

DISEÑO DE UN MANUAL DE GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN PARA EL CONSEJO DE GOBIERNO DE RÉGIMEN ESPECIAL DE GALÁPAGOS APLICANDO COBIT 4.1 EN EL DOMINIO ADQUIRIR E IMPLEMENTAR

Angel Ernesto Quimbiulco Carrillo¹, Msc. Mauricio Campaña²

Unidad de Gestión de Postgrados, Escuela Politécnica del Ejército, Sangolquí, Ecuador

1 ESPE, Ecuador, angeloqc@outlook.com

2 ESPE, Ecuador, emcampania@espe.edu.ec

RESUMEN:

La gestión de la Tecnología de la Información es un factor crítico de éxito y en la mayoría de los casos es determinante para la operación y funcionamiento correcto y seguro de las organizaciones, se han desarrollado marcos de referencia y estándares a nivel internacional que recogen las mejores prácticas para alinear los objetivos de TI con los de la organización.

El Consejo de Gobierno de Régimen Especial de Galápagos es el organismo responsable de la administración de la provincia, la planificación y el Ordenamiento Territorial, el manejo de los recursos y la organización de las actividades que se realizan en Galápagos.

Los Objetivos de Control para la Información y las Tecnologías Relacionadas (COBIT), ayudan a satisfacer las necesidades de la administración estableciendo un puente entre los riesgos del negocio, los controles necesarios y los aspectos técnicos. Provee buenas prácticas y presenta actividades en una estructura manejable y lógica. Las “Buenas prácticas” de COBIT reúne el consenso de expertos, quienes ayudarán a optimizar la inversión de la información y proporcionarán un mecanismo de medición que permitirá juzgar cuando las actividades van por el camino equivocado.

El presente proyecto efectúa una evaluación técnica informática del Sistema de Información de la institución mediante la aplicación de COBIT 4.1 y propone el diseño de un Manual de Gestión de TI para una administración adecuada de los procesos de TI que soportan la estrategia del negocio.

Palabras Clave: COBIT, Objetivos de Control, Manual de Gestión de TI.

ABSTRACT:

Managing Information Technology is a critical success factor and in most cases is critical to the operation and proper and safe operation of organizations have developed frameworks and international standards that reflect the best practices to align IT objectives with those of the organization.

The Governing Council of Galapagos Special Regime is the body responsible for the administration of the province, planning and land use planning, resource management and organization of the activities taking place in Galapagos.

Control Objectives for Information and related Technology (COBIT), help meet the needs of the administration building a bridge between business risks, the necessary controls and technical aspects. Provides best practices and presents activities in a manageable and logical structure. The "Best Practices" COBIT meets the consensus of experts who will help optimize the investment of information, and provide a mechanism for measuring the activities will judge when they are on the wrong path.

This project carries out a technical assessment of computer information system of the institution by implementing COBIT 4.1 and proposes the design of an IT Management Manual for proper management of IT processes that support the business strategy.

Keyword: COBIT, Control Objectives, IT Management Manual.

I. INTRODUCCIÓN

Hoy en día, las organizaciones enfrentan grandes y urgentes retos que las obligan a desarrollar prácticas adecuadas y efectivas de Gobierno de TI para asegurar el cumplimiento de sus metas y objetivos.

Es conocido que la TI aporta rápida y continuamente valor, grandes beneficios y crea importantes oportunidades, pero simultáneamente ofrece una diversidad de opciones y presenta nuevos riesgos que obligan a su Gobierno para alinearla a la estrategia de la organización de tal manera que se puedan evitar y controlar los riesgos asociados. (ENIAC, 2012)

Las organizaciones deben cumplir con requerimientos de calidad, fiduciarios y de seguridad, tanto para su información, como para sus activos. La gerencia deberá además optimizar el empleo de sus recursos disponibles, los cuales incluyen: personal, instalaciones, tecnología, sistemas de aplicación y datos. Para cumplir con esta actividad, así como para alcanzar sus objetivos, la gerencia debe entender el estado de sus propios sistemas de TI y decidir el nivel de seguridad y control que deben proveer estos sistemas.

