Artículo de revisión

Gobierno de TI – Estado del arte

IT Governance – State of the art

Ingrid Lucía Muñoz Periñán, MsC.
PMP- Lead Auditor ISO 27001 - Cobit Certificate.
Docente en Gerencia de proyectos y seguridad de la información
Universidad Icesi. Cali (Colombia)
ilmunoz@gmail.com

Gonzalo Ulloa Villegas. Ph.D
Decano - Facultad de Ingeniería
Universidad Icesi. Cali (Colombia)
gulloa@icesi.edu.co

Fecha de recepción: Mayo 10 de 2011
Fecha de aceptación: Junio 10 de 2011

Palabras clave

Gobierno corporativo, COSO, Cobit, ISO/IEC 38500,Calder-Moir, ISO 27002, ITIL, ISO/IEC 20000, Gobierno de TI.

Keywords

Corporate governance, COSO, Cobit, ISO/IEC 38500, Calder-Moir, ISO 27002, ITIL, ISO/IEC 20000 IT governance.

Colciencias tipo 3

Resumen

El artículo hace un balance del estado del arte sobre los conceptos que relacionan el gobierno corporativo y el gobierno de TI. Hace una revisión histórica de la evolución de los marcos de referencia y las normas asociadas hasta llegar a la actualidad. Ayuda al lector a tener un entendimiento general del tema del Gobierno de Tecnologías de Información y le permite elaborar un concepto propio del mismo, para de esta forma, utilizar los marcos de control, los estándares y las regulaciones, como apoyo para una debida implementación de estos en su organización. Esto le permitirá alinear las TI con los objetivos del gobierno corporativo.

Abstract

This paper evaluates the state of the art and concepts that links corporate governance and IT governance. Makes an historical review of the frameworks' evolution and related standards up to now. Helps the reader to have a general understanding of the IT Governance topics and lets develop our own concept of it. Helps to use further the control frameworks, standards and regulations for a proper implementation of these in his organization to align IT with the corporate governance.

I. Introducción

Las empresas y los gobiernos dependen hoy en día de las tecnologías de información (TI) para su funcionamiento y desarrollo. Hacen enormes esfuerzos e inversiones en TI con el objetivo de ser más eficientes, más seguras, cumplir con su misión y con los aspectos claves de su planeación estratégica. Infortunadamente muchas de ellas funcionan como silos, aisladas unas de otras, las divisiones no se comunican y los esfuerzos de un área son desconocidos o entorpecidos por otras. Una de las áreas claramente afectada por este fenómeno es el área de TI, que muchas veces tiene objetivos claros pero estos no están necesariamente alineados con los objetivos del negocio. Otro problema que frecuentemente se adiciona al anterior ocurre por la pobre alineación estratégica entre ambos, ya que los ritmos de desarrollo del área de TI y los ritmos del negocio son diferentes (Ross & Weil, 2002).

Por la naturaleza misma de la tecnología, en muchos casos otras dependencias declaran su ignorancia en el tema, lo que contribuye a aislar aún más el área de TI.

El gran problema del gobierno de TI es alinear los objetivos estratégicos de TI con los de la organización. Pareciera este solo un problema de planeación estratégica pero no es necesariamente solo este aspecto el que debe tenerse en cuenta; las áreas de TI están sometidas a diferentes presiones pues deben apoyar la marcha del negocio, soportar además presiones regulatorias, técnicas y comerciales. La respuesta rápida a estas presiones puede llevar fácilmente a perder el alineamiento con la organización y dedicarse a resolver problemas puntuales (Weill, Subramani & Broadbent, 2002).

Las TI se ven en muchas organizaciones como un gasto o un mal necesario y debido al carácter demasiado técnico de sus directores el área de TI es incapaz de demostrar el valor agregado que presta a la organización, al punto que si este no fuera demasiado evidente, la unidad desaparecería.

Por otro lado aparecen nuevas tecnologías y procesos de negocio que hacen que las TI deban responder a otras necesidades u operar bajo otros esquemas, como por ejemplo los procesos de tercerización de TI a todos los niveles, la computación en la nube (Cloud Computing), étc. Estas nuevas tendencias marcan nuevos retos para el desarrollo de los procesos y servicios que debe proveer la unidad de TI dentro de una empresa. No importa cuál sea el modelo usado, las TI deben estar presentes para el apoyo de la organización.

Producir el concepto de gobierno de TI y todo lo relacionado con él para lograr la alineación e integración con el gobierno corporativo ha sido un gran esfuerzo de la academia, firmas consultoras, asociaciones de investigación, organizaciones de estándares y entidades reguladoras.

Entre otros esfuerzos se puede mencionar los que realizan entidades especializadas como: ISACA (*Information Systems Audit and Control Association*), ITGI (*IT Governance*

Institute) ITSMF (*IT Service Management Forum*) IT GOVUK (*IT Governance UK*) y ECGI (*European Corporate Governance Institute*) y organizaciones desarrolladoras de estándares como: ISO/IEC (*International Organization for Standardization / International Electrotechnical Commission*) y BSI (*The British Standards Institution*). Los aportes de las entidades reguladoras, que vienen emitiendo reportes de absoluto interés y vigencia como son: el Informe Coso –*Internal Control - Integrated Framework*– (Committee on Sponsoring Organizations of the Treadway Commission [COSO], 1992); el Informe Cadbury –*Report of the Committee on the Financial Aspects of Corporate Governance*– (Cadbury, 1992); el Código Olivencia de Buen Gobierno –*El Gobierno de las Sociedades Cotizadas*– (Olivencia, 1998); el Informe Turnbull –*Report of the Committee on the Financial Aspects of Corporate Governance*– (The Financial Reporting Council [FRC], 2005); el Informe Winter –*Report of the High Level Group of Company Experts on a Modern Regulatory Framework for Company Law in Europe*– (Winter, 2002); el Informe Aldama –*Informe de la Comisión Especial para el fomento de la transparencia y seguridad en los mercados y en las sociedades cotizadas*– (Aldama y Miñon, 2003); y *El Company Law and Corporate Governance* (European Commission, 2011). *Principios de la OCDE para el Gobierno de las sociedades* (Organización para la Cooperación y el Desarrollo Económicos [OCDE], 1999); y *Enhancing Corporate Governance in Banking Organizations del Bank for International Settlements* (Basel Committee on banking supervision, 2005 &2006) cuyos reportes han tenido origen, entre otros, por los escándalos de Enron (Bryce, 2002; McLean & Elkind, 2005) y Worldcom (Jeter, 2003) donde en últimas se han producido fraudes en la información que presentan las corporaciones, a los accionistas y al mundo, aprovechando la falta de control en las tecnologías de información.

Este artículo muestra una evolución partiendo desde el significado de *Gobernanza*, Gobierno corporativo, para llegar a una definición de gobierno de TI con sus principios, objetivos, áreas de enfoque y la necesidad de tener un marco de control para su implantación. Se presentan algunos marcos de control y diferentes marcos de referencia y estándares con los cuales se desarrolla la forma como se puede realizar la implementación de un gobierno de TI, siguiendo estas recomendaciones (ITGI, 2007). Finalmente se presenta el análisis de los conceptos y algunas conclusiones.

II. Conceptos y definición de gobierno corporativo

Antes de poder pasar a una definición más formal de gobierno de TI, es necesario comprender a que se refiere el gobierno en la empresa. Según la Real Academia Española (RAE) gobernanza se define como "arte o manera de gobernar que se propone como objetivo el logro de un desarrollo económico, social e institucional duradero, promoviendo un sano equilibrio entre el Estado, la sociedad civil y el mercado de la economía (RAE, 2005) y Gobierno es el elemento que resulta de organizar a las personas con el propósito de alcanzar los objetivos de la comunidad, de entre los cuales

destacan la protección del territorio, la seguridad de sus habitantes y su desarrollo integral.

Según el ITGI (Carrillo, 2009) el gobierno corporativo es un conjunto de responsabilidades y prácticas ejecutadas por la junta directiva y la gerencia ejecutiva, teniendo como objetivos:

- Proveer dirección estratégica
- Asegurar el logro de los objetivos
- Establecer que los riesgos se administran adecuadamente
- Verificar que los recursos de la empresa se utilizan responsablemente

Según la OCDE (2004) el gobierno corporativo es el sistema por el cual las sociedades son dirigidas y controladas. La estructura del gobierno corporativo especifica la distribución de los derechos y responsabilidades entre los diferentes participantes de la sociedad, tales como el directorio, los gerentes, los accionistas y otros agentes económicos que mantengan algún interés en la empresa. El gobierno corporativo también provee la estructura a través de la cual se establecen los objetivos de la empresa, los medios para alcanzar estos objetivos, así como la forma de hacer un seguimiento a su desempeño.

La Corporación Andina de Fomento CAF en su marco regulatorio Lineamientos para un Código Andino de Gobierno Corporativo, que contiene un conjunto de buenas prácticas y medidas regulatorias para mejorar las prácticas empresariales en los países que integran la región (Bolivia, Colombia, Ecuador, Perú y Venezuela), define el gobierno corporativo como el conjunto de prácticas, formales e informales, que gobiernan las relaciones entre los administradores y todos aquellos que invierten recursos en la empresa, principalmente accionistas y acreedores. Es obvio que unas buenas prácticas de gobierno corporativo garantizan un mejor uso de los recursos en las empresas, contribuyen a una mayor transparencia contable y mitigan los problemas de información asimétrica que caracterizan a los mercados financieros. En estas circunstancias, unas buenas prácticas de gobierno corporativo son la clave para el acceso de las empresas a los mercados de capital (CAF/IAAG, 2005).

