Gestión y Sociedad

Volume 5 | Number 1 Article 2

2012-06-01

Marco de referencia para auditorías integrales de sistemas en las mipymes colombianas

Roberto Carlos Díaz Alonso
Corporación Universitaria de la Costa (CUC), Barranquilla, Colombia, roberalonso24@gmail.com

Marco de referencia para auditorías integrales de sistemas en las mipymes colombianas

Roberto Carlos Díaz Alonso*

Recibido: 20 de enero del 2012 – **Aprobado**: 22 de marzo del 2012

Resumen

Este artículo presenta un marco de referencia de auditoría de sistemas aplicable a las micro, pequeñas y medianas empresas (mipymes) colombianas, a partir del trabajo articulado con las diferentes normas técnicas, estándares y mejores prácticas mundiales en el ámbito de la tecnología de la información (TI) y control interno para la realización de auditorías integrales de sistemas. Para ello se estudia el comportamiento que ha tenido el sector de las mipymes en la economía colombiana en TI y se analizan los estándares o normas técnicas de COBIT (Control Objectives for Information and Related Technologies), ITIL (Biblioteca de Infraestructura de Tecnologías de Información), ISO 2700X, ISO 900X, entre otros.

Palabras clave

Gobierno de tecnología de la información, seguridad de la información, COBIT, ITIL, ISO 27002, COSO, alineación, auditoría de sistemas.

* Contador público egresado de la Corporación Universitaria de la Costa (CUC), Barranquilla, Colombia; especialista en Estudios Pedagógicos; especialista en Auditoría de Sistemas de Información, CUC. Diplomado en Docencia y mediación pedagógica en la Virtualidad y Herramientas web 2.0, Universidad Autónoma de Bucaramanga (UNAB), Colombia. Correos electrónicos: roberalonso24@gmail.com; rdiaz1@cuc.edu.co

Roberto Carlos Díaz Alonso

Framework for Comprehensive System Audits in Colombian MSMEs

Abstract

This article presents a framework of systems audit applicable to Micro, Small and Medium Enterprises (MSMEs) in Colombia, based on the joint work with different technical norms and standards, and best global practices in the field of information technology (IT) and internal control for comprehensive system audits. For this purpose, we study the behavior of the MSME sector in Colombian economy in IT and analyze standards or technical norms of COBIT (Control Objectives for Information and Related Technologies), ITIL (Information Technology Infrastructure Library), ISO 2700X and ISO 900X, among others.

Keywords

Government of Information Technology, Information Security, COBIT, ITIL, ISO 27002, COSO, Alignment, Systems Audit.

Introducción

En este artículo se determina si la auditoría de sistemas enfocada solo al cumplimiento normativo no representa ningún tipo de interés para los gerentes, más allá de, en el mejor de los casos, cumplir con la ley. Este tipo de escenarios demuestra día a día que cada vez se hace más necesaria la integración de los estándares internacionales para lograr auditorías efectivas que garanticen un gobierno corporativo de tecnología de la información (TI) gestionable y acorde con las necesidades del negocio, así como unos servicios de tecnología altamente eficientes.

De este modo se convierte en imperativo estratégico observar estándares y normas técnicas como ITIL (Biblioteca de Infraestructura de Tecnologías de Información, siglas en inglés), que representa el conjunto de mejores prácticas *adoptadas* y *aceptadas* por la industria en materia de gestión de servicio de TI. Esta se basa en el estándar mundial para el área de IT ITIL (Biblioteca de Infraestructura de TI), que sirve como guía y base para la definición de nuevas acciones de mejora de los servicios, en espacial en la preparación de auditorías contra el estándar ISO/IEC 20000-1:2005. (ISO20000, 2010).

COBIT (Control Objectives for Information and Related Technologies) es "un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso" (Micrositios Ltda., 2005). Por su parte, ISO 2700X (ISO/IEC 17799) —también denominada como ISO 27002— "es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por la International Organization for Standardization y por la Comisión Electrotécnica Internacional en el 2000 (Wikipidia, s. f.). Por su parte, "ISO 9000 designa un conjunto

de normas sobre calidad y gestión continua de calidad, establecidas por la Organización Internacional para la Estandarización ISO" (Wikipidia, s. f.).

ISO 2700X se puede aplicar en cualquier tipo de organización o actividad orientada a la producción de bienes o servicios, así como procedimientos de administración de riesgos, con el fin de tener en cuenta como aspectos esenciales del gobierno de TI: la gestión del servicio, la seguridad de la información y la teoría de riesgos, en concordancia con los tres grandes temas que exige la auditoría de hoy y en cascada: gobierno, riesgos, control.

Hoy en día, en las organizaciones, la auditoría se concibe como una actividad de evaluación independiente que agrega valor mediante el hallazgo de oportunidades de mejora a los procesos y en el caso de los sistemas de información, su ayuda radica en:

> [...] la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones (Armando, 2002, p. 122).

Antecedentes y teorías básicas

El progreso de los países está medido por la capacidad de generación de riqueza que posea, y para nadie es secreto que en este aspecto la actividad empresarial juega un papel fundamental como motor de la sociedad dentro de la economía capitalista. En el caso particular de nuestro país, la mayor parte de la actividad empresarial se encuentra en las mipymes:

> En Colombia hay 1 343 521 empresas en los sectores de industria, comercio y servicios, que ocupan 2 818 430 trabajadores, en donde el 99% de estas empresas son micro con un total de 1 653 493 trabajadores, que corresponde al 58,67% del total. Las microempresas son en su mayoría empresas familiares, estratos 1, 2 y 3 (Sánchez, 2007, p. 23).

No obstante, para que la actividad empresarial pueda ser sostenible en el tiempo requiere avances en el conocimiento humano, como instrumento principal de su racionalización. Al respecto, a lo largo de la historia han surgido múltiples disciplinas que buscan el efectivo control de los recursos, como la contabilidad, administración y en el ámbito de la automatización de tareas, la ingeniería de sistemas de información. Pero, a medida que estos saberes surgían —unos primeros que otros, en el mundo se desarrollaba la auditoría a la par de la contabilidad— como proceso asegurador de la actividad comercial:

> Existe la evidencia de que alguna especie de auditoría se practicó en tiempos remotos. El hecho de que los soberanos exigieran el mantenimiento de las cuentas de su residencia por dos escribanos independientes, pone de manifiesto que fueron tomadas algunas medidas para evitar desfalcos en dichas cuentas. A medida que se desarrolló el comercio, surgió la necesidad de las revisiones independientes para asegurarse de la adecuación y finalidad de los registros mantenidos en varias empresas comerciales. La auditoría como profesión fue reconocida por primera vez bajo la Ley Británica de Sociedades Anónimas de 1862 y el reconocimiento general tuvo lugar durante el periodo de mandato de la ley (Lara, 2011, p. 19).

