MARCO DE TRABAJO PARA AUDITORIAS INTEGRALES DE SISTEMAS EN LAS MICROS, PEQUEÑAS Y MEDIANAS EMPRESAS COLOMBIANAS

LUIS CARLOS BRIEVA BERRIO

ROBERTO CARLOS DIAZ ALONSO

CORPORACIÓN UNIVERSITARIA DE LA COSTA CUC

DEPARTAMENTO DE POSTGRADOS

ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS DE INFORMACION

BARRANQUILLA - COLOMBIA

2011

MARCO DE TRABAJO PARA AUDITORIAS INTEGRALES DE SISTEMAS EN LAS MICROS, PEQUEÑAS Y MEDIANAS EMPRESAS COLOMBIANAS

LUIS CARLOS BRIEVA BERRIO

ROBERTO CARLOS DIAZ ALONSO

Trabajo de Grado Para optar el titulo de:
Especialista en Auditoria en Sistemas de Información

Docente de la Asignatura Proyectos de investigación
Mg. VICTOR MANUEL MONTAÑO ARDILA

CORPORACIÓN UNIVERSITARIA DE LA COSTA CUC

DEPARTAMENTO DE POSTGRADOS

ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS DE INFORMACION

BARRANQUILLA - COLOMBIA

2011

CORPORACION UNIVERSITARIA DE LA COSTA CUC
ESPECIALIZACION EN AUDITORIA DE SISTEMAS DE INFORMACION

Nota de Aceptación

_____

_____

_____

_____
Firma del Presidente del jurado

_____
Firma del Jurado

_____
Firma del Jurado

Barranquilla, 30 de Septiembre del 2011

DEDICATORIA

Agradezco a DIOS por todas las cosas que me ha dado y por esta oportunidad para realizar esta especialización. A mis padres Roberto Díaz Mangones y Eneida Josefa Alonso Mercado de Díaz, por su comprensión, paciencia y tolerancia y por su apoyo en los momentos difíciles. A mis hermanos Catherine, Heidy, Fabián, y mi esposa Sirly Sánchez por su apoyo y ayuda. A mi sobrinita Karen Patricia Severiche Díaz por los momentos en los cuales me levantaba el ánimo con sus tiernas preguntas, los doctores Miguel Antequera, Jose Yarzagaray, por la oportunidad que me brindaron, al ofrecerme esta especialización, y Gustavo Quevedo, por su apoyo y colaboración incondicional.

ROBERTO CARLOS

DEDICATORIA

Agradezco a DIOS por todas las cosas que me ha dado y por esta oportunidad de crecimiento profesional y personal a través de esta especialización. A mis padres Farides Margoth Berrío de Brieva y Néstor Eloy Brieva Montes, por su apoyo en los momentos difíciles y su paciente disposición para levantarme en momentos de dificultad. A mi hermana Betty, y mis dos sobrinos Samantha y Henry por toda esa motivación que implica ver a una nueva criatura entregar su afecto sin condiciones ni intereses particulares. Agradezco a Juan Carlos Yepes Montoya, Maria Teresa Villegas, Omar Arteaga, Arturo del Castillo e Ignacio Cortés por permitirme distribuir mi tiempo entre el estudio y el trabajo, para obtener estos resultados, fruto del trabajo colectivo de las personas mencionadas en esta dedicatoria y muchas otras, que de una u otra manera, me tendieron la mano en los momentos de dificultad.

LUIS CARLOS

AGRADECIMIENTOS

Los autores de la presente investigación, expresan sus agradecimientos a:

La Corporación Universitaria de la Costa CUC y al programa de postgrado por darnos la oportunidad de realizar esta especialización.

Nuestros directores de colectivo Ing. Víctor Montaño y Gustavo Quevedo, quien con su apoyo, colaboración y comprensión nos llevo a feliz termino este trabajo.

A nuestros profesores Alfonso López, Gustavo Quevedo, Samuel Mantilla, Lucio Molina, Víctor Montaño, Fernando Ferrer, Gabriel Tavera, Nelson Camargo, Javier Santiago Chinchilla, Juan Hernán Rodríguez, Eduardo González. Por sus enseñanzas y concejos impartidos durante la especialización.

A todos nuestros compañeros de la especialización, y en especial a nuestro grupo de trabajo, por todos los momentos compartidos, tanto de dificultad como de alegría, a todos y cada uno, gracias por la colaboración prestada.

A todos los Estudiantes, Profesores, y Empresas, por su colaboración en la realización de este trabajo.

Barranquilla, 2 de Octubre de 2011

Ingeniero
VICTOR MONTAÑO ARDILA
Coordinador de la especialización Auditoria de Sistemas de Información
Corporación Universitaria de la Costa, CUC
Barranquilla

Cordial saludo

Por medio de la presente hacemos constar que siendo asesores del trabajo de grado de los estudiantes ROBERTO CARLOS DIAZ ALONSO Y LUIS CARLOS BRIEVA BERRIO, titulado: "MARCO DE TRABAJO PARA AUDITORIAS INTEGRALES DE SISTEMAS EN LAS MICROS, PEQUEÑAS Y MEDIANAS EMPRESAS COLOMBIANAS", estamos de acuerdo con los objetivos, alcances obtenidos, propuesta y recomendaciones emitidas en el presente proyecto.

Atentamente,

VICTOR MONTAÑO ARDILA
Coordinador de la especialización auditoria de sistemas de información

GUSTAVO QUEVEDO
Licenciado Proyectos de Investigación

RESUMEN

En el desarrollo de esta investigación se propone un MARCO DE TRABAJO PARA AUDITORIAS INTEGRALES DE SISTEMAS EN LAS MICROS, PEQUEÑAS Y MEDIANAS EMPRESAS COLOMBIANAS.

Con la alineación entre COBIT, ITIL e ISO 27002, ha permitido a las grandes empresas concentrar sus esfuerzos en lograr mayores beneficios para el negocio con una visión más sistémica y menos enfocada al cumplimiento: “La implementación de las mejores prácticas debería ser consistente con el marco de control y la gestión de riesgos de la empresa, apropiada para la empresa e integrada con otras metodologías y prácticas que estén siendo utilizadas. Los estándares y las mejores prácticas no son una panacea; su efectividad depende de cómo se implementan y mantienen. Estas son mucho más útiles cuando son aplicadas como un bloque de principios y como un punto de partida para adaptar procedimientos específicos.

Con 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 optimo de todos los recursos que apoyen los procesos de las Pymes, que contribuirán al mejoramiento de los procesos, dado que éstas no han implementado un marco de referencia para la planificación y organización de la infraestructura tecnológica que deben soportar cada uno de sus procesos.

ABSTRACT:

In developing this research proposes an AUDIT FRAMEWORK FOR INTEGRATED SYSTEMS MICRO, SMALL AND MEDIUM ENTERPRISES COLOMBIAN.

With the alignment between COBIT, ITIL and ISO 27002, has allowed large companies to concentrate their efforts on achieving greater business benefits in a more systemic and less focused on compliance: "The implementation of best practices should be consistent with the control framework and risk management of the company, appropriate to the enterprise and integrated with other methodologies and practices that are being used. The standards and best practices are not a panacea, its effectiveness depends on how they are implemented and maintained. These are most useful when applied as a block of principles and as a starting point for adapting specific procedures.

This research gives the SMEs an opportunity to align the strategies of each standard with the strategies they want to accomplish, to achieve the optimum use of all resources to support the processes of SMEs, which contribute to the improvement of processes, because they have not implemented a framework for planning and organization of the technological infrastructure that must support each of its processes.

PALABRAS CLAVES:

Gobierno de TI, Seguridad de la Información, COBIT, ITIL, ISO 27002, COSO, Alineación, auditoría de Sistemas**.** Dominios, Procesos, Actividades, Objetivos de Control.

KEY WORDS:

IT Governance, Information Security, COBIT, ITIL, ISO 27002, COSO, alignment, Systems audit, Domains, Processes, Activities, Control Objectives

TABLA DE CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

INTRODUCCION

En este documento se determinara si la Auditoría de Sistemas enfocada solo al cumplimiento normativo no representa ningún tipo de interés para los gerentes, más allá que, en el mejor de los casos, cumplir con la ley. Este tipo de escenarios demuestran día a día que cada vez se hace más necesaria la integración de los estándares internacionales para lograr auditorias verdaderamente efectivas que garanticen un gobierno corporativo de TI gestionable y acorde a 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" (Las siglas de ITIL significan (Information Technology Infrastructure Library o Librería de Infraestructura de Tecnologías de Información). Metodología desarrollada a finales de los años 80's por iniciativa del gobierno del Reino Unido, específicamente por la OGC u Oficina Gobernativa de Comercio Británica (Office of Goverment Comerce).

Esta metodología es la aproximación más globalmente aceptada para la gestión de servicios de Tecnologías de Información en todo el mundo, ya que es una recopilación de las mejores prácticas tanto del sector público como del sector privado.)"[1]. COBIT "(es precisamente 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.)"[2]. ISO 2700X(ISO/IEC 17799 "(denominada también 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 año 2000)"[3] e ISO 9000"(ISO 9000 designa un conjunto de normas sobre calidad y gestión continua de calidad, establecidas por la Organización Internacional para la Estandarización (ISO")[4]. Se pueden 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

[1] http://www.monografias.com/trabajos31/metodologia-itil/metodologia-itil.shtml
[2] http://www.channelplanet.com/index.php?idcategoria=13932
[3] http://es.wikipedia.org/wiki/ISO_27002
[4] http://es.wikipedia.org/wiki/ISO_9000

como aspectos esenciales el Gobierno de TI, la Gestión del Servicio, Seguridad de la Información y Teoría de Riesgos, en concordancia con los tres grandes tópicos que exige la auditoría de hoy y a nivel de cascada: Gobierno, Riesgos, Control.

Es así como hoy en día la auditoría se concibe al interior de las organizaciones 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."[5]

[5] JIMENEZ, Armando. Historia de la Auditoría. www.monografías.com

0.1. PLANTEAMIENTO DEL PROBLEMA

Desde los orígenes de la actividad económica mundial los comerciantes, hoy empresarios, han encontrado como una necesidad imperante establecer mecanismos de control que les permitiese conocer con certeza cuanta riqueza poseían y producían. Es así como en estos albores de la economía, aparece la contabilidad como un medio fundamental de control de la riqueza, permitiendo establecer asignaciones de recursos de acuerdo a una priorización de las necesidades; pasando por diferentes etapas de la humanidad hasta llegar a la decisiva Revolución Industrial que crea las condiciones básicas en las que se movería la economía capitalista: La automatización de las labores más operativas, concentrando al recurso humano hacia labores cada vez más especializadas y por otro lado, la racionalización de la producción y la riqueza como producto de esta primera condición.

Llegando al momento actual de la economía mundial, donde los grandes grupos económicos toman el control de los mercados en detrimento de las empresas más débiles, es de destacar uno de los hechos que está influyendo en forma decisiva en el ahondamiento de dicha brecha: La integración de los sistemas informáticos, que permiten obtener información decisiva para la toma de decisiones en un tiempo cada vez menor para un mundo más acelerado. La información procesada en los sistemas de información está dirigida a dos grandes grupos: los clientes Internos y Externos. Estos exigen que la información presentada sea confiable y para ello se busca la opinión de un tercero que certifique los datos que se procesaron antes, por ello los auditores buscan asegurar los sistemas de información los cuales deben proveer una seguridad razonable de los datos que son previamente procesados, disminuyendo el margen de error que puedan presentar; con esto se asegura que los datos procesados estén acorde con las exigencias requeridas.

Pero más allá de enfocarse la tecnología como recurso para la generación de información financiera, hoy en día el factor tecnológico es decisivo en la innovación de los procesos, productos y servicios ofrecidos; empresa que no esté dispuesta a ello, está destinada a la pérdida de su mercado y como consecuencia de ello a la quiebra. El tema es de suma relevancia a nivel de la actividad económica y en especial, a nivel de microempresas, pequeñas y medianas empresas; si consideramos las dimensiones que este representa en el total de la actividad productiva nacional: “Representan el 96.4% de los establecimientos, aproximadamente el 63% del empleo; el 45% de la producción

manufacturera, el 40% de los salarios y el 37% del valor agregado. Son más de 650.000 empresarios cotizando en el sistema de seguridad social"[6]. ¿Cómo incorporar el uso de las Tecnologías de Información a los procesos de negocio de la compañía, a la cadena de valor de la misma?

Las Mipymes ofrecen hoy un gran reto a los nuevos profesionales, entre estos tal vez el más importante es ¿Cómo aumentar la productividad, crecer y mantener la tecnología sin que esto signifique dejar de aumentar el nicho de mercado y seguir generando utilidades para ser sostenibles? Es una pregunta que desde distintas áreas merece ser respondida, pero sólo un enfoque sistémico logrará que se logre crear un solo sistema integrado de gestión que contemple y armonice mundos como la calidad, seguridad y salud ocupacional, ambiental y las mejores prácticas financieras y contables. Semejante sinergia si bien no es fácil de alcanzar, si es un reto que merece ser iniciado desde las distintas áreas del conocimiento: Contabilidad, Ingenierías (Sistemas, Industrial, Procesos), Administración y… tal vez como la más importante para lograr tal cambio se encuentra la Auditoría como aquella disciplina que presta sus servicios de aseguramiento a las organizaciones en la consecución de sus objetivos.

De modo similar los sistemas de información deben ser capaces de soportar tal concordancia mediante su armonización interna, soportando las mejores prácticas en Control Interno, Seguridad de la Información, Calidad, Gestión de Servicios informáticos y Gestión de Riesgos, dando lugar, para el mantenimiento del sistema a servicios de aseguramiento de auditores de sistemas tanto internos como externos a la organización quienes de manera similar, deben poseer un cúmulo de conocimientos integrados entre los diferentes frentes que componen el mundo de TI, que creen soluciones –recomendaciones en el mundo de la auditoría- que aporten un verdadero valor agregado e integrador entre las diferentes normas técnicas, estándares y mejores prácticas mundiales.

En este sentido cabe destacar el gran trabajo que ha efectuado IT Governance Institute en relación a la armonización de estándares y buenas prácticas, otorgando de herramientas útiles a la alta dirección para capitalizar de mejor forma sus esfuerzos. El alineamiento entre COBIT, ITIL e ISO 27002, ha permitido a las grandes empresas concentrar sus esfuerzos en lograr mayores beneficios

[6] BUSINESS SCHOOL. Negociemos con Colombia. http://www.businesscol.com/empresarial/pymes/

para el negocio con una visión más sistémica y menos enfocada al cumplimiento: "La implementación de las mejores prácticas debería ser consistente con el marco de control y la gestión de riesgos de la empresa, apropiada para la empresa e integrada con otras metodologías y prácticas que estén siendo utilizadas. Los estándares y las mejores prácticas no son una panacea; su efectividad depende de cómo se implementan y mantienen. Estas son mucho más útiles cuando son aplicadas como un bloque de principios y como un punto de partida para adaptar procedimientos específicos. Para evitar prácticas que nunca se pongan en ejecución ('shelfware'), la dirección y el staff deben entender lo que hay que hacer, cómo hacerlo y porqué es importante hacerlo."[7]

Desde este punto de vista debemos plantearnos las siguientes preguntas:

¿Es posible integrar un Marco de Trabajo con las diferentes normas técnicas, estándares y mejores prácticas mundiales a nivel de TI y Control Interno para la realización de Auditorías Integrales de Sistemas en las Micros, Pequeñas y Medianas Empresas Colombianas?

