender el objetivo del trabajo, por ejemplo cuando se les solicita que evalúen controles específicos: ver cómo la empresa realiza una diferencia de cambio, cuál es la rotación de inventarios, etc.

El ingeniero de sistemas no tiene un perfil contable, ya que en esta carrera no tienen por ejemplo materias como control interno, auditoría de estados contables, etc., entonces el conocimiento contable lo han adquirido mediante capacitación en las propias firmas y con la experiencia adquirida durante el desarrollo de sus trabajos, coincidiendo los tres que la experiencia es muy importante. Uno de los expertos incluso nos habló de que el personal del área contable también debe poseer conocimientos de sistemas, los cuales se adquieren también a través de la capacitación y la experiencia en la propia firma.

4. ***¿Su trabajo es totalmente independiente del que realiza el auditor presentándole sólo el informe al final del mismo?***

En general el trabajo lo realizan en forma coordinada, muchas veces en conjunto que es lo ideal, donde la comunicación es fluida y permanente.

Uno de los profesionales agregó que en ocasiones se trabaja en forma más independiente, es en el caso de los controles generales que ya de antemano saben que siempre deben ser evaluados. Con respecto a los controles específicos el trabajo se realiza en continuo contacto con los auditores ya que necesitan este resultado a la brevedad, muchas veces la interpretación de resultados no solamente la gente de informática la puede realizar, sino que depende del auditor ver si ese resultado es importante, si es material o no, por lo tanto con respecto a los controles de aplicación se trabaja más en conjunto.

5. ¿En qué momento del proceso de la auditoría intervienen?

Según las respuestas el trabajo del experto se realiza en dos instancias, la primera en lo que se denomina visita interina, donde concurren a las oficinas del cliente antes de la fecha de cierre y en una segunda instancia luego del cierre del ejercicio.

En la primera instancia realizan la evaluación del control interno, se testean los controles generales, se analizan y evalúan los riesgos, el inherente y el de control y en base a esto se establece la naturaleza y el alcance de los procedimientos que se realizarán en la visita final, luego del cierre del balance.

Con respecto a los controles generales, éstos se prueban en la primera instancia, ahí se revisa también si estuvieron vigentes desde el inicio del ejercicio hasta esa visita interina (por ejemplo hasta setiembre) y después en la segunda visita (mes posterior al cierre) alcanza con hacer un seguimiento menor para obtener evidencia de si los mismos estuvieron vigentes durante todo el año (hasta el cierre) y si se comprueba esto entonces se calificará al control como efectivo, pues no sirve de nada un control que se implemente a la mitad del ejercicio, al final o que se haya dejado de usar.

En la segunda instancia, en la visita final, además de los controles mencionados anteriormente se realizarán en su mayoría las pruebas de los controles de aplicación porque hay que trabajar sobre balances ya definitivos.

6. ***¿Realiza una planificación del trabajo o cuenta con una guía escrita proporcionada por la firma para la cual trabaja?***

El hecho de trabajar en firmas internacionales implica que tengan que seguir una metodología definida y guiarse por normas internacionales que respetan las normas locales, pero que dan un marco profesional para realizar la auditoría, eso también incluye regulaciones específicas no solo para el auditor financiero sino también para el personal de sistemas, es decir que existe una metodología global dentro de cada firma, está todo predefinido, incluso papeles de trabajo estándar que tienen que llenar. Lo básico está estipulado internacionalmente, incluso cuentan con herramientas de software que los van guiando en la ejecución.

Existen procedimientos estándares y específicos que deben realizar, determinadas pautas y normas que hay que respetar, pero al igual que los auditores contables, los expertos también tienen que realizar una planificación del trabajo y lo hacen en coordinación con ellos.

Se planifica siempre en cada auditoría. La planificación es muy importante y la coordinación de las visitas con el cliente también, ya que siempre hay que ver si la persona de sistemas está disponible y coordinar las entrevistas haciendo los contactos con anticipación. Hay otro factor importante que influye en la coordinación de las visitas al cliente y es que la gran mayoría de las empresas cierran balance al 31 de diciembre, por lo tanto realizar una planificación adecuada es sumamente importante para poder cumplir con todos los compromisos.

7. ***¿Cuáles son las etapas de su trabajo? ¿Varían según las características de la empresa auditada?***

Coinciden en que el trabajo se desarrolla en grandes etapas y que no varían según las características de la empresa.

Nos hablaron de una etapa de conocimiento del negocio, luego viene una etapa de planificación básica y por último la etapa de ejecución de esos controles donde irán comunicando en forma continua los resultados al auditor.

8. ¿Algunos de estos pasos pueden ser llevados a cabo fuera de la entidad auditada?

Sí, coinciden en ello aunque la teoría dice que deberían trabajar en las oficinas del cliente, hay casos en que físicamente trabajan en sus propias oficinas, no es lo ideal, pero como muchos de los controles que hacen se basan en información que les da el cliente y que la procesan en sus equipos, entonces da lo mismo que trabajen en un lugar o en otro.

Coinciden en que es más práctico realizar el trabajo en la entidad auditada, porque de esta forma pueden evacuar las dudas en el momento consultando con las personas adecuadas, como por ejemplo los usuarios del sistema. También depende de cuán complejo es el procedimiento, si éste requiere una interacción continua con el cliente entonces va a ser necesario trabajar en las oficinas de éste. Si lo que se quiere es ver la configuración del sistema o la seguridad física de un centro de cómputos, entonces será imposible realizarla fuera de la entidad.

En esta pregunta dos de los expertos se extendieron sobre el tema de confidencialidad de la información, ya que ésta queda acordada previamente en la carta de compromiso, por lo cual cada vez que extraen información del cliente van a realizarlo a través de herramientas que encriptan la información, como mecanismo de seguridad ante robos de notebook, que hacen que la información en los discos esté encriptada y así inaccesible si no se cuenta con la clave de usuario y la contraseña.

Tal es la preocupación del cliente por mantener la confidencialidad de la información, que hay quienes solicitan expresamente que la información no salga físicamente de la empresa, que se trabaje únicamente en las oficinas del cliente y como ejemplo nos comentaron de casos en que les hacen dejar las notebook en la empresa auditada o incluso trabajar solamente en las computadoras de la misma. En este punto uno de los expertos comentó que en su opinión esto es una utopía, ya que la mayoría de las empresas no están preparadas para la confidencialidad de la información, por ejemplo, no están preparadas para la protección de los puertos USB en donde cualquiera puede extraer información, tampoco están preparados para evitar que se conecte una red inalámbrica, o un ADSL móvil y directamente salir por Internet y extraer información. En realidad para cualquier empresa es mucho más fuerte lo formal que tiene su carta de contratación por la cual el auditor es responsable de tener prácticas adecuadas para mantener la confidencialidad.

El grado de sensibilidad con respecto a la información va a depender de cada cliente, del grado de confianza que se tenga en los auditores o de la experiencia previa que hayan tenido y del tipo de acuerdo que se haya hecho a nivel de gerencia, en el ejemplo de "no sacar información de la empresa", debe quedar previamente establecido en la carta de compromiso de auditoría, en ella hay párrafos que se refieren al uso de la información, la responsabilidad y al tema de la confidencialidad, el objetivo de todo eso es dejarlo acordado en lo previo.

9. ¿Existe alguna normativa en que deba basarse para desarrollar el trabajo, por ejemplo COBIT?

Los tres expertos se basan en la metodología y formas de trabajo que tienen definidas cada una de las firmas, entonces nos dicen que de alguna forma están alineados tanto a este marco de referencia internacional como a otros, porque las metodologías globales se basan en ellos, incluyendo COBIT. Realizan una auditoría basada en el programa de trabajo de cada firma que toma todo lo referente a este marco de referencia en lo que tiene que ver con controles y seguridad.

