

**GUÍAS DE AUDITORÍA PARA EL DIAGNÓSTICO DE UN MODELO DE
GOBIERNO DE TI FUNDAMENTADO EN LOS LINEAMIENTOS
ESTABLECIDOS POR COBIT 4.1 E ITIL 3.0.**

**MARIA LUISA ÁVILA GOLDFARB
DEISY ESTHER CASTRO MARQUEZ
GRACE MARIA SANCHEZ PATERNOSTRO**

**UNIVERSIDAD DE LA COSTA
ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS DE INFORMACIÓN
BARRANQUILLA, ATLANTICO
2013**

**GUÍAS DE AUDITORÍA PARA EL DIAGNÓSTICO DE UN MODELO DE
GOBIERNO DE TI FUNDAMENTADO EN LOS LINEAMIENTOS
ESTABLECIDOS POR COBIT 4.1 E ITIL 3.0.**

**MARIA LUISA ÁVILA GOLDFARB
DEISY ESTHER CASTRO MARQUEZ
GRACE MARIA SANCHEZ PATERNOSTRO**

DIRECTOR: ING. VICTOR MONTAÑO ARDILA

**TESIS PRESENTADA PARA OBTAR AL TÍTULO DE ESPECIALISTA EN
AUDITORÍA DE SISTEMAS DE INFORMACIÓN**

**UNIVERSIDAD DE LA COSTA
FACULTAD DE POSTGRADO
ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS DE INFORMACIÓN
BARRANQUILLA, ATLANTICO
2013**

NOTA DE ACEPTACION

Firma del Presidente del Jurado

Firma del Jurado N° 1

Firma del Jurado N° 2

Barranquilla, Diciembre de 2013

RESUMEN

Este proyecto fue desarrollado para que dentro de las organizaciones el personal involucrado, La alta dirección, los gerentes, auditores, oficiales de cumplimiento y directores de TI, trabajen en armonía para estar seguros que las mejores prácticas los conducen a servicios de TI económicos y bien controlados. Además, para que pueda ser usado como punto de referencia para la construcción de una herramienta personal que permita la evaluación de la empresa auditada.

Los lineamientos tomados de COBIT e ITIL suministran una base a las organizaciones para implementar servicios sólidos y eficaces para apoyar a sus clientes en su negocio, y para seguir haciéndolo en el largo plazo.

PALABRAS CLAVES

Gobierno de TI, Gestión de Servicios de TI, Seguridad de la Información, Gestión de Riesgos de TI, Niveles de Acuerdo de Servicios (SLAs), Acuerdo de Nivel Operativo (OLAs), Indicador clave de rendimiento (KPI), Paquete principal de servicio (CSP).

ABSTRACT

This project was developed for that within organizations, the stakeholders(top management, managers, auditors, compliance officers and IT managers), works in harmony to make sure that best practices lead them to affordable IT and well controlled. In addition to that it can be used as a reference point for building a personal tool that allows the evaluation of the audited company.

The guidelines taken from COBIT and ITIL provide a basis for organizations to implement strong and effective services to support customers in their business and to keep doing it in the long run.

KEY WORDS

IT Governance, IT Service Management, Information Security, IT Risk Management, Service Level Agreement (SLAs), Operative Level Agreement (OLAs), Key Performance Indicator (KPI), Core Service Package (CSP).

DEDICATORIA

Primero que todo agradecer a Dios por permitirme llevar a cabo y culminar la especialización y este proyecto de grado.

A mi familia por apoyarme en todo momento, por su comprensión y confianza.

A mis compañeros de trabajo y amigas por el compromiso y empeño que le pusimos cada uno de nosotros para sacar adelante este proyecto, en especial Grace Sánchez por toda la paciencia que nos tuvo.

A mis amigos de siempre que me apoyaron en todo momento y siempre estuvieron pendientes de mí.

Especialmente al Ingeniero Víctor Montaña Ardila por su constante ayuda y guía en el proyecto, porque siempre tuvo confianza en nosotras.

Ing. María Luisa Avila Goldfarb

DEDICATORIA

A través de la presente dedicatoria, deseo agradecer ante todo a Dios y a mis padres por el apoyo continuo y sostenible para la culminación de esta tesis de Especialización de Grado.

Agradezco también a mis compañeras de tesis que sin su valiosa ayuda incondicional y tenacidad a lo largo de la elaboración de este documento habría sido imposible su culminación.

Agradezco a mi Tutor de tesis, Victor Manuel Montaña Ardila, por haber creído en la realización de este proyecto y agradecerle su ayuda, paciencia, conocimiento, consejos y sus buenas prácticas, en todo momento, para la exitosa culminación de éste.

Por último, agradezco a todos mis compañeros de Especialización de forma general por su apoyo y buena amistad en el periodo en que compartimos el curso de este programa de Especialización.

Ing. Desiy Castro Marquez.

DEDICATORIA

Mi tesis la dedico con todo mi amor y cariño:

A DIOS que me dio la oportunidad de vivir y de regalarme una familia maravillosa.

A mis padres que me dieron la vida y han estado conmigo en todo momento. Gracias por todo papá y mamá por darme una carrera para mi futuro y por creer en mí. Los quiero con todo mi corazón y este trabajo es para ustedes.

A mis hermanos Sthefanny, Luis y Jose gracias por estar conmigo y apoyarme siempre. Y a mi sobrino Joshua que siempre esta en mi corazón.