La OCDE (1999) propuso un conjunto de principios de buen gobierno que fueron respaldados por los ministros de la OCDE. Desde entonces han sido una referencia para los responsables políticos, inversionistas, empresarios y otros actores interesados en promover iniciativas de carácter legislativo y reglamentario, tanto en países miembros de la OCDE como en los no-miembros (OCDE, 2004).

En 2001, después de las crisis de Enron (Bryce, 2002) y WorldCom (Jeter, 2003) se hizo un análisis en Inglaterra por la Federación Internacional de Contables (Carrillo, 2009) y se concluyó que un buen gobierno corporativo no garantiza el éxito, si la ejecución no es correcta.

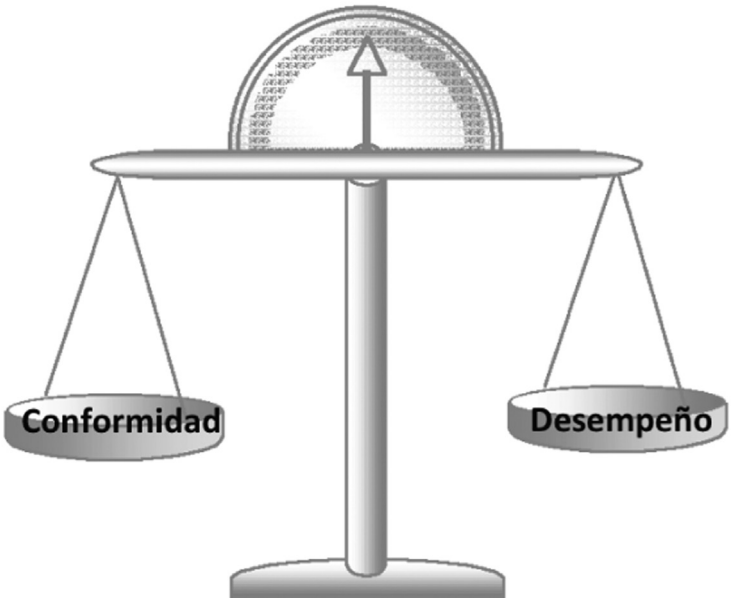

Figura 1. El gobierno empresarial requiere un balance entre desempeño y conformidad

A partir de este estudio se ha ido extendiendo el concepto de gobierno empresarial; se indica que el gobierno corporativo garantiza la dimensión de conformidad, pero se concluye que no basta garantizar la conformidad sino que se requiere de la ejecución y que el gobierno empresarial tiene dos dimensiones:

- Gobierno corporativo, cuya misión es la conformidad
- Gobierno de negocio, cuya misión es el desempeño

La conformidad se adhiere a la legislación, políticas y requerimientos de auditoría y el desempeño exige que las tecnologías de información se involucren en la organización. Ambas deben guardar un equilibrio, como se ilustra en la Figura 1.

El gobierno corporativo y el gobierno de negocio están íntimamente relacionados, dado que el corporativo entrega informes de un ciclo económico y se rinde cuentas sobre esa información, se hace necesario controlar la ejecución de todos los procesos que generan esta información, que es el gobierno de negocio, donde aparecen los activos de la empresa y dentro de esos activos está la tecnología de información, es decir, el concepto de gobierno de TI está dentro del gobierno de negocio, que es una dimensión del gobierno empresarial y esto lleva años atrás, es decir, no viene desde el marco de referencia de Cobit. La Figura 2 muestra las dos dimensiones del gobierno empresarial: gobierno corporativo y gobierno de negocio.

Gobierno de la Empresa	
Gobierno Corporativo	Gobierno del Negocio
Procesos de Conformidad	Procesos de Ejecución
Presidente/CEO	Planeación Estratégica y Alineamiento
Directores no Ejecutivos	Toma de Decisiones Estratégicas
Comité de Auditoria	Gestión Estratégica del Riesgo
Comité remuneraciones	Cuadro Integral de Mando
Gestión del Riesgo	Sistemas Estratégicos de la Empresa
Auditoría Interna	Mejora Continua
Responsabilidad Seguridad	**Creación del Valor Utilización de Recursos**

Figura 2. Gobierno de la empresa de una manera más amplia, con dos dimensiones: gobierno corporativo y gobierno del negocio (Weill & Ross, 2004)

Esto se resume en el modelo de Peter Weill y Jeane W. Ross, marco que permite asociar el gobierno empresarial, con el gobierno de TI (Ver Figura 3).

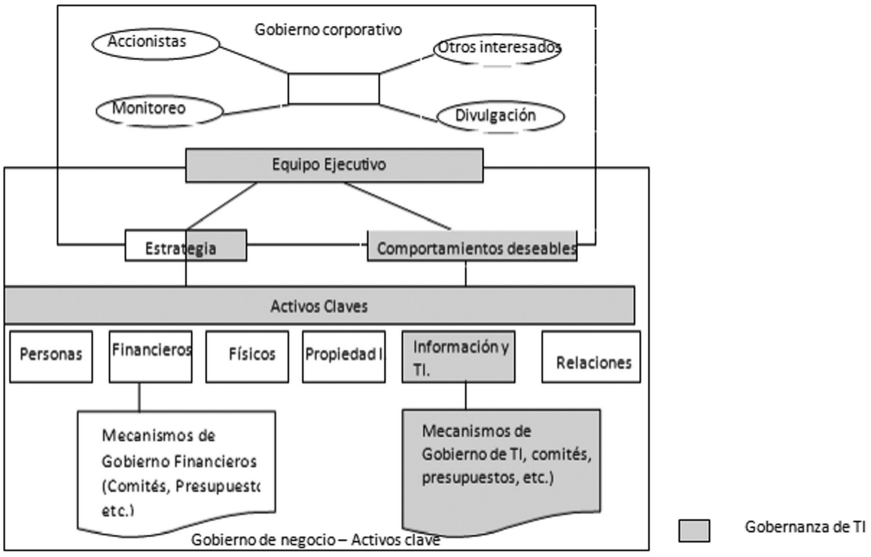

Figura 3. Adaptación del modelo de Peter Weill y Jeanne W. Ross (Weill & Ross, 2004)

III. Conceptos de gobierno de TI y su definición, principios, áreas de enfoque, interesados

El gobierno de TI, como se explicó, hace parte del gobierno empresarial. Se define como la estructura de relaciones y procesos para dirigir y controlar la empresa hacia el logro de sus objetivos, por medio de agregar valor, al tiempo que se obtiene un balance entre el riesgo y el retorno sobre las TI y sus procesos.

El gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que TI en la empresa soporta los objetivos del negocio. Facilita que la empresa aproveche al máximo su información, maximiza los beneficios, capitaliza las oportunidades y gana ventajas competitivas (Palao, 2010).

Son la Junta Directiva y la Gerencia Ejecutiva las responsables del gobierno de TI.

Según el IT Governance Institute, el gobierno de TI tiene cuatro principios fundamentales (ITGI, 2007):

- Dirigir y controlar
- Responsabilidad
- Rendición de cuentas
- Actividades

El gobierno de TI tiene interesados internos y externos, con distintas preocupaciones, a las que el gobierno de TI tiene que darles respuesta. Entre los interesados internos se pueden mencionar al gerente de TI, la junta directiva y los gerentes ejecutivos y de negocios, el gerente de riesgo y cumplimiento y el auditor de TI. Los interesados externos son fundamentalmente los auditores externos, los clientes, los reguladores y los proveedores, cada uno con preguntas e inquietudes particulares.

Otro concepto de gobierno de TI se plantea como: definir los derechos de decisión y el marco de rendición de cuentas para alentar una conducta deseable en el uso de TI (Weill & Ross, 2004).

También podría definirse como: "Es el uso eficiente de los recursos de TI para apoyar el cumplimiento de los objetivos del negocio (ITGI, 2008a)".

Así como un buen gobierno corporativo es elemental para asegurar y alinear las decisiones claves de negocio, con la visión y estrategia de la compañía, un buen gobierno de TI es crítico para asegurar que las decisiones de TI estén alineadas a los objetivos de la compañía (Garbarino, 2010).

Las actividades del gobierno de TI se pueden agrupar en cinco áreas de enfoque que son ilustradas en la Figura 4 (ITGI, 2007):

- Alineamiento estratégico
- Entrega de valor
- Administración de riesgos
- Administración de recursos
- Medición del desempeño

Figura 4. Áreas de enfoque del gobierno de TI (ITGI, 2007)

Según el informe IT *Governance Broad Briefing* del ITGI (2003) una de las claves para el éxito del desempeño de TI es la inversión óptima, utilización y asignación de recursos de TI (personas, aplicaciones, tecnología, instalaciones, datos) en el servicio de las necesidades de la empresa. La mayoría de las empresas no pueden maximizar la eficiencia de sus activos de TI y optimizar los costos relacionados con estos activos. Además, el mayor desafío en los últimos años ha sido saber dónde y cómo externalizar –y luego saber cómo administrar los servicios externalizados– de manera que proporcionen los valores prometidos a un precio aceptable.

