DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

MAESTRIA EN GERENCIA DE SISTEMAS IX PROMOCION

TESIS PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN GERENCIA DE SISTEMAS

TEMA: "AUDITORÍA INFORMÁTICA EN LA EMPRESA ENAP SIPETROL S.A DE ACUERDO A LA METODOLOGÍA COBIT VERSIÓN 4.1"

AUTORES: NELLY ROCIO PEREZ ESPINOSA

MARCO ANTONIO CHUQUIMARCA VEGA

DIRECTOR: ING. GIOVANNI ROLDAN

SANGOLQUÍ

2015

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACION

CERTIFICADO

ING. GIOVANNI ROLDÁN
Director

ING. MÓNICA JIMBO
Oponente

CERTIFICAN

Que el trabajo titulado "AUDITORIA INFORMATICA EN LA EMPRESA ENAP SIPETROL S.A. DE ACUERDO A LA METODOLOGIA COBIT VERSION 4.1", realizado por Nelly Pérez Espinosa y Antonio Chuquimarca Vega, ha sido guiado y revisado periódicamente y cumple normas estatutarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Universidad de la Fuerzas Armadas ESPE.

Debido a que el presente trabajo servirá de guía práctica a los estudiantes y profesionales que necesiten realizar una auditoría informática basada en Metodología Cobit versión 4.1, se recomienda su publicación.

El mencionado trabajo consta de un documento empastado y un disco compacto, el cual contiene los archivos en formato portátil de Acrobat (PDF). Autorizan a Nelly Pérez Espinosa y Antonio Chuquimarca Vega, entregar el mismo a la unidad de Gestión de Postgrados.

Sangolquí, Abril de 2015

ING. GIOVANNI ROLDÁN
DIRECTOR

ING. MÓNICA JIMBO
OPONENTE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

MAESTRÍA EN GERENCIA DE SISTEMAS IX PROMOCIÓN

DECLARACIÓN DE RESPONSABILIDAD

Nelly Rocío Pérez Espinosa

Marco Antonio Chuquimarca Vega

DECLARAMOS QUE:

El proyecto de grado denominado "AUDITORIA INFORMATICA EN LA EMPRESA ENAP SIPETROL S.A. DE ACUERDO A LA METODOLOGIA COBIT VERSION 4.1", ha sido desarrollado en base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de nuestra autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, Abril de 2015

Nelly Pérez Espinosa

Antonio Chuquimarca Vega

UNIVERSIDAD DE LAS FUERZAS ARMADAS

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACION

MAESTRIA EN GERENCIA DE SISTEMAS IX PROMOCION

AUTORIZACION

Nelly Pérez Espinosa y Antonio Chuquimarca Vega, autorizamos a la Universidad de las Fuerzas Armadas ESPE, la publicación en la biblioteca virtual de la Institución, el trabajo "AUDITORÍA INFORMATICA EN LA EMPRESA ENAP SIPETROL S.A. DE ACUERDO A LA METODOLOGIA COBIT VERSION 4.1", cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Sangolquí, Abril de 2015

Nelly Pérez Espinosa

Antonio Chuquimarca Vega

DEDICATORIA

"Dedico este trabajo a mi familia, en especial a mi querida madre Elvia Espinosa, quien es ejemplo de perseverancia, fortaleza y optimismo, quien con sus enseñanzas y palabras de amor me da el aliento suficiente para seguir esforzándome día a día."

Nelly Pérez Espinosa

"Se dedica este proyecto a mi esposa Mercedes y a mis hijos Daniela y Nicolás, por haber permitido utilizar su tiempo en este proyecto, a su comprensión y amor incondicional"

Antonio Chuquimarca Vega

AGRADECIMIENTO

"Un agradecimiento especial al Ing. Giovanny Roldan, Ing. Carlos Procel e Ing. Mónica Jimbo por el tiempo y la ayuda para la elaboración del presente proyecto, a Antonio Chuquimarca por ser el compañero y amigo en esta larga jornada."

Nelly Pérez Espinosa

"Gracias a Dios por los dones recibidos, a las personas que guiaron este trabajo, Ing. Giovanni Roldán, Ing. Mónica Jimbo e Ing. Carlos Procel y a Nelly Pérez por su lucidez, claridad de pensamiento y paciencia en el desarrollo de este proyecto."

Antonio Chuquimarca Vega

CONTENIDO

CERTIFICADO i
AUTORÍA DE RESPONSABILIDAD ii
AUTORIZACIÓN iii
DEDICATORIA iv
AGRADECIMIENTO v
INDICE GENERAL vi
RESUMEN xiii
ABSTRACT xiv
1 CAPITULO I 1
1.1 METODOLOGÍA COBIT 4.1 1
1.1.1 Marco Teórico 1
1.1.2 Origen de la Metodología Cobit 1
1.1.3 Documentos de Referencia 3
1.1.4 Dominios Cobit versión 4.1 5
1.1.5 Procesos Cobit 6
1.1.6 Objetivos de Control 8
1.1.7 Marco de Trabajo de Cobit 12
1.1.8 Modelos de Madurez 13
2 CAPITULO II 15
2.1 Introducción 15
2.2 Objetivos de la Auditoría Informática 16
2.3 Descripción del Ámbito del Negocio 16
2.4 Descripción del Ámbito de TI 19
2.4.1 Principales Procesos de TI 19
2.4.2 Infraestructura de la Organización 20
2.5 Selección de Procesos a Auditar 24
2.5.1 Criterios de Selección 24
2.5.2 Análisis de las Metas del Negocio 26
2.5.3 Objetivos y Metas de TI 28
2.5.4 Relación entre las Metas del Negocio y Metas de TI 30
2.5.5 Relación entre Metas de TI y Procesos Cobit 32
2.5.6 Correlación entre Procesos Cobit vs Metas de TI 33
2.5.7 Resumen de Dominios y Procesos Cobit 4.1 a ser Auditados 35

3 CAPITULO III 36
3.1 Introducción 36
3.2 Preparación del Plan de Auditoría 36
3.3 Asignación de las Tareas al Equipo Auditor 37
3.4 Preparación de los Documentos de Trabajo 37
3.5 Plan de Auditoría 37
3.5.1 Objetivo de la Auditoría 37
3.5.2 Alcance 38
3.5.3 Criterios de Auditoría 38
3.5.4 Equipo Auditor 38
3.5.5 Responsabilidades: 38
3.5.6 Áreas a ser Auditadas 39
3.5.7 Proceso de Auditoría 39
3.5.8 Cronograma de Auditoría 41
3.6 Análisis de los Procesos Seleccionados 42
3.6.1 PO PLANEAR Y ORGANIZAR 42
3.6.2 DS ENTREGAR Y DAR SOPORTE 65
3.6.3 AI ADQUIRIR E IMPLEMENTAR 96
3.6.4 ME MONITOREAR Y EVALUAR 100
4 CAPITULO IV 119
4.1 Metodología 119
4.2 Objetivos del Capítulo 119
4.3 Resultado de la Auditoría 120
4.3.1 PO PLANEAR Y ORGANIZAR 121
4.3.2 DS ENTREGAR Y DAR SOPORTE 149
4.3.3 AI ADQUIRIR E IMPLEMENTAR 187
4.3.4 ME MONITOREAR Y EVALUAR 192
4 INDICADORES DE DESEMPEÑO 212
4.4 Establecimiento del Nivel de Madurez de la Industria 213
4.5 Establecimiento del Nivel de Madurez para cada Proceso 215
4.5.1 PO PLANEAR Y ORGANIZAR 215
4.5.2 DS - ENTREGAR Y DAR SOPORTE 219
4.5.3 AI ADQUIRIR E IMPLEMENTAR 223
4.5.4 ME MONITOREAR Y EVALUAR 224

5 CAPITULO V 228
5.1 INFORME FINAL DE AUDITORIA 228
6 CAPITULO VI 239
6.1 PROYECTOS ASOCIADOS A LAS RECOMENDACIONES 239
6.2 PRINCIPALES ACCIONES PROPUESTAS 243
6.2.1 Esquema de un Plan Estratégico de TI 243
6.2.2 Esquema de Desarrollo de Proyectos 245
6.2.3 Análisis de procesos de TI 246
6.2.4 Análisis de funciones de TI 247
6.2.5 Proyecto de Análisis de Gestión de Riesgos de TI 249
6.2.6 Clasificación de la información 250
6.2.7 Definición de Acuerdos de Niveles de Servicio (SLA's) 251
6.2.8 Esquema de un Plan de Continuidad de TI 251
6.2.9 Esquema de una Política de Seguridad 254
6.2.10 Esquema de un plan de seguridad 255
6.2.7 Administración de Operaciones 256
6.3 Plan de Implementación 256
6.3.1 FASE I 261
6.3.2 FASE II 261
6.3.3 FASE III 262
7 CAPITULO VII 278
7.1 CONCLUSIONES 278
7.2 RECOMENDACIONES 282

