Facultad de Ciencias Económicas
UNIVERSIDAD NACIONAL DE LA PLATA
60 aniversario 1953-2013
Secretaría de Asuntos Académicos

Colección 60 Aniversario | Libros de Cátedra

Carlos Alberto Slosse
(compilador)

CONTABILIDAD VIII

Auditoría

Edulp
Editorial de la Universidad de La Plata

Facultad de Ciencias Económicas
UNIVERSIDAD NACIONAL DE LA PLATA
60 aniversario 1953-2013
Secretaría de Asuntos Académicos

CONTABILIDAD VIII

AUDITORÍA

Carlos Alberto Slosse
(compilador)

Ana María Cóccaro
Marcela Falvella
Lorena María Martires
Carlos Alberto Rumitti

edulp
Editorial de la Universidad de La Plata

Slosse, Carlos
Contabilidad VIII auditoría / Carlos Slosse; compilado por Carlos Slosse. - 1a ed. - La Plata: EDULP, 2013.
E-Book.

ISBN 978-987-1985-11-1

1. Contabilidad. 2. Auditoría. I. Slosse, Carlos , comp. II. Título.
CDD 657.45

Editorial de la Universidad Nacional de La Plata (Edulp)
47 N.° 380 / La Plata B1900AJP / Buenos Aires, Argentina
Teléfonos: (0221) 427-3992 / 427-4898
editorial@editorial.unlp.edu.ar
www.editorial.unlp.edu.ar

Corrección: Cintia Kemelmajer / Diagramación: Andrea López Osornio

Edulp integra la Red de Editoriales Universitarias Nacionales (REUN)

Primera edición, 2013
ISBN N.º 978-987-1985-11-1

Queda hecho el depósito que marca la Ley 11.723

ÍNDICE

PRÓLOGO

Con mucho gusto la cátedra que dirijo ha aceptado la invitación que nos cursaran la Secretaria de Asuntos Académicos, Contadora Laura Catani, y el Director del Departamento de Contabilidad, Contador Rubén Galle, en el sentido de producir, con motivo del 60° aniversario de creación de nuestra facultad, un texto con temas técnicos.
De los varios temas que integrantes de nuestra Cátedra vienen investigando, hemos incorporado -en función de su grado de avance- tres. Ellos son:

-*El sistema de control interno en las empresas*, a cargo de la profesora Lorena Martires. Lorena se desenvuelve en el campo profesional dedicada al área de una entidad financiera provincial, la más grande e importante de la provincia de Buenos Aires. A pesar de su juventud, aquilata ya una significativa experiencia, que la ha llevado a incursionar en el importante tema de lo que significa un buen y eficiente sistema de control interno dentro de cada organización. Ello hace al funcionamiento de un buen gobierno corporativo. Hace a la búsqueda de la eficiencia operativa, con *sensores* de cómo están marchando los diversos procesos operativos, tanto en empresas de servicios como en aquellas dedicadas a la fabricación y venta de productos.
El lector encontrará matices dentro de un tema caro a los sentimientos de cualquier profesional en Ciencias Económicas que hacen a una concepción moderna del control, se dedique a la actividad que sea.

-*Auditoría de instrumentos financieros derivados*, a cargo de la profesora Ana María Cóccaro. Ana María actúa profesionalmente en un importante grupo empresario argentino, con múltiples actividades. Por esa variada experiencia, ha elegido un tema que ha cobrado notoriedad e importancia en los últimos tiempos, a raíz de los cada vez más complejos mecanismos de la denominada *ingeniería financiera*. Ellos no sólo se encuentran en las grandes

organizaciones; también, aunque con menor complejidad, se aprecian en medianas empresas.

La labor del auditor frente a la existencia de este tipo de instrumentos (se insiste, de complejidad variable pero cada vez mayor), *no es sencilla*. Debe, en primer lugar, conocer su funcionamiento, para luego diseñar y aplicar técnicas de revisión apropiadas. También aquí son de extrema importancia los mecanismos de control interno que deben *rodear* el funcionamiento de estas herramientas del *arsenal* que el sistema financiero ofrece a las empresas para su financiamiento.

-*La nube. Mitos y realidades*, producido por los profesores Carlos Alberto Rumitti y Marcela Falvella, aborda un tema también de gran actualidad: el referido a la auditoria de sistemas informáticos tercerizados (fenómeno que por diversas razones adoptan muchas organizaciones, en nuestro país y en el mundo). En el mundo TI (el de la Tecnología informática, con sus TIC'S, tecnologías de la información y la comunicación, servicios vinculados) también los desarrollos se producen a ritmo endemoniado. Y, sin duda, el profesional en Ciencias Económicas, auditor, especialista en sistemas de información y otros, debe seguir dicho andar a la misma velocidad.

Los autores, con lenguaje claro y sencillo, accesible a todo el mundo, destierran algunos *mitos*, pero aportan una valiosa contribución para nuestro desempeño profesional, en particular como auditores de información financiera procesada, producida, gestada, a través de esos vehículos. Se acabó, en muchísimos casos, el denominado *working paper* en los legajos del auditor consistente en profusos y tediosos detalles; lo mismo sucede con el famoso *tilde* del auditor. Ahora, con el uso de modernas herramientas informáticas por parte de las empresas, la nube es otra manera de auditar procesos, sistemas y, en definitiva, validar, verificar la razonabilidad de determinada información contable-financiera.

Esperamos con estos trabajos realizar una contribución a toda la comunidad profesional respecto de temas novedosos, en dos casos, y en el de control interno abordándolo con un enfoque moderno.

Deseo, por último, destinar unas líneas a una serie de agradecimientos. En primer lugar, a las autoridades de la Facultad de Ciencias Económicas de la UNLP, en particular al Decano, Martín López Armengol, a nuestra Secretaria de Asuntos Académicos, Laura Catani, y al Director del Departamento de Contabilidad, Rubén Galle (y su Sub-Directora, la colega Nora Antonelli) que nos permiten trabajar con un *clima* ideal: siempre dispuestos a atendernos, con una amplia predisposición al diálogo, escuchando, con solicitudes siempre razonables. A los autores de los trabajos aquí presentados, por su empeño y dedicación, y a Guillermina Mercapidez, nuestra Jefa de Trabajos Prácticos, quien ha efectuado un excelente trabajo de coordinación, y, por último, a todos los integrantes de la cátedra: Cristina Gadea, Ana María Cóccaro, Carlos Aberto Rumitti, Graciela Merani, Guillermina Mercapidez, María Migoya, Lorena Mártires, Ana María Plastino, Julieta Richiusa, Marcela Falvella, Griselda Iriarte, Emiliana Timossi, Hernán Rosso, Jimena Rodríguez, Julia Stefanizzi, Gabriela Castiglioni, Betiana Montaña, Paula Cardelli y Germán De Luca, por su permanente predisposición y dedicación.

CARLOS ALBERTO SLOSSE

La Plata, octubre de 2013

CAPÍTULO 1

LA NUBE - MITOS Y REALIDADES

Carlos Alberto Rumitti
Marcela Falvella

Introducción

Los desarrollos tecnológicos de los últimos años, han colocado sobre el escenario una gran cantidad de servicios y herramientas basadas en Internet, gran parte de los cuales están orientados a realizar el intercambio de información, en cualquier momento y desde cualquier lugar, por medio de diversos y variados dispositivos móviles.

Esta tendencia creciente de multiplicación de dispositivos electrónicos personales, constituye un problema para la seguridad de los datos de algunas organizaciones, colocándolas en un lugar más vulnerable, teniendo en cuenta que en la actualidad, operan aproximadamente 5 billones de dispositivos móviles, 25 % de ellos con posibilidades de conexión web.

La tendencia a la *portabilidad*, la inmediatez y la digitalización de los procesos de negocios es irreversible y su impacto en la estructura de las organizaciones requiere una adaptación cultural que a menudo supera las posibilidades de asimilación y, por otra parte, genera una estructura de costos fijos elevada, producto de altas inmovilizaciones en recursos (equipamiento) de TI. Este equipamiento, por los avances tecnológicos, es el de rápida obsolescencia.

En este marco, debe gestionarse la información. Ésta es un conjunto de procesos por los cuales se controla su ciclo de vida, desde su obtención, ya

sea por creación o captura, hasta su disposición final, en archivos o la eliminación de la misma. Estos procesos incluyen, también, garantizar el cumplimiento de los objetivos básicos de la seguridad de la información: integridad, disponibilidad y confidencialidad.

Actualmente se concibe a la información como el mayor activo que cualquier organización posee y debe proteger de intromisiones o ataques -la moneda del siglo XXI, según el NIST-; sin embargo, la seguridad absoluta no existe, o en todo caso, de existir, sería a costos tan elevados que la convertirían en inalcanzable. Ante esta situación, se presenta la necesidad de evaluar y resolver qué hacer con el riesgo vinculado a los constantemente nuevos desafíos de TI.

Otra cuestión a resolver es la disyuntiva entre asumir los costos fijos que implica una estructura propia de TI o tercerizar la prestación de servicios informáticos y transformarlos en *ágilmente* variables.

Las nuevas –o no tan nuevas- tendencias, se orientan hacia la tercerización, hoy llamada computación en la nube (*cloud computing*), que ha sido definida por el NIST como un modelo conveniente, que mediante una petición de acceso de red permite disponer de un conjunto compartido de recursos informáticos configurables -como redes, servidores, almacenamiento, aplicaciones y servicio-, que pueden ser rápidamente aprovisionados y puestos en producción con un mínimo de esfuerzo de gestión o de la interacción con el proveedor de la nube.

La otra alternativa es asumir las inmovilizaciones y costos fijos que resultan de una estructura propia de TI. Sin embargo, acotarse y/o cerrarse no parece ser la solución a este problema, porque no acompañar el avance tecnológico deja a la organización rápidamente fuera del sistema.

Si bien parece que el equilibrio siempre es lo recomendable, la duda es cómo alcanzarlo: ¿optamos por estructura propia, *cloud* o un mix? En el presente trabajo, aportamos algunos elementos de análisis que ayudan a evaluar la situación en cada caso particular. La gestión de riesgos, es determinante en estas decisiones.

Cuestiones generales

Como primera medida, desterremos los mitos: la nube no existe, sólo se trata de una metáfora y forma parte de su marketing.

Siempre hay un *lugar* físico –servidores de bases de datos- donde los datos se encuentran almacenados, y la tercerización de servicios informáticos tampoco es nueva, sólo cambió la forma de prestar el servicio a la luz de la nuevas tecnologías y la generalización de la web.

Existen una gran cantidad de servicios disponibles actualmente. Algunos ejemplos de *nube* son: *Google*, *Yahoo*, *Amazon*, *Dropbox*, además de los específicos que prestan muchas compañías, incluso en forma gratuita, hasta cierto volumen de transacciones y/o almacenamiento.

a. Modalidades de prestación de servicios *cloud*:

i. **IaaS: *Infraestructure as a Service* (Infraestructura como servicio):** consiste en la provisión de equipamiento *virtual*. Es el nacimiento y base de todo. Se provee de recursos informáticos, servidores, conexiones, almacenamiento y las herramientas necesarias para construir un ambiente de aplicaciones preparado para servir a los múltiples requerimientos de las organizaciones.

   Es el que permite mayor participación del usuario y mayor grado de auditabilidad.

   Beneficios:

   - Rapidez en la provisión o reemplazo de los recursos y servicios.
   - Mayores posibilidades de control por parte del usuario.
   - Costo variable según requerimiento del usuario.

ii. **PaaS**: ***Platform as a Service* (Plataforma como servicio):** relacionado con la provisión de plataformas (hardware y sistemas operativos). Genera todas las facilidades requeridas para construir y entregar aplicaciones basadas en la web y servicios disponibles por Internet. Proporciona un ambiente de

desarrollo para la generación de aplicaciones. Es específico para ese fin y no está definido para procesos operativos.

Beneficios:

- Las aplicaciones pueden ser compartidas.
- Pueden construirse y compartirse otras aplicaciones.
- Menor tiempo en desarrollos e implementación.
- Costo variable según requerimiento del usuario.

iii. **SaaS: *Software as a Service* (Aplicaciones como servicio)**: se refiere a aplicaciones alojadas en remoto (correo, seguridad, programas). Es un modelo que permite utilizar software y consiste en la *adhesión* a una aplicación puesta a disposición por un proveedor de servicios desde la nube de Internet, para ser utilizada por diferentes usuarios.

Es una modalidad en la que no hay más participación del usuario que las predefinidas en la aplicación, por lo tanto se asemeja a un contrato de adhesión, sin que exista posibilidad alguna de fijar condiciones de uso en particular. Tiene limitaciones de acceso para su auditabilidad.

Beneficios:

- El cliente no necesariamente debe tener un área especializada para soportar el sistema.
- La garantía de disponibilidad de la aplicación y su correcta funcionalidad es parte del servicio que brinda la firma proveedora de software.
- No es necesaria la compra de una licencia para utilizar el software, sino el pago de un alquiler o renta por el uso.

b. Modelos de implementación

Los tipos más frecuentes son:

i. **Nube privada**: la infraestructura es operada únicamente por una organización individual y administrada por la organización o por un tercero.

ii. **Comunidad nube:** la infraestructura es compartida por varias organizaciones o apoya a una comunidad específica que tiene intereses comunes entre sí. Podría ser gestionada por las organizaciones de la comunidad o de un tercero y puede existir dentro o fuera del local.

iii. **Nube pública**: la infraestructura está disponible para el público en general y es propiedad de una organización que vende servicios en la nube.

iv. **Nube híbrida**: modelo del NIST, en el cual múltiples sistemas en la nube se encuentran conectados, permitiendo que los programas y datos se muevan fácilmente de un sistema a otro.

c. Tipología de proveedores

i. ***Cloud hosting***: son similares a los servicios ofrecidos por empresas de hosting tradicional. La diferencia principal radica en que un servicio en la nube se paga por lo que se utiliza y se puede ampliar o disminuir los recursos del sistema en cuestión.

ii. ***Cloud computing*****:** son ofertados por las grandes empresas del sector informático. Permiten obtener una mayor personalización en la solución informática contratada. Requiere mayor conocimiento técnico por parte del contratante.

d. Ventajas de la nube

i. **Acceso desde cualquier sitio y con varios dispositivos.** Los programas y archivos están en la nube, es suficiente una conexión a Internet para acceder a ellos y usarlos de modo remoto. Permite que varias personas trabajen a la vez en un mismo documento en tiempo real. Con respecto a los dispositivos de acceso, actualmente son múltiples: puede ser con PC fijo, un laptop, un tablet PC, un iPad, un smartphone.

ii. **Todo el software está en un solo sitio.** Evita tener que instalar y actualizar programas y archivos en cada uno de los dispositivos y equipos que se utilicen. Solo hace falta tener instalado es un navegador de Internet con el que acceder a la nube y trabajar en ella.

iii. **Ahorro en software y hardware.** En la nube, un mismo programa lo comparten muchos usuarios, sin necesidad de tener que comprar o desarrollar una copia individual para cada uno de ellos. Esto disminuye costos.

iv. **Ahorro en mantenimiento técnico.** Sin programas instalados o redes de PC complejas que configurar y mantener, los usuarios de la nube deben tener menos problemas informáticos. El proveedor de la nube se encarga del mantenimiento técnico de sus propios servidores. El usuario no necesita saber crear redes de computadoras para compartir recursos, porque puede hacerlo a través de la nube.

v. **Escalabilidad.** Un sistema informático es escalable si puede crecer para responder a necesidades más exigentes. Esto es crucial sobre todo para las empresas. Con la nube, la escalabilidad está garantizada sin tener que invertir más de lo necesario. Si un usuario de la nube necesita más o menos capacidad de proceso o de almacenamiento, el proveedor de la nube se lo facilitará casi en tiempo real. Eso optimiza los recursos en todo momento.

vi. **¿Seguridad?** Hay una gran discusión sobre si la nube es o no más segura que los modelos tradicionales y, seguramente, ambas alternativas sean ciertas.

La cuestión parte desde el ambiente de seguridad en TI con que dispone el usuario. Normalmente, la inversión en seguridad es elevada y requiere una inmovilización de fondos que excede las posibilidades de los pequeños usuarios. Generalmente los particulares y las PyMES están en esta

situación y, por lo tanto, son los mayores usuarios de servicios cloud.

No sucede lo mismo con las grandes empresas, en las que la inversión en TI es elevada, generando un ambiente adecuado de confianza en cuanto al resguardo de sus datos. En estos casos, no hay motivos por los cuales acceder a servicios *cloud*, excepto los costos.

e. Inconvenientes de la nube

i. **(Falta de) seguridad y privacidad.** Utilizando los servicios en la nube, los datos ya no se guardan en soportes del usuario, sino que se almacenan *en la nube*, es decir, en soportes del proveedor. Esto implica dejar de tener control sobre ellos porque se transfieren a un tercero. Nunca se puede estar seguro acerca de quién accede a esa información o si está o no protegida con un nivel adecuado de seguridad, menos aún su localización física. Es un riesgo para usuarios particulares y empresas. En ambos casos, deben confiar informaciones internas y confidenciales a un tercero, que puede o no ser fiable. La confiabilidad del servicio depende de la fortaleza técnica y financiera del proveedor del servicio. Aún cuando el proveedor del servicio, a través de los acuerdos de niveles de servicio (SLA), se compromete a llevar un control de la seguridad de la aplicación y la infraestructura - así como de la privacidad de la información almacenada en las instalaciones-, existe riesgo. Se traslada la confianza del resguardo al tercero proveedor. Pero esto puede mitigarse, al menos en parte. La ISO 27001 es para la seguridad de la información. Es una norma redactada por los mejores especialistas del mundo en el campo de la seguridad de la información y su objetivo es proporcionar una metodología para la implementación de la seguridad de la información en una organización. Permite que

una organización sea *certificada*, lo cual significa que una entidad de certificación independiente ha confirmado que la seguridad de la información se ha implementado en esa organización de la mejor forma posible. En *cloud,* la organización cede el control de muchos aspectos de la seguridad, transfiriendo los mismos al proveedor. Aquí son básicas las actividades de respuesta a incidentes. Como también cuestiones de identidad y control de acceso, aislamiento de software y disponibilidad durante una interrupción del servicio.

ii. **Sin Internet no hay nube.** En la computación en la nube todo depende que la conexión a Internet funcione. Si no es así, el usuario no podrá acceder a los servicios ni a sus datos, y sus clientes tampoco.

iii. **Problemas de cobertura legal.** Son varios los problemas legales que pueden generarse Los servidores de la nube pueden estar en cualquier parte del mundo y no está claramente definida la jurisdicción. Si hay problemas, no está claro qué ley debe aplicarse o si ésta podrá proteger al cliente.

iv. **Conflictos de propiedad intelectual u otros.** La información de los clientes ya no está en sus manos, con lo que pueden surgir problemas sobre a quién pertenece.

v. **Protección de datos personales.** El riesgo existe por las posibles violaciones a la protección de datos sensibles, impuesta por las leyes de protección de datos personales y la circulación transfronteriza de la información; por lo tanto, sólo está permitida por acuerdo y con autorización del dueño de los datos, hacia países que cuenten con legislación similar referente a la protección de datos (por ejemplo, España).

Cuestiones contractuales

La utilización de *cloud* a través de la web genera relaciones con efectos jurídicos entre las partes con un elevado grado de complejidad y riesgo. El avance tecnológico es vertiginoso y supera ampliamente la capacidad del derecho para adecuarse y comprender las nuevas situaciones.

En este caso, existen cuestiones que se encuentran en pleno proceso de elaboración, como por ejemplo la doctrina de los medios de prueba y las formas de expresar el consentimiento; en tanto que otras, derivadas del hecho que los centros de datos de la nube pueden estar geográficamente dispersos, requieren una adaptación (como por ejemplo la competencia de los jueces, la ley aplicable y la jurisdicción).

Aquí debemos ubicarnos en las posibilidades que tiene el cliente del servicio de nube de establecer condiciones al momento de contratar. Si por ejemplo, se tratara de *Google*, que contrata con *Amazon* un servicio de nube, es muy probable que *Google* pueda negociar y acordar condiciones en el SLA (*Service Level Agreement*). Pero si se trata de un usuario particular, pequeño como habitualmente sucede, ni siquiera existirá contrato, y de existir, seguramente será un contrato de adhesión que no permitirá al usuario la más mínima especificación y tampoco tendrá a quién contactar en caso de incidentes.

Así, la jurisdicción, la ley aplicable e incluso hasta el idioma del contrato, son impuestos generalmente por el proveedor web. La dependencia generada se dá en términos casi imposibles de cambiar.

