La Tecnología de la Información y el Control Interno en el marco de NIIF y NIAAS

Information of Technology and Internal Control within the framework of IFRS and NIAAS

MSc. Christian Vaca Benalcázar
Universidad Tecnológica Israel
patos_nice@hotmail.com

Fecha de recepción: 20/07/2016
Fecha de aceptación: 24/10/2016

Resumen:

La información permite a las empresas establecer estrategias financieras, comerciales u operativas independiente de su tamaño, giro de negocio o lugar en el que se encuentren domiciliadas. Uno de los estándares que permite que esta información sea comparable y legible en cualquier parte del mundo son las Normas Internacionales de Información Financiera NIIF. Con el avance de la tecnología y el bajo costo para el acceso ilimitado a medios informáticos de procesamiento de información que van desde hojas electrónicas, software de gestión administrativa y financiera, hasta los más avanzados ERP (Enterprise Resource Planning) hace de la Tecnología de la Información uno de los recursos más importantes dentro de las empresas. En un ambiente automatizado los datos procesados deben cumplir con normas de control interno que aseguren y garanticen a los stakeholders los principios de la seguridad de la información.

Palabras claves: Tecnologías de Información, NIIF, COSO, Control Interno.

Abstract

The information allows to the companies establishing financial, commercial and operational strategies independent of their size, business score or geographic localization. IFRS - International Financial Reporting Standards is one of the standards that allows this information to be comparable and readable around the world. The technology advancement and the low cost for unlimited information processing computer access from spreadsheets, administrative and financial management software to the most advanced ERP (Enterprise Resource Planning) makes to ToI one of the most important resources in the companies. The information in automated environment processed must comply with the internal control standards to ensure and guarantee to the stakeholders the security information values.

Keywords: Information Technology, IFRS, COSO, Internal Control.

Introducción

Las Normas Internacionales de Información Financiera (NIIF) son un estándar que permite revelar la información financiera de las compañías de manera que su comparación sea confiable, transparente y sencilla en cualquier parte del mundo.

En Ecuador, la Superintendencia de Compañías, según resolución 08-G-DSC-010 del 20 de noviembre del 2008, estableció bajo 3 grupos la fecha límite para que las compañías reguladas por este Organismo de Control adopten este estándar (Tabla 1).

Tabla 1: Transición a NIIF por Tipo de Compañías

Grupo	Fecha de Aplicación	Tipo de Compañías	Periodo de Transición
1	1 de Enero de 2010	Compañías y entes regulados por la Ley de Mercado de Valores, Compañías que ejercen actividades de Auditoría Externa.	2009
2	1 de Enero de 2011	Compañías con Activos totales iguales o superiores a USD 4.000.000 al 31 de diciembre del 2007, Las Compañías Holding o tenedoras de acciones que voluntariamente hayan conformado grupos empresariales, Compañías de Economía Mixta, Entidades del Sector Público, Sucursales de Compañías Extranjeras u otras empresas extranjeras estatales, paraestatales, privadas o mixtas, organizadas como personas jurídicas y las asociaciones que éstas formen y que ejerzan sus actividades en el Ecuador.	2010
3	1 de Enero de 2012	Compañías no consideradas en el grupo 1 y 2.	2011

Fuente: Superintendencia de Compañías Resolución 08-G-DSC-010
Elaborado por: El Autor.

La conversión a NIIF es más que cambios contables y financieros. La adopción de esta norma tiene como efecto: cambio a los procesos operativos y políticas contables, modificación a las aplicaciones de TI, mayor inversión en la capacitación del recurso humano, cambio en los flujos de información y un nuevo enfoque para el análisis de la información generada debido a que se necesita de un mayor nivel de detalle para la información a revelar en los Estados Financieros.

El objetivo de este documento es analizar los tipos de riesgo relacionados desde el punto de vista de la tecnología de la información, así como las diferentes metodologías que existen para la evaluación de la efectividad del control interno que aseguren el correcto desempeño de sus componentes.

