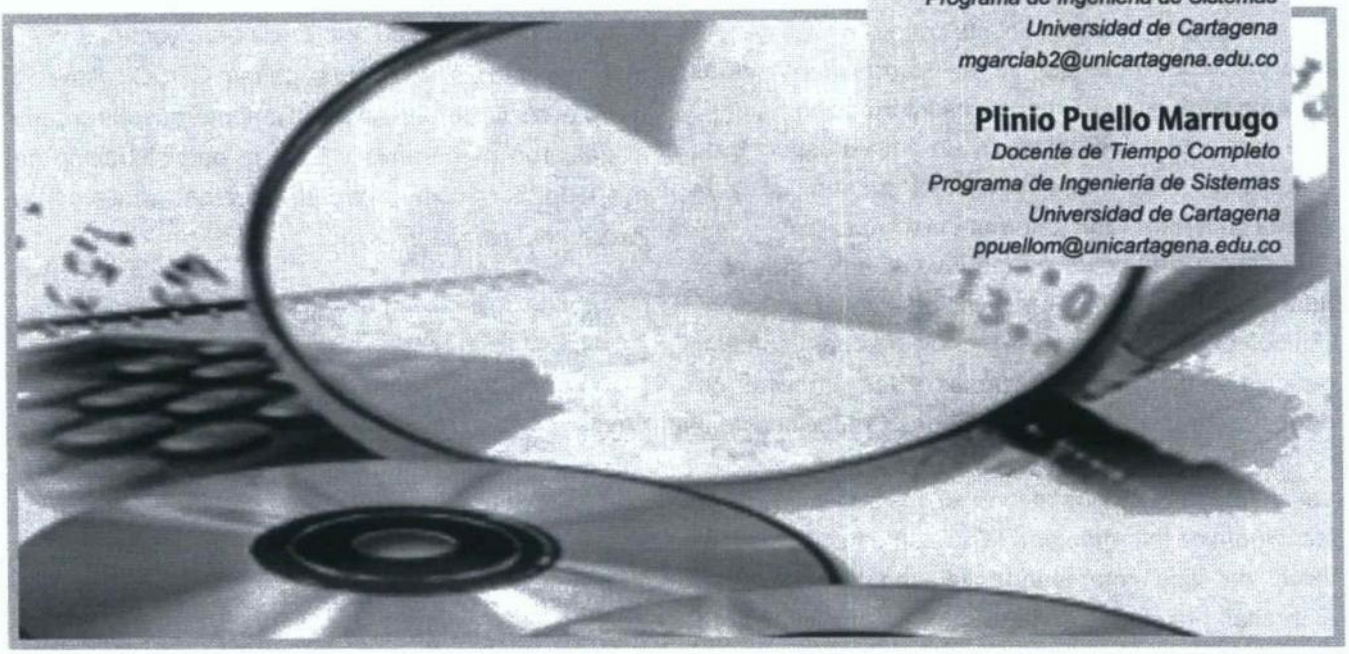
Método cobit y su aplicación

Diana Marcela Mendoza del Risco
Ingeniera de Sistemas
Universidad de Cartagena
diana_m2r@ingenieros.com

Miguel Ángel García Bolaños
Docente de Tiempo Completo
Programa de Ingeniería de Sistemas
Universidad de Cartagena
mgarciab2@unicartagena.edu.co

Plinio Puello Marrugo
Docente de Tiempo Completo
Programa de Ingeniería de Sistemas
Universidad de Cartagena
ppuellom@unicartagena.edu.co



RESUMEN: En toda organización un elemento crítico para la supervivencia es la correcta administración de la información y de las tecnologías de la información o TI. Para muchas organizaciones la información y las tecnologías que las manipulan representan los activos más importantes. En búsqueda de proteger estos elementos se han diseñado distintos mecanismos o métodos para asegurar la integridad, confiabilidad, seguridad y disponibilidad de los mismos a través de las auditorías informáticas, este trabajo se centrará en el método COBIT, sus características y su aplicación, como un mecanismo eficaz en el proceso de las auditorias.