En los casos en que pueda celebrarse un acuerdo de niveles de servicio (SLA), que tienen como función, en principio, especificar las expectativas de funcionamiento, establecer responsabilidad, fijar remedios y consecuencias si el servicio no es el acordado por ambas partes, deben tenerse presentes dos principios rectores:

- se transfieren los datos al proveedor del servicio, por lo tanto hay una pérdida de control;
- el grado de dependencia del proveedor de c*loud*;

En este marco, los aspectos generales a contemplar en el acuerdo deben comprender:

- términos de uso: define las especificaciones técnicas relacionadas con la entrega y calidad del servicio;
- lista y definición completa de los servicios brindados por el proveedor;
- acuerdos de Nivel de Servicio, informes periódicos: métrica para determinar si el proveedor suministra en servicio en los términos acordados y un mecanismo de auditoría para evaluarlo;
- cumplimiento de cuestiones legales.

En cuanto a las especificaciones de detalle, debería referirse a:

- **Confidencialidad:** operaciones de traslado de datos y almacenamiento. Los datos deben ser encriptados, tanto en movimiento como en reposo. Los detalles de los algoritmos de encriptación y las políticas de control deben especificarse.
- **Propiedad de los datos:** se debe establecer en el contrato, en forma clara, que la organización mantiene la propiedad de los todos sus datos, pero también debe asegurarse que el proveedor no adquiera derechos o licencias a través de los acuerdos para usar datos en su propio beneficio.
- **Disponibilidad:** se deben especificar el nivel de disponibilidad que el proveedor se compromete a mantener. La garantía de disponibilidad suele perderse cuando el cliente incumple alguna cláusula (como por ejemplo, la demora en el pago de alguna cuota del servicio). Se deben aclarar términos y condiciones para obtenerla nuevamente en caso de corresponder.
- **Niveles de potencia de cálculo, almacenamiento y ancho de banda contratados**: deben asegurarse.
- **Seguridad:** nivel de seguridad en las instalaciones. Lista con medidas de seguridad. Política de gestión de copias de

seguridad, gestión de incidentes. Plan de seguridad y recupero ante desastre.

- **Suspensión del servicio:** guarda más relación con los contratos en los que sólo existe un único servidor. En caso de **cloud**, también puede producirse debido a actualizaciones en la infraestructura informática del proveedor. Si se contrató un servicio 24x7x365, esto no debería suceder.
- **Servicio de soporte:** tiempo que el proveedor necesita para recuperar el sistema cuando se ha producido un error.
- **Modificaciones:** especificar claramente las opciones de modificación del contrato o terminación del mismo. Sobre todo en lo relativo a recuperación y borrado de información.
- **Privacidad y cumplimiento normativo:** detalle de las políticas de privacidad y cumplimiento de la legislación vigente.
- **Duración, permanencia y modificación del servicio**: pueden acordarse desde permanencias mínimas, hasta renovaciones automáticas. Debe preverse la escalabilidad y la reducción de servicio de acuerdo a las necesidades, dado que es uno de los motivos básicos de contratación de servicios *cloud*.
- **Baja del servicio:** se establecen las formas y condiciones en que debe formularse, como así también el momento en que la misma entra en vigencia, la fecha tope para trámites, el estado de la deuda, la migración de datos y aplicaciones a otro proveedor.
- **Garantías postcontractuales:** retorno ordenado de la información, acuerdos de confidencialidad.
- **Precio del servicios:** pagos, cantidad y periodicidad, efectos de la mora, cambios en listas de precios.
- **Jurisdicción y Ley aplicable:** domicilio en caso de controversia.

Cómo se observa, cada ítem específico expuesto implica uno o varios factores de riesgo para el cliente *cloud*. Constituyen a la vez, un listado útil para el auditor en base al cual puede planificar procedimientos para evaluación de riesgos derivados de la contratación.

Cuestiones de control

Cloud computing no está exento de riesgos. Cuanto más compleja es la infraestructura informática utilizada, existen mayores oportunidades e interés en su vulneración.

El siguiente análisis, brinda una síntesis de los principales riesgos y algunas medidas que permiten su mitigación.

f. Principales riesgos de seguridad y privacidad asociados

i. **Abuso y uso malicioso:** las ventajas y oportunidades que se ofrecen también son aprovechadas por piratas informáticos para efectuar sus ataques.

ii. **Fugas internas de información:** los ataques también pueden ser internos: ya sea por acciones deliberadas y mal intencionadas, o bien por fallas humanas involuntarias. Estos acontecimientos suelen traer aparejados perdida de información, con todo lo que ello implica.

iii. **APIS inseguras:** las APIS (*Application Programming Interface)* son el único punto de interacción con los programas que se están ejecutando en la nube. Son la puerta de acceso hacia los servicios, cuando desde una plataforma se pone a disposición información para ser accedida por otras aplicaciones. Por ello, es fundamental contar con una muy buena política de seguridad.

iv. **Suplantación de identidad:** no es un riesgo propio de la nube, pero aquí reviste una relevancia especial. Generalmente los sistemas requieren una identificación (*password*). Dependiendo del uso que se este haciendo del

cloud, pueden resultar poco seguras. Se tiende actualmente a la Federación de Identidades.

v. **Cumplimiento legal:** en nuestro país está vigente la Ley 25326, de protección de datos personales, que impone restricciones de acceso y disponibilidad.

Esta enumeración de riesgos, se enfoca claramente hacia los datos y no es eliminable, porque el cliente los transfiere al dominio de un tercero, en ocasiones aún sin la autorización del dueño. Simplemente, pueden mitigarse si se observan las siguientes medidas de control:

g. Mitigación de riesgos, medidas de control:

i. Virtualización y segmentación:

1. **Virtualización:** varias máquinas virtuales pueden ser ejecutadas en un único servidor, pero cada máquina ejecuta un sistema operativo en forma aislada. Una máquina virtual es una capa de software que se instala entre el hardware y el sistema operativo. Individualmente, son menos vulnerables que un sistema operativo, pero si son varias las que operan simultáneamente, su grado de complejidad aumenta y elimina esa ventaja.
2. **Segmentación de datos**: permite que los mismos residan -fragmentados o no- en diferentes servidores, incluso en distintos centros de datos. Además al mantener datos en varias localizaciones de manera simultánea, se dispone de un sistema de seguridad prácticamente en tiempo real. El prestador debe garantizar los riesgos de la redundancia.

ii. **Control perimetral:** es recomendable la instalación y configuración de un *firewell*, dado que se encarga de monitorear todas las comunicaciones que se realizan desde o

hacia el equipo o la red y decide si las permite o no, dependiendo de las reglas preestablecidas por el administrador del sistema.

iii. **Criptografía**: es recomendable utilizar algún nivel de cifrado para la información que viaja por la nube, preferentemente asimétrica. De este modo, si algún usuario no autorizado intercepta los datos no puede leer su contenido. Protege las conexiones de red entre los usuarios y las aplicaciones de la nube y las conexiones entre los administradores del sistema y los servicios de la nube.

iv. **Gestionar los *logs* del sistema:** Aunque es posible que no se tenga acceso a toda la información sobre los eventos del sistema, se deben almacenar y revisar todos los *logs*; como también realizar copias de seguridad y almacenarlos en lugares distintos. Es recomendable que los *logs* y datos de incidentes se gestiones en forma centralizada.

v. **Protección de datos:** sabida es la sensibilidad de algunos datos y las consecuencias que podría traer para la organización su pérdida o deformación. Por lo tanto debe analizarse cuidadosamente cuales serán los datos que se depositan en la nube.

vi. **Control de integridad. u**tilizar funciones matemáticas –*hash*, para verificar que los datos no han sufrido modificaciones durante el traslado.

vii. **Gestión de cambios:** mantener un historial de modificaciones de los datos o ficheros guardados en la nube.

viii. **Copias de Seguridad:** programar periódicamente copias de seguridad. Permitiendo recuperar datos cuando otras medidas han fallado, asegurando la continuidad del negocio.

ix. **Plan de continuidad del negocio y recuperación ante desastres:** asegurarse que durante una interrupción del

servicio las operaciones criticas se puedan reanudar inmediatamente y el resto en tiempo prudencial.

x. **Control de acceso:** garantizar que los usuarios sólo utilizan los datos y procesos para los que han sido autorizados.

xi. **Políticas de Seguridad:** limitar a los usuarios la posibilidad de borrar elementos del sistema y proteger equipos, como así también impedir el acceso de intrusos.

xii. **Gobernanza:** garantizar que los sistemas sean seguros y que los riesgos estén gestionados es un desafió. Por lo tanto, se requiere instalar adecuadamente los mecanismos y herramientas de auditoría para determinar cómo se almacenan los datos, como se protegen y cómo se utilizan, tanto para comprobar el servicio como para verificar las políticas y estándares en la provisión del servicio.

xiii. **Ubicación de los datos:** un problema es la ausencia de información acerca de cómo se ha implementado la infraestructura, motivo por el cual no se tienen información de cómo y dónde son almacenados los datos. Parte de la solución al problema la aporta que el proveedor posea certificaciones de seguridad o la realización de auditorías externas. Se le suma a esto que la información suele viajar por varios países, con lo cual es más complejo aún establecer un marco regulatorio.

xiv. **Propiedad de los datos:** se debe establecer en forma clara en el contrato que la organización mantiene la propiedad de todos los datos, pero también debe asegurarse que el proveedor no adquiere derechos o licencias a través de los acuerdos para usar datos en su propio beneficio. Es habitual la cesión de derechos sobre datos o fotos en la utilización de servicios *cloud* (por ejemplo *Facebook*).

xv. **Gestión de Riesgos:** la organización debe confirmar que los controles de seguridad están implementados correctamente y

cumplen los requisitos. El establecimiento de un nivel de confianza depende del grado de control que una organización esté dispuesta a delegar en el proveedor para que sea éste quien implemente los controles necesarios. Si el nivel de confianza va por debajo de las expectativas y la organización no puede aplicar medidas correctivas, debe decidirse entre la aceptación de un riesgo mayor o el rechazo del servicio.

También en este caso, la enumeración es útil para la planificación de auditoría, toda vez que cada medida de control sugerida apunta a mitigar un factor de riesgo del sistema.

Auditoría de servicios *cloud*

Sin dudas, la auditoría de servicios *cloud* constituye un nuevo desafío para el contador público como coordinador de equipos de auditoría multidisciplinarios.

La conformación ideal del equipo a nuestro entender debe, necesariamente, incluir un especialista en seguridad informática –nivel 2 o 3- y un abogado, especializado en derecho informático.

Lo primero a definir es a quién se le prestará el servicio, si al proveedor o al contratante, dado que son totalmente diferentes.

Si es al proveedor, además del examen de auditoría informática, es probable que deba extendérsele un informe sobre evaluación de controles –SAS 70, actualmente incluidos en la Resolución Técnica N° 37 de la FACPCE- para que acredite seguridad ante sus clientes.

Si se trata del cliente *cloud*, el servicio se orientará hacia la evaluación de riesgos y controles derivados de su contratación y al grado de seguridad que brinda el servicio a la luz de su utilización para elaborar información financiera.

Posicionándonos desde el lado del auditor del cliente *cloud*, la pregunta es cuáles serían los objetivos de auditoría o qué tipo de procedimientos podemos

aplicar al respecto, atentos a las limitaciones de acceso que seguramente tendremos para el desarrollo de la tarea.

Entendemos que el punto medular es el grado de seguridad de la información que el cliente deposita en el proveedor de servicios *cloud*: por lo tanto, los procedimientos apuntan primordialmente a evaluar los tres requisitos del triángulo CIA: *confidencialidad, integridad y disponibilidad.* Como fácilmente se observa, estos tres requisitos cubren un amplio espectro de riesgo.

Resulta obvio también, que cumplido lo antedicho, es necesario evaluar la información que se utilizará como soporte de Estados Financieros de acuerdo a los parámetros tradicionales, en los casos en que ésta se soporte en servicios *cloud*, como ya sucede, sobre todo, en PyMES.

La cuestión es cuál es el alcance de los procedimientos que pueden aplicarse. Si se trata de evaluación de controles, lo más probable es que no se tenga acceso a los sistemas de control del tercero prestador del servicio, por lo tanto, hay que acudir a métodos alternativos que consisten en verificar que el proveedor acredite certificaciones de calidad o seguridad en cuanto a sus sistemas o suministre un informe SAS 70 tipo 2. Difícilmente pueda ejecutar pruebas de cumplimiento.

Estos elementos no eliminan el riesgo, pero en la medida de su acreditación, elevan el grado de confianza, y sus niveles dependerán del tipo de certificación que se trate. Por ejemplo, a nuestro criterio, una garantía de implementación COBIT brinda un grado de confianza mayor que una certificación ISO 27000.

Con respecto a la aplicación de pruebas sustantivas y analíticas, dependen de la modalidad de servicio contratado. En principio, un servicio IaaS resulta más permeable a la auditoría que un servicio SaaS, dado que en el primero, toda la estructura de TI está disponible, desde los programas, a las redes, a los datos, mientras que en el servicio SaaS, solamente podemos acceder a ingresos y salidas, agravado porque carece de ambiente de *testing*, por lo tanto no son posibles las pruebas con lotes.

En la modalidad SaaS, la aplicación de procedimientos se limita a cotejo de entrada/salida por fuera del sistema, seguimiento de registros de transacciones

y algunas pruebas analíticas, que podrán resultar suficientes o no, depende de las circunstancias.

El principio general es que la modalidad IaaS brinda mayor transparencia que la modalidad SaaS. En cuanto a PaaS, es ambiente de desarrollo, por lo tanto muy específico.

¿Qué referencias toma el auditor para el desarrollo de la tarea? Como siempre, primero, los aspectos legales y las normas vigentes, luego la doctrina y, en este caso, los estándares y normas de calidad, que brindan un amplio marco de referencia para el ejercicio de la tarea.

En la enumeración que sigue, a modo informativo, sintetizaremos el contenido de los más difundidos y utilizados a nivel mundial.

h. Guidelines on Security and Privacyin Public cloud Computing - NIST

En diciembre de 2011, el Instituto Nacional de Normas y Tecnología, dependiente del Departamento de Comercio de Estados Unidos, publica la Norma SP 800-144, referida a una serie de cuestiones a ser tenidas en cuenta en la contratación de una nube pública.

Es un trabajo completo que brinda un marco de referencia adecuado, actualizado y bastante preciso, presentado mediante nueve ítems de control a ser observados.

A continuación, el modelo:

AREAS	RECOMENDACIONES
Gobierno	Extender las prácticas organizativas relativas a las políticas, procedimientos y criterios utilizados para el desarrollo de aplicaciones y la prestación de servicios en la nube, así como el diseño, implementación, pruebas, uso y control de los servicios de empleados o contratados. Establecer mecanismos y herramientas de la auditoría para garantizar las prácticas de organización en todo el ciclo de vida del sistema.
Conformidad	Entender los diferentes tipos de leyes y reglamentos que las obligaciones de seguridad y privacidad imponen a la organización y la computación en nube, especialmente las relacionadas con ubicación determinada, la privacidad y los controles de seguridad, administración de registros y requerimientos legales. Revisar y evaluar las ofertas del proveedor de la nube con

	respecto a los requisitos organizativos que deben cumplir y velar por que los términos del contrato satisfagan adecuadamente los requisitos. Asegurar que las capacidades del proveedor de la nube y los procesos de descubrimiento electrónico no comprometen la privacidad o la seguridad de datos y aplicaciones.
Confianza	Asegurar que los acuerdos de servicios provean medios suficientes de *clustering* para permitir la visibilidad en los controles de seguridad y privacidad y los procesos empleados por el proveedor de la nube, y sus actuaciones en el tiempo. Establecer derechos exclusivos de propiedad claros en el tiempo. Programa de Gestión de Riesgos lo suficientemente flexible como para adaptarse a la constante evolución y el cambio del paisaje de riesgo para el ciclo de vida del sistema. Monitorear continuamente el estado de seguridad del sistema de información para apoyar las decisiones en curso de gestión de riesgos.
Arquitectura	Comprender las tecnologías subyacentes que el proveedor de la nube utiliza para servicios de suministro, incluidas las consecuencias que implicaban los controles técnicos sobre la seguridad y la privacidad del sistema, a lo largo del ciclo de vida completo del sistema y en todos sus componentes.
Gestión de identidades y acceso	Establecer medidas de protección adecuadas que estén vigentes para asegurar la autenticación, autorización y otras identidades para acceder a funciones de gestión, y que sean adecuadas para la organización.
Aislamiento de software	Entender la virtualización y otras técnicas de aislamiento lógico que el proveedor de la nube emplea en su arquitectura de software multi-arrendatario, y los riesgos involucrados por la utilización de multiplexación en máquinas virtuales.
Protección de datos	Evaluar la idoneidad de las soluciones del proveedor de la nube para gestión de datos y la capacidad de controlar el acceso a los mismos, para asegurarlos den reposo, en tránsito, y en uso, y para desinfectarlos. Tome en consideración el riesgo que recopilen datos de la organización con los de otras organizaciones cuyos perfiles. Los datos pueden ser utilizados por el mismo proveedor para transferirlos terceros, fuera del control del cliente, incluso para *phishing*. Entender y sopesar los riesgos involucrados en la gestión de claves criptográficas con las instalaciones disponibles en el entorno de la nube y los procesos de las empresas establecidas por el proveedor de la nube.
Disponibilidad	Comprender los procedimientos contratados para garantizar la disponibilidad, backup y recuperación de datos y recuperación ante desastres, y asegurar que cumplen con la continuidad de la organización y los requisitos de planificación de contingencia. Asegúrese de que durante una grave perturbación intermedia o prolongada o un desastre, las operaciones críticas se pueda reanudar inmediatamente, y que todas las operaciones puedan reanudarse en un tiempo de una manera oportuna y organizada.
Respuesta a Incidentes	Comprender el contrato y los procedimientos para respuesta a incidentes y garantizar que cumplan con los requisitos de la organización. Asegúrese de que el proveedor de la nube tiene un proceso transparente en el lugar y los mecanismos de respuesta suficiente para compartir información durante y después de un incidente.

	Asegúrese de que la organización pueda responder a los incidentes de manera coordinada con el proveedor de la nube de conformidad con sus respectivas funciones y responsabilidades para el entorno informático.

La norma proporciona también un enfoque de acuerdo a la etapa por la cual atraviesa el proceso durante su ciclo:

AREAS	RECOMENDACIONES
Las actividades preliminares	Identificar la seguridad, privacidad y otros requisitos de la organización de servicios en la nube a satisfacer, como criterio para la selección de un proveedor de nube. Analizar los controles de seguridad y privacidad del entorno de un proveedor de la nube y evaluar el nivel de riesgo implicado con respecto a los objetivos de control de la organización. Evaluar la capacidad del proveedor de la nube y el compromiso de ofrecer servicios durante el período de destino y cumplir con la seguridad y la privacidad de los niveles estipulados.
Poner en marcha y actividades coincidentes	Asegúrese que todos los requisitos contractuales se indican explícitamente en el contrato de servicio, incluidas las disposiciones de privacidad y seguridad, y que éstos sean aprobados por el proveedor de la nube. Involucre a un asesor jurídico en la revisión del contrato de servicio y en las negociaciones sobre los términos del servicio. Evalúe continuamente el desempeño de los proveedores de la nube y la calidad de los servicios aprovisionados para asegurar que todas las obligaciones contractuales se cumplan y para gestionar y mitigar los riesgos.
Actividades finales	Avise al proveedor de la nube sobre los requisitos contractuales que deben ser observados a la terminación. Revocar todos los derechos de acceso físicos y electrónicos asignados al proveedor de la nube y la recuperación de elementos físicos y las divisas de manera oportuna. Asegurar que los recursos puestos a disposición de la organización o en poder del proveedor de la nube en los términos del contrato de servicio sean devueltos o recuperados en una forma utilizable, y que la información ha sido borrada correctamente.

i. ITIL - *Information Technology Infraestructura Library* (Biblioteca de Infraestructura de Tecnologías de Información).

Las recomendaciones fueron desarrolladas en los años 1980 por la *Central Computer and Telecommunications Agency* (CCTA) del gobierno británico, como respuesta al incremento en el uso de las tecnologías de la información y la falta de estándares

Se creaban ad hoc pautas de evaluación y en oportunidades se cometían errores, mayores costos y falta de uniformidad a la hora de comparar. La difusión fue recién a mediados de los años 1990.

Básicamente, se trata de un marco para facilitar la implementación de ciclo de vida para la Gestión de Servicios TI organizado en cinco títulos principales:

- Estrategia de Servicio
- Servicio de Diseño
- Transición del Servicio
- Operación del Servicio
- Mejora continua del Servicio

Estos procedimientos son independientes del proveedor y han sido desarrollados para servir de guía, abarcando infraestructura, desarrollo y operaciones de TI. La Gestión de Servicios ITIL se halla integrada en la actualidad en el estándar ISO 2000.

j. COBIT (1996) Objetivos de Control para Sistemas de Información y Tecnología Relacionada

Es, a nuestro criterio, el estándar más completo sobre el tema y además, ampliamente aceptado. Inspirado en COSO que lo precede la Norma ISO 17799 define políticas en materia de control interno sobre la información y sistemas de TI.