Antecedentes sobre las normas técnicas y estándares internacionales

En nuestro entorno se hace cada vez más común que en las grandes empresas se mencionen las mejores prácticas mundiales en relación con

las diferentes disciplinas que intervienen en el quehacer empresarial: finanzas, calidad, administración y, en los últimos años, las tecnologías de la información se encuentran a la orden del día dentro de los diferentes proyectos de las grandes corporaciones, al invertir cantidades considerables de recursos en ello.

Con el objetivo de lograr una sincronización exitosa entre TI y el negocio, en Inglaterra, a finales de los años ochenta, surgió la Biblioteca de Infraestructura de Tecnologías de Información (ITIL) que fue desarrollada:

> [...] al reconocer que las organizaciones dependen cada vez más de la Informática para alcanzar sus objetivos corporativos. Esta dependencia en aumento ha dado como resultado una necesidad creciente de servicios informáticos de calidad que se correspondan con los objetivos del negocio, y que satisfagan los requisitos y las expectativas del cliente (TI, ITIL-Gestión de Servicios, 2011, p. 34).

Asimismo, se reconoce que:

> [...] el énfasis pasó de estar sobre el desarrollo de las aplicaciones TI a la gestión de servicios TI. La aplicación TI (a veces nombrada como un sistema de información) solo contribuye a realizar los objetivos corporativos si el sistema está a disposición de los usuarios y, en caso de fallos o modificaciones necesarias, es soportado por los procesos de mantenimiento y operaciones (TI, ITIL-Gestión de Servicios, 2011, p. 35).

Por otra parte, el desarrollo vertiginoso en las redes informáticas trajo consigo un aumento considerable en la velocidad de procesamiento y en la transmisión de información del negocio, pero con riesgos cada vez mayores en lo referente a seguridad de los datos transportados por estos medios; en este sentido, vemos cómo en la actualidad, la convergencia de las tecnologías de la información han ocasionado una tecnodependencia que impide una separación certera entre la seguridad propia de las aplicaciones (seguridad informática) con la seguridad de la información como tal. Por esta razón, reconociendo el amplio espectro que implica el concepto de seguridad de la información, se decidió acoger como un estándar certificable la ISO 17799 —anteriormente British Standard (BS) 7799/1999— en el 2005, la cual más tarde se convirtió en la ISO 27002:

> Hasta 2005, el estándar más conocido en el entorno de seguridad informática era el ISO 17799, pero con la limitación de ser un "código de prácticas" (*Information technology —Security techniques Code of practice for information security management)*, en el momento que se publica su última revisión, se anuncia el desarrollo de una serie de estándares ISO 27000, dedicada exclusivamente a la seguridad informática. Con esto se le da un nuevo alcance a la seguridad, porque no solo es llevar un código de mejores prácticas sino [también es] establecer un estándar certificable de forma similar al ISO 9000 (el primero de esa serie en publicarse fue el ISO 27001) (Palomino, 2007, p. 46).

Las ventajas en lo organizacional de aspirar a una certificación o de alinear sus procesos hacia estándares certificados confluyen principalmente en las siguientes: 1) se puede aprovechar una curva de aprendizaje adquirida por experiencias exitosas y también por los errores anteriores en la implementación de los requerimientos de la norma; 2) la organización se pone *a tono* con prácticas certificadas, lo que en sí mismo ya es una garantía razonable de que, a raíz de una buena implementación, mejorarán los procesos involucrados; 3) implementar *la mejor forma* de realizar los procesos implica ahorros considerables a las compañías en cuanto a tiempo, recursos empleados, cumplimiento del marco legal aplicable si se adapta la norma

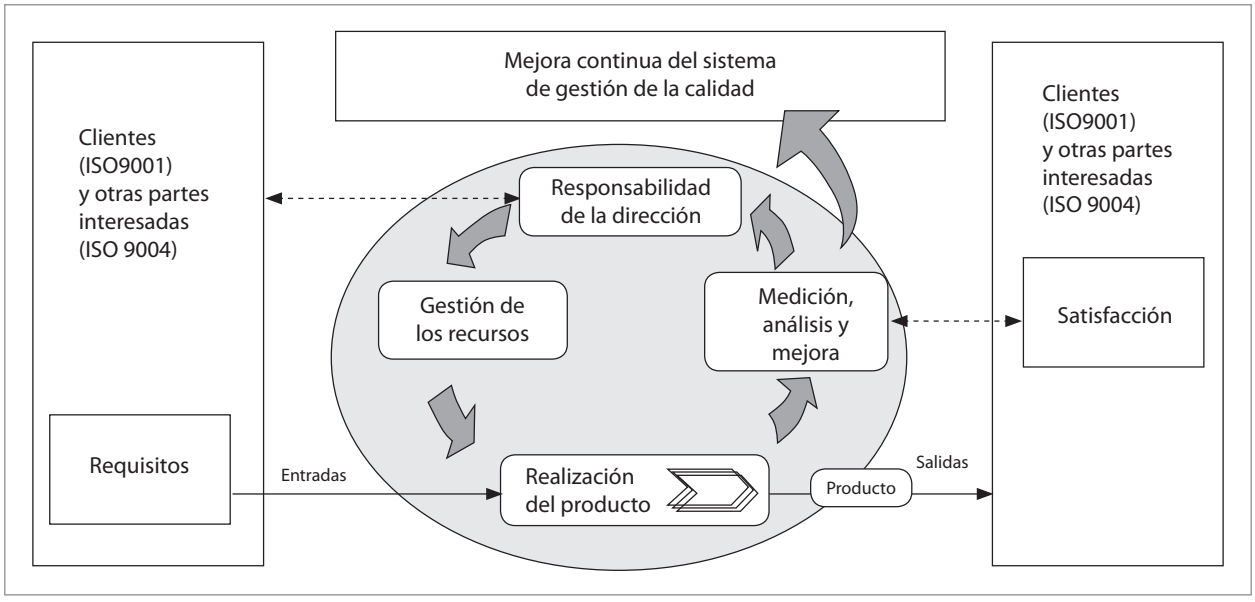
certificable a la realidad normativa del entorno del negocio; todo esto repercute directamente en una disminución de costes y por ende en el mejoramiento de la eficiencia; 4) el alineamiento de los procesos con la norma certificable genera mejoras en la eficacia de la organización, dada su capacidad de efectuar solo aquellas tareas que contribuyen al logro de los objetivos del negocio.

