AUDITORÍA DE GESTIÓN DE PROCESOS EN EL DEPARTAMENTO DE TIC'S DE LA EMPRESA COCASINCLAIR EP, UTILIZANDO EL MARCO DE REFERENCIA COBIT 4.1

Marco Suárez [1], Gabriel Chiriboga[2]

1 Departamento de Ciencias de la Computación, Universidad de las Fuerzas Armadas ESPE, Sangolquí, Ecuador
2 Departamento de Ciencias de la Computación, Universidad de las Fuerzas Armadas ESPE, Sangolquí, Ecuador
md_suarezt@hotmail.com; gechiriboga@espe.edu.ec

RESUMEN: *El Departamento de TIC'S de la empresa COCASINCLAIR EP, entrega sus productos o servicios con poco o nada de procedimientos y sin la documentación que respalde su gestión. No se tiene claro cómo están sus procesos internos, el nivel de servicios referente al soporte técnico, la seguridad de la plataforma informática implementada y la seguridad de la información que es tratada.*

El presente documento, muestra los resultados de una auditoria a los procesos de Tecnologías de Información en la empresa COCASINCLAIR EP, mediante la aplicación de un estándar o un marco de referencia reconocido mundialmente llamado COBIT. La auditoria es realizada utilizando la Guía de Aseguramiento de COBIT 4.1.

Mediante la revisión de los seis procesos más relevantes de TI, los cuales fueron resultado de aplicar la matriz de riesgos considerando los criterios de Seguridad de la Información: Confidencialidad, Integridad y Disponibilidad, se determina la situación del Departamento de TIC'S de la empresa COCASINCLAIR EP y se propone a la Gerencia General las recomendaciones que permitan alcanzar un nivel de madurez aceptable de los procesos auditados.

Palabras Clave: *Auditoria, TI (Tecnologías de Información), COBIT (Objetivos de Control de Tecnologías de Información), Instituto de Gobernabilidad de TI, Guía de Aseguramiento de COBIT.*

ABSTRACT: *The Department of ITC'S of company COCASINCLAIR EP delivers its products or services with little or no procedures without supporting documentation management. It is not clear how their internal processes, the level of technical support services relating to the security of the computer platform and implemented information security that is treated.*

This paper shows the results of an audit of the processes of IT in the company COCASINCLAIR EP, by applying a standard or framework of reference globally recognized COBIT called... The audit is performed using COBIT Assurance Guide 4.1.

By reviewing the six most relevant IT processes, which were obtained using the risk matrix considering the criteria of information security : Confidentiality , Integrity and Availability , the Department of ITC'S Company COCASINCLAIR EP is determined General Management and the proposed recommendations to achieve an acceptable level of maturity of the processes audited.

Keywords: *Audit, IT (Information Technology), COBIT (Control Objectives for Information and related Technology), IT Institute Governance, COBIT Assurance Guide.*

I. INTRODUCCIÓN

La administración o gobernabilidad de las Tecnologías de Información y Comunicaciones (TIC's), puede ser un tema complejo por la gran cantidad de aspectos que involucran las herramientas de hardware y software existentes en el mercado, las mismas que en algún momento deben conjugarse para satisfacer los requerimientos en una empresa.

El presente artículo, muestra la revisión de seis procesos de TI, utilizando una metodología para identificar los procesos más relevantes mediante la matriz de riesgos, se determina el nivel de madurez y las recomendaciones para cada proceso auditado, apegados a lo señalado en el marco de referencia COBIT 4.1.

Como resultado general de la auditoria a los seis procesos de TI, estos se encuentran en un nivel de madurez básico o repetible (nivel 2) de acuerdo al nivel de madurez definido por el Software Engineering Institute (SEI).

En la sección Metodología, se detallan varios conceptos referentes al estándar COBIT, así como la metodología utilizada en el desarrollo de la tesis. Posteriormente, en la sección Evaluación de Resultados y Discusión, se aplica la metodología hasta identificar los seis procesos más relevantes del Departamento de TIC'S para luego evaluarlos utilizando lo señalado en COBIT 4.1 Assurance Guide. Finalmente, se presentan las conclusiones de la auditoría.