Palabras Claves: Auditoría Informática, COBIT, Metodología, Aplicación.

ABSTRACT: In any organization a critical element for survival is the proper information management and information technology or IT. For many organizations the information and the technologies that manipulate them represent the most important assets. Seeking to protect these elements there are different mechanisms or methods designed to ensure the integrity, reliability, security and availability of data through computer audits, this paper will focus on the COBIT approach, its characteristics and its application as an effective mechanism in the process of audits.

Keywords: Computer Audit, COBIT, Methodology, Application.

1. introducción

Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de la información y de la Tecnología de Información (TI) vinculada a esta labor. En esta sociedad global (donde la información viaja a través del "ciberespacio" sin las restricciones de tiempo, distancia y velocidad). (Mendoza, 2010), este aspecto crítico emerge de:

· La creciente dependencia en información y en los sistemas que proporcionan dicha información
· La creciente vulnerabilidad y un amplio espectro de amenazas, tales como las "ciber amenazas" y la guerra de información (information warfare).
· La escala y el costo de las inversiones actuales y futuras en información y en tecnología de información;
· El potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos

Las empresas exitosas reconocen los beneficios de la tecnología de información y la utilizan para impulsar el valor de sus interesados (stakeholders). Estas empresas también entienden y administran los riesgos asociados, tales como el aumento en requerimientos regulatorios, así como la dependencia crítica de muchos procesos de negocio en TI.

Por ello la necesidad del aseguramiento del valor de TI, la administración de los riesgos asociados estas TI, así como el incremento de requerimientos para controlar la información, se entienden ahora como elementos clave del Gobierno Corporativo. El valor, el riesgo y el control constituyen la esencia del gobierno de TI[i].

El gobierno de TI es responsabilidad de los ejecutivos, del consejo de directores y consta de liderazgo, estructuras y procesos organizacionales que garantizan cual TI en la empresa sostiene y extiende las estrategias y objetivos organizacionales.

Más aún, el gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que estas soporten los objetivos del negocio, permitiendo el aprovechamiento de la información, maximizando así los beneficios, capitalizando las oportunidades y ganando ventajas competitivas. Estos resultados requieren un marco de referencia para controlar la TI, que se ajuste y sirva como soporte a COSO[ii], el marco de referencia de control ampliamente aceptado para el gobierno corporativo y para la administración de riesgos, así como otros recursos similares e igualmente compatibles[iii].

Las organizaciones deben alcanzar los estándares de calidad, satisfacer los requerimientos fiduciarios y de seguridad de su información, así como de todos sus activos. La dirección también debe optimizar el uso de los recursos disponibles de TI, incluyendo aplicaciones, información, infraestructura y personas. Para descargar estas responsabilidades, así como para lograr sus objetivos, la dirección debe entender el estatus de su arquitectura empresarial para TI y decidir qué tipo de gobierno y de control debe aplicar.

2. COBIT

Los Objetivos de Control para la Información y la Tecnología relacionada (COBIT) brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas de COBIT son la representación de lo que según los expertos consideran son la mejor decisión. Están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones habilitadas por TI, asegurando la entrega del servicio y brindando una medida contra la cual juzgar cuando las cosas no vayan bien.

Para que TI satisfaga con éxito los requerimientos del negocio, la dirección debe implementar un sistema de control interno o un marco de trabajo. El marco de trabajo de control COBIT contribuye a estas necesidades de la siguiente manera[iv]:

· Estableciendo un vínculo con los requerimientos del negocio
· Organizando las actividades de TI en un modelo de procesos generalmente aceptado
· Identificando los principales recursos de TI a ser utilizados
· Definiendo los objetivos de control gerenciales a ser considerados

La orientación al negocio que enfoca COBIT consiste en alinear las metas de negocio con las metas de TI, brindando métricas y modelos de madurez para medir sus logros, e identificando las responsabilidades asociadas del dueño de los procesos de negocio y de TI.