A su vez a dichas normas se suman después las exigencias específicas que podrá tener el cliente o los entes reguladores de su rubro, por ejemplo el caso típico en Uruguay es el

sistema financiero que está regulado por el BCU y éste exige que los bancos apliquen determinadas normas específicas, por ejemplo que el control interno en el área de TI en los bancos deberá ser evaluado en el marco del COBIT, pero como las metodologías utilizadas en las firmas se basan en dicho marco entonces se cumple con la exigencia. También para el caso de los bancos en particular el BCU pide que se realice la revisión del CI cada tres años, es decir una revisión trienal. A todo esto se agrega luego una serie de estándares mínimos, que son profundizaciones específicas, como por ejemplo sobre resguardo de información, procesamiento externo, generaciones de información del BCU, particularidades del sistema contable, o sea hay varias regulaciones y va aumentando el número de ellas y todas estas exigencias surgen a partir de la existencia de ente regulador.

Por otro lado también hay empresas que dependen de una casa matriz en el exterior, por lo tanto se estaría en un caso de auditoría regional o global, esto implica que estén sujetas a otras normas y otros requerimientos. De todas formas en la opinión de uno de los expertos, estos requerimientos son bastante menos de los que debe tomar en cuenta el auditor financiero.

10. Cuando se entrevista con el departamento de informática de la empresa auditada, ¿concurre con un cuestionario predeterminado para recabar la información básica?

Los expertos entrevistados nos mencionan que se basan en un programa de trabajo. En la firma a la que pertenece uno de los expertos lo común es que el personal nuevo realice un cuestionario para saber si cubre todo el programa de trabajo y usan ese cuestionario en las entrevistas, pero luego con el tiempo ya dejan de basarse en él, pues con la experiencia ya saben que tienen que cubrir una serie de puntos y cada integrante del equipo de sistemas realiza las entrevistas como les queda más práctico, pero siempre basándose en el programa de trabajo.

En otra de las firmas se cuenta con una guía, por lo menos de controles generales, pero tampoco es una guía encasillada, hay clientes donde hay preguntas que hay que hacer sí o sí,

pero en otros clientes esas preguntas no son relevantes, ya que algunos son más dependientes de TI que otros.

El otro experto nos habla de que hay un fuerte trabajo para organizar y planificar una entrevista, donde se utiliza el conocimiento del negocio que realizó el auditor financiero más toda una serie de investigaciones sobre el caso, para tener un punto de partida de forma tal que nunca se concurre a un cliente sin saber nada sobre él, ni tener nada planificado.

En resumen, los expertos realizan una planificación de su trabajo obteniendo información de muchas fuentes, utilizando lo relevado por auditores financieros, Internet, Intranet, etc. y siguen un programa de trabajo definido en cada una de las firmas.

11. ¿También necesita recabar información en algún otro departamento distinto al de informática?

Los tres expertos concuerdan en que es necesario recabar información en otras áreas, una posibilidad es cuando los expertos participan junto con los auditores en el entendimiento del negocio, o sea cuando aparece un lenguaje técnico que ellos no pueden entender, lo que se da mucho en empresas tecnológicas, también puede ocurrir que se tenga que ir a otras áreas ya que si bien muchas organizaciones tienen departamentos de informática, no siempre éstos gestionan todos los recursos de sistemas.

Para los controles generales basta con relevar el área informática, en cambio para la parte de los controles de aplicación muchas veces depende del propio usuario y no tanto del área de sistemas, por ejemplo ciertos controles que el experto hace con los datos del sistema muchas veces le tiene que solicitar a los usuarios que le ejecuten ciertos reportes o consultas, entonces en definitiva son los propios usuarios quienes les brindan la información y ni siquiera tienen que ir al área de informática. Además muchas veces este departamento se encarga de la compra de los paquetes de informática, los instalan, les brindan luego el soporte pero no saben nada del paquete en sí, entonces cuando el experto tiene alguna duda sobre el programa deben consultar a los propios usuarios o recabar información con los proveedores del mismo.

12. ¿Solicita algún tipo de documentación a la empresa, como por ejemplo organigrama, cursograma o flujograma?

Los tres expertos nos manifestaron que si realizan un pedido de documentación, ellos comienzan su trabajo con una solicitud de información inicial y en general muchas cosas las piden en papel porque de esta forma pierden menos tiempo en las entrevistas, entonces por ejemplo, en lugar de que le tengan que explicar la estructura de un departamento y los roles de cada uno de los integrantes, le proporcionan un organigrama y así podrán tener una primera aproximación de cómo está estructurada la entidad e ir detectando deficiencias. Todo este tema de la documentación es muy variado, por ejemplo hay empresas que están dentro del proceso de calidad ISO y entonces tienen sus procesos todos documentados, con registros precisos, auditados y otras que no cuentan con algo así.

13. ¿Es común que las empresas le proporcionen abiertamente toda la información requerida por usted, o suelen presentársele trabas a su trabajo?

Los tres profesionales coinciden en que depende de la sensibilidad que tenga el cliente, hay clientes que son más sensibles que otros al momento de brindar la información, de la misma forma hay información que es más sensible y las empresas no quieren entregarla, sobre todo cuando se revisa la seguridad de los sistemas donde entran en juego las contraseñas y los permisos para navegar en los mismos. Uno de los expertos ejemplificó la situación diciendo que las direcciones de IP de la red, que es algo muy específico, como no se requiere conocerlas entonces esa información no la piden y sería un riesgo de seguridad para la empresa brindarla a terceros.

Buscan siempre tener una comprensión de cómo es la arquitectura de red, cómo es su ubicación geográfica, las conexiones, servidores y demás, pero prefieren no tener informaciones muy específicas que pudieran ser utilizadas por hackers, solicitando por este motivo niveles más conceptuales de información.

14. ¿Cuánto es el tiempo promedio estimado para llevar a cabo su trabajo?

Las tres firmas concuerdan que el tiempo promedio estimado para realizar el trabajo es muy variable. El mismo depende de cada cliente, si se encuentran ante una primera auditoria o si es recurrente, si las empresas son grandes o chicas, si hay controles específicos o no, así como también del alcance de los procedimientos a realizar, de la efectividad de esos controles probada en años anteriores y del grado de dependencia de TI de dichas empresas.

Con respecto al tamaño de la empresa nos aclaran que si bien hay una relación entre tamaño y tiempo, a veces no es tan directamente proporcional, pues se puede tener el caso de empresas que son grandes pero no tienen una gran infraestructura de TI, porque no es dependiente de TI en gran medida, por ejemplo un frigorífico y en este caso por mayor que sea la infraestructura el tiempo insumido puede ser mucho menor que en otras auditorías de empresas medianas con computación dominante.

Uno de los expertos nos expresó que para trabajos chicos y que se realizan en forma recurrente, alcanza con la participación de ellos en un día de trabajo, donde pueden realizar una actualización de un trabajo anterior, pero solo si la empresa es chica y solo ven lo general y algún control específico, para clientes grandes su trabajo podría llegar a una semana y ante clientes grandes donde se esté realizando una auditoria por primera vez su participación puede llevar un tiempo estimado de 2 a 3 semanas, ya que en este último caso se prueban muchos controles que después al año siguiente se evalúan en forma más rápida y automatizada.

Los otros dos expertos estimaron, sólo como pauta, que en una organización de computación dominante la participación del personal de informática de la firma estaría entre un 10 y un 15% del tiempo total de la auditoria financiera.