El Consejo de Gobierno de Régimen Especial de Galápagos es el organismo responsable de la administración de la provincia, la planificación y el Ordenamiento Territorial, el manejo de los

recursos y la organización de las actividades que se realizan en Galápagos, soportado por tecnología de última generación y personal preparado para el cumplimiento de sus funciones.

El Departamento de Informática es el responsable de elaborar, desarrollar y proponer la implementación de nuevos proyectos de tecnologías y sistemas de información en coordinación con Secretaría Técnica y Presidencia, además de ejecutar planes de mantenimiento preventivo / correctivo y brindar soporte técnico solicitado por las distintas unidades administrativas del CGREG.

Se han identificado serias falencias en las estrategias de desarrollo, implementación, integración, mantenimiento y gestión del cambio en las soluciones de TI adoptadas en el CGREG, esto debido a que no existe una adecuada administración de los procesos de TI, los cuales son manejados de forma intuitiva.

La causa de estos inconvenientes podría deberse a la ausencia de una definición formal y falta de documentación que detallen las actividades de los procesos a ejecutarse, no es posible medir el grado de madurez o eficiencia de los mismos. Se requiere medir en forma efectiva el grado de desempeño de los procesos en el Dominio Adquirir e Implementar, para determinar si las actividades están siendo ejecutadas de forma correcta.

El presente trabajo realiza una evaluación técnica informática al CGREG¹ empleando el marco de referencia COBIT 4.1 para determinar los grados de madurez de los procesos de TI y como estos afectan a los criterios de información, obteniendo una visión clara del nivel de aporte a los requerimientos del negocio de forma cuantitativa. Con esta información se procede a elaborar el Manual de Gestión de Tecnologías de Información tomando en cuenta las consideraciones de COBIT para alcanzar procesos adecuadamente administrados y que soportan la estrategia del negocio, y concluye con la validación práctica del manual mediante el rediseño de dos procesos del dominio Adquirir e Implementar empleando la herramienta desarrollada.

II. METODOLOGÍA

Para el desarrollo del presente trabajo se ha seleccionado a la investigación Correlacional, que es un tipo de estudio que tiene como propósito evaluar la relación que exista entre dos o más variables en un contexto en particular. Se observarán situaciones ya existentes dentro del CGREG en su ambiente natural; estas no fueron provocadas intencionalmente. Este estudio a su vez será de tipo transversal, ya que la recolección de información se hará en un solo momento y en un tiempo único; el propósito es describir las variables y analizar su incidencia e interrelación en un determinado momento.

En base a lo indicado las etapas de la investigación fueron las siguientes:

1. Definir el Problema de investigación
2. Plantear Hipótesis de trabajo
3. Revisión de la literatura
4. Determinar el diseño operacional:

¹ Consejo de Gobierno de Régimen Especial de Galápagos

- Identificar variables pertinentes
 - Seleccionar los sujetos apropiados
 - Establecer instrumentos para la obtención de datos.
 - Seleccionar las técnicas de correlación estadística apropiada para los datos
5. Recolección de datos
 6. Analizar los datos por medio de correspondientes técnicas correlacionales e interpretar los resultados.
 7. Preparar informe escrito

A. Marco de Trabajo

COBIT ha sido diseñado para ser la herramienta de gobierno de TI que ayuda a entender y administrar los riesgos y beneficios asociados con la Tecnología de Información. Define dos conceptos fundamentales:

- Control: Son políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos de negocio serán alcanzados y que eventos no deseables serán prevenidos, detectados y corregidos. (ISACF, 1996)
- Objetivo de Control en TI: propósito que se desea alcanzar implementando procedimientos de control en una actividad en particular. (ISACF, 1996)

a) Perspectiva General

Para proporcionar la información que la empresa requiere para lograr sus objetivos, la empresa necesita invertir, administrar y controlar los recursos de TI usando un conjunto estructurado de procesos que provean los servicios y que entreguen la información empresarial solicitada.