El marco referencial se compone de:

- **COBIT Objetivos de control**. Establece un estándar de buenas prácticas de control identificadas en 4 dominio, 34 objetivos de control de alto nivel y 302 objetivos de control detallados.
- **Directrices de Auditoría**. Es una guía para el auditor y establece objetivos de auditoría a satisfacer de acuerdo a la estructura de los objetivos de control y para cada uno de ellos.
- **ERM.** Se refiere a gestión de riesgos.
- **COBIT.** Modelos de madurez.

Su extensión impide el tratamiento, dado que excede el marco de este trabajo, por lo que referimos al estándar en cuanto a su contenido.

k. SAS 70 (*Statement on Auditing Estándar Nº 70*).

Es un estándar de auditoría reconocido internacionalmente y desarrollado por el AICPA (*American Institute of Certified Public Accountants*) en 1992.

El reporte consiste en una revisión centralizada por parte de un auditor independiente (auditor del servicio), de los servicios tercerizados y está diseñado para proveer información a las organizaciones usuarias y a sus auditores, acerca del control interno de la organización de servicios. Es, en principio, una comunicación de auditor a auditor.

El principal objetivo es el de brindar al auditor financiero la evidencia suficiente sobre el grado de control interno dentro de una organización de servicios que ha sido subcontratada por el cliente, limitando su alcance de revisión a los controles del cliente auditado, que dependen del servicio subcontratado y que son relevantes para la producción de información financiera, en la medida que tengan un impacto significativo sobre los Estados Financieros.

Al momento de planificar una auditoria sobre los Estados Financieros del cliente, el objetivo de esta norma es que el auditor puede realizar los procedimientos de revisión del control interno en la organización de servicio o basarse en el informe de otro auditor.

Según establece la norma (SAS 70) existen dos tipos de informes –compromisos- que difieren en la profundidad de los procedimientos aplicados:

- **Tipo I:** informe sobre los controles puestos en marcha, a través del cual se emite una opinión sobre el diseño e implementación de controles internos de la organización de servicios.
- **Tipo II**: informe sobre controles puestos en marcha y pruebas sobre la eficacia operativa de dichos controles; describe la efectividad de la operatoria de los controles diseñados e implementados, emitiendo también una

opinión sobre la efectividad de la operación, referido a un periodo de tiempo determinado, no menor a seis meses.

Un trabajo típico incluye:

- Realizar pruebas en el lugar, en varios puntos en el tiempo para determinar la eficacia de los controles puestos en operación y la efectividad operativa de los controles (informes de tipo II).
- Pruebas, que por lo general incluyen la investigación, inspección y observación.
- Preparación de un proyecto de informe que será revisado por el servicio de organización para la exactitud e integridad de los datos.
- La entrega de una carta a la administración de cualquier control deficiente cubiertas durante el curso de la revisión.
- Emisión del informe SAS 70 en versión impresa y electrónica .pdf

SAS 70 es por lo tanto un estándar para los usuarios de centros de datos que tiene por objetivo, brindar un aseguramiento sobre la seguridad del mismo y que opera bajo sistemas de control adecuados.

Cabe mencionar que la Resolución Técnica N° 37 de la FACPCE incluye este tipo de servicios en forma específica.

I. *ISO Internacional Organization for Standarization* (Organización Internacional para la Estandarización)

Es una organización no gubernamental organizada como una Federación Mundial de Organismos Nacionales de Normalización.

Las normas ISO surgen para armonizar la gran cantidad de normas sobre gestión de calidad y seguridad existentes en los distintos países.

Familia ISO 27000: esta serie tiene como objetivo definir requisitos para un Sistema de Gestión de la seguridad de la Información (SGSI), con el fin de garantizar la selección de controles de seguridad adecuados para proteger la información y está compuesta por:

- **ISO 27000:** publicada el 1 de Mayo de 2009, esta norma proporciona una visión general de las normas que componen la serie 27000, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción del ciclo Plan-Do-Check-Act y términos y definiciones que se emplean en toda la serie 27000. Está siendo revisada, con fecha prevista de segunda edición para mayo de 2013.
- **ISO 27001**: publicada el 15 de octubre de 2005, es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. En su anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. Actualmente, este estándar se encuentra en periodo de revisión en el subcomité ISO SC27, con fecha prevista de publicación de segunda edición en mayo de 2013.

m. ISAE 3402: Norma Internacional sobre Aseguramiento Nº 3402 – Informes de Aseguramiento sobre los Controles en una Organización de Servicio Comité Internacional de Normas y Estándares de Auditoria (IAASB) – diciembre 2009. SSAE 16. Declaración sobre normas de aseguramiento Nº 16 – Informe sobre los Controles en una Organización de Servicio – Diciembre 2010 – AICPA

SSAE 16 e ISAE 3402, requiere de la aseveración por escrito de la administración de una organización de servicios, acerca del alcance y objetivos de contratación de un auditor de servicios. Esto implica la asignación de responsabilidades adicionales a la administración de las organizaciones de servicio. Las intervenciones de los auditores de servicio, estarán basadas en las aseveraciones, por lo que la administración debe proporcionar una aseveración por escrito, aún cuando el auditor siga informando sobre le tema.

La descripción del sistema debe incluir:

- Objetivos de control y controles relacionados.
- Aspectos del marco de control interno de la organización alineado con COSO.
- Los tipos de servicios prestados, incluidas las diferentes clases de transacciones procesadas.
- Los controles compensatorios pertinentes de las entidades usuarias.
- Procedimientos y registros contables relacionados con los servicios prestados, incluido el inicio, autorización, registro, procesamiento y corrección de las transacciones.
- Cualquier cambio en el sistema durante el periodo cubierto por el informe.
- Hechos y condiciones relevantes adicionales a las transacciones.
- El proceso utilizado para elaborar reportes y otra información para las entidades.

Se requiere la opinión sobre el diseño de los controles para todo el periodo bajo examen. El cambio relevante en el ISAE 3402 es que el reporte no sólo contendrá la descripción de controles, sino una carta firmada por la misma organización de servicios, adonde asegura que razonablemente los controles permiten el logro de los objetivos de control. Este documento se conoce como la aseveración de la gerencia.

Respecto del SAE 70 tipo I no se han introducido modificaciones significativas, en lo concerniente al tipo II tanto la presentación como el diseño deberán ser

evaluados en todo el período sujeto a examen y cualquier cambio significativo que sufra el sistema de control deberá ser revelado por la gerencia de la organización, y evaluado y probado por el auditor.

SSAE 16 sólo informa sobre los controles relacionados con la información financiera. Si se requieren garantías de los controles directamente relacionados con los centros de datos, incluyendo la privacidad, seguridad y disponibilidad; se requiere un SOC 2 informe.

n. Servicio de organización de controles (SOC)

Son informes de control interno sobre los servicios prestados por una organización de servicios, que proporcionan información que los usuarios necesitan para evaluar y mitigar los riesgos asociado a un servicio externo.

Las modalidades son:

- **SOC 1.** Informe sobre los controles de una organización de servicios relacionados con el usuario interno sobre la información financiera (SSAE 16).
- **SOC 2.** Informe sobre los controles en una organización de servicios relacionados con la disponibilidad, proceso de integridad, confidencialidad o privacidad.
- **SOC 3**. Informe para organizaciones de servicio.

o. COSO de gestión de riesgos empresarios *cloud computing*:

El Comité de Organizaciones Patrocinadoras de la Comisión *Treadway* (COSO), es una iniciativa conjunta de cinco organizaciones del sector privado y se dedica a proporcionar liderazgo de pensamiento a través de la elaboración de marcos y orientaciones sobre la gestión de riesgo, control interno y disuasión del fraude.

Es una guía en el seguimiento de los principios de la Gestión de Riesgos -ERM – Marcos integrados para evaluar y mitigar los riesgos derivados de la computación en la nube.

Específicamente aborda:

- Concepto de *cloud computing*.
- Oportunidades y riesgos.
- Aplicación del Marco COSO ERM a las opciones del *cloud*.
- Recomendaciones a los riesgos de *cloud*.

Con respecto a la aplicación del Marco COSO a las opciones de *cloud*, el enfoque es desde los cinco componentes de sistema de control interno COSO (ambiente de control evaluación de riesgo, actividades de control, comunicación y monitoreo), adecuado a una marcada evaluación de riesgos según COSO II.

Además, contiene una lista de preguntas que los miembros del Consejo de Administración de una organización deberían considerar:

- ¿Quién en la gestión es responsable de entender y gestionar los riegos empresariales asociados con la computación en la nube?
- ¿La administración cuenta con procesos eficaces para controlar la computación en la nube?
- ¿Qué están haciendo los competidores con respecto a la computación en la nube?

as definiciones de control interno y los objetivos del marco de trabajo no han cambiado. El control interno se define como un proceso destinado a garantizar tres objetivos razonables: garantía de la eficacia y eficiencia de las operaciones, información confiable y cumplimiento de leyes y reglamentos. Asimismo, según la definición de COSO, “el riesgo es la posibilidad de que un evento ocurra y afecte adversamente el logro de los objetivos”.

Ante los cambios en el entorno operativo del negocio frente a servicios *cloud* la gerencia debe entender que con la mayoría de soluciones nube, la organización tiene menos control directo de la solución y por lo tanto mayor riesgo inherente.

El informe brinda una serie de recomendaciones respecto de los riesgos más significativos y la posible respuesta desde las medidas de control. Una síntesis a continuación:

Riesgo	Respuesta
Posibilidad de desarrollo e implementación de actividades no autorizadas por la Dirección en la nube	Definición de políticas y controles aplicables a la nube.
Falta de transparencia en la contratación y procesos.	Evaluación del ambiente de control CSP
Seguridad, cumplimiento, fuga de datos.	Clasificación de datos (activos) políticas y procesos.
Transparencia y renunciar al control directo sobre los datos,	Administración de supervisión y operaciones de vigilancia de controles,
Fiabilidad, rendimientos de alto valor, incidentes, ataques, respuestas.	Gestión de incidentes. Una organización debe evaluar la capacidad del CSP para ofrecer una adecuada respuesta a incidentes, además de sus propios procedimientos de respuesta a incidentes de interrupción del sistema y los escenarios de robo de datos.
Incumplimiento de la normativa	Seguimiento del entorno externo
Proveedores de tecnología	Elaboración de una estrategia de salida
Incumplimiento con los requisitos de divulgación	Nuevas revelaciones en la información financiera.

Conclusiones

En principio, y desde la posición del contratante del servicio podríamos concluir que:

- es una solución que conlleva un cierto grado de riesgo;
- este riesgo está en función al grado de criticidad de la información que se envía a la nube y del riesgo derivado de los procesos que involucra;
- resulta necesario en forma previa a tomar una decisión, realizar un inventario de activos, clasificarlos y evaluar los riesgos;
- al momento de formalizar el SLA, debe consultarse con un abogado especializado;

- la utilización por parte del estado, hoy parece no aconsejable para la información estratégica;
- deben destruirse los mitos, pero también los fantasmas: es muy común que aún considerando los riesgos de la transferencia de datos a un tercero, la evaluación en general de la seguridad que dispone un usuario haga le resulte aconsejable subir a la nube.

En cuanto al auditor, debe afrontar el nuevo desafío ante los avances tecnológicos. También constituyen una oportunidad inmejorable.

La tarea será necesariamente multidisciplinaria, sin embargo, no nos caben dudas que la coordinación compete al contador público, por su incumbencia en auditoría y su formación específica en sistemas de información, que trasciende lo técnico e incluye los aspectos legales.

Los especialistas en sistemas, cumplen en esta ocasión una función inestimable desde sus competencias en cuestiones de seguridad lógica y aspectos funcionales de los servicios contratados y técnicos de sistemas, en tanto que los asesores legales brindan un valioso aporte desde su especialización en derecho informático, una rama joven del derecho y sobre normas de contratación en el campo del derecho internacional privado. Llegada la instancia, la asesoría en materia penal tiene también su espacio en este esquema.

Las normas de referencia para esta tarea fueron citadas, y particularmente en nuestro país, la Resolución Técnica Nº 37 de la FACPCE trata, específicamente, los informes que se requieren y el trabajo de un experto.

Nótese que con respecto al trabajo de un experto, la Resolución citada dispone –II.b.9- que: “Cuando el contador utiliza el trabajo de un experto, evaluará si el experto tiene la competencia, la capacidad, la objetividad y la independencia necesarias para sus fines, dependiendo del riesgo involucrado”. El contador debe poseer una cierta capacitación que le permita comprender, para poder cumplir estos requisitos.

Los objetivos de auditoría ya fueron planteados, pero a modo de resumen:

- evaluación de la eficacia del control interno de los servicios y seguridad (provistos por el proveedor en la nube);
- identificación las deficiencias de control interno dentro de la organización del cliente y su interrelación con el proveedor del servicio;
- evaluación de la certificación del proveedor en materia de control interno;
- evaluación del proceso de empatía entre los sistemas de control del proveedor y del usuario;
- selección de los parámetros a utilizar en la labor: existe una amplia gama de estándares y normas, en función de los cuales se realizará el trabajo de auditoría.

Básicamente, la auditoria debería cubrir:

- **Cuestiones de gobernabilidad:** la relación entre el proveedor y el cliente. Aspectos de control. Contratación.
- **Manejo de crisis – plan:** alcance del plan, selección de escenarios, probabilidad de ocurrencia, y respuestas. Pruebas de mantenimiento.
- **Seguridad de la información:** ***confidencialidad, integridad, disponibilidad.*** Políticas, monitoreo, manejo de incidentes, implementación y seguimiento de políticas al efecto, selección de tecnologías de seguridad. Protección de activos, fundamentalmente datos.

CAPÍTULO 2

AUDITORÍA DE LOS INTRUMENTOS FINANCIEROS DERIVADOS

Ana María Cóccaro

La Universidad debe tener un alma que la haga vivir,
y esa alma deber ser forjada de ciencia,
de ilustración y de amor...

JOAQUÍN V. GONZÁLEZ

Resumen

Los instrumentos financieros derivados son una herramienta de gestión de riesgos (eminentemente financieros) que las empresas utilizan con asiduidad en los últimos tiempos, como consecuencia de la modernización de la gestión empresarial y la revelación cada vez más frecuentes de escándalos financieros, cuyo ejemplo más sonoro sea quizás el caso *Lehman Brothers Inc.* en los Estados Unidos. Por tratarse de un producto nuevo y sofisticado es importante conocer los estándares internacionales definidos en materia contable y auditoria, siendo este ultimo el objetivo del presente trabajo. La Norma Internacional de Auditoría 1012 “Auditoría de Instrumentos Financieros Derivados”, describe los procedimientos a aplicar para opinar sobre la razonabilidad de los instrumentos financieros derivados de un ente.

El presente trabajo analiza en forma detallada cada uno de estos procedimientos, con el fin de que los auditores que enfrentan el desafío de auditar estos nuevos productos cuenten con un marco teórico conceptual para llevar a cabo sus labores en forma adecuada y de acuerdo a los estándares internacionales.

Introducción

Los instrumentos financieros derivados han surgido como instrumentos de cobertura en respuesta a la volatilidad que a lo largo del tiempo han experimentado los tipos de cambio, las tasas de intereses, los precios de las acciones, los bonos como también de materias primas (*commodities*) y diversos instrumentos financieros. En la actualidad, son utilizados para administrar activos/pasivos y especulación, donde los agentes financieros obtienen ventajosas ganancias por la variación de los precios de los subyacentes.

Los derivados se negocian tanto en mercados OTC[1] (*Over The Counter*) como en mercados organizados. Los productos negociados en los mercados OTC se adaptan a las necesidades particulares de los contratantes, por lo que no presentan la característica de la estandarización, en tanto los que se negocian en los mercados organizados tiene como principal característica que son estandarizados.

Uno de los mercados organizados más importantes de productos derivados a nivel mundial es el *CME Group* de Chicago, producto de la fusión de tres de las bolsas estadounidenses más importantes, la *New York Mercantile Exchange* o Bolsa Mercantil de Nueva York (NYMEX) que constituye la bolsa de materias primas (*commodities*) más importantes del mundo donde se negocia el mayor volumen de opciones y futuros de éstas; el *Chicago Mercantile Exchange* (CME), su fuerte competidor; mercado en el que no sólo se negocian productos relacionados con materias primas sino que también se intercambian derivados de productos financieros, como tasas de interés, índices bursátiles, divisas, bonos y acciones; y por último el *Chicago Board of Trade* (CBOT), donde se negocia todo tipo de derivados.

[1] OTC: Mercados no organizados.

Objetivo del trabajo

Los instrumentos financieros derivados son productos nuevos y sofisticados, y por ello es importante conocer los estándares internacionales definidos en materia contable y auditoría, siendo este último el objetivo del presente trabajo.

La Norma Internacional de Auditoria 1012 “Auditoria de Instrumentos Financieros Derivados”, describe los procedimientos a aplicar para obtener evidencias sobre la razonabilidad de los instrumentos financieros derivados de un ente. El propósito de este trabajo es brindar un análisis de los procedimientos de auditoría, con el fin de que el profesional que enfrenta el desafío de auditar las afirmaciones contenidas en los estados financieros relacionados con los instrumentos financieros derivados cuente con un marco teórico conceptual para llevar a cabo sus labores en forma adecuada y de acuerdo a los estándares internacionales.

Instrumentos Financieros Derivados

Marco Referencial

Para cumplir con el objetivo antes planteado, se presentará el siguiente marco teórico conceptual necesario para llevar a la auditoría: la descripción de los instrumentos financieros derivados enfocados hacia el conocimiento de nuevos productos.

La principal característica de los tiempos que nos toca vivir es el cambio. Nuestra sociedad está atravesando una drástica revolución, cuyas causas últimas son los profundos avances que se producen cada día, en el tratamiento y difusión de la información. Si el cambio afecta de manera decisiva a cualquier manifestación de la actividad humana, la profesión contable no puede sustraerse a estas profundas mutaciones. En consecuencia, el auditor debe desarrollar su labor teniendo como objetivo principal el prepararse para el cambio. Con ello, estaremos desarrollando la capacidad de la persona para enfrentarse a problemas y decisiones no necesariamente idénticos a los contenidos en los libros de estudio. Desarrollar la auditoría desde el punto de

vista de los procedimientos de auditoría es, sin duda, limitarla sólo a sus funciones históricas.

La auditoría tiene hoy distintas características, por ejemplo:

- su vinculación con la realidad económica;
- su confiabilidad al servicio de los usuarios en la toma de decisiones;
- su carácter de disciplina formalizada;
- su contenido social como consecuencia de la responsabilidad social de la unidad económica.

A estos puntos habría que añadir el proceso de armonización y globalización de las normas de auditoría. Entre las posibles características actuales de nuestra disciplina, hay que subrayar especialmente la relativa a la responsabilidad social. Por lo tanto, es necesario que el profesional conozca su responsabilidad social futura y que, en consecuencia, en los encuentros de profesionales se discutan cuestiones tales como:

- el papel importante de la información y con ello, el auditar el buen funcionamiento de los mercados de todo tipo de factores, de productos de trabajo y financieros;
- su contribución a la propia estabilidad de la sociedad y el desarrollo económico de la misma.

Junto a la responsabilidad social, la formación ética cobra una importancia singular que debe impregnar toda la disciplina y, con ello, la actitud profesional, más allá de cuál sea la materia a auditar. Se trata de animar efusivamente a los profesionales en el ejercicio de la capacidad de juicio y de criterio, combinado con la búsqueda y manejo de fuentes bibliográficas. La búsqueda de información es trascendental en nuestros tiempos. Ya no importa tanto tener conocimientos sino saber buscarlos en el momento y en el lugar adecuado.

Concepto

Un derivado es un instrumento cuyo valor se encuentra referenciado al de un activo subyacente, que puede ser una materia prima, una acción, un bono, una tasa de interés, una divisa, un índice, un futuro, entre otros; es decir, si el

contrato establece una compra-venta de soja, el valor del contrato dependerá del valor de la soja al final del mismo.

Los derivados pueden establecer un derecho o una obligación de realizar una determinada operación en una fecha futura a un precio preestablecido a la hora de suscribir el contrato. Los activos más utilizados en los contratos derivados incluyen acciones, bonos, materias primas (*commodities*), tales como: soja, algodón, oro, además de monedas, tasas de interés e indicadores del mercado. Hoy, los derivados de tasa y moneda representan más del 70% de los derivados que se comercializan. Las principales características de estos instrumentos financieros son:

- su valor cambia en respuesta a los cambios de un activo subyacente;
- se requiere una inversión inicial muy pequeña o nula;
- se liquidan en una fecha futura.

Actividades con los Derivados

El uso de derivados está asociado principalmente a tres tipos de actividades por parte del ente.

- Cobertura (*hedgers*): inmunizar los riesgos de variables financieras o precios de bienes (*commodities*). Los agentes financieros utilizan cobertura porque son adversos al riesgo.
- Especulación o negociación (*speculators*): aprovechar el aplacamiento para obtener altas tasa de interés. Los agentes financieros utilizan la especulación porque son indiferentes o neutrales al riesgo.
- Arbitraje (*arbitraguers*): aprovechar la falta de sincronización entre los precios en el mercado de contado y el mercado de derivados, a través de la ejecución simultanea de operaciones de compraventa, para obtener un rendimiento positivo con una inversión inicial nula.