En términos generales, COBIT es un grupo de indicadores que permiten tener una idea de cómo va un proyecto determinado. Se encuentra actualmente en la versión 4.1 y fueron creados por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA).
Consta de una serie de procesos que se describen a continuación (Boletin 54, 2007):

· Planeación y Organización. Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.
· Adquisición e Implementación. Para llevar a cabo la estrategia de TI, las soluciones de esta deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.
· Servicios y Soporte: En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.
· Seguimiento. Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

COBIT es un marco de referencia y un grupo de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los Interesados (Stakeholders). COBIT permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas. COBIT constantemente se actualiza y armoniza con otros estándares. Por lo tanto, COBIT se ha convertido en el integrador de las mejores prácticas y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con el negocio. La estructura de procesos de COBIT y su enfoque de alto nivel orientado a la empresa brindan una visión completa de TI y de las decisiones a tomar acerca de la misma.

Los beneficios de implementar COBIT como marco de referencia de gobierno sobre TI incluyen[v]:

· Mejor alineación, con base en su enfoque de negocios.
· Una visión, entendible para la gerencia, de lo que hace TI.
· Propiedad y responsabilidades claras, con base en su orientación a procesos.
· Aceptación general de terceros y reguladores.
·Entendimiento compartido entre todos los Interesados, con base en un lenguaje común.
· Cumplimiento de los requerimientos COSO para el ambiente de control de TI.

3. Requerimientos de COBIT

COBIT asegura que existan productos de calidad, que a través de ciertas métricas o indicadores es posible conseguir. Para ello deben existir planes de contingencia, esto es conocido como Framework de Continuidad, (Ferrer, 2010), que garantiza que exista integridad y de ésta forma poder evitar la pérdida de la información.

Se necesita un sistema alterno con las mismas capacidades que el sistema principal o dependiendo de las políticas organizacionales (variando la capacidad de un 20% a un 50%) que especifique la entidad, y que sea funcional las 24 horas los 7 días de la semana durante todo el año, que reaccione al instante en caso de que el sistema principal deje de funcionar.

Esto posiblemente implique que ambos sistemas se encuentren interconectados y sincronizados de tal forma que cualquier evento quede registrado en el sistema alterno. Sin embargo, otra solución sería mantener backups constantes, aunque esto no es muy seguro dado que ante cualquier daño físico, los procesos dentro del mismo pueden corromperse o dañarse y la continuidad se vería comprometida.

En nuestro medio un sistema así resulta muy complicado, dado que todo se traduce en costos; el tener otro que sea utilizado solo cuando el actual falle sería algo innecesario e inapropiado.
Es necesario realizar un análisis de riesgos, para poder identificar los elementos necesarios y los procesos que vale la pena realizar, puesto que al ser un sistema costoso, no representa algo fácil de asumir.
Actualmente, si se desea implementar una metodología de éste tipo se hace necesario transformar muchos de los esquemas manejados en la actualidad.

4. Estado del Arte del Modelo COBIT

Como se mencionó previamente COBIT actualmente va por la versión 4.1, a continuación se describirán algunos antecedentes relacionados a éste modelo con el fin de demarcar la tendencia a la que se dirige en nuestra actualidad.

COBIT ha sido desarrollado como un estándar generalmente aplicable y aceptado para las buenas prácticas de seguridad y control en Tecnología de Información (TI). Se fundamenta en los Objetivos de Control existentes de la Information Systems Audit and Control Foundation (ISACF), mejorados a partir de estándares internacionales técnicos, profesionales, regulatorios y específicos para la industria, tanto existentes como en surgimiento. Los Objetivos de Control resultantes han sido desarrollados para su aplicación en sistemas de información en toda la empresa. El término "generalmente aplicable y aceptado" es utilizado explícitamente en el mismo sentido que los Principios de Contabilidad Generalmente Aceptados (PCGA o GAAP por sus siglas en inglés). Para propósitos del proyecto, "buenas prácticas" significa consenso por parte de los expertos[vi].