15. ¿Tiene la misma importancia la evaluación del hardware que la del software?

Los tres expertos coinciden en que se le da más importancia al software, en el sentido de que se tiene más interacción con el auditor financiero y con la información que él utiliza, se controla todo lo que es software y datos. En el hardware no hay mucha variante, en general cuentan con buenos equipos, sólo depende de cómo se configuren los sistemas operativos, las redes y las aplicaciones sobre ellos.

Todas las empresas trabajan con plataformas que de alguna forma son similares, por ejemplo el AS 400 tiene desde el punto de vista de seguridad lógica una gran cantidad de atributos y de parámetros configurables que permiten establecer controles como contraseñas, controles sobre permisos de auditoría, que permiten registrar los accesos dentro de los archivos de bibliotecas de datos. El AS 400 permite hacer un monitoreo más estricto, hay otras plataformas que también tienen estos atributos como las que usan UNIX, LINUX y también WINDOWS, éste en las últimas versiones incorpora elementos de seguridad más interesantes y está claro que el software funciona para determinadas plataformas y ahí es donde se relaciona indirectamente con el hardware.

El foco del trabajo del experto no es determinar si el hardware es adecuado o no para las necesidades del negocio, esto no está dentro de los objetivos, ya que desde el punto de vista contable no tiene influencia.

De la misma forma expresaron que de encontrar algún tipo de riesgos, como por ejemplo la obsolescencia en los equipos que pueda llegar a comprometer a la entidad o que sea significativo para la misma, será incluida en la carta de recomendaciones para evitar que se llegue a situaciones extremas.

16. ¿Se le pide a Ud. que evalúe la existencia de un plan de contingencias, o dicha evaluación la realiza el auditor?

Dos de las firmas expresaron que la evaluación de un plan de contingencias es una tarea propia del experto y no del auditor financiero. Dicho plan está atado al tema de la continuidad del negocio el cuál a su vez se relaciona con la disponibilidad de la información.

El plan de contingencias no es un requisito que los auditores establezcan para determinar la efectividad o no de los controles generales, es un elemento más que se evalúa y del cual surgen comentarios al respecto. Es más, no todas las empresas tienen un plan de contingencia bien diseñado incluso no todos tienen uno, la mayoría utilizan procedimientos de respaldos para cubrirse ante situaciones y dependerá de cada situación cómo se maneja.

17. ¿Cuáles son los controles generales que evalúa? ¿Y cuáles son los de aplicación? ¿Se les asigna más importancia a unos que a otros?

Uno de los expertos nos respondió que los controles generales se dividen en cuatro grandes áreas que son: seguridad lógica, seguridad física, control de cambios e implementación de nuevos sistemas y operaciones.

Con respecto a la seguridad lógica, los tres profesionales coinciden en que se deberá controlar que estén bien definidos los privilegios que posee cada empleado, ver si son razonables de acuerdo al cargo, si están asignados a las personas correctas, si se controla lo que hacen, que no cualquiera pueda modificar los datos y que quien lo haga lo realice en forma autorizada, controlar si existen pistas de auditoría que luego puedan ser revisadas, etc. Deben evaluar cómo son los procedimientos, por ejemplo cómo se realiza la creación y la eliminación de usuarios, que sean autorizados por la persona responsable, cuando ingresa alguien nuevo que no se le den permisos excesivos y de la misma forma cuando egresa que sean eliminados del sistema. Por otro lado también existen controles más técnicos, parámetros que se configuran en las aplicaciones y que permiten implementar controles que hacen que cualquiera no pueda acceder a la información.

Con respecto a la seguridad física, es importante que el centro de cómputos esté cerrado, que tenga buenas condiciones ambientales porque a veces pueden producirse fallas en los equipos al dejar de funcionar el aire acondicionado, si se detecta alguna debilidad se le informa al auditor aunque esto no es impedimento para el desarrollo de la auditoría, solo se tendrá en cuenta para las recomendaciones.

Con respecto al control de cambios, nos hablaron que deben hacer hincapié en controlar que cuando la empresa realiza una modificación en un sistema actual o cuando compra sistemas nuevos, se estén realizando las pruebas antes de empezar a usarlos y se documenten las mismas, entonces verificarán que existan ambientes separados, uno donde estén los sistemas funcionando y otro donde se realiza el desarrollo y la prueba, así como también corroborar quién realizó ese pasaje de producción, o sea comprobar que la misma persona que pone a funcionar los sistemas no sea la que los modifica, de manera que son controles independientes. En resumen se corrobora que los cambios estén autorizados por el negocio, que haya una segregación de funciones en el proceso y que haya monitoreo sobre los cambios.

Por último con respecto a las operaciones deberán verificar que existan respaldos, controles de antivirus, ver cómo son los procesos que se ejecutan, por ejemplo es bastante común en las empresas grandes que tienen sucursales que de noche haya un proceso que consolide información, si bien cada vez más se tiende a tener todo en línea y en tiempo real, hay ciertos procesos que se ejecutan de noche entonces todo esto es parte de las operaciones, ver cómo se controla que todas las sucursales transmitieron toda la información, que no quedó nada perdido y que no se duplicó ninguna transacción.

Todas las pruebas que se realizan sobre los controles generales son para evaluar si éstos son efectivos o inefectivos, después hacen una evaluación más general para esa categoría de controles de accesos lógicos o de administración de cambios, en función del set de controles que hayan y de los riesgos que estén involucrados, tratan de ver si existe un nivel de riesgo razonable, o sea que no hayan deficiencias significativas que puedan llegar a impactar en la integridad de los datos. Una vez obtenida esa conclusión de efectivo o inefectivo se le informan los resultados al equipo de auditoría, a quienes les será útil para determinar el alcance de las pruebas de los controles, obtener la evidencia electrónica y además para establecer los procedimientos sustantivos. Se utiliza información que surge de los sistemas, entonces lo que se intenta es darle un grado mayor de confianza a esa información, desde este punto de vista lo que se logra es hacer más eficiente la auditoría en cuanto a tratar de insumir la mínima cantidad de horas y mantener controlado ese riesgo de auditoría.

Los controles de aplicación se dividen en: controles de entrada, de procesamiento y de salida, en general el foco es el procesamiento, acá lo que se le pide a los expertos es que vean cómo se hace ese proceso, lo que hacen ellos en general son muchos recálculos, por ejemplo los auditores les piden que verifiquen si la diferencia de cambio, la previsión por obsolescencia o la previsión por incobrabilidad están bien calculadas, entonces para eso los expertos solicitan los datos al cliente y hacen el cálculo por su cuenta y ven si les da el mismo resultado que a la empresa.

Con respecto a la importancia de unos u otros controles nos manifestaron que no hay una única respuesta, siempre va en relación a los riesgos, no se puede decir que unos son más importantes que otros. Los controles de aplicación se basan también en los controles generales porque las aplicaciones se sustentan en una plataforma informática donde deben estar presentes siempre los controles generales, éstos son básicos. Se puede tener controles de aplicación efectivos y tener controles generales inefectivos, el dilema que se le presenta al auditor es, cómo a partir de esa situación con controles generales inefectivos se puede probar la eficacia de los controles de aplicación.

Dada la naturaleza que tienen los programas y los datos, si se prueba que en el año la posibilidad de que los datos sean modificados sin autorización o la posibilidad de que un programa esté fallando sea baja, entonces el riesgo también es bajo. Las fallas pueden ser ocasionadas por un fraude o por un tema operativo. Si se tiene un procedimiento de aplicación de cambios donde se probaron los cambios, los usuarios finales los validaron, se documentaron y fueron autorizados por el negocio, es muy poco probable que exista un cambio que se haya introducido en un programa que tenga posibilidad de fraude o de error operativo que genere un impacto en la contabilidad.