II. METODOLOGÍA

2.1 Conceptos generales

2.1.1 Información

La importancia de la "INFORMACIÓN", radica en que ha pasado a convertirse en un activo estratégico y el más valioso en las organizaciones, que permite fundamentalmente tomar decisiones oportunas, por lo tanto es necesario asegurar dicha información y el medio que lo contiene.

La Seguridad de la Información, se enfoca en garantizar a través del uso de técnicas o estándares la confidencialidad, integridad y disponibilidad de la información almacenada en un sistema informático, además de la implementación de los elementos de control que regulen los aspectos físicos, lógicos y legales del sistema.

2.1.2 Auditoria

La Auditoría en Informática es la revisión y evaluación de los controles, sistemas y procedimientos de la informática; de los equipos de cómputo, su utilización, eficiencia y seguridad; comparados con criterios establecidos, que dan como resultado un informe que contiene las recomendaciones para mejorar y optimizar sus procesos.

2.1.3 Marco de Referencia COBIT 4.1

El objetivo de los estándares que existen en el mercado, es proveer marcos referenciales de tal manera que el Director de Tecnología provea a la Gerencia General capacidades para entender mejor los servicios y procesos de TI.

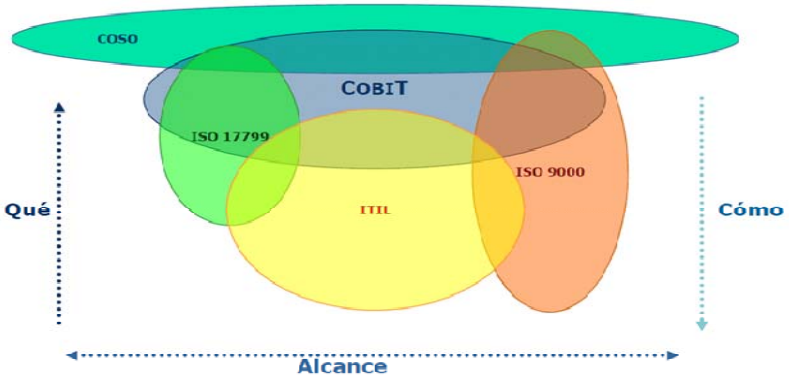

Figura No. 1: Estándares y mejores prácticas en el mercado [1]

- **COSO**, The **Committee of Sponsoring Organizations of the Treadway Commission**, es un marco de referencia de control ampliamente aceptado para gobierno corporativo y

[1] La Gobernabilidad de la Tecnología, Geovanni Roldán C.

para la administración de riesgos, así como a marcos compatibles similares.

- **COBIT**, **Control Objectives for Information and related Technology,** es un marco de referencia para la administración de TIC'S que provee herramientas administrativas como métricas y modelos de madurez para complementar el marco de referencia de control, propuesto por el IT Governance Institute.
- **ITIL, IT Infrastructure Library,** es una colección de "best practices" en la administración del servicio de TIC.
- **CMMi Capability Maturity Model Integrated,** modelo que propone un conjunto de prácticas maduras para mejorar la calidad del proceso de desarrollo del software y de los sistemas.
- **ISO/IEC 17799:2000, 27001:2005 Code of Practice for Information Security Management,** estándar internacional de seguridad de la información.
- **ISO 9001,** específica los requisitos para un Sistema de Gestión de la Calidad (SGC) que pueden utilizarse para su aplicación interna por las organizaciones.

COBIT brinda 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 representan el consenso de los expertos. Están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones habilitadas por TI, asegurarán la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien.

COBIT es un marco de referencia y no un "recetario" entendido como la panacea de la administración de TI, COBIT está alineado con otros estándares y buenas prácticas y puede ser usado junto con ellos.

2.1.3.1 Componentes de COBIT

Como respuesta a las necesidades del gobierno de TI, el marco de trabajo COBIT se creó con las características principales de ser orientado a negocios, orientado a procesos, basado en controles e impulsado por mediciones.