A mi amor Luis, por siempre estar a mi lado, brindándome todo su amor, entrega, dedicación. Mil gracias porque siempre estas a mi lado sin condiciones.

A mi hijo Angelo, porque lucharé siempre por ser un ejemplo a seguir en todos los aspectos de mi vida y hacer que pueda sentirse siempre orgulloso.

A mis compañeras y a nuestro director Victor Manuel Montaña Ardila porque a pesar de las dificultades logramos sacar adelante el proyecto.

Ing. Grace Sanchez Paternostro

CONTENIDO

1. INTRODUCCIÓN	1
2. PLANTEAMIENTO DEL PROBLEMA	2
3. JUSTIFICACIÓN	3
4. OBJETIVOS	4
4.1. Objetivo General	
4.2. Objetivos Específicos	
5. MARCOS REFERENCIALES	5
5.1. Marco Teórico	5
5.1.1. Antecedentes y Teorías Básicas del Problema	5
5.1.2. Marco Conceptual	15
5.2. Marco Legal	17
5.3. Delimitaciones	17
5.3.1. Delimitación Temporal	
5.3.2. Delimitación Espacial	
5.4. Limitaciones	17
6. DISEÑO METODOLÓGICO	18
6.1 Tipo de Investigación	18
6.2 Método de Investigación	18
6.3 Técnicas de Recolección de Información	18
7. CONCLUSION	19
8. BIBLIOGRAFIA	20

1. INTRODUCCIÓN

En la actualidad es necesario aplicar estándares de mejores prácticas como una herramienta para dirigir y supervisar todas las actividades relacionadas con el gobierno de TI, estableciendo pautas que nos permitan escoger el Marco de Referencia que se quiere implementar así como también definir la posición de una empresa frente a determinado Marco de Referencia y de esta manera definir hacia donde se quiere llegar así como también hasta donde es conveniente que la empresa llegue. También es necesario que los auditores puedan orientar a la alta dirección en el proceso de selección de estos estándares y la aplicación en la empresa, determinando entonces cual es el estándar conveniente y la posición de la empresa frente al mismo, para esto debe contar con el conocimiento y la información suficiente que le permita desarrollar a cabalidad todos los procesos.

En el caso específico de este proyecto el grupo investigador ha querido recopilar material relevante de las Mejores Prácticas para el Gobierno de TI utilizando los Marcos de Referencia COBIT e ITIL complementándolas con las Guías de Aseguramiento de COBIT, con el fin de diseñar un documento que pueda ser usado como punto de referencia para la construcción de una herramienta personal que permita la evaluación de la empresa auditada.

COBIT es un marco de referencia globalmente aceptado para el gobierno de TI basado en estándares de la industria y las mejores prácticas. Una vez implementado, los ejecutivos pueden asegurarse que se ajusta de manera eficaz con los objetivos del negocio y dirigir mejor el uso de TI para obtener ventajas comerciales.

ITIL es un marco de trabajo de las mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI). ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI.

Los procesos de ITIL pueden ser utilizados para lograr y demostrar el cumplimiento con los objetivos de control COBIT. En el documento a desarrollar el grupo investigador tomara los puntos articulables entre los marcos de referencia de COBIT e ITIL, estructurándolos de tal manera que sea posible proporcionar al auditor las Guías de Auditoria con base en un modelo articulado de COBIT e ITIL para de esta manera lograr un desarrollo eficiente y eficaz de las iniciativas de aseguramiento para el gobierno de TI.

2. PLANTEAMIENTO DEL PROBLEMA

No hay duda de que las políticas y procedimientos de gestión eficaces ayudan a asegurar que TI se gestiona como un componente más de las actividades cotidianas. La adopción de estándares y mejores prácticas facilita la rápida aplicación de buenos procedimientos y evita retrasos en la creación innecesaria de nuevos enfoques en los que hay que ponerse de acuerdo.

Sin embargo, las mejores prácticas adoptadas han de ser compatibles con un marco de gestión de riesgos y de control apropiado para la organización, debiendo integrarse con otros métodos y prácticas que se estén utilizando. Los estándares y las mejores prácticas no son una panacea; su efectividad depende de cómo se implementen y se mantengan actualizados. Son muy útiles cuando se aplica como un conjunto de principios y como punto de partida para la adaptación de procedimientos más específicos.

Para asegurar que las políticas y los procedimientos se utilizan con eficacia, se requiere un cambio de manera que la administración y el personal entiendan qué hacer, cómo hacerlo y por qué es importante.

Para que las mejores prácticas sean eficaces, es mejor utilizar un lenguaje común y un enfoque estándar orientado hacia las necesidades reales del negocio, ya que garantiza que todos sigan el mismo conjunto de objetivos, asuntos y prioridades. Todas las empresas necesitan adaptar el uso de estándares y prácticas para ajustarlos a sus requisitos individuales. Los marcos COBIT e ITIL utilizados como guía pueden desempeñar un papel muy útil. COBIT para ayudar a definir qué debería hacerse e ITIL muestra el cómo para los aspectos de la gestión de servicios.

Por tal razón el equipo investigador plantea el siguiente interrogante: ¿Podrán las Guías de auditoría fundamentadas en los lineamientos establecidos por COBIT 4.1 articulados con ITIL 3.0 constituirse como una herramienta para el diagnóstico de un modelo de Gobierno de TI?