¿Es posible crear un Marco de Trabajo para Auditorias Integrales de Sistemas en las Micros, Pequeñas y Medianas Empresas Colombianas?

- ¿Identifica la forma como la auditoría de sistemas, a partir de un marco integrado entre los estándares y normas técnicas mencionadas, contribuye en el encuentro de oportunidades de mejora en las Mipymes colombianas?
- ¿Desarrolla un marco referencial base que abarque el universo auditable de las Mipymes en su conjunto, adaptable a sus particularidades de acuerdo a su agrupamiento productivo?
- ¿Contribuye con una metodología que apunte a arrojar auditorías de costo razonable para las Mipymes, así como oportunidades de mejora pertinentes con su realidad económica?

[7] Alineando COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 en Beneficio de la Empresa. IT Governance Institute. Pag 11. 2008

0.2. JUSTIFICACION E IMPORTANCIA DEL ESTUDIO

El contexto de esta investigación apunta al estudio concienzudo del impacto que las Tecnologías de Información tienen en el mundo empresarial hoy como factor diferenciador de las empresas, pero sobre todo se enfoca en como la Auditoría como profesión proveedora de servicios de Aseguramiento y Consultoría –este trabajo se enfocará al Aseguramiento solamente- puede jugar un papel determinante como aliada de la administración para el descubrimiento de oportunidades de mejora que redunden en mejores sinergias en la relación Tecnología – Estrategia Organizacional.

En el entorno empresarial moderno no se duda en un instante en acudir a estándares, normas técnicas, regulación y mejores prácticas para encontrar soluciones estratégicas a la pregunta básica de cómo gestionar una organización, en especial y en nuestro caso particular, desde lo tecnológico. Todo este cúmulo de guías existe y son ampliamente utilizadas y difundidas en las grandes corporaciones, pero en las Mipymes, en especial las colombianas, estas prácticas aún parecen lejanas; y surgen muchas dificultades en el momento de su implantación. Sólo la articulación concienzuda de estos estándares, orientados hacia un denominador común –Control Interno, Gobierno de TI, Servicios Empresariales, Gestión de Riesgos y/o Seguridad de la Información- permitirá encontrar soluciones que se alejen del hasta ahora altamente investigado campo teórico y profundicen en el quehacer práctico de las Mipymes en una implantación que sea Costo-Eficiente, diferenciadora de la competencia y propenda por el aseguramiento del éxito empresarial, este ultimo campo de nuestro quehacer auditor.

No obstante aunque el caso colombiano es crítico, vale la pena reseñar el escenario europeo, para hacernos una idea de la problemática que enfrentamos “La Business Software Alliance (BSA) ha elaborado un estudio en el que asegura que la mayoría de las pymes europeas no cuentan con políticas de software ni realizan auditorías de sistemas, unas prácticas que hacen peligrar la seguridad de estas empresas. Ignorar las consecuencias legales que el uso del software pirata conlleva para las pymes es peligroso. Así lo asegura la BSA en un estudio que ha realizado entre 2.000 pymes de Europa Occidental (concretamente de los países Reino Unido, España, Suecia, Alemania, Francia, Italia, Bélgica y Holanda) y en el que pone de manifiesto, según la asociación, la

"actitud negligente" que muchos directores de pequeñas y medianas empresas mantiene en lo referente a la piratería y la gestión de los sistemas informáticos"[8].

Los principales datos emanados del estudio son que un 37% de las compañías encuestadas reconocen no tener directrices para proteger sus sistemas informáticos de posibles abusos cometidos por sus empleados. Asimismo, el informe concluye que menos del 50% de las pymes europeas realizan regularmente auditorías de sistemas.

Es de anotar que el estudio nos demuestra que una Auditoría de Sistemas enfocada solo al cumplimiento normativo no representa ningún tipo de interés para los gerentes, más allá que, en el mejor de los casos, cumplir con la ley. Este tipo de escenarios demuestran día a día que cada vez se hace más necesaria la integración de los estándares internacionales para lograr auditorias verdaderamente efectivas que garanticen un gobierno corporativo de TI gestionable y acorde a 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 COSO, ITIL, COBIT, ISO 2700X y el enfoque al cliente de ISO 9000, así como procedimientos de Administración de Riesgos, con el fin de tener en cuenta como aspectos esenciales el Gobierno de TI, la Gestión del Servicio, Seguridad de la Información y Teoría de Riesgos, en concordancia con los tres grandes tópicos que exige la auditoría de hoy y a nivel de cascada: Gobierno, Riesgos, Control.

De ahí que la investigación acometida pretenda dilucidar un camino factible en la consecución de la articulación de los estándares internacionales CObIT, ISO 27001, ISO 9000 e ITIL junto al enfoque al cliente de ISO 9000 en pro de elaborar unas guías de auditoría que ofrezcan una solución económica, oportuna y beneficiosa para la realización de auditorías en las Mipymes Colombianas.

[8] http://www.idg.es/computerworld/Menos-del-50-por-ciento-de-las-pymes-de-Europa-Occ/seccion-ti/articulo-133041

0.3. OBJETIVOS

0.3.1 Objetivo General

Generar un Marco de Trabajo articulado con las diferentes normas técnicas, estándares y mejores prácticas mundiales a nivel de TI y Control Interno para la realización de Auditorías Integrales de Sistemas en las Micros, Pequeñas y Medianas Empresas Colombianas?

0.3.2 Objetivo Específicos

0.3.2.1. Identificar la forma como la auditoría de sistemas, a partir de un marco integrado entre los estándares y normas técnicas mencionadas, contribuye en el encuentro de oportunidades de mejora en las Mipymes colombianas.

0.3.2.2. Desarrollar un marco referencial base que abarque el universo auditable de las Mipymes en su conjunto, adaptable a sus particularidades de acuerdo a su agrupamiento productivo.

0.3.2.3. Contribuir con una metodología que apunte a arrojar auditorías de costo razonable para las Mipymes, así como oportunidades de mejora pertinentes con su realidad económica.

0.4. DELIMITACIONES

0.4.1 Delimitación Espacial

Esta investigación tendrá como marco de acción el entorno empresarial de las Mipymes en el territorio nacional, ya que se hará un análisis y articulación entre los estándares COSO, CObIT e ITIL y normas técnicas ISO 27001, con un enfoque al cliente basado en ISO 9000, direccionado hacia los requisitos y objetivos de control estrictamente necesarios para una adecuada armonización en atención a la realidad nacional de las Mipymes, como representación del 96.4% de los establecimientos de comercio nacionales.

0.5. MARCO TEÓRICO Y ESTADO DEL ARTE

0.5.1. Antecedentes y Teorías Básicas del Problema

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 Microempresas, Pequeñas y Medianas Empresas: "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"[9].

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, tales como la Contabilidad, Administración y a nivel de 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 medidas (SIC) que se desarrollo 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 auditoria como profesión fue reconocida por primera vez bajo la Ley Británica de Sociedades Anónimas de 1862 y el reconocimiento general tuvo lugar durante el período de mandato de la Ley"[10] "Un sistema metódico y normalizado de contabilidad era deseable para una adecuada información y para la prevención del fraude". También

---

[9] SÁNCHEZ C., John Jairo, OSORIO G., Jaime, BAENA M., Ernesto. Algunas aproximaciones al problema de financiamiento de las PYMES en Colombia. Universidad Tecnológica de Pereira. Scientia et Technica Año XIII, No 34, Mayo de 2007.

[10] www.actiweb.es/msucreseccion29infysis/archivo1.pdf

reconocía..."Una aceptación general de la necesidad de efectuar una versión independiente de las cuentas de las pequeñas y grandes empresas"[11]. Como vemos, en estos humildes inicios, la auditoría tenía una misión importante encomendada: Garantizar la adecuación de la información financiera a los registros contables.

Dada la significativa evolución que a través del tiempo presentaron las herramientas contables, la auditoría avanza de la contabilización minuciosa de transacciones a la utilización de la estadística y a la entrega de nuevos productos a las organizaciones. Es así como comenzamos a hablar en la auditoría de aspectos administrativos, laborales, operacionales y… alrededor de 1960 de Auditoría a Sistemas de Información, "A medida que los auditores independientes se apercibieron de la importancia de un buen sistema de control interno y su relación con el alcance de las pruebas a efectuar en una auditoría independiente, se mostraron partidarios del crecimiento de los departamentos de auditoría dentro de las organizaciones de los clientes, que se encargaría del desarrollo y mantenimiento de unos buenos procedimientos del control interno, independientemente del departamento de contabilidad general. Progresivamente, las compañías adoptaron la expansión de las actividades del departamento de auditoría interna hacia áreas que están más allá del alcance de los sistemas contables"[12].

Es así como hoy en día la auditoría se concibe al interior de las organizaciones 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."[13]

De esta definición caben destacar varios aspectos importantes: 1) Utilización: El hecho de que los sistemas de información tengan un uso –y por consiguiente un valor de uso-, nos lleva a pensar en los SI como un *servicio*, que por sí solo, si bien no determina el éxito organizacional, si ayuda a su consecución, 2) Controles: Los sistemas de información, en sí mismos deben poseer mecanismos

11 JIMENEZ, Armando. Historia de la Auditoría. www.monografías.com

12 JIMENEZ, Armando. Historia de la Auditoría. www.monografías.com

13 JIMENEZ, Armando. Historia de la Auditoría. www.monografías.com

adecuados de control que permitan minimizar errores y/o la ocurrencia de fraudes, 3) Eficiencia: Los servicios prestados por TI deben ser vistos como generadores o propulsores de la generación de valor dentro de la organización, 4) Seguridad: Los sistemas de información si bien permiten una mayor agilidad en los negocios, también son un foco de mayores vulnerabilidades, que dependiendo de su criticidad y el apetito por el riesgo de la organización debe ser asumido y posteriormente minimizado, hasta dejar un riesgo residual consciente y tolerable. Podemos notar que para cada uno de estos elementos, a nivel internacional existen unas mejores prácticas que deben ser observadas: para la gestión del servicio se observa ITIL, para la Seguridad de la información, el estándar adecuado es la familia de ISO:2700X, y para la implementación del adecuado gobierno corporativo de TI –como articulador último de TI, sus objetivos y los de la organización- existe COBIT, el cual se encuentra alineado con COSO, y como garante de la calidad de los procesos ejecutados en las organizaciones la familia ISO 9000.

A nivel normativo, en Colombia la práctica de la auditoría tiene algunos guiños en la normatividad, tales como la Ley 45 de 1990, que versa en su Artículo 9o. "*De los papeles de trabajo. Mediante papeles de trabajo, el Contador Público dejará constancia de las labores realizadas para emitir su juicio profesional. Tales papeles, que son propiedad exclusiva del Contador Público, se preparan conforme a las normas de auditoría generalmente aceptadas*", en el artículo 25, numeral 3 de la suspensión "*Actuar con (manifiesto) quebrantamiento de las normas de auditoría generalmente aceptadas"*, y en el articulo 33 aparece como obligación del Consejo Técnico de la Contaduría Pública en el numeral 1 "*Adelantar investigaciones técnico científicas, sobre temas relacionados con los principios de contabilidad y su aplicación, y las normas y procedimientos de auditoría.*" Pero en temas de Auditoría propiamente dichos la aplicación de los estándares internacionales es hoy por hoy, la fuente de información utilizada con mayor frecuencia por los profesionales del área. Sin embargo a nivel de marcos de gobierno o sistemas de Gestión, en el sector público encontramos la aplicación de la NTCGP:1000 y MECI, para el sector financiero encontramos SARO, como el Sistema de Administración de Riesgos Operativo o ISO NTC 5254 a nivel de Administración de Riesgos globales en la compañía.

Es necesario resaltar, sin embargo que los estándares internacionales han sido desarrollados para las grandes corporaciones y que, para las Pequeñas y Medianas Empresas es poco lo que se ha avanzado al respecto. Un buen punto de referencia, a nivel de auditoría, son la aplicación de las ISA

a nivel financiero o el COBIT Quickstart, Gobierno de TI; para la realización de auditorías e implementación de gobierno respectivamente, a nivel de PYMES –insumo importante para nuestra labor-, que lleva a nivel de detalle, cuáles de estas normas tienen aplicabilidad en este tipo de empresas.

Un dato interesante, que puede ser extrapolado a otros sectores económicos es lo acontecido en el sector financiero: "Las instituciones financieras más grandes, si bien tienden a operar en un número más grande de jurisdicciones, con mayores exigencias de cumplimiento, gastan en promedio el 4% de su base total de gastos en las actividades de gobierno y cumplimiento. En contraste, las instituciones financieras más pequeñas gastan en promedio el 6% de sus gastos totales"[14]

Dada la abundancia de herramientas conceptuales que existe –entre estándares y normas técnicas-, tratadas muy a menudo de forma separada, cabría preguntarse ¿Es posible articular estos estándares en las auditorías efectuadas a las PYMES colombianas con el fin de generar recomendaciones integrales en este tipo de empresas cuya capacidad de lograr economías de escala es menor?.

[14] MANTILLA B., Samuel Alberto. Control Interno Efectivo. Hacia un nuevo estándar internacional. Deloitte & Touche Ltda. - Ed. Planeta Colombiana S.A. Pags 23-24

0.6. DISEÑO METODOLOGICO

0.6.1. Tipo de Estudio

El desarrollo de esta investigación, será de carácter descriptivo, en la cual se detallarán las características fundamentales de los estándares y normas internacionales mencionados anteriormente, con la finalidad de analizar y encontrar los objetivos comunes entre los ya nombrados, con el fin de integrarlos y elaborar un marco referencial para efectuar auditorías de sistemas en observancia de todas estos marcos conceptuales para las Mipymes. El enfoque que se manejara en esta investigación es cuantitativo-cualitativo por cuanto requiere algunos datos de las Mipymes a nivel de encuestas y su posterior tratamiento estadístico, pero la integración de los marcos conceptuales será a nivel de la teoría que estos presentan.

0.6.2. Método de Estudio.

Para el logro de los objetivos propuestos en esta investigación, se utilizara el método inductivo-deductivo, ya que partiremos de situaciones particulares, estudiando el comportamiento que ha tenido el sector de las Mipymes en la economía colombiana a nivel de TI, para llegar a unas conclusiones que nos indique las necesidades del sector a nivel de Auditoría de Sistemas; a su vez de esas necesidades identificadas partiremos a estudiar el marco general de cada estándar y/o norma técnica (COBIT, ITIL, ISO 2700x, ISO 900X).