Similar a la familia de normas técnicas ISO 2700X, se encuentran *regulando* en el ámbito de los procesos organizacionales y como garante de que el producto o servicio efectuado cumpla con unos requerimientos mínimos de calidad, la familia de normas técnicas ISO 900X, la cual tiene su origen en la norma BS 5750, publicada en 1979 por la entidad de normalización británica que tenía como objetivo la consecución de mejores procedimientos para la actividad militar (figura 1):

> [...] se comenzó a exigir a los fabricantes que mantuvieran por escrito todos los procedimientos, para que estos fueran luego aprobados. A partir de 1959 en los Estados Unidos se utilizó un programa de requerimientos de calidad para los suministros militares. En 1968 la OTAN especificó la AQAP (*Allied Quality Assurance Procedures* o aseguramiento de calidad para los procedimientos de los aliados) para aplicarla a los insumos militares de la alianza. Con el tiempo y la presión de los compradores de insumos, la idea de la estandarización fue más allá del ámbito militar, y en 1971, el Instituto de Estandarización Británico publicó la norma BS 9000, específicamente para el aseguramiento de la calidad en la industria electrónica; esta siguió desarrollándose para en 1970 pasar a ser la BS 5750, más general y aplicable ("¿Qué es Iso 9000?", 2011, p. 12).

De esta norma se derivó la primera versión de la norma técnica ISO 9000:1987. Valga decir que con el paso del tiempo la familia de ISO 900X ha ganado en lo referente a la inclusión en forma explícita del concepto de mejora continua y el

Figura 1. Modelo del sistema de gestión de calidad



Fuente: "Análisis del sistema de gestión de la calidad de Conformat" (http://www.gestiopolis.com/administracion-estrategia/analisis-del-sistema-de-gestion-de-la-calidad.htm)

monitoreo y seguimiento de la satisfacción del cliente; asimismo, se han eliminado gradualmente los requerimientos documentales que entorpecen la labor de la organización.

Actualmente se ha convertido en lugar común para diferentes autores estudiosos de los sistemas de gestión y mapear los requerimientos de las diferentes normas técnicas en cuestión. Como ejemplo podríamos citar los anexos de la norma ISO 27002 que mapea esta norma con los requisitos exigidos por la ISO 9001; una tarea especialmente importante porque provee de herramientas a administradores de sistemas de gestión, alta dirección y auditores para ejecutar su labor e identificar sinergias que permitan una implementación/evaluación costo-eficiente para la compañía.

Como marco de referencia para los objetivos de control de las tecnologías de la información encontramos COBIT, desarrollado por Isaca, que tiene como objetivo presentar un modelo que permita implementar y auditar "la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso" (Micrositios Ltda., 2005). De esta manera, COBIT se convirtió en la herramienta de clase mundial por excelencia implementada por las grandes organizaciones para adecuar sus sistemas de información a las mejores prácticas en materia de control y gobierno de TI:

> [...] la estructura del modelo COBIT propone un marco de acción donde se evalúan los criterios de información, como por ejemplo la seguridad y calidad, se auditan los recursos que comprenden la tecnología de información, como por ejemplo el recurso humano, instalaciones, sistemas, entre otros, y finalmente se realiza una evaluación sobre los procesos involucrados en la organización (Micrositios Ltda., 2005).

Entendiendo el punto de vista del autor, vemos que en el COBIT confluyen algunos elementos comunes a los anteriores marcos de referencia y normas técnicas citadas: seguridad (ISO 27001) y procesos (ITIL), enfocados al cliente con criterios de calidad (ISO 9000), llevando esto a la posibilidad de desarrollar un marco de trabajo único que garantice profundidad y multidisciplinariedad para trabajos de aseguramiento de TI. En efecto:

> COBIT está basado en marcos de referencia establecidos, tales como CMM de SEI (Software Engineering Institute), ISO 9000, ITIL e ISO/IEC 27002; sin embargo, COBIT no incluye tareas y pasos de procesos porque, aunque está orientado a procesos de TI, es un marco de referencia para gestión y control antes que un marco de referencia para procesos. COBIT se focaliza en lo que una empresa necesita hacer, no cómo lo tiene que hacer, y la audiencia objetivo es la alta gerencia, los gerentes funcionales, los gerentes de TI y los auditores (It Govemance Institute, 2008, p. 7).

COBIT se basa en marcos de referencia establecidos, como *CMM del Software Engineering Institute, ISO 9000, ITIL e ISO/IEC 27002*. Sin embargo, COBIT no incluye los pasos del proceso y las tareas ya que, si bien se orienta hacia los procesos de TI, es un marco de gestión y control en lugar de un marco de proceso. Asimismo, COBIT se centra en lo que una la empresa tiene que hacer, no cómo debe hacerlo y el público objetivo es la alta dirección, alta dirección de TI y los auditores.

Partiendo de esta premisa tenemos que, si bien los objetivos de COBIT, la ITIL y las normas técnicas ISO/IEC 9000 e ISO/IEC 27000 son sustancialmente diferentes, la construcción de COBIT está basada en distintos marcos de referencia en el mundo y por ello, partiendo de COBIT como elemento de cohesión se puede obtener un alineamiento consistente entre las mencionadas normas técnicas y estándares

> IT best practices need to be aligned to business requirements and integrated with one another and with internal procedures. COBIT can be used at the highest level, providing an overall control framework based on an IT process model that should suit every organisation generically. Specific practices and standards such as ITIL and ISO/IEC 27002 cover discrete areas and can be mapped to the COBIT framework, thus providing a hierarchy of guidance materials (It Govemance Institute, 2008, p. 22).