Este estándar es relativamente pequeño en tamaño, cuyo fin es el de ser práctico y responde, en la medida de lo posible, a las necesidades de negocio, manteniendo al mismo tiempo una independencia con respecto a las plataformas técnicas de TI adoptadas en una organización. El proporcionar indicadores de desempeño (normas, reglas, etc.), ha sido identificado como prioridad para las mejoras futuras que se realizarán al marco referencial.

El desarrollo de COBIT, ha traído como resultado la publicación del Marco Referencial general y de los Objetivos de Control detallados, y le seguirán actividades educativas. Estas actividades asegurarán el uso general de los resultados del Proyecto de Investigación COBIT.

El desarrollo de COBIT ha resultado en la publicación de:

a) Resumen Ejecutivo. El cual, adicionalmente a esta sección de antecedentes, consiste en un Síntesis Ejecutiva (que proporciona a la alta gerencia entendimiento y conciencia sobre los conceptos clave y principios de COBIT) y el Marco Referencial (el cual proporciona a la alta gerencia un entendimiento más detallado de los conceptos clave y principios de COBIT e identifica los cuatro dominios de COBIT y los correspondientes 34 procesos de TI);

b) Marco Referencial. Que describe en detalle los 34 objetivos de control de alto nivel e identifica los requerimientos de negocio para la información y los recursos de TI que son impactados en forma primaria por cada objetivo de control.

c) Objetivos de Control. Los cuales contienen declaraciones de los resultados deseados o propósitos a ser alcanzados mediante la implementación de 302 objetivos de control detallados y específicos a través de los 34 procesos de TI;

d) Guías de Auditoría. Las cuales contienen los pasos de auditoría correspondientes a cada uno de los 34 objetivos de control de TI de alto nivel para proporcionar asistencia a los auditores de sistemas en la revisión de los procesos de TI con respecto a los 302 objetivos detallados de control recomendados para proporcionar a la gerencia certeza o unas recomendaciones de mejoramiento.

e) Conjunto de Herramientas de Implementación. El cual proporciona lecciones aprendidas por organizaciones que han aplicado COBIT rápida y exitosamente en sus ambientes de trabajo.

COBIT evolucionará a través de los años y será el fundamento de investigaciones futuras. Por lo tanto, se generará un familia de productos COBIT y al ocurrir esto, las tareas y actividades que sirven como la estructura para organizar los Objetivos de Control de TI, serán refinadas posteriormente; también será revisado el balance entre los dominios y los procesos a la luz de los cambios en la industria.

Una temprana adición significativa visualizada para la familia de productos COBIT, es el desarrollo de las Guías Gerenciales (Management Guidelines) que incluyen Factores Críticos de Éxito, Indicadores Clave de Desempeño y Medidas Comparativas (Benchmarks). Esta adición proporcionará herramientas a la gerencia para evaluar el ambiente de TI de su organización con respecto a los 34 objetivos de control de alto nivel de COBIT. Los factores críticos de éxito identificarán los aspectos o acciones más importantes para la administración y tomar dichas acciones o considerar los aspectos para lograr el control sobre sus procesos de TI. Los Indicadores Clave de Desempeño proporcionarán medidas de éxito que permitan conocer a la gerencia si un proceso de TI está alcanzando los requerimientos de negocio. Las Medidas Comparativas definirán niveles de madurez que pueden ser utilizadas por la gerencia para:

· Determinar el nivel actual de madurez de la empresa
· Determinar el nivel de madurez que desea lograr, como una función de sus riesgos y objetivos
· Proporcionar una base de comparación de sus prácticas de control de TI contra empresas similares o normas de la industria.

Las investigaciones y publicaciones han sido posible gracias a contribuciones de Unysis, Unitech Systems, Inc., MIS Training Institute, Zergo, Ltd., y Coopers & Lybrand. El Forum Europeo de Seguridad (European Security Forum -ESF-) amablemente puso a disposición material para el proyecto. Otras donaciones fueron recibidas de capítulos miembros de ISACA de todo el mundo.