En resumen el tema de los controles generales es importante pero no sólo los controles generales, pues no sirve probar solo éstos sin probar los controles de aplicación.

18. ***¿Cuándo considera que un control general es inefectivo? ¿Cuáles son las posibles soluciones a esos controles inefectivos?***

En una de las firmas el experto nos respondió que la efectividad de un control depende en parte del criterio que tenga el auditor y de la situación en particular, por lo tanto se evalúa el peso que pueda tener cada control dentro de la organización, por ejemplo si una empresa tiene políticas y procedimientos establecidos y se detecta una excepción, pero hay una explicación por parte del negocio en relación a dicha excepción, se evalúa el riesgo que tenga el mismo y en función de ello se establece si es efectivo o inefectivo dicho control. Tanto para probar controles generales como para probar cualquier otro control entra a jugar la forma en que el experto selecciona la muestra, el alcance de la misma y el grado de confianza que se desea tener.

Existen una serie de controles que se encuentran típicamente implementados en todas las organizaciones, lo cual no significa que ante la ausencia de uno de ellos se dé por inefectiva la categoría ya que pueden existir otros controles que mitiguen los mismos riesgos.

Uno de los expertos nos mencionó que si un control funciona con deficiencias, la efectividad o no del mismo depende del peso que tenga la suma de cada una de las deficiencias, es decir si son deficiencias que a nivel individual son insignificantes pero que en la suma son significativas, entonces se concluye como inefectivo; de lo contrario, cuando estamos ante un entorno en el cual hay deficiencias que son todas no significativas y cada una apunta a mitigar riesgos distintos, de forma tal que el impacto que pueda llegar a tener en los estados contables sea no relevante o nulo, entonces se ve como efectivo.

19. ***¿Qué TAACs utiliza para evaluar dichos controles? ¿Con qué herramientas informáticas concurre? ¿Son software de uso generalizado o específicos desarrollados para la firma para la cual trabaja?***

Nos respondieron que se utiliza software genérico de auditoría como ACL o IDEA y otros desarrollados en Uruguay. Hay software para la parte de análisis y manipulación de los datos, eso como técnica asistida por computadora. Otro elemento que se usa para evaluar la seguridad lógica, sobre todo de las plataformas, ya a nivel de sistemas operativos son los SCRIPT programados, que son programas que los puede desarrollar cada firma y lo que hacen es, dependiendo de cada sistema operativo, obtener la configuración que tienen los

distintos archivos del sistema y esos resultados luego se analizan y comparan con resultados esperados, por ejemplo si se quiere determinar si un sistema tiene configuradas políticas de contraseñas o no, se le puede preguntar al funcionario de sistemas si las está utilizando o no, o si las tiene definidas en un documento, o de lo contrario se puede, a través de esos programas, de esos SCRIPT, obtener archivos con la configuración que está parametrizada, establecida en los servidores y entonces en base a esa configuración y en base a esa plataforma en particular, se va a determinar si esos controles están implementados o no.

Se podrían utilizar también herramientas de escritorio como Excel y herramientas para la parte de documentación, Access en particular no se usa ya que se utiliza ACL y la ventaja que tiene este software genérico de auditoría respecto a Access es que no permite modificar los datos y desde el punto de vista de auditoría esto es muy bueno porque asegura mantener la evidencia que les brinda el cliente. Access en la práctica permite modificar los datos y eso podría generar diferencias ya sea de forma accidental o intencional. Lo que permite ACL es que no se puedan modificar los archivos del cliente, pero si permite realizar todas las tareas que se hacen con los datos como: sumar, relacionar con otras tablas, generar distintas vistas, etc.

Para la parte de controles generales utilizan muy pocas herramientas, ya que la mayor parte del trabajo consiste en ver los procedimientos que realiza la empresa auditada, ver cómo se controla la seguridad, ver las características del centro de cómputos, etc., solo se usa alguna herramienta para sacar información del sistema, por ejemplo si se quiere analizar los usuarios de la red cuentan con una herramienta que devuelve la información de los usuarios y ciertos atributos de ellos, como por ejemplo cuándo fue la última vez que se conectaron, si tienen o no contraseña, cuándo fueron cambiadas, en definitiva todo lo referente a los accesos lógicos a los sistemas. Este tipo de herramientas las llevan los expertos a la empresa que están auditando, pero antes de usarlas se le explica al cliente en qué consisten y qué es lo que hacen para que éste autorice o no su uso, hay casos en que el cliente brinda la información que le solicita el especialista pero usando sus propias herramientas.

Después que obtienen esa información de usuarios, los especialistas en sistemas utilizan las herramientas de procesamiento de datos antes mencionadas (ACL o IDEA), que ya tienen programado cómo procesar toda la información recabada, o sea que reciben el archivo, lo

procesan y solucionan los problemas que puedan surgir en forma automática, se usan para analizar usuarios y contraseñas.

En las pruebas de los controles de aplicación se usan para realizar todos los recálculos, por ejemplo las diferencias de cambio, las previsiones, etc. En realidad el uso de ACL e IDEA es porque tienen muchas funciones predefinidas y preprogramadas que hacen fácil un cierto cálculo, como por ejemplo si se quiere calcular la antigüedad de un inventario solo se tiene que ejecutar dos botones en un menú y ya lo hace automático, a diferencia del Excel que es manual. Otra de las ventajas del uso de ACL e IDEA es que todo queda documentado, entonces en cualquier momento se puede ir a consultar lo que se hizo, además si se quiere repetir al año siguiente se puede hacer perfectamente porque todo queda registrado, de esta forma entonces se facilita el trabajo. Por otro lado, como desventaja de estas herramientas es que se requieren conocimientos específicos para su manejo y esto no es algo tan básico como puede ser Excel.

También puede utilizarse una herramienta llamada Datawarehouse que es un software general que puede o no poseer el cliente, si éste lo tiene, entonces los expertos lo utilizan, por ejemplo en la caja de un banco, en la generación de un depósito, se están ejecutando transacciones y toda esa información después se puede consultar, pero para consultarla muchas empresas lo que hacen es transferirla a otro repositorio en el cual esa información queda casi estática, se actualiza una vez por día y se realizan consultas que son más fáciles para el usuario. Por ejemplo si se tiene un balance y se quiere ver un saldo entonces sobre éste se puede hacer doble clic y muestra cómo está compuesto, muestra los asientos, luego se hace doble clic sobre éstos y se ve un resumen de un asiento de ventas y detalla todas las facturas que se realizaron y si se quiere ver esa factura, entonces se hace doble clic sobre ella y muestra todas sus líneas y de esta forma se puede ver qué artículos se vendieron, esto sería como un efecto cascada. Los expertos verifican que no haya pérdida de información, porque la realidad son las transacciones y lo que se está viendo es una extracción.

Existen casos en los cuales hay mucha información y determinadas herramientas no sirven porque no tienen demasiada capacidad, para esas situaciones lo que se usa son bases de datos como SQL, depende de la situación.

En general los expertos tratan de usar sus propias herramientas porque les permiten obtener la misma información en todos los lugares y de esta manera procesarla en forma automática.

Con respecto a la pregunta de si son software de uso generalizado o específico, ACL e IDEA son productos comerciales que desarrollaron empresas independientes que no son auditoras y en general todas las empresas de auditoría usan los mismos. Además las empresas tienen por ejemplo software específico para llevar adelante la auditoría y documentarla, pero no para probar los controles, sino para dejar documentado lo que se hizo y para que quede evidencia de que se siguieron todos los pasos.