Bibliografía

Anexos

INDICE DE TABLAS

Tabla 1 Comparación entre COSO, COBIT e ITIL xx
Tabla 2 Detalle de hardware 22
Tabla 3 Detalle de Software 23
Tabla 4 Roles y Responsabilidades de TI 23
Tabla 5 Relación entre Objetivos y Metas TI 29
Tabla 6 Relación entre Metas del Negocio y TI 31
Tabla 7 Relación Metas de TI y Procesos Cobit 4.1 32
Tabla 8 Matriz de Procesos Cobit 4.1 a Metas de TI de Enap-Sipetrol 34
Tabla 9 Responsabilidades del Equipo Auditor 38
Tabla 10 Cronograma de Auditoría 41
Tabla 11 Matriz RACI PO1 42
Tabla 12 Matriz RACI PO4 49
Tabla 13 Matriz RACI PO9 60
Tabla 14 Matriz RACI DS2 65
Tabla 15 Matriz RACI DS4 70
Tabla 16 Matriz RACI DS5 79
Tabla 17 Matriz RACI DS13 90
Tabla 18 Matriz RACI AI5 96
Tabla 19 Matriz RACI ME1 100
Tabla 20 Matriz RACI ME3 105
Tabla 21 Matriz RACI ME4 110
Tabla 22 Indicadores de Desempeño PO1 128
Tabla 23 Indicadores de Desempeño PO4 141
Tabla 24 Indicadores de Desempeño PO9 148
Tabla 25 Indicadores de Desempeño DS4 164
Tabla 26 Indicadores de Desempeño DS5 177
Tabla 27 Indicadores de Desempeño DS13 186
Tabla 28 Indicadores de Desempeño AI5 191
Tabla 29 Indicadores de Desempeño ME1 197
Tabla 30 Indicadores de Desempeño ME3 202
Tabla 31 Indicadores de Desempeño ME4 212
Tabla 32 Análisis Resultados Encuesta 214
Tabla 33 Resumen Niveles de Madurez 239

Tabla 34 Proyectos Sugeridos 243
Tabla 35 Proyectos Asociados a las Recomendaciones 257
Tabla 36 Proyectos por Afinidad en el BSC 258

INDICE DE CUADROS

Cuadro 1 Análisis Proceso PO1 43
Cuadro 2 Análisis Proceso PO4 50
Cuadro 3 Análisis Proceso PO9 61
Cuadro 4 Análisis Proceso DS2 66
Cuadro 5 Análisis Proceso DS4 71
Cuadro 6 Análisis Proceso DS5 80
Cuadro 7 Análisis Proceso DS13 91
Cuadro 8 Análisis Proceso AI5 97
Cuadro 9 Análisis Proceso ME1 101
Cuadro 10 Análisis Proceso ME3 106
Cuadro 11 Análisis Proceso ME4 111
Cuadro 12 Análisis Proceso PO1 121
Cuadro 13 Análisis Proceso PO4 129
Cuadro 14 Análisis Proceso PO9 142
Cuadro 15 Análisis Proceso DS2 149
Cuadro 16 Análisis Proceso DS4 154
Cuadro 17 Análisis Proceso DS5 165
Cuadro 18 Análisis Proceso DS13 178
Cuadro 19 Análisis Proceso AI5 187
Cuadro 20 Análisis Proceso ME1 192
Cuadro 21 Análisis Proceso ME3 198
Cuadro 22 Análisis Proceso ME4 203
Cuadro 23 Esquema para desarrollar un Plan Estratégico de TI 243
Cuadro 24 Esquema para el Desarrollo de Proyectos 245
Cuadro 25 Análisis de Procesos de TI 246
Cuadro 26 Análisis de Funciones de TI 248
Cuadro 27 Esquema para la Gestión de Riesgos de TI 249
Cuadro 28 Clasificación de la Información 250

Cuadro 29 Esquema de un Plan de Continuidad 251
Cuadro 30 Esquema de una Política de Seguridad 254
Cuadro 31 Software Libre para Gestión de Incidentes 255

INDICE DE FIGURAS

Figura 1 Producción Anual de Petróleo xvii
Figura 2 Inversión en Tecnología xviii
Figura 3 Integración Cobit con Estándares 3
Figura 4 Estructura Cobit 5
Figura 5 Procesos Cobit 7
Figura 6 Principio Básico de Cobit 8
Figura 7 Interrelaciones de los componentes 9
Figura 8 El Cubo de Cobit 13
Figura 9 Representación Gráfica Modelos de Madurez 14
Figura 10 Diagrama de Procesos de Negocio 17
Figura 11 Procesos del Área de Tecnología de Información 20
Figura 12 Infraestructura Tecnológica 21
Figura 13 Sistemas de Voz y Datos 22
Figura 14 Definir las Metas de TI 25
Figura 15 BSC ENAP-SIPETROL 27
Figura 16 Resumen Procesos Cobit 4.1 a ser auditados 35
Figura 17 Resumen Procesos Cobit 4.1 a ser auditados 38
Figura 18 Modelo de Madurez Proceso PO1 215
Figura 19 Modelo de Madurez Proceso PO4 216
Figura 20 Modelo de Madurez Proceso PO9 218
Figura 21 Modelo de Madurez Proceso DS2 219
Figura 22 Modelo de Madurez Proceso DS4 220
Figura 23 Modelo de Madurez Proceso DS5 221
Figura 24 Modelo de Madurez Proceso DS13 222
Figura 25 Modelo de Madurez Proceso AI5 223
Figura 26 Modelo de Madurez Proceso ME1 224
Figura 27 Modelo de Madurez Proceso ME3 225
Figura 28 Modelo de Madurez Proceso ME4 226

Figura 30 Fases para la Implementación de Proyectos Sugeridos 259

RESUMEN

Actualmente, la mayoría de organizaciones dependen de los servicios que entrega el área de tecnología tanto en hardware, software y comunicaciones, requiere que sus procesos sean controlados y medidos a fin de alinearlos con los objetivos organizacionales y de utilizar los recursos asignados de manera eficiente. Determinar la gestión y nivel de desempeño de los procesos de TI en ENAP-SIPETROL, por medio de una auditoría informática. El equipo auditor sugiere proyectos de mejora basados en el informe final de auditoría, se utilizó COBIT 4.1 como guía debido a que es el integrador de las mejores prácticas de TI estableciendo un marco de trabajo para el adecuado Gobierno de TI que utiliza 210 objetivos de control para los 34 procesos de Cobit versión 4.1, agrupados en 4 dominios y los mide a través de los niveles de madurez en una escala de 0-5, este es el punto hasta el cual un determinado proceso esta explícitamente definido, administrado, medido y controlado. Los procesos auditados son el resultado de la relación entre Metas del Negocio, Objetivos y Metas de TI y Procesos Cobit. Dichas relaciones permitieron conocer cuáles procesos contienen la mayor cantidad de metas que permiten cumplir con los objetivos de TI, se obtiene el nivel de madurez de los procesos auditados para evidenciar la situación actual de TI concluyendo que el 73% de los procesos deben ser mejorados. El mayor riesgo que afecta al negocio es la falta de corresponsabilidad e involucramiento de la Dirección General en la toma de decisiones del área, delegando la responsabilidad a la Gerencia de TI. Finalmente los procesos que tienen relación con la seguridad y continuidad del negocio no contemplan un plan de acción ya que no forman parte del plan estratégico del negocio, constituyendo un grave riesgo para la organización.

PALABRAS CLAVE:

- **AUDITORÍA INFORMÁTICA**
- **COBIT**
- **OBJETIVOS DE CONTROL**
- **MODELOS DE MADUREZ**
- **PROCESOS**

ABSTRACT

At present, most organizations rely on services that deliver the IT department in hardware, software and communications, making it a vital area, to do that IT requires internal processes which must be controlled and measured in order to align with organizational goals and to use the resources in an efficient manner. Define the management and performance of IT processes in ENAP SIPETROL, through an information technology audit. In addition, the audit team presents a Final Audit Report to suggest projects and improve IT area. COBIT 4.1 was used as a guide for the implementation of the information technology audit, since Cobit is the integrator of best practices of IT establishing a framework for the proper government that uses 210 control objectives for 34 processes in the version 4.1, grouped in 4 domains and measures them through the maturity levels on a scale of 0-5, this is the point to which a specific process is explicitly defined, managed, measured, and controlled. Audited processes are the result of the relationship between business goals, objectives and goals of IT and Cobit processes. These relationships were showed in the processes which contain the largest number of goals that meet the objectives of IT. As result Maturity levels in audited processes, concluding that 73% of the processes should be improved. Finally the greatest risk affecting the business is the lack of responsibility and involvement of the management Learn in the decision-making of the area, delegating full responsibility in the IT management. The processes that relate to the security and continuity of the business do not include an action plan since they do not form part of the strategic business plan, constitute a serious risk to the organization.

