# El rol de la auditoría de sistemas de información en la evaluación del gobierno de tecnologías de información en las organizaciones

## The role of information system audit in the evaluation of information technology governance in organizations

**JUAN FEDERICO GÓMEZ-ESTUPIÑÁN**
*Ingeniero de Sistemas*
*Especialista en Telemática*
*Grupo de Investigación GIPROCAS*
*Universidad de Boyacá, Colombia*
*jfgomez@uniboyaca.edu.co*

Recibido: 25/06/2012 Aceptado: 17/10/2013

## RESUMEN

Uno de los aspectos críticos en la función informática de las organizaciones es el gobierno de Tecnologías de Información (TI) que se enfoca en alinear estratégicamente las TI con la empresa, buscando que se produzcan los beneficios esperados a nivel empresarial. El artículo presenta el resultado de la revisión de algunas de las normas, estándares o marcos de referencia que se han desarrollado para apoyar el gobierno de TI en las organizaciones, haciendo énfasis en el denominado Control Objetives for Information and Related Technology - COBIT. Posteriormente se diserta sobre la importancia de la auditoría informática en las organizaciones y se reflexiona sobre el papel de la auditoría informática en la evaluación del gobierno de TI en las empresas y cómo COBIT, dada su naturaleza y estructura, se convierte en el referente ideal para realizar un proceso de auditoría informática, particularmente auditoría de gobierno de TI.



**Palabras clave:** Gobierno de TI, COBIT, Auditoría de Sistemas de Información



## ABSTRACT

One of the critical aspects in the Information Technologies (IT) function in organizations is the IT governance, that focuses on strategically aligns IT with the company, seeking to occur the expected benefits at the business level. The paper presents some reviews of the rules, standards or frameworks that have been developed to support IT governance in organizations, with an emphasis on the so-called Control Objectives for Information and Related Technology COBIT. Subsequently, it discusses the importance of Information Technologies audit in organizations and reflects on the role of audit in the assessment of IT governance in organizations, aspects that must be considered, and as COBIT, given its nature and structure, becomes the ideal reference for an IT audit process, particularly audit of IT governance.



**Keywords**: IT governance, COBIT, Information Systems Audit.

## INTRODUCCIÓN

El Gobierno de Tecnologías de Información - TI - hace referencia a la gestión y el control de todos los aspectos relacionados con las tecnologías de información, requeridos para apoyar el logro de los objetivos empresariales y agregar valor a la organización. Su propósito es alinear los objetivos, planes y operaciones de TI con los de la organización. El gobierno de Tecnologías de Información integra un conjunto de buenas prácticas para su gestión, que permita justificar su inversión, que asegure a la organización administrar estratégicamente la información, que se aprovechen al máximo las oportunidades que brinde el entorno y que se obtengan ventajas competitivas.

Para apoyar el gobierno de TI existe un conjunto de normas y estándares que reúnen buenas prácticas y ofrecen alternativas de solución a diversos problemas de gestión al respecto. Algunas de las más reconocidas y aceptadas son: Information Technology Infrastructure Library - ITIL, Control Objectives for Information and Related Technology - COBIT, normas ISO/IEC 20000, Project Management Body of Knowledge - PMBOK y Capability Maturity Model Integration - CMMI.

La auditoría informática o auditoría de sistemas de información, según la definición propuesta por la Asociación de Auditoría y Control de Sistemas de Información (Information Systems Audit and Control Association - ISACA), consiste en la "revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados y las interfaces correspondientes".

Una de las áreas de la auditoría de Sistemas de Información es la auditoría del gobierno de TI. El estándar de auditoría para gobierno de TI propuesto por ISACA (2004a) define que los deberes que establece esta norma para el auditor son: a) revisar y evaluar si la función de los Sistemas de Información - SI - está alineada con la misión, visión, valores, objetivos y estrategias de la organización, b) revisar si la función de los SI tiene una declaración en cuanto al desempeño esperado por la empresa y evaluar su cumplimiento, c) revisar y evaluar la eficacia de los recursos de SI y el desempeño de los procesos administrativos, d) revisar y evaluar el cumplimiento de los requisitos legales, ambientales y de calidad de la información, así como de los requisitos fiduciarios y de seguridad, e) utilizar un enfoque basado en riesgos para evaluar la función de SI, f) revisar y evaluar el ambiente de control de la organización y g) revisar y evaluar los riesgos que pueden afectar de manera adversa el entorno de SI que apoyan los procesos del negocio.