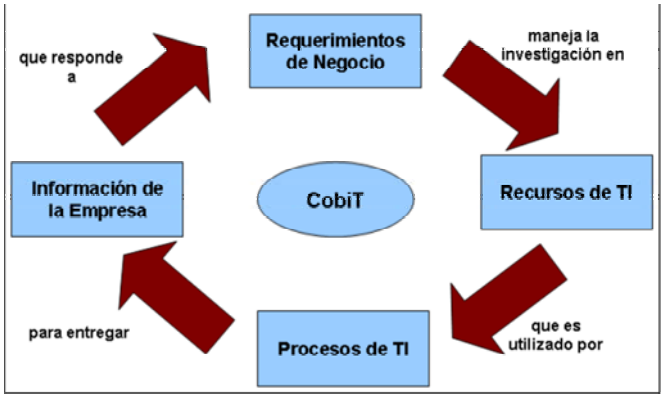

Figura No. 2: Principio Básico de COBIT [2]

2.1.3.1.1 Criterios o requerimientos de información.- Efectividad, Eficiencia, Confidencialidad, Integridad, Disponibilidad, Cumplimiento.

2.1.3.1.2 Recursos de TI.- Aplicaciones, Información, Infraestructura, Personas.

2.1.3.1.3 Procesos de TI.- Los principales procesos de TI que incluye COBIT son: Arquitectura, Manejo de Proyectos, Manejo de software, Manejo de cambio, Manejo de recursos, Seguridad Informática, Contrataciones, Manejo de Problemas, Contingencia.

2.1.3.1.4 Dominios.- COBIT define las actividades de TI en un modelo genérico de procesos organizado en cuatro dominios. Los dominios se equiparan a las áreas tradicionales de TI, los dominios son: Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte, Monitorear y Evaluar.

[2] COBIT 4.1

2.1.3.2 Cubo de COBIT

Los recursos de TI son manejados por procesos de TI para lograr metas de TI que respondan a los requerimientos del negocio. Este es el principio básico del marco de trabajo COBIT, como se ilustra en el cubo COBIT.

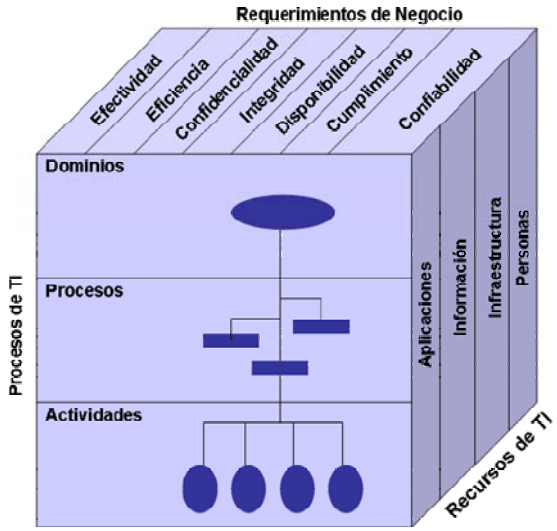

Figura No. 3: El Cubo de COBIT

2.1.3.3 Modelos de Madurez

El modelo de madurez para la administración y el control de los procesos de TI, se basa en un método de evaluación de la organización, de tal forma que se pueda evaluar a sí misma desde un nivel de no-existente (0) hasta un nivel de optimizado (5). Este enfoque se deriva del modelo de madurez que el Software Engineering Institute (SEI) definió para la madurez de la capacidad del desarrollo de software.