20. ¿Cuáles son los procedimientos básicos, aquellos que usted considera indispensables?

En general nos hablan de que se realiza una distinción entre qué es lo que se controla y cómo se controla, siempre se evalúa todo lo relacionado a los controles generales (los de seguridad, los de cambios, los de operaciones, etc.) y con respecto a los controles de aplicación, se evaluarán los que sean solicitados. En cuanto a cómo se controla, esto también varía según el tipo de control, primero se indaga y luego se corrobora. Siempre hay que indagar cómo se realizan los controles, pero esto sólo sirve para ver el diseño, no se está probando que el control funcione bien, luego para realizar la prueba y ver si funciona, se lleva a cabo la corroboración, la cual se realiza con una persona independiente. En otras situaciones también se utiliza la observación, donde se le solicita al usuario que muestre cómo ejecuta una transacción en el sistema, para ver si realmente el control funciona, por ejemplo supongamos un sistema de compras que pide autorizaciones para aquellos importes que sobrepasan ciertos límites, en este caso lo que se hace es ingresar una compra por un importe mayor al límite y observar si el sistema traba la compra y solicita la autorización adecuada.

En resumen los procedimientos más usados entre otros son: el recálculo, la observación y la indagación. En realidad cada auditoría tiene sus particularidades, por ejemplo para un determinado cliente la cuenta de bienes de cambio puede no ser tan significativa como podría llegar a ser otra cuenta, entonces en base a ese grado de significancia, a cómo impacta en el balance y a la evaluación previa de controles generales, resulta necesario hacer determinados

procedimientos o no. Por lo general el procedimiento estándar es el análisis de los asientos diarios, con el objetivo de detectar errores, en algunas de las firmas les llaman internamente análisis de "asientos insólitos", lo que se hace entonces es tratar de analizar en función de todos los asientos, evaluar ciertos elementos o hipótesis que se deberían cumplir. Se analiza el porcentaje de asientos que hay para cada capítulo, además de hacer todos los controles que habitualmente se hacen sobre el balance (sobre activo, pasivo, patrimonio y resultados), también se hacen análisis de montos, se buscan asientos que tengan importes que son múltiples de mil o de diez mil, para ver si hay números redondos, habitualmente éstos indican transacciones manuales y para éstos se analizan las fechas, por ejemplo ver si hay asientos que se hacen los sábados, los domingos o los días feriados, ese tipo de procedimientos los define el auditor financiero y los expertos lo que hacen es utilizar las herramientas por tener el conocimiento más práctico en el uso de las mismas.

Existen costos de recursos, habitualmente cuando las firmas de auditoría acuerdan los honorarios con los clientes, tratarán de optimizar los mismos de forma tal de poder tener la mayor cantidad de tiempo posible disponible, tratando de realizar los procedimientos clave y a su vez también de reducir la mayor cantidad de riesgos, la idea no es hacer procedimientos que no le sirvan o no le aporten utilidad a la auditoría de EECC, es decir concentrarse en aquellos puntos críticos, ya que todo está relacionado con el tema de eficiencia.

21. Cuando la auditoría es recurrente, ¿se vuelve todos los años a realizar la evaluación de sus sistemas, o solo si la empresa realizó una actualización de los mismos? ¿Es necesario hacer una rotación de controles? En caso afirmativo, ¿Qué ventajas y desventajas tiene la rotación de controles?

En la metodología específica de una de las firmas está estipulado que los controles generales no se rotan, el motivo se debe a las características particulares que tienen esos controles. Sin embargo para los controles de aplicación y los controles que son de negocio, su metodología ya tiene previsto la posibilidad de rotarlos tratando de mantener un riesgo de control bajo. Para muchos de estos controles se puede tener un riesgo identificado y si existe una variedad de ellos y mitigan los mismos riesgos, se pueden rotar, a modo de ejemplo si se cuenta con cinco controles de aplicación se pueden probar tres de ellos y a su vez esos tres se van

rotando año a año, esto se puede hacer siempre y cuando los tres que se prueban cubran un riesgo razonable.

En el caso de los controles generales es más complicado, sobre todo por el hecho de ser sostén de los controles de aplicación, esto hace que al volver al año siguiente la situación pueda no ser la misma que la del ejercicio anterior, por ejemplo un parámetro se pudo haber modificado de un día para el otro y después volver a configurarse como estaba antes, esto hace que el riesgo que está asociado ahí sea más alto, lo cual disminuye el grado de confianza del experto en estos casos, debido a esto todos los años vuelven a realizar el mismo relevamiento, de tal forma que muchas veces los clientes se molestan porque se revisa lo mismo otra vez, aunque la parte crítica de identificación es más breve ya que cuentan con la documentación del año anterior, conocen el entorno y las aplicaciones entonces directamente prueban o corroboran si esos controles todavía están funcionando en forma efectiva.

El experto nos expresa que en su experiencia, por lo menos para el caso de Uruguay donde se está avanzando mucho en el uso de TI, ningún año es igual a otro porque en cada auditoría cuando concurren a la empresa se encuentran que hay una aplicación nueva, o se dejó de usar alguna, o se agregaron funcionalidades, o se cambió el servidor, o siempre hay algún cambio que de alguna forma u otra también termina impactando sobre la TI, esto justifica aún más el hecho de tener que volver a revisar. Incluso la conformación de los departamentos habitualmente también tiene un grado de rotación bastante interesante en el área de sistemas, esto hace que no solamente exista un tema de políticas, de procedimientos o de infraestructura, sino que además hay temas organizacionales, entonces el factor rotación es un factor crítico para la eficacia de los controles, son muy pocas las empresas que realmente tienen documentado los procedimientos y que esos sean realmente los que se realizan, en cambio con procedimientos basados en políticas aprobadas, la idea es que cualquiera que sea la persona deberá seguir el mismo camino definido para cada procedimiento.

Otro de los expertos nos expresa que cuando se trata de una auditoría recurrente existen determinadas normas y criterios para utilizar los trabajos de control interno de otros años, básicamente lo que se encuentra en el tema del control interno es el concepto de diseño e

implementación y eficacia operativa de los controles. En las auditorías recurrentes hay que hacer todos los años la parte de diseño e implementación, porque piden que esto se realice siempre y la eficacia operativa se va re-utilizando en la medida en que no haya cambiado el control con respecto al diseño e implementación.

Con respecto a la rotación de controles nos aclara que en función de lo anterior se realiza un plan de rotación. Bajo el supuesto de que una auditoría se va a basar en los controles, existe todo un tema de cómo se va a obtener la seguridad en esa auditoría y entonces habrá que buscar la eficacia operativa de todos estos controles claves y principales que están cubriendo los distintos ciclos de negocio y de tecnología, esto se realiza en el primer año y para los años siguientes el experto empieza a basarse en un plan de rotación. En su opinión en el caso de un esquema así de rotación, cuando no se prueba la eficacia operativa igual se prueba el diseño e implementación y hay que confirmar que el control se mantiene activo, que es lo más común en las empresas, no se da al caso de que estén cambiando constantemente sus sistemas, entonces se verifica esto y si cambió la rotación ya no es válida.

22. En el caso que se trate de la primera auditoría de su firma, ¿le sirven las evaluaciones de expertos de la auditoría anterior?

En estos casos solicitan la documentación, piden los últimos informes de auditoría, el tema es que lo que se obtiene es un informe, no los papeles de trabajo, por lo tanto no se sabe qué controles fueron probados. Si de la auditoría anterior surgieron una serie de observaciones, entonces se realizará un seguimiento de las mismas partiendo del informe que realizó la otra firma. Hay mucha información que se podrá consultar, es otra fuente más de conocimiento del cliente, se basan en las debilidades que encontraron para ver si la empresa realizó las correcciones y así planificar las pruebas que se realizarán.