3. JUSTIFICACIÓN

Actualmente se ha venido trabajando en relación a los estándares de seguridad para desarrollar unos métodos (GUIAS) que brinden más eficiencia en el momento de consultar o implementar información en todas aquellas empresas, instituciones o particulares que necesitan adaptar el uso de estándares y prácticas tales como COBIT e ITIL para ajustarlos a sus requisitos individuales. Lo que el grupo investigador plantea con este proyecto es una herramienta que se constituye en un diseño articulado entre los marcos de referencia COBIT e ITIL, mediante el cual las entidades interesadas se les faciliten el manejo de la información al momento de implementar Mejores Prácticas en la empresa, en este caso específico COBIT alineado con ITIL para el gobierno de TI, con el fin de ofrecer un manejo eficiente para este tipo de servicio.

La decisión de tomar el marco de referencia articulado de COBIT e ITIL v3, fue por las grandes posibilidades y facilidades que le brindan al proyecto, a través de COBIT utilizando las mejores prácticas y herramientas para el monitoreo y la gestión de las actividades de TI, ayudando a los ejecutivos a comprender y gestionar las inversiones de TI durante su ciclo de vida y proporcionando un método para evaluar si los servicios de TI y las nuevas iniciativas satisfacen los requisitos empresariales y así sea probable que entreguen los beneficios esperados. y mediante ITIL proporcionando un marco de trabajo de mejores prácticas integral, consistente y coherente para la gestión de servicios de TI y los procesos relacionados, la promoción de un enfoque de alta calidad para el logro de la eficacia y eficiencia del negocio de la gestión de servicios de TI. ITIL intenta respaldar mas no fijar los procesos de negocio de una organización. En este contexto, la OGC no aprueba el término "Cumplimiento con ITIL". El papel del marco de trabajo de ITIL es describir los enfoques, las funciones, los roles y procesos en los que las organizaciones pueden basar sus propias prácticas. El rol de ITIL es brindar orientación.

Con la puesta en marcha del proyecto el grupo investigador pretende desarrollar una herramienta base para las empresas, instituciones o particulares interesadas la cual les va a poder brindar un servicio con mayor calidad y así poder satisfacer a todos sus usuarios proporcionando una forma de trabajo más eficiente del Gobierno de TI.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Construir las guías de auditoría con base en un modelo articulado de COBIT e ITIL 3.0 para el gobierno de TI.

4.1 OBJETIVOS ESPECÍFICOS

- Establecer los aspectos articulables entre los marcos de referencia COBIT e ITIL 3.0.
- Definir los aspectos a revisar, evaluar y verificar para responder a los requerimientos de COBIT e ITIL 3.0.
- Establecer los recursos de TI, los criterios de calidad de la información y los focos de gobierno de TI a considerar en la revisión de cada uno de los aspectos evaluables.

5. MARCOS REFERENCIALES

5.1 MARCO TEÓRICO

5.1.1 Antecedentes y teorías básicas.

COBIT

Los ejecutivos necesitan la certeza de que pueden confiar en los sistemas de información y en la información producida por los sistemas, y así obtener un retorno positivo de las inversiones en TI. COBIT permite que los ejecutivos de negocios entiendan mejor cómo dirigir y gestionar el uso de las TI en la empresa y el estándar de mejores prácticas que se espera de los proveedores de TI. COBIT proporciona las herramientas para dirigir y supervisar todas las actividades relacionadas con las TI.

COBIT es un marco de referencia globalmente aceptado para el gobierno de TI basado en estándares de la industria y las mejores prácticas. Una vez implementado, los ejecutivos pueden asegurarse de que se ajusta de manera eficaz con los objetivos del negocio y dirigir mejor el uso de TI para obtener ventajas comerciales. COBIT brinda un lenguaje común a los ejecutivos de negocios para comunicar las metas, objetivos y resultados a los profesionales de auditoría, informática y otras disciplinas.

COBIT brinda las mejores prácticas y herramientas para el monitoreo y la gestión de las actividades de TI.

El uso de las TI es una inversión importante que debe ser gestionado. COBIT ayuda a los ejecutivos a comprender y gestionar las inversiones de TI durante su ciclo de vida y proporciona un método para evaluar si los servicios de TI y las nuevas iniciativas satisfacen los requisitos empresariales y sea probable que entreguen los beneficios esperados.

Existe una tremenda diferencia entre las empresas que realizan una buena gestión de TI y las que no lo hacen, o no pueden. COBIT permite el desarrollo de políticas claras y mejores prácticas para la administración de TI. El marco ayuda a aumentar el valor obtenido de TI. También ayuda a las organizaciones a gestionar los riesgos relacionados con TI y a asegurar el cumplimiento, la continuidad, seguridad y privacidad.

Debido a que COBIT es un conjunto de herramientas y técnicas probadas y aceptadas internacionalmente, su implementación es una señal de buena gestión en una organización. Ayuda a los profesionales de TI y a usuarios de empresas a demostrar su competencia profesional a la alta dirección. Como ocurre con muchos procesos de negocio genéricos, existen estándares y mejores prácticas de la industria de TI que las empresas deberían seguir cuando utilizan las TI. COBIT se nutre de estas normas y proporciona un marco para implementarlas y gestionarlas.

Una vez que se identifican e implementan los principios clave de COBIT para una empresa, los ejecutivos ganan confianza en que la utilización de las TI puede ser gestionada de forma eficaz.