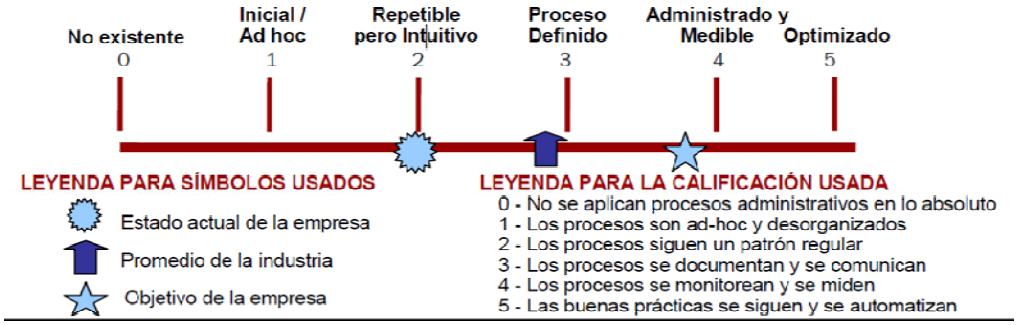

Figura No. 4 Representación Gráfica de los Modelos de Madurez [3]

El marco de trabajo general de COBIT, está compuesto por cuatro dominios que contienen 34 procesos genéricos, administrando los recursos de TI para proporcionar información al negocio de acuerdo con los requerimientos del negocio y de gobierno.

2.1.4 Riesgos de TI

El riesgo es la probabilidad de que un evento ocurra y éste afecte o tenga consecuencias negativas. Sin embargo los riesgos pueden reducirse o manejarse, es decir se puede gestionar el riesgo.

La Gestión de Riesgo es un proceso estructurado para determinar, analizar, valorar y clasificar el riesgo que afectan al logro de los objetivos, para posteriormente implementar mecanismos que permitan controlarlo.

[3] COBIT 4.1

2.1.4.1 Matriz de Riesgos

La Matriz de Riesgos es una herramienta que nos permite identificar las situaciones críticas, que pueden afectar a una organización, es una guía visual, que facilita determinar prioridades para la atención y toma de decisiones de determinados riesgos identificados.

2.2. Metodología aplicada

2.2.1 Matriz de Riesgos del Departamento de TIC'S

De acuerdo a los objetivos de la tesis, se procede a identificar los riesgos del Departamento de TIC'S en la empresa COCASINCLAIR EP orientados a determinar cuáles son los más relevantes.

2.2.2 Metodología de identificación de Riesgos utilizando COBIT 4.1.

La metodología a utilizarse es la propuesta por Julio R. Jolly Moore & Gerardo Alcarraz, en el documento Auditoría Continua: Mejores Prácticas y Caso Real.

Los riesgos de TI se encuentran en no poder satisfacer a la Empresa los requerimientos de información, es decir, el Departamento de TIC'S debería bridar EFECTIVIDAD, EFICIENCIA, CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD, CUMPLIMIENTO y CONFIABILIDAD.

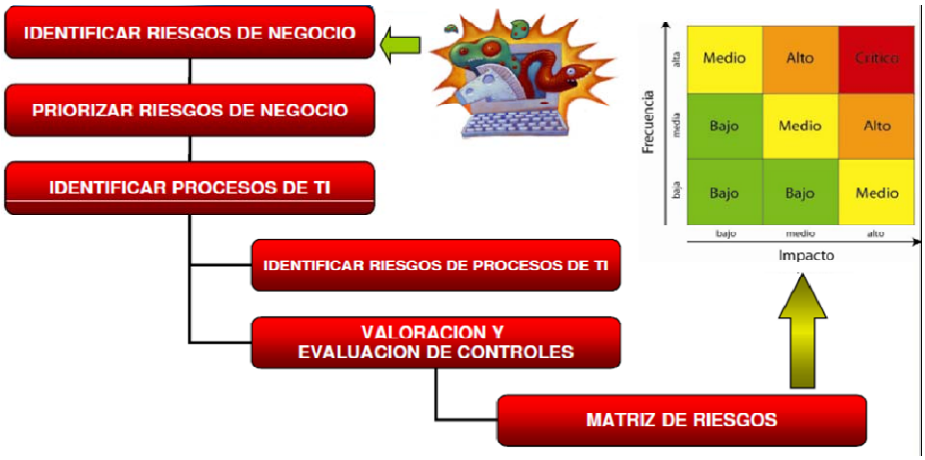

Figura No. 5 Metodología de identificación de riesgos usando COBIT. [4]

En el siguiente capítulo, se muestra los resultados de aplicar esta metodología con la explicación respectiva hasta obtener los procesos más relevantes de TI que se van a auditar.