En particular uno de los expertos se extendió en esta pregunta realizando la aclaración de que con respecto al trabajo de terceros, en su firma tienen como política interna para el primer año no hacer un enfoque de confianza en los controles, porque tienen que entender no solamente los sistemas, sino también el funcionamiento de la empresa, hay que entender los riesgos del negocio, entonces habitualmente se hace un enfoque más sustantivo y a al año

siguiente si se puede empezar a optar por la confianza en los controles. En relación al uso del trabajo de expertos externos primeramente evalúan por quién fue hecho el trabajo, las competencias que tenga esa persona, se mira la firma para la cual trabaja y además habría que ver los procedimientos de auditoría que realizó, si hay procedimientos que no se hicieron y hay riesgos que quedaron no cubiertos evidentemente no van a confiar. También ejemplificó el uso de trabajo de terceros en el caso de clientes que tienen el informe SAS 70, que es una evaluación que se le hace a los proveedores de sistemas para que cuando los clientes de ese proveedor de tecnología sean auditados, se les entrega a los auditores externos ese informe SAS 70 para que sirva como evidencia de que ya fueron auditados con un reporte que es estándar, conocido, en este caso el auditor externo lo que hace es evaluar las conclusiones del SAS 70, sería un ejemplo de uso de expertos en forma indirecta, otro ejemplo es cuando existen auditorías internas en las organizaciones, la idea es tratar de ver si se puede confiar en las tareas que realiza la auditoría interna para los controles, ahí se evalúa la independencia que tiene dicho departamento, que no dependa de la gerencia financiera sino directamente de la alta gerencia, las competencias y habilidades que tengan los auditores internos, los procedimientos que se hayan llevado a cabo, el alcance y en función de todo esto se evalúa el cumplimiento de esos controles que ellos tienen estipulados y no se va directamente a la prueba del control, en este caso también se trata de una evaluación del trabajo de terceros, la idea es no volver hacer trabajo que ya fue hecho, es pérdida de tiempo para la auditoría y para el cliente también tener que volver a hacer lo mismo.

23. ¿Cómo le presenta al auditor el resultado de la evaluación de los sistemas?

Uno de los expertos comentó que para comunicar los resultados de los controles generales tienen un modelo específico de informe donde están los nombres de los controles que se probaron, si son efectivos o no en su diseño y en su eficacia operativa y una conclusión sobre si de alguna forma son confiables o no, si se pueden basar en ellos para hacer ciertas pruebas. Para los controles de aplicación también nos mencionó que poseen un modelo, donde se expresa el objetivo del control, el procedimiento que ejecutaron y la conclusión para ver si ese control adicional que el auditor les pidió que evaluaran, es efectivo o no. Todo eso lo documentan y se lo dan al auditor y él lo incorpora en el software que usa para documentar la auditoría, por lo tanto queda documentado todo el trabajo y además elaboran memos que

dicen quién lo hizo, quién lo revisó, la fecha en que se hizo, etc. Existen diversos papeles de trabajo que han de completar para dejar sus tareas documentadas.

Otro de los expertos nos habla también que la metodología a seguir en cuanto a la documentación de la auditoría en sí, en su firma esta dividida en secciones, por ejemplo una de ellas tiene que ver con la planificación de la auditoría, donde uno de los temas centrales es el conocimiento del proceso contable, tienen que obtener toda la parte del conocimiento de informática porque sustenta a la generación de transacciones y la contabilización de las mismas, entonces se va a interactuar con el auditor contable en esta etapa y esto se realiza en los comienzos de la auditoría. Después con respecto a las pruebas de los controles, se va generando intercambio de información con los auditores y a su vez se va generando también documentación al respecto. Para él, el informe final sería lo que corresponde a la carta de control interno, donde pueden aparecer una serie de debilidades, problemas de seguridad y de acceso que hayan surgido durante la auditoría, eso es lo que para él es más parecido a un informe final que luego va a terminar siendo parte de la carta de control interno, pues en realidad cada una de las entrevistas que realizó y controles que probó terminan en documentos con observaciones, con hallazgos y todo esto se transforma en un flujo de información permanente entre auditoría financiera y el departamento de TI.

El experto de la restante firma, sigue en la línea de que la idea no es trabajar en forma separada sino de trabajar en conjunto, lo que determina que los auditores no reciban el informe al final sino que vayan teniendo un conocimiento en forma oportuna de la eficacia o ineficacia de un control, porque la idea es tratar de ser eficientes y de antemano saber, antes de emitir cualquier informe, cuál control es efectivo y cuál no, entonces deben informarlo oportunamente. De todas formas al finalizar emiten un memo de conclusiones en el cual se documentan las principales deficiencias, las conclusiones y a nivel integrado de trabajo poseen una herramienta de documentación que les permite ir detallando las conclusiones de los controles que van probando y a su vez los auditores pueden ir consultando y viendo cuál es la situación durante la marcha, incluso sirve como elemento de comunicación y como elemento de documentación, es una herramienta que utilizan a nivel interno de la firma, la cual les permite trabajar en equipo, cada uno la tiene en su computadora y conectándose a la red o a través de Internet, permite de alguna forma a cada uno tener una vista de lo que es el trabajo de auditoría y dentro de ese entorno de trabajo poder incluir las conclusiones, la

documentación, los papeles de trabajo, etc. y queda visible para todos, se trata de una herramienta que está prevista evidentemente para países como EEUU o países grandes que tienen distintas locaciones y trabajan en distintos lugares físicos, pero también es útil para documentar los resultados del trabajo.

Anexo 2

A.2 – Entrevista realizada a un auditor

1- ¿Cómo impacta el entorno computarizado en la auditoría de EECC?

Hay ciertas empresas donde es necesario hacer determinadas pruebas de sistemas, por ejemplo en los bancos, más allá de que también se realicen pruebas sustantivas en estas empresas se necesita realizar básicamente pruebas de sistemas debido al tipo de operativa o al gran volumen de transacciones.

Si nos centramos en un ambiente altamente computarizado, el mayor impacto es que en este tipo de entorno se necesita si o si verificar que existan en la empresa controles sobre los sistemas informáticos.

2 - ¿En qué situaciones no es necesaria la participación del experto en las auditorías de estados contables?

Cada vez es más raro encontrar una entidad cuyos procesos no dependan en cierto grado de un ambiente computarizado, porque las empresas han ido incorporando mayor cantidad de módulos en sus sistemas informáticos, por ejemplo para la facturación, cuentas corrientes, contabilidad, etc., los cuales son cada vez más integrados.

Una situación en la que no sería necesaria la participación del experto, sería la de una empresa que utilice un paquete de software de uso generalizado y reconocido en plaza, de esta forma si la empresa cuenta con un sistema cerrado, que ya está predeterminado y comprobado su funcionamiento, entonces el auditor va a confiar en las funcionalidades del mismo, pero deberá verificar los accesos que se les ha dado a cada funcionario y no mucho

más, aunque no sería lo común en una empresa mediana o grande, que son las que básicamente necesitan después auditoría por lo cual ahí ya iríamos directo a un ambiente computarizado.

Tiene que ser muy cerrado el sistema como para no necesitar el apoyo del experto, no siempre en la misma escala, hay empresas en las que se necesita mucho más apoyo como en el caso de los bancos, en comparación con una mediana empresa que compra y vende, pero esto no quiere decir que no se requiera, es otro tipo de apoyo.

3- ¿Qué tipo de enfoque se aplica en estos casos?