KEY WORDS:

- **IT AUDITING**
- **COBIT**
- **CONTROL OBJECTIVES**
- **MATURITY MODELS**
- **PROCESSES**.

AUDITORIA INFORMATICA EN LA EMPRESA ENAP SIPETROL S.A. DE ACUERDO A LA METODOLOGIA COBIT VERSION 4.1

Analizando la realidad del entorno de negocios en el país, se encuentra que las empresas ejercen su administración interna generando áreas operativas, las mismas que funcionan de forma independiente y no integrada como debería dictarlo una adecuada gestión.

Bajo ese concepto el área de tecnología ha venido funcionando muchas veces de manera independiente del resto de las áreas de la empresa lo cual la ha mantenido alejada de las necesidades de la organización y con soluciones, en ocasiones costosas y poco funcionales lo cual ha afectado la imagen de TI considerando su función como un gasto en lugar de una inversión que permita reducir costes y optimizar las tareas en las diferentes áreas a las que se debe.

Es por ello, que un profesional a cargo de Tecnología, debe plantearse sobre el adecuado funcionamiento del área, para lo cual debe reconsiderar la función de gestión, tomando en cuenta, en primer lugar, la alineación de los objetivos de Tecnología con los objetivos del negocio, un adecuado funcionamiento de los procesos de tecnología con una utilización de recursos acorde a los que la empresa pueda proveerle y con una respuesta rápida a los requerimientos del negocio y el entorno en el que se desenvuelve.

La organización debe por tanto ser capaz de reconocer el valor generado por el uso de la tecnología y considerar a la información como el activo más importante ya que actualmente es posible enviarla de un sitio a otro sin restricciones de tiempo o espacio, esto a más de ser una ventaja también trae consigo muchas amenazas debido a que la información está expuesta a una serie de riesgos que deben ser considerados tales como: accesos no autorizados, exposición a virus o eventos que afecten la infraestructura en la que se mantiene.

La gestión de Tecnología bajo este escenario, debe apoyar los requerimientos del negocio para lo cual la gerencia debe aportar con los lineamientos estratégicos y

participar en las decisiones claves para crear conjuntamente valor y controlar los riesgos, incorporando para ello el concepto de Gobierno de Tecnología de la Información, cuyo objetivo principal es generar una estructura de relaciones y procesos para dirigir y controlar la empresa y de esta manera alcanzar los objetivos planteados. ¿Cómo determinar entonces que esta gestión sea la adecuada y correcta?

Utilizando una herramienta de administración independiente y objetiva que analice tanto la gestión como el cumplimiento acorde a prácticas definidas y establecidas a través de los años y que permite identificar desvíos y generar correcciones como es la auditoría.

Esta auditoría debe contar con un marco estructurado y desarrollado para tratar temas específicos de tecnología considerando por tanto a COBIT (Objetivos de Control para la Información y Tecnología Relacionada) como la herramienta idónea para realizar este análisis del área de tecnología dentro de la organización y obtener un diagnóstico de su funcionamiento y gestión.

JUSTIFICACION E IMPORTANCIA

ENAP SIPETROL S.A., es filial de la Empresa Nacional del Petróleo de Chile, ENAP, y opera en el Ecuador desde enero de 2003, con la misión de explorar y explotar yacimientos hidrocarburíferos, bajo los más altos estándares de calidad y seguridad de la industria petrolera, siempre en armonía con el medioambiente y la sustentabilidad.

ENAP SIPETROL S.A, se encuentra dentro de las 200 empresas más importantes en el Ecuador (EKOS, 2013) (Anexo 1), aporta millones de dólares en ingresos tanto de la venta del crudo como del impuesto generado por la extracción, en la siguiente figura se muestra el resumen en valores correspondiente al año 2009, 2010, 2011 y 2012.

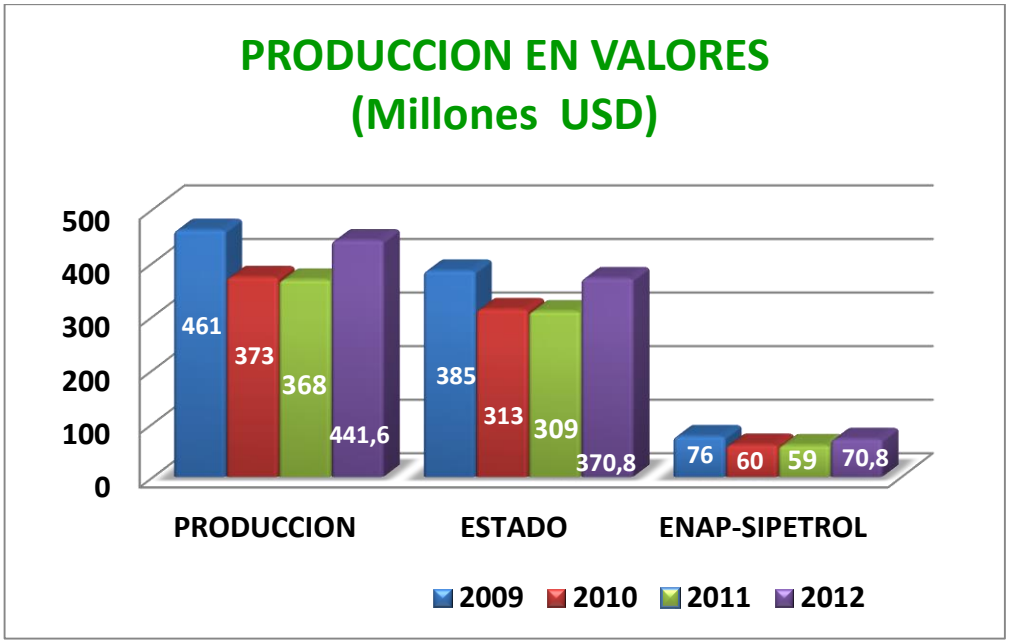


Figura 1 Producción Anual de Petróleo

Para ENAP SIPETROL S.A, la información y la tecnología que la soporta, representan los activos más valiosos de la empresa debido, a que gracias a la tecnología de punta utilizada para el análisis de imágenes en 2 o 3 dimensiones de los yacimientos es posible ubicar más reservas de petróleo y extraerlo con el menor

riesgo, minimizando de esta manera los costos de perforación y extracción. La organización se preocupa en invertir en tecnología anualmente para la renovación y mantenimiento en software y hardware necesarios para ser competitivos en el mercado, a continuación se presenta la inversión realizada en los dos últimos años en el ámbito tecnológico.

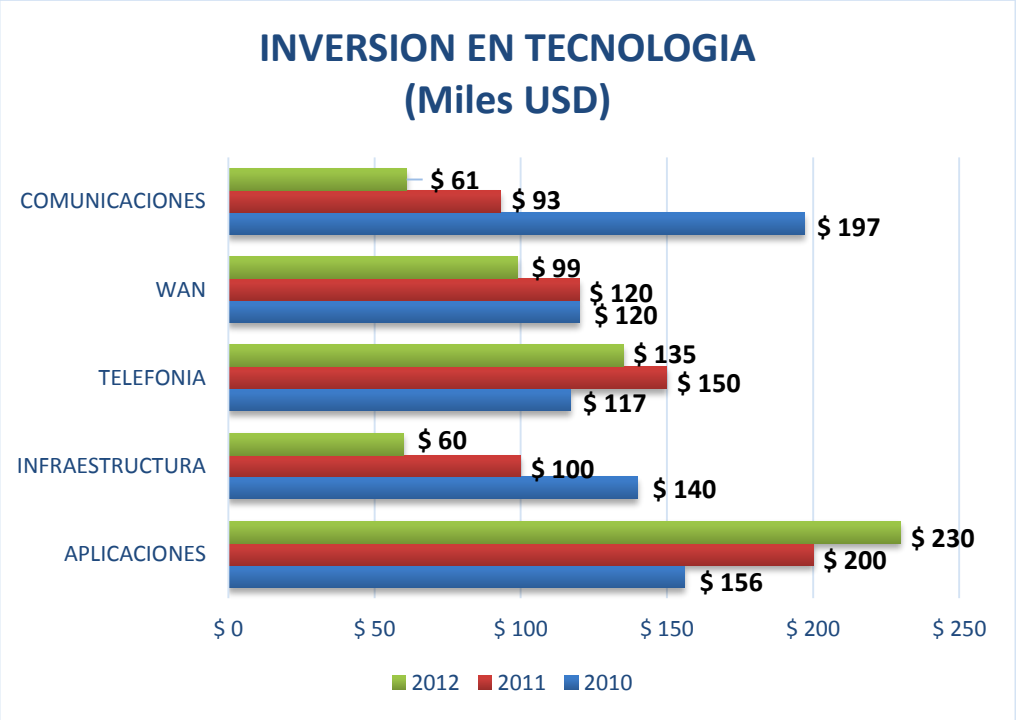


Figura 2 Inversión en Tecnología

En ENAP SIPETROL S.A., no se ha realizado ninguna auditoría informática que permita evaluar el funcionamiento del área de sistemas, la Dirección considera indispensable realizar una evaluación que permita:

- Alinear los objetivos del Negocio con los objetivos de TI
- Evaluar el desempeño actual del área de tecnología
- Determinar los riesgos de TI que afecten al Negocio
- La verificación del cumplimiento de la Normativa en este ámbito
- Generar nuevos proyectos de los resultados obtenidos en la Auditoría

Inicialmente, la auditoría de sistemas solamente se encargaba de la revisión de los sistemas de información en las áreas de desarrollo, operación y mantenimiento. Este concepto ha cambiado debido a la expansión e importancia de la tecnología en todas las áreas que conforman una empresa, ampliándose el concepto a una Auditoría Informática.

Actualmente, las Auditorías Informáticas se encargan de evaluar y verificar políticas, controles, procedimientos y seguridad en los recursos dedicados al manejo de la información, mediante la aplicación de una metodología que debe de ejecutarse con objetividad y oportunidad.

La necesidad de contar con lineamientos y herramientas estándar para el ejercicio de las auditorias informáticas ha promovido la creación y desarrollo de metodologías actualmente aceptadas: ***COSO*** (*Committee of Sponsoring Organizations* – Comité de Soporte de las Organizaciones, ***COBIT*** (*The Control Objectives for Information and related Technology* – Objetivos de Control para la Información y Tecnología Relacionada), e ***ITIL*** (*The Information Technology Infrastructure Library* – Biblioteca de Infraestructura de Tecnologías de la Información).

A continuación se realiza una comparación de las principales características de estas 3 metodologías:

Tabla 1

Comparación entre COSO, COBIT e ITIL

CARACTERISTICAS	COSO	COBIT	ITIL
Dirigido a	Administración	Administración, Usuarios, Auditores de Sistemas, Responsables de TI	Administración, Usuarios, Responsables de TI
El Control Interno es Visto como	Procesos	Conjunto de procesos incluyendo políticas, procedimientos, prácticas y estructura Organizacional	Fases del proceso de Servicio
Enfoque	Lineamientos Empresariales con énfasis en el área financiera	Tecnología de la información	Gestión de Servicios
Los Objetivos Organizacionales de Control Interno	Eficacia y eficiencia de las operaciones Confiabilidad de la Información financiera Cumplimiento con las leyes y normas aplicables	Efectividad y Eficiencia de las operaciones Confidencialidad, Integridad y disponibilidad de la información Cumplimiento con leyes y normas	Efectividad y Eficiencia de las operaciones Confidencialidad, Integridad y disponibilidad de la información Cumplimiento con leyes y normas
Componentes, Dominios o Fases	Componentes: Ambiente de Control Análisis del Riesgo Actividades de Control Información y Comunicación Monitoreo	Dominios: Planeación y Organización Adquisición e Implementación Prestación de Servicio y Soporte Seguimiento	Fases del ciclo de vida del servicio: Estrategia de Servicio Diseño de Servicio Transición de Servicio Operación del Servicio Mejoramiento Continuo del Servicio
Evaluación de la Efectividad del Control Interno	En un punto del tiempo	Por un periodo de tiempo	Por un periodo de tiempo
Responsable por el control interno	Financiero	TI	Responsable de TI
Acción		Qué Hacer?	Cómo hacer?
Creación	1992	1996	1980

En conclusión, COSO es una metodología cuyo concepto abarca a toda la organización pero desde el ámbito Financiero, en su lugar **COBIT** a más de ser una herramienta de auditoría es una herramienta de Gestión de TI, es por esta razón que se ha seleccionado a la Metodología Cobit versión 4.1 como herramienta para realizar la auditoría informática a la empresa Enap Sipetrol S.A., ya que su nivel de aplicación es muy amplio y tiene como objetivo el analizar la efectividad y eficiencia de las operaciones, confidencialidad, integridad y disponibilidad de la información y el cumplimiento con las leyes y normas. El presente proyecto se enfocará en aquellos procesos que proporcionen el mayor beneficio a la organización.

1 CAPITULO I

1.1 METODOLOGÍA COBIT 4.1

1.1.1 Marco Teórico

Control Objetives for Information and Related Technologies (COBIT), surgió en el año 1996 bajo el auspicio de dos organizaciones internacionales dedicadas al control de la gestión por medio de objetivos de control como son el Instituto para el Gobierno de las Tecnologías de la Información (ITGI) y la Asociación para la auditoría y Control de Sistemas de Información (ISAFS) debido a la necesidad de contar con una herramienta de control dedicada solamente al área de tecnología y no como parte de una auditoría de gestión empresarial y financiera, tal como era contemplado bajo las normas de COSO marco de referencia del control del negocio cuyas definiciones de efectividad y eficiencia de las operaciones así como de confiabilidad de la información y cumplimiento de leyes y regulaciones se ampliaron para todo el manejo de la información y no solo al capítulo encargado de la revisión de los sistemas informáticos que manejan la información de los sistemas contables principalmente.

1.1.2 Origen de la Metodología Cobit

Para una mejor comprensión de la génesis de la Metodología Cobit se incluye en la Figura No. 3, que permite establecer las referencias de su origen.

“Para las actividades de desarrollo y actualización de COBIT ya mencionadas, se usó una amplia base de más de 40 estándares de TI, marcos de trabajo, directrices y mejores prácticas para garantizar la integridad de COBIT en la resolución de todas las áreas de gobierno y control de TI. Debido a que COBIT se enfoca en el que se requiere para lograr una administración y control adecuados de TI, se posiciona a un alto nivel. Los estándares de TI más detallados y las mejores prácticas se encuentran a un nivel de detalle inferior describiendo cómo gestionar y controlar específicos aspectos de TI. COBIT actúa como integrador de estos diferentes materiales de guía, resumiendo los objetivos clave bajo un marco de trabajo paraguas que también

enlaza los requerimientos de gobierno y negocio. Para esta versión actualizada de COBIT 4.1, seis de los principales estándares mundiales relacionados con TI, marcos de trabajo y prácticas como las principales referencias de soporte para garantizar una cobertura, consistencia y alineación adecuada, estas son:

- COSO: Control Interno – Marco de Trabajo Integrado, 1994 Administración de Riesgos Empresarial – Marco de Trabajo Integrado, 2004
- Oficina de Comercio Gubernamental (OGC®): Biblioteca de Infraestructura de TI® (ITIL®), 1999-2004
- Organización Internacional para la Estandarización: ISO/IEC 27000
- Instituto de Ingeniería de Software (SEI®): SEI Modelo de madurez de la capacidad (CMM®), 1993 SEI Integración del modelo de madurez de la capacidad (CMMI®), 2000.
- Instituto de Gestión de Proyectos (PMI®): Guía para el Cuerpo de Conocimiento de Gestión de Proyectos (PMBOK®), 2004.
- Foro de Seguridad de Información (ISF): El estándar de buenas prácticas para la seguridad de la información, 2003.

Referencias adicionales utilizadas en el desarrollo de COBIT 4.1 incluyen:

- Objetivos de Control de TI para Sarbanes-Oxley: El Rol de TI en el Diseño e Implementación de Controles Internos Sobre Informes Financieros, 2ª Edición, Instituto de Gobierno de TI, USA, 2006 • Manual de Revisión CISA, ISACA, 2006" (IT Governance Institute, 2007).