COBIT es un marco de trabajo para control de Gobierno de TI, define un conjunto de dominios, procesos y objetivos de control y presenta las actividades en una estructura manejable y lógica. Además, reúne una serie de lecciones aprendidas, experiencias, buenas prácticas e indicadores para el control. Tiene cuatro características principales: orientado a negocios, orientado a procesos, basado en controles y dirigido por mediciones. Esto lo convierte en el marco de referencia ideal para un proceso integral de auditoría de sistemas de información, particularmente la auditoría de gobierno de TI.

## GOBIERNO DE TECNOLOGÍAS DE INFORMACIÓN (GOBIERNO DE TI)

Las Tecnologías de Información y Comunicaciones han avanzado dramáticamente y se ha masificado su uso en las organizaciones y en todas las áreas del quehacer humano, estas tecnologías ofrecen actualmente grandes capacidades de procesamiento y almacenamiento de información, inimaginables hace muy poco tiempo. Las organizaciones hacen grandes inversiones en Tecnologías de Información con el propósito de ser más eficientes, seguras y apoyar el logro de sus objetivos. La importancia de las TI en las organizaciones es inobjetable, sin embargo, el panorama es inquietante, debido a la existencia de factores como: sistemas que no funcionan adecuadamente, interrupción de servicios, deficiente atención a los usuarios, pérdidas de tiempo y de productividad de los usuarios causadas por problemas de la infraestructura tecnológica, conflictos entre el área de TI con las demás áreas de la organización y muchas veces los objetivos del área de Tecnologías de Información no están alineados con los objetivos del negocio. Se ha detectado que las causas de todos estos problemas radican principalmente en la gestión de la función informática, es decir es un asunto de gobierno de TI (Aenor, 2009).

Según lo que plantea el Information Technologies Governance Institute - ITGI (2007), el Gobierno de TI hace referencia a la gestión y el control de todo lo relacionado con Tecnologías de Información, para apoyar el logro de los objetivos empresariales y agregar valor a la organización, este se enfoca en alinear las TI y el negocio. De otra parte, Palao (2010) afirma que el gobierno de TI hace parte integral del gobierno corporativo, integra un conjunto de buenas prácticas para la gestión tecnológica que permitan justificar la inversión en Tecnologías de Información y define el cómo la organización debe administrar estratégicamente la información y el conocimiento para aprovechar las oportunidades que genere el entorno, obteniendo ventajas competitivas.

Adicionalmente Muñoz y Ulloa (2011) plantean que el gran reto del Gobierno de TI es alinear los objetivos estratégicos del área de Tecnologías de Información con los de la organización, esto no es solo un problema de planeación estratégica, esta área está sometida a presiones internas para que responda a las necesidades cambiantes de los usuarios y apoye efectivamente a la empresa en el logro de sus objetivos, de la misma forma existen factores externos relacionados con normas gubernamentales que se deben cumplir, la aparición de nuevas tecnologías y aspectos comerciales relacionados con los proveedores de tecnología.

ITGI (2007), define que las actividades de gobierno de TI se enfocan fundamentalmente a cinco grandes áreas, estas se muestran esquemáticamente en la Figura 1 y se describen a continuación:

- *Alineación Estratégica*: Alinear los objetivos, planes y operaciones de Tecnologías de Información con los de la organización.
- *Entrega de Valor*: Asegurar que las Tecnologías de Información genere los beneficios prometidos, enfocándose en optimizar costos y ofrecer el valor intrínseco de las TI.
- *Administración de Recursos*: Inversión óptima en recursos de Tecnologías de Información y gestión de los mismos.
- *Administración de Riesgos*: Análisis y gestión de riesgos, determinar las responsabilidades de la gestión de riesgos en la organización.
- *Medición del Desempeño*: Monitoreo de TI en aspectos como el uso de recursos, desempeño de los procesos, entrega de servicios y desarrollo de proyectos.


*Figura 1. Áreas del Gobierno de TI Fuente: IT Governance Institute (ITGI, 2007)*

**Normas, estándares y marcos de trabajo para el gobierno de TI**

Paralelamente con el gran avance tecnológico en el sector Tecnologías de Información, se han desarrollado un conjunto de normas, estándares, marcos de trabajo, mejores prácticas y metodologías

que ayudan a las organizaciones a gestionar estos entornos tecnológicos, cada vez más complejos pero a su vez más esenciales, que ofrecen alternativas de solución a los problemas de gestión de TI encontrados, en síntesis, que sirven de marco de referencia para el gobierno de TI en las organizaciones. A continuación se mencionan algunas de las más reconocidas y aceptadas en el ámbito de las Tecnologías de Información.