0.6.3. Técnicas de Recolección de Información.

Para la recolección de la información se emplearán las fuentes primaria y secundaria, para la primera cuya técnica serán la ejecución de encuestas y su posterior cotejo y análisis –fuente primaria-, y para la segunda la documental con sus fuentes principales como internet, las bibliotecas públicas y privadas, revistas económicas, informe de prensa, memorias de grado y organismos estatales, etc. que contribuirán al enriquecimiento del estudio para que sea lo más veraz.

CAPITULO I

0.7. GENERALIDADES DE LOS ESTANDARES INTERNACIONALES, NORMAS TECNICAS Y PYMES

0.7.1. Antecedentes Sobre las Normas Técnicas y Estandares Internacionales

En nuestro entorno, se hace cada vez más común que en las grandes empresas se haga mención de las mejores prácticas a nivel mundial en relación a 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.

Con el objetivo de lograr una sincronización exitosa entre TI y el negocio, surge en Inglaterra a finales de los años ochenta, 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"[15]. Así mismo 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) sólo 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."[16]

[15] http://itil.osiatis.es/Curso_ITIL/. Pag 2
[16] http://itil.osiatis.es/Curso_ITIL/. Pag 2

Por otra parte, el desarrollo vertiginoso en las redes informáticas trajo consigo un aumento considerable en la velocidad de procesamiento y transmisión de información del negocio, pero con riesgos cada vez mayores en lo referente a seguridad de los datos transportados por estos medios y, en este sentido, vemos como 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. Es por ello que, reconociendo el amplio espectro que implica el concepto de Seguridad de la Información, se decide acoger como un estándar certificable la ISO 17799 –anteriormente BS (British Standard) 7799/1999- en el 2005 y convertir 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 sólo es llevar un código de mejores prácticas sino establecer un estándar certificable de forma similar al ISO 9000 (el primero de esa serie en publicarse fue el ISO 27001)."[17] Las ventajas a nivel 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 si mismo ya es una garantía razonable de que, a raíz de una buena implementación, mejorarán los procesos involucrados, 3) El implementar "la mejor forma" de realizar los procesos implica ahorros considerables a las compañías en términos de tiempo, recursos empleados, cumplimiento del marco legal aplicable –si se adapta la norma certificable a la realidad normativa del entorno del negocio-; todo esto repercutiendo 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.

[17] http://seguinfo.wordpress.com/2007/09/02/la-evolucion-del-estandar-iso-27001/

Similar a la familia de normas técnicas ISO 2700X; se encuentra "regulando" a nivel de 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: "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."[18] De allí esta norma se derivo 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 explicita del concepto de mejora continua y el monitoreo y seguimiento de la satisfacción del cliente, así como 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, mapear los requerimientos de las diferentes normas técnicas en cuestión. Como ejemplo podríamos citar los anexos de la norma ISO 27002 que mapea a 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,

[18] http://www.misrespuestas.com/que-es-iso-9000.html

orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso"[19]; de esta manera CObIT se ha convertido 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."[20]. Entendiendo el punto de vista del autor vemos que en 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. Tal afirmación es sustentada por "CObIT is based on established frameworks, such as the Software Engineering Institute's CMM, ISO 9000, ITIL and ISO/IEC 27002. However, CObIT does not include process steps and tasks because, although it is oriented towards IT processes, it is a control and management framework rather than a process framework. CObIT focuses on what an enterprise needs to do, not how it needs to do it, and the target audience is senior business management, senior IT management and auditors."[21] (CObIT se basa en marcos de referencia establecidos, tales 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. 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, ITIL, y las normas técnicas ISO/IEC 9000 e ISO/IEC 27000 son sustancialmente diferentes, la construcción de CObIT esta basada en distintos marcos de referencia a nivel mundial y, por ello partiendo de CObIT como elemento de cohesión se puede obtener un alineamiento consistente entre las mencionadas normas

[19] http://www.channelplanet.com/index.php?idcategoria=13932
[20] http://www.channelplanet.com/index.php?idcategoria=13932
[21] Aligning CObIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit. IT Governance Institute. Pag 11. 2008

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.”[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 normas como ITIL e ISO / IEC 27002 cubren áreas especificas y se pueden mapear con el marco de referencia CObIT, proporcionando así 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 “como 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 a auditar en las PyMES.

[22] Aligning CObIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit. IT Governance Institute. Pag 22. 2008

CAPITULO II

0.8. DESARROLLO DE LAS PYMES: EL PAPEL DE LAS AUDITORÍAS COMBINADAS DE TI

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."[23] Es de anotar de la presente definición que la globalización es un proceso y como tal posee dinamismo, este último impulsado gracias 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 TICs y el Internet."[24] 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."*[25](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 tecnología de la información (TI) y el uso de TI para impulsar el valor de sus accionistas. Estas empresas también entienden y gestionar 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

23 http://es.wikipedia.org/wiki/Globalizaci%C3%B3n

24 http://es.wikipedia.org/wiki/Globalizaci%C3%B3n

25 COBIT Quickstart. IT Governance Institute. Pag 8. 2d Edition. 2007

locales, como anteriormente sucedía con la atenuante de que todos ellos conocen con claridad el papel que TI juega 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 coste y plazo adecuados debido a su mayor riesgo. Para solucionar esto se recurren a las 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 éstas.
- 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."[26]

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."[27] No obstante en presentar las PYMES esta enorme ventaja, encontramos a las Pequeñas y Medianas Empresas rezagadas en materia de TI (en incluso de otras disciplinas), las cuales no encuentran en este tema algo interesante para aportarle a sus negocios, por una razón fundamental: "Muchas empresas no manejan IT de una manera cohesiva, sino más bien distribuida, lo cuál deriva en islas de hardware, software, servicios de telecomunicaciones, cada quien respondiendo por sus respectivos departamentos, sin ver el servicio completo al usuario final"[28]. Esta visión incompleta y fragmentada del universo TI genera desconfianza en la alta dirección (trátese en las PyMES de un organismo colegiado, gerente, o

26 http://es.wikipedia.org/wiki/Peque%C3%B1a_y_mediana_empresa

27 http://es.wikipedia.org/wiki/Peque%C3%B1a_y_mediana_empresa

28 www.intraemprendedor.com/2006/09/26/itil-un-resumen-enfocado-a-pymes/

gerente-propietario) que no encuentra valor agregado para alcanzar los objetivos del plan de negocios.

Esta percepción de los dueños de negocios PyMES de 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 IT sigue vigente sin importar el tamaño de la empresa"[29]; para abordar el reto existen las buenas prácticas y normas técnicas respectivas de acuerdo a la materia de estudio, que pueden jugar un papel crucial para el desarrollo de las PyMES por cuanto, 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 a la capacidad de consecución de recursos de la compañía y los objetivos a 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."*[30] (El motor detrás de CObIT Quickstart es la necesidad de los administradores de TI de las organizaciones más pequeñas de una herramienta sencilla de usar que acelerará la aplicación de los principales objetivos de control de 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*

29 www.intraemprendedor.com/2006/09/26/itil-un-resumen-enfocado-a-pymes/

30 COBIT Quickstart. IT Governance Institute. Pag 15. 2d Edition. 2007

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."[31] (CObIT puede ser utilizado al más alto nivel de Gobierno de TI, proporcionando un marco de control general basada en un modelo de proceso de TI provisto por ITGI para adaptarse a cada empresa de forma genérica. También hay una necesidad de procesos detallados, de procesos prácticos estandarizados. Las prácticas y normas específicas, tales como ITIL e ISO / IEC 27002, cubrir áreas específicas y se pueden mapear al marco CObIT, proporcionando así una jerarquía de materiales de orientación).

Así, 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 TI a la gestión de la calidad (ISO/IEC 9000) o se debe evaluar primero la calidad y luego adentrarnos en el mundo 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 TI, en nuestro caso ITIL, CObIT e ISO/IEC 27002)? La pregunta debe ser resuelta de acuerdo a las circunstancias particulares de cada PyME así, si lo que queremos es efectuar una auditoría integral enfocada hacia TI lo correcto es alinear la norma técnica de calidad a los requerimientos del mundo TI, pero si nuestra intención es realizar una auditoría de calidad y adicionar un valor agregado evaluando algunos aspectos detallados de TI, lo mas conveniente es arrancar desde ISO/IEC 9000 y alinear los requisitos de la norma a los requerimientos del mundo TI. En nuestro caso de estudio partiremos desde la primera óptica ya que nuestro objetivo son las auditorías integrales de TI para las PyMES.

[31] Aligning CObIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit. IT Governance Institute. Pag 7. 2008

CAPITULO III

0.9. UNIVERSO DE AUDITORIA 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 a nivel mundial en relación a 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.

Es, de este modo como en 1992 a raíz de 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.” Así, este comité define los siguientes objetivos y componentes en su marco de control, mediante la siguiente interacción:

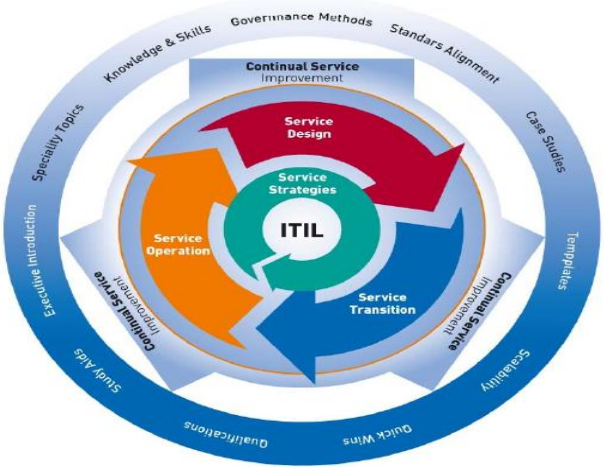
FIGURA 1. RELACION ENTRE OBJETIVOS Y COMPONENTES

Fuente: Los nuevos conceptos del control interno. Informe COSO (Modelo de Control COSO – Objetivos & Componentes de Control) - http://www.mercadotendencias.com/informe-coso-definicion-de-control-interno/

Por otra parte, con el objetivo de lograr una sincronización exitosa entre TI y el negocio, surge en Inglaterra a finales de los años ochenta, 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"[32]. Así mismo 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) sólo 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."[33]

32 http://itil.osiatis.es/Curso_ITIL/. Pag 2
33 http://itil.osiatis.es/Curso_ITIL/. Pag 2

FIGURA 2. MODELO DE GESTION DEL SERVICIO ITIL



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

Por otro lado, el desarrollo vertiginoso en las redes informáticas trajo consigo un aumento considerable en la velocidad de procesamiento y transmisión de información del negocio, pero con riesgos cada vez mayores en lo referente a seguridad de los datos transportados por estos medios y, en este sentido, vemos como 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. Es por ello que, reconociendo el amplio espectro que implica el concepto de Seguridad de la Información, se decide acoger como un estándar certificable la ISO 17799 –anteriormente BS (British Standard) 7799/1999- en el 2005 y convertir 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 sólo es llevar un código de mejores prácticas sino

establecer un estándar certificable de forma similar al ISO 9000 (el primero de esa serie en publicarse fue el ISO 27001)."[34]

Las ventajas a nivel 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) El implementar "la mejor forma" de realizar los procesos implica ahorros considerables a las compañías en términos de tiempo, recursos empleados, cumplimiento del marco legal aplicable –si se adapta la norma certificable a la realidad normativa del entorno del negocio-; todo esto repercutiendo 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.

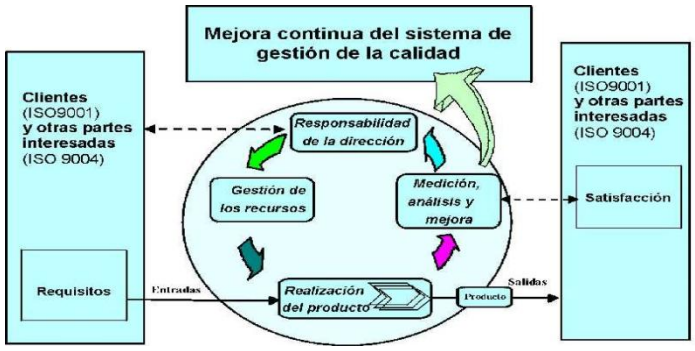
FIGURA 3. MODELO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION (CÍRCULO DE DEMING)

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

[34] http://seguinfo.wordpress.com/2007/09/02/la-evolucion-del-estandar-iso-27001/

Similar a la familia de normas técnicas ISO 2700X; se encuentra "regulando" a nivel de 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: "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."[35] 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 monitoreo y seguimiento de la satisfacción del cliente, así como se han eliminado gradualmente los requerimientos documentales que entorpecen la labor de la organización.

FIGURA 4. MODELO DEL SISTEMA DE GESTION 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

35 http://www.misrespuestas.com/que-es-iso-9000.html

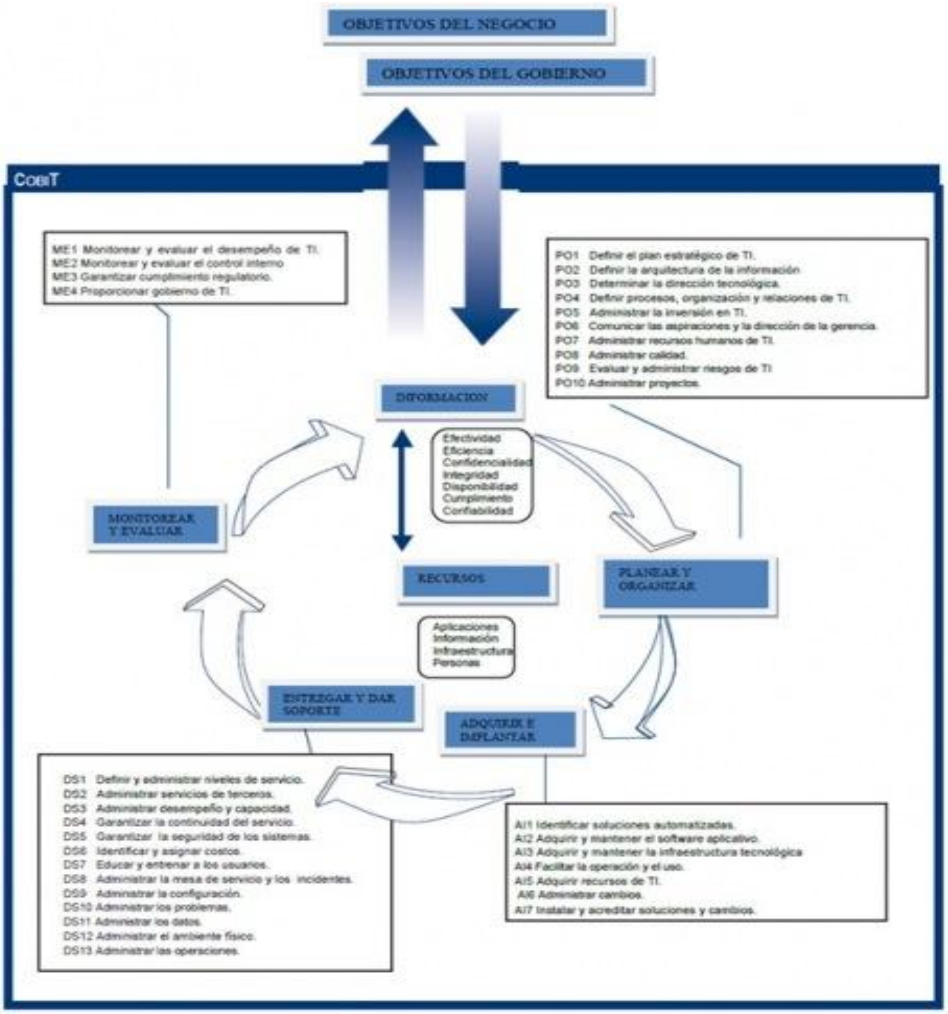
Actualmente se ha convertido en lugar común para diferentes autores estudiosos de los sistemas de gestión, mapear los requerimientos de las diferentes normas técnicas en cuestión. Como ejemplo podríamos citar los anexos de la norma ISO 27002 que mapea a esta norma con los requisitos exigidos por la ISO 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"[36]; de esta manera CObIT se ha convertido 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."[37].