Los ejecutivos de las empresas pueden esperar los siguientes resultados de la adopción de COBIT:

- Los gerentes y el staff de TI entenderán totalmente como es que el negocio y TI pueden trabajar en forma conjunta para la entrega exitosa de las iniciativas de TI.
- Los costos totales del ciclo de vida de TI serán más transparentes y predecibles.
- TI ofrecerá información más oportuna y de mayor calidad.
- TI entregará proyectos de mejor calidad y más exitosos.
- Los requisitos de seguridad y privacidad serán más claros y la implementación será monitoreada con mayor facilidad.
- Los riesgos de TI serán gestionados con mayor eficacia.
- Las auditorías serán más eficientes y exitosas.
- El cumplimiento de TI con los requisitos regulatorios serán una práctica normal de gestión.

Las versiones de COBIT, incluyen lo siguiente:

- Marco de trabajo: Explica cómo es que COBIT organiza la gestión del gobierno de TI, los objetivos de control y las mejores prácticas de los procesos y dominios de TI, y los relaciona con las necesidades del negocio. El marco contiene un conjunto de 34 objetivos de control de alto nivel, uno para cada proceso de TI, agrupados en cuatro dominios: Planificar y Organizar, Adquirir e Implementar, Entregar y dar soporte, Monitorear y Evaluar (Figura 1).

- Las descripciones del proceso incluyen cada uno de 34 procesos de TI, cubriendo las áreas de responsabilidad de la empresa y de TI desde el principio hasta el final.
- Los objetivos de control proveen los objetivos de gestión de las mejores prácticas genéricas para los procesos de TI.
- Las directrices de gestión ofrecen herramientas para ayudar a asignar responsabilidades y medir el desempeño.
- El modelo de madurez proporciona perfiles de los procesos de TI que describen los posibles estados actuales y futuros.

PLANEAR Y ORGANIZAR (PO)

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada. Este dominio cubre los siguientes cuestionamientos típicos de la gerencia:

- ¿Están alineadas las estrategias de TI y del negocio?
- ¿La empresa está alcanzando un uso óptimo de sus recursos?
- ¿Entienden todas las personas dentro de la organización los objetivos de TI?
- ¿Se entienden y administran los riesgos de TI?
- ¿Es apropiada la calidad de los sistemas de TI para las necesidades del negocio?

ADQUIRIR E IMPLEMENTAR (AI)

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio. Este dominio, por lo general, cubre los siguientes cuestionamientos de la gerencia:

- ¿Es probable que los nuevos proyectos generen soluciones que satisfagan las necesidades del negocio?

- ¿Es probable que los nuevos proyectos sean entregados a tiempo y dentro del presupuesto?
- ¿Trabajarán adecuadamente los nuevos sistemas una vez sean implementados?
- ¿Los cambios no afectarán a las operaciones actuales del negocio?

ENTREGAR Y DAR SOPORTE (DS)

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativas. Por lo general cubre las siguientes preguntas de la gerencia:

- ¿Se están entregando los servicios de TI de acuerdo con las prioridades del negocio?
- ¿Están optimizados los costos de TI?
- ¿Es capaz la fuerza de trabajo de utilizar los sistemas de TI de manera productiva y segura?
- ¿Están implantadas de forma adecuada la confidencialidad, la integridad y la disponibilidad?

MONITOREAR Y EVALUAR (ME)

Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno. Por lo general abarca las siguientes preguntas de la gerencia:

- ¿Se mide el desempeño de TI para detectar los problemas antes de que sea demasiado tarde?
- ¿La Gerencia garantiza que los controles internos son efectivos y eficientes?
- ¿Puede vincularse el desempeño de lo que TI ha realizado con las metas del negocio?
- ¿Se miden y reportan los riesgos, el control, el cumplimiento y el desempeño?