**Information Technology Infrastructure Library - ITIL**

Es un marco de trabajo público que provee un conjunto de conceptos y mejores prácticas para la gestión de servicios de las TI. Concreta un modelo de procesos muy amplio que abarca desde la definición de la estrategia hasta la gestión de la infraestructura. La gran aceptación de ITIL se debe a la calidad de sus buenas prácticas y a la flexibilidad para adaptarlas a las necesidades particulares de las organizaciones. La versión ITIL v3 que apareció en 2007 hace mayor énfasis en la integración de las Tecnologías de Información con el negocio y se estructura en torno al ciclo de creación de servicios, consta de 5 volúmenes: Service Strategy, Service Design, Service Transition, Service Operation y Continual Service Improvement (itSMF, 2007), (OGC, 2007).

**Control Objectives for Information and Related Technology - COBIT**

Es un marco de trabajo para control de Gobierno de TI. Define dominios, procesos y objetivos de control; presenta las actividades en una estructura manejable y lógica. Es un conjunto de mejores prácticas e indicadores para el control y auditoría de los sistemas de información. Fue creado por ISACA, es promovido por ITGI y ha extendiendo su alcance hacia las métricas de las Tecnologías de Información y las disciplinas de gobierno de las TI (ITGI, 2007).

**Las Normas ISO/IEC 20000**

Definen los procesos y las actividades esenciales para que las áreas de TI puedan prestar un servicio eficiente y alineado con las necesidades de la empresa u organización. Están construidas sobre la base del modelo ITIL, son pautas específicas para la gestión de los servicios que ofrecen las áreas o los proveedores de Tecnologías de Información. Estas normas articulan el proceso de prestación de los servicios articulados sobre un sistema de gestión del servicio (Aenor, 2009). Es un estándar reconocido mundialmente para certificar la Gestión de Servicios de TI de las organizaciones (ISO/IEC, 2005).

**Project Management Body of Knowledge PMBOK**

Es un marco para la gestión de proyectos de desarrollo de software, describe los procesos, herramientas y técnicas utilizados para dirigir un proyecto y obtener un resultado exitoso. Proporciona y promueve un vocabulario común para analizar, escribir y aplicar conceptos de la dirección de proyectos.

El conocimiento contenido en esta norma evolucionó a partir de las buenas prácticas reconocidas por profesionales del área, quienes contribuyeron eficazmente a su desarrollo. El Project Management Institute (PMI) considera la norma como una referencia fundamental en el ámbito de la dirección de proyectos para sus certificaciones y programas de desarrollo profesional (PMI, 2008).

**Capability Maturity Model Integration CMMI**

Es el modelo más aceptado para la medición de la madurez de los procesos de gestión en la construcción de aplicaciones. CMMI es una evolución de estándar inicial CMM, que fue desarrollado por el Software Engineering Institute - SEI. Inicialmente fue diseñado para procesos de desarrollo de software, pero actualmente se ha ampliado, proporcionando un modelo completo de evaluación de la madurez de las actividades de desarrollo de software de una organización. Es un modelo estructurado que incluye un gran conjunto de buenas prácticas útiles para optimizar las actividades propias de una organización de TI. La última versión crea un nuevo modelo CMMI for Services, que se superpone en gran medida con el ámbito central de ITIL (Chrissis, Konrad y Shrum, 2011).

Cabe anotar que no existe un único marco o estándar universal que cubra exhaustivamente todos los aspectos de las Tecnologías de Información. Algunos marcos enfatizan en el gobierno de TI, otros se orientan hacia la gestión de servicios de Tecnologías de Información, la seguridad informática, la gestión de proyectos informáticos y la medición de la madurez de los procesos de construcción de software. Varios de estos marcos se complementan parcialmente, tienen elementos comunes o presentan enfoques distintos que dificultan su integración o aproximación con otros modelos. Sin embargo, en las versiones recientes de algunos de estos marcos, como en el caso de COBIT, se han realizado esfuerzos para armonizar su estructura con otros marcos, que permita que éstos se utilicen complementariamente y apoyen eficazmente los procesos de Gobierno de TI. Se han desarrollado documentos adicionales que relacionan aspectos específicos de un marco de trabajo con otros marcos, con el propósito de alinearlos para que su aplicación en las organizaciones genere mayores beneficios.

## COBIT, CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY

COBIT ofrece un conjunto de mejores prácticas e indicadores para el control y auditoría de los sistemas de información, tiene cuatro características principales que son: orientado a negocios, orientado a procesos, basado en controles y dirigido por mediciones (ITGI, 2007).

**Orientado a Negocios**

Es una guía integral para la dirección y los responsables de los procesos de negocio en la organización, así como para los proveedores de servicios, usuarios y auditores de TI. Su principio básico es

obtener la información que la organización requiere para alcanzar sus objetivos, identificar necesidades de inversión en Tecnologías de Información, administrar y controlar dichas inversiones (ISACA, 2007).

Para satisfacer los objetivos del negocio, la información suministrada debe cumplir con los siguientes criterios: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento (legalidad) y confiabilidad.