Generalmente han sido utilizados para cobertura de riesgos asociados a un negocio o fines especulativos, lo cual ha hecho crecer al mercado de los Derivados. Por ejemplo, suponga por un momento que una empresa genera sus flujos de efectivo en pesos, y emite una deuda en dólares con la

finalidad de aprovechar una tasa de interés más baja; en este caso, la empresa estaría expuesta el riesgo de tipo de cambio por aumentos en el mismo. Para hacer la cobertura, la empresa podría comprar los dólares a un precio específico con fecha de entrega al vencimiento de la deuda.

Clases de Instrumentos Financieros Derivados

Los instrumentos financieros derivados más conocidos en los mercados financieros son:

- los contratos futuros o *forwards*;
- los intercambios de flujos de efectivo o *swaps*;
- las opciones.

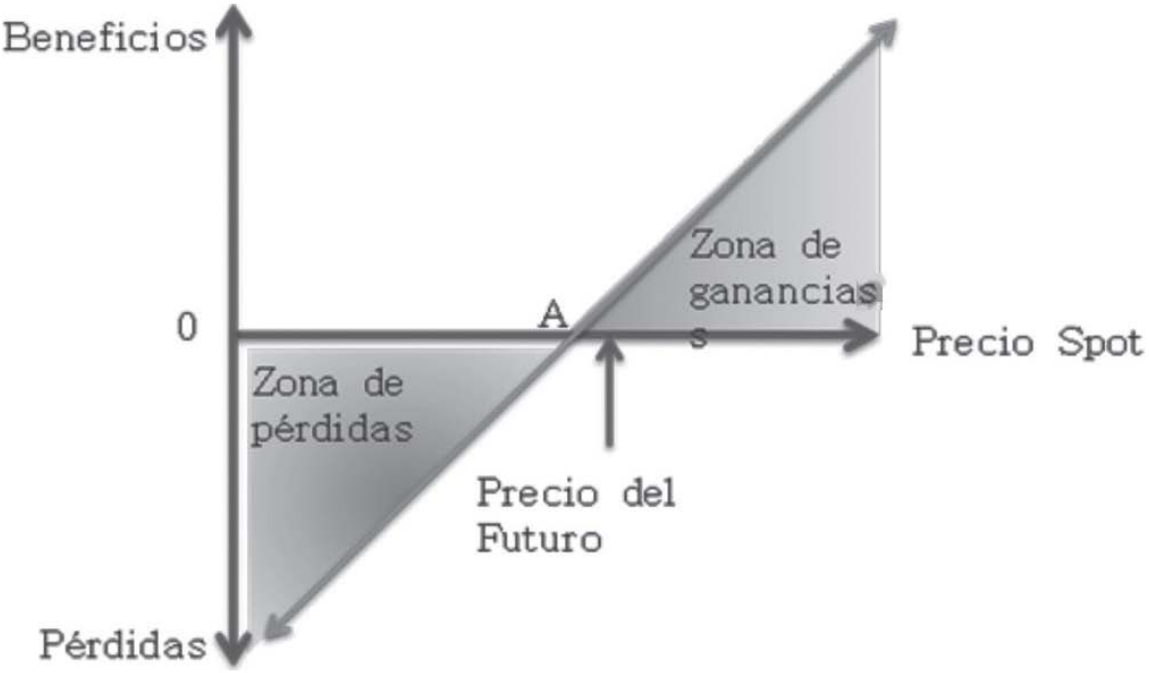
En los mercados organizado o bursátiles se negocian los futuros y las opciones. Las características de estos instrumentos se encuentran estandarizadas y se puede acceder a las cotizaciones en las bolsas donde se negocian. En los mercados no organizados o OTC se negocian los *forwards* y los *swaps*, instrumentos no estandarizados. Estos instrumentos son elaborados a la medida de las necesidades de los suscriptores, por lo que su valor no se puede obtener de la cotización de un mercado organizado.

Futuros

Los futuros son contratos que establecen la obligación de realizar la compra o la venta del subyacente, también a un precio previamente establecido y en una fecha futura. A continuación se gráfica un futuro con una posición larga, donde ambas partes tienen la obligación de realizar la compraventa y no se paga una prima, solamente se debe cancelar una garantía. Si el precio del subyacente en el mercado de contado se encuentra a la derecha del precio del futuro se tiene ganancias, y a la izquierda se obtendría una pérdida inevitable.

Gráfico N°1[2]

Compra de un futuro



Forwards

Los *forwards* son contratos que presentan las mismas características que los futuros, la única diferencia es en cuanto al mercado donde son negociados. El comportamiento de dichos instrumentos es igual al ejemplificado en el gráfico n° 1. Si el precio del subyacente en el mercado de contado se encuentra a la derecha del punto de equilibrio, se tienen ganancias, y a la izquierda, se obtendría una pérdida inevitable.

Swaps

Los *swaps* o permutas son contratos mediante los cuales dos partes se comprometen a intercambiar una serie de flujos de efectivo en una fecha futura, basados en un subyacente y una cantidad de principal determinado.

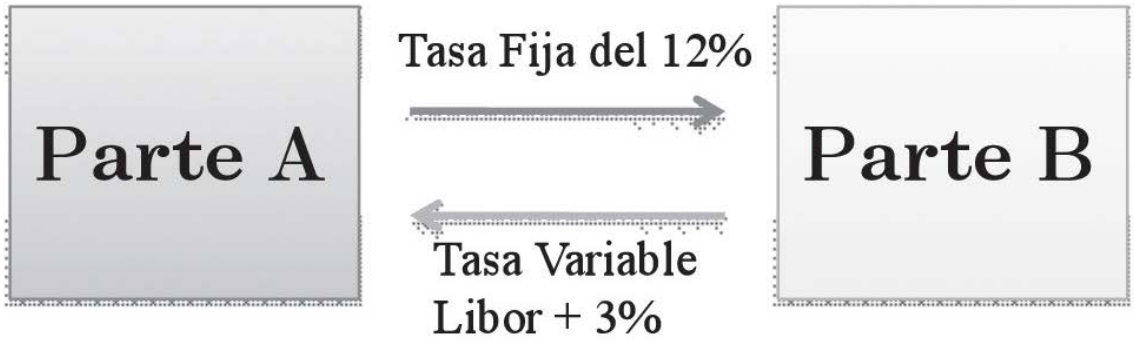
El siguiente gráfico muestra un ejemplo de *swap* de tasas de interés. Mediante este instrumento, dos contratantes acuerdan intercambiar flujos basados en

[2] Figueroa, Vernor Mesen. "La Auditoría de los Instrumentos Financieros Derivados".

una tasa de interés: una parte fija, una tasa variable y la otra fija. La premisa básica para llevar a cabo este tipo de contratos es que las partes tienen ventajas en las tasas inversas a las preferencias de endeudamiento. Por ejemplo. A tiene ventaja en tasa fija, pero prefiere endeudarse a tasa variable, y B tiene ventaja en tasa variable pero prefiere endeudarse a tasa fija, por lo cual deciden intercambiarse los flujos de efectivo de manera que ambos obtienen mejores tasas de las que hubiesen obtenido sin la permuta.

Gráfico N° 2[3]

Swap de intereses



Opciones

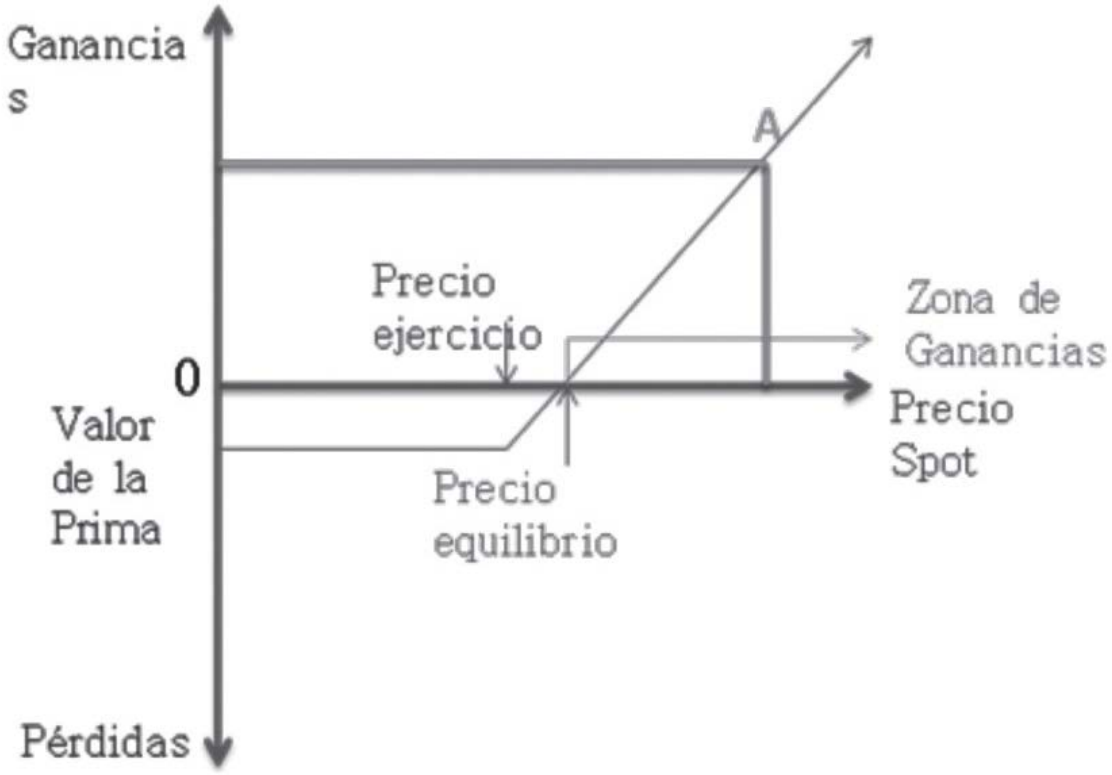
Las opciones son contratos que brindan al suscriptor el derecho pero no la obligación de realizar la compra (*call*) o venta (*put*) del subyacente, en una fecha futura, a un precio de ejercicio previamente establecido, para lo cual el comprador de la opción paga una prima. El gráfico No 3 muestra una posición larga en una opción de compra, la cual le da derecho al comprador -pero no obligación- de comprar en una fecha futura el subyacente a un precio previamente pactado. En este caso el comprador tiene la expectativa de que los precios del subyacente van a subir: de cumplirse su expectativa y sobrepasar el precio de ejercicio, obtendría una ganancia al comprar el subyacente a un precio más bajo que en el mercado de contado. En el gráfico se puede observar esta zona a la derecha del punto de equilibrio; a la izquierda

[3] Figueroa, Vernor Mesen. La Auditoría de los Instrumentos Financieros Derivados.

de dicho punto no se ejerce la opción y la pérdida se limita a la prima cancelada.

Gráfico N° 3[4]

Compra de una opción *call*

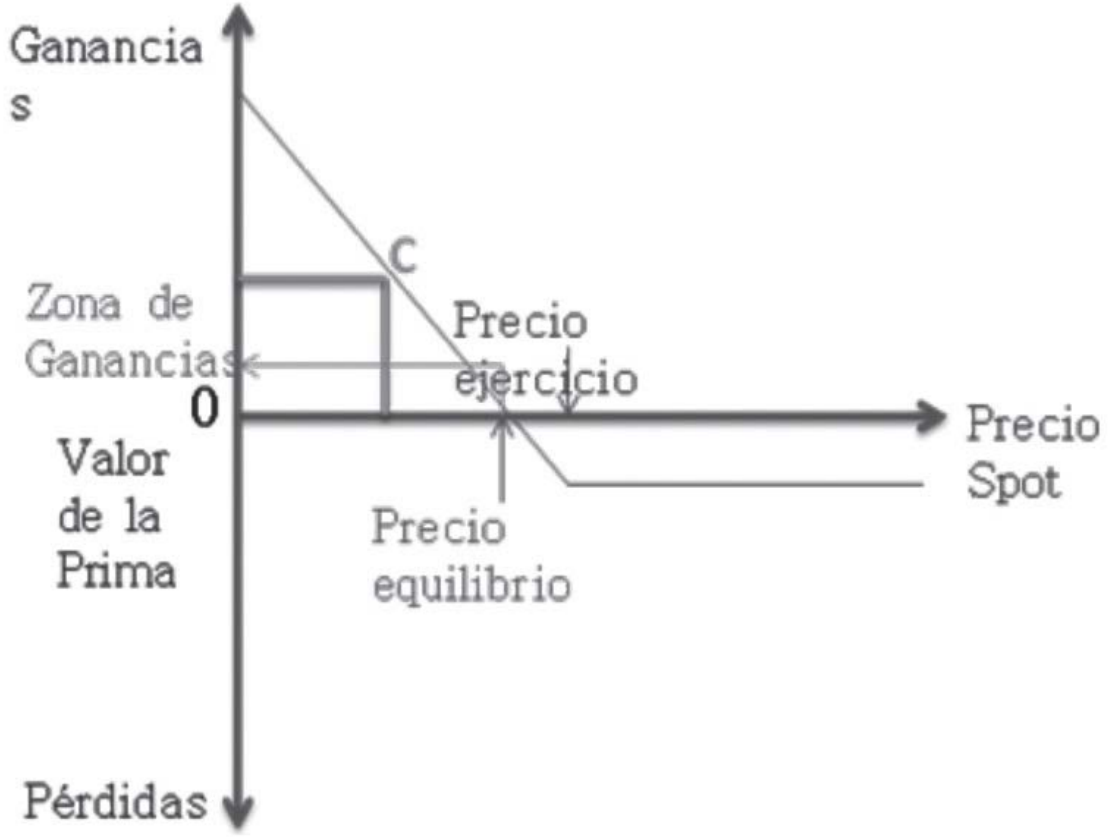


En el gráfico N° 4 se observa una posición larga en una opción de venta, en este caso el comprador tiene el derecho pero no la obligación de vender el subyacente al precio de ejercicio. Es la posición contraria al gráfico n° 1, adonde el suscriptor gana si los precios bajan, puesto que tiene la posibilidad de vender a un precio más alto que en el mercado del subyacente, por lo tanto, la zona de ganancias se encuentra a la izquierda del punto de equilibrio.

[4] Figueroa, Vernor Mesen. La Auditoría de los Instrumentos Financieros Derivados.

Gráfico N° 4[5]

Compra de una opción *put*



Norma Internacional de Auditoría 1012

"Auditoría de Instrumentos Financieros Derivados"

La Norma Internacional de Auditoría 1012 "Auditoría de Instrumentos Financieros Derivados" es la norma de auditoría que brinda las pautas al auditor para opinar acerca de la razonabilidad de los instrumentos derivados contenidos en los estados financieros del ente.

[5] Figueroa, Vernor Mesen. La Auditoría de los Instrumentos Financieros Derivados.

Responsabilidad de la gerencia

La NIA 200[6] establece que la gerencia del ente es responsable de la preparación y presentación de los estados financieros. Como parte del proceso de preparación de dichos estados financieros, la gerencia efectúa afirmaciones especificas relacionadas con los instrumentos financieros derivados. Los responsables de la dirección de un ente, a través de la supervisión de la gerencia, son responsables del diseño y la implementación de un sistema de control interno para:

- monitorear el riesgo y el control financiero;
- dar una seguridad razonable de que el uso de instrumentos derivados del ente que cumple con las políticas de gestión;
- asegurar que el ente cumple las leyes y los reglamentos aplicables;
- la integridad de los sistemas de contabilidad y de presentación de información financiera del ente con el fin de asegurar la confiabilidad de la presentación de información contable sobre actividades relacionadas con instrumentos financieros derivados por parte de la gerencia.

Responsabilidad del Auditor

La NIA 200[7] establece que el objetivo de la auditoría es permitir al auditor expresar en un dictamen si los estados financieros han sido preparados en todos los aspectos significativos de acuerdo con el marco aplicable de presentación de información financiera.

La responsabilidad del auditor en relación a los instrumentos financieros derivados, en el contexto de la auditoría de estados financieros tomados en conjunto, es considerar si la afirmaciones de la gerencia relacionadas con los derivados, dan como resultado estados financieros preparados en todos sus aspectos significativos de acuerdo con el marco aplicable de presentación de información financiera.

El auditor puede necesitar conocimientos y aptitudes especiales para planificar y desarrollar procedimientos de auditoría en relación con ciertas afirmaciones

[6] NIA 200. Objetivo y Principios Generales que rigen una Auditoria de Estados Financieros.
[7] NIA 200. Objetivo y Principios Generales que rigen una Auditoria de Estados Financieros.

sobre instrumentos derivados. Las aptitudes y conocimientos especiales, que también son aplicables para los miembros del equipo de trabajo, incluyen:

- las características operativas y el perfil de riesgo de la industria en la cual opera el ente;
- los instrumentos financieros derivados utilizados por el ente y sus características;
- el sistema de información del ente en relación con los instrumentos derivados;
- los métodos de evaluación del instrumento derivado;
- los requisitos del marco de presentación de información financiera en cuanto a las afirmaciones incluidas en los estados financieros relacionados con los instrumentos derivados.

Aspectos claves en la planificación del auditor

A continuación se describe el conocimiento del ente y los procedimientos de auditoría específicos que el auditor debe tener en cuanto a su planificación y desarrollo de su tarea, a efecto de poder obtener evidencias de auditoría validas y suficientes acerca de la razonabilidad de las afirmaciones contenidas en los estados financieros relacionados instrumentos financieros derivados.

Conocimiento del ente y de su entorno

En primera instancia, todo auditor debe conocer y por ende documentar en forma apropiada los aspectos que tienen relación directa con la gestión que la administración del ente hace de los instrumentos derivados de su propiedad:

- conocimiento del negocio y la industria;
- factores económicos con grado de influencia sobre la naturaleza y extensión de los derivados del ente;
- conocimiento y experiencia de la administración;
- disponibilidad de información oportuna y confiable de la administración;
- objetivos para el uso de los derivados.
-

Identificación de los riesgos financieros clave con derivados

El auditor toma conocimientos de los principales tipos de riegos financieros relacionados con las actividades y los instrumentos derivados a los cuales puede estar expuesto el ente. Ellos son:

- Riesgo de mercado: se relaciona con las pérdidas económicas causales por cambios adversos en el valor razonable del instrumento derivado, tales como tasa de interés, tipo de cambio, índice de precios o precios subyacentes entre otros.
- Riesgo crediticio: se relaciona con el riesgo de que un cliente o contraparte no cumpla con una obligación por su valor total, ya sea a su vencimiento o en cualquier momento posterior.
- Riesgo de liquidación: es el riesgo de que una parte de la operación se liquide sin recibir valor del cliente o contra-parte.
- Riesgo de solvencia: se relaciona con el riesgo de que el ente no tenga fondos disponibles para cumplir con los compromisos de pago a medida que vence.
- Riesgo legal: se relaciona con las perdidas resultantes de una acción legal o reglamentaria que invalida o impide el cumplimiento por parte del usuario final o su contraparte, según los términos del contrato o los acuerdos de compensación de saldos relacionados.

Evaluación de riesgos y ambiente de control

El auditor realizará la evaluación de riesgos y control interno que le permita a este último establecer tanto el nivel de confianza que puede depositar sobre los controles implementados por el ente para el manejo operativo y contable de sus instrumentos derivados como definir la naturaleza, extensión y oportunidad de las pruebas adicionales de auditoría que debe llevar a cabo para probar la razonabilidad del componente sujeto de su examen. Los aspectos que engloba una evaluación de riesgos y de control interno se detallan a continuación:

-Riesgo Inherente. De acuerdo con la NIA 200[8], el riesgo inherente es "la susceptibilidad de una aseveración a una declaración inexacta que podría ser significativo, en forma individual o en conjunto con otras declaraciones inexactos, en el supuesto de que no existieran controles relacionados".

En el caso particular de los instrumentos financieros derivados, estos usualmente tienen un alto riesgo inherente, dado que resulta bastante difícil para el auditor obtener evidencia de auditoría acerca de la intención con la cual dichos instrumentos financieros fueron adquiridos. Además, su registro contable es muy complejo y la susceptibilidad a cambios en su valor hacen muy probable el que la administración de un ente pueda incurrir en errores significativos en su valuación y exposición. Factores que podrían afectar el análisis del riesgo inherente en las afirmaciones sobre derivados son:

- los propósitos económicos y comercial de las actividades del ente con derivados;
- las actividades con derivados van desde posiciones donde el objetivo primario es reducir o eliminar el riesgo a posiciones donde el objetivo es la especulación;
- la complejidad del derivado;
- la operación que dio origen al derivado involucró el intercambio de dinero o no;
- la experiencia del ente con los derivados;
- el derivado es una característica incorporada en un acuerdo;
- los factores externos que afectan al derivado;
- el derivado es negociable en bolsa de valores nacionales o extranjeras;
- el derivado puede exceder el valor reconocido en los estados financieros.

