La Importancia de IT en el Diseño, Implementación y Sostenimiento del Control Interno

Alfredo Angel Pagano

Director Enterprise Risk Services

Deloitte

XI Conferencia Latinoamericana de Auditoría Interna

Argentina 2006






Deloitte.

Agenda

- Gobierno de IT
- Relación Gobierno Corporativo – Gobierno IT
- Criterios de Evaluación Aspectos IT

El rol de la Tecnología de la Información

- Para la mayoría de las organizaciones, IT es dominante en los procesos de negocio y de control interno. Hay muy pocos controles que no dependan de algún modo de IT.
- Las Aplicaciones de Sistemas son comúnmente utilizadas para iniciar, registrar, procesar e informar transacciones de negocio.
- Controles relevantes de IT: incluidos en aplicaciones financieras (controles de aplicación), como así también los de infraestructura de IT.

Por Qué Gobierno de IT?

IT governance, es responsabilidad de la alta gerencia y del Directorio de las organizaciones, y consiste en el liderazgo, organización de la estructura y los procesos que aseguran que IT sostiene y acompaña a las estrategias generales de la organización y sus objetivos.

Problemas de IT Reconocidos por los Ejecutivos

- Inadecuada o incompleta visión del funcionamiento de IT
- Fallas Operacionales
- Problemas e incidentes
- Altos costos de IT con bajo retorno sobre la inversión
- Problemas de recursos humanos de IT – gestión y retención de talentos
- Administración de datos
- Ausencia de conocimiento de sistemas críticos
- Desconexión entre las estrategias de IT y las del negocio

IT Governance - Objetivos

Direccionar los esfuerzos de IT, para asegurar que se cumplen los siguientes objetivos:

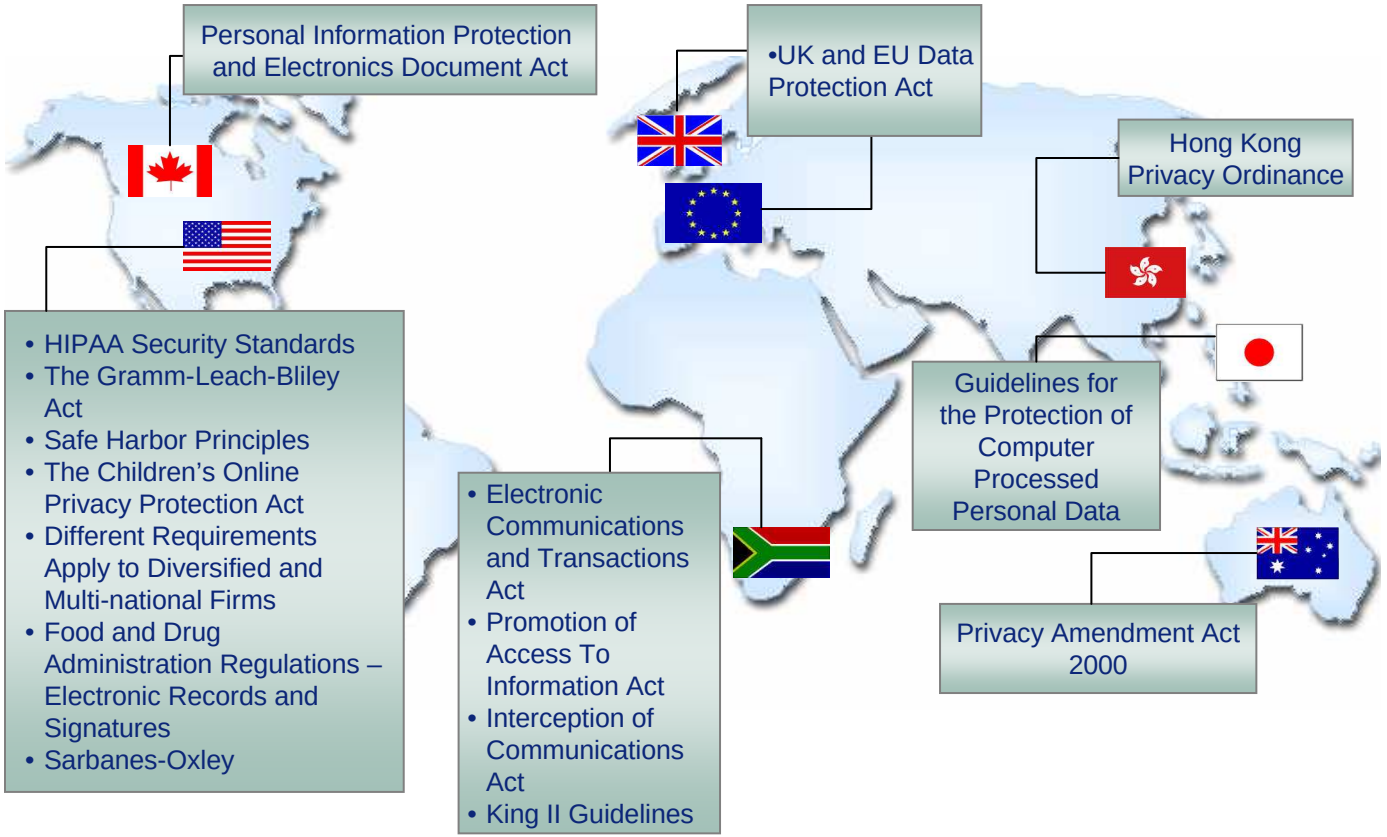
- Alineación de IT con la organización general
- Utilización de IT para permitir a la organización maximizar los beneficios y explotar las oportunidades
- Utilización responsable de los recursos de IT
- Gestión apropiada de los riesgos relacionados con IT