En cuanto a los recursos de TI, COBIT define básicamente los siguientes:

- *Las Aplicaciones*, los sistemas automáticos y sistemas manuales para el procesamiento de la información.
- *La Información* en todas sus formas, que es generada por los sistemas de información a partir del procesamiento de los datos de entrada.
- *La Infraestructura*, tecnología de hardware y software (sistemas operativos, sistemas de gestión de bases de datos, redes, herramientas de desarrollo, entre otros) y las instalaciones físicas donde se encuentran.
- *Las Personas* involucradas en las diferentes actividades de la función informática de la organización.

**Orientado a Procesos**

El marco de trabajo define las actividades del área de Tecnologías de Información en un modelo genérico de dominios, procesos y objetivos de control. La versión COBIT 4.1 define 4 dominios, 34 procesos y un total de 220 objetivos de control (ITGI, 2007). Los dominios son:

- *Planear y Organizar (PO).* Proporciona la orientación para la entrega de soluciones y la entrega de servicio. Tiene como objetivos formular estrategias y tácticas; identificar cómo el área TI contribuye al negocio y a planear, comunicar y gestionar la realización de la visión estratégica. Consta de 10 procesos.
- *Adquirir e Implementar (AI).* Entrega las soluciones y las convierte en servicios. Sus objetivos son identificar, desarrollar, adquirir, implementar, e integrar soluciones de TI, el manejo de los cambios y mantenimiento de sistemas existentes. Está conformado por 7 procesos.
- *Entregar y Dar Soporte (DS).* Recibe las soluciones y las hace utilizables por los usuarios finales. Sus objetivos son la entrega real de los servicios requeridos y la gestión de la seguridad, continuidad, datos y facilidades operacionales. Consta de 13 procesos.
- *Monitorear y Evaluar (ME).* Monitorea todos los procesos para asegurar la dirección correcta. Tiene como objetivos la gestión del desempeño, el monitoreo y control interno, verificar el cumplimiento de regulaciones y los aspectos relacionados con el gobierno de TI. Lo conforman 4 procesos.

**Basado en Controles**

El concepto de control hace referencia a las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para ofrecer una seguridad razonable y que los objetivos de negocio se alcanzarán, así como que los eventos no deseados serán prevenidos o detectados y corregidos oportunamente.

Un objetivo de control define el resultado o propósito que se desea alcanzar mediante la implementación de procedimientos específicos en la función informática de las organizaciones. Los objetivos están definidos con una fuerte orientación a los procesos de negocio. COBIT 4.1 define en total 220 objetivos de control de Tecnologías de Información para el proceso general, para cada uno de los 34 procesos específicos y además incluye los controles de aplicación. Estos objetivos de control proporcionan un conjunto completo de requerimientos de alto nivel a considerar por la gerencia, para un control efectivo de cada proceso de TI en la organización.

Dado que los objetivos de control de Tecnologías de Información están organizados por procesos de las mismas, el marco de trabajo establece vínculos claros entre los requerimientos de gobierno de TI, procesos y controles. Los procesos de TI de COBIT tiene un objetivo de control de alto nivel y varios objetivos de control detallados. En conjunto los objetivos de control representan las características de un proceso bien administrado (ITGI, 2007; ISACA, 2011).

**Dirigido por Mediciones**

Las organizaciones deben tener la capacidad de medir su desempeño con el propósito de saber dónde se encuentran y dónde se requieren mejoras e implementar un conjunto de herramientas gerenciales que permitan monitorear estas mejoras. COBIT atiende estos aspectos mediante modelos de madurez, medición del desempeño y metas de actividades (ISACA, 2007).

Los modelos de madurez facilitan la evaluación y comparación (benchmarking) para la identificación de las mejoras necesarias en la capacidad. Un modelo de madurez para la administración y el control de los procesos de las Tecnologías de Información es un método de evaluación de la organización, que parte desde un nivel de no-existente (0) hasta un nivel de optimizado (5). Estos niveles definen perfiles de procesos de TI que una empresa reconocería como descripciones de estados posibles, actuales y futuros. Los modelos de madurez COBIT permitirán a la dirección identificar aspectos como: dónde se encuentra hoy la organización, el estatus actual de la industria, dónde desea estar la organización en el futuro y el crecimiento requerido entre “como es ahora” y “como será”.

La medición del desempeño se hace con metas y métricas de Tecnologías de Información. COBIT define tres niveles de metas: las que establecen lo que el negocio espera del área de TI; las que determinan qué deben generar los procesos para dar soporte a los objetivos del área; las métricas que miden

el desempeño de los procesos para estimar la probabilidad de alcanzar las metas propuestas. Hay dos tipos de métricas básicas: las medidas de resultado, que indican cuando las metas se han cumplido y los indicadores de desempeño, que muestran si es probable conseguir las metas (ISACA, 2011).