-Riesgo de Control. De acuerdo con la NIA 200[9], el riesgo de control es "el riesgo de que el control interno de una entidad no prevenga, detecte o corrija en forma puntual cualquier declaración inexacta que pudiera ocurrir en una

[8] NIA 200. Objetivo y Principios Generales que rigen una Auditoria de Estados Financieros.
[9] NIA 200. Objetivo y Principios Generales que rigen una Auditoria de Estados Financieros.

aseveración y que podría ser significativa, en forma individual o bien en conjunto con otras declaraciones inexactas".

En materia de auditoría de instrumentos financieros derivados, es muy frecuente que el auditor afronte un riesgo de control alto, en vista de que por la naturaleza y complejidad de los instrumentos derivados, resulta difícil y costoso que la administración de un ente diseñe y opere controles importantes sobre este tipo de operación. Esta situación limita notablemente la prevención o detección y corrección de errores significativos en los estados financieros auditados. Otras consideraciones que podrían afectar el análisis del riesgo de control por parte del auditor son:

- las políticas y los procedimientos que rigen las actividades con derivados y reflejan los objetivos de la gerencia;
- procedimientos de la gerencia para informar al personal sobre los controles;
- procedimientos de la gerencia para captar información sobre derivados;
- procedimientos de la gerencia para asegurar de que los controles sobre derivados que están funcionando según lo previsto.

-Significación. De acuerdo con la NIA 320[10], en una partida, saldo, transacción o revelación se considera que la información es significativa cuando "su omisión o declaración distorsionada pudiera influir en las decisiones económicas de los usuarios tomadas sobre la base en los estados financieros".

Los instrumentos financieros derivados se caracterizan por su volatilidad y sus altos niveles de riesgo en lo relacionado a su precio de mercado, liquidez y eventual incobrabilidad. Los efectos colaterales que la adquisición y venta de este tipo de instrumentos financieros pueden traer sobre los resultados de operación, posición financiera y flujos de efectivo de un ente pueden ser significativos, razón por la cual usualmente el auditor deberá clasificar estas aseveraciones como de alta significatividad.

[10] NIA 320. Significación de las auditorías.

-Pruebas de controles. Una vez que el auditor ha obtenido una conocimiento general del ente y su entorno y ha realizado una evaluación apropiada de los riesgos y del control interno establecidos por el ente para el manejo operativo y contable de los instrumentos derivados, el auditor procederá a realizar pruebas sobre los controles, las cuales le permitan obtener evidencia de auditoría acerca de su adecuado diseño y funcionamiento.

Algunas de las pruebas de control para obtener evidencias de auditoría sobre la eficacia a considerar son:

- verificar que los instrumentos financieros derivados se han usado de acuerdo con las políticas y lineamientos convenidos y dentro de los límites de autoridad;
- verificar que se han aplicado procesos de toma de decisiones apropiados y si se comprenden las razones para celebrar operaciones seleccionadas;
- obtener evidencia de que los derivados están sujetos a mediciones oportunas y apropiadas, y a la presentación de información sobre exposición al riesgo independientemente del agente bursátil;
- verificar que se han enviado confirmaciones a contrapartes y las confirmaciones recibidas de contrapartes han sido comparadas con los registros contables y conciliadas con ellos en forma apropiada;
- obtener evidencia de que los criterios de intencionalidad de uso están autorizados en forma apropiada, incluyendo cualquier cambio posterior en dichos criterios, como operaciones de cobertura o especulativas.

-**Procedimientos Sustantivos.** Los procedimientos sustantivos de auditoría se realizarán para obtener evidencias, con el fin de detectar distorsiones significativas en los estados contables, y son de dos tipos: (a) procedimientos analíticos; y (b) pruebas de detalle de operaciones y saldo.

Los procedimientos analíticos pueden ser útiles para evaluar ciertas políticas de gestión de riegos en relación con los derivados, por ejemplo, los limites de crédito. A continuación se detallan los procedimientos sustantivos relacionados con las afirmaciones de los derivados.

1. Existencia y ocurrencia:

- confirmar con el tenedor del derivado o la contraparte en el mismo;
- revisión de los convenios y otras formas de documentación de respaldo;
- investigación y observación.

2. Derechos y obligaciones:

- confirmar con el tenedor del derivado o la contraparte del mismo;
- revisión de los convenios y otras formas de documentación de respaldo.

3. Integridad:

- confirmar con el tenedor del derivado o la contraparte en el mismo acercad el detalle de todos los derivados y operaciones con el ente;
- revisión de las declaraciones de los agentes bursátil en relación con la existencia de operaciones con derivados y posiciones mantenidas;
- revisión de las confirmaciones de contrapartes recibidas pero no cotejadas con los registros de operaciones;
- revisión de partidas de conciliación no resueltas;
- lectura de acuerdos;
- revisión de documentación que se relacione con hechos posteriores ocurridos después de la fecha de corte de los estados financieros;
- investigación y observación;
- lectura de actas de directorio y asambleas de socios, las cuales contengan información relevante acerca de la forma en la cual la administración gestiona sus instrumentos financieros derivados.

4. Valuación y medición:

- confirmar con el tenedor del derivado o la contraparte en el mismo acerca de sus valores de mercado tanto al momento de compra o venta del derivado como al cierre del período sujeto de auditoría;
- revisar la solvencia de las contrapartes en la operación de derivados;
- obtener evidencias que corroboren el valor razonable de los derivados medidos o informados a valor razonable.

5. Presentación y revelación de información:

- comprobar que los métodos de presentación y revelación utilizados por la administración son congruentes con el marco de presentación de información financiera;
- comprobar que los estados financieros reflejan de forma razonable y fidedigna la posición financiera, los flujos de efectivo y los resultados de operación del ente.

Declaraciones de la gerencia

La NIA 580 “Declaraciones de la Gerencia” establece que el auditor debe obtener declaraciones de la gerencia, incluso declaraciones escritas sobre asuntos de importancia para los estados financieros cuando razonablemente no se pueda esperar que existan evidencias validas y suficientes de auditoría. Según el volumen y complejidad de las actividades con instrumentos derivados, las declaraciones de la gerencia sobre los derivados pueden incluir declaraciones sobre:

- los objetivos de la gerencia con respecto de los instrumentos financieros derivados, por ejemplo, si los instrumentos derivados se utilizan como cobertura o con fines especulativos;
- las afirmaciones en los estados financieros concernientes a los instrumentos financieros derivados, por ejemplo: *los registros reflejan todas las operaciones con instrumentos derivados,* o *se han identificado todos los instrumentos derivados incorporados,* o *los supuestos y las metodologías utilizadas en los modelos de valuación de instrumentos derivados son razonables*;
- si todas las operaciones han sido realizadas entre partes independientes y a valor razonable de mercado;
- los términos de las operaciones con instrumentos derivados;
- si hay acuerdos secundarios asociados a los instrumentos derivados;
- si el ente ha celebrado algún opción por escrito;
- si el ente cumple con los requisitos de documentación del marco de presentación de información financiera para instrumentos derivados que

sean condiciones suspensivas para el tratamiento de contable de determinadas coberturas.

Comunicaciones con la gerencia y con los responsables de la dirección

La auditoría puede tomar conocimiento de asuntos en el desarrollo de su tarea que considere que deban ser comunicados a la administración. La NIA 260[11] requiere que el auditor considere temas de auditoría de interés para los directivos que surjan de sus tareas y sean comunicados a la administración en forma oportuna. Respecto a los instrumentos derivados, esos temas pueden ser:

- debilidades importantes en el diseño o el funcionamiento de los sistemas de contabilidad y de control interno;
- falta de compresión por parte de la gerencia sobre la naturaleza o el alcance de actividades con derivados o con los riesgos asociados;
- ausencia de una política integral sobre la estrategia y los objetivos en el uso de instrumentos derivados.

Evolución del mercado de Instrumentos Financieros Derivados

Resulta de importancia hacer referencia a algunos sucesos que han marcado el desarrollo del mercado de los derivados y que se asocian de forma directa con la necesidad de que los auditores tengan un papel protagónico dentro del proceso de desarrollo y consolidación del mercado.

Pasado del mercado de los Instrumentos Financieros Derivados

Mientras que la comercialización de derivados ha crecido enormemente en estos años, existe evidencia de que estos instrumentos han sido utilizados desde la antigua Grecia. Aristóteles, en sus memorias, relata cómo un filósofo griego llamado Thalus realizó ganancias atractivas por un acuerdo de opciones

[11] NIA 260. Comunicaciones a los Directivos de Temas Relacionados con la auditoría.

alrededor del siglo VI a.C. Por otro lado, existe evidencia que el uso de los contratos *forwards* predominaba entre los comerciantes europeos en tiempos medievales. En el siglo XII d.C. se comenzaron a utilizar contratos *forwards* con una carta llamada carta de justicia donde básicamente se comprometían a la entrega de un bien a un cierto precio en un lugar establecido, a lo que hoy se le conoce como los futuros. El primer registro de un mercado de futuros formal viene del siglo XVII d.C. en Japón, adonde los dueños feudales japoneses enviaban arroz a sus almacenes en las ciudades más importantes y después emitían tickets que otorgaban el derecho para la entrega posterior del arroz a un precio fijo establecido al momento de la entrega del producto.

Los derivados (tal como los conocemos hoy en día) tuvieron un auge en la década de los setenta. El colapso del sistema de tipo de cambio fijo abrió la oportunidad y la necesidad de los derivados de moneda; mientras tanto, los avances financieros en modelos como el Binomial y el *Black & Scholes* tomaban cada vez más importancia y sobre todo empezaron a ser confiables para todos los involucrados en el área de finanzas.

Presente del mercado de los Instrumentos Financieros Derivados

La existencia de un entorno de negocios más volátiles e inciertos en Argentina, está obligando a los operadores financieros a un total replanteamiento de sus estrategias de negocio y por consiguiente de sus mecanismos para minimizar los posibles riesgos que puedan afectar a su patrimonio. Es así como durante los últimos años tanto los intermediarios financieros como las empresas de nuestro país han empezado a considerar como una posibilidad real el uso de los instrumento financieros derivados como mecanismo de cobertura de los riesgos que con mayor frecuencia afrontan nuestras empresas:

- riesgos de mercado;
- riesgos de liquidez ;
- riesgos de crédito.

Futuro del mercado de Instrumentos Financieros Derivados

Después de tantas pérdidas generadas por el manejo especulativo, se puede decir que mucho del daño que se le hizo a las instituciones financieras fue a consecuencia de los instrumentos derivados. No se le puede prohibir a las empresas el uso medido o desmedido de instrumentos derivados, eso sería equivalente a decirles cuántos días de crédito deben otorgar a sus clientes o cuánta mercancía comprar. Sin embargo, lo que se espera de los instrumentos derivados es lo siguiente:

- desde el punto de vista de normatividad contable, la exposición en las notas a los estados contables del ente van a tener cambios importantes. De hecho, tanto el IASB (*International Accounting Standards Board*) y el FASB (*Financial Accounting Standards Board*) han emitido documentos para su revisión, en los que se exige mayor detalle en cuanto al uso de derivados;
- desde el punto de vista de regulación, los derivados extrabursátiles serán los más afectados. No es posible que un mercado que puede hacer que los bancos más grandes entren en bancarrota de la noche a la mañana no esté regulado. Además, mucha de esta falta de regulación se magnificó con empresas que simplemente no tenían la solvencia para enfrentar el monto nominal de derivados que sustentaban. Es decir, sus montos nominales eran más grandes que sus activos;
- las instituciones que fijan calificaciones a las empresas tendrán que incluir de una mejor manera la posibilidad de bancarrota o insolvencia a consecuencia de los instrumentos derivados;
- frente a los escándalos financieros, muchas empresas se vieron afectadas financieramente. Seguramente, el comité de riesgos de cada una de ellas hará que los administradores disminuyan el uso excesivo o especulativo de estos instrumentos;
- finalmente, el mercado actual de los instrumentos derivados es tan grande que se podría cubrir cualquier riesgo asociado al negocio. Sin embargo, se espera que los instrumentos derivados aún crezcan más en cuanto a productos.

Reflexión final

Como un elemento de reflexión final, no se puede omitir el ejercicio de someter a análisis los principales retos y desafíos que los profesionales en auditoría enfrentarán a futuro y sobre todo establecer cuáles deben ser los compromisos y planteamientos que éstos deben asumir frente al proceso de globalización e integración en materia de normativa de auditoría. En este sentido, figuran:

- Lograr la obtención del conocimiento y destrezas requeridas, a efecto de que los profesionales en auditoría puedan adaptarse a los cambios que plantea el proceso de globalización e integración económica y por consiguiente el poder mantener una posición profesional competitiva frente a un entorno empresarial dinámico y evolutivo, como el que plantean tanto el uso de los instrumentos financieros derivados como la adopción de las nuevas bases de reconocimiento y medición establecidas por las Normas Internacionales de Información Financiera (NIIF) y los procedimientos de auditoría propuestos por las Normas Internacionales de Auditoria (NIA).
- Contribuir de forma efectiva en la difusión tanto a nivel formal como informal de los procedimientos de auditoría que todo auditor debe utilizar para obtener evidencia válidas y suficiente de auditoría, la cual le permitirá emitir una opinión acerca de la razonabilidad de los criterios contables que un ente utiliza para el registro contable de los instrumentos financieros derivados.
- Participar en forma activa en los procesos que conllevan la ruptura de paradigmas y consecuentemente vencer la resistencia al cambio que por naturaleza tienen muchos auditores, en lo relativo al uso efectivo y generalizado de los procedimientos de auditoría establecidos por las Normas Internacionales de Auditoria (NIA) y en particular a los procesos de auditoría en los cuales está implícita la auditoria de derivados.
- Promover el desarrollo del mercado de instrumentos financieros derivados, dado que este tipo de activos y pasivos financieros representan una opción apropiada y rentable por medio de la cual el

ente pueden minimizar el impacto que sobre ellas puede tener la materialización de los riesgos de mercado, de crédito y de liquidez.

Lo antes descrito es cierto en vista de que los instrumentos financieros derivados usualmente son un mecanismo muy eficaz y de bajo costo para la mitigación de riesgos antes citados. El conocimiento de la operativa, los criterios de contabilización y los procedimientos de auditoría de relacionados con los derivados representan una excelente oportunidad para los auditores, en razón del enorme potencial que este mercado posee en la expectativa de negocios tanto a nivel de los intermediarios financieros como de las empresas.

CAPÍTULO 3

CONTROL INTERNO

Lorena María Martires

Introducción

El presente trabajo pretende generar una visión global sobre la temática de *control interno*, su relevancia, bondades, razón de ser, características, responsables, limitaciones e interesados.

Asimismo, intenta transmitir que la evaluación del control interno por parte del auditor externo de estados contables es fundamental para definir el enfoque de auditoría a aplicar, y a la vez destacar que un buen sistema de control interno colabora con un manejo eficaz y eficiente del negocio, por eso es de interés para el dueño y el administrador de la empresa.

Antes de abordar el tema, me atrevo a comenzar con un ejemplo que puede ayudar a generarle al lector una idea de lo que es el control interno desde el sentido común.

A mi estudio llegaron dos jóvenes empresarios: Gustavo y Nacho, para solicitar mis servicios profesionales de auditor. Ambos tienen la concesión exclusiva de una reconocida marca de indumentaria femenina, Gustavo en La Plata y Nacho en Mar del Plata.

Gustavo y Nacho tienen varias cosas en común: ambos son emprendedores, se dedican exactamente a la misma actividad, lo hacen en plazas comerciales de similares características, tienen idéntica cantidad de locales e igual cantidad de empleados, y hasta se propusieron los mismos objetivos para el presente año:

1. Aumentar las ventas en más del 30% respecto del año anterior.
2. Ser reconocido en el mercado local por la buena atención de sus empleadas.

Sin embargo Nacho y Gustavo tienen formas distintas de manejar sus negocios:

NACHO	GUSTAVO
Efectúa un plan comercial anual y se mantiene permanentemente informado sobre la evolución de sus ventas y la de los competidores a través de reportes semanales que le prepara su contador, información que utiliza para decidir qué estrategia comercial adoptar si es necesario cambiar la actual.	Confía en que su carisma de buen vendedor, el que transmite a sus empleadas, será suficiente para lograr el objetivo planteado de incremento de ventas.
Tiene una política de reclutamiento de empleadas donde evalúa las aptitudes comerciales y también las condiciones éticas de las mismas. Controla la asistencia con tarjetas magnéticas que alimentan automáticamente el sistema de liquidación de sueldos.	Tiene un sistema informal de reclutamiento ya que confía plenamente en su intuición. No cuenta con un sistema formal de registro de asistencia y licencias
Tiene una caja fuerte ignífuga donde guarda los valores previo al depósito bancario. Paga a todos los proveedores con cheque. El tesorero deposita diariamente todas las cobranzas en el banco. El contador efectúa conciliaciones bancarias mensuales.	Utiliza la misma caja para cobranzas que para pagos. Deposita el excedente del fondo de maniobra semanalmente en el banco. Paga a los proveedores indistintamente con efectivo o cheque. El tesorero, quien maneja los fondos, realiza una conciliación bancaria a fin de año.
Realiza una toma de inventario mensual, que controla con el sistema informático de stock que se actualiza con cada compra y venta.	Una vez por temporada realiza un inventario.

Las registraciones contables las efectúa un contador independiente de las tareas operativas de la empresa, previo verificar la información del sistema informático con la documentación de respaldo.	Las registraciones contables las efectúa cada jefe operativo (tesorero, jefe de ventas, encargado del depósito) según la información que arroja el sistema informático, sin efectuar control alguno.
Genera un ambiente de control positivo transmitiendo a sus empleados con el ejemplo y la palabra la importancia de que cada uno cumpla los controles que su función requiere.	En su afán de ser reconocido por sus empleados como *amigo,* con su lenguaje gestual y actitud demuestra que el control no es necesario cuando hay buenas intenciones.

El conjunto de medidas que adopta Nacho para cumplir sus objetivos no son más que su propio sistema de control interno.

Desde el punto de vista de mi labor de auditor, no va a ser lo mismo hacer una auditoría de los estados contables de la empresa de Nacho, que de la empresa de Gustavo. Una primera intuición seguramente los llevara a pensar que la primera demandará menos trabajo. Este *demandar menos trabajo* significa que en la empresa de Nacho, que tiene un buen control interno (previo a probar que funcione), se supone que cada uno hace lo que tiene que hacer, y por lo tanto es probable que los estados contables, que devienen de que distintos sistemas y personas generen información, reflejen la realidad. Por lo tanto como auditor, voy a tener que aplicar menos procedimientos o procedimientos menos costosos apoyados en algunos de los controles de Nacho para satisfacerme de la razonabilidad de los saldos de esos estados.

En cambio, en la empresa de Gustavo, que parece no tener un sistema de control interno fuerte, voy a tener que hacer muchos mas procedimientos para poder opinar sobre la razonabilidad de sus estados contables.

En los libros de auditoría esto se traduce con el siguiente concepto: se debe analizar el control interno de una empresa para determinar el alcance, la naturaleza y la oportunidad del trabajo de auditoría, o sea se usa para definir el enfoque de auditoría a aplicar.

Complementariamente, me gustaría introducir otro concepto básico: más allá de su contribución a la planificación del auditor, el control interno tiene la finalidad de ayudar al empresario a cumplir sus objetivos. En nuestro ejemplo, seguramente Nacho no desarrolló todos los controles mencionados anteriormente para facilitar nuestro trabajo de auditoría, sino que lo hizo para poder cumplir sus propios objetivos.

Hacia una definición de control interno

El antiguo comerciante y también luego los primeros industriales, atendían sus negocios en forma personal, por lo cual no tenían la necesidad imperiosa de practicar un control sobre las operaciones, ya que ellos mismos las efectuaban, y si detectaban algún error localizaban su origen y lo corregían. Esto ocurría por que en una sola persona se agrupaban las funciones de adquisición de insumos, elaboración de la producción, venta, cobranza y –rudimentaria- administración.

Con el paso del tiempo y debido al desarrollo industrial y económico, los comerciantes o industriales propietarios no pudieron seguir atendiendo personalmente los problemas productivos, comerciales y administrativos, y se vieron obligados a subdividir o delegar funciones dentro de la organización y la respectiva responsabilidad de los hechos operativos o de gestión. Pero dicha delegación de funciones y responsabilidades no estuvo sola en el proceso, ya que en forma paralela se debieron establecer sistemas o procedimientos que previeran fraudes o errores, que protegieran el patrimonio, que dieran información coherente y que permitieran una gestión eficiente.

“Así nace el control como una función gerencial, para asegurar y constatar que los planes y políticas preestablecidas se cumplan tal como fueron fijados.

Un sistema de control interno eficiente sólo podrá establecerse en una empresa que se encuentre correctamente organizada, entendiéndose que organización es la estructura del ente y además el ordenamiento lógico de los elementos o

componentes que la integran, de forma tal que cumpla con los objetivos, políticas y fines para los cuales dicha empresa fue creada.

El control cumple un rol retroalimentador al interior de la empresa, debido a que cada función de la organización está sujeta a la aplicación de diversas formas de control.