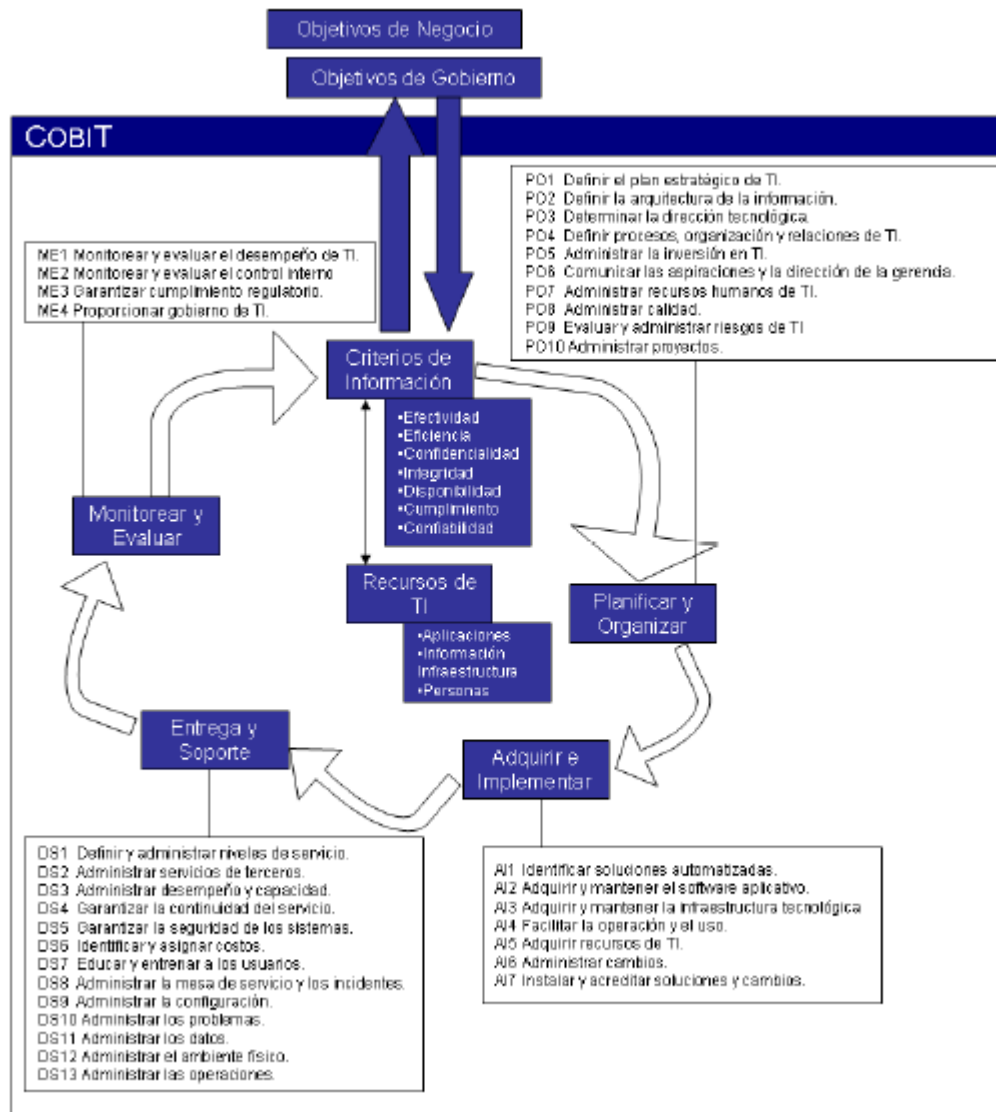


Figura 1 - Modelo Cobit

Las organizaciones siguen haciendo importantes inversiones en negocios posibilitados por TI: Inversiones en el mantenimiento, crecimiento o transformación del negocio que tienen un componente crítico de TI. La experiencia y un creciente volumen de investigaciones empíricas demuestran que dichas inversiones, cuando se gestionan bien dentro de un marco de gobierno efectivo, generan oportunidades importantes en las organizaciones para la creación de valor.

Muchas organizaciones han creado valor mediante la selección de las inversiones oportunas y la gestión efectiva de las mismas desde la concepción, pasando por la implementación, hasta la realización del valor esperado. Sin embargo, sin un

gobierno efectivo y una buena gestión, estas inversiones generan una oportunidad igualmente significativa para erosionar o destruir valor.

Una lección fundamental es que la inversión en TI ya no trata solamente de implementar soluciones de TI, sino que cada vez más trata de implementar el cambio posibilitado por TI. Esto implica mayor complejidad y mayor riesgo que en el pasado. Las prácticas de gestión que tradicionalmente se han aplicado ya no son suficientes. El mensaje es claro: las inversiones de negocio posibilitadas por TI pueden dar enormes beneficios, pero solo con los procesos de gobierno y gestión apropiados y el pleno compromiso e implicación de todos los niveles de dirección. Hasta ahora, sin embargo, la dirección no ha tenido un procedimiento claro que indique la forma de considerar las inversiones en TI o de informar sobre o monitorizar el posible éxito o fracaso de dichas inversiones.

Al considerar que existía una falta de guías de inversión y gestión de TI, el IT Governance Institute, trabajando conjuntamente con otros profesionales líderes en la comunidad de negocio y TI, lanzó la iniciativa Val IT.

Esta iniciativa, en la que se incluyen investigaciones, publicaciones y servicios de soporte, tiene como objetivo ayudar a la gerencia a abordar este reto, así como garantizar que las organizaciones logren un valor óptimo de las inversiones de negocio posibilitadas por TI, a un coste económico, y con un nivel conocido y aceptable de riesgo. Val IT constituye una extensión y complemento de COBIT, que proporciona un marco de control global para el gobierno de TI.

ITIL

Hoy, las organizaciones dependen de las TI para satisfacer sus objetivos corporativos y sus necesidades de negocios, entregando valor a sus clientes. Para que esto ocurra de una forma gestionada, responsable y repetible, la empresa debe asegurar que los servicios recibidos de alta calidad de TI deben:

- Satisfacer las necesidades de la empresa y los requisitos de los usuarios.
- Cumplir con la legislación.
- Asignarse y entregarse de forma eficaz y eficiente.
- Revisarse y mejorarse de forma continua.

La gestión de servicios de TI se refiere a la planificación, aprovisionamiento, diseño, implementación, operación, apoyo y mejora de los servicios de TI que sean apropiados a las necesidades del negocio. ITIL proporciona un marco de trabajo de mejores prácticas integral, consistente y coherente para la gestión de

servicios de TI y los procesos relacionados, la promoción de un enfoque de alta calidad para el logro de la eficacia y eficiencia del negocio en la gestión de servicios de TI.

ITIL intenta respaldar mas no fijar los procesos de negocio de una organización. En este contexto, la OGC no aprueba el término "Cumplimiento con ITIL". El papel del marco de trabajo de ITIL es describir los enfoques, las funciones, los roles y procesos en los que las organizaciones pueden basar sus propias prácticas. El rol de ITIL es brindar orientación en el nivel organizacional más bajo que pueda aplicarse.