**Otras iniciativas relacionadas con COBIT**

Se han desarrollado otras iniciativas basadas COBIT las cuales se enfocan en apoyar un aspecto particular de Tecnologías de Información y que se pueden utilizar como referentes adicionales en un proceso de gobierno de TI. Una de estas iniciativas es Val IT implementado por ITGI, este producto busca responder a la necesidad que tienen las organizaciones de optimizar las inversiones en Tecnologías de Información y asegurar el valor agregado que estas deben generar. Val IT complementa a COBIT desde el punto de vista financiero y de negocio y es una herramienta de ayuda para los responsables de la entrega de valor a partir de TI (ITGI, 2006). Para una mejor comprensión de esta herramienta, ITGI con la colaboración de un grupo de especialistas, desarrolló un caso de estudio completo donde se hace una aplicación práctica de COBIT y Val IT en una entidad financiera (Bría, 2007).

Risk IT es otro marco de trabajo relacionado con COBIT, que reúne un conjunto de mejores prácticas para la gestión eficaz de riesgos de Tecnologías de Información en las instituciones. Se soporta en una colección de principios, guías, procesos y directrices de gestión asociados con riesgos de TI. Una organización que utiliza COBIT como marco de gobierno de TI, puede utilizar Risk IT como complemento para optimizar la estimación y administración de los riesgos asociados a la función informática. Dado que la gestión de riesgos de Tecnologías de Información es una práctica global, Risk IT está destinado una amplia población objetivo que incluye el nivel directivo de la organización, los responsables de las funciones de TI, los responsables de la gestión de riesgos empresariales en esta área y los stakeholders externos (ISACA, 2009).

El principio fundamental del marco de trabajo para el control COBIT, es que las organizaciones deben invertir en recursos de Tecnologías de Información, administrar y controlar eficazmente dichos recursos para soportar los procesos, de tal forma que permitan obtener la información con los criterios de calidad requeridos para apoyar efectivamente el logro de los objetivos corporativos. Los recursos de Tecnologías de Información son utilizados por los procesos para alcanzar las metas del área, que respondan a los requerimientos del negocio. La Figura 2 muestra el cubo COBIT que representa esquemáticamente este principio y sintetiza el marco de trabajo. De una parte identifica los requerimientos de información del negocio como son la efectividad, eficiencia, integridad, disponibilidad, cumplimiento y confiabilidad y de otra, representa la estructura general del marco de trabajo en términos de dominios, procesos, actividades y objetivos de control. Adempás identifica los recursos básicos de Tecnologías de Información como son las aplicaciones, la información, la infraestructura y las personas.

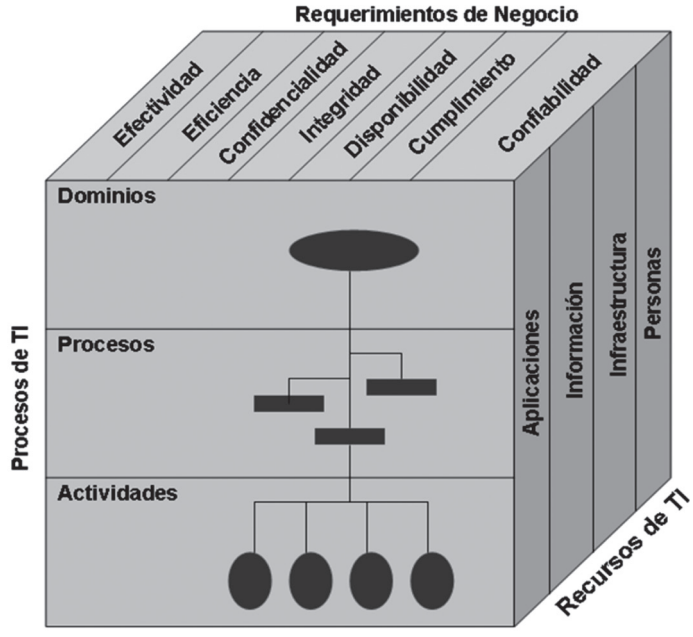


*Figura 2. Cubo COBIT Fuente: IT Governance Institute (ITGI, 2007)*

La versión COBIT 5 se encuentra en proceso de evaluación, esta versión es el producto del esfuerzo de ISACA para la próxima generación de guías sobre gobierno de TI, teniendo en cuenta las nuevas tendencias al respecto. COBIT 5 integra otras marcos referenciales entre ellos Val IT y Risk IT (ISACA, 2012).