36 http://www.channelplanet.com/index.php?idcategoria=13932

37 http://www.channelplanet.com/index.php?idcategoria=13932

FIGURA 5. MARCO DE TRABAJO GENERAL DE COBIT



Fuente: IT Governance Institute, Cobit 4.1 – Isaca - Modelo CobIT

Entendiendo el punto de vista del autor vemos que en CObIT confluyen algunos elementos comunes a los anteriores marcos de referencia y normas técnicas citadas: Seguridad (ISO 27001), procesos (ITIL) y 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. Tal afirmación es sustentada por “CObIT is based on established frameworks, such as the Software.

Engineering Institute's CMM, ISO 9000, ITIL and ISO/IEC 27002. However, CObIT does not include process steps and tasks because, although it is oriented towards IT processes, it is a control and management framework rather than a process framework. CObIT focuses on what an enterprise needs to do, not how it needs to do it, and the target audience is senior business management, senior IT management and auditors."[38] (*CObIT se basa en marcos de referencia establecidos, tales 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. 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*).

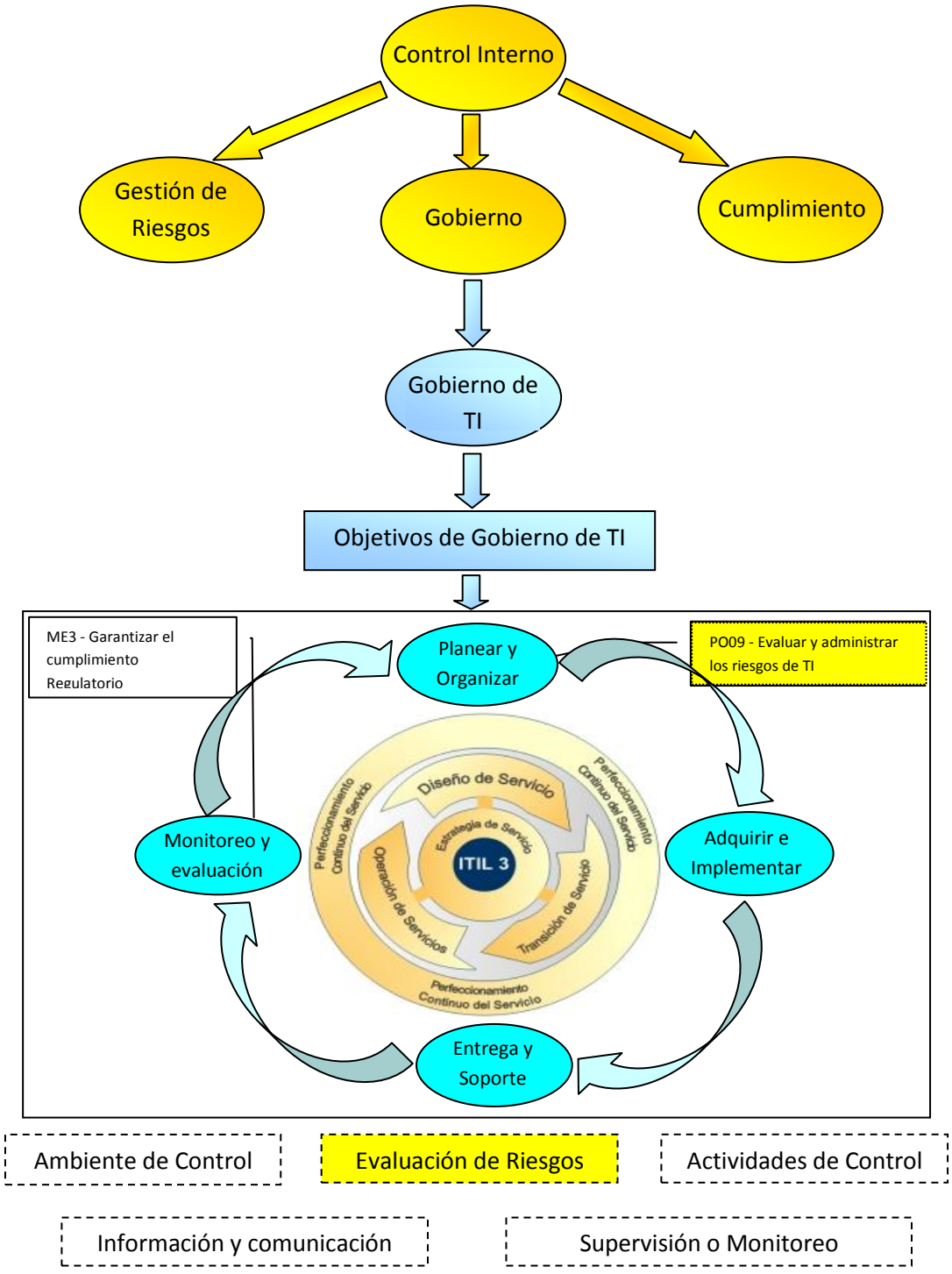
Partiendo de esta premisa tenemos que, si bien los objetivos de CObIT, ITIL, y las normas técnicas ISO/IEC 9000 e ISO/IEC 27000 son sustancialmente diferentes, la construcción de CObIT esta basada en distintos marcos de referencia a nivel mundial y, por ello partiendo de CObIT como elemento de cohesión 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."[39] *(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 normas como ITIL e ISO / IEC 27002 cubren áreas específicas y se pueden mapear con el marco de referencia CObIT, proporcionando así una jerarquía de materiales de orientación.).*

38 Aligning CObIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit. IT Governance Institute. Pag 11. 2008

39 Aligning CObIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit. IT Governance Institute. Pag 22. 2008

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”, incluyendo COSO e ITIL ¿Cuál es la mejor manera de integrar los diversos estándares y normas técnicas enfocadas a la realidad de las PyMES?

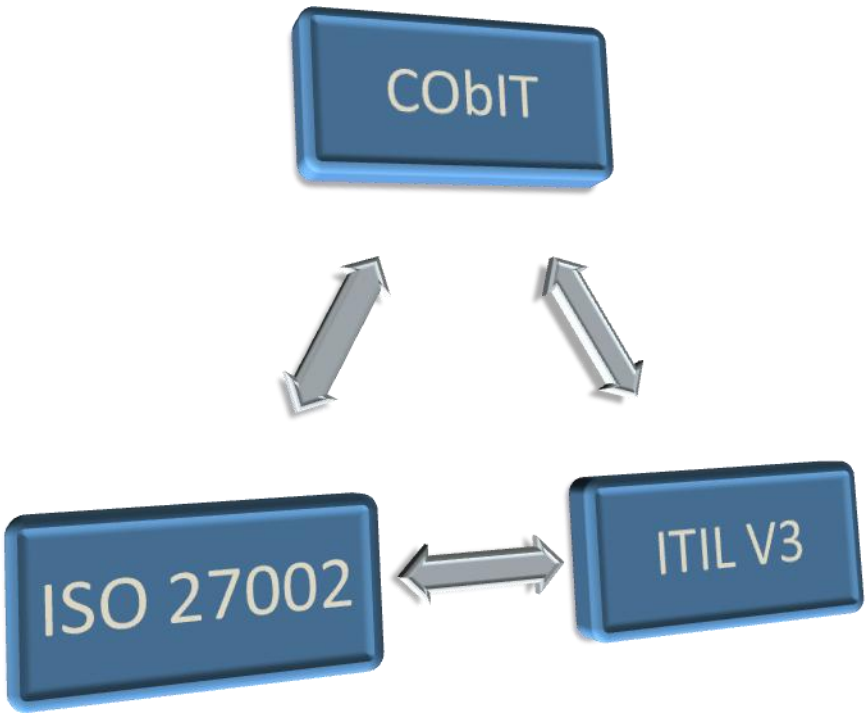
FIGURA 6. MARCO DE CONTROL INTEGRADO ENTRE COSO, COBIT E ITIL



Como vemos existe una perfecta entre los elementos del Control Interno y los Dominios para el cumplimiento de los Objetivos de TI. Ahora, ¿Cómo pueden ser materializados los objetivos de 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. Veremos a continuación el detalle de cada una de estas, teniendo en cuenta que para efectuar auditorias en MiPYMES no es necesario tener en cuenta todos los objetivos de control propuestos por CObIT; por ellos tomaremos como base *CObIT Quickstart 2nd Edition*.

Nuestro enfoque de trabajo se fundamenta en el siguiente modelo:

FIGURA 7. COBIT – ISO 27002 – ITIL V3



Donde se partirá 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 MyPYMES según IT Governance Institute.

COblT/ Objetivos de Control	ITIL	ISO 27001	
PO1 Definir un Plan Estratégico de TI			
PO1.2 Alineación de TI con el Negocio	SS 2.1 ¿Qué es gestión del servicio? SS 2.3 El proceso de negocio SS 2.4 Principios de la gestión del servicio		
PO1.3 Evaluación del Desempeño y la Capacidad Actual	SS 4.4 Preparar la ejecución CSI 5.2 Evaluaciones		
PO1.4 Plan Estratégico de TI	SS 3.3 Tipos de proveedor de servicio SS 3.5 Fundamentos de la estrategia del servicio SS 4.1 Definir el mercado SS 4.2 Desarrollar las ofertas SS 4.3 Desarrollar activos estratégicos SS 4.4 Preparar la ejecución SS 5.5 Gestión de la demanda SS 6.5 Estrategia de sourcing		
PO1.5 Planes Tácticos de TI	SS 4.4 Preparar la ejecución SS 7.1		

	Implementación a través del ciclo de vida SS 7.2 Estrategia y diseño SS 7.3 Estrategia y transiciones SS 7.4 Estrategia y operaciones		
PO1.6 Administración del Portafolio de TI	SS 2.5 El ciclo de vida del servicio SS 3.4 Estructuras del servicio SS 4.2 Desarrollar las ofertas SS 4.3 Desarrollar activos estratégicos SS 5.3 Gestión del portafolio de servicios SS 5.4 Métodos de gestión del portafolio de servicios SS 5.5 Gestión de la demanda SD 3.4 Identificar y documentar los requisitos y drivers del negocio SD 3.6.1 Diseño de soluciones de servicios SD 3.6.2 Diseño de sistemas de soporte, especialmente el portafolio de servicios		
PO2 Definir la Arquitectura de la Información			
PO2.2 Diccionario de Datos Empresarial y Reglas de Sintaxis de	SD 5.2 Gestión de los datos y la información	7.1.1.1. Inventario de Activos 11.1.1. Política de	

Datos	SD 7 Consideraciones tecnológicas	Control de acceso	
PO2.3 Esquema de Clasificación de Datos	SD 5.2 Gestión de los datos y la Información	7.2.1 Lineamientos de clasificación 10.7.1. Gestión de los medios removibles 10.8.1. Procedimientos y politicas de información y software 10.8.2. Acuerdos de intercambio. 11.1.1. Política de Control de acceso	
PO2.4 Administración de Integridad	SD 5.2 Gestión de los datos y la información ST 4.7 Gestión del conocimiento		
PO4 Definir los Procesos, Organización y Relaciones de TI			
PO4.6 Establecimiento de Roles y Responsabilidades	SS 2.6 Funciones y procesos a través del ciclo de vida SD 6.2 Análisis de actividades SD 6.4 Roles y responsabilidades ST 6.3 Modelos organizacionales para apoyar la transición de servicios SO 6.6 Roles y responsabilidades en la operación del servicio CSI 6 Organización para la mejora continua del servicio	6.1.2. Coordinación de la Seguridad de la información 6.1.3. Asignación de responsabilidades de la seguridad de la información 6.1.5. Acuerdos de confidencialidad 8.1.1 Roles y responsabilidades 8.1.2 Verificación 8.1.3 Términos y condiciones del empleo 8.2.2 Educación, entrenamiento y concientización en seguridad de información 15.1.4 Protección de datos y	

		privacidad de la información personal	
PO4.7 Responsabilidad de Aseguramiento de Calidad de TI	CSI 6 Organización para la mejora continua del servicio		
PO4.8 Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento	SD 6.4 Roles y responsabilidades	6.1.1 Compromiso de la gerencia con la seguridad de la información 6.1.2 Coordinación para la seguridad de la información 6.1.3 Asignación de las responsabilidades para la seguridad de la información 8.1.1 Roles y responsabilidades 8.2.1 Responsabilidades de la Gerencia 8.2.3 Procesos disciplinarios 15.1.1 Identificación de legislación aplicable 15.1.2 Derechos de propiedad intelectual 15.1.3 Protección de registros organizacionales 15.1.4 Protección de datos y privacidad de la información personal 15.1.6 Regulación de controles criptográficos 15.2.1 Cumplimiento con políticas y estándares de seguridad	
PO4.10 Supervisión		6.1.2 Coordinación para la seguridad de la información 6.1.3 Asignación de las responsabilidades para la seguridad	

		de la información 7.1.3 Uso aceptable de activos 8.2.1 Responsabilidades de la Gerencia	
PO4.11 Segregación de Funciones	ST 3.2.13 Asegurar la calidad de un servicio nuevo o modificado SO 5.13 Gestión de seguridad de la información y la operación del servicio	8.2.1 Responsabilidades de la Gerencia 10.1.3 Segregación de funciones 10.1.4 Separación de los entornos de desarrollo, pruebas y producción 10.6.1 Controles de red	
PO4.14 Políticas y Procedimientos para Personal Contratado		6.1.5 Acuerdos de confidencialidad 6.2.1 Identificación de riesgos relacionados con terceros 6.2.3 Considerar la seguridad en los acuerdos con terceros 9.1.5 Trabajo en áreas seguras 15.1.5 Prevención del uso indebido de instalaciones de procesamiento de información	
PO4.15 Relaciones	SD 4.2.5.9 Desarrollar contratos y relaciones	6.1.6 Relación con las autoridades 6.1.7 Relación con grupos de interés especial	
PO5 Administrar la Inversión en TI			
PO5.3 Proceso Presupuestal	SS 5.2 Retorno sobre la inversión	5.1.2 Revisión de la política de seguridad de la información	
PO5.4 Administración de Costos de TI	SS 5.1 Gestión financiera (esp. 5.1.2.7)	5.1.2 Revisión de la política de seguridad de la información 13.2.2 Aprendiendo de los incidentes de	

		seguridad de información	
PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia			
PO6.2 Riesgo Corporativo y Marco de Referencia de Control Interno de TI		5.1.1 Documento de la política de seguridad de la información 6.2.2 Considerar la seguridad al tratar con los clientes 7.1.3 Uso aceptable de activos 8.2.2 Educación, entrenamiento y concientización en seguridad de información 8.3.2 Devolución de activos 9.1.5 Trabajo en áreas seguras 9.2.7 Eliminar la propiedad 10.7.3 Procedimientos para el manejo de la información 10.8.1 Políticas y procedimientos para el intercambio de información 10.9.3 Información de dominio público 11.1.1 Políticas de control de acceso 11.3.1 Uso de contraseñas 11.3.2 Equipos desatendidos de usuario 11.3.3 Políticas de escritorios y pantallas limpias 11.7.1 Computación	

		móvil y las comunicaciones 11.7.2 Teletrabajo 12.3.1 Políticas de uso de controles criptográficos 15.1.2 Derechos de propiedad intelectual 15.1.5 Prevención del uso indebido de instalaciones de procesamiento de información 15.2.1 Cumplimiento con políticas y estándares de seguridad	
PO6.3 Administración de Políticas para TI		5.1.1 Documento de la política de seguridad de la información 5.1.2 Revisión de la política de seguridad de la información 6.1.1 Compromiso de la gerencia con la seguridad de la información 8.1.1 Roles y responsabilidades	
PO6.4 Implantación de Políticas de TI		6.1.1 Compromiso de la gerencia con la seguridad de la información 6.1.8 Revisión independiente de la seguridad de la información 6.2.3 Considerar la seguridad en los acuerdos con terceros 8.2.2 Educación, entrenamiento y concientización en seguridad de información	