b) Los Requerimientos de Negocio

Basados en las necesidades de información que requieren los propietarios de negocio para cumplir con sus metas y objetivos. Se tienen requerimientos de calidad orientados con la entrega del servicio; fiduciarios (efectividad, eficiencia, confiabilidad y cumplimiento) y requerimientos de seguridad (integridad y disponibilidad). COBIT traduce estos 7 requerimientos de negocio en *criterios de información*, las cuales son necesidades del negocio que tienen que ser satisfechas.

c) Los Recursos de TI

En COBIT se definen como: aplicaciones, datos, infraestructura y personas para responder a los requerimientos que el negocio tiene hacia TI.

d) Los Procesos de TI

COBIT define un estándar que busca agrupar los 34 procesos en 4 dominios. Los dominios persiguen crear una colección natural de procesos. Entonces se tienen 3 polos en el Marco de Referencia: Los criterios de información, que son los requerimientos del negocio, los recursos de TI que se dispone para proveer la información, y los procesos de TI, que cierran el círculo y alinean los recursos con los criterios de información de acuerdo a la figura 1:

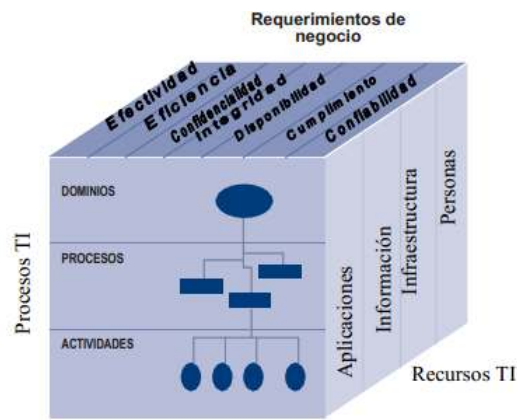


Figura 1. Integración de Componentes de COBIT

A continuación se listan los cuatro Dominios de COBIT, con los respectivos procesos:

PLANEAR Y ORGANIZAR (PO) Cubre las estrategias y tácticas, tiene que ver con identificar la manera en que TI puede contribuir de la mejor manera al logro de los objetivos del negocio.

- PO1 Definir un plan estratégico de TI
- PO2 Definir la arquitectura de la información
- PO3 Determinar la Dirección Tecnológica
- PO4 Definir los procesos, Organización y Relaciones de TI
- PO5 Administrar la inversión en TI
- PO6 Comunicar las aspiraciones y la Dirección de la Gerencia
- PO7 Administrar Recursos Humanos de TI
- PO8 Administrar la calidad
- PO9 Evaluar y administrar los riesgos de TI
- PO10 Administrar Proyectos

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 del cambio y mantenimiento de los sistemas para garantizar que satisfagan los objetivos del negocio.

- AI1 Identificar soluciones automatizadas.
- AI2 Adquirir y mantener software aplicativo
- AI3 Adquirir y mantener infraestructura tecnológica
- AI4 Facilitar la operación y el uso
- AI5 Adquirir recursos de TI
- AI6 Administrar cambios
- AI7 Instalar y acreditar soluciones y cambios

ENTREGAR Y DAR SOPORTE (DS) 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.

- DS1 Definir y administrar los niveles de servicio
- DS2 Administrar los servicios de terceros
- DS3 Administrar el desempeño y la capacidad
- DS4 Garantizar la continuidad del servicio
- DS5 Garantizar la seguridad de los sistemas
- DS6 Identificar y asignar costos
- DS7 Educar y entrenar a los usuarios
- DS8 Administrar la mesa de servicio y los incidentes
- DS9 Administrar la configuración
- DS10 Administrar los problemas
- DS11 Administrar los datos
- DS12 Administrar el ambiente físico
- DS13 Administrar las operaciones

MONITOREAR Y EVALUAR (ME) Todos los procesos 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 de gobierno.

- ME1 Monitorear y evaluar el desempeño de TI
- ME2 Monitorear y evaluar el control interno
- ME3 Garantizar el cumplimiento regulatorio
- ME4 Proporcionar gobierno de TI.