Las mejores prácticas de TI tienen que alinearse a los requerimientos del negocio e integrarse entre sí y con los procesos internos. COBIT se puede utilizar al más alto nivel, proporcionando un marco de control general sobre la base de un modelo de procesos de TI que debe adaptarse a cada organización de forma genérica. Las prácticas específicas y las normas como la ITIL e ISO/IEC 27002 cubren áreas específicas y se pueden mapear con el marco de referencia COBIT, para así proporcionar una jerarquía de materiales de orientación.

Comprendiendo lo anterior, la pregunta natural que surge es: si el marco conceptual de COBIT surge del alineamiento de diversos estándares que desarrollan el *cómo hacer*, ¿cuál es la mejor manera de integrar los diversos estándares y normas técnicas enfocadas a la realidad de las pymes? Esta pregunta es la que intentaremos desarrollar en el resto del trabajo, con el objetivo de desarrollar unas guías de auditoría con los puntos de control claros por auditar en las pymes.

Desarrollo de las pymes: el papel de las auditorías combinadas de tecnología de la información

En el contexto actual de la economía mundial, hablar de desarrollo, competitividad y libre comercio nos lleva de inmediato a pensar en el término globalización que puede ser definida como:

> [...] un proceso económico, tecnológico, social y cultural a gran escala, que consiste en la creciente comunicación e interdependencia entre los distintos países del mundo unificando sus mercados, sociedades y culturas, a través de una serie de transformaciones sociales, económicas y políticas que les dan un carácter global (Wikipedia, s. f.).

Es de anotar de la presente definición que la globalización es un proceso y como tal posee dinamismo, este último impulsado por a los avances acelerados en materia de telecomunicaciones: "En lo tecnológico la globalización depende de los avances en la conectividad humana (transporte y telecomunicaciones) facilitando la libre circulación de personas y la masificación de las TIC y el Internet" (Wikipedia, s. f.). Las empresas que logran reconocer estas realidades comprenden bien el papel que TI puede jugar en el negocio:

> For many enterprises, information and the technology that supports it represent their most valuable, but often least understood, assets. Successful enterprises recognise the contribution and benefits of information technology (IT) and use IT to drive their stakeholders' value. These enterprises also understand and manage the associated risks such as increasing regulatory compliance and critical dependence of many business processes on IT (It Govemance Institute, 2007, p. 8).

Para muchas empresas, la información y la tecnología que la soporta representan lo más valioso y a menudo menos entendido, los activos. Las empresas de éxito reconocen la contribución y los beneficios de la TI y el uso de esta para impulsar el valor de sus accionistas. Estas empresas también entienden y gestionan los riesgos asociados como el aumento de cumplimiento de la normativa y la dependencia crítica de muchos procesos de negocio en TI.

Por ello, para el sector empresarial la globalización representa un reto y a la vez una oportunidad, ya que los competidores se encuentran ubicados en la aldea global y no solamente en las economías locales, como anteriormente sucedía con la atenuante de que todos ellos conocen con claridad el papel que TI desempeña en el negocio ¿Cuál es el factor diferenciador entre un negocio y otro? Esta anotación adquiere especial relevancia si tomamos como objeto de estudio las pymes (pequeñas y medianas empresas), empresas que por su estructura, tamaño, número de trabajadores y monto de activos o patrimonio presentan algunas desventajas frente a las grandes empresas:

- Financiación. Las empresas pequeñas tienen más dificultad de encontrar financiación a un costo y plazo adecuados debido a su mayor riesgo. Para solucionar esto se recurren a las sociedades de garantía recíproca (SGR) y capital riesgo.
- Empleo. Son empresas con mucha rigidez laboral y que tiene dificultades para encontrar mano de obra especializada. La formación previa del empleado es fundamental para estas.
- Tecnología. Debido al pequeño volumen de beneficios que presentan estas empresas no pueden dedicar fondos a la investigación, por lo que tienen que asociarse con universidades o con otras empresas.
- Acceso a mercados internacionales. El menor tamaño complica su entrada en otros mercados. Desde las instituciones públicas se hacen esfuerzos para formar a las empresas en las culturas de otros países.

Sin desconocer lo anterior, las pymes también presentan como una de sus principales ventajas "su capacidad de cambiar rápidamente su estructura productiva en el caso de variar las necesidades de mercado, lo cual es mucho más difícil en una gran empresa, con un importante número de empleados y grandes sumas de capital invertido" (Wikipedia, s. f.). No obstante, por el hecho de que las pymes presenten esta enorme ventaja, las encontramos rezagadas en materia de TI (en incluso de otras disciplinas), las cuales no encuentran en este tema algo interesante para aportarles a sus negocios, por una razón fundamental: "Muchas empresas no manejan IT de una manera cohesiva, sino más bien distribuida, lo cual deriva en islas de hardware, software, servicios de telecomunicaciones, cada quien respondiendo por sus respectivos departamentos, sin ver el servicio completo al usuario final" (IntraEmprendedor, s. f.). Esta visión incompleta y fragmentada del universo de la TI genera desconfianza en la alta dirección (trátese en las pymes de un organismo colegiado, gerente o gerente-propietario) que no encuentra valor agregado para alcanzar los objetivos del plan de negocios.

Esta percepción de los dueños de negocios pymes de la TI implica un gran reto, puesto que hoy más que nunca es imperativo adecuar las tecnologías de la información en los procesos de negocio: "el reto de administrar toda el área de TI sigue vigente sin importar el tamaño de la empresa" (IntraEmprendedor, s. f.); para abordar el reto existen las buenas prácticas y normas técnicas respectivas de acuerdo con la materia de estudio, que pueden desempeñar un papel crucial para el desarrollo de las pymes por cuanto que al someterse al filtro de estas, permite conocer el estado actual de los procesos y reconocer la brecha existente para establecer planes de acción que permitan optimizar los procesos de acuerdo con la capacidad de consecución de recursos de la compañía y los objetivos por alcanzar.

Algunos institutos, como el ITGI, han diseñado marcos de referencia como COBIT *Quickstart* que está diseñada para una implementación rápida en compañías que, o bien desean implementar COBIT de forma rápida o sencillamente poseen una menor envergadura (léase pequeñas y medianas empresas):

> The driver behind COBIT Quickstart is the need of IT managers of smaller organisations for a simple-to-use tool that will speed up the implementation of key IT control objectives. Equally, IT managers of larger organisations can leverage the tool to 'quickstart' the initial phases of a broader IT governance implementation (It Govemance Institute, 2007, p. 15).