La existencia del control se fundamenta en la planificación: si no existe planificación no hay un motivo para controlar, por esto la función primordial del control en la organización es evaluar las metas planteadas por ésta.

De lo anterior se desprende que el control consiste en un proceso de evaluación constante de las actividades desarrolladas por la empresa, comparando su resultado con la planificación; por ello, dicha evaluación entregará las herramientas necesarias para que la dirección realice las correcciones correspondientes con el objetivo de reorientar las metas definidas en la planificación.

La expresión *control interno* es generalmente utilizada para enunciar el conjunto de directrices y normas emanadas de los dueños o máximos ejecutivos, para dirigir, coordinar y controlar a sus subordinados, con el propósito de que se cumplan los objetivos de la empresa.

Si bien existen varias definiciones sobre *control interno,* transcribimos a continuación la que considero mas universalmente aceptada, que fue la dictada por el informe COSO (*Committee of Sponsoring Organizations of the Treadway Commission*) sobre el cual profundizaremos mas adelante.

El control interno es un proceso efectuado por el consejo de administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:

- Eficacia y eficiencia de las operaciones: incluye los objetivos de desempeño y de utilidad y la salvaguarda de los recursos contra pérdida.
- Fiabilidad de la información financiera: incluye preparación de EECC confiables y la prevención contra información contable fraudulenta.
- Cumplimiento de leyes y normas que sean aplicables.

Relación entre control interno y auditoría

El sistema de control interno de un ente es responsabilidad de la dirección del mismo, así como también lo es la emisión de los estados contables. Es necesario que la Dirección establezca un sistema competente de control puesto que le ayudará a cumplir sus metas. Esto es independiente de la auditoría externa de estados contables. No obstante, para el auditor resulta importante evaluar su funcionamiento pues influye decisivamente en la naturaleza, alcance y oportunidad de los procedimientos de auditoría que aplicará.

Es precisamente en la RT 7, y también en su reciente sucesora RT 37, norma legal de auditoría vigente para la Argentina, donde se señala como primer procedimiento de auditoría a cumplir por el auditor la "evaluación de las actividades de control de los sistemas que son pertinentes a su revisión, siempre que con relación a su tarea, el auditor decida depositar confianza en tales actividades".

En la medida que la empresa posea controles que funcionando adecuadamente permitan concluir que las afirmaciones contenidas en los EECC son válidas, el auditor centrará su atención únicamente en esos controles, en desmedro de aquellos que si bien son necesarios para el cumplimiento de los objetivos de la empresa, no tienen vinculación directa con el objetivo de auditoría. Esto se relaciona con el concepto de control clave, que es aquel control que reúne dos condiciones:

- proporciona satisfacción de auditoría relevante, siempre que esté operando efectivamente;
- la proporciona de modo mas eficiente que otros procedimientos.

Un ejemplo sería que si la empresa tiene como una norma de control interno la realización de un inventario mensual practicado por un empleado independiente de almacenes y de contabilidad, éste seguramente va a ser un control clave para el auditor, si prueba que se cumple, ya que brindará satisfacción del saldo de la cuenta mercaderías. En cambio, otro control, como puede ser un control presupuestario efectuado por la gerencia -si bien no se

discute su importancia-, no proporciona evidencia para ninguna afirmación de los EECC y, por lo tanto, no será un control clave para el auditor.

Los nuevos conceptos de control interno: el informe COSO

El informe COSO sobre control interno fue publicado en Estados Unidos en 1992, tras un largo periodo de más de cinco años de discusión. Fue el resultado de un grupo de trabajo conformado por distintas instituciones que regulan la actividad profesional en EEUU, de contadores públicos, auditores internos y externos y ejecutivos financieros, quienes integraron la Comisión *Treadway*. El nombre COSO es una sigla que significa *Committee of Sponsoring Organizations de la Treadway Commission*. Dicha comisión se reunió con la finalidad de identificar los factores que originan la presentación de información financiera falsa o fraudulenta y emitir las recomendaciones que garantizasen la máxima transparencia informativa en tal sentido.

El informe COSO ha pretendido -y se considera que ha logrado- que académicos, legislativos, directores de empresas, auditores internos y externos y líderes empresariales tengan una referencia conceptual común de lo que significa el control interno.

El estudio ha tenido gran aceptación y difusión en los medios financieros y en los consejos de administración de las organizaciones, resaltando la necesidad de que los administradores y altos directores presten atención al control interno, tal como COSO lo define, enfatizando la necesidad de los comités de auditoría y de una calificada auditoría interna y externa, recalcando la necesidad de que el control interno sea un proceso integrado que forme parte de los procesos de los negocios y no pesados mecanismos burocráticos añadidos a los mismos.

Considerando el enfoque del informe COSO, así como la bibliografía mas universalmente aceptada sobre control interno, se exponen a continuación los conceptos difundidos en el mismo.

Los controles internos se diseñan e implantan con el fin de detectar, en un plazo deseado, cualquier desviación respecto a los objetivos de rentabilidad establecidos para cada empresa y de prevenir cualquier evento que pueda evitar el logro de los objetivos, la obtención de información confiable y oportuna y el cumplimiento de leyes y reglamentos. Los controles internos fomentan la eficiencia, reducen el riesgo de pérdida de valor de los activos y ayudan a garantizar la confiabilidad de los estados financieros y el cumplimiento de las leyes y normas vigentes. En sentido amplio, se define como un proceso efectuado por el consejo de administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:

1. Eficacia y eficiencia de las operaciones.
2. Confiabilidad de la información financiera.
3. Cumplimiento de las leyes y normas aplicables.

La anterior definición refleja ciertos conceptos fundamentales.

- El control interno es un *proceso*, un medio utilizado para la consecución de un fin, no un fin en sí mismo.
- El control interno lo llevan a cabo las *personas*, no se trata solamente de manuales de políticas e impresos, sino de personas en cada nivel de la organización.
- El control interno solo puede aportar un *grado de seguridad razonable*, no la seguridad total, a la dirección y al consejo de administración de la entidad.
- El control interno está pensado para facilitar la consecución de *objetivos* propios de cada entidad.

El control interno consta de cinco componentes relacionados entre sí. Se derivan de la manera en que la dirección dirige la empresa y están integrados en el proceso de dirección. Antes de enunciar dichos componentes, quiero resaltar que el control interno bajo esta visión de proceso dista mucho de la perspectiva de algunos que lo ven como un elemento añadido a las actividades de una entidad o como una carga inevitable impuesta por los organismos reguladores. El sistema de control interno está entrelazado con las actividades operativas de la entidad y existe por razones

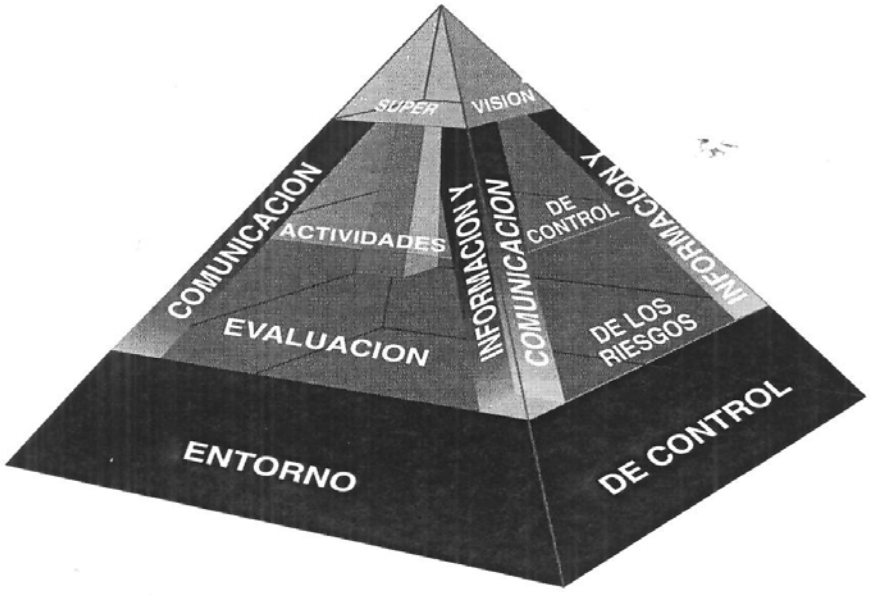
empresariales. Los controles internos son más efectivos cuando se incorporan a la infraestructura de una entidad y forman parte de su esencia. Deberían ser *incorporados* y no *añadidos*.

Componentes del control interno

1. Ambiente de control - 2. Evaluación de riesgos - 3. Actividades de control – 4. Información y comunicación - 5. Supervisión

Estos componentes del control interno y los vínculos existentes entre ellos se reflejan gráficamente en la ilustración siguiente. El modelo refleja el dinamismo del sistema de control interno, por ejemplo, la evaluación de riesgos no solo influye en las actividades de control, sino que también puede dejar en evidencia que las necesidades de información o las actividades de supervisión deberían reconsiderarse.

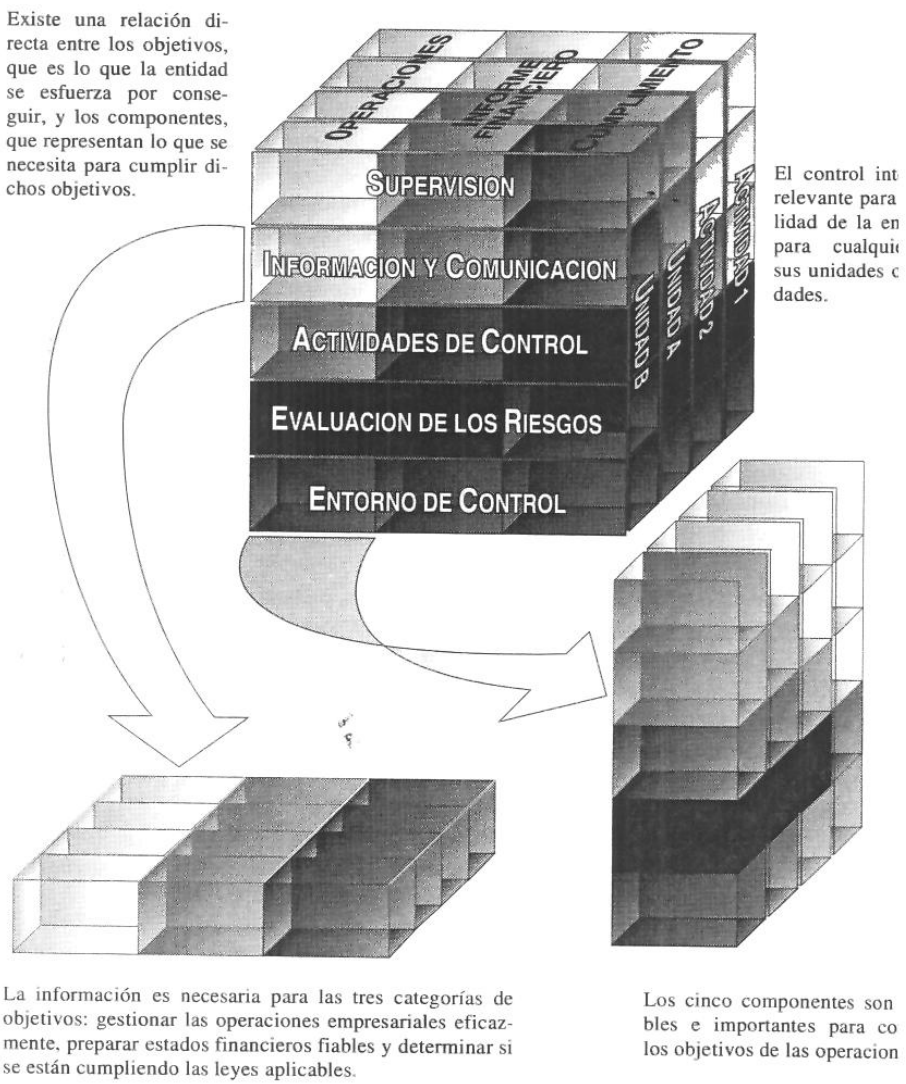
Componentes del control interno



El *entorno de control* aporta el ambiente en el que las personas desarrollan sus actividades y cumplen con sus responsabilidades de control. Sirve como base de los otros componentes. Dentro de este entorno, los directivos *evalúan los riesgos* relacionados con el cumplimiento de determinados objetivos. Las *actividades de control* se establecen para ayudar a asegurar que se pongan en práctica las directrices de la dirección para hacer frente a dichos riesgos. Mientras tanto, la *información* relevante se capta y se comunica por toda la organización. Todo este proceso es *supervisado* y modificado según las circunstancias.

También debemos decir que existe una relación directa entre: 1) los objetivos, que es lo que la entidad se esfuerza por conseguir, y 2) los componentes, que representan lo que necesita para cumplir dichos objetivos. Esta relación se ilustra mediante una matriz tridimensional que podemos ver en el gráfico siguiente:

Relación entre objetivos y componentes



Las tres categorías de objetivos (operacionales, de información financiera y de cumplimiento) están representados por columnas. Los cinco componentes están representados por filas. Las unidades o actividades de la entidad

(sucursales, unidades de negocio, actividades funcionales como compras o marketing) están representadas por la tercera dimensión de la matriz.

Cada fila cruza las tres categorías de objetivos y es aplicable a las tres. Como ejemplo, la información contable (del componente información y comunicación) es necesaria para gestionar eficazmente las operaciones empresariales, formular estados financieros fiables y determinar si la entidad está cumpliendo con las normas al respecto que le sean aplicables.

El control interno es importante para la empresa en su totalidad y para cada una de sus partes. Esta relación se refleja en la tercera dimensión, que representa las filiales, divisiones y actividades funcionales o de otro tipo.

Todos los miembros de la organización son responsables del control interno, aunque no todos con el mismo grado de responsabilidad:

- La dirección: el director general (máximo ejecutivo de una empresa) es el responsable último y debería asumir la *titularidad* del sistema de control interno.
- El consejo de administración: la dirección es responsable ante el consejo de administración, el cual debe ofrecer orientación, pautas de actuación y una visión global del negocio.
- Auditores internos: desempeñan un papel importante en la evaluación de la eficacia de los sistemas de control.
- Otros empleados: el control interno es, hasta cierto punto, la responsabilidad de todos los miembros de una organización, y debe ser una parte explícita o implícita de la descripción del puesto de trabajo de cada uno. Casi todos los empleados producen información utilizada en el sistema de control interno o realizan las funciones necesarias para efectuar el control.

Por otra parte, algunos terceros ajenos a la entidad suelen contribuir al sistema de control interno. Los auditores externos, aportando una opinión independiente y objetiva, contribuyen directamente mediante la auditoría de los estados financieros e indirectamente proporcionando recomendaciones. Otros terceros que proporcionan información útil para llevar a cabo el control interno son: organismos de control, clientes, analistas financieros, medios de

comunicación. Sin embargo, los terceros no son responsables del sistema de control interno de una entidad ni forman parte de él.
Desarrollamos, a continuación, cada componente del control interno.

Entorno de control. El entorno de control aporta el ambiente en el que las personas desarrollan sus actividades y cumplen con sus responsabilidades de control, marca la pauta del funcionamiento de una organización e influye en la percepción de sus empleados respecto al control. Es la base de todos los demás componentes del control interno, aportando disciplina y estructura. Los factores del ambiente de control incluyen la integridad, los valores éticos y la capacidad de los empleados de la entidad, la filosofía de dirección y el estilo de dirección, la manera en que la dirección asigna la autoridad y las responsabilidades y organiza y desarrolla profesionalmente a sus empleados así como la atención y orientación que proporciona el consejo de administración. El ambiente de control tiene una incidencia generalizada en la estructuración de las actividades empresariales, en el establecimiento de objetivos y en la evaluación de riesgos.
Las entidades sometidas a un control eficaz se esfuerzan por tener personal competente e inculcan en toda la organización una actitud positiva frente al control.
Se enuncian, a continuación, algunos factores del entorno de control que inciden de forma significativa en la eficiencia del entorno de control.
La **Integridad y valores éticos** se apoya en la existencia e implantación de códigos de conducta u otras políticas relacionadas con las prácticas profesionales aceptables, y en la forma en que se llevan a cabo las negociaciones con empleados, proveedores, clientes, competidores, etc. (si la dirección lleva a cabo sus actividades empresariales con un alto nivel ético).
A su vez, hay situaciones que pueden incitar a los empleados a cometer actos indebidos: la falta de controles o controles ineficaces, el alto nivel de descentralización sin las políticas de apoyo necesarias -que impide que la dirección esté informada sobre las acciones llevadas a cabo en los niveles más bajos-, una función de auditoría interna débil, un consejo de administración

poco eficaz, sanciones por comportamiento indebido insignificantes, o que no se hacen públicas.

El ambiente de control y la cultura de la organización están influidos de forma significativa por el Consejo de Administración y el Comité de Auditoría, el grado de independencia del Consejo o del Comité de Auditoría respecto de la dirección, la experiencia y la calidad de sus miembros, grado de implicación y vigilancia y el acierto de sus acciones son factores que inciden en la eficacia del control interno.

Evaluación de riesgos. Toda entidad debe hacer frente a una serie de riesgos tanto de origen interno como externo que deben evaluarse. Una condición previa a la evaluación de los riesgos es el establecimiento de objetivos en cada nivel de la organización que sean coherentes entre sí. La evaluación del riesgo consiste en la identificación y análisis de los factores que podrían afectar la consecución de los objetivos y, en base a dicho análisis, determinar la forma en que los riesgos deben ser administrados y controlados. Debido a que las condiciones económicas, industriales, normativas continuarán cambiando, es necesario disponer de mecanismos para identificar y afrontar los riesgos asociados con el cambio.

Los objetivos pueden agruparse en tres grandes categorías:

Objetivos relacionados con las operaciones: se refieren a la eficacia y eficiencia de las operaciones de la entidad, incluyendo los objetivos de rendimiento y rentabilidad y la salvaguarda de los recursos contra posibles pérdidas. Estos objetivos varían en función de la elección de la dirección respecto a estructuras y rendimiento.

Objetivos relacionados con la información financiera: se refieren a la preparación de estados financieros confiables y a la prevención de la falsificación de la información financiera. A menudo, estos objetivos están condicionados por requerimientos externos.

Objetivos de cumplimiento: estos objetivos se refieren al cumplimiento de las leyes y normas a las que está sujeta la entidad. Dependen de factores externos (tales

como la reglamentación en materia de medio ambiente). #n algunos casos tienden a ser parecidos en todas las entidades, en otros, en todo un sector.

A nivel de empresa, los riesgos pueden ser la consecuencia de factores externos como internos.

A continuación se presentan algunos ejemplos:

Factores externos: los avances tecnológicos, las necesidades o expectativas cambiantes de los clientes –que pueden influir en el desarrollo de productos-, el proceso de producción, el servicio a cliente, la fijación de precios, etc. Los cambios económicos pueden repercutir en las decisiones sobre financiamiento, inversiones y desarrollo.

Factores internos: los problemas con los sistemas informáticos pueden perjudicar las operaciones de la entidad. Los cambios de responsabilidades de los directivos pueden afectar la forma de realizar determinados controles. Un consejo de administración o un comité de auditoría débil o ineficaz puede dar lugar a que se produzcan indiscreciones.

Se han desarrollado muchas técnicas para identificar riesgos. La mayoría de las desarrolladas por auditores internos y externos en el momento de determinar el alcance de sus actividades comprenden métodos cualitativos o cuantitativos para identificar y establecer el orden de prioridad de las actividades de alto riesgo. Además de identificar los riesgos a nivel de empresa, también debe hacerse a nivel de cada actividad de la empresa: esto ayuda a enfocar la evaluación de los riesgos en las unidades o funciones más importantes del negocio, como ventas, producción y desarrollo tecnológico. La correcta evaluación de los riesgos a nivel de actividad contribuye a que también se mantenga un nivel aceptable de riesgo para el conjunto de la entidad.

Una vez identificados los riesgos a nivel de entidad y por actividad debe llevarse a cabo un análisis de riesgos que puede ser:

- una estimación de la importancia del riesgo;
- una evaluación de la probabilidad o frecuencia de que se materialice el riesgo;
- medidas a adoptar para evitar los riesgos.

Existe una diferencia entre el análisis de los riesgos, que forma parte del control interno, y los planes, programas y acciones resultantes que la dirección considere necesarios para afrontar dichos riesgos. Estas acciones son parte del proceso de gestión, pero no son un elemento del sistema de control interno.
Los cambios en la economía, los nuevos empleados, los sistemas de información nuevos, el crecimiento rápido o los cambios en la reglamentación pueden hacer que un sistema de control eficaz ya no lo sea. En el contexto del análisis de riesgos resulta fundamental que exista un proceso para identificar las condiciones que hayan cambiado, y tomar las acciones pertinentes. Deben existir mecanismos para identificar los cambios ocurridos, o susceptibles de ocurrir a corto plazo en la medida de lo posible. Los mecanismos deben estar orientados hacia el futuro, de manera que la entidad pueda prever los cambios significativos y elaborar los planes correspondientes.