III. EVALUACIÓN DE RESULTADOS Y DISCUSIÓN

3.1 Aplicación de la Metodología

Luego de definir la metodología, se procede a presentar los resultados obtenidos en el Departamento de TIC'S de la empresa COCASINCLAIR EP.

- **Identificar Riesgos de Negocio.-** Esta etapa consiste en listar los criterios / requerimientos del estándar de COBIT 4.1 con los riesgos asociados a estos criterios, es decir, el no tener implementados los controles eficiente y eficazmente, puede, ocasionar que las Tecnologías de Información no cubra las expectativas de Negocio.
- **Priorizar los riesgos de negocio.- S**e pone en orden de prelación los criterios de acuerdo a su criticidad y enfocados en la seguridad de la información (de acuerdo al objetivo de la tesis), es decir, Confidencialidad, Integridad y Disponibilidad.

[4] Auditoría Continua: Mejores Prácticas y Caso Real , Julio R. Jolly Moore & Gerardo Alcarraz

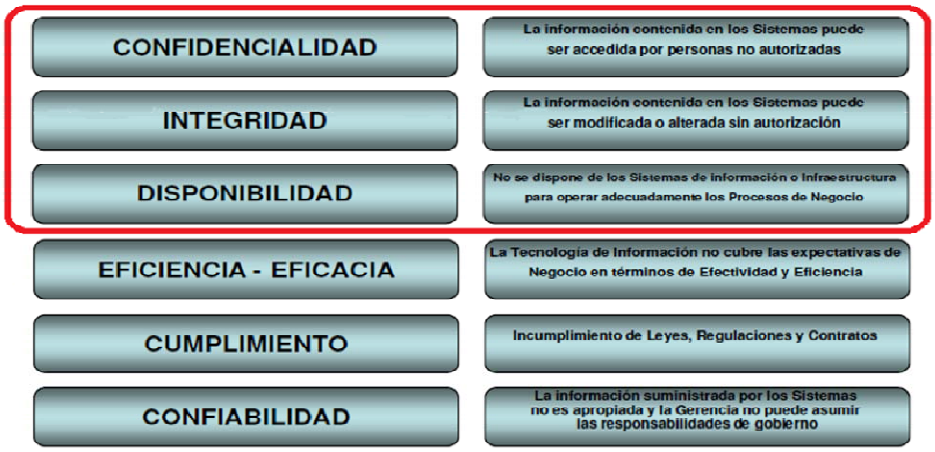

Figura No. 6 Priorización de los riesgos de negocio.

- **Identificar los procesos de TI.-** Se procede a cruzar con los procesos que se verán afectados y a catalogarlos como primarios (P) o secundarios (S) con respecto a las áreas de enfoque del Gobierno de TI, de acuerdo al estándar de COBIT 4.1. Como resultados se identificaron 18 procesos.

	Criterios de Información de CobiT						
	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
Planear y Organizar							
PO1 Definir un plan estratégico de TI	P	S					
PO2 Definir la arquitectura de la información	S	P	S	P			
PO3 Determinar la dirección tecnológica	P	P					
PO4 Definir los procesos, organización y relaciones de TI	P	P					S
PO5 Administrar la inversión en TI	P	P					
PO6 Comunicar las aspiraciones y la dirección de la gerencia	P					S	
PO7 Administrar recursos humanos de TI	P	P					
PO8 Administrar la calidad	P	P		S			S
PO9 Evaluar y administrar los riesgos de TI	S	S	P	P	P	S	S
PO10 Administrar proyectos	P	P					
Adquirir e Implementar							
AI1 Identificar soluciones automatizadas	P	S					
AI2 Adquirir y mantener software aplicativo	P	P		S			S
AI3 Adquirir y mantener infraestructura tecnológica	S	P		S	S		
AI4 Facilitar la operación y el uso	P	P		S	S	S	S
AI5 Adquirir recursos de TI	S	P				S	
AI6 Administrar cambios	P	P		P	P		S
AI7 Instalar y acreditar soluciones y cambios	P	S		S	S		
Entregar y Dar Soporte							
DS1 Definir y administrar los niveles de servicio	P	P	S	S	S	S	S
DS2 Administrar los servicios de terceros	P	P	S	S	S	S	S
DS3 Administrar el desempeño y la capacidad	P	P			S		
DS4 Garantizar la continuidad del servicio	P	S			P		
DS5 Garantizar la seguridad de los sistemas			P	P	S	S	S
DS6 Identificar y asignar costos		P					P
DS7 Educar y entrenar a los usuarios	P	S					
DS8 Administrar la mesa de servicio y los incidentes	P	P					
DS9 Administrar la configuración	P	S			S		S
DS10 Administrar los problemas	P	P			S		
DS11 Administrar los datos				P			P
DS12 Administrar el ambiente físico				P	P		
DS13 Administrar las operaciones	P	P		S	S		
Monitorear y Evaluar							
ME1 Monitorear y evaluar el desempeño de TI	P	P	S	S	S	S	S
ME2 Monitorear y evaluar el control interno	P	P	S	S	S	S	S
ME3 Garantizar el cumplimiento regulatorio						P	S
ME4 Proporcionar gobierno de TI	P	P	S	S	S	S	S