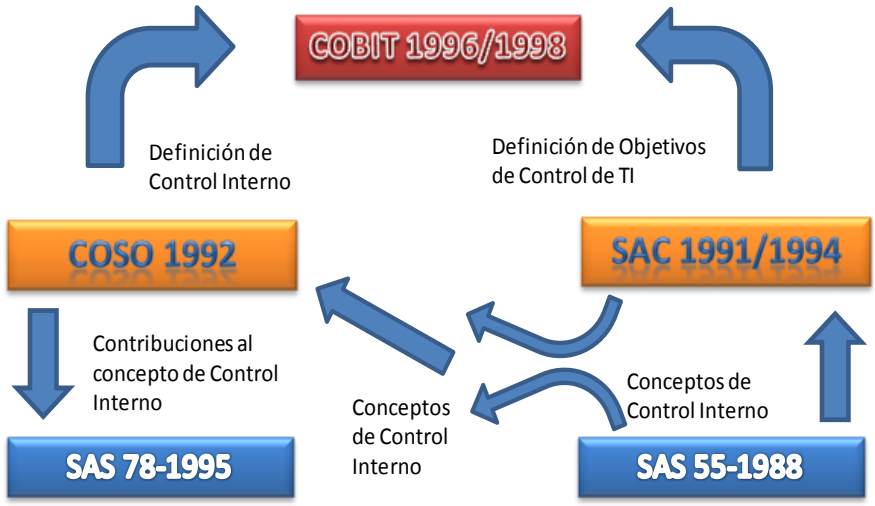


Figura 3 Integración Cobit con Estándares

Fuente: (IT Governance Institute, 2007), Apéndice IV

1.1.3 Documentos de Referencia

Cobit dispone de un conjunto de documentos que permiten su comprensión y despliegue dentro de la empresa descritos brevemente a continuación para su mejor entendimiento y tomado directamente de su publicación.

"El resumen informativo al consejo sobre el gobierno de TI, 2ª Edición—Diseñado para ayudar a los ejecutivos a entender por qué el gobierno de TI es importante, cuáles son sus intereses y cuáles son sus responsabilidades para administrarlo.

Directrices Gerenciales / Modelos de madurez—Ayudan a asignar responsabilidades, medir el desempeño, llevar a cabo benchmarks y manejar brechas en la capacidad.

Marco de Referencia Explica cómo COBIT organiza los objetivos de gobierno y las mejores prácticas de TI con base en dominios y procesos de TI, y los alinea a los requerimientos del negocio.

Objetivos de control—Brindan objetivos a la dirección basados en las mejores prácticas genéricas para todas los procesos de TI.

Guía de Implementación de Gobierno de TI: Usando COBIT y Val TI 2ª Edición. Proporciona un mapa de ruta para implementar gobierno TI utilizando los recursos COBIT y Val TI.

Prácticas de Control de COBIT: Guía para Conseguir los Objetivos de Control para el Éxito del Gobierno de TI 2ª Edición. Proporciona una guía de por qué vale la pena implementar controles y cómo implementarlos.

Guía de Aseguramiento de TI: Usando COBIT – Proporciona una guía de cómo COBIT puede utilizarse para soportar una variedad de actividades de aseguramiento junto con los pasos de prueba sugeridos para todos los procesos de TI y objetivos de control." (IT Governance Institute, 2007, pág. 7)

Como punto de partida Cobit 4.1 define su misión dentro de su marco de trabajo expresando:

"Investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de los gerentes de negocio, profesionales de TI y profesionales de aseguramiento." (IT Governance Institute, 2007, pág. 9)

Analizando la misión de Cobit 4.1, se establece que su principal interés es la orientación hacia el negocio para lo cual plantea generar un marco de control hacia la gestión y administración de TI que permanezca en constante actualización y sea utilizado como norma internacional con un enfoque hacia usuarios que puedan aprovechar de sus resultados y con sus decisiones generar un adecuado funcionamiento del área tecnológica.

Cobit 4.1, para su despliegue utiliza un enfoque por procesos de la organización, permitiendo su aplicación en cualquier tipo de empresa independiente de su tamaño o actividad. Considera 4 dominios principales los mismos que a su vez contienen objetivos de control de alto nivel y para su verificación establece de manera general actividades que debe cumplir.

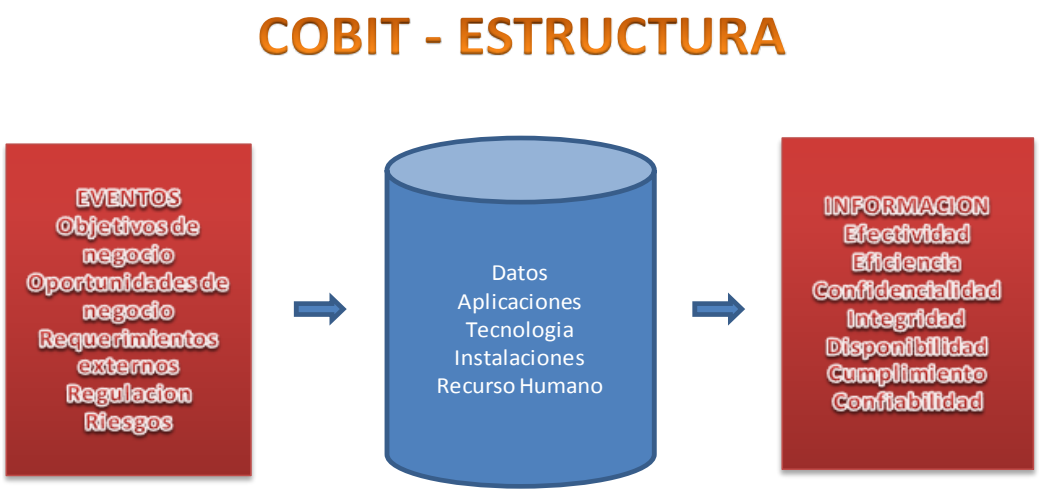


Figura 4 Estructura Cobit

Fuente: (IT Governance Institute, 2007), Pag.9, Estados Unidos

1.1.4 Dominios Cobit versión 4.1

Los dominios principales en los que Cobit establece sus objetivos de control son:

- Planear y Organizar - PO
- Adquirir e Implementar - AI
- Entregar y Dar Soporte - DS
- Monitorear y Evaluar- ME

1.1.4.1 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 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.

1.1.4.2 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.

1.1.4.3 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.

1.1.4.4 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.

1.1.5 Procesos Cobit

A lo largo de estos cuatro dominios, COBIT 4.1, ha establecido 34 procesos de TI. Mientras la mayoría de las empresas han definido las responsabilidades de planear, construir, ejecutar y monitorear para TI, y la mayoría tienen los mismos procesos clave, pocas tienen la misma estructura de procesos o le aplicaran todos los 34 procesos de COBIT. COBIT proporciona una lista completa de procesos que puede ser utilizada para verificar que se completan las actividades y responsabilidades; sin embargo, no es necesario que apliquen todas, y, aún más, se pueden combinar según sean las necesidades de cada empresa. A continuación se detallan los 34 procesos de COBIT 4.1:

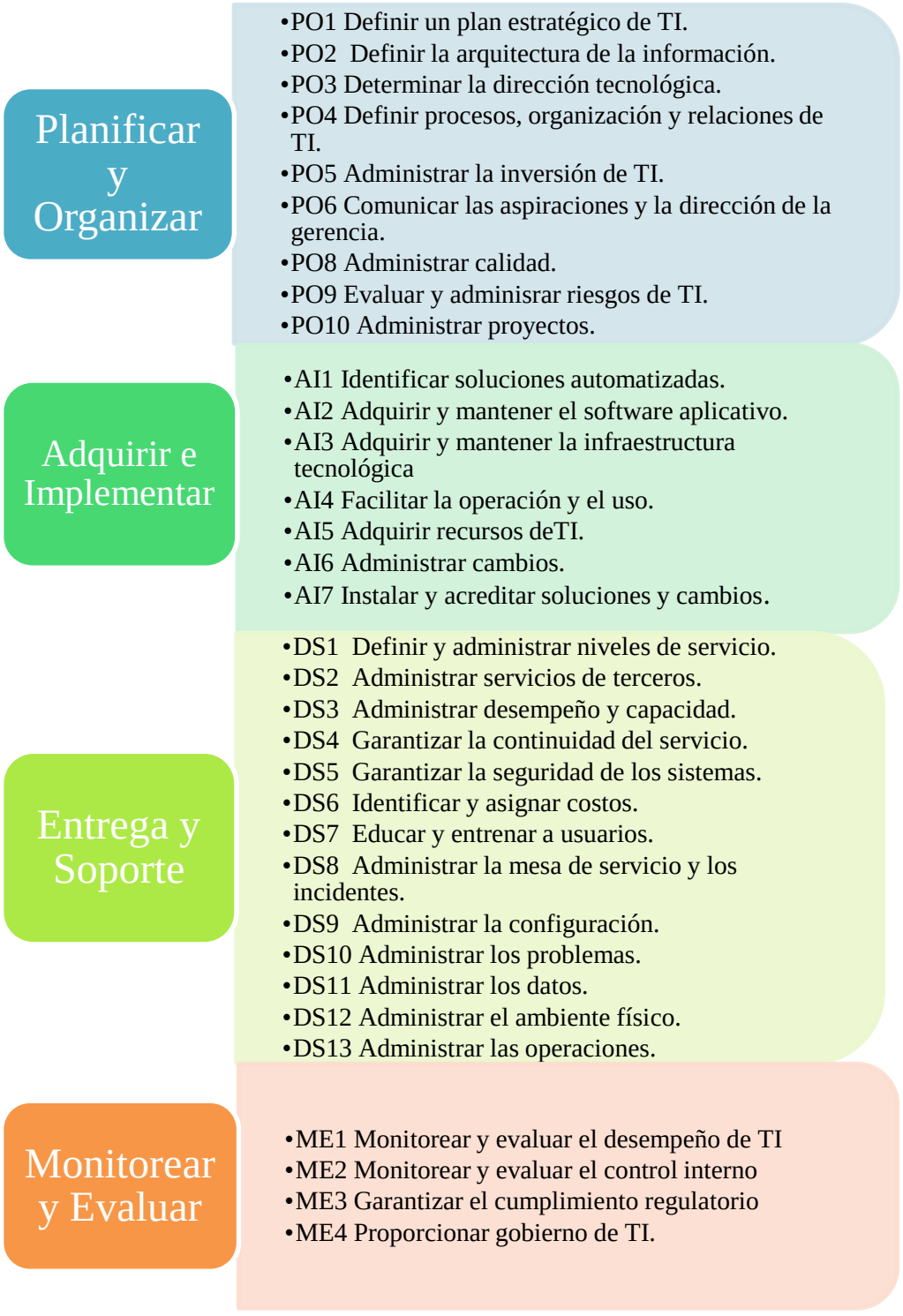


Figura 5 Procesos Cobit

1.1.6 Objetivos de Control

Los Objetivos de Control se constituyen en una declaración formal de lo que cada proceso debe contener de acuerdo a las mejores prácticas de gestión empresarial y aplicadas para la gestión de tecnología: aplicaciones, infraestructura, recursos financieros y recurso humano completando de esta manera el enfoque de un proceso y por medio de políticas, prácticas y estructuras diseñadas por la organización, permitan tener una seguridad de que los objetivos del negocio se alcancen y cualquier evento no deseado sea prevenido detectado y corregido.

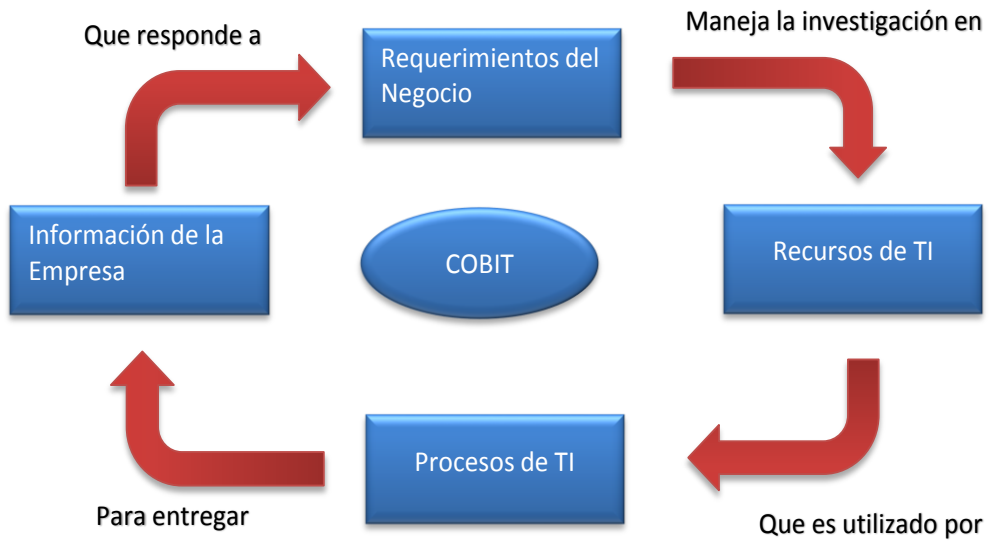


Figura 6 Principio Básico de Cobit

Fuente: (IT Governance Institute, 2007), Pag.10, Estados Unidos

Es importante tomar en cuenta lo que en el marco de trabajo aclara respecto a los objetivos de control.

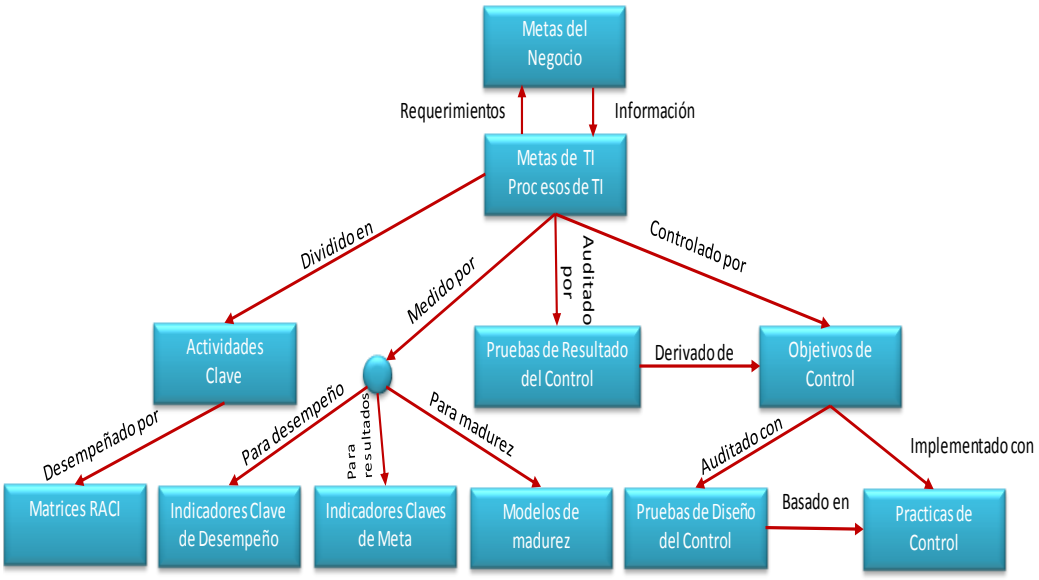


Figura 7 Interrelaciones de los componentes

Fuente: (IT Governance Institute, 2007), Pag.8, Estados Unidos

Es posible en este gráfico presentar las interrelaciones entre los componentes de Cobit en los que se puede mirar el soporte hacia el gobierno de TI, de administración, de control y de auditoría de los diferentes interesados.

Cobit como tal es considerado un marco de referencia, enfocado a los requerimientos del negocio tomando en cuenta los criterios que la información debe contemplar como son:

“Efectividad, tiene que ver con que la información sea relevante y pertinente a los procesos del negocio y se proporcione de una manera oportuna, consistente y utilizable.

Eficiencia, consiste en que la información sea generada con el óptimo (más productivo y económico) uso de recursos.

Confidencialidad, se refiere a la protección de la información sensitiva contra revelación no autorizada.

Integridad, está relacionada con la precisión y veracidad de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.

Disponibilidad, se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.

Cumplimiento, tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas externas.

Confiabilidad, se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.” (IT Governance Institute, 2007, págs. 10-11).

La alineación entre los objetivos del negocio y los objetivos de TI es de suma importancia para Cobit ya que se convierten en estrategias habilitantes hacia el cumplimiento de los resultados esperados tanto del negocio como de TI.

Para el cumplimiento de todo lo anterior es Cobit los resume en los siguientes:

“Las aplicaciones incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.

- La información son los datos en todas sus formas, de entrada, procesados y generados por los sistemas de información, en cualquier forma en que sean utilizados por el negocio.

- La infraestructura es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.

• Las personas son el recurso humano requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran.” (IT Governance Institute, 2007, pág. 12).

1.1.6.1 Controles y Mediciones

…..Todo proceso requiere de controles por lo que en Cobit “Control se define como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable que los objetivos de negocio se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos. Los objetivos de control de TI proporcionan un conjunto completo de requerimientos de alto nivel a considerar por la gerencia para un control efectivo de cada proceso de TI. Los controles se definen como:

- •Sentencias de acciones de gerencia para aumentar el valor o reducir el riesgo.
- •Consisten en políticas, procedimientos, prácticas y estructuras organizacionales.
- •Están diseñadas para proporcionar un aseguramiento razonable de que los objetivos de negocio se conseguirán y que los eventos no deseables se prevendrán, detectarán y corregirán.