Es importante que las organizaciones implementen los procesos de gobierno de TI utilizando para tal fin alguno de los marcos de trabajo disponibles. Debido al enfoque y la estructura del marco de trabajo para el control COBIT, este sería el más adecuado en la medida que incluye un tratamiento exhaustivo de todos los aspectos relacionados con Tecnologías de Información, vincula los objetivos con los requerimientos del negocio, organiza las actividades en un modelo de procesos, identifica los recursos fundamentales, define los aspectos de control que deben ser considerados y establece un conjunto de métricas y modelos de madurez para la medición y evaluación de los procesos pertinentes.

COBIT está dirigido a las grandes, pequeñas y medianas empresas, incluso se ha desarrollado una versión básica para éstas últimas, que también puede ser utilizado por empresas grandes que deseen implementar rápidamente el gobierno de TI. COBIT se puede aplicar complementariamente con otros marcos y con los productos adicionales desarrollados y que están basados o relacionados con el marco de trabajo.

## AUDITORÍA INFORMÁTICA

Según Hernández (1995), el concepto de auditoría hace referencia a un proceso formal de revisión y evaluación con el propósito de verificar el cumplimiento oportuno de las políticas y procedimientos de cada una de las áreas de la organización. Echenique (2001), define la auditoría como un examen crítico que se hace con el objeto de evaluar la eficacia y la eficiencia de una sección u organismo y determinar cursos alternativos de acción para mejorar la organización y lograr los objetivos propuestos.

Tradicionalmente en las organizaciones han existido auditorías como la financiera, administrativa, interna y de cumplimiento, entre otras. La incursión de las Tecnologías de Información en las organizaciones y su uso masivo, hizo necesario reconsiderar la forma como se llevan a cabo los procesos de auditoría y pensar en nuevas estrategias y herramientas de revisión y evaluación. Se habla entonces de la auditoría informática o auditoría de sistemas de información.

Inicialmente este nuevo tipo de auditoría se enfocaba exclusivamente al procesamiento electrónico de datos, a la evaluación de las aplicaciones informáticas, particularmente en lo relacionado con los controles de entrada de datos, controles de procesamiento y controles de salida. Actualmente su ámbito se ha expandido y abarca todos los aspectos relacionados con TI. Una definición más amplia, propuesta por ISACA (2011), plantea que la auditoría informática o auditoría de sistemas de información consiste en la revisión y evaluación de todos los aspectos, o parte de ellos, relacionados con los sistemas automáticos de procesamiento de la información, incluyendo los procedimientos no automáticos asociados con éstos y las interfaces correspondientes.

La definición anterior es bastante amplia e infiere la existencia de varias áreas o campos de la auditoría informática. Según Piattini y Del Peso (2001), algunas de estas áreas son:

- Auditoría del Gobierno de TI
- Auditoría de la Seguridad Informática
- Auditoría de Aplicaciones Informáticas
- Auditoría de Bases de Datos
- Auditoría de Redes de Computadores
- Auditoría del Desarrollo de Sistemas de Información

Estas áreas no son excluyentes entre sí y de hecho algunas se sobreponen en aspectos específicos. Un ejemplo de esto es lo relacionado con seguridad lógica, lo cual se tendrá en cuenta tanto en la auditoría de la seguridad informática como en la auditoría de aplicaciones, incluso en auditoría de redes

de computadores. Para el caso que nos ocupa nos concentraremos particularmente en la auditoría del gobierno de TI.

## EL ROL DE LA AUDITORÍA INFORMÁTICA PARA LA EVALUACIÓN DEL GOBIERNO DE TI

Uno de los campos de la auditoría informática tiene que ver con la revisión y evaluación de la gestión de la función informática en la organización. Cuando se habla de gestión necesariamente se hace referencia al gobierno de TI, que incluye los aspectos de la alineación estratégica de Tecnologías de Información con el negocio para apoyar el logro de los objetivos empresariales, el valor agregado que esta área da al negocio, la administración de recursos, la administración de riesgos y la medición del desempeño. El marco de referencia ideal para realizar la auditoría de gobierno de TI es el marco de trabajo para el control COBIT.

Los diferentes recursos que componen el marco mencionado se pueden utilizar como referentes de las mejores prácticas. COBIT establece que "…*es responsabilidad de la gerencia salvaguardar todos los activos de la empresa. Para descargar esta responsabilidad, así como para lograr sus expectativas, la gerencia debe establecer un adecuado sistema de control interno*". COBIT puede ser utilizado por la alta dirección de la empresa, la dirección de TI y por los auditores de SI. Su aplicación permite la comprensión de los objetivos del negocio, la comunicación de mejores prácticas y las recomendaciones con base en estándares de referencia generalmente aceptados (ISACA, 2004a). El marco de referencia incluye:

- *Objetivos de Control*. Declaraciones genéricas de alto nivel y detalladas sobre un nivel mínimo de buen control.
- *Prácticas de Control*. Razonamiento práctico y guías sobre cómo implementar los objetivos de control.
- *Directrices de Auditoría*. Guías para cada área de control orientadas hacia una mejor comprensión, cómo evaluar cada control, cómo evaluar el cumplimiento y la estimación del riesgo en caso de que los controles no se cumplan.
- *Directrices Gerenciales*. Guías sobre cómo evaluar y mejorar el desempeño del proceso de Tecnologías de Información, utilizando modelos de madurez, métricas y factores críticos de éxito. Proporcionan un marco de referencia administrativo, orientado hacia una permanente y proactiva autoevaluación del control.