PO6.5 Comunicación de los Objetivos y la Dirección de TI	ST 5.1 Gestión de las comunicaciones y el compromiso SO 3.6 Comunicaciones	5.1.1 Documento de la política de seguridad de la información 6.1.1 Compromiso de la gerencia con la seguridad de la información 6.1.2 Coordinación para la seguridad de la información	
PO8 Administrar la Calidad			
PO8.2 Estándares y Prácticas de Calidad	SS 7.5 Estrategia y mejora ST 3.2.13 Asegurar la calidad de un servicio nuevo o modificado ST 4.5 Validación del servicio y pruebas (ITIL se enfoca en la transición y en las pruebas continuas del servicio) CSI Apéndice A Guía Complementaria		
PO10 Administrar Proyectos			
PO10.1 Marco de Trabajo para la Administración de Programas			
PO10.2 Marco de Trabajo para la Administración de Proyectos			
PO10.6 Inicio de las Fases del Proyecto			
PO10.7 Plan Integrado del Proyecto	SD Apéndice D Diseñar y planificar documentos y sus contenidos		

PO10.9 Administración de Riesgos del Proyecto			
AI1 Identificar Soluciones automatizadas			
AI1.1 Definición y Mantenimiento de los Requerimientos Técnicos y Funcionales del Negocio	SS 7.5 Estrategia y mejora SS 8.1 Automatización del servicio SD 3.2 Diseño balanceado SD 3.3 Identificación de requerimientos de servicios SD 3.4 Identificar y documentar los requisitos y drivers del negocio SD 3.5 Actividades de diseño SD 3.6.1 Diseño de soluciones de servicios SD 3.6.2 Diseño de sistemas de soporte, especialmente el portafolio de servicios SD 3.6.3 Diseño de la arquitectura tecnológica SD 3.6.4 Diseño de procesos SD 3.6.5 Diseño de sistemas de medición y métricas SD 3.8 Limitaciones del diseño SD 3.9 Arquitectura orientada al servicio SD 4.3.5.8	8.2.2 Educación, entrenamiento y concientización en seguridad de información 12.1.1 Análisis y especificación de los requisitos de seguridad 10.3.2 Aceptación del sistema	

	Dimensionamiento de aplicaciones SD Apéndice D Diseñar y planificar documentos y sus contenidos ST 3.2.5 Alinear los planes de transición del servicio con las necesidades del negocio		
AI1.3 Estudio de Factibilidad y Formulación de Cursos de Acción Alternativos	SD 3.6.1 Diseño de soluciones de servicios SD 3.7.1 Evaluación de soluciones alternativas ST 3.2.4 Maximizar la reutilización de procesos y sistemas establecidos		
AI2 Adquirir y mantener software aplicativo			
AI2.1 Diseño de Alto Nivel	SD 3.6.1 Diseño de soluciones de servicios SD 3.6.3 Diseño de la arquitectura tecnológica		
AI2.2 Diseño Detallado	SS 8.2 Interfaces del servicio SD 4.2.5.2 Requisitos acordados y documentados de los nuevos servicios; definir los requisitos de los niveles de servicios SD 5.3 Gestión de aplicaciones		
AI3 Adquirir y			

mantener infraestructura tecnológica			
AI3.1 Plan de Adquisición de Infraestructura Tecnológica	SD 3.6.3 Diseño de la arquitectura tecnológica		
AI3.2 Protección y Disponibilidad del Recurso de Infraestructura	SD 4.6.5.1 Controles de seguridad SO 5.4 Gestión y soporte de servidores	12.1.1 Análisis y especificación de los requisitos de seguridad	
AI3.3 Mantenimiento de la Infraestructura	SO 5.4 Gestión y soporte de servidores SO 5.5 Gestión de redes SO 5.7 Administración de bases de datos SO 5.8 Gestión de servicios de directorio SO 5.9 Soporte de estaciones de trabajo SO 5.10 Gestión de middleware SO 5.11 Gestión Internet/web	9.1.5 Trabajo en áreas seguras 9.2.4 Mantenimiento de equipos 12.4.2 Protección de los datos de prueba de sistema 12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo 12.6.1 Control de vulnerabilidades técnicas	
AI4 Facilitar la operación y el uso			
AI4.1 Plan para Soluciones de Operación	SD 3.6.1 Diseño de soluciones de servicios ST 3.2.5 Alinear los planes de transición del servicio con las necesidades del negocio ST 3.2.9 Planificar la liberación y el despliegue de paquetes		

	ST 4.4.5.1 Planificación ST 4.4.5.2 Preparación para la construcción, pruebas y despliegue ST 4.4.5.5 Planificar y preparar el despliegue		
AI4.2 Transferencia de Conocimiento a la Gerencia del Negocio	ST 3.2.5 Alinear los planes de transición del servicio con las necesidades del negocio ST 4.7 Gestión del conocimiento		
AI4.3 Transferencia de Conocimiento a Usuarios Finales	ST 3.2.8 Proveer sistemas para la transferencia de conocimientos y el soporte de decisiones ST 4.4.5.8 Soporte temprano ST 4.7 Gestión del conocimiento		
AI4.4 Transferencia de Conocimiento al Personal de Operaciones y Soporte	ST 3.2.8 Proveer sistemas para la transferencia de conocimientos y el soporte de decisiones ST 4.4.5.5 Planificar y preparar el despliegue ST 3.7 Documentación ST 4.4.5.11 Errores detectados en el entorno de desarrollo SO 4.6.6 Gestión	10.1.1 Procedimientos operativos documentados 10.3.2 Aceptación del sistema 10.7.4 Seguridad de la documentación de sistemas 13.2.2 Aprendiendo de los incidentes de seguridad de información	

	de conocimiento (actividades operativas)		
AI5 Adquirir recursos de TI			
AI5.1 Control de Adquisición	SD 3.7.2 Adquisición de la solución elegida	6.1.5 Acuerdos de confidencialidad	
AI5.2 Administración de Contratos con Proveedores	SD 4.2.5.9 Desarrollar contratos y relaciones SD 4.7.5.3 Nuevos proveedores y contratos	6.1.5 Acuerdos de confidencialidad 6.2.3 Considerar la seguridad en los acuerdos con terceros 10.8.2 Acuerdos de intercambio 12.5.5 Outsourcing de desarrollo de software	
AI5.3 Selección de Proveedores	SD 3.7.1 Evaluación de soluciones alternativas SD 4.7.5.3 Nuevos proveedores y contratos SD Apéndice I Ejemplo de una declaración de requerimiento y/o una invitación a ofertar		
AI6 Administrar cambios			
AI6.1 Estándares y Procedimientos para Cambios	SD 3.2 Diseño balanceado SD 3.7 Actividades subsiguientes del diseño ST 3.2 Políticas para la transición del servicio ST 3.2.1 Definir e implementar una política formal para la transición del servicio	10.1.2 Gestión de cambios 12.5.3 Restricciones en los cambios a los paquetes de software	

	ST 3.2.2 Implementar todos los cambios a los servicios a través de la transición del servicio ST 3.2.7 Establecer controles y disciplinas eficaces ST 4.1 Planificación y soporte para la transición ST 4.1.4 Políticas, principios y conceptos básicos ST 4.2 Gestión de cambios		
AI6.3 Cambios de Emergencia	ST 4.2.6.9 Cambios de emergencia	10.1.2 Gestión de cambios 11.5.4 Uso de utilitarios del sistema 12.5.1 Procedimiento de control de cambios 12.5.3 Restricciones en los cambios a los paquetes de software 12.6.1 Control de vulnerabilidades técnicas	
AI6.4 Seguimiento y Reporte del Estatus de Cambio	ST 3.2.13 Asegurar la calidad de un servicio nuevo o modificado ST 3.2.14 Mejora proactiva de la calidad durante la transición del servicio ST 4.1.5.3 Planificar y coordinar la transición del servicio ST 4.1.6 Brindar soporte al proceso de transición	10.1.2 Gestión de cambios	

AI6.5 Cierre y Documentación del Cambio	ST 4.2.6.4 Valorar y evaluar el cambio ST 4.2.6.7 Revisar y cerrar el registro del cambio ST 4.4.5.10 Revisar y cerrar la transición del servicio ST 4.4.5.9 Revisar y cerrar un despliegue SO 4.3.5.5 Cierre	10.1.2 Gestión de cambios	
AI7 Instalar y acreditar soluciones y cambios			
AI7.3 Plan de Implantación	ST 3.2.9 Planificar la liberación y el despliegue de paquetes ST 4.1.5.2 Preparación para la transición del servicio ST 4.4.5.2 Preparación para la construcción, pruebas y despliegue ST 4.4.5.3 Construcción y Pruebas ST 4.4.5.4 Pruebas y pilotos del servicio ST 4.4.5.5 Planificar y preparar el despliegue		
AI7.4 Ambiente de Prueba	ST 3.2.14 Mejora proactiva de la calidad durante la transición del servicio ST 4.4.5.2 Preparación para la	10.1.4 Separación de los entornos de desarrollo, pruebas y producción 12.4.3 Control de acceso al código fuente de los programas 12.5.2 Revisión técnica	

	construcción, pruebas y despliegue ST 4.4.5.3 Construcción y pruebas ST 4.4.5.4 Pruebas y pilotos del servicio	de las aplicaciones luego de cambios en el sistema operativo	
AI7.5 Conversión de Sistemas y Datos			
AI7.6 Pruebas de Cambios	ST 3.2.14 Mejora proactiva de la calidad durante la transición del servicio ST 4.4.5.4 Pruebas y pilotos del servicio ST 4.5.5.5 Ejecutar pruebas ST 4.5.5.6 Evaluar criterios de fin de pruebas y reportar	6.1.4 Proceso de autorización para las instalaciones de procesamiento de información 12.4.3 Control de acceso al código fuente de los programas 12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo	
AI7.7 Prueba de Aceptación Final.	ST 4.4.5.4 Pruebas y pilotos del servicio ST 4.5.5.5 Ejecutar pruebas ST 4.5.5.6 Evaluar criterios de salida y reportar	10.3.2 Aceptación del sistema 12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo 12.5.4 Fuga de información	
AI7.8 Promoción a Producción	ST 4.4.5.5 Planificar y preparar el despliegue ST 4.4.5.6 Realizar transferencia, despliegue y retiros SO 4.3.5.4 Cumplimiento		
AI7.9 Revisión Posterior a la Implantación	ST 3.2.13 Asegurar la calidad de un servicio nuevo o modificado		

	ST 4.1.5.3 Planear y coordinar la transición del servicio ST 4.4.5.10 Revisar y cerrar la transición del servicio ST 4.4.5.7 Verificar despliegue ST 4.4.5.9 Revisar y cerrar un despliegue ST 4.6 Evaluación SO 4.3.5.5 Cierre		
DS1 Definir y administrar los niveles de servicio			
DS1.3 Acuerdos de Niveles de Servicio	SD 4.2.5.2 Requisitos acordados y documentados de los nuevos servicios; definir los requisitos de los niveles de servicios SD Apéndice F Ejemplos de ANS y Acuerdos de niveles de operación	10.2.1 Entrega de servicios	
DS1.6 Revisión de los Acuerdos de Niveles de Servicio y de los Contratos	SD 4.2.5.4 Comparar, medir y mejorar la satisfacción del cliente SD 4.2.5.5 Examinar y revisar los acuerdos suscritos y el alcance del servicio SD 4.2.5.8 Examinar y revisar los ANS, alcance del servicio y los		

	acuerdos suscritos		
DS2 Administrar los servicios de terceros			
DS2.2 Gestión de Relaciones con Proveedores	SD 4.2.5.9 Desarrollar contratos y relaciones SD 4.7.5.2 Clasificación de proveedores y mantenimiento de la base de datos de proveedores y contratos SD 4.7.5.4 Gestión y desempeño de proveedores y contratos SD 4.7.5.5 Renovación y/o término de contratos	6.2.3 Considerar la seguridad en los acuerdos con terceros 10.2.3 Gestión de cambios a los servicios de terceros 15.1.4 Protección de datos y privacidad de la información personal	
DS2.3 Administración de Riesgos del Proveedor	SD 4.7.5.3 Nuevos proveedores y contratos SD 4.7.5.5 Renovación y/o término de contratos	6.2.1 Identificación de riesgos relacionados con terceros 6.2.3 Considerar la seguridad en los acuerdos con terceros 8.1.2 Verificación 8.1.3 Términos y condiciones del empleo 10.2.3 Gestión de cambios a los servicios de terceros 10.8.2 Acuerdos de intercambio	
DS2.4 Monitoreo del Desempeño del Proveedor	SD 4.7.5.4 Gestión y desempeño de proveedores y contratos	6.2.3 Considerar la seguridad en los acuerdos con terceros 10.2.1 Entrega de servicios 10.2.2 Monitoreo y revisión de los servicios de terceros 12.4.2 Protección de los	

		datos de prueba del sistema 12.5.5 Outsourcing de desarrollo de software	
DS3 Administrar el desempeño y la capacidad			
DS3.1 Planeación del Desempeño y la Capacidad	SD 4.3.5.1 Gestión de la capacidad para el negocio SD Apéndice J Contenido típico de un plan de capacidad CSI 5.6.2 Gestión de la capacidad	10.3.1 Gestión de la capacidad	
DS3.2 Capacidad y Desempeño Actual	SD 4.3.5.2 Gestión de la capacidad del servicio SD 4.3.5.3 Gestión de la capacidad de los componentes SO 4.1.5.2 Notificación de eventos SO 4.1.5.3 Detección de eventos SO 5.4 Gestión y soporte de servidores CSI 4.3 Mediciones del servicio	10.3.1 Gestión de la capacidad	
DS3.3 Capacidad y Desempeño Futuros	SD 4.3.5.1 Gestión de la capacidad para el negocio SD 4.3.5.2 Gestión de la capacidad del servicio SD 4.3.5.3 Gestión de la capacidad de los componentes SD 4.3.5.7 Modelamiento y tendencias	10.3.1 Gestión de la capacidad	