1. Riesgos asociados a las Tecnologías de la Información

Según Anuario Estadístico Societario publicado por la Superintendencia de Compañías al año 2014 se registra 55.619 empresas, como se muestra en la Tabla 2:

Tabla 2: Tipo de Compañías – Movimientos Financieros 2012

Tipo de compañía	Cantidad		Activo		Pasivo		Patrimonio		Ingresos	
	No.	%	USD	%	USD	%	USD	%	USD	%
Grande	3.038	5	65.707.432.198	72	39.618.076.678	73	26.089.355.526	71	86.145.654.312	81
Mediana	7.332	13	12.741.031.540	14	7.683.614.890	14	5.057.416.649	14	14.033.813.953	13
Pequeña	17.919	32	8.009.712.785	9	4.532.057.915	8	3.477.630.655	9	5.816.881.330	5
Micro	27.312	49	5.052.740.337	6	2.687.441.788	5	2.365.034.912	6	673.229.850	1
No definido**	18	0	14.460	0	1.256	0	13.204	0	0	0
Total	**55.619**	**100**	**91.510.931.319**	**100**	**54.521.192.528**	**100**	**36.989.450.947**	**100**	**106.669.579.445**	**100**

Fuente: Anuario Estadístico Superintendencia de Compañías 2012, Por tamaño de las Compañías. Elaborado por: El Autor

** Corresponde a compañías de reciente constitución y/o que no contienen valores en sus principales variables financieras que les permita ser clasificadas.

Según publicación del Diario El Hoy: *"La aplicación de tecnología o informática en las tareas administrativas de las pequeñas y medianas empresas todavía no es suficiente en Ecuador. De las 300 mil que existen en el país, solo el 40% cuenta con un programa tecnológico. Según un estudio de Memory Computación, el miedo al uso de*

la tecnología y, sobre todo, la creencia de que es un producto caro, son las razones fundamentales que alejan a los dueños de las empresas de las soluciones informáticas: desde el manejo de caja y facturación, a un sofisticado sistema para banco. El acceso a programas básicos puede costar entre $600 y $3.000, aunque también hay soluciones informáticas más integrales cuyos costos llegan hasta los $100 mil." (Diario El Hoy, 2008).

La importancia de conocer estos datos y su relación con el uso de tecnologías de la información y la implementación de NIIF radica en el comportamiento proporcional que existe entre el tamaño de la empresa y las operaciones (transacciones productivas, comerciales y administrativas) que van a procesar en sus aplicaciones y los riesgos inherentes a los que está expuesta esta información de tener un sistema de control interno deficiente, o peor aún, carecer de uno.

Debido a la alta complejidad del reporte financiero bajo NIIF, el control interno debe ser reforzado o implementado en las empresas por medio de su Gerencia Financiera, o de ser el caso, de acuerdo al tamaño de la compañía o de sus operaciones contar con un Área de Auditoría Interna que apoye en el establecimiento de políticas y procedimientos (análisis de contratos, reconocimiento del ingreso, activación y depreciación de activos, provisión de cartera, inventarios, etc.) que fortalezcan el ambiente de control, el Gobierno Corporativo y el Gobierno de TI.

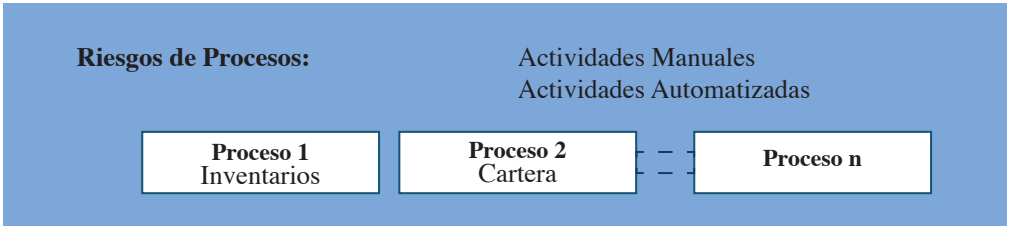
Para hablar de controles a nivel de TI en un proceso de adopción y reporte bajo NIIF, primero debemos entender los riesgos tecnológicos a los que está expuesta la Compañía.