Debajo de ese nivel, para implementar ITIL en una organización se requieren los conocimientos específicos de sus procesos de negocio para ajustar ITIL a fin de lograr una eficacia óptima.

Es útil pensar en la estructura de gestión de servicios como una pirámide con el estándar internacional ISO/IEC 20000:2005 en la cima (Figura 2).



Figura 2 - ITIL V.3.0

Se trata de una especificación formal y las organizaciones pueden obtener la acreditación para demostrar el cumplimiento con la norma. Por debajo de la cima está la capa de mejores prácticas de ITIL, que ayuda a asegurar y demostrar que las disposiciones de la norma se están cumpliendo. De manera similar, los procesos de ITIL pueden ser utilizados para lograr y demostrar el cumplimiento con los objetivos de control COBIT (la función de los apéndices del presente

documento es mostrar la relación entre las dos estructuras). Así que si ITIL es la capa intermedia, la adaptación de ITIL para satisfacer las necesidades de una organización en particular es el nivel más bajo, la base más amplia de la implementación de ITIL.

En ITIL v3, el desarrollo más significativo ha sido el paso de un marco de trabajo basado en procesos a una estructura integral que refleje el ciclo de vida de los servicios de TI. Un ejemplo de uso frecuente es ver las fases operativas de diseño, transición y operación, como los radios de una rueda, con la estrategia en el centro y la mejora continua del servicio alrededor del borde. En este nuevo contexto, los procesos clave se han actualizado, pero más significativo aún, ITIL ahora describe las funciones de gestión, las actividades y la estructura organizativa de los servicios de TI, además de los aspectos de aprovisionamiento y de estrategia, así como la integración con el negocio.

ITIL v3 consta de 5 libros basados en el ciclo de vida del servicio (Figura 3):

1. Estrategia de Servicio (SS)
2. Diseño del Servicio (SD)
3. Transición del Servicio (ST)
4. Operación del Servicio (SO)
5. Mejora Continua del Servicio (CSI)

Estrategia de Servicio (SS)	Diseño del Servicio (SD)	Transición del Servicio (ST)	Operación del Servicio (SO)	Mejora Continua del Servicio (CSI)
<ul style="list-style-type: none"> Gestión del servicio Ciclo de vida del servicio Activos del servicio y creación de valor Tipos y estructuras de proveedores de servicios Estrategia, mercados y oferta Gestión financiera Gestión del portafolio de servicios Gestión de la demanda Diseño organizacional, cultura y desarrollo Estrategia de aprovisionamiento Automatización e interfaces de servicios Herramienta para estrategias Desafíos y riesgos 	<ul style="list-style-type: none"> Diseño balanceado Requisitos, indicadores, actividades y limitantes Arquitectura orientada al servicio Gestión de servicios de negocio Modelos de diseño de servicios Gestión del catálogo de servicios Gestión de niveles de servicios Capacidad y disponibilidad Continuidad de servicios de TI Seguridad de la información Gestión de proveedores Gestión de datos y de la información Gestión de aplicaciones Roles y herramientas Análisis de impacto en el negocio Desafíos y riesgos Paquete de diseño de servicios Criterios de aceptación de servicios Documentación Aspectos ambientales Marco de trabajo de maduración de procesos 	<ul style="list-style-type: none"> Objetivos, principios, políticas, contexto, roles y modelos Planificación y soporte Gestión del cambio Activos del servicio y gestión de la configuración Liberación y distribución Validación y prueba del servicio Evaluación Gestión del conocimiento Gestionando las comunicaciones y el compromiso Gestión de partes interesadas Sistema de gestión de configuraciones Introducción por etapas Desafíos y riesgos Tipos de activos 	<ul style="list-style-type: none"> Equilibrio en la operación del servicio Salud operacional Comunicación Documentación Eventos, incidentes y problemas Atención de requerimientos Gestión de accesos Monitoreo y control Gestión de la infraestructura y el servicio Gestión de instalaciones y del Data Center Seguridad física y de la información Mesa de servicios Gestión técnica de operaciones de TI y de aplicaciones Roles, responsabilidades y estructuras organizacionales Soporte tecnológico a la operación del servicio Gestionando los cambios, proyectos y riesgos Desafíos Guía complementaria 	<ul style="list-style-type: none"> Objetivos, métodos y técnicas Cambio organizacional Propiedad Drivers Gestión de niveles de servicios Medición del servicio Gestión del conocimiento Benchmarking Modelos, estándares y calidad Proceso de mejoramiento de los siete pasos CSI Retorno sobre la inversión (ROI) y aspectos de negocio Roles Matriz RACI Herramientas de soporte Implementación Gobierno Comunicaciones Desafíos y riesgos Innovación, corrección y mejoramiento Apoyo de las mejores prácticas a la mejora continua del servicio (CSI)

Figura 3 – Sinergia de ITIL v.3.0

Estrategia de Servicio

Se enfoca en el estudio de mercado y posibilidades mediante la búsqueda de servicios innovadores que satisfagan al cliente tomando en cuenta la real factibilidad de su puesta en marcha. Así mismo se analizan posibles mejoras para servicios ya existentes. Se verifican los contratos con base en las nuevas ofertas de proveedores antiguos y posibles nuevos proveedores, lo que incluye la renovación o revocación de los contratos vigentes.