El motor detrás de COBIT Quickstart es la necesidad de los administradores de la TI de las organizaciones más pequeñas de una herramienta sencilla de usar que acelerará la aplicación de los principales objetivos de control de la TI. Del mismo modo, los administradores de TI de las grandes organizaciones pueden aprovechar de *Quickstart*, como las fases iniciales de una implementación más amplia del gobierno de TI.

Pero además de lo anterior, el ITGI también provee herramientas que realizan funciones de alineamiento entre diferentes normas técnicas y estándares, así encontramos *Aligning COBIT*® 4.1, ITIL® V3 and ISO/IEC 27002 *for Business Benefit* que:

> COBIT can be used at the highest level of IT governance, providing an overall control framework based on an IT process model that is intended by ITGI to generically suit every enterprise. There is also a need for detailed, standardised practitioner processes. Specific practices and standards, such as ITIL and ISO/IEC 27002, cover specific areas and can be mapped to the COBIT framework, thus providing a hierarchy of guidance materials (It Govemance Institute, 2008, p. 22).

COBIT puede ser utilizado en el más alto nivel del gobierno de TI, proporcionando un marco de control general basado en un modelo de proceso de TI provisto por la ITGI para adaptarse a cada empresa de forma genérica. También hay una necesidad de procesos detallados, de procesos prácticos estandarizados. Las prácticas y las normas específicas, como ITIL e ISO/IEC 27002, cubrir áreas específicas y se pueden mapear al marco COBIT, para así proporcionar una jerarquía de materiales de orientación.

De esta manera, observamos que partiendo de COBIT *Quickstart*, y pasando por *Aligning COBIT*® 4.1, ITIL® V3 and ISO/IEC 27002 *for Business Benefit,* encontramos una forma expedita de enmarcar la gestión del gobierno de TI para las pymes y a su vez alinear estos requerimientos con lo exigido por ITIL e ISO/IEC 27002. Ahora bien, la pregunta que sigue es: ¿se deben alinear las normas técnicas, marco de gobierno y buenas prácticas en la TI a la gestión de la calidad (ISO/IEC 9000) o se debe evaluar primero la calidad y luego adentrarnos en el mundo de la TI —en este caso el término *"mundo TI* hará referencia al conjunto de buenas prácticas, marcos de referencia y normas técnicas utilizados para evaluar la función de la TI, en nuestro caso ITIL, COBIT e ISO/IEC 27002—?

La pregunta debe ser resuelta de acuerdo con las circunstancias particulares de cada pyme, si lo que queremos es efectuar una auditoría integral enfocada hacia la TI lo correcto es alinear la norma técnica de calidad a los requerimientos del mundo de la TI, pero si nuestra intención es realizar una auditoría de calidad y adicionar un valor agregado evaluando algunos aspectos detallados de TI, lo más conveniente es arrancar desde ISO/IEC 9000 y alinear los requisitos de la norma a los requerimientos del mundo de la TI. En nuestro caso de estudio partiremos desde la primera óptica, ya que nuestro objetivo son las auditorías integrales de las TI para las pymes.

Universo de auditoría en las mipymes: marco referencial y metodología integrada

En nuestro entorno se hace cada vez más común que en las grandes empresas se haga mención

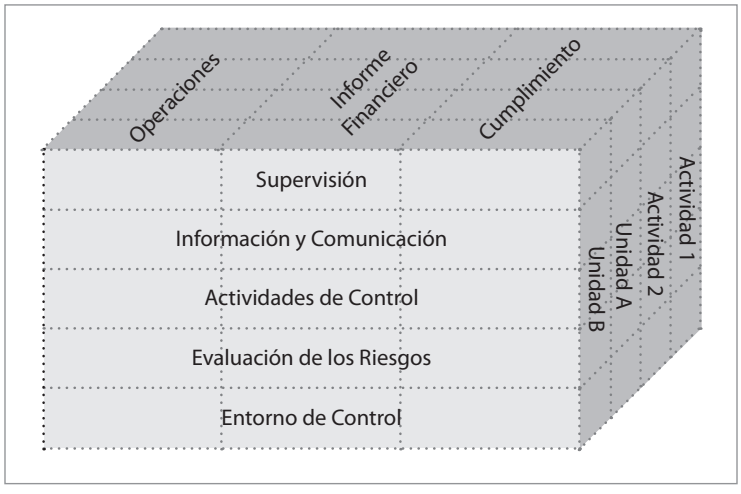
de las mejores prácticas mundiales en relación con las diferentes disciplinas que intervienen en el quehacer empresarial: finanzas, calidad, administración y, en los últimos años, las tecnologías de la información se encuentran a la orden del día dentro de los diferentes proyectos de las grandes corporaciones, invirtiendo cantidades considerables de recursos en ello. El control interno se convierte cada vez más en parte integral del negocio y una forma de desarrollar los negocios y los controles son vistos como algo natural a los procesos y no una necesaria carga externa que ralentizaba la actividad empresarial. Ver en el control interno como el marco sobre el cual descansa la estrategia empresarial ha traído múltiples beneficios a las organizaciones que comprenden los beneficios que esto genera en la administración en un mundo globalizado con mayor incertidumbre: con mayor nivel de riesgo.

De este modo, en 1992, debido a los estudios del Committee Of Sponsoring Organizations (adelantados desde 1985):

> Se trataba entonces de materializar un objetivo fundamental: definir un nuevo marco conceptual del control interno, capaz de integrar las diversas definiciones y conceptos que venían siendo utilizados sobre este tema, logrando así que, al nivel de las organizaciones públicas o privadas, de la auditoría interna o externa, o de los niveles académicos o legislativos, se cuente con un marco conceptual común, una visión integradora que satisfaga las demandas generalizadas de todos los sectores involucrados. (Committee of Sponsoring Organizations, 1985).