Actividades de control. Son las políticas y los procedimientos que ayudan a asegurar que se llevan a cabo las instrucciones de la dirección. Ayudan a asegurar que se tomen las medidas necesarias para controlar los riesgos relacionados con la consecución de los objetivos de la entidad.
Hay actividades de control en toda la organización, a todos los niveles y en todas las funciones. Incluyen una gama de actividades tan diversa como aprobaciones, autorizaciones, verificaciones, conciliaciones, revisiones de rentabilidad operativa, salvaguarda de activos y segregación de funciones.
Las actividades de control pueden dividirse en tres categorías, según el tipo de objetivo de la entidad con el que están relacionadas: las operacionales, la confiabilidad de la información financiera y el cumplimiento de la legislación aplicable.
Existen muchas descripciones de tipos de actividades de control, que incluyen desde controles preventivos a controles detectivos y correctivos, controles manuales, controles informáticos y controles de dirección.
Algunos ejemplos:
Análisis efectuados por la dirección: los resultados obtenidos se analizan comparándolos con los presupuestos, las previsiones, los resultados de

ejercicios anteriores y de los competidores, con el fin de evaluar en que medida se están alcanzando los objetivos.

Gestión directa de funciones por actividades: los responsables de las diversas funciones o actividades revisan los informes sobre resultados alcanzados.

Proceso de información: se aplican una serie de controles para comprobar la exactitud, totalidad y autorización de las transacciones. Se controla el desarrollo de nuevos sistemas y la modificación de los existentes, al igual que el acceso a los datos, archivos y programas informáticos.

Controles físicos: los equipos de fabricación, las inversiones financieras, la tesorería y otros activos son objeto de protección y periódicamente se someten a recuentos físicos cuyos resultados se comparan con las cifras que figuran en los registros de control.

Indicadores de rendimiento: el análisis combinado de diferentes conjuntos de datos (operativos o financieros) junto con la puesta en marcha de acciones correctivas, constituyen actividades de control.

Segregación de funciones: con el fin de reducir el riesgo de que se cometan errores o irregularidades, las tareas se reparten entre los empleados.

Información y comunicación. Hay que identificar, recopilar y comunicar información pertinente en tiempo y forma que permitan cumplir a cada empleado con sus responsabilidades. Los sistemas de información generan informes, que contienen información operativa, financiera y la correspondiente al cumplimiento, que posibilitan la dirección y el control del negocio. Dichos informes contemplan no sólo los datos generados internamente, sino también información sobre incidencias, actividades y condiciones externas, necesaria para la toma de decisiones y para formular informes financieros. Debe haber una comunicación eficaz en un sentido amplio, que fluya en todas las direcciones a través de todos los ámbitos de la organización, de arriba hacia abajo y a la inversa. Las responsabilidades de control han de tomarse en serio. Los empleados tienen que comprender cuál es su papel en el sistema de control interno y cómo las actividades individuales están relacionadas con el

trabajo de los demás. Asimismo, tiene que haber una comunicación eficaz con terceros, como clientes, proveedores, organismos de control y accionistas.

La calidad de la información generada por los diferentes sistemas afecta la capacidad de la dirección de tomar decisiones adecuadas al gestionar y controlar las actividades de la entidad. Resulta imprescindible que los informes ofrezcan suficientes datos relevantes para posibilitar un control eficaz.

Contenido: ¿contiene toda la información necesaria? Oportunidad: ¿se facilita en el tiempo adecuado? Actualidad: ¿es la más reciente disponible? Exactitud: ¿los datos son correctos? Accesibilidad: ¿puede ser obtenida fácilmente por las personas adecuadas? Por otra parte, si bien los sistemas de información forman parte del sistema de control interno, también han de ser controlados.

Además de recibir la información necesaria para llevar a cabo sus actividades, todo el personal, especialmente los empleados con responsabilidades importantes, deben tomar en serio sus funciones comprometidas al control interno. Cada función concreta ha de especificarse con claridad: cada persona tiene que entender los aspectos relevantes del sistema de control interno, cómo funcionan los mismos, saber cuál es su papel y responsabilidad en el sistema. Al llevar a cabo sus funciones, el personal de la empresa debe saber que cuando se produzca una incidencia conviene prestar atención no sólo al propio acontecimiento, sino también a su causa. De esta forma, se podrá identificar la deficiencia potencial en el sistema tomando las medidas necesarias para evitar que se repita. Asimismo, el personal tiene que saber cómo sus actividades están relacionadas con el trabajo de los demás, esto es necesario para conocer los problemas y determinar sus causas y la medida correctiva adecuada. El personal debe saber los comportamientos esperados, aceptables y no aceptables. Los empleados también necesitan disponer de un mecanismo para comunicar información relevante a los niveles superiores de la organización. Los empleados de primera línea, que manejan aspectos claves de las actividades todos los días, generalmente son los más capacitados para reconocer los problemas en el momento que se presentan. Deben haber líneas directas de comunicación para que esta información llegue a niveles superiores y, por otra parte, debe haber disposición de los directivos para escuchar.

Además de una comunicación interna, ha de existir una eficaz comunicación externa. Los clientes y proveedores podrán aportar información de gran valor sobre el diseño y la calidad de los productos o servicios de la empresa, permitiendo que la empresa responda a los cambios y preferencias de los clientes. Por otra parte, toda persona deberá entender que no se tolerarán actos indebidos, tales como sobornos o pagos ilícitos.

Supervisión. Los sistemas de control interno requieren supervisión, es decir, un proceso que compruebe que se mantiene el adecuado funcionamiento del sistema a lo largo del tiempo. Esto se consigue mediante actividades de supervisión continua, evaluaciones periódicas o una combinación de ambas cosas. La supervisión continua se da en el transcurso de las operaciones. Incluye tanto las actividades normales de dirección y supervisión, como otras actividades llevadas a cabo por el personal en la realización de sus funciones. El alcance y frecuencia de las evaluaciones dependerá de la evaluación de riesgos y de la eficiencia de los procesos de supervisión. Los sistemas de control interno y, en ocasiones, la forma en que los controles se aplican, evolucionan con el tiempo, por lo que procedimientos que eran eficaces en un momento dado, pueden perder su eficacia o dejar de aplicarse. Las causas pueden ser la incorporación de nuevos empleados, defectos en la formación y supervisión, restricciones de tiempo y recursos y presiones adicionales. Asimismo, las circunstancias en base a las cuales se configuró el sistema de control interno en un principio también pueden cambiar, reduciendo su capacidad de advertir sobre los riesgos originados por las nuevas circunstancias. En consecuencia, la dirección tendrá que determinar si el sistema de control interno es adecuado en todo momento y con capacidad de asimilar los nuevos riesgos.

Es necesaria la existencia de una **supervisión continua** ya que existe una gran variedad de actividades que permiten efectuar un seguimiento de la eficacia del control interno, como comparaciones, conciliaciones, actividades corrientes de gestión y supervisión así como otras actividades rutinarias.

Respecto al **alcance y** la **frecuencia** de la evaluación del control interno, variarán según la magnitud de los riesgos objeto de control y la importancia de los controles para la reducción de aquellos. Así, los controles actuarán sobre los riesgos de mayor prioridad y los más críticos para la reducción de un determinado riesgo serán objeto de evaluación más frecuente. La evaluación del control interno forma parte de las funciones normales de auditoría interna y también resulta de peticiones especiales por parte del consejo de administración, la dirección general y los directores de filial o de división. Por otra parte, el trabajo realizado por los auditores externos constituye un elemento de análisis a la hora de determinar la eficacia del control interno. Una combinación del trabajo de las dos auditorías, la interna y la externa, posibilita la realización de los procedimientos de evaluación que la dirección considere necesarios.

Para el **proceso de evaluación** de un sistema de control debe mantenerse una disciplina en todo el proceso, si bien los enfoques y técnicas varían. El evaluador deberá entender cada una de las actividades de la entidad y cada componente del sistema de control interno objeto de la evaluación. Conviene primero centrarse en el funcionamiento teórico del sistema, es decir en su diseño, lo cual implicará conversaciones previas con los empleados de la entidad y la revisión de la documentación existente. La tarea del evaluador es averiguar el funcionamiento real del sistema. Es posible que, con el tiempo, determinados procedimientos diseñados para funcionar de un modo determinado se modifiquen para funcionar de otro modo, o simplemente se dejen de realizar. A veces se establecen nuevos controles, no conocidos por las personas que, en un principio, describieron el sistema, por lo que no se hallan en la documentación existente. A fin de determinar el funcionamiento real del sistema, se mantendrán conversaciones con los empleados que aplican y se ven afectados por los controles, se revisarán los datos registrados sobre el cumplimiento de los controles, o una combinación de estos dos procedimientos. El evaluador analizará el diseño del sistema de control interno y los resultados de las pruebas realizadas. Este análisis se efectuará bajo la

óptica de los criterios establecidos, con el objeto último de determinar si el sistema ofrece una seguridad razonable respecto a los objetivos establecidos

Existe una gran variedad de **metodologías y herramientas de evaluación**, incluyendo hojas de control, cuestionarios y técnicas de flujogramación, técnicas cuantitativas, relaciones de objetivos de control, identificando los objetivos genéricos de control interno. Algunas empresas comparan sus sistemas de control interno con los de otras entidades, lo que se conoce generalmente como *benchmarking*.

El nivel de **documentación soporte del sistema de control interno** de la entidad varía según la dimensión y complejidad de la misma y otros aspectos análogos. Las entidades grandes normalmente cuentan con manuales de políticas, organigramas formales, descripciones de puestos, instrucciones operativas, flujogramas de los sistemas de información, etc. Muchos controles son suaves y no tienen documentación, sin embargo, se aplican asiduamente, resultando muy eficaces. Se puede comprobar este tipo de controles de la misma manera que los controles documentados. El hecho de que los controles no estén documentados no impide que el sistema de control interno sea eficaz o que pueda ser evaluado.

Limitaciones del control interno

El control interno puede ayudar a que una entidad consiga sus objetivos de rentabilidad y a prevenir la pérdida de recursos, puede ayudar a la obtención de información financiera confiable, puede reforzar la confianza en que la empresa cumple con la normatividad aplicable; pero no importa lo bien concebido que esté y lo bien que funcione, únicamente puede dar un grado de seguridad razonable -no absoluta- a la dirección y al consejo en cuanto a la consecución de los objetivos de la entidad. El control interno no puede hacer que un gerente malo se convierta en un buen gerente. Asimismo, los cambios en la política o en los programas gubernamentales, las acciones que tomen los competidores o las condiciones económicas pueden estar fuera de control de la dirección. El

control interno (incluso un control interno eficaz) funciona a diferentes niveles con respecto a los diferentes objetivos. En el caso de los objetivos relacionados con la eficacia y eficiencia de las operaciones (consecución de su misión básica, de los objetivos de rentabilidad y análogos) el control interno puede ayudar a asegurar que la dirección sea consciente del progreso o del estancamiento de la entidad.

Elusión de los controles por la dirección

El sistema de control interno no puede ser más eficaz que las personas responsables de su funcionamiento. Incluso en aquellas entidades que tienen un buen ambiente de control (aquellas que tienen elevados niveles de integridad y conciencia del control) existe la posibilidad de que el personal directivo eluda el sistema de control interno. El término *elusión de los controles por la dirección* en el sentido en que se emplea aquí se refiere a la omisión de políticas o procedimientos establecidos con finalidades ilegítimas, con ánimo de lucro personal o para mejorar la presentación de la situación financiera o para disimular el incumplimiento de obligaciones legales. La elusión incluye prácticas tales como actos deliberados de falsificación ante bancos, abogados, contadores y proveedores, así como la emisión intencionada de documentos falsos, entre otras. La elusión no se debe confundir con la intervención, términos que se refieren a los actos de la dirección efectuados con finalidades legítimas, que se desvían de las políticas y procedimientos establecidos. La intervención de la dirección es necesaria para hacer frente a transacciones o acontecimientos puntuales y no recurrentes que, de otra forma, no serían procesados correctamente por el sistema de control. Las intervenciones se hacen de manera abierta y tienen su correspondiente soporte documental, mientras que la elusión normalmente ni se documenta ni se comunica, en un claro intento de encubrir los hechos.

Confabulación

La confabulación de dos o más personas puede provocar fallas en el sistema de control. Cuando las personas actúan de forma colectiva para cometer y encubrir un acto, los datos financieros y otras informaciones de gestión pueden verse alterados de un modo no identificable por el sistema de control.

Relación costo/beneficio

Las entidades deben considerar los costos y beneficios relativos a la implantación de controles. A la hora de decidir si se ha de implantar un determinado control, se considerarán tanto el riesgo de fracaso como el posible efecto en la entidad, junto a los costos correspondientes a la implantación del nuevo control. Existen distintos niveles de precisión en cuanto a la determinación del costo y el beneficio de la implantación de controles. Generalmente resulta mas fácil determinar el costo, pudiéndose cuantificar de forma bastante precisa. Normalmente se tienen en cuenta todos los costos directos correspondientes a la implantación de un control, así como los costos indirectos si resultan cuantificables. Algunas empresas también incluyen los costos de oportunidad asociados al uso de recursos.

El informe COSO II

El 29 se septiembre del 2004 se lanzó el Marco de Control denominado COSO II, que según su propio texto no contradice al COSO I, siendo ambos marcos conceptualmente compatibles. Sin embargo, este marco se enfoca a la gestión de los riesgos (más allá de la intención de reducir riesgos que se plantea en COSO I) mediante técnicas como la administración de un portafolio de riesgos.

Con el informe COSO I, de 1992, se modificaron los principales conceptos del Control Interno dándole a este una mayor amplitud. El Marco de Control denominada COSO II de septiembre del 2004, establece nuevos conceptos que, como se explicó anteriormente, no entran en contradicción con los conceptos establecidos en COSO I. El nuevo marco amplía la visión del riesgo a eventos negativos o positivos, o sea, a amenazas u oportunidades; a la localización de un nivel de tolerancia al riesgo; así como al manejo de estos eventos mediante portafolios de riesgos.

La idea fuerza que alienta el COSO II es una especie de tratado de ciencia actuarial mas seguridad de la tecnología de la información mas un código de buenas prácticas de gobierno corporativo. Esto queda reflejado en algunos párrafos: “La gestión de los riesgos corporativos es que las entidades existen con el fin último de generar valor para sus grupos de interés” pero “la búsqueda de equilibrio entre intereses, a menudo contrarios, puede resultar complicada y frustrante”. Grupo de interés se define como un “conjunto de personas físicas o jurídicas que colaboran con una entidad o están afectadas por ella”.

El COSO II se presenta gráficamente en formato de matriz tridimensional, que relaciona:

- categorías de objetivos: estrategia – operaciones – información – cumplimiento;
- la entidad y sus unidades;
- los componentes: ambiente interno – establecimiento de objetivos– Identificación de eventos – evaluación de riesgos – respuesta a los riesgos – actividades de control – información y comunicación – supervisión.

Antes de seguir, vamos a detallar algunas definiciones reseñadas en el Informe.

• Riesgo inherente: el riesgo a que se somete una entidad en ausencia de acciones de la dirección para alterar o reducir su probabilidad de ocurrencia e impacto.

• Riesgo aceptado: la cuantía, en sentido amplio, del riesgo que una entidad está dispuesta a asumir para realizar su misión (o visión).

• Riesgo residual: el riesgo remanente después de que la dirección haya llevado a cabo una acción para modificar la probabilidad o impacto a un riesgo.
• Tolerancia al riesgo: la variación aceptable en la consecución de un objetivo.

El COSO II demuestra una sutil sensibilidad hacia la seguridad en forma de preocupación por los sistemas de información, otras veces como sistemas informáticos o tecnología de la información o, escuetamente, tecnología, considerando su importancia en profundidad. Incluso concreta que el "concepto de 'seguridad razonable' refleja la idea de que la incertidumbre y el riesgo están relacionados con el futuro, que nadie puede predecir con precisión, y no implica que la gestión de riesgos corporativos fracase con mucha frecuencia".

Respecto a los roles y la responsabilidad, el COSO II reseña, además de los habituales *consejo de administración, dirección, director, directores financieros* y *auditores externos*, también a *auditores internos, otro personal de la entidad, terceros, legisladores y reguladores, terceros en interacción con la entidad, proveedores de servicios externos, analistas financieros, agencias certificadoras de solvencia financiera* y *medios de comunicación*.

En los capítulos sobre limitaciones de gestión de riesgos corporativos y el referente a qué hacer, que personaliza algunos roles y responsabilidades, llega incluso a las *asociaciones profesionales* y a los *educadores*, pero insistiendo en la importancia de los miembros *del consejo de administración, alta dirección, reguladores* y *otro personal de la entidad*.

Debe considerarse que el complejo legisladores/reguladores/supervisores en USA ha reaccionado con significativa rapidez ante los escándalos financieros como *Enron, WorldCom* y *Adelphia* entre otros, ya que alumbró la *Sarbanes Oxley Act* en 2002, potenció la SEC (*Securities and Exchange Commission*), creó la PCAOB (*Public Company Accounting Oversight Board*), y aceleró la publicación del COSO II, facilitando un marco teórico-práctico ante la avalancha normativa.

La NIA 315 y su relación con el control interno

La Norma Internacional de Auditoría 315, “entendimiento de la entidad y su entorno y evaluación de los riesgos de representación errónea de importancia relativa”, entró en vigor a partir de diciembre de 2004.

El propósito de esta Norma Internacional de Auditoría es establecer normas y proporcionar guías para obtener un entendimiento de la entidad y su entorno, incluyendo su control interno, y para evaluar los riesgos de representación errónea de importancia relativa en una auditoría de estados financieros.

En el punto 41 la NIA 315 dice que “el auditor deberá obtener un entendimiento del control interno relevante para la auditoría. El auditor usa el entendimiento del control interno para identificar los tipos de representaciones erróneas potenciales, considerar factores que afectan a los riesgos de representación errónea de importancia relativa, y diseñar la naturaleza, oportunidad y extensión de procedimientos adicionales de auditoría”. Esto tiene el mismo espíritu de las normas de auditoría aplicables en Argentina (RT 7, ahora RT 37) cuando en su punto 2.5.1 la primera mencionaba como procedimiento inicial de auditoría para reunir los elementos de juicio válidos y suficientes, la “evaluación de las actividades de control de los sistemas que son pertinentes a su revisión, siempre que, con relación a su tarea, el auditor decida depositar confianza en tales actividades. Esta evaluación es conveniente que se desarrolle en la primera etapa porque sirve de base para perfeccionar la planificación en cuanto a la naturaleza, extensión y oportunidad de las pruebas de auditoría a aplicar”.

La NIA 315 recoge todos los conceptos del sistema de control interno vertidos en el informe COSO I y II, que ya explicamos en los acápites anteriores, razón por la cual en esta parte solo expondremos aquellos conceptos que se resaltan y ejemplos que agreguen valor a lo descripto anteriormente.

La forma en que se diseña e implementa el control interno varía con el tamaño y complejidad de una entidad. Específicamente, las entidades pequeñas pueden usar medios menos formales y procesos y procedimientos más sencillos para lograr sus objetivos. Por ejemplo, las entidades pequeñas con implicación activa de la administración en el proceso de información financiera

pueden no tener descripciones extensas de procedimientos contables o políticas detalladas por escrito. Para algunas entidades, en particular entidades muy pequeñas, el gerente-dueño puede desempeñar funciones que en una entidad mayor se consideraría que pertenecen a varios de los componentes del control interno.

Por lo tanto, los componentes del control interno pueden no distinguirse claramente dentro de las entidades pequeñas, pero sus fines subyacentes son igualmente válidos.

Respecto a los controles relevantes para la auditoría, la NIA 315 dice que hay una relación directa entre los objetivos de una entidad y los controles que implementa para proporcionar seguridad razonable sobre su logro. Los objetivos de la entidad, y por lo tanto sus controles, se relacionan con información financiera, operaciones y cumplimiento; sin embargo, no todos estos objetivos y controles son relevantes para la evaluación del riesgo por el auditor. Ordinariamente, los controles que son relevantes para una auditoría son pertinentes al objetivo de la entidad de preparar estados financieros para fines externos que den un punto de vista verdadero y razonable (o se presenten razonablemente respecto de todo lo importante) de acuerdo con el marco de referencia de información financiera aplicable y la administración del riesgo que puede dar origen a una representación errónea de importancia relativa en dichos estados financieros. Es un caso de juicio profesional del auditor, sujeto a los requisitos de esta NIA, si un control, en lo individual o en combinación con otros, es relevante para las consideraciones del auditor al evaluar los riesgos de representación errónea de importancia relativa y al diseñar y desempeñar procedimientos adicionales en respuesta a los riesgos evaluados. Al ejercer ese juicio, el auditor considera en las circunstancias el componente aplicable y factores como: el juicio del auditor sobre la importancia relativa, el tamaño de la entidad, la naturaleza del negocio de la entidad, incluyendo su organización y características de propiedad, la diversidad y complejidad de las operaciones de la entidad, los requisitos legales y reglamentarios aplicables, la naturaleza y complejidad de los sistemas que son

parte del control interno de la entidad, incluyendo el uso de organizaciones de servicios.