Diseño del Servicio

Una vez identificado un posible servicio el siguiente paso consiste en analizar su viabilidad. Para ello se toman factores tales como infraestructura disponible, capacitación del personal y se planifican aspectos como seguridad y prevención ante desastres. Para la puesta en marcha se toman en consideración la reasignación de cargos (contratación, despidos, ascensos, jubilaciones, etc), la infraestructura y software a implementar.

Transición del Servicio

Antes de poner en marcha el servicio se deben realizar pruebas. Para ello se analiza la información disponible acerca del nivel real de capacitación de los usuarios, estado de la infraestructura, recursos IT disponibles, entre otros. Luego se prepara un escenario para realizar pruebas; se replican las bases de datos, se preparan planes de rollback y se realizan las pruebas. Luego de ello se limpia el escenario hasta el punto de partida y se analizan los resultados, de los cuales dependerá la implementación del servicio. En la evaluación se comparan las expectativas con los resultados reales.

Operación del Servicio

En este punto se monitoriza activa y pasivamente el funcionamiento del servicio, se registran eventos, incidencias, problemas, peticiones y accesos al servicio.

Mejora Continua del Servicio

Se utilizan herramientas de medición y feedback para documentar la información referente al funcionamiento del servicio, los resultados obtenidos, problemas ocasionados, soluciones implementadas, etc. Para ello se debe verificar el nivel de conocimiento de los usuarios respecto al nuevo servicio, fomentar el registro e investigación referentes al servicio y disponer de la información al resto de los usuarios.

Desde 1991, ITIL ha sido patrocinado y apoyado por itSMF, un proveedor y grupo de usuarios que ahora tiene presencia en más de 40 países de todo el mundo. Es una organización sin fines de lucro y un actor importante en el desarrollo continuo y promoción de las mejores prácticas en la gestión, estándares y calificaciones de servicios TI. El itSMF provee una red accesible de expertos de la industria, fuentes de información y eventos para ayudar a los países miembros a abordar los problemas de gestión de servicios de TI y lograr la entrega de servicios consistentes, de alta calidad, internos y externos, a través de la adopción de mejores prácticas. A nivel mundial, el itSMF ahora cuenta con más de 6.000 empresas asociadas, públicas y privadas, que incluyen más de 70.000 personas.

5.1.2 MARCO CONCEPTUAL

ISACA: Es un líder mundialmente reconocido, proveedor de conocimiento, certificaciones, comunidad, apoyo y educación en seguridad y aseguramiento de sistemas de información (SI), gobierno empresarial, administración de TI así como riesgos y cumplimiento relacionados con TI.

ITGI: Es una entidad de investigación independiente y sin fines de lucro que proporciona orientación para la comunidad global de negocios relacionada al gobierno de activos de TI. El ITGI fue establecido por ISACA en 1998, para ayudar a los ejecutivos y a profesionales de TI a asegurar que las tecnologías de información entreguen valor y mitiguen sus riesgos a través del alineamiento con los objetivos de la empresa, que los recursos de TI se asignen apropiadamente y que se mida el desempeño de TI.

ITSMF:(Information Technology Service Management Forum) es una comunidad mundial cuya actividad gira en torno a la creación y difusión de las buenas prácticas y las experiencias relativas a la gestión de los servicios y el gobierno de las TI. Está centrada en intercambiar puntos de vista, compartir experiencias y participar en el desarrollo continuo de mejores prácticas y estándares.

OGC:(Office of Government Commerce) En español Oficina de Comercio Gubernamental, es una organización del gobierno del Reino Unido responsable de las tareas que mejoran la eficiencia y la eficacia de los procesos de negocios de gobierno. Su misión es trabajar con organizaciones del sector público para ayudarlos a lograr eficiencias, valor por las inversiones en actividades comerciales y mejorar el éxito de los programas y proyectos. La OGC soporta el logro de estos objetivos a través de la concentración de sus esfuerzos en un amplio rango de programas de mejoramiento a través de tres actividades significativas en organizaciones del sector público: eficiencia, gestión de proyectos y programas, y compras.

RISK IT: Es el riesgo del negocio asociado con el uso, la propiedad, la operación, la participación, la influencia y la adopción de las TI dentro de la empresa. Se trata de eventos relacionados con las TI que podrían afectar el negocio. Esto puede ocurrir tanto en la frecuencia y magnitud incierta, y crea dificultades para alcanzar las metas y objetivos estratégicos.

Gestión del riesgo empresarial es un componente esencial de la administración responsable de cualquier organización. Debido a su importancia para el negocio en general, los riesgos de TI deben ser tratados como otros riesgos clave de negocios.

El marco Risk IT explica los riesgos de TI y permite a los usuarios: integrar la gestión de riesgos de TI con el ERM general, comparar y evaluar los riesgos de TI

con el apetito de riesgo y la tolerancia al riesgo de la organización y comprender la forma de gestionar el riesgo.

Los riesgos de TI se gestionarán por todos los líderes de negocio clave dentro de la organización, no es sólo un problema técnico del departamento de TI.

TI:(Tecnologías de Información) Conforman el conjunto de recursos necesarios para manipular la información: los ordenadores, los programas informáticos y las redes necesarias para convertirla, almacenarla, administrarla, transmitirla y encontrarla.