Así, este comité definió los siguientes objetivos y componentes en su marco de control, mediante la siguiente interacción (figura 2):

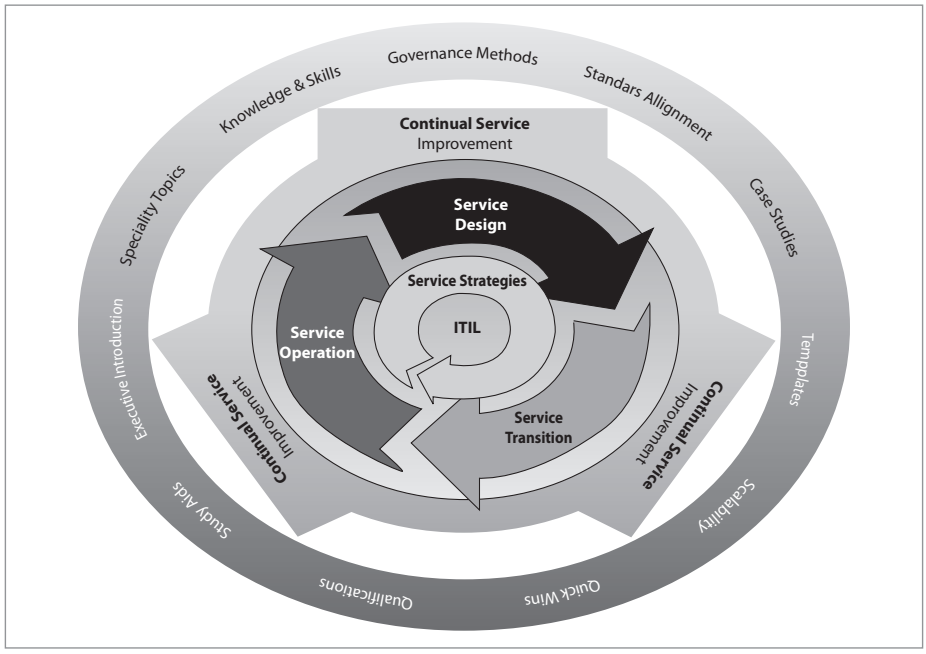
Figura 2. Relación entre objetivos y componentes



Fuente: "Los nuevos conceptos del control interno". Informe COSO (Modelo de Control COSO. Objetivos & Componentes de Control)

Por otra parte, dado que el éxito de las organizaciones cada vez más se encuentra asociado a los requisitos y expectativas del cliente, se hizo necesario desarrollar la Biblioteca de Infraestructura de Tecnologías de la Información (ITIC). El modelo de gestión del servicio ITIC se representa en la figura 3.

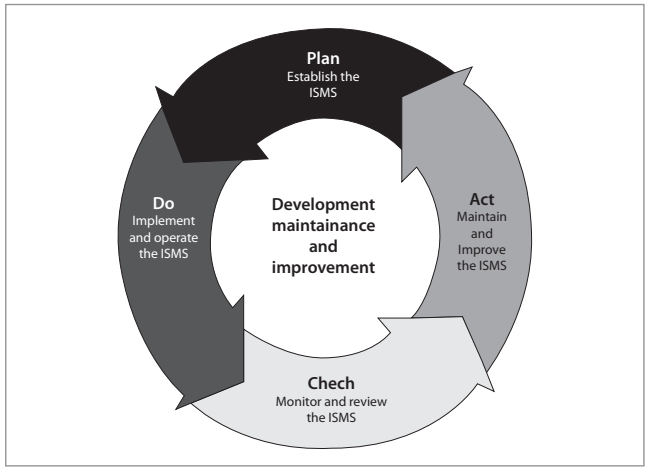
Figura 3. Modelo de gestión del servicio ITIL



Fuente: EuroPortal ITIL - Expertos en Gestión de Servicios Informáticos - http://www.portal-itil.eu/ITILv3.php

De igual manera, y como se dijo antes, últimamente el desarrollo vertiginoso en la redes informáticas ha traído consigo un aumento considerable en la velocidad de procesamiento y en la transmisión de información del negocio. Este hecho ha aumentado los riesgos en seguridad para los datos transportados por estos medios. De ahí la necesidad de implementar modelos de sistemas de gestión de seguridad de la información (figura 4).

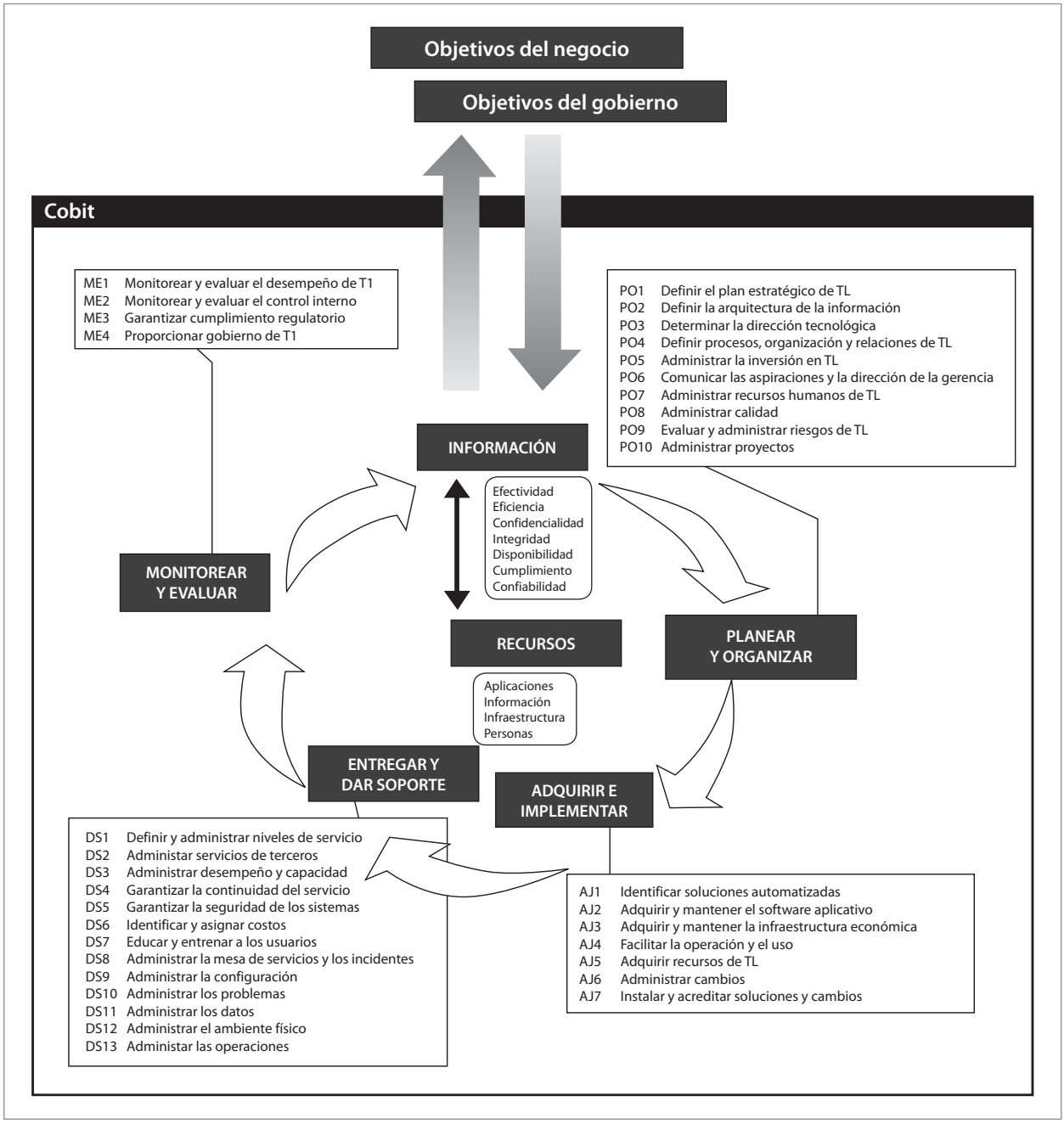
Figura 4. Modelo del sistema de gestión de seguridad de la información (Círculo de Deming)