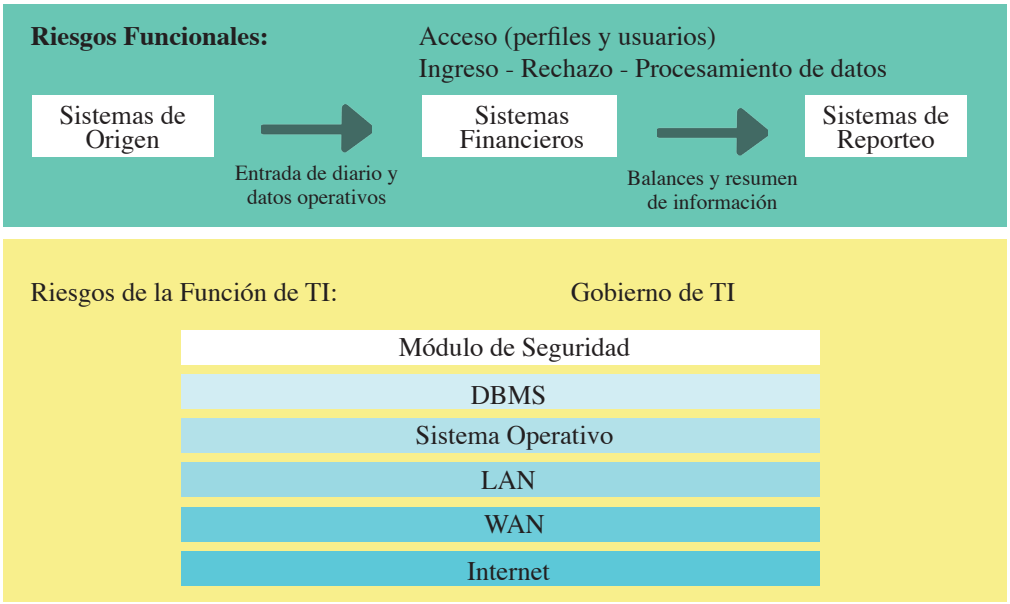
Kincaid James, en la guía de estudio para el examen de certificación en autoevaluación de control – CCSA, define al riesgo como: "la probabilidad de que ocurra un evento que pueda tener un impacto en el alcance de los objetivos. El riesgo se mide en términos de consecuencias y probabilidad de que este ocurra." (JAMES, 2008).

Los riesgos afectan al cumplimiento de los objetivos de las organizaciones, por lo tanto bajo Gestión de Riesgos se los puede categorizar como: Riesgos Estratégicos, Operacionales, de Reportes y de Cumplimiento.

Según PriceWaterHouse existen 3 tipos de riesgos inherentes a los que se exponen las empresas que hacen uso de sistemas computarizados para sus procesos de negocio, estos son: Riesgos de Procesos de Negocio, Riesgos de Sistemas de Información y Riesgos de la función de tecnología de información.

Gráfico 1: Tipo de Riesgos Inherentes





Fuente: PWC, Boletín de Asesoría Gerencial
Elaborado por: Tipo de Riesgos Inherentes

1.1 Riesgos de Procesos:

Incrementan su probabilidad e impacto de acuerdo al nivel de automatización que tengan y el macroproceso que afecten, por ello es importante que la Gerencia General apoye iniciativas para la elaboración y socialización de un código de ética y conducta, reglamento interno, políticas y procedimientos que ayuden a controlar y mitigar estos riesgos.

1.2 Riesgos Funcionales:

Los riesgos funcionales están a nivel de los sistemas de información y la arquitectura de sistemas y pueden estar en la autenticación, ingreso y procesamiento de la Información.

Durante la autenticación, la correcta definición de perfiles de usuario permite controlar:

1. Acceso no autorizado a transacciones o información sensibles, por ejemplo personal del Área Comercial que pueda modificar o visualizar información relacionada a nómina.

2. Falta de segregación de funciones a fin de mitigar riesgos de fraude, por ejemplo personal del Área de Comercial que pueda ingresar pedidos, facturar y despachar, modificar precios y descuentos sin un nivel de autorización, modificar las características de crédito de un cliente, son eventos que podrían desencadenar un posible fraude.