La auditoría informática o auditoría de Sistemas de Información es una actividad especializada que requiere la definición de unos estándares que apliquen específicamente a este campo. Con el objetivo de contribuir con este propósito, ISACA (2004a) ha publicado una serie de documentos donde se definen un conjunto de estándares, directrices y procedimientos que se deben tener en cuenta en un proceso de auditoría de SI.

Los estándares definen requisitos obligatorios para la auditoría y establecen los deberes y el nivel mínimo de desempeño de los auditores, requeridos para cumplir cabalmente con sus responsabilidades profesionales, establecidas en el código de ética profesional de ISACA (ISACA, 2004b). Las directrices proporcionan guías sobre la aplicación de los estándares de auditoría de SI.

Los procedimientos presentan ejemplos que podría seguir un auditor durante la ejecución de una auditoría de SI, proporcionan información sobre cómo cumplir con los estándares al ejecutar la auditoría, pero no establecen los requisitos correspondientes. Tanto las directrices como los procedimientos tienen como objetivo principal proveer mayor información sobre cómo cumplir con los Estándares de Auditoría de SI (ISACA, 2004a).

El estándar de auditoría para gobierno de TI propuesto por ISACA (2005) tiene como propósito ofrecer unos lineamientos que el auditor de Sistemas de Información debe tener en cuenta durante el proceso de auditoría. Los deberes que establece esta norma para el auditor, son los siguientes:

- Revisar y evaluar si la función de SI está alineada con la misión, visión, valores, objetivos y estrategias de la organización.
- Revisar si la función de SI tiene una declaración clara en cuanto al desempeño esperado por la empresa (eficacia y eficiencia) y evaluar su cumplimiento.
- Revisar y evaluar la eficacia de los recursos de SI y el desempeño de los procesos administrativos.
- Revisar y evaluar el cumplimiento de los requisitos legales, fiduciarios, de seguridad, ambientales y de calidad de la información.
- Utilizar un enfoque basado en riesgos para evaluar la función de SI.
- Revisar y evaluar el ambiente de control de la organización.
- Revisar y evaluar los riesgos que pueden afectar de manera adversa el entorno de SI. La auditoría debe asistir a la organización identificando y evaluando las exposiciones significativas al riesgo y contribuir al mejoramiento de la administración de riesgos y los sistemas de control.

Este estándar también establece unas recomendaciones adicionales y determina una serie de documentos sobre directrices y procedimientos que el auditor debe utilizar como guía para desarrollar su trabajo. Como documentos de soporte fundamental están las Directrices Gerenciales y el Marco de Referencia COBIT (ISACA, 2005).

Un proceso integral de auditoría informática debería estar soportado en una metodología robusta que incluya aspectos de planeación y ejecución. Se propone el desarrollo de una metodología integral de auditoría de gobierno TI, soportada en el marco de trabajo COBIT, que incluya las Directrices Gerenciales y el Marco Referencial que contiene todos los objetivos de control de los dominios y procesos allí establecidos. También se utilizarían como referencias adicionales las iniciativas Val IT y Risk IT, así como los documentos sobre gobernabilidad de TI publicados por el IT Governance Institute, y los estándares, directrices y procedimientos de auditoría de gobierno de TI definidos en los documentos de ISACA, particularmente los relacionados con la independencia organizacional de la auditoría de SI, ética y competencias profesionales del auditor informático, planeación, evaluación de riesgos, proceso, evidencias y el informe de auditoría de SI.

## CONCLUSIONES

Conjuntamente con los avances de las tecnologías de información y las comunicaciones, se han implementado una serie de normas, estándares y marcos de trabajo que tienen como objetivos apoyar eficazmente a las organizaciones en el gobierno de TI.

Para las organizaciones, además de contar con la infraestructura tecnológica necesaria y el recurso humano requerido, es indispensable disponer de un proceso de gobierno de TI que permita alinear estratégicamente los objetivos del área de Tecnologías de la Información con los objetivos corporativos, para generar el valor agregado que se espera obtener con las inversiones en este campo.