Según el mismo informe, el *Balanced Scorecard* traduce la estrategia en acción para lograr los objetivos con un sistema de medición del rendimiento que va más allá de mediciones convencionales, la contabilidad, la medición de las relaciones y los activos basados en el conocimiento necesario para competir en la era de la información: la orientación al cliente, el proceso, la eficiencia y la capacidad de aprender y crecer (Kaplan & Norton, 1996).

El uso del cuadro de mando integral de TI presentado en el informe de Alec Cram (2007) es uno de los medios más eficaces para ayudar a la junta directiva y de gestión a lograr la alineación de TI y de negocio. El objetivo es la creación de un vehículo para la gestión de informes a la junta para fomentar el consenso entre los principales interesados acerca de los objetivos estratégicos de TI, para demostrar la eficacia y el valor agregado de las TI y lo que se comunicará acerca de su rendimiento, riesgos y posibilidades (Ver Tabla 1).

Alineamiento estratégico	Se enfoca en asegurar el enlace de los planes del negocio y de TI; en definir, mantener y validar la proposición de valor de TI y en alinear las operaciones de TI con las operaciones de la empresa. Según el informe IT Governance Broad Briefing del ITGI (ITGI, 2003) la pregunta clave es si la inversión de una empresa de TI está en armonía con sus objetivos estratégicos (la intención, la estrategia actual y objetivos de la empresa) y por lo tanto la construcción de las capacidades necesarias para ofrecer un valor empresarial. Este estado de la armonía que se conoce como "la alineación." Es complejo, multifacético y nunca del todo logrado.
Entrega de valor	Se refiere a ejecutar la proposición de valor a través de todo el ciclo de entrega, asegurando que TI entrega los beneficios acordados alineados con la estrategia, concentrándose en la optimización de costos, y demostrando el valor intrínseco de TI. Según el informe IT Governance Broad Briefing del ITGI (ITGI, 2003) dice que la entrega de valor de las TI se traduce en entregar a tiempo y dentro del presupuesto. "El valor de IT está en el ojo del espectador".
Administración de riesgos	Requiere: - Conciencia de riesgo por parte de los directores superiores de la empresa. - Un claro entendimiento del apetito de riesgo de la empresa. - Un entendimiento de los requerimientos de cumplimiento. - Transparencia sobre los riesgos significativos de la empresa. - Implementar las responsabilidades de la administración de riesgos dentro de la organización.
Administración de recursos	Se refiere a la inversión óptima y a la adecuada administración de los recursos críticos de TI tales como: aplicaciones, información, infraestructura, datos.
Medición del desempeño	Da seguimiento y supervisa la estrategia de implementación, la finalización de proyectos, el desempeño de procesos y la entrega de servicio. Si no hay forma de medir y evaluar las actividades de TI, no es posible gobernarlas ni asegurar el alineamiento, la entrega de valor, la administración de riesgos y el uso efectivo de los recursos.

Tabla 1. Áreas de enfoque de gobierno de TI ITGI (ITGI, 2007)

Se plantean cuatro perspectivas según el IT BSC (Cram, 2007) cada una diseñada para responder a una pregunta sobre la forma de hacer negocios de la empresa, de tal manera que el gobierno de TI y el negocio se alineen (Figura 5).

Perspectiva	
Financiera	Proveer buen retorno sobre la inversión en las inversiones del negocio habilitadas por las TI
	Administrar los riesgos del negocio relacionados con TI
	Incrementar el gobierno corporativo y la transparencia
Cliente	Mejorar orientación y servicio al cliente
	Ofrecer productos y servicios competitivos
	Establecer la disponibilidad y continuidad del servicio
	Crear agilidad en responder a requerimientos de cambio en el negocio
	Obtener optimización de costos para entrega de servicios
	Obtener información útil/confiable para toma de decisiones estratégicas
Interna	Mejorar/mantener la funcionalidad del proceso de negocio
	Reducir costos de proceso
	Proveer cumplimiento con leyes externas, regulaciones y contratos
	Proveer cumplimiento con políticas internas
	Administrar los cambios del negocio
	Mejorar/mantener productividad operativa y del personal
Aprendizaje y crecimiento	Administrar innovación del negocio y de productos
	Adquirir/mantener personal motivado y con destrezas

Figura 5. Perspectivas según el BSC para alinear el negocio con TI

El valor, el riesgo y el control constituyen la esencia del gobierno de TI (ITGI, 2007). El gobierno de TI efectivo, debe responder tres preguntas:

» ¿Qué decisiones se deben tomar a fin de asegurar una efectiva administración y uso de TI?
» ¿Quién debe tomar esas decisiones?
» ¿Cómo se tomarán y monitorearán tales decisiones?

IV. Descripción de un marco de control, propósitos y características

Las organizaciones no pueden hacer una entrega efectiva de lo que demandan los requerimientos del negocio y de gobierno sin adoptar e implementar un marco de control y de gobierno con los siguientes propósitos (ITGI, 2008b):

» Enlazarse con los requerimientos del negocio.
» Hacer que el desempeño sea transparente a la luz de estos requerimientos.
» Organizar las actividades de TI dentro de un modelo de procesos generalmente aceptado.
» Identificar los principales recursos a controlar.
» Definir los objetivos de control de la administración a ser considerados.

Lo anterior significa que para poder implantar gobierno de TI en una organización es absolutamente necesario basarse en un marco de control que muestre el "Qué" se debe hacer y dé unos estándares para realizar el "Cómo". Esto ofrece alrededor de un 50% y lo demás debe desarrollarlo la misma organización.

Un marco de control debe tener las siguientes características, recomendadas por ISACA para cualquier marco de referencia de control (ITGI, 2007):

» Brindar un fuerte enfoque en el negocio.
» Definir un lenguaje común.
» Ayudar a alcanzar requerimientos regulatorios.
» Contar con la aceptación general entre la organización.
» Asegurar la orientación a procesos.

Brindar un fuerte enfoque en el negocio. La medición del desempeño de TI debe enfocarse sobre su contribución para hacer posible y expandir la estrategia de negocios.

Definir un lenguaje común. Construye seguridad y confianza entre los participantes, para tener a todos sintonizados en el mismo canal, al definir términos críticos y brindar un glosario que aclare alguna duda existente.

Ayudar a alcanzar requerimientos regulatorios. Permite dar respuesta a los controles internos necesarios para evitar un mal manejo de la información generada para el gobierno corporativo.

Contar con la aceptación general entre la organización. Permite ser probado y globalmente aceptado para incrementar la contribución de TI al éxito de la organización.

Asegurar la orientación a procesos. Aprovechando la propiedad de los procesos estos están definidos, asignados y aceptados y la organización está en mejor capacidad para mantener el control durante los períodos de cambios rápidos o crisis organizacionales.

V. Marcos de gobierno de TI

A lo largo de la literatura se encuentra un número importante de marcos diseñados para dar soporte a la implementación de distintos aspectos del gobierno de TI; cada uno de ellos enfoca las prioridades en distintos aspectos del gobierno de TI, haciéndolos, en buena medida, complementarios. Sin embargo se pueden revisar tres marcos principales:

- La versión de Cobit©4.1 del IT Governance Institute (ITGI, 2007) que llamaremos simplemente Cobit en adelante, acompañada de ValIT™ del IT Governance Institute (Val IT, 2008) y Risk IT™ del IT Governance Institute (RiskIT, 2009).
- La norma ISO que trata sobre el gobierno corporativo: ISO 38500 (ISO/IEC, 2008)
- El modelo de Calder-Moir (Calder, 2008).

A continuación se presentan cada uno de estos modelos de forma resumida.

A. Cobit©4.1 (Control Objectives for Information and related Technology)

El marco de trabajo de Cobit fue creado por el ITGI (ITGI, 2007) y ha evolucionado hasta lo que hoy se conoce como Cobit 4.1, 2007, vigente hasta la fecha del presente artículo.

La misión de Cobit es investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado y aceptado internacionalmente, para la adopción, por parte de las empresas y el uso diario, por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento (ITGI, 2007).

El marco de trabajo Cobit se creó con las siguientes características principales: orientado a negocios, orientado a procesos, basado en controles e impulsado por mediciones.

1. Orientado al negocio

La orientación a negocios es el tema principal de Cobit. Está diseñado para ser utilizado no sólo por proveedores de servicios, usuarios y auditores de TI, sino también –y principalmente– como guía integral para la gerencia y para los dueños de los procesos

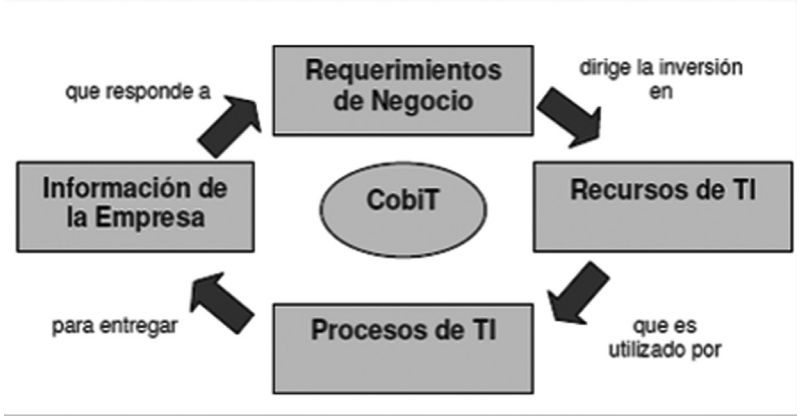

Figura 6. Principio de Cobit (ITGI, 2007)

de negocio. Como marco de control y gobierno para TI se enfoca en dos áreas clave:

- Brindar la información requerida para apoyar los objetivos y requerimientos del negocio.
- Tratar la información como el resultado de la aplicación combinada de los recursos de TI relacionados que necesitan ser administrador por los procesos de TI.