Fuente: http://www.chullohack.com/wp-content/uploads/2010/02/iso27001.jpg

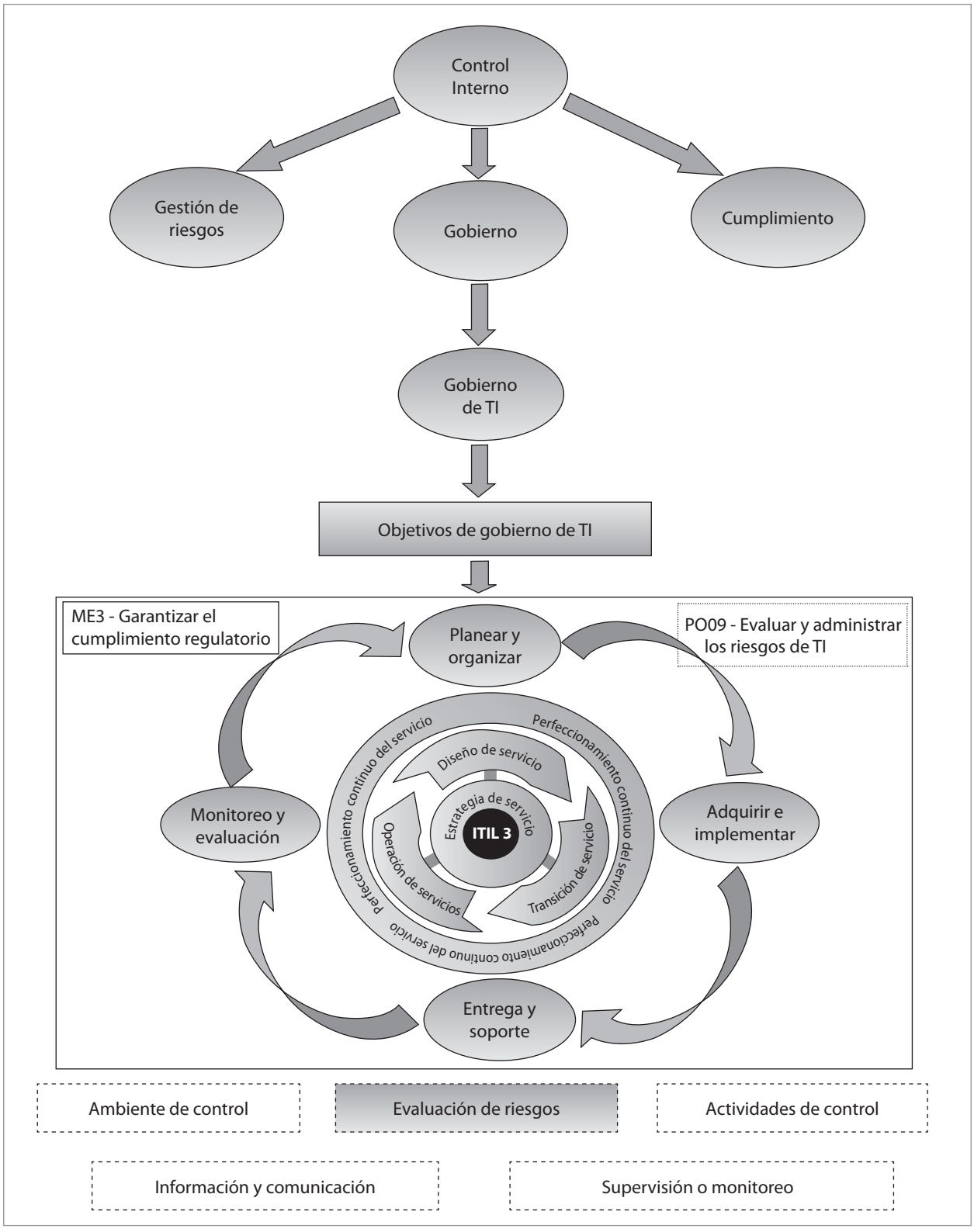
Como ya se ha dicho, debe existir un modelo de gestión y control de los sistemas de información y tecnología. En este contexto aparece COBIT, una herramienta de clase mundial implementada por las grandes organizaciones para adecuar sus sistemas de información a las mejores prácticas en temas de control y gobierno de TI (veánse figuras 5 y 6).