Los controles sobre la integridad y exactitud de la información producida por la entidad pueden ser también relevantes para la auditoría si el auditor se propone hacer uso de la información para diseñar v desempeñar procedimientos adicionales. La experiencia previa del auditor con la entidad y la información obtenida para entender la entidad y su entorno a lo largo de la auditoría ayudan al auditor a identificar los controles relevantes para la auditoría. Más aún, aunque el control interno se aplique a toda la entidad o a cualquiera de sus unidades de operación o procesos de negocios, puede no ser relevante para la auditoría un entendimiento del control interno relativo a cada una de las unidades de operación y procesos de negocios de la entidad.

Los controles relativos a objetivos de operaciones y cumplimiento pueden, sin embargo, ser relevantes para una auditoría si son pertinentes a datos que el auditor evalúa o utiliza al aplicar procedimientos de auditoría. Por ejemplo, pueden ser relevantes para una auditoría los controles pertinentes a datos no financieros que el auditor usa en procedimientos analíticos, como estadísticas de producción, o controles para detectar incumplimiento de leyes y reglamentaciones que puedan tener un efecto directo y de importancia relativa en los estados financieros, como controles sobre el cumplimiento de leyes y reglamentos de impuestos usados para determinar las provisiones para el impuesto a las ganancias pueden ser relevantes para la auditoría.

Una entidad generalmente tiene controles relativos a objetivos que no son relevantes para una auditoría y, por lo tanto, no necesitan considerarse. Por ejemplo, una entidad puede apoyarse en un sistema sofisticado de controles automatizados para proporcionar operaciones eficientes y efectivas (como el sistema automatizado de controles de una línea aérea comercial para mantener programación de vuelos), pero estos controles ordinariamente no serían relevantes para la auditoría.

El control interno sobre salvaguarda de activos sobre adquisición, uso, o disposición no autorizados, puede incluir controles relativos a objetivos de información financiera y de operaciones. Para obtener un entendimiento de

cada uno de los componentes del control interno, la consideración del auditor de los controles de salvaguarda generalmente se limita a los que son relevantes para la confiabilidad de la información financiera. Por ejemplo, el uso de controles de acceso, como contraseñas, que limitan el acceso a los datos y programas que procesan los desembolsos de efectivo puede ser relevante para una auditoría de estados financieros. A la inversa, los controles para prevenir el uso excesivo de materiales de la producción generalmente no son relevantes para una auditoría de estados financieros.

La principal responsabilidad por la prevención y detección de fraude y error descansa tanto en los encargados del gobierno corporativo como en la administración de una entidad. Al evaluar el diseño del ambiente de control y determinar si se ha implementado, el auditor entiende cómo la administración, con la supervisión de los encargados del gobierno corporativo, ha creado y mantenido una cultura de honestidad y conducta ética, y ha establecido los controles apropiados para prevenir y detectar el fraude y error dentro de la entidad.

Las entidades pequeñas pueden implementar los elementos del ambiente de control de manera diferente a las entidades mayores. Por ejemplo, las entidades pequeñas podrían no tener un código de conducta por escrito, sino desarrollar una cultura que enfatice la importancia de la integridad y de la conducta ética a través de comunicaciones orales y con el ejemplo de la administración. De modo similar, los encargados del gobierno corporativo en las entidades pequeñas pueden no incluir un miembro independiente o externo.

Generalmente, las actividades de control que pueden ser relevantes para una auditoría pueden categorizarse como políticas y procedimientos correspondientes a:

- ✓ Revisiones de desempeño: estas actividades de control incluyen revisiones y análisis de desempeño real versus presupuestos, pronósticos y desempeño del periodo anterior; relacionar diferentes conjuntos de datos operativos y financieros entre sí, junto con análisis de las relaciones y acciones de investigación y correctivas; comparar datos internos con fuentes externas de información; y revisar el desempeño

funcional o de actividad, como la revisión que hace un gerente de préstamos al consumidor en un banco de los informes por sucursal, región, y tipo de préstamo para aprobaciones y cobros de los préstamos.

- ✓ Procesamiento de información: se realiza una variedad de controles para verificar la exactitud, integridad y autorización de las transacciones. Los dos grandes agrupamientos de actividades de control de los sistemas de información son los controles de aplicación y los controles generales de TI. Los controles de aplicación sirven para el procesamiento de aplicaciones individuales. Estos controles ayudan a asegurar que ocurrieron las transacciones, que están autorizadas, y que son registradas y procesadas de manera completa y exacta. Los ejemplos de controles de aplicación incluyen verificar la exactitud aritmética de los registros, mantenimiento y revisión de saldos de cuentas y balances de comprobación, controles automatizados como verificaciones de edición de datos de entrada y verificaciones de secuencia numérica, y seguimiento manual de informes de excepción. Los controles generales de TI son políticas y procedimientos que se relacionan con muchas aplicaciones y soportan el funcionamiento efectivo de los controles de aplicación ayudando a asegurar la operación apropiada continua de los sistemas de información. Los controles generales de TI comúnmente incluyen controles sobre centros de datos y operaciones en red, adquisición, cambio y mantenimiento de software del sistema; seguridad de acceso, y adquisición, desarrollo y mantenimiento del sistema de aplicación. Estos controles se aplican a entornos de computadora central, microcomputadoras y de usuario final. Los ejemplos de estos controles generales de TI son controles de cambio de programas, controles que restringen el acceso a programas o datos, controles sobre la implementación de nuevas emisiones de aplicaciones de software en paquetes, y controles sobre software del sistema que restringen acceso a, o monitorean, el uso de servicios del sistema que pudieran cambiar datos o registros financieros sin dejar un rastro de auditoría.

- ✓ Controles físicos: estas actividades abarcan la seguridad física de los activos, incluyendo salvaguardas adecuadas como instalaciones aseguradas sobre el acceso a activos y registros, autorización para acceso a programas de computadora y archivos de datos, y conteo periódico y comparación con cantidades mostradas en los registros de control (por ejemplo, comparar los resultados de conteo de efectivo, valores e inventario con los registros contables). El grado en que los controles físicos que se proponen son relevantes para la confiabilidad de la preparación de los estados financieros y, por lo tanto, para la auditoría, depende de circunstancias como cuando los activos son altamente susceptibles a malversación. Por ejemplo, estos controles ordinariamente no serían relevantes cuando se detectaran pérdidas de inventario conforme a inspección física periódica y se registraran en los estados financieros. Sin embargo, si para fines de información financiera la administración se apoya exclusivamente en registros de inventario perpetuo, los controles de seguridad física serían relevantes para la auditoría.
- ✓ Segregación de deberes: asignar a personas diferentes las responsabilidades de autorizar transacciones, registrarlas y mantener custodia de los activos, tiene la intención de reducir las oportunidades de permitir a alguna persona estar en posición tanto de perpetrar como de ocultar errores o fraude en el curso normal de los deberes de la persona. Los ejemplos de segregación de deberes incluyen informar, revisar y aprobar conciliaciones, y aprobación y control de documentos.

Ciertas actividades de control pueden depender de la existencia de políticas apropiadas de más alto nivel establecidas por la administración o por los encargados del gobierno corporativo. Por ejemplo, los controles de autorización pueden delegarse bajo lineamientos establecidos, como criterios de inversiones establecidos por los encargados del gobierno corporativo; alternativamente, las transacciones no rutinarias como adquisiciones o desembolsos importantes pueden requerir aprobación específica de alto nivel, incluyendo en algunos casos la de los accionistas.

Gobierno corporativo y su relación con el control interno

El concepto de gobierno corporativo (GC), es el conjunto de principios y normas que regulan el diseño, integración y funcionamiento de los órganos de gobierno de la empresa, como son los tres poderes dentro de una sociedad: los accionistas, el directorio y la alta administración.

Un buen gobierno corporativo provee los incentivos para proteger los intereses de la compañía y los accionistas, y monitorizar la creación de valor y uso eficiente de los recursos brindando una transparencia de información. El concepto apareció hace algunas décadas en los países más desarrollados del oeste de Europa, en Canadá, los Estados Unidos y Australia, como consecuencia de la necesidad que tenían los accionistas minoritarios de una empresa de conocer el estado que guardaba su inversión; esto es, querían saber qué se estaba haciendo con su dinero y cuáles eran las expectativas futuras. Esto hizo que los accionistas mayoritarios de un negocio y sus administradores iniciaran un proceso de apertura de la información, así como de profesionalización y transparencia en el manejo del mismo.

La *Organización para la Cooperación y el Desarrollo Económicos* (OCDE), emitió en mayo de 1999 y revisó en 2004 sus "Principios de Gobierno Corporativo" en los que se encuentran las ideas básicas que dan forma al concepto que es utilizado por los países miembros y algunos otros en proceso de serlo.

Los principios de la OCDE contemplan que el marco de GC debe:

- ✓ proteger los derechos de accionistas;
- ✓ asegurar el tratamiento equitativo para todos los accionistas, incluyendo a los minoritarios y a los extranjeros;
- ✓ todos los accionistas deben tener la oportunidad de obtener una efectiva reparación de los daños por la violación de sus derechos;
- ✓ reconocer los derechos de terceras partes interesadas y promover una cooperación activa entre ellas y las sociedades en la creación de riqueza, generación de empleos y logro de empresas financieras sustentables;

- ✓ asegurar que haya una revelación adecuada y a tiempo de todos los asuntos relevantes de la empresa, incluyendo la situación financiera, su desempeño, la tenencia accionaria y su administración;
- ✓ asegurar la guía estratégica de la compañía, el monitoreo efectivo del equipo de dirección por el consejo de administración y las responsabilidades del consejo de administración con sus accionistas.

Hoy en día es tan importante el gobierno corporativo como un desempeño financiero eficiente. Se supone que muchos inversores pagarían más por una compañía con un buen gobierno corporativo; ya que este elemento les brinda una mayor seguridad a su inversión asegurando sanas prácticas corporativas. Cuanto mayor sea la transparencia y más información exista, mayor será la confianza de los inversores en el mercado. Por lo anterior, el gobierno corporativo, lejos de ser una moda, representa un concepto necesario para la sostenibilidad y crecimiento de las empresas.

La relación entre control interno y gobierno corporativo es directa ya que los tres órganos -gerencia o administración, accionistas y directorio- tendrán interés y responsabilidad en que la empresa cuente con un sistema de control interno fuerte, y que le proporcione un grado de seguridad razonable en cuanto a la consecución de los objetivos planificados. Una de las responsabilidades más importantes de los encargados del gobierno corporativo incluye un proceso para revisar la efectividad del control interno de la entidad

Un buen sistema de control interno contribuye a un manejo eficaz y eficiente del negocio, que es básicamente responsabilidad de la administración; pero el directorio será quien vele por el cumplimiento de los objetivos de la empresa, aprobando los planes, definiendo controles, inculcando una conducta ética y controlando el desempeño de administración. Por su parte, los accionistas aprobarán la labor del directorio y los estados contables que deben surgir de información financiera confiable, por lo que también tienen un especial interés en la existencia de un sistema de control interno eficaz y eficiente

La importancia de las responsabilidades de los encargados del gobierno corporativo se reconoce en códigos de prácticas, también llamados *best practices* o *benchmarking*.

El *benchmarking* puede definirse como un proceso sistemático y continuo para evaluar comparativamente los productos, servicios y procesos de trabajo en organizaciones. Consiste en tomar *comparadores* a aquellos productos, servicios y procesos de trabajo que pertenezcan a organizaciones que evidencien las mejores prácticas sobre el área de interés, con el propósito de transferir el conocimiento de las mejores prácticas y su aplicación.

Este proceso continuo de comparar actividades, tanto en la misma organización como en otras empresas, lleva a encontrar la mejor; para luego intentar copiar esta actividad generando el mayor valor agregado posible. Hay que mejorar las actividades que generan valor y reasignar los recursos liberados al eliminar o mejorar actividades que no generen valor (o no sea el deseado).

Algunas empresas comparan sus sistemas de control interno con los de otras entidades, lo que se conoce generalmente como *benchmarking*. El *benchmarking* es la consecuencia de una administración para la calidad, además de ser una herramienta en la mejora de procesos.

Conclusión

El antiguo comerciante atendía su negocio en forma personal, por lo cual no tenía la necesidad de practicar un control sobre las operaciones, ya que el mismo las efectuaba y si detectaba algún error localizaba su origen y lo corregía. Esto ocurría por que en una sola persona se agrupaban las funciones de adquisición de insumos, elaboración de la producción, la venta, la cobranza y la rudimentaria administración.

Con el paso del tiempo y debido al desarrollo industrial y económico, los comerciantes o industriales propietarios se vieron obligados a subdividir o delegar funciones dentro de la organización, y la respectiva responsabilidad de los hechos operativos o de gestión. Pero dicha delegación de funciones y responsabilidades no estuvo sola en el proceso, ya que en forma paralela se debieron establecer sistemas o procedimientos que previeran fraudes o

errores, que protegieran el patrimonio, que dieran información coherente y que permitieran una gestión eficiente. Así nace el control como una función gerencial, para asegurar y constatar que los planes y políticas preestablecidas se cumplan tal como fueron fijados.

La expresión *control interno* es generalmente utilizada para enunciar el conjunto de directrices y normas emanadas de los dueños o máximos ejecutivos, para dirigir, coordinar y controlar a sus subordinados, con el propósito de que se cumplan los objetivos de la empresa. Como ejemplos de estas normas podemos citar: disponer niveles de autorización a medida que las operaciones se tornan más complejas, resguardar en cajas fuertes los valores y documentos importantes, generar una estructura con segregación de funciones, esto es asignar a personas diferentes las responsabilidades de autorizar transacciones, registrarlas y mantener la custodia de los activos, definir controles de acceso al ingreso de datos con contraseñas, establecer acceso restringido a lugares con activos o información importante.

Si bien existen varias definiciones sobre *control interno,* adoptamos para el presente trabajo la que consideramos mas universalmente aceptada, que fue la dictada por el informe COSO en el año 1992. Dicho informe lo define como un proceso efectuado por el consejo de administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías: Eficacia y eficiencia de las operaciones, Confiabilidad de la información financiera y Cumplimiento de las leyes y normas aplicables.

El informe COSO define para el sistema de control interno la existencia de cinco componentes relacionados entre sí: Ambiente de control, Evaluación de riesgos, Actividades de control, Información y comunicación y Supervisión. El ambiente de control es la base de todos los demás componentes, aporta disciplina y estructura, dentro de este entorno los directivos evalúan los riesgos que afectan a la organización y que podrían atentar contra el cumplimiento de los objetivos, para luego diseñar las actividades de control que minimicen dichos riesgos. Mientras tanto la información relevante se capta y se comunica

por toda la organización. Todo este proceso es supervisado y modificado cuando es necesario.

Todos los miembros de la organización son responsables del control interno, aunque no todos con el mismo grado de responsabilidad. De hecho casi todos los empleados producen información utilizada en el sistema de control interno o realizan las funciones necesarias para efectuar el control.

No obstante la dirección, considerando por tal al máximo ejecutivo de una empresa, es el principal responsable y debería asumir la *titularidad* del sistema de control interno.

No es ajena la responsabilidad para el Gobierno Corporativo. Un buen sistema de control interno contribuye a un manejo eficaz y eficiente del negocio, que es básicamente responsabilidad de la Administración; pero el Directorio será quien vele por el cumplimiento de los objetivos de la Empresa, aprobando los planes, definiendo controles, inculcando una conducta ética y controlando el desempeño de la Administración. Por su parte los accionistas (dueños) aprobarán la labor del Directorio y también serán los encargados de aprobar los estados contables que deben surgir de información financiera confiable, por lo que también tienen un especial interés en la existencia de un sistema de control interno apropiado.

El auditor externo debe analizar el control interno del ente objeto de su auditoría, pues esto condicionará la naturaleza, alcance y oportunidad de los procedimientos de auditoría que aplicará. Es decir que en la medida que la empresa posea controles, que funcionando adecuadamente permitan concluir que las afirmaciones contenidas en los estados contables son válidas, el auditor centrará su atención únicamente en esos controles, planificando fundamentalmente pruebas de cumplimiento de controles y en menor medida pruebas sustantivas, a la inversa si se encuentra frente a un ente que tiene un débil sistema de control interno, o habiendo diseñado un buen sistema de control el mismo no funciona adecuadamente, planificará una auditoria basada en pruebas sustantivas, con el mayor costo que esto implica.

Por último vale la pena considerar que el control interno tiene sus limitaciones, puede ayudar a que una entidad consiga sus objetivos de rentabilidad y a

prevenir la pérdida de recursos, puede ayudar a la obtención de información financiera confiable, puede reforzar la confianza en que la empresa cumple con la normatividad aplicable; pero no importa lo bien concebido que esté y lo bien que funcione, únicamente puede dar un grado de seguridad razonable, no absoluta, a la dirección y al consejo de administración en cuanto a la consecución de los objetivos de la entidad. El control interno no puede hacer que un gerente malo se convierta en un buen gerente.

LOS AUTORES

Lorena María Martires

Contador Público UNLP con post grado de especialista en Procedimiento Fiscal y Ley Penal Tributaria y Previsional UNLP. Desde 1999 Ayudante diplomada de Contabilidad VIII- Auditoría- en la Facultad de Ciencias Económicas (UNLP).
Desde 1996 desarrolla su profesión en el sistema financiero, habiéndose desempeñado como analista en el Banco Central de La Republica Argentina, jefe de equipo de auditoria interna en el Banco Municipal de La Plata, y desde 2006 en el Banco de la Provincia de Buenos Aires en el área de Créditos, análisis de riesgo y auditoría de balances.

Marcela Falvella

Contador Público por la UNLP. Cursó la Maestría en Auditoría Gubernamental en la Universidad Nacional de San Martín (UNSAM) y actualmente se encuentra elaborando su tesis. Es Docente Adjunta en la Cátedra de Contabilidad Pública de la Universidad Atlántida Argentina y Ayudante Diplomada de las Cátedras de Contabilidad IV y VIII de la Facultad de Ciencias Económicas de la UNLP. Además es miembro permanente del área de capacitación de la Contaduría General de la Provincia y Contador Fiscal Delegado del organismo desde 1999.

Carlos Alberto Rumitti

Contador Público por la Universidad del Centro de la Provincia de Buenos Aires. Profesor Adjunto Regular en la Cátedra de Contabilidad VIII- Auditoría de la Facultad de Ciencias Económicas de la UNLP, y Profesor Adjunto Regular en Auditoría de la Universidad Nacional de Mar del Plata, Profesor Adjunto a cargo de las cátedras de Auditoría I y Auditoría II de la Universidad CAECE, en

Auditoría de Sistemas Computarizados en la Universidad Atlántida Argentina y profesor de postgrado de Auditoría de Sistemas en la UNS. Desde 1987 se desempeña como profesional en empresas del sector privado y participó también en el desarrollo y asesorando diversos proyectos provinciales desde la función pública. Es autor de los Apéndices Técnicos “Seguridad de la Información” (2007), “Del Glifo al Algoritmo” (2007) y “Firma Digital” (2007) publicados en la Revista En Blanco del Ministerio de Economía.

Ana María Cóccaro

Contador Público (UNLP) y Magíster en Disciplinas Bancarias por la Facultad de Ciencias Económicas (UNLP en convenio con la Universitá di Siena, Facoltá de Scienze Economiche e Bancarie, Italia). En 2009 fue distinguida con el premio Jerarquía del Área Técnica de la Facultad de Ciencias Económicas (UNLP) por el trabajo ”Una Aproximación Jurídica Contable hacia el Concepto de Patrimonio Ambiental”. Es Profesora Adjunta Ordinaria en la cátedra de Contabilidad VIII- Auditoría de la UNLP y docente asociada en la cátedra de Auditoría I y II de la Universidad Católica de La Plata. También es coordinadora de la Cátedra Libre “Alejandro Korn”, dependiente de la Secretaria de Extensión Universitaria de la Presidencia de la UNLP.

El sistema de control interno en las empresas o entes constituye un significativo aporte a lo que debiera ser una permanente búsqueda de la eficiencia en la gestión de negocios. Los buenos manuales de procedimientos administrativos y operativos, luego efectivamente aplicados en el funcionamiento de los diversos sectores, constituyen la piedra angular de lo que conlleva poseer un buen ambiente de control de la organización. El tema del control interno se vincula estrechamente con otro muy en boga: el denominado gobierno corporativo. Es decir, que existan líneas de responsabilidad claramente definidas con funciones específicas legisladas de manera concreta.

La colección 60 aniversario Libros de Cátedra de la Facultad de Ciencias Económicas, *responde a una convocatoria de la Secretaría de Asuntos Académicos, que tiene como objetivo central fortalecer la enseñanza de grado y potenciar las capacidades de los equipos de cátedra para producir materiales de estudio, y al mismo tiempo permitir otros modos de transmisión y apropiación del saber.*

ISBN 978-987-1985-11-1