La evaluación de la capacidad de los procesos basada en los modelos de madurez de COBIT es una parte clave de la implementación del gobierno de TI. Después de identificar los procesos y controles críticos de TI, el modelo de madurez permite identificar y demostrar a la dirección las brechas existentes, entonces se pueden crear planes de acción para llevar estos procesos hasta el nivel objetivo de capacidad deseado.

B. MATERIALES Y MÉTODOS

Las pruebas empleadas en la fase de diagnóstico y evaluación de procesos de TI que permitieron determinar los grados de madurez en conjunto con las herramientas de COBIT se describen a continuación:

La observación: es la captación previamente planeada y el registro controlado de datos con una determinada finalidad para la investigación, mediante la percepción visual o acústica de un acontecimiento.² (Heinemann K. , 2007)

La entrevista: Como técnica cualitativa, es una de las vías más comunes para investigar la realidad social. Consiste en la recogida de información a través de un proceso de comunicación, en el transcurso del cual el entrevistado responde a cuestiones, previamente diseñadas en función

² K. Heinemann, de Introducción a la Metodología de la Investigación Empírica, Mc Graw-hill, 2007, p. 135.

de las dimensiones que se pretende estudiar, planteadas por el entrevistador.³ (GARZON, 2008)

C. DISEÑO E IMPLEMENTACIÓN

Para la primera fase, que corresponde a la evaluación de los procesos de TI, se construyó una metodología que permitió recopilar información primaria mediante la aplicación de entrevistas a personal clave de la Unidad de Gestión Tecnológica del CGREG para posteriormente calcular los niveles de madurez de cada uno de los objetivos de alto nivel del Dominio Adquirir e Implementar definido por COBIT.

A continuación se muestran las diferentes fases ejecutadas de manera secuencial para lograr el objetivo de determinar el nivel de madurez de los procesos de TI:

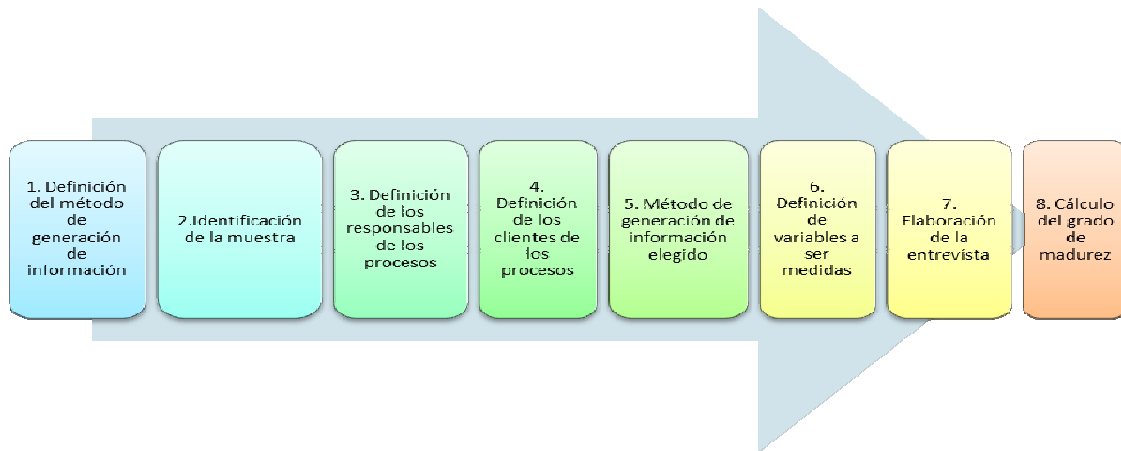


Figura 2. Metodología de evaluación de procesos

Luego, empleando los valores de los grados de madurez se procedió a calcular los criterios de información mediante el empleo de los “Mapas de Control” definidos por COBIT, finalmente se procedió a establecer la estructura del Manual de Gestión de TI para el CGREG, considerando 3 etapas fundamentales: definición, evaluación y cumplimiento de procesos de TI, con lo cual se garantiza que se satisface los requerimientos del negocio, y se incrementa los niveles de madurez de los procesos a un nivel administrado y medible. La estructura del manual se muestra a continuación:

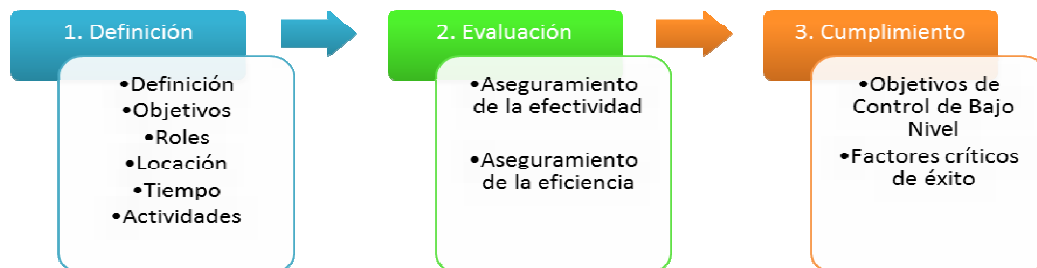


Figura 3. Estructura del Manual de Gestión de TI

3

Para cada una de las fases se desplegaron un conjunto de actividades, las definiciones de cada uno de los componentes y los entregables que conforman la estructura del Manual de Gestión de TI:

1. Fase de Definición del proceso:

- 1.1 Definición del proceso
- 1.2 Diagrama de flujo
- 1.3 Catálogo de actividades

2. Fase de Evaluación del proceso:

- 2.1 Aseguramiento de la Efectividad
 - 2.1.1 Aseguramiento de efectividad de servicio o tarea
 - 2.1.2 Aseguramiento de efectividad integral del proceso
- 2.2 Aseguramiento de la Eficiencia
 - 2.2.1 Aseguramiento de eficiencia de servicio o tarea
 - 2.2.2 Aseguramiento de eficiencia integral del proceso

3. Fase de cumplimiento del proceso:

- 3.1 Cumplimiento de Objetivos de Control de Bajo Nivel
- 3.2 Cumplimiento de factores críticos de éxito

III. EVALUACIÓN DE RESULTADOS Y DISCUSIÓN

A continuación se detallan los resultados de la evaluación efectuada a los 7 procesos del Dominio Adquirir e Implementar:

Tabla 1. Grado de Madurez de los procesos AI

Proceso	Grado de Madurez Actual
AI1 Identificar Soluciones Automatizadas	1.42
AI2 Adquirir y Mantener Software Aplicativo	1.38
AI3 Adquirir y Mantener Infraestructura Tecnológica	1.93
AI4 Facilitar la Operación y el Uso	1.76
AI5 Adquirir Recursos de TI	2.05
AI6 Administrar Cambios	1.41
AI7 Instalar y Acreditar Soluciones y Cambios	1.98

La información gráfica de la Tabla I se puede observar en la figura 4, los niveles de madurez más altos se encuentran en los procesos AI5 Adquirir Recursos de TI (2,05) y AI7 Instalar y Acreditar Soluciones y Cambios (1,98), mientras que los grados más bajos corresponden a AI2 Adquirir y

Mantener Software Aplicativo (1,38) y AI6 Administrar Cambios (1,41).