Alineamiento del Gobierno de IT con el Gobierno Corporativo

- Es importante que el Gobierno de IT esté alineado con el sistema de gobierno corporativo general. Ambos deben ser compatibles entre sí y formar parte del mismo sistema de monitoreo y control;

- Si los sistemas de gobierno no se encuentran alineados y coordinados, esto deriva en el aislamiento de la organización de Sistemas del resto del negocio, lo cual reforzaría el criterio de que las áreas de sistemas operan "bajo sus propias reglas".

Regulaciones Globales Requieren que el Buen Gobierno Corporativo se Extienda al Ambiente de IT



Marco de Control

- COSO - marco de control estándar de Control Interno
- COSO no provee una guía específica de controles de IT.
- Algunas fuentes reconocidas para suplementar COSO en temas de IT son:
  - CobiT (Control Objectives for Information Technology)
  - ISO 17799 - 27001

Ambiente de Control

- El ambiente de control de IT es parte del ambiente de control general.
- El “tone at the top” debe existir en IT desde el nivel del CIO.
- Se deben establecer responsabilidades y dueños de los controles específicamente
- Deben existir políticas y procedimientos de los controles de IT formalmente documentados.

Evaluación de Riesgos

- Debe existir un proceso de evaluación de riesgos de IT.
- Los riesgos de IT incluyen temas como seguridad, operaciones, disponibilidad, etc., que impactan en la confiabilidad de ICFR.
- La alta gerencia **debe** entender el impacto de los riesgos de IT relacionados con los controles de IT.

Información y Comunicación

- Implementación de infraestructura, estándares y procesos que soporten las comunicaciones.
- Oportuna generación de informes para la Gerencia
- Accesibilidad a las políticas, procedimientos, descripciones de puestos de trabajo y responsabilidades de IT.
- Correcta consolidación y comunicación de reportes e información financiera.

Monitoreo

- Se deben monitorear los controles internos de IT para evaluar constantemente la efectividad del diseño y su aplicación.
- Se debe controlar que la documentación de IT sea adecuada.
- Deben existir auditorias internas del área de IT
- Debe existir un proceso de control y monitoreo de las actividades de remediación y escalamiento.
- Monitoreo de seguridad continuo.

Ambiente de IT y sus Riesgos

Indicadores de Riesgos Potenciales de IT

- Violaciones de seguridad
- Disponibilidad inconsistente
- Interfaces demasiado complejas
- Sistemas sin soporte
- Inesperado aumento en volumen de transacciones
- Cambios excesivos a los programas
- Sistemas no documentados
- Sistemas “customizados” en exceso
- Confianza excesiva en controles manuales
- Implementaciones no estandarizadas
- Conversiones problemáticas de datos
- Controles del ambiente de IT inconsistentes
- Implementación de tecnologías nuevas y no probadas
- Importante rotación de los puestos claves del área de IT

Principios de la Evaluación de los Controles de Tecnología de la Información

- **Controles de IT a nivel de procesos / transacciones vs el nivel de controles generales**

  – **Nivel de aplicación**: vinculados directamente con objetivos de control que se relacionan con los procesos de negocio y los estados financieros.

  – **Nivel de controles generales**: Los objetivos del control computacional general **soportan** los controles de aplicación manuales y automatizados que se relacionan directamente con los procesos de negocio de la organización.

Controles de IT: Áreas de Controles Generales

¿Qué son?

CGC son actividades de control que proveen razonable seguridad de alcanzar los objetivos de control relacionados con el procesamiento de información financiera dentro del ambiente de procesamiento de la computadora.