5. Caso de Estudio

En el artículo "Método para el Control Interno de TI en MyPes Basado en Metodología COBIT", (Urquizo, 2010), se plantea la necesidad de utilizar COBIT como mecanismo de solución a dos problemáticas importantes: debilidad en la aplicación de metodologías similares y el acceso limitado a herramientas computacionales.

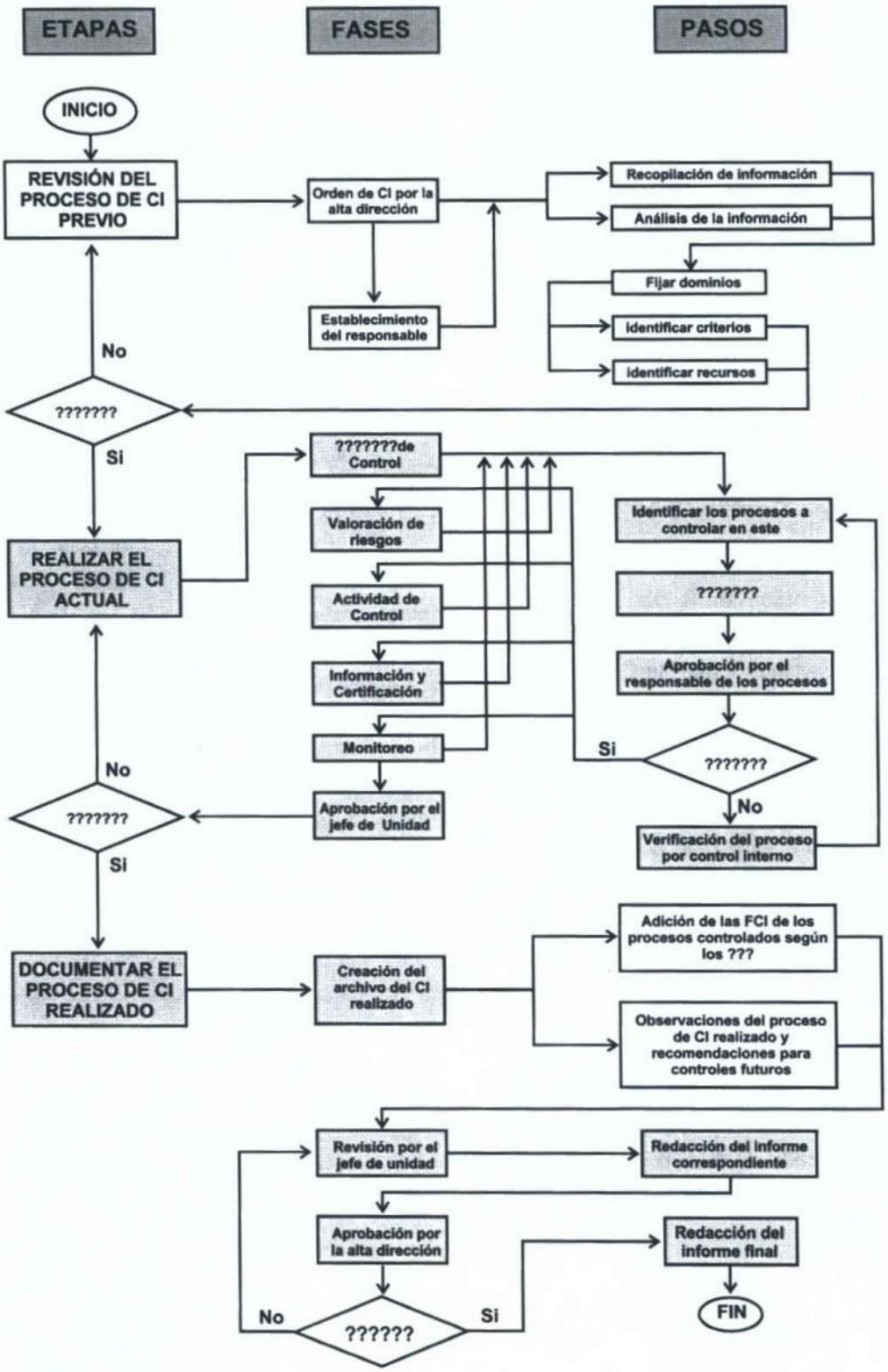
Con base en lo anterior se trazó como objetivo principal "Desarrollar un método que guíe la realización del control interno de tecnologías de información utilizando la metodología COBIT para medianas y pequeñas empresas, para realizar la presentación formal de información apoyando una adecuada la toma de decisiones y a la vez permitiendo controlar las tecnologías de información de manera efectiva."[vii]]