Figura No. 7 Cruce de los procesos con los criterios de información

- **Valoración de criterios**

CRITERIOS	RELACIÓN	VALORACIÓN
Confidencialidad	P	6
	S	3
Integridad	P	4
	S	2
Disponibilidad	P	2
	S	1

Siguiendo con la metodología, se procede a totalizar los criterios y a priorizarlos en orden descendente

PROCESOS DE TI	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TOTAL CRITERIOS
PO9 Evaluación de Riesgos	6	4	2	**12**
DS05 Garantizar la seguridad del sistema	6	4	1	**11**
PO2 Definir la arquitectura de información	3	4		**7**
AI6 Administración de Cambios		4	2	**6**
DS01 Definición del nivel de servicio	3	2	1	**6**
DS02 Administración del servicio de terceros	3	2	1	**6**
DS12 Administración de Instalaciones		4	2	**6**
DS11 Administración de datos		4		**4**
AI3 Adquisición y mantenimiento de arquitectura TI		2	1	**3**
AI4 Desarrollo y mantenimiento de Procedimientos de TI		2	1	**3**
AI7 Instalar y acreditar soluciones y cambios		2	1	**3**
DS13 Administración de Operaciones		2	1	**3**
PO8 Asegurar el cumplir requerimientos externos		2		**2**
AI2 Adquisición y mantenimiento de SW aplicativo		2		**2**
DS04 Asegurar el servicio continuo			2	**2**
DS03 Administración de la capacidad y el desempeño			1	**1**
DS09 Administración de la configuración			1	**1**
DS10 Administración de problemas e incidentes			1	**1**

Consecuentemente, los procesos que serán sujetos de la auditoría son:

PO9: EVALUAR Y ADMINISTRAR RIESGOS DE TI
DS05: GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS
PO2: DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN
DS01: DEFINIR Y ADMINISTRAR NIVELES DE SERVICIO
DS02: ADMINISTRAR SERVICIOS DE TERCEROS
DS12: ADMINISTRAR EL AMBIENTE FÍSICO

- **Identificación de los riesgos relacionados a los procesos de TI**
  A continuación, se detallan los riesgos asociados a los procesos anteriormente identificados.