La gerencia de la empresa necesita tomar decisiones relativas a estos objetivos de control seleccionando aquellos aplicables, decidiendo aquellos que deben implementarse, eligiendo cómo implementarlos (frecuencia, extensión, automatización, etc.) y aceptando el riesgo de no implementar aquellos que podrían aplicar.

La declaración anterior permite definir el alcance de los objetivos de control que sean relevantes para una organización para lo cual se debe definir los procesos que son importantes en la empresa y en los cuales sea aplicable.

Los controles efectivos reducen el riesgo, aumentan la probabilidad de la entrega de valor y aumentan la eficiencia, debido a que habrá menos errores y un enfoque de administración más consistente. Además, COBIT ofrece ejemplos ilustrativos para cada proceso, los cuales no son exhaustivos o preceptivos de:

- Entradas y salidas genéricas
- Actividades y guías sobre roles y responsabilidades en una matriz RACI
- Metas de actividades clave (las cosas más importantes a realizar)
- Métricas

1.1.7 Marco de Trabajo de Cobit

El marco de trabajo COBIT, relaciona los requerimientos de información y de gobierno a los objetivos de la función de servicios de TI. El modelo de procesos COBIT permite que las actividades de TI y los recursos que los soportan sean administrados y controlados basados en los objetivos de control de COBIT, y alineados y monitoreados usando las metas y métricas 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.

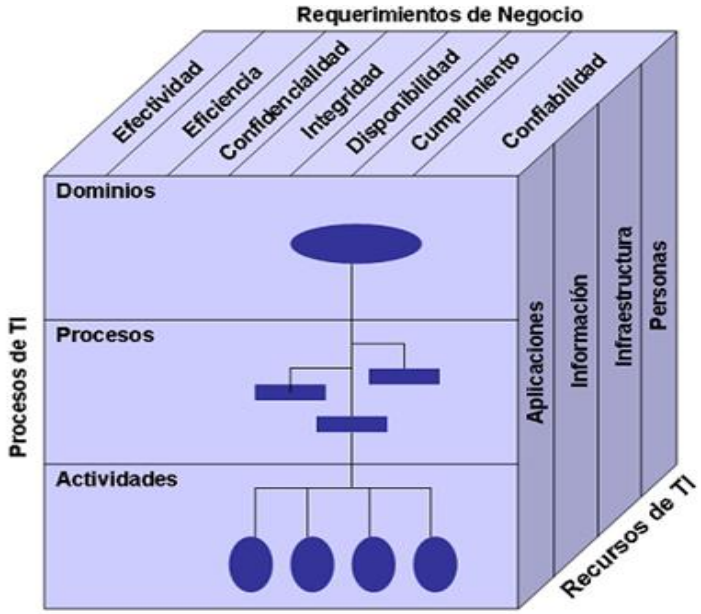


Figura 8 El Cubo de Cobit

Fuente: (IT Governance Institute, 2007), Pag.25, Estados Unidos

1.1.8 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 definió para la madurez de la capacidad del desarrollo de software. Cualquiera que sea el modelo, las escalas no deben ser demasiado granulares, ya que eso haría que el sistema fuera difícil de usar y sugeriría una precisión que no es justificable debido a que en general, el fin es identificar dónde se encuentran los problemas y cómo fijar prioridades para las mejoras. Los niveles de madurez están diseñados como perfiles de procesos de TI que una empresa reconocería como descripciones de estados posibles, actuales y futuros. No están diseñados para ser usados como un modelo limitante, donde no se puede pasar al siguiente nivel superior sin haber cumplido todas las condiciones del nivel inferior. Con los modelos de madurez de COBIT, no hay intención de medir los niveles de forma precisa o probar a certificar que un nivel se ha conseguido con exactitud.

El método gráfico que utiliza Cobit para describir el modelo de madurez alcanzado por la organización da en un solo vistazo la información relevante para definir la condición de un proceso.

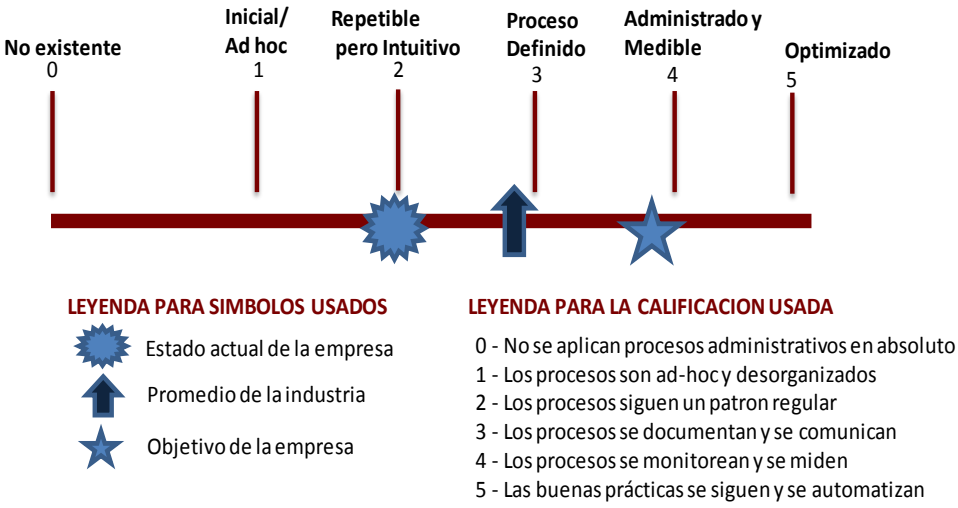


Figura 9 Representación Gráfica Modelos de Madurez

Fuente: (IT Governance Institute, 2007), Pag.18, Estados Unidos

2 CAPITULO II

ALCANCE DE LA AUDITORÍA INFORMATICA

2.1 Introducción

La información, actualmente, se ha convertido en el activo principal de las empresas, dicha información requiere de sistemas informáticos los cuales utilizan recursos tecnológicos y humanos. Estos sistemas son cada vez más complejos y requieren de una supervisión y control debido al nivel de especialización al que se ha llegado.

La Auditoría Informática en sus inicios era una extensión de la auditoría contable cuyo objetivo era encontrar errores en la administración y ejecución de los sistemas tecnológicos implementados, ahora se ha visto que este concepto ha trascendido y la auditoría informática se encarga de evaluar y verificar políticas, controles, procedimientos y seguridad en los recursos dedicados al manejo de la información, mediante la aplicación de una metodología que debe ejecutarse con formalidad y oportunidad. La Metodología Cobit era utilizada como una herramienta para la Auditoría Informática, actualmente, este concepto ha cambiado debido a que integra las mejores prácticas de Gestión de Tecnología, convirtiéndose en un Marco de Referencia para una adecuada Administración de TI[1].

El objetivo principal de este proyecto es ser una guía para la Dirección de TI, ya que el informe final, a más de describir los problemas encontrados en la Gestión de TI, presentará soluciones y recomendaciones a los mismos.

En este capítulo se desarrollarán las tareas previas al proceso de auditoría entre ellas:

- Definir los Objetivos de la auditoría.
- Describir el ámbito del negocio.

[1] (http://auditoriasistemas.com, 2013)

- Describir el ámbito de TI.
- Establecer el alcance de la auditoría informática, determinando los procesos de COBIT 4.1 a ser auditados.

2.2 Objetivos de la Auditoría Informática

Los objetivos de la presente Auditoría Informática son los siguientes:

- Evaluar la gestión y el desempeño actual del Departamento de TI
- Determinar el nivel de madurez de los procesos seleccionados en la auditoría informática.
- Determinar los riesgos de TI que afecten al negocio.
- Generar un informe final que sirva de guía para el mejoramiento del área de Tecnología.
- Agregar valor al proceso de auditoría, generando soluciones y recomendaciones a la Gerencia de TI sobre los hallazgos encontrados.

2.3 Descripción del Ámbito del Negocio

Enap Sipetrol s.a. es una empresa dedicada a la exploración y explotación de petróleo en el oriente ecuatoriano en los bloques de MDC (Mauricio Dávalos Cordero) y PBH (Paraíso, Biguno y Huachito) con una producción promedio de 15.000 barriles al día. En el año 2003, inició sus operaciones en el Ecuador como socio de Petroecuador.

Durante los 9 años de funcionamiento la empresa tuvo un crecimiento del 100% debido a la construcción de oficinas y plantas de procesamiento de crudo en el oriente ecuatoriano.