El marco de trabajo Cobit se basa en el principio mostrado en la Figura 6.

Este marco describe cómo los procesos de TI entregan la información que el negocio necesita para alcanzar sus objetivos. Para controlar esta entrega, Cobit brinda tres componentes claves. Cada uno forma una dimensión del cubo de Cobit:

- Requerimientos del negocio o criterios de información (7)
- Recursos de TI (4)
- Procesos de TI (34)

a. Criterios de información

Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en Cobit como requerimientos de información del negocio. Existen siete requerimientos de negocio o criterios de información: cuatro requerimientos fiduciarios y tres de seguridad.

Los requerimientos fiduciarios: efectividad, eficiencia, confiabilidad y cumplimiento, son tomados directamente de las mejores prácticas recomendadas por COSO (COSO, 1992; PriceWaterhouseCoopers, 2009) Marco de Referencia Integrado – Control Interno, el marco de referencia de control ampliamente aceptado para gobierno corporativo y para la administración de riesgos, así como de marcos compatibles

similares. La confiabilidad de información, sin embargo, fue ampliada para incluir toda la información (no solo la financiera). Los requerimientos de seguridad son: confidencialidad, integridad y disponibilidad.

b. Recursos de TI

Los recursos de TI identificados en Cobit incluyen: aplicaciones, información, infraestructura y personas, definidas así:

- Las aplicaciones, que incluyen tanto sistemas de usuarios automatizados como procedimientos manuales que procesan información.
- La información, es decir los datos en todas sus formas, de entrada, procesados y generados por los sistemas de información, en cualquier forma en que sean utilizados por el negocio.
- La infraestructura, esto es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.
- Las personas, el equipo humano requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Las personas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran.

c. Procesos de TI

Los treinta y cuatro procesos están distribuidos en los cuatro dominios presentados en la Figura 7, donde planear y organizar (PO) tiene diez procesos, adquirir e implementar (AI) 7, entregar y dar soporte (DS) 13, y monitorear y evaluar (ME) 4.

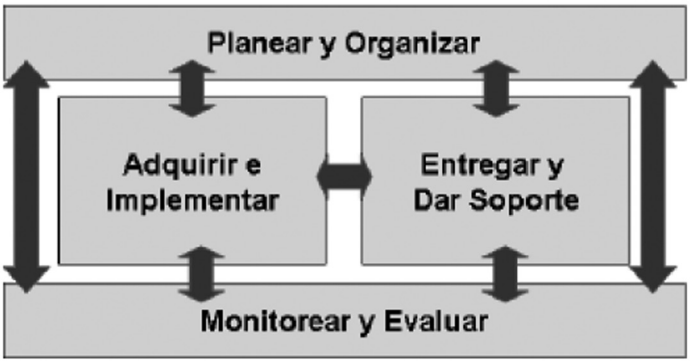

Figura 7. Procesos de Cobit (ITGI, 2007)

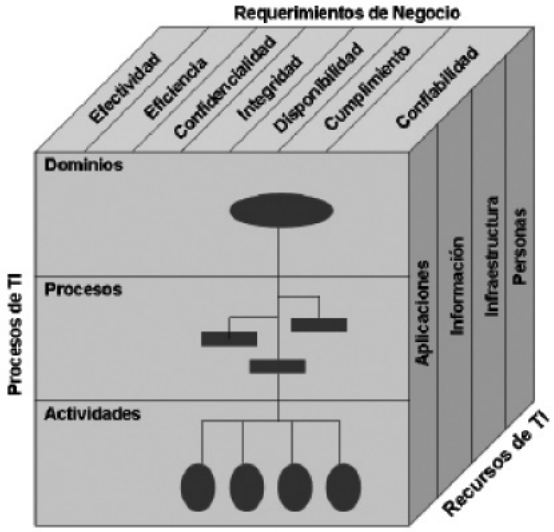

Figura 8. Cubo de Cobit (ITGI, 2007)

Los procesos son una serie de actividades que especifican lo que el negocio necesita para lograr sus objetivos. La entrega de información es controlada a través de 34 objetivos de control de alto nivel, uno para cada proceso y las actividades son acciones que se requieren para obtener resultados medibles.

Para resumir, los recursos de TI son manejados por procesos de TI para lograr metas de TI que respondan a los requerimientos del negocio. Este es el principio básico del marco de trabajo Cobit, como se ilustra en el cubo de Cobit (Figura 8).

Lo interesante de este modelo es que logra mapear las cuatro perspectivas del IT Balanced Scorecard (Kaplan & Norton, 1996): financiera, cliente, interna y aprendizaje y crecimiento (ver Figura 5) para un total de 17 perspectivas, con 28 objetivos de TI, con los treinta y cuatro procesos y los siete criterios de información o requerimientos de negocio, lo que de cierta manera permitiría una posible alineación estratégica.

Cobit es un marco de referencia (framework) que además de lo anterior tiene más de 200 objetivos de control detallados y más de 3.000 prácticas de control, sin embargo las organizaciones necesitan utilizar sólo aquellos controles que requieran, por ejemplo, para cumplir con la Conformidad en SOX (Sarbanes-Oxley, 2002) o Basilea II (Basel Commitee on banking supervision, 2005) entre otros.

Cobit ha sido alineado con estándares que apoyan el gobierno de TI como por ejemplo ISO 17799 –hoy ISO 27002–, ITIL y también para conformidad con SOX. Se pueden encontrar documentos de referencia como son:

» IT Control Objectives for Sarbanex-Oxley: The Role IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition (ITGI, 2006)
» Alineando-Cobit-4.1,-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa-v2.7 (ITGI, 2008b).

2. Orientado a Procesos

El marco de trabajo de Cobit proporciona un modelo de procesos de referencia y un lenguaje común para que todos en la empresa visualicen y administren las actividades de TI. Ver Figura 8 (ITGI, 2007).

3. Basado en controles

Cobit define objetivos de control para los 34 procesos, así como para el proceso general y los controles de aplicación. Cada uno de los procesos de TI de Cobit tiene un objetivo de control de alto nivel y varios objetivos de control detallados. Como un todo, representan las características de un proceso bien administrado.

4. Guiado por la medición

Las empresas deben medir dónde se encuentran y dónde se requieren mejoras, e implementar un juego de herramientas gerenciales para monitorear dicha mejora. Cobit atiende estos temas a través de: modelos de madurez, metas y mediciones de desempeño para los procesos de TI y metas de actividades.

» Modelos de madurez, que facilitan la evaluación por medio de benchmarking y la identificación de las mejoras necesarias en la capacidad.
» Metas y mediciones de desempeño para los procesos de TI, que demuestran cómo los procesos satisfacen las necesidades del negocio y de TI, y cómo se usan para medir el desempeño de los procesos internos basados en los principios de un marcador de puntuación balanceado (*Balanced Scorecard*).
» Metas de actividades, que facilitan el desempeño efectivo de los procesos.

Cobit se ha ido engrosando con otros marcos de referencia para complementar temas de agregar valor con ValIT y riesgos de TI con Risk IT. ValIT es un marco de referencia que constituye una extensión y complemento de Cobit, que proporciona un marco de control global para el gobierno de TI (Val IT, 2008). En concreto, Val IT se centra en la decisión de invertir –¿estamos haciendo lo correcto? Y en la realización de beneficios –¿estamos obteniendo beneficios? mientras que Cobit se enfoca en la ejecución –¿lo estamos haciendo correctamente? –¿Lo estamos logrando bien? Risk IT, por su parte, proporciona un marco integral para el control y la gestión de las organizaciones de soluciones y servicios de TI y aunque Cobit establece las mejores prácticas para la gestión de riesgos y proporciona un conjunto de controles para mitigar los riesgos de TI, Risk IT establece las mejores prácticas con el fin de fijar un marco para las

organizaciones para identificar, gobernar y administrar los riesgos asociados a su negocio. El marco de riesgos de TI es utilizado para ayudar a implementar el gobierno de TI a las organizaciones que lo han adoptado o planean hacerlo (RiskIT, 2009).