Figura 5. Marco de trabajo general de COBIT



Fuente: IT Governance Institute, COBIT 4.1 – Isaca - Modelo COBIT

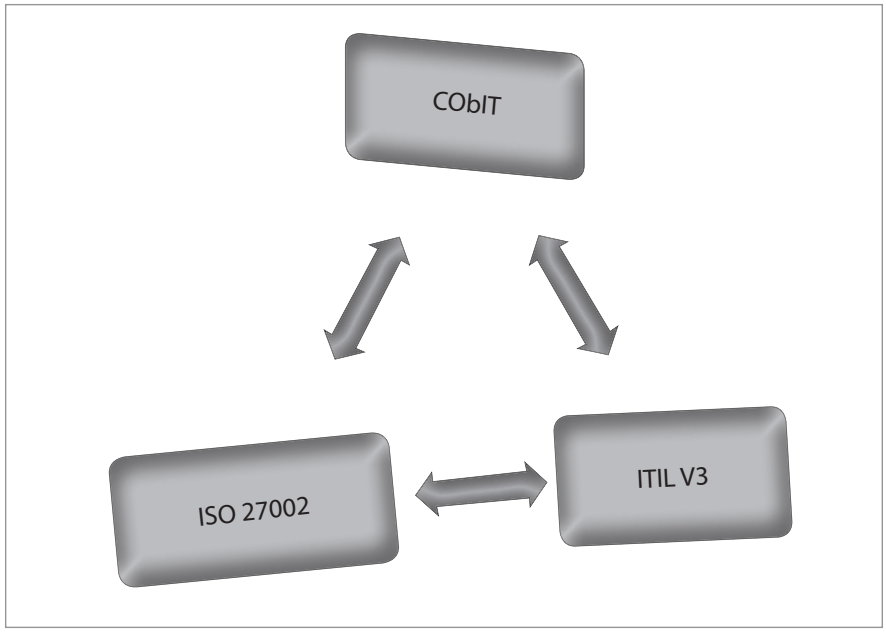
Figura 6. Marco de control integrado entre COSO, COBIT e ITIL



Fuente: elaboración propia.

Como vemos, existe una perfecta sincronía entre los elementos del control interno y los dominios para el cumplimiento de los objetivos de la TI. Ahora, ¿cómo pueden ser materializados los objetivos de la TI en procedimientos y prácticas concretas para el quehacer empresarial? La respuesta se encuentra en la alineación de COBIT con ITIL, ISO 2700X e ISO 900X. En la figura 7 se verá el detalle de cada una de estas, teniendo en cuenta que para efectuar auditorías en mipymes no es necesario tener en cuenta todos los objetivos de control propuestos por COBIT; por ello se tomará como base COBIT *Quickstart 2nd Edition*. Nuestro enfoque de trabajo se fundamenta en la figura 7. En esta se parte del objetivo detallado de control de COBIT hacia los requisitos de ISO 27002 e ITIL V3 respectivamente. Este enfoque está sustentado en el documento "Alineando COBIT 4.1, ITIL V3 e ISO 27002 en beneficio de la empresa", así como COBIT Quickstart, que posee los requerimientos mínimos de control para las empresas mipymes según IT Governance Institute.

Figura 7. COBIT, ISO 27002 y ITIL V3



Fuente: elaboración propia

Conclusiones

En el desarrollo del presente artículo podemos decir que la articulación entre COBIT, ITIL e ISO 27002 ayuda a las pymes a concentrar sus esfuerzos en lograr mayores beneficios para el negocio con una visión más sistémica y menos enfocada al cumplimiento. Se observa que las pymes no han implementado un marco de referencia para la planificación y la organización de la infraestructura tecnológica que deben soportar cada uno de sus procesos.

Esta investigación les brinda a la pymes una oportunidad de alinear las estrategias de cada estándar con las estrategias que ellas quieren realizar, para alcanzar el uso óptimo de todos los recursos que apoyen los procesos de las

pymes, que contribuirán al mejoramiento de los procesos.

Este modelo está enfocado fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones facilitadas por la TI, asegurarán la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien. El Modelo COBIT, las normas ISO 27002 y la ITIL representan las mejores prácticas, para su implementación en las pymes y la articulación de cada una de ellas conforman un modelo guía útil para una adecuada planificación de TI, ya que brindan la oportunidad de alinear las estrategias de la TI con las estrategias de estas organizaciones, de alcanzar el uso óptimo de todos sus recursos, todo lo cual ayudará a satisfacer las necesidades de la entidad y los requisitos de los usuarios, cumplir con la legislación, prestar un mejor servicio, revisarse y mejorarse de forma continua. Con la implementación de estos estándares se contribuirá a proporcionar una base de control de la TI en estas organizaciones.

Referencias

Armando, J. (2002, dic.). Historia de la Auditoría. Recuperado el 11 de diciembre del 2011, de http://www.monografias.com/trabajos12/condeau/condeau.shtml

IntraEmprendedor (2006). ITIL un resumen enfocado a pymes. Recuperado el 11 de diciembre del 2011, de http://www.intraemprendedor.com/2006/09/26/itil-un-resumen-enfocado-a-pymes/.

ISO 20000 (2010). Introducción ISO 20000 Colombia. Recuperado el 10 de diciembre del 2011, de www.iso20000.com.ar/intro_col.html.

IT Governance Institute (2007). *COBIT Quickstart* (2d ed.). Governace Institute.

IT Governance Institute (2008). *Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa.* Governace Institute.

Lara, C. (2011). *Auditoría de sistemas.* Recuperado el 10 de diciembre del 2011, de http://www.actiweb.es/msucreseccion29infysis/

Micrositios Ltda. (2005). *El modelo COBIT para auditoría y control de sistemas de información*. Recuperado el 10 de diciembre del 2011, de http://www.channelplanet.com/index.php?idcategoria=13932

Palomino, M. D. (2007, sep.). Seguridad informática. En *La evolución del estándar ISO 27001*. Recuperado el 10 de diciembre del 2011, de http://seguinfo.wordpress.com/2007/09/02/la-evolucion-del-estandar-iso-27001/

¿Qué es ISO 9000? (2011). Recuperado el 10 de diciembre del 2011, de http://www.misrespuestas.com/que-es-iso-9000.html

Sánchez C., J. J. (2007, mayo). Algunas aproximaciones al problema de financiamiento de las pymes en Colombia. *Scientia et Technica, XIII* (34).

TI, ITIL-Gestión de Servicios (2011). *Fundamentos de la Gestión TI > ITIL > ¿Qué es ITIL?* Recuperado el 10 de diciembre del 2011, de http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php

Wikipedia la enciclopedia. (s. f.). Normas ISO 9000. Recuperado el 11 de diciembre del 2011, de http://es.wikipedia.org/wiki/ISO_9000.