PROCESOS DE TI	DEFINICIÓN DE COBIT	DEFINICIÓN DE RIESGO
PO9 EVALUAR Y ADMINISTRAR RIESGOS	Elaborar un marco de trabajo de administración de riesgos el cual está integrado en los marcos gerenciales de riesgo operacional, evaluación de riesgos, mitigación del riesgo y comunicación de riesgos residuales.	Los riesgos de TI no son identificados, analizados, tratados y comunicados de manera adecuada.
DS05 GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS.	Definir políticas, procedimientos y estándares de seguridad de TI y en el monitoreo, detección, reporte y resolución de las vulnerabilidades e incidentes de seguridad.	No se tiene criterios para comparar la gestión de la seguridad de los sistemas (accesos, autorizaciones, modificaciones) antes, durante y después de su uso.
PO2 DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN	Establecer un modelo de datos empresarial que incluya un esquema de clasificación de información que garantice la integridad y consistencia de todos los datos.	Datos diversos de varias fuentes, no se mantiene un estándar o formato. Los datos pueden ser modificados y no se puede determinar la veracidad de los mismos.
DS01 DEFINIR Y ADMINISTRAR NIVELES DE SERVICIO	Identificar los requerimientos de servicio, el acuerdo de niveles de servicio y el monitoreo del cumplimiento de los niveles de servicio.	Incumplir estándares de servicio por falta de control y de seguimiento por servicio. Las especificaciones pueden estar mal detalladas o incompletas.
DS02 ADMINISTRAR SERVICIOS DE TERCEROS	Establecer relaciones y responsabilidades bilaterales con proveedores calificados de servicios cumplidos por terceros, y el monitoreo de la prestación del servicio para verificar y asegurar la adherencia a los convenios.	Desconocimiento de las responsabilidades contractuales de los proveedores por servicio prestado, puede ocasionar incumplimiento de contratos o convenios.
DS12 ADMINISTRAR EL AMBIENTE FÍSICO	Proporcionar y mantener un ambiente físico adecuado para proteger los activos de TI contra acceso, daño o robo.	Se producen interrupciones en los Servicios de TI debido a problemas físicos de los Equipos y/o Instalaciones.

3.2 Resultados de la Auditoria.

El objetivo de IT Assurance Guide, es proporcionar orientación sobre el uso de COBIT para apoyar la gobernabilidad por medio de procesos de aseguramiento de TI. Esta guía muestra cómo se deben evaluar los controles de los procesos.

Para cada uno de los procesos auditados y de acuerdo a las evidencias encontradas (cuestionarios y documentos), se establecen las observaciones, efectos, causas y recomendaciones, posteriormente se determina el nivel de madurez.

No.	DOMINIO	NOMBRE DEL PROCESO	NIVEL DE MADUREZ
1	PLANEAR Y ORGANIZAR	**PO9**: EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI	1
2	ENTREGAR Y DAR SOPORTE	**DS5**: GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS	2

3	PLANEAR Y ORGANIZAR	**PO2**: DEFINIR LA ARQUITECTURA DE LA INFORMACIÓN	1
4	ENTREGAR Y DAR SOPORTE	**DS1**: DEFINIR Y ADMINISTRAR LOS NIVELES DE SERVICIO.	2
5	ENTREGAR Y DAR SOPORTE	**DS2**: ADMINISTRAR LOS SERVICIOS DE TERCEROS	3
6	ENTREGAR Y DAR SOPORTE	**DS12**:ADMINISTRACIÓN DEL AMBIENTE FÍSICO	2

Tabla No.1 Nivel de Madurez de los procesos auditados en la empresa COCASINCLAIR EP

Esto demuestra en general que los procesos auditados, se encuentran en un nivel básico o repetible, que siguen un patrón regular. La empresa ha definido ciertas actividades o controles para el tratamiento de la información y que se encuentran plasmadas en la infraestructura de TI.

IV. TRABAJOS RELACIONADOS

Actualmente no existen trabajos de tesis de postgrado en la Universidad de las Fuerzas Armadas ESPE relacionados a una auditoría de procesos de TIC'S, aplicando la metodología propuesta por Julio R. Jolly Moore & Gerardo Alcarraz.

V. CONCLUSIONES Y TRABAJO FUTURO

- A través del uso de un estándar, una metodología o una combinación entre estas, se pueden optimizar los recursos tecnológicos y alinear los objetivos del Departamento de TIC'S a los objetivos del negocio desde la fases de la planificación, operación, control y finalmente a la evaluación de sus procesos.

- Los estándares o marcos de referencia para la administración de las Tecnologías de Información, se han ido desarrollando y mejorando con el pasar de los años y son utilizados por grandes empresas a nivel mundial, esto ha permitido sustentar los resultados obtenidos de la revisión de los procesos en el Departamento de TIC'S de la empresa COCASINCLAIR EP.