La auditoría de gobierno de TI busca revisar y evaluar integralmente si su función está alineada con la organización, con el desempeño de sus funciones, con el uso eficaz y eficiente de los recursos, con el cumplimiento de los requisitos legales, ambientales y de calidad, y con el manejo adecuado de los riesgos asociados a las TI y el ambiente de control en la organización.

COBIT reúne lecciones aprendidas, experiencias y buenas prácticas de gobierno de TI, está orientado a la organización y sus procesos, se basa en controles y es dirigido por mediciones. Por estas razones y complementándolo con otras iniciativas como Val IT y Risk IT, se consolida como el marco de referencia ideal para un proceso integral de auditoría de sistemas de información.

## REFERENCIAS BIBLIOGRÁFICAS


AENOR Asociación Española de Normalización y Certificación. (2009). *ISO/IEC 20000. Guía completa de aplicación para la gestión de los servicios de tecnologías de información*. Madrid: AENORediciones. pp. 15-53.

Bría, R. (2007). Gobierno de TI utilizando COBIT® y Val IT™: TIBO – Caso de Estudio (2da ed.). USA: ITGI.

Chrissis, M. B., Konrad, M. y Shrum, S. (2011). CMMI for development: Guidelines for process integration and product improvement (3ra ed.). Upper Saddle River, NJ: Addison-Wesley Professional.

Echenique, J. A. (2001). Auditoría en Informática (2da ed.). México: Edit. McGraw-Hill.

Hernández, E. (1995). Auditoría en informática un enfoque metodológico (1ra ed.). México: Edit. CECSA.

ISACA Information Systems Audit and Control Association. (2004a). Norma de auditoría de SI. Estatuto de auditoría. Documento No. S1. Recuperado el 7 de junio de 2012 de http://www.isaca.org/Knowledge-Center/Standards/Documents/Standards-IT-Spanish-S1.pdf

ISACA Information Systems Audit and Control Association. (2004b). Norma de auditoría de SI. Ética y normas profesionales. Documento No. S3. Recuperado el 7 de junio de 2012 de http://www.isaca.org/Knowledge-Center/Standards/Documents/Standards-IT-Spanish-S3.pdf

ISACA Information Systems Audit and Control Association. (2005). Estandar de Auditoría de SI. Gobernabilidad de TI. Documento S10. Recuperado el 7 de junio de 2012 de http://www.isaca.org/Knowledge-Center/Standards/Documents/Standards-IT-Spanish-S10.pdf

ISACA Information Systems Audit and Control Association. (2007). COBIT Quickstart. (2da ed.). Recuperado el 12 de junio de 2012 de http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-Quickstart-2nd-Edition.aspx

ISACA Information Systems Audit and Control Association. (2009). Risk IT. Marco de Riesgos de TI. Recuperado el 12 de junio de 2012 de http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-framework-spanish.pdf

ISACA Information Systems Audit and Control Association. (2011). COBIT 4.1: Framework for IT Governance and Control. Recuperado el 7 de mayo de 2011 de http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

ISACA Information Systems Audit and Control Association. (2012). COBIT5: A Business Framework for the Governance and Management of Enterprise IT. Recuperado el 27 de junio de 2012 de http://www.isaca.org/COBIT/Pages/default.aspx

ISO/IEC. (2005). ISO/IEC 20000-1:2005 Information technology -- Service management -- Part 1: Specification. USA.

ITGI IT Governance Institute. (2007). COBIT 4.1 Marco de Trabajo, Objetivos de Control Directrices Gerenciales y Modelos de Madurez. Recuperado el 7 de mayo de 2012 de http://www.isaca.org/Knowledge-Center/COBIT/Documents/COBIT4.1spanish.pdf

ITGI IT Governance Institute. (2006). Enterprise Value: Governance of IT Investments, The Val IT Framework. Recuperado el 8 de mayo de 2012 de http://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Pages/Val-IT1.aspx

ITSMF The IT Service Management Forum. (2007). An Introductory Overview of ITIL v3.UK: IT Service Management Forum Limited.

Muñoz, I. L. y Ulloa G. (2011). Gobierno de TI – Estado del Arte. En: Revista Sistemas y Telemática, 3(17), 23-53. Cali: Universidad ICESI.

OGC Office of Government Commerce. (2007). ITIL v3 Service operation book. London: The Stationery Office.

Palao, M. (2010). Reflexión sobre el Estado del Arte del Buen Gobierno TIC. Bogotá: ISACA.

Piattini, M. y Del Peso, E. (2001). Auditoría Informática. Un enfoque práctico (2da ed). México: Alfaomega Grupo Editor. México.

PMI Project Management Institute. (2008). Guía de los fundamentos para la dirección de proyectos-Guía del PMBOK (4ta ed.). Pennsylvania: PMI Inc.