	SD 4.3.8 Gestión de la Información		
DS3.5 Monitoreo y Reporte	SD 4.3.5.4 Actividades de soporte de la gestión de la capacidad SD 4.3.5.5 Gestión y control de umbrales SD 4.3.5.6 Gestión de la demanda SD 4.4.5.1 Actividades reactivas de la gestión de la disponibilidad		
DS4 Garantizar la continuidad del servicio			
DS4.1 Marco de Trabajo de Continuidad de TI	SD 4.5 Gestión de continuidad de servicios de TI SD 4.5.5.1 Etapa 1 – Inicio CSI 5.6.3 Gestión de continuidad de servicios de TI	6.1.6 Relación con las autoridades 6.1.7 Relación con grupos de interés especial 14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio 14.1.2 Continuidad del negocio y evaluación de riesgos 14.1.4 Marco de planificación de continuidad del negocio	
DS4.2 Planes de Continuidad de TI	SD 4.5.5.2 Etapa 2 – Requisitos y estrategia SD 4.5.5.3 Etapa 3 – Implementación SD Apéndice K Contenido típico de	6.1.6 Relación con las autoridades 6.1.7 Relación con grupos de interés especial 14.1.3 Desarrollar e implementar planes de continuidad que incluyan	

	un plan de recuperación	la seguridad de la información	
DS4.3 Recursos Críticos de TI	SD 4.4.5.2 Actividades proactivas de la gestión de la disponibilidad SD 4.5.5.4 Etapa 4 – Operación continua	14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio 14.1.2 Continuidad del negocio y evaluación de riesgos	
DS4.5 Pruebas del Plan de Continuidad de TI	SD 4.5.5.3 Etapa 3 – Implementación SD 4.5.5.4 Etapa 4 – Operación Continua	14.1.5 Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio	
DS4.8 Recuperación y Reanudación de los Servicios de TI	SD 4.4.5.2 Actividades proactivas de la gestión de la disponibilidad SD 4.5.5.4 Etapa 4 – Operación Continua	14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio 14.1.3 Mantener o restaurar operaciones para asegurar la disponibilidad de la información	
DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones	SD 4.5.5.2 Etapa 2 – Requisitos y estrategia SO 5.2.3 Respaldo y restauración	10.5.1 Respaldo de la información	
DS5 Garantizar la seguridad de los sistemas			
DS5.3 Administración de Identidad	SO 4.5 Gestión de acceso	5.1.1 Documento de la política de seguridad de la información 5.1.2 Revisión de la política de seguridad de la información 6.1.2 Coordinación para la seguridad de la información 6.1.5 Acuerdos de	

		confidencialidad 8.2.2 Educación, entrenamiento y concientización en seguridad de información 11.1.1 Políticas de control de acceso 11.7.1 Computación móvil y las comunicaciones 11.7.2 Teletrabajo	
DS5.4 Administración de Cuentas del Usuario	SO 4.5 Gestión de acceso SO 4.5.5.1 Peticiones de acceso SO 4.5.5.2 Verificación SO 4.5.5.3 Habilitar privilegios SO 4.5.5.4 Monitorear el estado de la identidad SO 4.5.5.5 Registro y seguimiento de accesos SO 4.5.5.6 Eliminar o restringir privilegios	6.1.5 Acuerdos de confidencialidad 6.2.1 Identificación de riesgos relacionados con terceros 6.2.2 Considerar la seguridad al tratar con los clientes 8.1.1 Roles y responsabilidades 8.3.1 Responsabilidades en el cese 8.3.3 Eliminación de privilegios de acceso 10.1.3 Segregación de funciones 11.1.1 Políticas de control de acceso 11.2.1 Registro de usuarios 11.2.2 Gestión de privilegios 11.2.4 Revisión de derechos de acceso de usuarios 11.3.1 Uso de contraseñas 11.5.1 Procedimientos seguros de inicio de sesión 11.5.3 Sistema de gestión de contraseñas 11.6.1 Restricción de	

		acceso a la información	
DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad	SO 4.5.5.6 Eliminar o restringir privilegios SO 5.13 Gestión de seguridad de la información y la operación del servicio	6.1.8 Revisión independiente de la seguridad de la información 10.10.2 Monitoreo del uso del sistema 10.10.3 Protección de logs 10.10.4 Logs de administrador y de operador 12.6.1 Control de vulnerabilidades técnicas 13.1.2 Reporte de debilidades de seguridad 15.2.2 Verificación de cumplimiento técnico 15.3.1 Controles de auditoría de sistemas de información	
DS5.6 Definición de Incidente de Seguridad	SD 4.6.5.1 Controles de seguridad (cobertura de alto nivel, sin detalle) SD 4.6.5.2 Gestión de brechas de seguridad e incidentes	8.2.3 Procesos disciplinarios 13.1.1 Reporte de eventos de seguridad de información 13.1.2 Reporte de debilidades de seguridad 13.2.1 Responsabilidades y procedimientos 13.2.3 Recolección de evidencia	
DS5.9 Prevención, Detección y Corrección de Software Malicioso		10.4.1 Controles contra código malicioso 10.4.2 Controles contra códigos móviles	
DS5.10 Seguridad de la Red	SO 5.5 Gestión de redes	6.2.1 Identificación de riesgos relacionados con terceros 10.6.1 Controles de red 10.6.2 Seguridad de los servicios de red 11.4.1 Política de uso de los servicios de red	

		11.4.2 Autenticación de usuarios para conexiones externas 11.4.3 Identificación de equipos en redes 11.4.4 Protección de puertos de configuración y diagnóstico remoto 11.4.5 Segregación en redes 11.4.6 Control de conexiones en la red 11.4.7 Control de enrutamiento en la red 11.6.2 Aislamiento de sistemas sensitivos	
DS6 Identificar y asignar costos			
DS6.3 Modelación de Costos y Cargos	SS 5.1 Gestión financiera SS 7.2 Estrategia y diseño		
DS7 Educar y entrenar a los usuarios			
DS7.1 Identificación de Necesidades de Entrenamiento y Educación	SO 5.13 Gestión de seguridad de la información y la operación del servicio SO 5.14 Mejora de las actividades operativas	8.2.2 Educación, entrenamiento y concientización en seguridad de información	
DS8 Administrar la mesa de servicio y los incidentes			
DS8.1 Mesa de Servicios	SO 4.1 Gestión de eventos SO 4.2 Gestión de incidentes SO 6.2 Mesa de servicios	14.1.4 Marco de planeamiento de continuidad del negocio	
DS8.2 Registro de Consultas de Clientes	SO 4.1.5.3 Detección de eventos SO 4.1.5.4 Filtrado	13.1.1 Reporte de eventos de seguridad de información 13.1.2 Se pueden	

	de eventos SO 4.1.5.5 Significado de los eventos SO 4.1.5.6 Correlación de eventos SO 4.1.5.7 Trigger SO 4.2.5.1 Identificación de incidentes SO 4.2.5.2 Log de incidentes SO 4.2.5.3 Clasificación de incidentes SO 4.2.5.4 Priorización de incidentes SO 4.2.5.5 Diagnóstico inicial SO 4.3.5.1 Selección por menú	agregar los reportes de debilidades de seguridad ya que se relacionan con la identificación de eventos 13.2.1 Responsabilidades y procedimientos 13.2.3 Recolección de evidencia	
DS8.3 Escalamiento de Incidentes	SO 4.1.5.8 Selección de respuestas SO 4.2.5.6 Escalamiento de incidentes SO 4.2.5.7 Investigación y diagnóstico SO 4.2.5.8 Resolución y recuperación SO 5.9 Soporte de estaciones de trabajo	13.1.2 Se pueden agregar los reportes de debilidades de seguridad ya que se relacionan con la identificación de eventos 13.2.3 Recolección de evidencia 14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio 14.1.4 Marco de planificación de continuidad del negocio	
DS8.4 Cierre de Incidentes	SO 4.1.5.10 Cerrar eventos SO 4.2.5.9 Cierre de incidentes	13.2.2 Aprendiendo de los incidentes de seguridad de información 13.2.3 Recolección de	

		evidencia	
DS8.5 Análisis de Tendencias	SO 4.1.5.9 Revisar acciones CSI 4.3 Mediciones del servicio (aproximada)	13.2.2 Aprendiendo de los incidentes de seguridad de información	
DS9 Administrar la configuración			
DS9.1 Repositorio y Línea Base de Configuración	SS 8.2 Interfaces del servicio ST 4.1.5.2 Preparación para la transición del servicio ST 4.3.5.2 Gestión y planificación	7.2.2 Etiquetado y manejo de la información 12.4.1 Control del software de operaciones 12.4.2 Protección de los datos de prueba de sistema	
DS9.2 Identificación y Mantenimiento de Elementos de Configuración	ST 4.1.5.2 Preparación para la transición del servicio ST 4.3.5.3 Identificación de la configuración ST 4.3.5.4 Control de la configuración ST 4.3.5.5 Contabilización y registro de estados	7.1.1 Inventario de activos 7.1.2 Propiedad de los activos 7.2.2 Etiquetado y manejo de la información 10.7.4 Seguridad de la documentación de sistemas 11.4.3 Identificación de equipos en redes 12.4.2 Protección de los datos de prueba de sistema 12.5.3 Restricciones en los cambios a los paquetes de software 12.6.1 Control de vulnerabilidades técnicas 15.1.5 Prevención del uso indebido de instalaciones de procesamiento de información	
DS9.3 Revisión de Integridad de la Configuración	ST 4.3.5.6 Auditoría y verificación SO 5.4 Gestión y soporte de servidores	7.1.1 Inventario de activos 10.7.4 Seguridad de la documentación de sistemas	

	SO 7 Consideraciones de tecnología (especialmente para licenciamiento, mencionado en SO 7.1.4)	12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo 15.1.5 Prevención del uso indebido de instalaciones de procesamiento de información	
DS11 Administrar los datos			
DS11.3 Sistema de Administración de Librerías de Medios		10.7.1 Gestión de medios removibles 10.7.2 Eliminación de medios 12.4.3 Control de acceso al código fuente de los programas	
DS11.4 Eliminación		9.2.6 Eliminación o reutilización segura de equipos 10.7.1 Gestión de medios removibles 10.7.2 Eliminación de medios	
DS11.5 Respaldo y Restauración	SO 5.2.3 Respaldo y restauración	10.5.1 Respaldo de la información	
DS11.6 Requerimientos de Seguridad para la Administración de Datos	SD 5.2 Gestión de los datos y la información	10.5.1 Respaldo de la información 10.7.3 Procedimientos para el manejo de la información 10.8.3 Medios de almacenamiento físico en tránsito 10.8.4 Mensajería electrónica 12.4.2 Protección de datos de prueba de sistema 12.4.3 Control de acceso al código fuente de los programas	
DS12 Administrar el ambiente físico			

DS12.1 Selección y Diseño del Centro de Datos		9.1.1 Perímetro de seguridad física 9.1.3 Seguridad de oficinas, salas e instalaciones 9.1.6 Áreas de acceso público, despacho y recepción	
DS12.2 Medidas de Seguridad Física	SO Apéndice E Descripción detallada de la gestión de las instalaciones	9.1.1 Perímetro de seguridad física 9.1.2 Controles físicos de ingreso 9.1.3 Seguridad de oficinas, salas e instalaciones 9.2.5 Seguridad de los equipos fuera de las instalaciones 9.2.7 Eliminar la propiedad	
DS12.4 Protección Contra Factores Ambientales	SO Apéndice E Descripción detallada de la gestión de las instalaciones	9.1.4 Protección contra amenazas externas y ambientales 9.2.1 Ubicación y protección de equipos 9.2.2 Servicios de soporte 9.2.3 Seguridad del cableado	
DS12.5 Administración de Instalaciones Físicas	SO 5.12 Gestión del centro de datos e instalaciones	9.2.2 Servicios de soporte 9.2.4 Mantenimiento de equipos	
DS13 Administrar las operaciones			
DS13.1 Procedimientos e Instrucciones de Operación	SO 3.7 Documentación SO 5 Actividades comunes de la operación del servicio SO Apéndice B Comunicaciones en la operación de servicio	10.1.1 Procedimientos operativos documentados 10.7.4 Seguridad de la documentación de sistemas	

DS13.4 Documentos Sensitivos y Dispositivos de Salida	SO 5.2.4 Datos electrónicos e Impresos		
DS13.5 Mantenimiento Preventivo del Hardware	SO 5.3 Gestión de mainframe SO 5.4 Gestión y soporte de Servidores	9.2.4 Mantenimiento de equipos	
ME1 Monitorear y Evaluar el Desempeño de TI			
ME1.2 Definición y Recolección de Datos de Monitoreo	SD 4.2.5.10 Reclamos y reconocimientos CSI 4.1c Paso Tres – Recopilación de datos CSI 4.1d Paso Cuatro – Procesar los datos	10.10.2 Monitoreo del uso del sistema	
ME1.4 Evaluación del Desempeño	SD 4.2.5.7 Ejecutar revisiones del servicio e instigar mejoras dentro del plan general de mejoramiento del servicio CSI 3 Principios de mejora continua de servicios CSI 4.1e Paso Cinco – Analizar los datos CSI 5.3 Benchmarking CSI 8 Implementar la mejora continua del servicio		
ME1.5 Reportes al Consejo Directivo y a Ejecutivos	CSI 4.1f Paso Seis – Presentar y utilizar la información		