B. ISO 38500 Corporate governance of information technology

Se publicó en junio de 2008. Se basa en la norma australiana AS8015:2005. Es la primera de una serie de estándares sobre el gobierno de TI (ISO/IEC, 2008). Su objetivo es proporcionar un marco de principios para que la dirección de las organizaciones lo utilicen al evaluar, dirigir y monitorear el uso de las tecnologías de la información (Bosch, 2008). Está alineada con los principios de gobierno corporativo recogidos en el Informe Cadbury (Cadbury, 1992) y en los principios de gobierno corporativo de la OCDE (OCDE, 1999). La norma define seis principios de un buen gobierno corporativo de TI:

- Responsabilidad
- Estrategia
- Adquisición
- Rendimiento
- Conformidad
- Conducta humana

El modelo de gobierno de TI presentado por el estándar posiciona tres tareas áreas: evaluar, dirigir y controlar, como la clave para dar dirección y controlar el desempeño de los roles de gestión en la conducción de la organización para la planificación, implementación y utilización operacional de TI (Toomey, 2009). La Figura 9 ilustra el modelo.

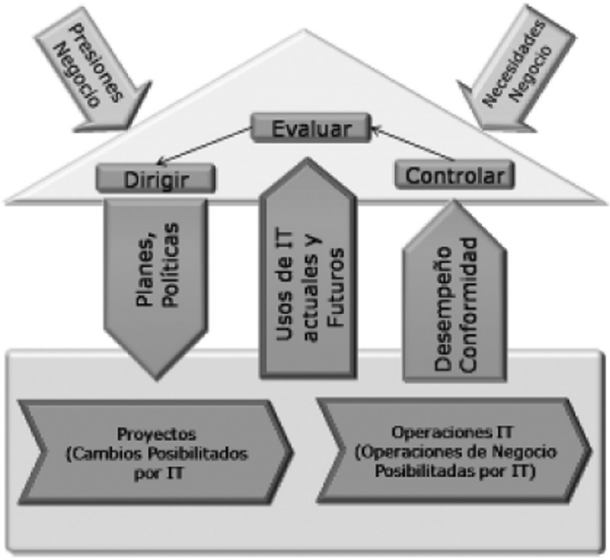

Figura 9. Modelo de gobierno IT ISO/IEC 38500 (Toomey, 2009)

El modelo puede ser rápidamente comprendido ya que el foco del gobierno de TI lleva directamente al modelo más básico de los negocios: Planear – Construir – Operar. Debe reconocerse que mientras este modelo es utilizado, a veces, por los especialistas de TI para explicar aspectos del ciclo de TI, es también ampliamente comprendido por los líderes de negocio y los educadores como el ciclo básico de la gestión de negocios. Y ese es el contexto en que se utiliza aquí. El ciclo de gestión de negocios se muestra en la Figura 10. (Toomey, 2009).

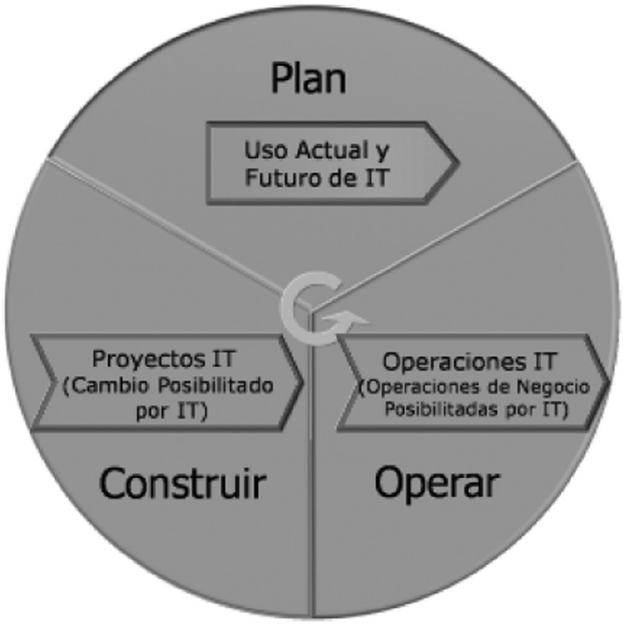

Figura 10. ISO 38500 Ciclo de negocios (Toomey, 2009)

La literatura indica que el ITGI a través de Cobit apoya al estándar mapeando para cada uno de sus seis principios, uno o más de los 34 procesos de Cobit, tal como se observa en la Figura 11.

C. El marco propuesto por Calder-Moir(2008)

Hay varios marcos de trabajo y estándares para el gobierno de TI, pero de alguna forma, ninguno provee el conjunto completo de gobierno de TI. Cuando estos marcos de trabajo y estándares son utilizados colectivamente, se vuelven muy confusos y obstruyen el propósito principal del gobierno de IT (Calder, 2008). Con muchos marcos de trabajo en existencia, ninguno es en sí mismo un marco de gobierno de IT completo.

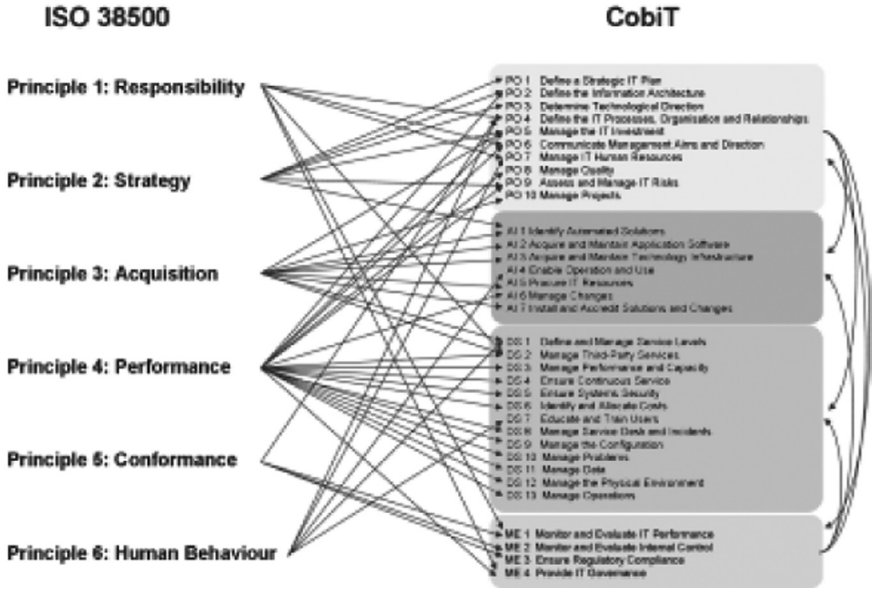

Figura 11. Alineación completa entre ISO 38500 y Cobit. (IT Governance Network, 2008)

El marco de gobierno de IT Calder-Moir es un metamodelo para coordinar modelos y organizar el gobierno de IT proveyendo guía estructural al enfocar el gobierno de IT. Al utilizar este modelo, la organización puede obtener el máximo beneficio de todos los otros marcos de trabajo y estándares (Garbarino, 2010). Es una herramienta sencilla para ayudar a las organizaciones a implementar la norma ISO / IEC 38500 para el gobierno de TI en el mundo real.

El marco de trabajo Calder-Moir para el gobierno de TI no es una solución más sino una forma de organizar los asuntos del gobierno y además apoyar a la compañía, los ejecutivos y los profesionales. Coloca las herramientas de TI en el contexto de un proceso de extremo a extremo y provee un punto común de referencia para la discusión de los distintos aspectos de la dirección y el desempeño de TI. El marco de trabajo consta de seis segmentos, cada uno de los cuales representa un paso de un proceso de extremo a extremo, que comienza con la estrategia de negocios y termina con el soporte operativo de TI para la obtención de valor empresarial frente a esa estrategia, leyéndose como si fuese un reloj a las 9:00am siguiendo los segmentos en sentido horario a través del proceso de extremo a extremo. Cada segmento está dividido en tres capas. La capa interna representa la junta directiva que dirige, evalúa y monitorea el soporte tecnológico para la empresa. La capa intermedia representa la dirección ejecutiva, que es responsable de administrar las actividades que llevan a cabo el proceso de extremo a extremo. La capa exterior representa los profesionales de TI que usan herramientas y metodologías probadas, a fin de planear,

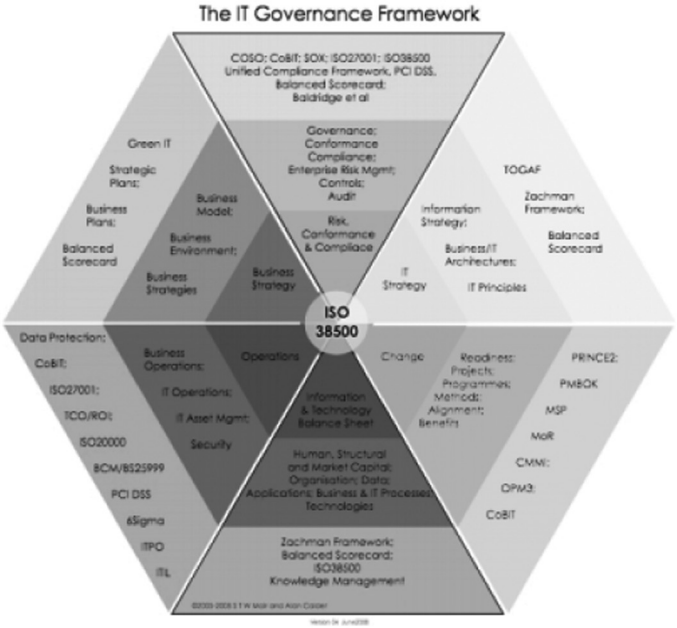

Figura 12. Modelo de Gobierno de TI Calder-Moir (Calder, 2008)

diseñar y realizar el soporte de TI para la empresa. La Figura 12 presenta el modelo propuesto (Calder, 2008).