- Los riesgos que se presentan en una empresa, están relacionados directamente a la afectación de las operaciones del negocio o en no poder seguir prestando el servicio en óptimas condiciones. La elaboración de un plan la continuidad del negocio, garantizaría que se ejecuten las actividades mínimas para que COCASINCLAIR EP siga funcionando hasta que vuelva a su normalidad los procesos afectados.

- Gestionar o administrar las TIC'S, requiere la definición de responsabilidades para los miembros del área, mecanismos para un uso eficiente y eficaz de los recursos, concienciar a la alta gerencia acerca de los costos de TI, brindar soporte técnico a la empresa con parámetros de evaluación del servicio, así como proponer la reducción de costos mediante la estandarización de aplicaciones o servicios.

- COBIT es un marco de referencia y no un "recetario" entendido como la panacea de la administración de TI, COBIT está alineado con otros estándares y buenas prácticas y puede ser usado junto con ellos.

- Los riesgos pueden encontrase en todo el Departamento de TI, en sus procesos, aplicaciones y servicios que brinda y los factores que pueden determinan posibles riesgos asociados a la parte interna y externa (proveedores, clientes). Los riesgos inherentes son parte del negocio, cada actividad tiene asociada uno o más riesgos.

- Hoy en día es muy importante la administración de los riesgos asociados a la tecnología, tales como el aumento en requerimientos regulatorios, así como la dependencia crítica de muchos procesos de negocio en TI. La información contenida en el hardware y manipulada a través de un software, es el activo más importante en la empresa COCASINCLAIR EP.

VI. AGRADECIMIENTOS

Un agradecimiento al Eco. Gabriel Chiriboga. B MSi, por su aporte y guía para la realización del presente documento, así como por su dedicación en la dirección de la tesis en la cual ha compartido sus conocimientos y experiencias adquiridas en el campo de la Auditoria.

Un agradecimiento especial a la Gerencia General de la empresa COCASINCLAIR EP, por permitirme aplicar mis conocimientos de Auditoria a los procesos que se realizan en el Departamento de TIC'S.

VII. REFERENCIAS BIBLIOGRÁFICAS

1. Cocasinclair EP. (2011-2015). *Plan estratégico institucional*.
2. Cocasinclair EP. (2012). *Plan anual de compras* (PAC).
3. Cocasinclair EP. (2012). *Estructura orgánica por procesos*.
4. Echenique, J. (2001). *Auditoría en informática*, (2da ed). México, Mc Graw Hill.
5. Espejo, O., & Torres, C. (2006). *Administración de tecnologías de la información*. México.
6. Hernández, E. (2000). *Auditoría en informática*, (2da ed). México. Cecsa.
7. IT Governance Institute. (2007). *Cobit 4.1*. Estados Unidos.
8. IT Governance Institute. (2007). *IT Assurance Guide Using Cobit.* Estados Unidos.
9. Jolly Moore, J., & Alcarraz, G. (2010). *Auditoría continua: mejores prácticas y caso real.* Congreso Latinoamericano de Auditoría Interna y Evaluación de Riesgos.
10. Piattini, M., & Del peso, E. (2001). *Auditoría informática un enfoque práctico*, (2da ed). México. Alfaomega.
11. Roldán, G. (2011). *Administración y Auditoria de las TIC's*.
12. Recuperado de *http://www.slideshare.net/guestfa372b/coso-2361475*
13. Recuperado de *http://www.protegete.info/*
14. Recuperado de *http://www.auditool.org/index.php?option=com_content&view=article&id=827:riesgo-tecnologico-su-medicion-como-prioridad-para-el-aseguramiento-del-negocio-&catid=57:auditoria-de-ti&itemid=112*
15. Recuperado de *http://www.sigweb.cl/biblioteca/matrizderiesgo.pdf*
16. Price Waterhouse Coopers. (2008). Recuperado de *http://www.pwc.com/ve/es/asesoria-gerencial/boletin/assets/boletin-advisory-edicion-09-2008.pdf*