	CSI 4.2 Reportes del servicio		
ME2 Monitorear y Evaluar el Control Interno			
ME2.2 Revisiones de Auditoría		5.1.2 Revisión de la política de seguridad de la información 6.1.8 Revisión independiente de la seguridad de la información 10.10.2 Monitoreo del uso del sistema 10.10.4 Logs de administrador y de operador 15.2.1 Cumplimiento con políticas y estándares de seguridad	
ME2.3 Excepciones de Control		15.2.1 Cumplimiento con políticas y estándares de seguridad	
ME2.4 Auto Evaluación del Control		15.2.1 Cumplimiento con políticas y estándares de seguridad	
ME2.5 Aseguramiento del Control Interno		5.1.2 Revisión de la política de seguridad de la información 6.1.8 Revisión independiente de la seguridad de la información 10.10.2 Monitoreo del uso del sistema 10.10.4 Logs de administrador y de operador 15.2.1 Cumplimiento con políticas y estándares de seguridad 15.2.2 Verificación de cumplimiento técnico 15.3.1 Controles de auditoría de sistemas de	

		información	
ME2.6 Control Interno para Terceros		6.2.3 Considerar la seguridad en los acuerdos con terceros 10.2.2 Monitoreo y revisión de los servicios de terceros 15.2.1 Cumplimiento con políticas y estándares de seguridad	
ME2.7 Acciones Correctivas		5.1.2 Revisión de la política de seguridad de la información 15.2.1 Cumplimiento con políticas y estándares de seguridad	
ME3 Garantizar el Cumplimiento Regulatorio			
ME3.1 Identificar los Requerimientos de las Leyes, Regulaciones y Cumplimientos Contractuales		6.1.6 Relación con las autoridades que tengan impacto potencial en TI 15.1.1 Identificación de legislación aplicable 15.1.2 Derechos de propiedad intelectual 15.1.4 Protección de datos y privacidad de la información personal	
ME4 Proporcionar Gobierno de TI			
ME4.1 Establecimiento de un Marco de Gobierno de TI	CSI 3.10 Gobierno CSI Apéndice A Guía complementaria		
ME4.2 Alineamiento Estratégico	SD 3.10 Gestión de servicio al negocio		
ME4.3 Entrega de Valor	SS 3.1 Creación de valor		
ME4.4 Administración de Recursos			
ME4.5 Administración de Riesgos	SS 9.5 Riesgos		
ME4.6 Medición del Desempeño	SS 4.4 Preparar la ejecución		

	SS 9.4 Efectividad en mediciones SD 3.6.5 Diseño de sistemas de medición y métricas CSI 4.3 Mediciones del servicio		

CONCLUSIONES

En el desarrollo del presente trabajo 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 organización de la infraestructura tecnológica que deben soportan 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 optimo 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, e 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, brindando la oportunidad de alinear las estrategias de TI con las estrategias de estas organizaciones, de alcanzar el uso optimo de todos sus recursos que ayudaran 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 contribuirá a proporcionar una base de control de TI en estas Organizaciones.

REFERENCIAS BIBLIOGRÁFICAS

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

AS/NZ 4360. Guía para la administración del riesgo.

COBIT 4.1. ISACA. Marco de Trabajo, Objetivos de Control, Directrices Gerenciales y Modelos de Madurez.

COBIT Control Practices. ISACA. Guidance to Achieve Control Objetives for Succesful IT Governance.

Cristrian Bailey. ITIL V. 3. Manual Técnico.

CMMI. Manual de Referencia.

Cubillos Gordillos,Amilkar; Garcia Munive, Javier, "ELABORACION DEL PLAN ESTRATEGICO EN SISTEMAS DE LA SECRETARIA DE CONTROL URBANO Y ESPACIO PUBLICO DE LA ALCALDIA DISTRITAL DE BARRANQUILLA", Corporación Universitaria de la Costa, Especialización en Auditoria de Sistemas de Información, Barranquilla, 2010.

(ERICKSON, 1986); Citado por: Documento PEÑA, Judith, Naturaleza de la Investigación, p 40 - 41.

ESTUPIÑAN G. Rodrigo. Administración de riesgos E.R.M y la Auditoría Interna. ECOE Ediciones, 2008

Gobierno de TI - TCP Sistemas e Ingeniería, http://www.tcpsi.com/servicios/gobierno_ti.htm

Introducción ISO20000 COLOMBIA, http://www.iso20000.com.ar/intro_col.html

IT Assurance Guide. Using COBIT. ISACA (2007).

IT Governance Institute, Cobit 4.1 – Isaca (2010).

ISO/IEC 27001, http://es.wikipedia.org/wiki/ISO/IEC_27001

ISO 27001 e ISO 27002. Manual de Referencia.

ICONTEC. ISO/IEC NTC 27002

MANTILLA B., Samuel Alberto. Control Interno Efectivo. Hacia un nuevo estándar internacional. Deloitte & Touche Ltda. - Ed. Planeta Colombiana S.A. 2008

MANTILLA B., Samuel Alberto. Control Interno. Informe COSO. Resumen ejecutivo, Estructura conceptual integrada. ECOE Ediciones - Commitee of Sponsoring Organizations of the Treadway Comission (COSO), 2005

MANTILLA B., Samuel Alberto. Auditoría Financiera de PYMES. ECOE Ediciones, 2008

Martinez del Vecchio, Zeudy Carroll, " PROPUESTA DE UN MARCO DE REFERENCIA PARA LA PLANEACION Y ORGANIZACIÓN DE LAS T.I.C. BASADO EN COBIT QUICK START, EN EL COLEGIO DE LA COMPAÑÍA DE MARIA LA ENSEÑANZA BARRANQUILLA", Corporación Universitaria de la Costa, Especialización en Auditoria de Sistemas de Información, Barranquilla, 2010.

SÁNCHEZ C., John Jairo, OSORIO G., Jaime, BAENA M., Ernesto. Algunas aproximaciones al problema de financiamiento de las PYMES en Colombia. Universidad Tecnológica de Pereira. Scientia et Technica Año XIII, No 34, Mayo de 2007.

BIBLIOGRÁFIA COMPLEMENTARIA

BUSINESSCOL. Sección PYMES. http://www.businesscol.com/empresarial/pymes/

Círculo de Deming, http://es.wikipedia.org/wiki/Deming

CONGRESO DE LA REPÚBLICA. Ley 43 de 1990.

COMPUTERWORLD. Menos del 50% de las pymes de Europa Occidental hace auditorías de sus Sistemas. La asociación asegura que estas prácticas hacen peligrar la seguridad de las empresas. Artículo periodístico. http://www.idg.es/computerworld/imprimir.aspx?ida=133041.

DELTA ASESORES. Inversión en TIC de PYMES de Colombia
http://www.deltaasesores.com/estadisticas/tecnologia/3100-inversion-en-tic-de-pymes-en-colombia

JARAMILLO S., Luís Javier. La difusión de tecnología para las Pymes: Es hora de concebir nuevos Mecanismos. http://www.universia.net.co - Universia Colombia

JIMENEZ, Armando. Historia de la Auditoría. www.monografías.com
(http://www.monografias.com/trabajos12/condeau/condeau.shtml)

http://www.monografias.com/trabajos47/riesgos-auditoria/riesgos-auditoria2.shtml#administ

http://www.monografias.com/trabajos12/auditor/auditor.shtml#defi

http://www.gestiopolis.com/recursos/documentos/fulldocs/ger/normascalidad.htm

http://www.misrespuestas.com/que-es-iso-9000.html

1. best-seller de 1985. New York, NY The Free Press.
http://es.wikipedia.org/wiki/Cadena_de_valor#cite_note-0

http://es.wikipedia.org/wiki/Modelo_de_Capacidad_y_Madurez

http://www.gestiopolis.com/recursos/documentos/fulldocs/fin/introcontrolinterno.htm

http://www.cgh.org.co/temas/descargas/elenfoquesistemico.pdf

http://es.wikipedia.org/wiki/Est%C3%A1ndar

http://www.agaex.com:8080/ploneagaex/productos/gobierno-ti-y-cobit

http://www.isacabcn.org/isaca-internacional.asp?llen=esp

http://es.wikipedia.org/wiki/Riesgo

www.fen.gov.co/.../MANUAL%20DE%20RIESGO%20OPERATIVO.pdf

http://es.wikipedia.org/wiki/Sinergia

http://www.alegsa.com.ar/Dic/sistema.php

http://www.monografias.com/trabajos31/metodologia-itil/metodologia-itil.shtml

http://www.channelplanet.com/index.php?idcategoria=13932

http://es.wikipedia.org/wiki/ISO_27002

http://es.wikipedia.org/wiki/ISO_9000

http://www.monografias.com/trabajos14/auditoriasistemas/auditoriasistemas.shtml

nuestro.net78.net/.../ACI%20–%20425%20Clase_01d%20Planificación,%20Normativas%20y%20Delitos%20Informáticos.ppt

http://www.gitltda.com/estandares.html

http://www.supernotariado.gov.co/supernotariado/images/smilies/Arc_Meci/Act_Mec_Fin_2008/cartilla-meci.pdf

http://www.alegsa.com.ar/Dic/bsa.php

http://es.wikipedia.org/wiki/Tecnolog%C3%ADas_de_la_informaci%C3%B3n_y_la_comunicaci%C3%B3n

http://dexonsoftware.wordpress.com/2010/08/10/portafolio-dexon-como-herramienta-para-cumplir-normativas-estatales-y-privadas/

http://www.networkworld.es/Articulo.aspx?ida=167076&seccion=&AspxAutoDetectCookieSupport=1

Sitio en Internet, Disponible en: http://hrplopez.gov.co/hospital/index.php?option=com_frontpage&itemid=1

Sitio en Internet, Disponible en:
http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php.

Sitio en Internet, Disponible en:
http://www.es.sgs.com/es/iso_20000?serviceId=10009985&lobId=1998.

Sitio en internet, Disponible en:
http://www.virtual.unal.edu.co/cursos/agronomia/2008868/lecciones/capitulo_2/cap2lecc2.htm.

Sitio en Internet, Disponible en:
http://www.deloitte.com/view/es_PE/pe/servicios/consultoria/tecnologia-de-la-informacion/gobierno-de-ti/index.htm.

ANEXOS

ANEXO 1 DEFINICIÓN DE TÉRMINOS BASICOS

ADMINISTRACIÓN DE RIESGOS. Es una aproximación científica del comportamiento de los riesgos, anticipando posibles pérdidas accidentales con el diseño e implementación de procedimientos que minimicen la ocurrencia de pérdidas o el impacto financiero de las pérdidas que puedan ocurrir. Planear, organizar y ejecutar procesos y actividades conducentes a asegurar que la empresa esté protegida apropiadamente contra riesgos que podrían afectarla.

AUDITORÍA DE SISTEMAS. La disciplina que mediante técnicas y procedimientos aplicados en una organización por personal independiente a la operación de la misma, evalúa la función de tecnología de información y su aporte al cumplimiento de los objetivos institucionales; emite una opinión al respecto y efectúa recomendaciones para mejorar el nivel de apoyo al cumplimiento de dichos objetivos.

AUDITORÍA. La auditoria puede definirse como «un proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados, cuyo fin consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como establecer si dichos informes se han elaborado observando los principios establecidos para el caso. La disciplina que mediante técnicas y procedimientos aplicados en una organización por personas independientes a la operación de la misma, evalúa el cumplimiento de los objetivos institucionales, emite una opinión al respecto y efectúa recomendaciones para mejorar el nivel de cumplimiento de dichos objetivos.

BS 5750. La BS 5750 es una serie de normas que regulan la calidad en el Reino Unido, apareciendo antes de ISO 9000, y que sigue vigente en esta nación, siendo equivalentes sus normas a las de esta última.

La norma BS 5750, que es la de los sistemas de calidad, tiene su origen en las compras militares. Debido a la naturaleza crucial de esos productos y a los problemas prácticos de investigar los productos defectuosos usados en las acciones, se puso énfasis en ver cómo se hacen los productos

y en los sistemas de calidad de los proveedores correspondientes. Se fijaron normas apropiadas para los sistemas de calidad, incluso a nivel internacional (OTAN) para los gobiernos que cooperan y los gobiernos aliados y con normas nacionales correspondientes.

BS 9000. La norma ISO 9000 es un estándar para sistemas de administración de la calidad. La norma es publicada y mantenida por la ISO (Organización Internacional para la estandarización, aunque ISO no es un acrónimo y solo sugiere igualdad), mientras que es administrada por entidades externas de acreditación y certificación. Lo que certifica la norma es el ajuste a las especificaciones del producto o servicio, y no el concepto popular de calidad como algo objetivamente bueno.

CADENA DE VALOR. La cadena de valor empresarial, o cadena de valor, es un modelo teórico que permite describir el desarrollo de las actividades de una organización empresarial generando valor al cliente final descrito y popularizado por Michael E. Porter en su obra Competitive Advantage: Creating and Sustaining Superior Performance.

CÍRCULO DE DEMING. El ciclo PDCA, también conocido como "Círculo de Deming o circulo de Gabo" (de Edwards Deming), es una estrategia de mejora continua de la calidad en cuatro pasos, basada en un concepto ideado por Walter A. Shewhart. También se denomina espiral de mejora continua. Es muy utilizado por los SGC. Las siglas PDCA son el acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar).

CMM. El Modelo de Madurez de Capacidades o CMM (Capability Maturity Model), es un modelo de evaluación de los procesos de una organización. Fue desarrollado inicialmente para los procesos relativos al desarrollo e implementación de software por la Universidad Carnegie-Mellon para el SEI (Software Engineering Institute).

COBIT. COBIT (Objetivos de Control para Tecnología de Información y Tecnologías relacionadas) COBIT, lanzado en 1996, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de TI. Vinculando tecnología informática y prácticas de control, COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

Es precisamente 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.

CONTROL INTERNO. El Control Interno es un proceso que lleva a cabo la Alta Dirección de una organización y que debe estar diseñado para dar una seguridad razonable, en relación con el logro

de los objetivos previamente establecidos en los siguientes aspectos básicos: Efectividad y eficiencia de las operaciones; confiabilidad de los reportes financieros y cumplimiento de leyes, normas y regulaciones, que enmarcan la actuación administrativa.

COSO. Es un documento que contiene las principales directivas para la implantación, gestión y control de un sistema de Control Interno. Debido a la gran aceptación de la que ha gozado, desde su publicación en 1992, el Informe COSO se ha convertido en el estándar de referencia en todo lo que concierne al Control Interno. No puede por lo tanto faltar una sección expresamente dedicada a este documento en toda web que pretenda dedicarse a la auditoria con profesionalidad.

ENFOQUE SISTÉMICO. El enfoque sistémico es la aplicación de la teoría general de los sistemas en cualquier disciplina.

En un sentido amplio, la teoría general de los sistemas se presenta como una forma sistemática y científica de aproximación y representación de la realidad y, al mismo tiempo, como una orientación hacia una práctica estimulante para formas de trabajo
Interdisciplinarias.

Estándares. El término estándar, de origen inglés, tiene varios significados:

- originalmente, en inglés, significaba bandera; color; pancarta; especialmente nacional u otra enseña; así porta estándar (te). El significado primario moderno que le siguió fue "lo que es establecido por la autoridad, la costumbre o el consentimiento general". En este sentido se utiliza como sinónimo de norma.
- en administración estándar significa un modelo que se sigue para realizar un proceso o una guía que se sigue para no desviarnos de un lugar al que se desea llegar.
- en química analítica un estándar es una preparación que contiene una concentración conocida de una elemento específico o substancia;
- en tecnología y otros campos, un estándar es una especificación que regula la realización de ciertos procesos o la fabricación de componentes para garantizar la interoperabilidad.
- en sociolingüística, la lengua estándar es el lecto considerado habitualmente correcto para la grafía, la fonología y la sintaxis de un idioma; puede o no corresponderse exactamente con las reglas fijadas por la academia de la lengua pertinente.