La junta directiva provee dirección sobre las estrategias de dirección y de negocios de la organización. Estas son analizadas y diseñadas por la gerencia ejecutiva. Las estrategias tienen que operar dentro de uno o más gobiernos corporativos. Estas estrategias también operan dentro de un ambiente de riesgos y se decide cuáles controles serán los más apropiados. Los primeros dos segmentos del modelo describen el rumbo de la organización y los resultados deseados, los límites dentro de los cuales se debe operar y los controles que serán más apropiados dentro de esos contextos.

Una vez establecidas las estrategias de negocios, las regulaciones de gobierno, la evaluación de riesgos y los controles, TI trabaja con la empresa con el fin de desarrollar la arquitectura y los planes para cumplir con esos requerimientos. El resultado es un conjunto de propuestas y planes que describen cómo deberían verse la empresa e TI, el desempeño esperado, los cambios requeridos para alcanzar ese desempeño, y los recursos implicados. Los procesos de gobierno de TI verifican que las propuestas cumplan la estrategia de la empresa y los requerimientos del gobierno corporativo, incluyendo el manejo de riesgos y controles, y ayudan a la junta a evaluar si se justifica realizar esos planes y propuestas.

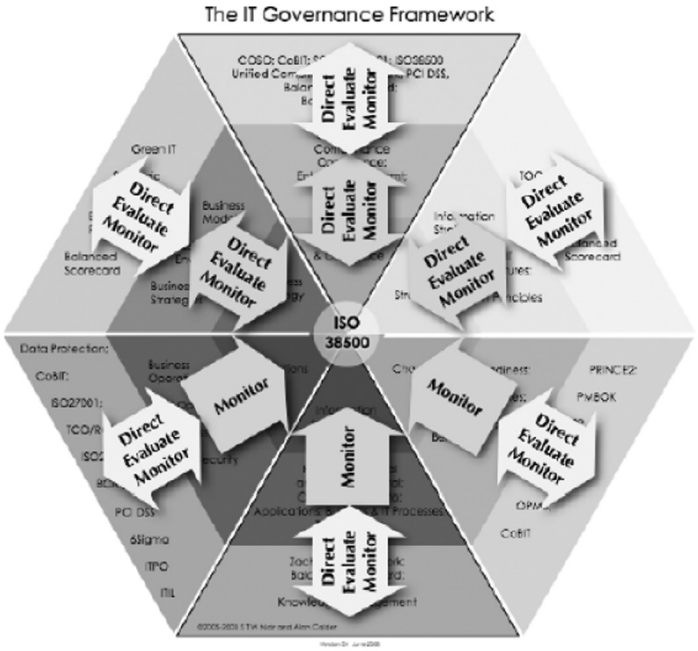

Figura 13. Evaluar, dirigir y monitorear en el modelo Calder-Moir (Calder, 2008)

Una vez que la junta aprueba los planes y propuestas, ellos pueden ser implementados a través de una serie de proyectos de cambio. Estos proyectos crean o actualizan las capacidades del negocio y de TI, lo que deben lograr en desempeño y los criterios de control establecidos durante las fases de planeación.

El modelo cumple con los tres principios claves de ISO/IEC 38500 como son evaluar, dirigir y monitorear, donde la junta: evalúa las condiciones del negocio, estrategias, límites y propuestas de TI; dirige para guiar la forma en que TI debería usarse, los principios de TI, la postura apropiada ante riesgos y las propuestas de inversión de TI; y monitorea todos los procesos del hexágono, estrategia de negocios, la empresa y los riesgos del entorno, límites, estrategia de TI, cambios, capacidades y operaciones (Figura 13).

A este modelo también le aplica el ciclo PHVA (planear, hacer, verificar, actuar) a alto nivel y a nivel detallado.

VI. Algunos estándares que apoyan el gobierno de TI

Los marcos de referencia con herramientas sólidas son esenciales para asegurar que los recursos de TI estén alineados con los objetivos del negocio y que los servicios y la información satisfagan los requisitos de calidad, financieros y de seguridad.

De acuerdo con los marcos de control presentados se observa la presencia de estándares que apoyan el gobierno de TI en alguno de ellos, los que permiten materializar el "cómo" para diferentes controles de TI. Se podrían mencionar a ISO 27001, ISO 27002, ISO 20000, BS 25999, ITIL, PCI DSS, PMBok (Project Management Institute, 2010) CMMI (Phillips, Gallagher, Richter, & Shrum, 2011; Chrissis, Konrad, & Shrum, 2011; Forrester, Buteau, & Shrum, 2011), entre otros. A continuación se presentan algunos de estos estándares: ITIL, ISO 20000 e ISO 27002.

A. ITIL v3

ITIL (Information Technology Infrastructure Library) es el conjunto de conceptos y mejores prácticas para la administración de servicios de TI (ITSM) para el desarrollo y las operaciones de TI establecido por la Oficina de Comercio del Gobierno del Reino Unido (OGC).

Originalmente se creó como una colección de libros, cada uno de los cuales cubría un área específica de prácticas de la administración de servicios de TI. ITIL se construyó utilizando el modelo de procesos de control y administración de las operaciones atribuido a Edwards Deming y a su ciclo Plan-Do-Check-Act –PDCA– (Arveson, 1998).

Publicado por primera vez en 1996 (v1) con más de treinta volúmenes, ITIL ha pasado por varios procesos de revisión, actualización y consolidación que lo llevaron a la versión 2 en 2000/2001 y a la versión actual (v3) publicada en mayo de 2007, que contiene cinco volúmenes:

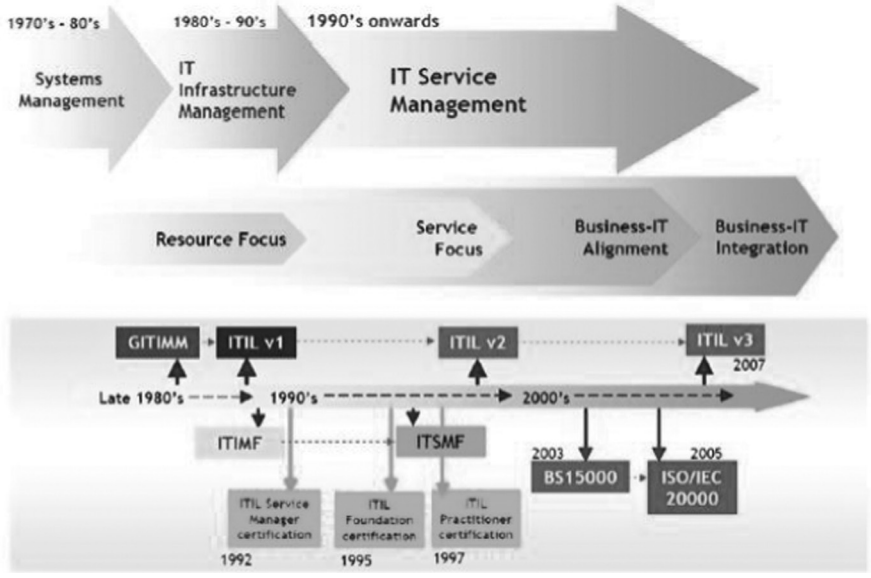

Figura 14. Evaluar, dirigir y monitorear en el modelo Calder-Moir (Calder, 2008)

- » ITIL Service Strategy (Iqbal & Nieves, 2007)
- » ITIL Service Design (Rudd & Lloyd, 2007)
- » ITIL Service Transition (Lacy & Macfarlane, 2007)
- » ITIL Service Operation (Office of Government Commerce , 2007)
- » ITIL Continual Service Improvement (Spalding, 2007)

Existen algunos marcos de gobierno de TI que referencian o tienen correlación con ITIL:

- » Cobit. ISACA ha editado un documento que permite mapear procesos de Cobit con sus correspondientes de ITIL (ITGI, 2008).
- » MOF (Microsoft Operations Framework). Basado en ITIL. Si bien es una implementación limitada de ITIL, Microsoft ha mapeado MOF como parte de la documentación del marco de referencia (Microsoft, 2010). Este marco certifica personas más no organizaciones.

B. ISO 20000

Es reconocido mundialmente como un estándar para certificar la Gestión de Servicios de TI de las Empresas y Organizaciones, ISO/IEC 20000 (International Organization for Standardization) e IEC (International Electrotechnical Commission) (ISO/IEC, 2005a) (ISO/IEC, 2005b).

La serie 20000 proviene de la adopción de la serie BS 15000 (BS15000 Associates Group, n.d) desarrollada por la entidad de normalización y certificación británica BSI (British Standard Institute) (Figura 15).

La norma ISO/IEC 20000 surge como respuesta a los requerimientos de clientes que no sólo querían que trabajaran con ellos consultores certificados, sino que requerían además que las empresas estuvieran certificadas.

La ISO/IEC 20000 es totalmente compatible con ITIL (*IT Infrastructure Library*) o guía de mejores prácticas para el proceso de GSTI. La diferencia es que el ITIL no es medible y puede ser implantado de muchas maneras, mientras que en la ISO/IEC 20000 las organizaciones deben ser auditadas y medidas frente a un conjunto establecido de requisitos.