3. Falta administración de usuarios y claves de acceso a fin de mitigar acceso a información y ambientes restringidos, por ejemplo instalación de programas sin licencia, o peor aún, que tengan algún virus informático.

En el ingreso de información, uno de los mayores inconvenientes es el ingreso de información incorrecta, incompleta, o duplicada que a largo plazo puede ocasionar errores durante el procesamiento de la información, por ejemplo códigos duplicados de productos podrían ocasionar que durante una toma física se ingrese el conteo por duplicado generando a largo plazo inventarios sobrevalorados y existencias ficticias de productos. Actualmente los sistemas cuentan o permiten validar campos requeridos como RUC o cédula. Así también existen controles a nivel de aplicación (logs de auditoría) para que el sistema reporte cambios o modificaciones atípicas, que según el nivel de automatización de estos controles sean monitoreados mitigando así riesgos de rechazo y procesamiento.

Es muy importante el análisis de los controles a implementar a nivel de procesamiento ya que un exceso de control podría restar rendimiento de procesamiento a la aplicación y generar cuellos de botella.

1.3 Riesgos de la Función de TI

La estructura del Área de TI debe estar correctamente definida, a fin de mantener un Gobierno de TI que ayude a la empresa al logro de objetivos. La falta de una correcta administración de TI puede ocasionar que existan tiempos muertos por fallas en la red, mala atención a clientes, riesgos tributarios por falta de emisión de comprobantes de venta, información desactualizada para la toma de decisiones. Si bien TI es un proceso de soporte, en la actualidad es de vital importancia su adecuada gestión, ya que esta aporta al desarrollo normal de otros procesos dentro de las organizaciones.

2. Normas de Auditoría y Control Interno

Las Normas de Auditoría Generalmente Aceptadas (NAGAS) son principios de general aplicación que permiten al auditor garantizar calidad en su trabajo profesional.

Las NAGAS son los 10 mandamientos del auditor y se clasifican en:

a. Normas Generales:
- Entrenamiento y capacidad profesional.

- Independencia.
- Cuidado o esmero profesional.

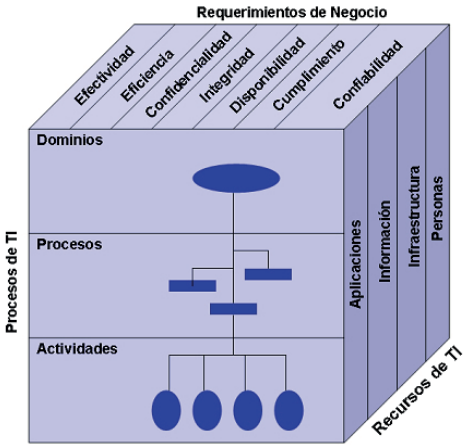
b. Normas de Ejecución del Trabajo
- Planeación y supervisión.
- Estudio y Evaluación del Control Interno
- Evidencia Suficiente y Competente

c. Normas de Preparación del Informe
- Aplicación de los principios de Contabilidad Generalmente Aceptados.
- Consistencia.
- Revelación Suficiente.
- Opinión del Auditor.

Adicional a la aplicación de las NAGAS, se debe cumplir con las disposiciones de las Normas Internacionales de Auditoría y Aseguramiento (NIAS) y para el caso de Auditoría Interna lo establecido en el Marco Internacional para la Práctica Profesional de la Auditoría Interna (IPPF). En Ecuador, para las instituciones del Sector Público, el área de Auditoría debe cumplir con las Normas de la Contraloría General del Estado.

El alto flujo de información que manejan las aplicaciones informáticas asociadas a procesos de negocio requieren un tratamiento especial que permita precautelar la integridad, confidencialidad y disponibilidad; y a la vez permita mejorar significativamente la gestión de la información, esto ha generado preocupaciones ante su vulnerabilidad es por ello que se han establecido marcos referenciales de control.

Gráfico 2: Marco COBIT



Fuente: COBIT 4.1

Las metodologías de mayor aceptación para gestión gobierno de TI y de riesgos son COBIT 4.1 y COSO ERM, respectivamente.