En las auditorías se decide si se hace un enfoque de control o un enfoque sustantivo, el tema aquí es cómo son los controles cuando el entorno es computarizado. Hay muchos controles que se pueden probar que habitualmente suelen ser más efectivos, éstos son los controles que hacen las propias máquinas, por ejemplo interfases y son más eficientes de probar que un control manual, como en el caso en que una persona chequea si lo que sale de un informe entra en el otro sistema, entonces cuanto más computarizado sea el entorno, más posibilidad de tener controles automatizados existe, por lo tanto el enfoque que se aplica en estos entornos es un enfoque de control.

4- ¿Cuáles son los principales procedimientos que habitualmente realiza en torno a los sistemas informáticos? ¿El alcance varía según las circunstancias de la empresa auditada?

Cuando se verifica que hay un ambiente computarizado y se decide que se va a confiar en ese ambiente se le solicita a sistemas que pruebe determinados controles generales, tales como ver si existen respaldos, los accesos, las claves de los distintos sistemas y otros, eso con respecto a los controles generales. Para los controles de aplicación lo que se hace es ir a la empresa, ver qué aplicaciones existen, qué controles están funcionando y de esta forma ver cómo esos controles influyen dentro del proceso que nosotros pretendemos auditar y ahí

definir qué controles y qué aplicaciones vamos a probar ya que no es necesario probarlas todas. Una vez definido esto, se diseña en conjunto con la gente de sistemas qué tipo de pruebas podemos realizar.

El alcance va a diferir "n" veces según el cliente y las pruebas que se definan, también se establece en qué oportunidad vamos a hacer las pruebas, cómo se van a realizar, si van a ser una repetición, si se va a indagar o ver si se va a rehacer el control, dependiendo de todo esto, se definirá junto con la persona encargada de sistemas qué es lo más adecuado.

5- ¿En qué momento de la auditoría solicita Ud. la intervención del experto?

Habitualmente en la etapa de planificación cuando se comienza a analizar cómo se van a probar los controles, es cuando se involucra al experto en sistemas y después continúa trabajando con nosotros durante toda la auditoria, ya que se irán haciendo pruebas y se irá decidiendo si esas pruebas son efectivas o no, o buscando otras pruebas o viendo cómo nosotros implementamos las mismas.

En el correr del trabajo nos va proporcionando la información, sus conclusiones y nosotros vemos si eso nos resulta efectivo o no, si nos resulta suficiente o no, entonces tenemos que requerirle otra prueba, buscar evidencia por otro lado, o que realice otra vez lo mismo, hasta que lleguemos a conclusiones que nos resulten satisfactorias para nuestro trabajo.

En primera instancia, uno toma la decisión de qué controles quiere probar, sobre todo cuando es primera auditoría, ya que cuando es recurrente se sabe más o menos como son los controles. En principio uno tiene una idea de lo que va a controlar y cómo lo va a hacer, puede ser que después surjan problemas y que no lo pueda probar de la misma forma. El experto nos dice si el control es efectivo o no, de acuerdo a lo que nosotros le solicitamos que pruebe. Tanto ellos como nosotros decidimos al final si eso es efectivo o no, mas allá de que la prueba que realizó sea efectiva yo voy a evaluar si esa prueba realmente a mi me permite tener evidencia suficiente, tal vez tenga que agregar alguna otra. Quienes terminan evaluando qué hacer en el trabajo de auditoría son los auditores, obviamente que los expertos

nos van a decir si la prueba funciona bien o no, pero si esto es suficiente para la auditoría lo determina el auditor.

6- ¿Cuál es el trabajo que Ud. le solicita?

En primera instancia intentamos definirle lo mas detallado posible lo que queremos hacer, habitualmente se hace en conjunto con ellos, por ejemplo si tenemos una interfase lo que solicitamos es probar que ésta vuelque bien los datos en el sistema que es de donde surge la información presentada en los EECC, el experto realizará una serie de pruebas y nos comunicará sus resultados, si nos parecen insuficientes se le solicitan más pruebas, es decir se realiza una continua retroalimentación, estamos en coordinación permanente, pero las pruebas las detallamos nosotros y las definimos con ellos.

7- ¿Cuáles son los controles generales que le pide que evalúe?

Al experto se le solicita que evalúe los controles generales, entre estos tenemos por ejemplo verificar si hay respaldos, qué sistema se está utilizando, si está desarrollado por la empresa o no, qué grado de dependencia se tiene del proveedor, accesos lógicos, modificaciones en el programa, la segregación de funciones, etc. En definitiva nosotros trabajamos con "x" controles estándar que ellos habitualmente realizan, eso no quita que yo les pueda agregar alguno.

8- ¿Y cuáles son los de aplicación?

Estos tienen que ser diseñados y definidos por nosotros porque no todas las empresas son iguales ni utilizan los mismos sistemas, como cualquier otro control no solo computarizado, se hacen para aquellos saldos o transacciones más rutinarias con mayor volumen de movimiento, en contraste con las cuentas con pocas transacciones donde si es posible realizar pruebas sustantivas, entonces cualquier tipo de pruebas de control las realizamos cuando son transacciones más rutinarias y de mayor volumen, los más comunes son los controles de

compra, los de administración de bienes de cambio, de facturación, probar la integridad, ver como es la registración, etc.

Habitualmente el control computarizado se relaciona con interfases o captación de información, que para este tipo de transacciones que son muy computarizadas, si o si hay que probarlas a través de un sistema, porque en estos casos es muy difícil hacer una prueba sustantiva.

Algunos ejemplos son: recálculo de diferencia de cambio, una prueba de una interfase de ventas, que la facturación pase directamente, que se contabilice directamente, que el sistema que factura esté integrado al sistema contable y entonces factura y se contabiliza, probar que en el sistema al sacar un producto directamente se actualiza el stock, todos esos son controles de aplicación. Otro ejemplo de esto, es cuando en las empresas que toman consumo (UTE, OSE, GAS), hay que probar que ese consumo que tomaron en un aparatito terminó yendo a la factura y cómo esa factura terminó registrada en la contabilidad y ver si esos datos que fueron a la contabilidad son los que se reflejaron en el Balance.

Puede haber otros controles que no son tan automáticos, cuando el sistema saca un aging (los clientes por vencimientos por ejemplo) y uso ese aging para calcular la previsión por incobrables, entonces yo le puedo pedir al sistema cómo es que estaba estructurado ese aging, si estaba bien armado o no, para asegurarme que no esté partiendo de una información que esté incorrecta. Otro tipo de control es cuando extraigo información del sistema y la doy como válida entonces para esto tengo que probar si efectivamente estuvo bien diseñada o no.

9- El auditor, ¿recibe capacitación en informática?

Nosotros utilizamos capacitación en esos programas, pero a nivel de usuario, para poder entender y hacer algún recálculo si necesitáramos entender lo que hizo previamente el experto, algo básico como para saber qué solicitarle.

10- ¿Cómo le presenta el experto el resultado de su trabajo? ¿Cómo utiliza el auditor ese informe?

En sí lo vas viendo durante todo el proceso, igual tiene un producto final que son determinados memorándum donde nos explican cuál fue el objetivo, el procedimiento realizado y las conclusiones a las que llegaron. Existe una parte formal, más allá que no te debería generar una sorpresa al recibirlo porque se ha mantenido un continuo contacto. Estos memorándum se archivan formando parte de los papeles de trabajo del auditor.

11- Cuando la auditoría es recurrente, ¿se vuelve todos los años a realizar los mismos controles?