La aparición de la serie ISO/IEC 20000 ha supuesto el primer sistema de gestión en servicio de TI certificable bajo una norma reconocida mundialmente. Hasta su aparición las organizaciones podían optar por aplicar el conjunto de mejoras prácticas dictadas por ITIL o certificar su gestión contra el estándar local británico BS 15000.

C. ISO/IEC 27002 (ISO/IEC, 2005d)

Es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000. Este estándar internacional establece las guías y principios

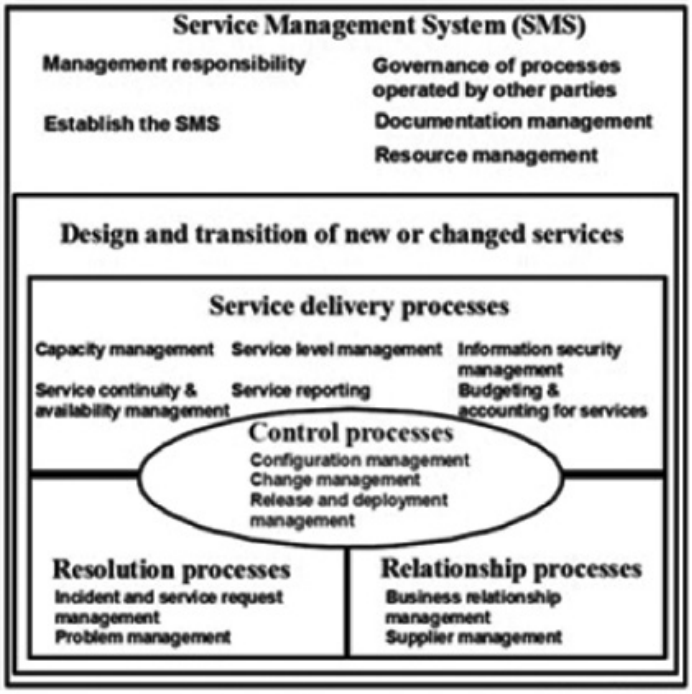

Figura 15. Esquema de ISO 20000 (ISO/IEC, 2005)

generarles para iniciar, implementar, mantener, y mejorar la gestión de seguridad de la información en una organización. Sus objetivos de control y controles son recomendados para cubrir los requerimientos de seguridad que han salido de una evaluación de riesgos (Calder, 2006).

Es una norma de buenas prácticas compuesta por once dominios, 39 objetivos de control y 133 controles para seguridad de la información. Los once dominios se presentan en la Figura 16.

Es el anexo A de la norma ISO/IEC 27001 (ISO/IEC, 2005c) que tiene como propósito brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI). Al igual que los demás estándares mencionados, el diseño e implementación del SGSI de una organización están influenciados por las necesidades y objetivos, los procesos empleados y el tamaño y estructura de la organización.

VII. Análisis de resultados

Revisando las iniciativas, estándares, informes y marcos referenciados para este artículo –algunos de ellos presentes desde 1992– se observa que durante casi dos décadas el tema

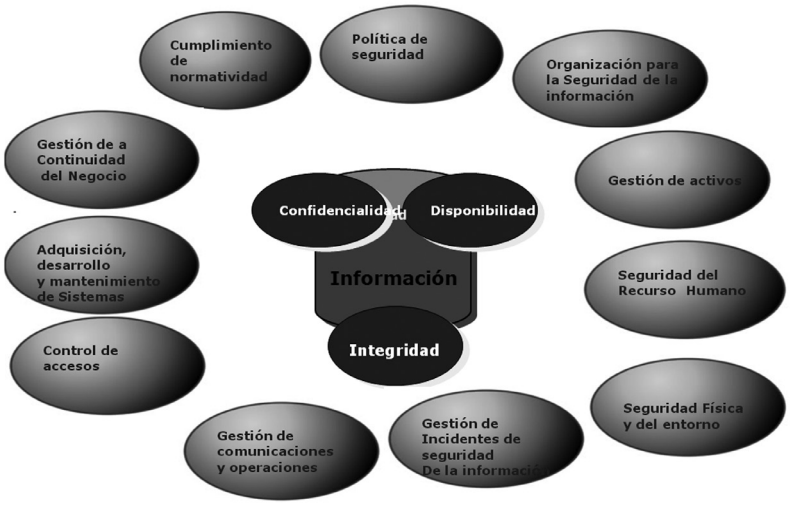

Figura 16. Dominios de la norma ISO/IEC 27002

de gobierno corporativo tiene relevancia, dada la necesidad de responder a los interesados clave en las organizaciones, como son: los accionistas, los acreedores, las entidades bancarias, entre otros, sobre la situación real de la organización y sus estados financieros.

Esta necesidad de presentar información confiable e íntegra, definitivamente dirige el tema a la necesidad actual del uso adecuado de las tecnologías de información, que son las que generan este tipo de información a las junta directivas, gerencias ejecutivas, accionistas, acreedores y el gobierno, entre otros.

El uso de las tecnologías de información que logre garantizar los requerimientos del negocio como son efectividad, eficiencia, confiabilidad, cumplimiento, disponibilidad, integridad y confidencialidad, requiere que se identifiquen con claridad los tipos de recursos o activos de la organización y unos procesos que se lleven a cabo para lograr la implementación de los controles que permitan cumplir con estos requerimientos del negocio.

Los procesos que se implementen deben ser dirigidos, planeados y controlados por las directivas y la dirección ejecutiva.

Los marcos de control presentados en el presente artículo: Cobit, ISO/IEC 38500, Calder-Moir tienen en común los siguientes puntos (Izquierdo, 2009):

» Responden al cómo administrar mejor las inversiones en TI y obtener valor a partir de su uso.

» Recomiendan siempre el alineamiento de las decisiones de TI con los objetivos de negocio.

- Buscan orientar sobre las mejores prácticas de dirección, evaluación y control de las TI en la organización.
- Se preocupan por el adecuado manejo de los recursos de TI, su desempeño y la administración del riesgo de TI.
- Como marcos de referencia, no proponen el uso de una herramienta específica, sino de un marco de actuación.

Los estándares y marcos de trabajo como ISO 20000, ITIL, ISO 27002, entre otros, pueden ser utilizados para implementar el "cómo" de un "qué" a partir de marcos de control como Cobit, ISO/IEC 38500 y Calder-Moir.

Al igual que los marcos de trabajo como ISO 20000, ITIL, ISO 27002, en la literatura se encuentran otros como el PMBok, CMMI, TOGAF, que también tienen un papel importante en el "cómo" durante la implementación de gobierno de TI.

Conclusiones

Hay varios marcos de gobierno de TI y varios estándares de apoyo para gestión de TI y las organizaciones requieren de seleccionar un marco de control, el que mejor se adapte a su organización, y apoyarse en diferentes estándares para ir desarrollando y aumentando la madurez del gobierno de TI en su organización.

No importa qué marco de control seleccione la organización. Cobit, ISO/IEC 38500 o Calder-Moir. Esta decisión le representa alrededor de un 50% de apoyo. El restante 50% se debe generar con actividad interna de implementación.

El gobierno de TI y su desarrollo en la organización son un reto enorme y un proyecto a largo plazo para los responsables de los sistemas de información dentro de la organización (CIO).

El gobierno de TI tiene que hacer parte fundamental del gobierno corporativo de la organización, estar articulado con este y evolucionar conjuntamente con ella. Los CIO, hoy por hoy, han asumido varios estándares que de alguna manera apoyan el gobierno de TI, pero estas implementaciones deben ser articuladas con mayor claridad a través de una directriz corporativa y la selección de un marco de control que realmente permita no solo la alineación sino la integración entre el gobierno corporativo y el gobierno de TI.

Los marcos de referencia como Cobit e ITIL, ISO 20000, ISO 27002, PMBok, CMMI, TOGAF no son mutuamente excluyentes y pueden ser combinados para obtener un poderoso marco de referencia de mejores prácticas, control y gobierno en la gestión de servicios de TI.

Lo más importante es lograr utilizar un modelo integral, bien adaptado a la organización, que permita a las TI cumplir con las cinco áreas focales del gobierno de TI (ITGI, 2008). Lo importante no es cuál de los marcos de control se escoja (Cobit, Calder-Moir, ISO 38500) sino que se logre cumplir con las cinco áreas focales del gobierno de TI. S&T

Referencias bibliográficas

Aldama y Miñon, E. (2003). *Informe de la Comisión Especial para el fomento de la transparencia y seguridad en los mercados y en las sociedades cotizadas*. Recuperado de CNMV: http://www.cnmv.es/Portal_Documentos/Publicaciones/CodigoGov/Informefinal.PDF

Arveson, P. (1998). *The Deming cycle*. Recuperado de: http://www.balancedscorecard.org/thedemingcycle/tabid/112/default.aspx

Basel Commitee on banking supervision. (2005). *Basel II: International convergence of capital measurement and capital standards: a revised framework*. Basilea: Bank for International Settlements.

Basel Committee on banking supervision. (2006). *Enhancing corporate governance in banking organizations*. Basilea: Bank for International Settlements.