COBIT 4.1 (*Control Objective for Information and Related Technology* – Objetivos de Control para la Información y Tecnologías Relacionadas), es un marco de trabajo desarrollado por ISACA, que contiene las mejores prácticas enfocadas al control para optimizar las inversiones de TI. Establece 4 dominios (PO: Planear y Organizar; AI: Adquirir e Implementar; DS: Entrega y Soporte; y, ME: Monitorear y Evaluar) y 34 objetivos distribuidos para cada dominio distribuidos de la siguiente manera: PO = 10; AI = 7; DS = 13; ME = 4. La actualización más reciente es COBIT 5.

Gráfico 3: Cubo COSO ERM

Fuente: http://www.mapfre.com/fundacion/html/revistas/gerencia/n098/img/fotos/m53_7.jpg

COSO ERM (Committee Of Sponsoring Organization Of The Treadway Commission, Enterprise Risk Management – Comité de Organizaciones Patrocinadoras, Administración del Riesgo Empresarial), es un marco de referencia que contiene buenas prácticas de gestión de riesgos y una visión integradora del control interno mediante la administración de los riesgos empresariales. La versión más actualizada de este marco es COSO 2013.

COSO es una iniciativa conjunta de las siguientes organizaciones:

- Asociación de Contadores Públicos Norteamericanos (AAA)
- Instituto Norteamericanos de Contadores Públicos Certificados (AICPA)
- Asociación Internacional de Ejecutivos de Finanzas (FEI)

- Instituto de Gerentes de Contabilidad (IMA)
- Instituto de Auditores Internos (IIA)

Entre otros marcos de referencia que permiten evaluar el sistema de control interno podemos mencionar:

a. La Ley Sarbanes Oxley (SOX), que en su sección 404 establece las características mínimas que se deben cumplir para garantizar seguridad en el sistema de control interno.

b. Las Guías de Auditoría de Tecnología Global (Global Technology Audit Guide) GTAG desarrolladas por el Instituto de Auditores Internos.

c. La norma ISAE 3402, que es un estándar que tiene como finalidad proporcionar un informe que será utilizado por las entidades usuarias y sus auditores, sobre los controles en una organización de servicios que presta un servicio a las entidades usuarias que probablemente sea relevante para el control interno de las mismas al estar relacionado con la información financiera, complementa la NIA 402.

La efectividad de un control puede ser medida en términos de probabilidad que detecte, prevenga o corrija el riesgo para el que fue diseñado. El diseño, implementación y eficacia operativa de los controles debe ser evaluada periódicamente, a fin de poder realizar las actualizaciones o mejoras a los procesos.

Conclusiones y trabajos futuros

Considerando que hoy en día la tecnología de la información es usada en todas las organizaciones independientemente de su tamaño o giro de negocio, para el procesamiento de sus operaciones y la generación de información para la toma de decisiones, es importante conocer los riesgos a los que dicha información está expuesta; a fin de diseñar, implementar y monitorear controles.

Una vez implementado NIIF, es importante que las compañías mantengan una relación costo-beneficio al implementar controles, ya que el costo de un control no debe exceder los beneficios a recibir de la mitigación de un riesgo.

El desarrollo de cada una de las metodologías expuestas a nivel general en el presente documento es necesario para entender el alcance de cada uno, y poder adaptarlo a la realidad de cada empresa logrando así aportar al logro de los objetivos.

Bibliografía

Diario El Hoy. (18 de Febrero de 2008). Explored, Archivo Digital de Noticias desde 1994. Obtenido de Explored, Archivo Digital de Noticias desde 1994: http://www.explored.com.ec/noticias-ecuador/la-oferta-de-profesionales-supera-la-demanda-289263.html

JAMES, K. (2008). CCSA - Certificación en Autoevaluación de Control - Guía de Estudio Para el Examen. Florida: IIARF.

Coopers, P. (Mayo de 2010). Boletin de Asesoría Gerencial. Obtenido de https://www.pwc.com/ve/es/asesoria-gerencial/boletin/assets/edicion-05-2010.pdf

IT GOBERNANCE INSTITUTE. (2007). COBIT 4.1. Estados Unidos.