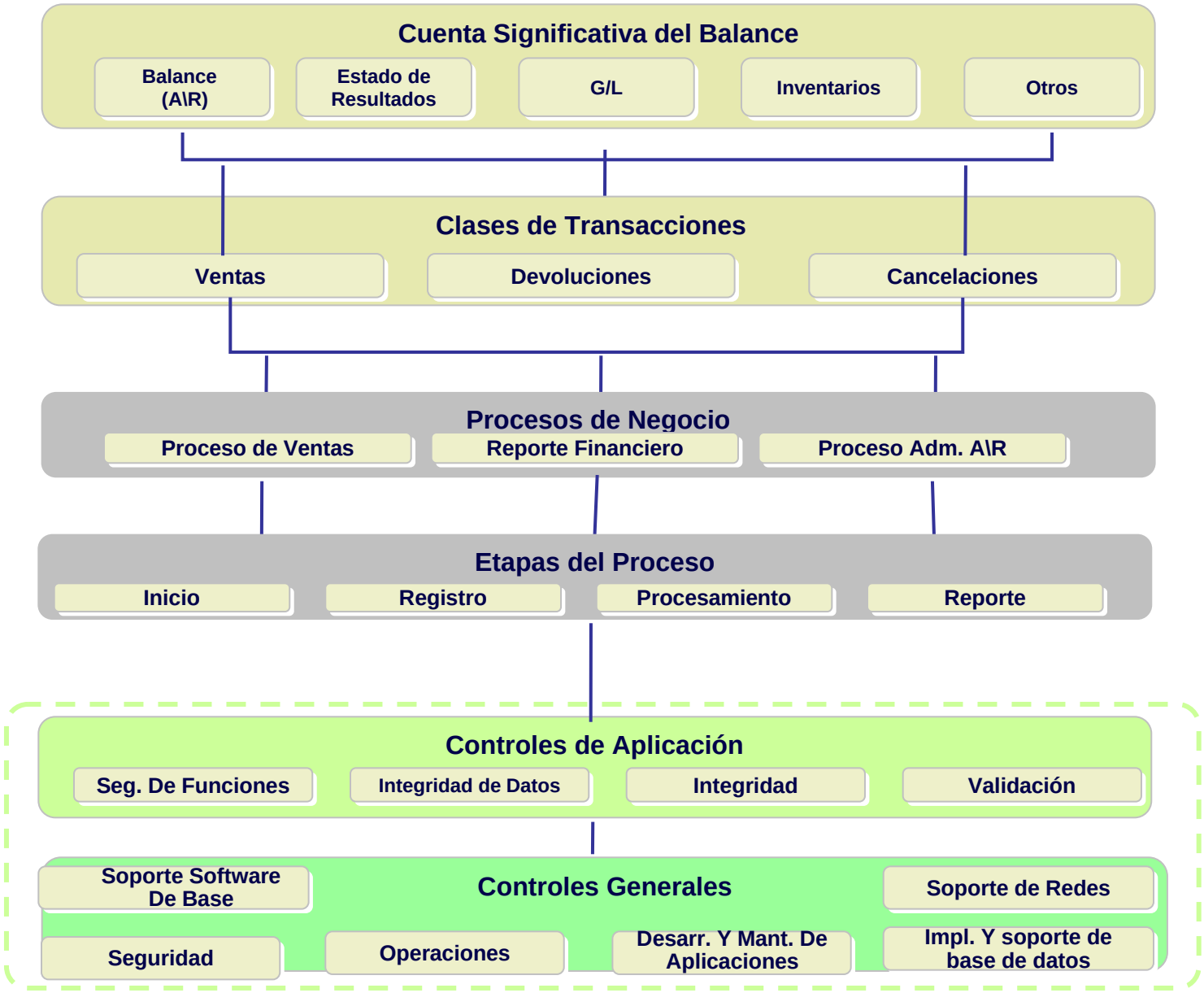
Operaciones de Sistemas de Información	Operaciones inefectivas de IT colocan a toda la infraestructura de IT en el riesgo de no soportar la operación de los sistemas ERP y aplicaciones financieras.
Seguridad de la Información	Una pobre seguridad y débiles controles de acceso proveen la oportunidad de accesos no autorizados, cambios o uso indebido de la información financiera.
Implementación y Mantenimiento de Sistemas de Aplicación	Aplicaciones implementadas o mantenidas inadecuadamente pueden conducir a procesamientos inexactos de información financiera, cálculos incorrectos o problemas de integridad.
Implementación y soporte de Base de Datos	Una inadecuada estructura y almacenamiento de la información financiera podría atentar contra la integridad de la información procesada por las aplicaciones de negocio.
Soporte de Red	La infraestructura de la red debe contribuir a la transmisión de información exacta, oportuna y completa. Seguridad de red, firewalls, y protección de virus son críticas para la integridad y la seguridad de las aplicaciones.
Soporte del Software de Base	El software de base sustenta los ERP y las aplicaciones financieras. Si no son implementados, soportados o mantenidos, las aplicaciones que se ejecutan sobre estos podrían producir resultados inesperados.