Bosch, A. (2008). *COSO - ISO 38500* [video]. Conferencia presentada en el tercer curso de verano itSMF – Universidad: El gobierno de TI. Recuperado de: http://www.youtube.com/watch?v=37zvCvb31cw&feature=relmfu

Bryce, R. (2002). *Pipe dreams: Greed, ego and the death of Enro*. New York, NY: PublicAffairs.

BS15000 Associates Group. (n.d). The ISO 20000 (BS15000 / BS 15000) ITSM Standard. Recuperado de: http://www.bs15000.org.uk/

Cadbury, A. (1992). *Report of the Committee on the financial aspects of corporate governance*. Londres, Inglaterra: Gee (Professional Publishing Ltd.).

CAF / IAAG. (Abril de 2005). *Lineamientos para un código andino de gobierno corporativo* (versión revisada). Recuperado de: http://gc.caf.com/upload/pubs/Lineamientos%20para%20un%20Codigo%20Andino%20de%20GC.pdf

Calder, A. (2006). Nueve claves para el éxito, una visión general de la implementación de la norma NTC-ISO/IEC 27002. Bogotá: ICONTEC.

Calder, A. (2008). *The Calder-Moir IT Governance Framework*. Recuperado de: http://www.itgovernance.co.uk/calder_moir.aspx

Carrillo, J. (2009). *Definiendo el alcance del gobierno de TI* [video]. Conferencia presentada en el tercer curso de verano itSMF – Universidad: El gobierno de TI. Recuperado de: http://www.youtube.com/watch?v=xUL8IBalh9I&feature=relmfu

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

Committee on Sponsoring Organizations of the Treadway Commission [COSO]. (1992). *Internal Control - Integrated Framework*. Durham, NC: American Institute of CPAs.

Cram, A. (2007). The IT balanced scorecard revisited. *Information system control journal (5)*, 1-5.

Financial Reporting Council. (2005). *Internal Control: Revised Guidance for Directors on the Combined Code*. London: Autor.

Forrester, E., Buteau, B., & Shrum, S. (2011). *CMMI for services: guidelines for superior service* (2a ed.). Upper Saddle River, NJ: Addison-Wesley Professional.

Garbarino, H. (2010). *Gobierno de TI. Organización, administración y control de las TI, un encuadre en Pymes*. Recuperado de: http://www.ort.edu.uy/fi/pdf/investigaciontuteladagarbarinoort.pdf

Hofmann, H. F., Yedlin, D. K., Mishler, J. W., & Kushner, S. (2011). *CMMI(R) for outsourcing: Guidelines for software, systems, and IT acquisition*. Addison-Wesley Professional.

Iqbal, M., & Nieves, M. (2007). *ITIL V3 Service strategy book*. London: The Stationery Office.

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

ISO/IEC. (2005b). *ISO/IEC 20000-2:2005 Information technology -- Service management -- Part 2: Code of practice*. Autor.

ISO/IEC. (2005c). *ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements*. Autor.

ISO/IEC. (2005d). *ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management*. Autor.

ISO/IEC. (2008). *ISO/IEC 38500 Corporate governance of information technology*. Autor.

IT Governance Network. (Agosto de 2008). *Implementing ISO 38500*. Obtenido de IT Governance Network: http://itgovernance.com/web/content/view/40/2/

ITGI. (2003). *Board Briefing on IT Governance, Second Edition*. Rolling Meadows, IL: Autor.

ITGI. (2006). *IT Control Objectives for Sarbanex-Oxley: The role of IT in the Design and Implementation of the Internal Control Over Financial Reporting (2 ed.)*. Rolling Meadows, IL: Autor.

ITGI. (2007). *Cobit 4.1*. Rolling Meadows, IL: Autor.

ITGI. (2008a). *IT Governance, global status report 2008*. Rolling Meadows, IL: Autor.

ITGI. (2008b). *Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio*

de la empresa. Rolling Meadows: Autor.

Izquierdo, F. (2009). Frameworks de IT-Governance – Estado del arte. *GRC Symposium*. Bogotá: ISACA - Colombian Chapter.

Jeter, L. (2003). *Disconnected: Deceit and Betrayal at WorldCom*. Hoboken, NJ: John Wiley & Sons.

Kaplan, R., & Norton, D. (1996). *The Balanced Scorecard*. Boston, MA : Harvard Business School Press.

Lacy, S., & Macfarlane, I. (2007). *ITIL V3 Service transition book*. London: The Stationery Office.

McLean, B., Elkind, P. (Escritores), & Gibney, A. (Dirección). (2005). *Enron: The Smartest Guys in the Room* [Película].

Microsoft. (Julio de 2010). *Microsoft operations framework /MOF extended guidance*. Recuperado de: www.microsoft.com/mof

Office of Government Commerce . (2007). *ITIL V3 Service operation book*. London: The Stationery Office.

Olivencia, M. (1998). *El Gobierno de las Sociedades Cotizadas*. Madrid: Comisión Especial para el estudio de un código ético de los consejos de administración de las sociedades.

Organización para la Cooperación y el Desarrollo Económicos [OCDE]. (1999). *Principios de la OCDE para el gobierno de las sociedades*. OECD Publishing.

OCDE. (2004). OCDE *Principios de Gobierno Corporativo*. Madrid: Ministerio de Economía y Hacienda de España.

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

Phillips, M., Gallagher, B. P., Richter, K. J., & Shrum, S. (2011). *CMMI® for acquisition: guidelines for improving the acquisition of products and services* (2a ed.). Addison-Wesley Professional.

PriceWaterhouseCoopers. (Agosto de 2009). *COSO Report. Control Interno*. Recuperado de: http://camara.ccb.org.co/documentos/4663_pwc___ccb___coso_report.pdf

Project Management Institute. (2010). *A guide to the project management body of knowledge. Pmbok guide* (4a ed.). Newton Square, PA: Project Management Institute.

Real Academia Española. (2005). *Diccionario de la lengua española* (22 ed.). Madrid: Espasa Calpe.

RiskIT. (2009). *Enterprise Risk: Identify, Govern and Manage IT Risk, in Risk IT*. Rolling Meadows, IL: ITGI.

Ross, J., & Weil, P. (November de 2002). Six IT Decision Your IT People Shouldn't Make. *Harvard Business Review*. Recuperado de: http://www.qualified-audit-partners.be/user_files/ITforBoards/GVIT_Harvard_Business_Review-Ross_Jeane___Weill_Peter_Six_IT_Decsions_Your_IT_People_Shouldnt_Make_2002.pdf.

Rudd, C., & Lloyd, V. (2007). *ITIL V3 Service design book*. London: The Stationery Office.

Sarbanes-Oxley. (Julio de 2002). Sarbanes-Oxley Act of 2002 Pub. L. No. 107-204, 116 Stat. 745. Washington D.C: The U.S Government Printing Office.

Spalding, G. (2007). *ITIL V3 Continual service improvement book (*2th Print). London: The Stationery Office.

Toomey, M. (Mayo de 2009). *A Framework for Governance and Management of IT*. Recuperado de: http://www.infonomics.com.au/Web%20Content/Documents/The_Infonomics_Letter_May_2009.pdf

Val IT. (2008). *Enterprise value: governance of IT investments. The Val IT framework 2.0.* Rolling Meadows, IL: ITGI.

Weill, P., & Ross, J. (2004). *IT Governance. How top performers manage IT decision rights for superior results.* Boston, MA.: Harvard Business School Press.

Weill, P., Subramani, M., & Broadbent, M. (Fall 2002). Building IT Infrastructure for Startegic Agility. *MIT SLOAN Management Review*, 27- 55

Winter, J. (2002). *Report of the High level group of company law experts of modern regulatory framework for company law in Europe.* Recuperado de: http://ec.europa.eu/internal_market/company/docs/modern/report_en.pdf

Currículum vitae

Ingrid Lucía Muñoz Periñán, M.Sc.

Project management profesional (PMP), *Cobit Foundation certificate*, auditor líder en seguridad de la información ISO 27001 por el *British Standard Institute*. Ingeniera Electrónica de la Universidad del Valle, con especialización en Gestión de informática organizacional y maestría en Gestión de informática y telecomunicaciones de la Universidad Icesi. Es consultora en gerencia de proyectos y seguridad de la información para diferentes compañías del sector privado y el gobierno, docente universitaria, coordinadora del Grupo de gobierno de TI y coordinadora académica del Diplomado de gerencia de proyectos bajo el PMBok-Cuarta Edición, en la Universidad Icesi.

Gonzalo Ulloa Villegas, Ph.D.

Doctor en Ciencias Técnicas de la Escuela Politécnica Federal de Lausanne, EPFL (Suiza). Ingeniero Electricista de la Universidad del Valle. Se desempeña como Decano de la Facultad de Ingeniería la de la Universidad Icesi. Fue Profesor del posgrado en redes de comunicaciones de la Universidad del Valle y profesor asistente en la cátedra de informática industrial de la Escuela Politécnica Federal de Lausanne (Suiza). Ha sido consultor en tecnologías de información y telecomunicaciones y ha participado en proyectos con el Estado y la empresa privada en temas de informática, telecomunicaciones, tecnologías de información y negocios electrónicos. Fue gerente de telemática en Transtel S.A., y gerente general de Suscriptores Audiovisuales (Cablevisión).