VAL IT: Es un framework de gobernabilidad que se puede utilizar para crear valor de negocio de las inversiones en TI. Consiste en un conjunto de principios rectores y una serie de procesos y mejores prácticas que se los define como un conjunto de prácticas de gestión claves para apoyar y ayudar a la gerencia ejecutiva y juntas a nivel empresarial. La última versión del framework, publicado por el IT Governance Institute (ITGI), basado en la experiencia de los profesionales y académicos globales, prácticas y metodologías fue nombrado Valor de la Empresa: Gobierno de TI Inversiones, el Val IT Framework 2.0. Este cubre los procesos y prácticas de gestión claves para tres dominios específicos y va más allá de las nuevas inversiones para incluir los servicios de TI, activos, otros recursos y los principios y procesos para la gestión de la cartera de TI.

BENCHMARKING: Es una técnica de gestión empresarial que pretende descubrir y definir los aspectos que hacen que una empresa sea más rentable que otra, para después adaptar el conocimiento adquirido a las características de nuestra propia compañía.

CALIDAD: Cuando un producto o servicio que nosotros adquirimos satisface nuestras necesidades y expectativas.

CRITERIOS: Normas, reglas o pruebas sobre las que se puede basar una opinión o decisión, o por medio de la cual se puede evaluar un producto, servicio, resultado o proceso.

EFICIENCIA: Es la óptima utilización de los recursos disponibles para la obtención de resultados deseados.

RIESGO: Se puede definir como una eventualidad que imposibilita el cumplimiento de un objetivo.

STAKEHOLDERS: Interesados directos e indirectos de una empresa que teniendo algún tipo de interés en las operaciones empresariales, le brindan su apoyo y ante los cuales la organización es responsable.

5.2 MARCO LEGAL

Esta guía se rige bajo los lineamientos del marco de trabajo ITIL 3.0, la cual el Office of Government Commerce (OGC) considera una referencia para describir los enfoques, las funciones, los roles y procesos en los que las organizaciones pueden basar sus propias prácticas.

5.3 DELIMITACIONES

5.3.1 Delimitación temporal. El proyecto consta de una etapa inicial que comenzó su ejecución el 14 de mayo de 2012 y de una etapa final en junio de 2013.

5.3.2 Delimitación espacial. El estudio y desarrollo del proyecto Guías de auditoría para el diagnóstico de un modelo de Gobierno de TI fundamentado en los lineamientos establecidos por Cobit 4.1 e ITIL 3.0 se llevara a cabo en la ciudad de Barranquilla más exactamente en la Corporación Universitaria de la Costa CUC.

5.4. LIMITACIONES

En la realización del proyecto se encontraron factores y situaciones que dificultaron el desarrollo del mismo, pero la falta de dominio sobre el idioma ingles representó un mayor impedimento ya que la mayoría de la bibliografía se encuentra escrita en dicho idioma. Pero aun asi el equipo dispuso de todos los recursos a su alcance para que el proyecto pudiera ser planificado, organizado, ejecutado y verificado.

6. DISEÑO METODOLÓGICO

6.1 TIPO DE INVESTIGACIÓN

Es una investigación descriptiva, porque se describen una serie de procedimientos y actividades a realizar, plasmados en unas guías de auditoría para el diagnóstico de un modelo de Gobierno de TI tomando como referencia los lineamientos establecidos por Cobit 4.1 e ITIL 3.0.

6.2 MÉTODO DE INVESTIGACIÓN

Para el proyecto de investigación, se utilizará el método observacional ya que se recopilarán las bases para la solución al problema planteado a través de los diferentes medios, y se organizara a partir de los conocimientos adquiridos y desarrollados, manteniendo siempre el rigor científico.

6.3 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

La información sobre COBIT e ITIL será recolectada a través de los documentos que se localizaran en las bibliotecas, revistas especializadas, documentos pdf y en Internet. La información se recolectará de forma directa, fundamentalmente mediante consultas, copias o impresiones del material encontrado.

7. CONCLUSIÓN

Para sobrevivir y prosperar, cada organización tiene que entender cómo crear valor para sí mismos y para sus clientes y la forma en que sus proveedores mejoran ese valor. Deben apreciar las decisiones estratégicas, tanto por su servicios propios y aquellos que reciben de los proveedores . Debido al entorno de constante cambio, la estrategia no es algo para hacer una vez, y las estrategias de servicio deberán desarrollarse , aplicarse y revisarse continuamente, al igual que todas las demás partes del Ciclo de Vida del Servicio. Si la estrategia es eficaz, entonces el esfuerzo en las otras etapas del ciclo de vida se aplicarán de manera adecuada y con éxito.

Los servicios son una forma predominante en que se crea y se transfiere el valor entre las organizaciones. Una gran cantidad de conocimientos y buenas prácticas está disponible para su uso si hay claridad sobre qué servicios pueden ser utilizados para apoyar el negocio del cliente.

Las guías descritas en este proyecto permiten describir los enfoques, las funciones, los roles y procesos en los que las organizaciones pueden basar sus propias prácticas.

8. BIBLIOGRAFÍA

- COBIT 4.1 (idioma español).
- ITIL 3.0 (idioma inglés).
- Guías de aseguramiento para cobit 4.1 (idioma inglés).

Sitios Web:

- <http://www.iti-officialsite.com/>
- <https://www.isaca.org/>
- <http://www.itgi.org/>
- <http://www.itsmfi.org/>
- http://es.wikipedia.org/wiki/Objetivos_de_control_para_la_informaci%C3%B3n_y_tecnolog%C3%ADas_relacionadas
- <http://en.wikipedia.org/wiki/COBIT>
- <http://www.bitcompany.biz/>