La determinación de qué controles probar siempre se realiza en base al que te resulta más eficiente y con el cual se mitiguen más riesgos. Si se considera que sirve ese control entonces año a año se puede seguir probando el mismo y si existe algún otro tipo de sospecha, se puede probar otro o agregar alguno, aunque no se saque el que se considera importante. La rotación de controles no es el cambiar los controles, sino basarse en ellos pero probar que funcionen un año uno y en otro año otro y así sucesivamente, nosotros eso no lo hacemos habitualmente, pero sabemos que en algunas empresas se hace, van rotando cuando prueban el control y lo que hacen es, año a año ver si cambió algo, pero efectivamente no lo prueban. Nosotros no es que mantengamos siempre los mismos, sino que los que definimos los probamos y definimos los que consideramos que mitigan mayores riesgos. Podemos agregar alguno en caso de duda o podemos modificar el tipo de control, no dejamos de probar un control porque lo probamos el año pasado, eso no quiere decir que tengamos que cambiarlo, eso no, siempre existe un juicio de qué controles son los que sirven y si se agrega uno o no, o si se saca uno es porque no era tan relevante como pensábamos, pero no es que tengamos una política que año a año hay que probar controles distintos.

12- ¿Qué ventajas y desventajas tiene la rotación de controles?

La rotación de controles tiene la ventaja de no acostumbrar al cliente en lo que vas a probar. Habitualmente conviene agregar algún control, en vez de rotarlos.

La desventaja es que tal vez te estás perdiendo controles que realmente tendrías que probar y no se probaron.

13- En el caso que se trate de la primera auditoría de su firma, ¿le sirven las evaluaciones de expertos de la auditoría anterior?

Me podría servir como guía de qué controles fueron evaluados para ver si a mi me sirve probar los mismos, no es que yo tome la opinión del experto de la auditoría anterior como válida, verifico que esos controles están este año y los tomo en cuenta después para probarlos, pero no considero la prueba que haya realizado el experto como la realizada por nosotros.

14- ¿Qué herramientas informáticas utiliza para desarrollar este trabajo?

Se puede usar entre otros, IDEA o ACL, mas allá de que pueden tener alguna funcionalidad distinta, en si son herramientas para facilitarle a la persona de sistemas determinados recálculos y determinadas pruebas, por ejemplo la diferencia de cambio. Excel habitualmente también puede ser una herramienta pero tiene la limitación de un número determinado de filas, mientras que IDEA o ACL no presentan este tipo de limitación, son herramientas que utiliza el experto para realizar ciertos controles, tienen determinadas funcionalidades automáticas, por ejemplo pueden obtenerse determinados reportes ya sea asientos hechos fuera de hora o asientos duplicados, son herramientas utilizadas para mejorar el trabajo y hacerlo mas rápido y eficiente.

15- ¿Son software de uso generalizado o específicos desarrollados para la firma en la cual trabaja?

ACL e IDEA son programas generales, hay después otros programas de auditoría que cada firma más o menos de porte desarrolla, por ejemplo programas propios que se utilizan para documentar la auditoría (llevar papeles de trabajo), y que no tienen nada que ver con un recálculo.

16- ¿Estas herramientas informáticas como IDEA, lo usa sólo el experto o lo usan también para la auditoría en general?

IDEA puede tener varios usos, por ejemplo para que el auditor saque muestras, también se puede usar Excel en vez IDEA. Éste último lo utilizamos también los auditores, pero a nivel de programa de auditoría, no a nivel de pruebas de sistemas.

17- ¿Cómo se realiza la evaluación de los controles?

Se va analizando el resultado del trabajo del experto y después se decide si todo lo recabado es suficiente o no, si se pueden agregan pruebas de controles, pruebas sustantivas o si se agrega una salvedad a la opinión porque hay determinados saldos, cuentas, transacciones que no pudieron ser probados o en último caso el auditor podrá abstenerse a opinar.

18- ¿Cuándo considera que un control general es inefectivo?

Cuando no cumple una política, cuando no mitiga riesgos, por ejemplo si la empresa no hace respaldos el control general es inefectivo, porque se corre el riesgo que hoy o mañana se quede sin información.

19- ¿Cuáles son las posibles soluciones a esos controles inefectivos?

Lo que se hace habitualmente es una carta de control interno sugiriéndole a la empresa que tiene ese problema, eso directamente no tiene por qué impactar en la auditoría de EECC de

este año, sino que se sabe que se tiene un riesgo a posteriori, que se tiene un problema de información pero no tiene por qué impactar directamente en el negocio, pudiendo impactar en otro momento o tal vez nunca.

En el caso de los controles generales, puede ser que tenga acceso una persona que no debería tenerlo y entonces habrá que aumentar las pruebas sustantivas para ver si efectivamente funcionó bien o no, como cualquier cuenta, si los controles generales o de aplicación no te resultan efectivos, o se considera que no tiene impacto en esta auditoría, o se busca otra forma de probarlo o se tiene que limitar la opinión.

En el caso de los controles de aplicación, si se tiene un problema de integridad en las ventas, se puede circularizar un 90 % de los clientes, o ver tendencias de ventas o ver precios promedios, o sea se buscan pruebas sustantivas que suplementen ese control que no está funcionando, en caso de poder aplicarlas.

Si un control falla, entonces hay que buscar otras pruebas, sustantivas o de control, si esas pruebas te dan la evidencia suficiente, se sigue adelante aunque el control sea inefectivo, si no te da la evidencia suficiente no se puede seguir y te va a afectar tu opinión de auditoría. Hay empresas que si te falla un control, no hay otra solución más que limitar la opinión.

Bibliografía

- ✓ Normativa emitida por organismos nacionales. (Circulares, resoluciones, pronunciamientos, etc.
  - BCU, Comunicación 179/03.
  - DGI, Resolución 1093/005 y modificaciones 480/009.
  - BCU, Circular Nº 1938 de fecha 30/08/2005
- ✓ Materiales publicados:
  - COBIT resumen ejecutivo – abril de 1998 2ª edición.
  - D'Olivo Blanco, Ma. Fernanda – Manguian Khurlopian, Jennifer – Sauleda Borrazas, Luis A., Una propuesta de profundización de la enseñanza del aporte de la tecnología de la información a la labor de auditoría, Uruguay 2002.
  - CECEA: publicaciones de las diferentes cátedras relacionadas con el tema. (Auditoría y Control Interno).
- ✓ Páginas WEB consultadas:
  - Dirección General impositiva (www.dgi.gub.uy)
  - Banco Central del Uruguay (www.bcu.gub.uy)
  - Auditoría Interna de la Nación (www.ain.gub.uy)
  - IFAC (es.ifac.org)
  - ISACA (www.isaca.org)
  - Facultad de Ciencias Económicas y Administración (www.ccee.edu.uy).
- ✓ Libros de diferentes autores:
  - Acha Iturmendi, J. José, Auditoría informática en la empresa, Editorial Paraninfo S.A., 1994.
  - Echenique García, J. Antonio, Auditoría en informática, McGraw Hill, 2ª edición, 2001.
  - Arens, Alvin A. y Loebbecke, James K., Auditoría: un enfoque integral, Prentice Hall Hispanoamericana S.A., 6ª edición, 1996.
  - Gubba, Hugo – Gutfraind, Jorge – Montone, Luis – Rodríguez, Ruben –Sauleda, Luis – Villamarzo, Ricardo, Auditoría: Guía para su planificación y ejecución, Central de Impresiones, año 2007.

- Fowler Newton, Enrique, Auditoría Aplicada: Tratado de Auditoría, segunda parte tomos I y II, Ediciones Macchi, año 1995.

✓ Apuntes de clase (materia: auditoría – Facultad de Ciencias Económicas y de Administración).