GOBIERNO DE TI. El Gobierno TI es un conjunto de procedimientos, estructuras y comportamientos utilizados para lograr una mejor relación entre los actores implicados en el funcionamiento y la administración de los sistemas de información en una organización.
El Gobierno TI se basa en la conclusión de que las TI han llegado a ser la base del funcionamiento de las organizaciones actuales.

ISACA. Information Systems Audit and Control Association. Publica Cobit y emite diversas acreditaciones en el ámbito de la seguridad de la información. En las tres décadas transcurridas desde su creación, ISACA se ha convertido en una organización global que establece las pautas para los profesionales de Gobierno, Control, Seguridad y Auditoria de información. Sus normas de auditoría y control de seguridad de la información son respetados por profesionales de todo el mundo.

Los orígenes de la profesión de auditoria, control y seguridad de las TIC se encuentran en la fundación, el año 1969, en los EUA de la EDPAA (Electronic Data Processing Auditors Association).

En 1993 el nombre de la asociación cambió a ISACA (Information Systems Audit and Control Association) y en 1998 ISACA fundó el ITGI (IT Governance Institute), encargado de desarrollar y divulgar conocimientos sobre el gobierno de los sistemas de información.

ISO 9000. ISO 9000 designa un conjunto de normas sobre calidad y gestión continua de calidad, establecidas por la Organización Internacional para la Estandarización (ISO").

ISO 17799 –anteriormente BS (British Standard) 7799/1999- en el 2005. ISO 17799 es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

ISO 17799 define la información como un activo que posee valor para la organización y requiere por tanto de una protección adecuada. El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

ISO NTC 5254. NTC 5254: Norma Técnica Colombiana de Gestión de Riesgos estándar de Gestión del Riesgo Colombiano elaborado y coordinado por el comité de riesgos del Instituto Colombiano de Normas Técnicas y Certificación - ICONTEC. El NTC 5254 se fundamentó en el estándar genérico de gestión de riegos de mayor aplicación a nivel mundial AS/NZS: 4360.

ISO 2700X. ISO 2700X(ISO/IEC 17799 "(denominada también 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 año 2000.

ITIL. Las siglas de ITIL significan (Information Technology Infrastructure Library o Librería de Infraestructura de Tecnologías de Información). Metodología desarrollada a finales de los años 80's por iniciativa del gobierno del Reino Unido, específicamente por la OGC u Oficina Gobernativa de Comercio Británica (Office of Goverment Comerce).

Esta metodología es la aproximación más globalmente aceptada para la gestión de servicios de Tecnologías de Información en todo el mundo, ya que es una recopilación de las mejores prácticas tanto del sector público como del sector privado.

La Business Software Alliance (BSA). Concepto del término bsa: (Bussines Software Alliance) Agrupación que protege desde 1988 los intereses de grandes compañías del software. Tiene como objetivo principal, proteger de la piratería a esas empresas.

MECI. Es el "Modelo Estandar de Control Interno" que permite el diseño, desarrollo y operación del Sistema de Control Interno en la entidad. Sus principios son: autocontrol, autorregulación y autogestión.

Sus objetivos: Coadyuvar al logro de los objetivos institucionales permitiendo establecer las acciones, políticas, métodos, procedimientos, mecanismos de prevención, de evaluación y de mejoramiento continúo en la entidad.

RIESGO. Posibilidad de que se produzca un Impacto determinado en un Activo, en un Dominio o en toda la Organización. Es la vulnerabilidad de "bienes jurídicos protegidos" ante un posible o potencial perjuicio o daño.

Aclaración del significado: Cuanto mayor es la vulnerabilidad mayor es el riesgo (e inversamente), pero cuanto más factible es el perjuicio o daño mayor es el peligro (e inversamente). Por tanto, el riesgo se refiere sólo a la teórica "posibilidad de daño" bajo determinadas circunstancias, mientras que el peligro se refiere sólo a la teórica "probabilidad de accidente o patología" bajo determinadas circunstancias, sucesos que son causas directas de daño. Por ejemplo, cuanto mayor es la velocidad de circulación de un vehículo en carretera mayor es el "riesgo de daño", mientras que cuanto mayor es la imprudencia al conducir mayor es el "peligro de accidente" (y también es mayor el riesgo del daño consecuente). Por consiguiente, el peligro es causa de riesgo o, lo que es equivalente, el riesgo es el efecto último de todas las causas.

SARO. El Sistema de Administración del Riesgo Operativo "SARO" es el conjunto de elementos tales como las políticas, procedimientos, documentación, estructura organizacional, registro de eventos de riesgo operativo, órganos de control, plataforma tecnológica, divulgación de la

información y capacitación, mediante los cuales la entidad identifica, mide, controla y monitorea el Riesgo Operativo.

SINERGIAS. Una sinergia (del griego συνεργία, «cooperación») es el resultado de la acción conjunta de dos o más causas, pero caracterizado por tener un efecto superior al que resulta de la simple suma de las dichas causas.

SISTEMA. Un sistema es un conjunto de partes o elementos organizados y relacionados que interactúan entre sí para lograr un objetivo. Los sistemas reciben (entrada) datos, energía o materia del ambiente y proveen (salida) información, energía o materia.

SISTEMAS DE INFORMACIÓN. Un sistema de información (SI) es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su posterior uso, generados para cubrir una necesidad (objetivo). Dichos elementos formarán parte de alguna de estas categorías:

Elementos de un sistema de información.

- Personas.
- Datos.
- Actividades o técnicas de trabajo.
- Recursos materiales en general (típicamente recursos informáticos y de comunicación, aunque no tienen por qué ser de este tipo obligatoriamente).

TECNOLOGÍAS DE INFORMACIÓN. Las tecnologías de la información y la comunicación (TIC o bien NTIC para Nuevas Tecnologías de la Información y de la Comunicación o IT para «Information Technology») agrupan los elementos y las técnicas utilizadas en el tratamiento y la transmisión de las informaciones, principalmente de informática, Internet y telecomunicaciones.

TICs. Son un conjunto de servicios, redes, software y dispositivos que tienen como fin la mejora de la calidad de vida de las personas dentro de un entorno y que se integran a un sistema de información interconectado y complementario.

ANEXO 2 CARTA DE ENTREGA Y AUTORIZACION DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCION PARCIAL O TOTAL, Y PUBLICACION ELECTRONICA DEL TEXTO COMPLETO DE TESIS Y TRABAJO DE GRADO

	NORMAS PARA LA ENTREGA DE TESIS Y TRABAJOS DE GRADO A LA UNIDAD DE INFORMACION	VERSION: 01
		FECHA: Febrero 2011
		CODIGO:DOC-VACRE-NETGUDI

CARTA DE ENTREGA Y AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO DE TESIS Y TRABAJOS DE GRADO

Barranquilla, Fecha

Marque con una X
Tesis ☐ **Trabajo de Grado** ☐

Yo Roberto Carlos Diaz Alonso, identificado con C.C. No. 72181645, actuando en nombre propio y como autor de la tesis y/o trabajo de grado titulado Marco de Trabajo para Auditorias integrales de Sistemas en las micros, pequeñas y medianas Empresas Colombianas presentado y aprobado en el año 2011 como requisito para optar al título de Especialista en Auditoria de Sistemas de Información;
hago entrega del ejemplar respectivo y de sus anexos de ser el caso, en formato digital o electrónico (DVD) y autorizo a la CORPORACIÓN UNIVERSITARIA DE LA COSTA, para que en los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia, utilice y use en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador de la obra objeto del presente documento.

Y autorizo a la Unidad de información, para que con fines académicos, muestre al mundo la producción intelectual de la Corporación Universitaria de la Costa, a través de la visibilidad de su contenido de la siguiente manera:

Los usuarios puedan consultar el contenido de este trabajo de grado en la página Web de la Facultad, de la Unidad de información, en el repositorio institucional y en las redes de información del país y del exterior, con las cuales tenga convenio la institución y Permita la consulta, la reproducción, a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato DVD o digital desde Internet, Intranet, etc., y en general para cualquier formato conocido o por conocer.

El AUTOR - ESTUDIANTES, manifiesta que la obra objeto de la presente autorización es original y la realizó sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de su exclusiva autoría y detenta la titularidad ante la misma. PARÁGRAFO: En caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión, EL ESTUDIANTE - AUTOR, asumirá toda la responsabilidad, y saldrá en defensa de los derechos aquí autorizados; para todos los efectos, la Universidad actúa como un tercero de buena fe.

Para constancia se firma el presente documento en dos (02) ejemplares del mismo valor y tenor, en Barranquilla D.E.I.P., a los 24 días del mes de Octubre de Dos Mil Once 2011

EL AUTOR - ESTUDIANTE: _____
FIRMA

	NORMAS PARA LA ENTREGA DE TESIS Y TRABAJOS DE GRADO A LA UNIDAD DE INFORMACION	VERSION: 01
		FECHA: Febrero 2011
		CODIGO:DOC-VACRE-NETGUDI

CARTA DE ENTREGA Y AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO DE TESIS Y TRABAJOS DE GRADO

Barranquilla, Fecha

Marque con una X
Tesis ☐ **Trabajo de Grado** ☐

Yo Luis Carlos Brieva Berrio, identificado con C.C. No. 1128047694, actuando en nombre propio y como autor de la tesis y/o trabajo de grado titulado Marco de Trabajo para Auditorias integrales de Sistemas en las micros, pequeñas y medianas empresas Colombianas presentado y aprobado en el año 2011 como requisito para optar al título de Especialista en Auditoria de Sistemas de Información; hago entrega del ejemplar respectivo y de sus anexos de ser el caso, en formato digital o electrónico (DVD) y autorizo a la CORPORACIÓN UNIVERSITARIA DE LA COSTA, para que en los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, Decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia, utilice y use en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador de la obra objeto del presente documento.

Y autorizo a la Unidad de información, para que con fines académicos, muestre al mundo la producción intelectual de la Corporación Universitaria de la Costa, a través de la visibilidad de su contenido de la siguiente manera:

Los usuarios puedan consultar el contenido de este trabajo de grado en la página Web de la Facultad, de la Unidad de información, en el repositorio institucional y en las redes de información del país y del exterior, con las cuales tenga convenio la institución y Permita la consulta, la reproducción, a los usuarios interesados en el contenido de este trabajo, para todos los usos que tengan finalidad académica, ya sea en formato DVD o digital desde Internet, Intranet, etc., y en general para cualquier formato conocido o por conocer.

El AUTOR - ESTUDIANTES, manifiesta que la obra objeto de la presente autorización es original y la realizó sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de su exclusiva autoría y detenta la titularidad ante la misma. PARÁGRAFO: En caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión, EL ESTUDIANTE - AUTOR, asumirá toda la responsabilidad, y saldrá en defensa de los derechos aquí autorizados; para todos los efectos, la Universidad actúa como un tercero de buena fe.

Para constancia se firma el presente documento en dos (02) ejemplares del mismo valor y tenor, en Barranquilla D.E.I.P., a los 24 días del mes de Octubre de Dos Mil once 200 11

EL AUTOR - ESTUDIANTE. LUIS CARLOS BRIEVA BERRIO

FIRMA

ANEXO 3 FORMULARIO DE LA DESCRIPCION DE LA TESIS O DEL TRABAJO DE GRADO

	NORMAS PARA LA ENTREGA DE TESIS Y TRABAJOS DE GRADO A LA UNIDAD DE INFORMACION	VERSION: 01 FECHA: Febrero 2011 CODIGO:DOC-VACRE-NETGUDI

F ORMULARIO DE LA DESCRIPCIÓN DE LA TESIS O DEL TRABAJO DE GRADO

TÍTULO COMPLETO DE LA TESIS O TRABAJO DE GRADO:

Marco de Trabajo para Auditorías integrales de Sistemas en las micros, pequeñas y medianas Empresas Colombianas.

SUBTÍTULO, SI LO TIENE:

AUTOR AUTORES

Apellidos Completos	Nombres Completos
Díaz Alonso	Roberto Carlos
Brieva Berrío	Luis Carlos

DIRECTOR (ES)

Apellidos Completos	Nombres Completos

JURADO (S)

Apellidos Completos	Nombres Completos

ASESOR (ES) O CODIRECTOR

Apellidos Completos	Nombres Completos

TRABAJO PARA OPTAR AL TÍTULO DE: Especialista en Auditoría de Sistemas de Información.

FACULTAD: _____

PROGRAMA: Pregrado ____ Especialización X

NOMBRE DEL PROGRAMA Especialización en Auditoría de Sistemas de Información.

ANEXO 4 NORMAS PARA LA ENTREGA TESIS Y TRABAJO DE GRADO A LA UNIDAD DE INFORMACION

	NORMAS PARA LA ENTREGA DE TESIS Y TRABAJOS DE GRADO A LA UNIDAD DE INFORMACION	VERSION: 01 FECHA: Febrero 2011 CODIGO:DOC-VACRE-NETGUDI

CIUDAD: Barranquilla **AÑO DE PRESENTACIÓN DEL TRABAJO DE GRADO:** 2011

NÚMERO DE PÁGINAS 95

TIPO DE ILUSTRACIONES:

- ☐ Ilustraciones
- ☐ Láminas
- ☐ Retratos
- ☒ Tablas, gráficos y diagramas
- ☐ Planos
- ☐ Mapas
- ☐ Fotografías

MATERIAL ANEXO (Vídeo, audio, multimedia o producción electrónica):

Duración del audiovisual: _____ minutos.

Número de casetes de vídeo: _____ Formato: VHS ___ Beta Max ___ ¾ ___ Beta Cam ____

Mini DV ____ DV Cam ____ DVC Pro ____ Vídeo 8 ____ Hi 8 ____

Otro. Cuál? _____

Sistema: Americano NTSC _____ Europeo PAL _____ SECAM _____

Número de casetes de audio: _____

Número de archivos dentro del DVD (En caso de incluirse un DVD diferente al trabajo de grado):

_____

PREMIO O DISTINCIÓN *(En caso de ser LAUREADAS o tener una mención especial)*:

_____

DESCRIPTORES O PALABRAS CLAVES EN ESPAÑOL E INGLÉS: Son los términos que definen los temas que identifican el contenido. (*En caso de duda para designar estos descriptores, se recomienda consultar con la Unidad de Procesos Técnicos de la Unidad de información en el correo biblioteca@cuc.edu.co, donde se les orientará).*

ESPAÑOL	INGLÉS
Esto se encuentra dentro del Proyecto	

RESUMEN DEL CONTENIDO EN ESPAÑOL E INGLÉS:(Máximo 250 palabras-1530 caracteres):

Esto se encuentra dentro del Proyecto