Controles de IT: Controles de Aplicación

- Contribuyen a asegurar la integridad, exactitud, autorización y la validez de las transacciones durante el procesamiento de las aplicaciones
- También contribuyen a asegurar que las interfaces con otros sistemas funcionan correctamente, y que todos los ingresos y salidas de información son íntegros y correctos.
- Los controles de aplicaciones son habitualmente incluidos dentro de las aplicaciones para prevenir o detectar transacciones no autorizadas.
- Los controles de aplicaciones relevantes deben ser identificados por la alta gerencia independientemente de quien sea el responsable de estos controles (IT o unidad de negocio) para su evaluación y monitoreo

Controles de IT: Controles de Aplicación

Objetivo	Controles de Aplicación
Todas las ordenes recibidas de clientes son ingresadas y procesadas.	• Los reportes de órdenes pendientes son generados diariamente para revisarlos. • Las órdenes incompletas son marcadas para revisarlas.
Las ordenes son procesadas sólo dentro del limite de crédito del cliente autorizado	• Las ordenes ingresadas que exceden el limite de crédito del cliente quedan pendientes para revisión previa a su proceso. • El acceso al cambio/anulación del limite de crédito del cliente requiere aprobación de la gerencia.
Sólo las ordenes validadas son procesadas.	• El acceso a la carga de órdenes está limitado al personal apropiado • Un número de Cliente válido es requerido previo al ingreso de una orden.
Las ordenes y sus cancelaciones son ingresadas correctamente.	• Los campos de datos críticos (fecha, dirección) son completados automáticamente • La información de devoluciones es comparada con la información original de la venta.



Principios de Evaluación de los Controles de Tecnología de la Información

Control de tecnología de la información que logra un objetivo de control a nivel de procesos/transacciones

Ejemplo 1:

Objetivo de control: Los montos de las cuentas por pagar se calculan y registran con exactitud.

Actividad de control: Los bienes recibidos son procesados en lotes y se cuadran los datos de entrada del lote; los lotes descuadrados se corrigen de inmediato.

Ejemplo 2:

Objetivos de control: Las adiciones a los archivos maestros de remuneraciones representan empleados vigentes.

Actividad de control: Se configura un mecanismo de seguridad para restringir el acceso para modificar los archivos maestros de remuneraciones.

Principios de Evaluación de los Controles de Tecnología de la Información

Un control de tecnología de la información que soporta la eficacia continua de los controles de aplicación

Ejemplo 1:

Actividad de control: Se define los procedimientos de procesamiento por lotes para asegurar que se procesan los trabajos y/o las transacciones hasta su conclusión normal o que se recuperan y vuelven a procesar.

Ejemplo 2:

Actividad de control: Mecanismo de seguridad que restringe el acceso a la realización de la administración de seguridad en el sistema.

Principios de Evaluación de los Controles de Tecnología de la Información

Compare la forma en que la naturaleza de la actividad de control determina la manera de evaluación de las deficiencias

Ejemplo seguridad:

Se restringe el acceso a la configuración principal de seguridad

Se restringe el acceso al archivo maestro de remuneraciones o se restringe el acceso al archivo maestro de proveedores

Ejemplo operaciones:

Se define los procedimientos de procesamiento por lotes para asegurar que se procesan los trabajos y/o las transacciones hasta su conclusión normal o que se recuperan y vuelven a procesar

Se coloca los bienes recibidos en lotes y se cuadran los datos de entrada del lote; los lotes descuadrados se corrigen de inmediato

Deficiencias en Controles Generales del Computador

Tres situaciones en las que una deficiencia de control al nivel de controles generales podría subir al nivel de una debilidad material

- Una deficiencia de control de aplicación relacionada con o causada por una deficiencia de control general se clasifica como una debilidad material.
- Una deficiencia de control general clasificada como una deficiencia significativa sigue sin corregir después de un periodo de tiempo razonable.
- Como resultado de la generalización y la relevancia de una deficiencia de control computacional general se llega a la conclusión de que existe una debilidad material en el ambiente de control de la empresa.

Repaso de lo Discutido

- La determinación de la naturaleza de los controles en los que confía la gerencia para lograr los objetivos de control es crítica.
  - Controles de Aplicación
  - Controles Generales del Computador
- Se evalúa las deficiencias de los controles generales con respecto a su efecto sobre los controles de aplicación.
- Tres situaciones en las que una deficiencia de control computacional general podría convertirse en una debilidad material:
  - Una deficiencia de control de aplicación relacionada con o causada por una deficiencia de control general se clasifica como una debilidad material.
  - La generalización y la relevancia de una deficiencia de control general lleva a la conclusión de que existe una debilidad material en el ambiente de control de la empresa.
  - Una deficiencia de control general clasificada como una deficiencia significativa sigue sin corregir después de un periodo de tiempo razonable.

Deloitte.

¡Gracias!

Alfredo Angel Pagano

apagano@deloitte.com