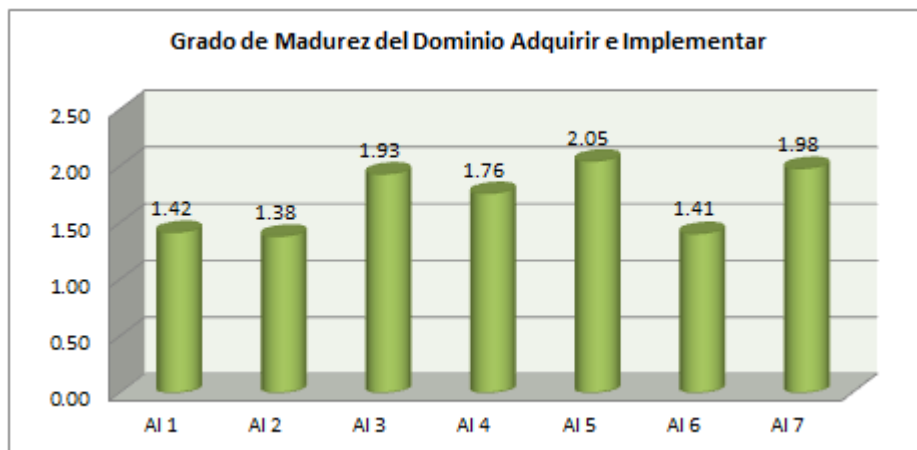


Figura 4. Gráfico de barras del Grado de Madurez de los procesos AI

Con el resumen que se muestra en la figura 4 se deduce que TI tiene en promedio un grado de madurez de 1.7 que le ubican en el Nivel 2, lo que implica que no hay una comunicación formal de los procedimientos estándar, dejando la responsabilidad al individuo; existe un alto grado de confianza en el conocimiento de los individuos, por tanto los errores son muy probables.

Luego de haber obtenido los grados de madurez de los procesos de TI, se procede a calcular los niveles de impacto en los criterios de información para determinar el porcentaje en que son satisfechos los requerimientos del negocio que soportan la estrategia institucional. A continuación se muestran los resultados obtenidos:

Tabla 2. Impacto de los criterios de información

Criterio de información	Nivel Actual
Efectividad	42.02%
Eficiencia	42.62%
Confidencialidad	0.00%
Integridad	41.82%
Disponibilidad	43.50%
Cumplimiento	48.18%
Confiable	37.92%

Nótese que para el criterio de información “Confidencialidad” el nivel actual es 0%, sin embargo es necesario aclarar que ningún objetivo de control del Dominio Adquirir e Implementar impacta de manera directa o indirecta sobre este criterio.

Por lo expuesto se puede concluir que los criterios de información en la actualidad están siendo satisfechos en promedio en un 42,68% con respecto al grado administrado y medible de acuerdo al marco de referencia COBIT. En general los criterios de información requieren ajustes en sus definiciones debido a sus niveles bajos.

En la figura 3 se puede observar gráficamente el resultado de los porcentajes obtenidos por cada criterio de información:

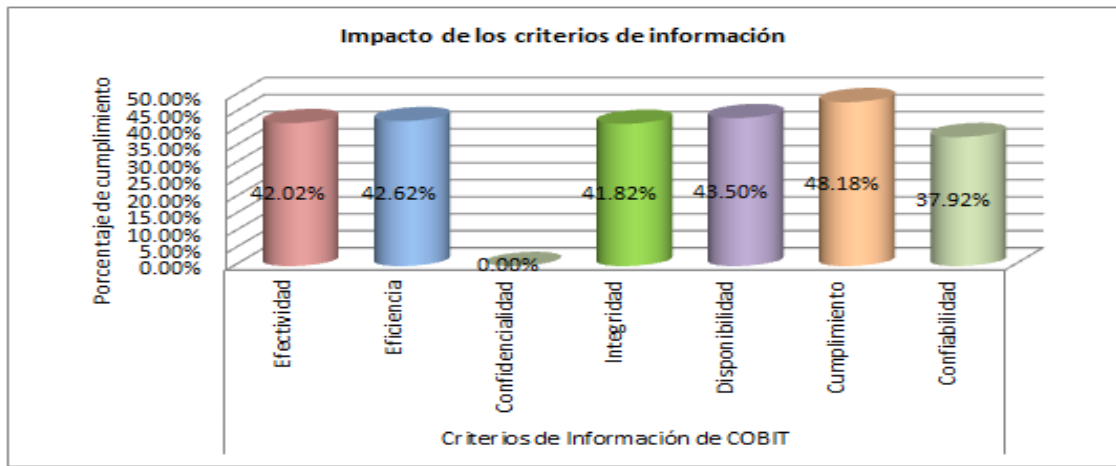


Figura 5. Representación del impacto de los criterios de información

IV. TRABAJOS RELACIONADOS

Se ha identificado el trabajo de tesis de Marcia Cordero Calderón y María del Carmen Ibujés con el tema “Auditoría de Riesgos Informáticos del Departamento de Sistemas de Teleamazonas Usando COBIT” de la Escuela Politécnica Nacional, y la tesis correspondiente a “Desarrollo de un Gobierno de TI para la empresa Fiduciaria Ecuador utilizando COBIT 4.1” de Hernán Arteaga Calispa de la Escuela Politécnica Nacional con los cuales se relacionó la aplicación del marco de referencia COBIT con lo cual se logró estructurar el Manual de Gestión de TI.

V. CONCLUSIONES Y TRABAJO FUTURO

- Los Modelos de Madurez de COBIT para el control sobre los procesos de TI determinaron la posición precisa de donde la institución está actualmente respecto a la norma y son el punto de partida para el Diseño del Manual de Gestión de TI.
- Producto de la aplicación del Marco de Referencia COBIT en la fase de diagnóstico de procesos de TI ha sido posible identificar que la Unidad Tecnológica se encuentra en un nivel en el cual la mayoría de sus procesos del Dominio Adquirir e Implementar son intuitivos y repetitivos; sin embargo se ha notado que la Coordinación de Sistemas están empezando a definir y normalizar procesos por la presión ejercida desde la Presidencia del CGREG.
- La Coordinación de Sistemas no puede detectar posibles deficiencias en la ejecución de procesos de manera proactiva y proponer mejoras debido a la falta de indicadores cuantitativos que permitan medir los niveles de eficacia y eficiencia de los procesos.
- En el CGREG no existe un adecuado manejo de los recursos tecnológicos que apoyen a la estrategia del negocio, a esto también se debe sumar la deficiencia y carencia de políticas en TI.
- El diseño del Manual de Gestión de TI permitió establecer procedimientos claros de definición, evaluación y cumplimiento de procesos que garantizan que los objetivos del negocio sean alcanzados y que se minimicen los riesgos existentes.

- La implementación del Manual de Gestión de TI asegura que se cuenten con las referencias necesarias para que los procesos de TI puedan alcanzar niveles administrados en los modelos de madurez de acuerdo al marco de referencia COBIT.

En cuanto a trabajos futuros se podrían abordar los siguientes temas:

- Ampliar el diagnóstico de los procesos de TI a los 3 Dominios definidos por COBIT que no fueron considerados en el presente estudio: Planear y Organizar, Entregar y dar Soporte, y Monitorear y Evaluar.
- Definir y documentar cada uno de los procesos de TI que la Unidad Tecnológica establezca como prioritarios en cada uno de los Dominios de COBIT.
- Efectuar mediciones de los niveles de eficacia y eficiencia con el apoyo del manual de gestión desarrollado y comparar si los indicadores satisfacen las metas de los procesos de TI.
- Estudiar los indicadores desarrollados y determinar si requieren nuevas variables que apoyen a la recolección de datos para el monitoreo de los procesos.

REFERENCIAS BIBLIOGRÁFICAS

ENIAC. (2012). *ENIAC*. Recuperado el 2012, de ENIAC: http://www.eniac.com/documentos-pdf/Ficha_Técnica_Introducción_e_Implantación_del_Gobierno_Corporativo_TIC.pdf

GARZON. (2008). *SUAGM*. Recuperado el 2012, de SUAGM: http://www.suagm.edu/umet/biblioteca/Reserva_Profesores/linna_irizarry_educ_173/como_elaborar_entrevistas.pdf

Heinemann, K. (2007). Introducción a la Metodología de la Investigación Empírica. En K. Heinemann, *Introducción a la Metodología de la Investigación Empírica* (pág. 135). Mc Graw-hill.

ISACF. (1996). Objetivos de Control. En *Objetivos de Control* (pág. 13). Rolling Meadows.