Teniendo como objetivos específicos
a) Realizar un análisis de la metodología COBIT e interrelacionarla con los componentes del control interno para determinar la cantidad de puntos coincidentes.
b) Plantear las guías de la metodología COBIT sobre el control interno de tecnologías de información para exponer la aplicabilidad de dicha metodología.

c) Desarrollar técnicas de control formales para las tecnologías de información de acuerdo al tamaño de las medianas y pequeñas empresas así como de la cantidad de personal con el que cuenten a fin de proporcionar un método que posea la capacidad de disgregación.

d) Proporcionar un prototipo de sistema que permita realizar el control interno de las tecnologías de información de manera automatizada, para facilitar la aplicación práctica del método.[viii]

El método desarrollado está conformado por 3 etapas: La etapa inicial viene constituida por la revisión del control interno previo, y se genera una nueva orden considerando aquellos puntos que presenten debilidades, al realizar una recopilación de la información y posteriormente un análisis de la misma, luego se fijan dominios y finalmente se identifican criterios y recursos, de otra forma se inicia una orden inicial (desde cero)


ETAPAS
FASES
PASOS
INICIO
REVISIÓN DEL PROCESO DE CI PREVIO
Orden de CI por la alta dirección
Establecimiento del responsable
Recopilación de información
Análisis de la información
Fijar dominios
identificar criterios
identificar recursos
No
???????
Si
REALIZAR EL PROCESO DE CI ACTUAL
???????de Control
Valoración de riesgos
Actividad de Control
Información y Certificación
Monitoreo
Aprobación por el jefe de Unidad
Identificar los procesos a controlar en este
???????
Aprobación por el responsable de los procesos
???????
Si
No
Verificación del proceso por control interno
No
???????
Si
DOCUMENTAR EL PROCESO DE CI REALIZADO
Creación del archivo del CI realizado
Adición de las FCI de los procesos controlados según los ???
Observaciones del proceso de CI realizado y recomendaciones para controles futuros
Revisión por el jefe de unidad
Redacción del informe correspondiente
Aprobación por la alta dirección
Redacción del informe final
No
??????
Si
FIN

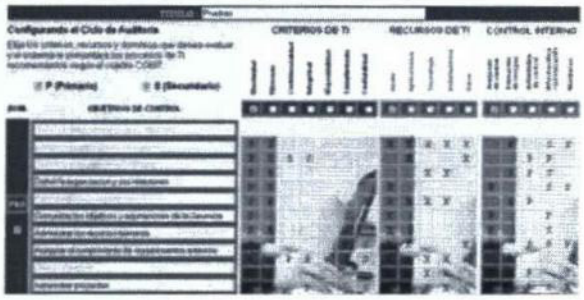
En la segunda etapa ya se realiza el Control Interno como tal recurriendo a las "Fichas de Control Interno" elaboradas, dentro de las cuales se resumen todos los procesos que deben llevarse a cabo. Cumpliendo con las fases de Antecedentes de Control, Valoración de Riesgos, Actividades de Control, Información y Comunicación para posteriormente realizar Monitoreo, acarreando actividades como Identificación a procesos de controles, Información a las Fichas de Control de los procesos identificados y Aprobación por el responsable de los procesos. Si no se cuenta con esta última aprobación entonces debe iniciarse nuevamente cada actividad, de ser lo contrario entonces debe recibir la Aprobación por el Jefe de la Unidad, que constituye la fase definitiva de ésta etapa.

Finalmente, la última etapa, en la cual se procede a documentar todo el proceso realizado, en este caso solo se deberá anexar las Fichas de Control Interno evaluadas, añadiendo el campo de observaciones si amerita el caso. Luego debe recibir una revisión por el Jefe de la Unidad y redactar el informe correspondiente para posteriormente contar con la aprobación por la Alta Dirección y proceder a la redacción del informe final, la situación contraria implicaría que todo el proceso de revisiones debe ser llevado a cabo nuevamente a partir del jefe de la unidad.

Una vez concluido el desarrollo del método COBIT, se procedió a plasmar el mismo en un prototipo de sistema tomando como metodología de desarrollo: RUP (Proceso Unificado Rational) en sus cuatro etapas:

· Inicio
· Elaboración
· Construcción
· Transición

Obteniendo como resultado un prototipo de fácil manejo para cualquier tipo de usuario, tal como se puede observar en el gráfico inferior:



6. Conclusión

COBIT es un marco de referencia, contiene un conjunto de herramientas y mecanismos que permiten obtener productos de calidad, basados en puntos específicos, los cuales son: Planeación y Organización, Adquisición e Implementación, Servicios y Soporte y finalmente Monitoreo. Cada una de estas actividades se encuentra subdividida y abarca una serie mucho más puntual de ejercicios.

La finalidad de COBIT es garantizar la efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información y de las herramientas de TI utilizadas en el proceso.

Aunque implementar este modelo representa costos y gastos para la administración de la organización, es eficaz y ha demostrado que funciona. Mediante el caso de estudio propuesto se comprobó que utilizando el modelo COBIT fue posible alcanzar las metas propuestas y el producto obtenido satisface las necesidades que la empresa manifestaba.

Referencias

Objetivos de Control para la Información y las Tecnologías Relacionadas. Decreto No 1806/99 – Resolución No 54. Gobierno de Mendoza. Fuente: www.isaca.org. Disponible en: http://www.comip.mendoza.gov.ar/cobit.doc. Consultado el día 16 de mayo de 2010.

Ferrer, O. F. Business Continuity Management. SISTESEG. Disponible en: http://www.sisteseg.com/files/Microsoft_PowerPoint_-_BCP_DRP_Metodolog_a_y_Conceptos.pdf. Consultado el día 23 de mayo de 2010

COBIT: Modelo para la auditoría y control de sistemas de información. Universidad EAFIT. Boletín 54. Publicado el día 10 de mayo de 2007. Disponible en: http://www.eafit.edu.co/NR/rdonlyres/5D56F83D-3D20-475D-914C-7C54C6494A6B/0/boletin54COBITMODELOPARAAUDITORIAYCONTROLDESISTEMASDEINFORMACI%C3%93N.pdfConsultado el día 28 de mayo de 2010

Urquizu, A. Método para el Control Interno de TI en MyPes Basado en la Metodología COBIT. Novedades Bolivarianas en Seguridad y TI – NOBOSTI. Disponible en: http://www.nobosti.com/spip.php?article375. Consultado el día 7 de junio de 2010

Notas

[i] Cobit 4.1. IT Governance Institute. Disponible en: http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=55981. Consultado el día 28 de mayo de 2010

[ii] COSO: Committee Of Sponsoring Organizations Of The Treadway Commission

[iii] Op. cit Mendoza, 2010.

[iv] Op cit: http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=55981, consultado el 30 de *mayo del* 2010.

[v] Ibídem

[vi] Op cit: Mendoza, 2010

[vii] Urquizu, A. Método para el Control Interno de TI en MyPes Basado en la Metodología COBIT. Novedades Bolivarianas en Seguridad y TI – NOBOSTI. Disponible en: http://www.nobosti.com/spip.php?article375. Consultado el día 3 dejunio de 2010

[viii] ibidem