En la siguiente figura se describen los procesos involucrados con el área de TI, para ello analizaremos la cadena de valor de la empresa:

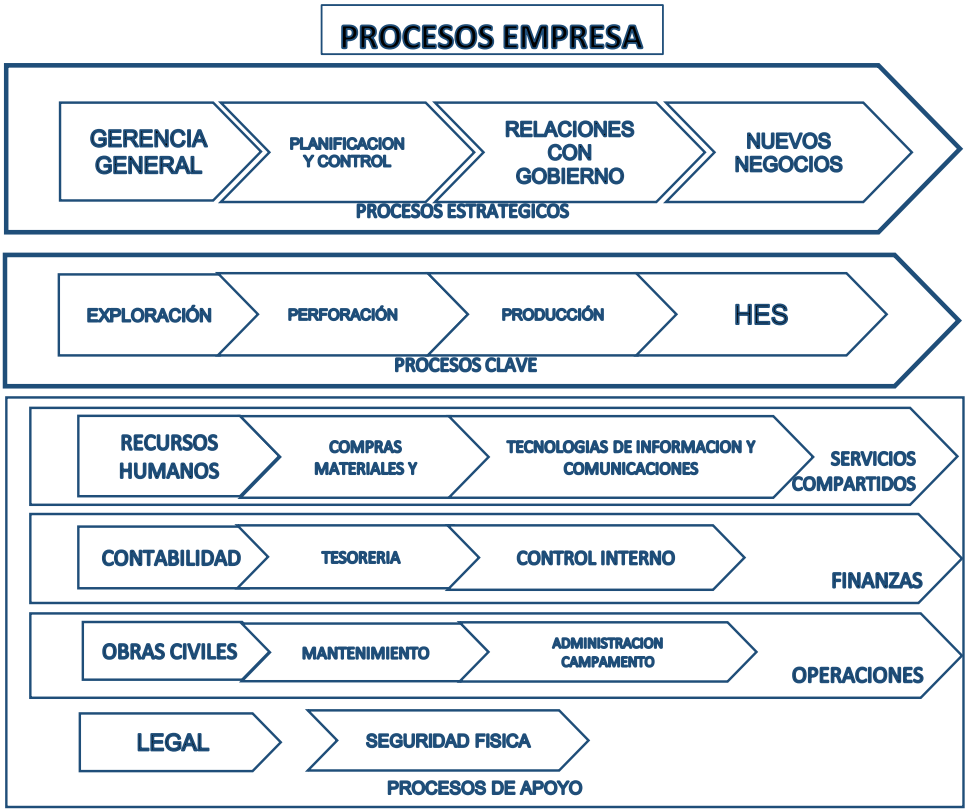


Figura 10 Diagrama de Procesos de Negocio

Todos los procesos de negocio se involucran en mayor o menor medida con el área de TI ya que utilizan sistemas de información, aplicaciones de software, o demandan de información para el desarrollo de las actividades diarias. A continuación se realiza una breve descripción de los procesos de negocio, detallando a continuación los procesos estratégicos.

Gerencia General: Es la responsable de definir las políticas generales del negocio y mantener los lineamientos de Casa Matriz (Chile).

Planificación y Control: Es el responsable del proceso de planificación y control de los planes estratégicos, presupuestarios y de inversiones.

Nuevos Negocios: Es el responsable de identificar y monitorear oportunidades de nuevos negocios.

Relaciones de Gobierno: Administra los contratos con Petroproducción a fin de evitar conflictos con el cliente, asegura el cumplimiento de las obligaciones legales y mantiene una relación saludable con las instituciones del estado.

Los procesos Claves de la Organización son:

Exploración: Este proceso está divido en varios subprocesos los cuales los más importantes son: Geología de Desarrollo, el cual se encarga del estudio y análisis de las formaciones productoras de petróleo, y Yacimientos, que se encarga del estudio de los yacimientos en producción y prever su vida útil así como los estudios y previsiones que se entregan a los entes de control.

Perforación: Este proceso se encarga de llegar a las formaciones de petróleo, que posteriormente entrega al área de Producción, en el caso de que la formación sea productora.

Producción: Este proceso está divido en varios subprocesos, de los cuales los más importantes son: Geología de Desarrollo, el cual se encarga del estudio y análisis de las formaciones productoras de petróleo, y Producción, que se encarga del levantamiento artificial del crudo para la entrega a Petroproducción.

HES: Es el responsable de que las operaciones se desarrollen dentro del cumplimento de las normas de seguridad y salud respetando el medio ambiente, las leyes y regulaciones aplicables a la industria.

Finalmente se describen los procesos de apoyo en la organización:

Finanzas: Es el responsable de la coordinación del proceso de planificación financiera para proyectar el flujo de caja y garantizar los fondos necesarios para la operación.

Servicios Compartidos: Este proceso está compuesto por: Materiales & Logística, Recursos Humanos y TI. Se encarga de proveer servicios a todas las áreas de la empresa en los ámbitos correspondientes.

Operaciones: Está compuesto por Obras Civiles, Mantenimiento Industrial y Administración de campamento, y es el responsable de proveer de personal técnico especializado para las operaciones en campo.

Legal: Es el responsable de velar por el cumplimiento de las leyes y resoluciones que afectan el negocio.

Seguridad Física: es el responsable de velar por la seguridad del personal y de las instalaciones en los sitios en los opera la compañía.

2.4 Descripción del Ámbito de TI

Debido al acelerado crecimiento de la compañía, se ha visto la necesidad de implementar nuevas tecnologías tanto en hardware, software y servicios asociados para satisfacer los requerimientos del negocio acorde a los estándares de la industria en cuanto a Tecnologías de la Información.

Dada la importancia del negocio, la organización tiene como política mantenerse a la vanguardia en cuanto a tecnología se refiere, es por ello que el hardware y software se renueva cada tres años y se dispone de hardware redundante en equipos críticos, así como de enlaces de respaldo en comunicaciones.

2.4.1 Principales Procesos de TI

Los procesos principales del área de tecnología son:

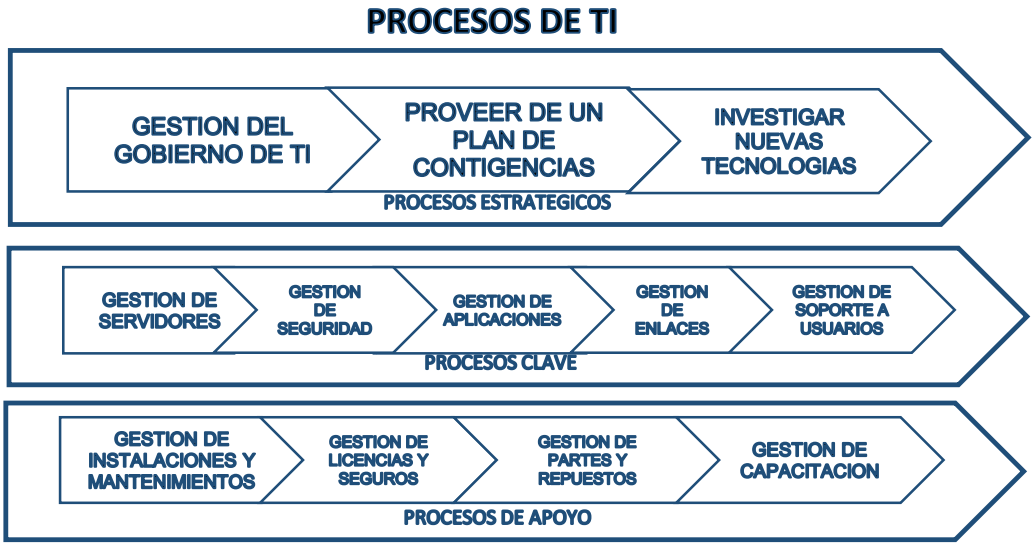


Figura 11 Procesos del Área de Tecnología de Información

Los Procesos Estratégicos son aquellos que le dan dirección al área de tecnología, y que al ser auditados reflejarán la relación entre la estrategia del TI versus la estrategia del negocio.

Los Procesos Clave son aquellos que permiten el adecuado funcionamiento del área de TI y que repercuten directamente a toda la organización.

Los Procesos de Apoyo se los realiza de acuerdo a la demanda de las diferentes áreas, sin embargo, su buen funcionamiento es imprescindible en la ejecución de los procesos anteriores.

Dada la importancia que tiene cada uno de los procesos en el normal funcionamiento del área de tecnología, se ve la necesidad de auditarlos para conocer el estado actual de los mismos.

2.4.2 Infraestructura de la Organización

A continuación se describen las plataformas y los sistemas de información que están apoyando el proceso del negocio, así como la interconectividad con otras plataformas o sistemas, por medio del siguiente gráfico.

TECNOLOGIA ACTUAL

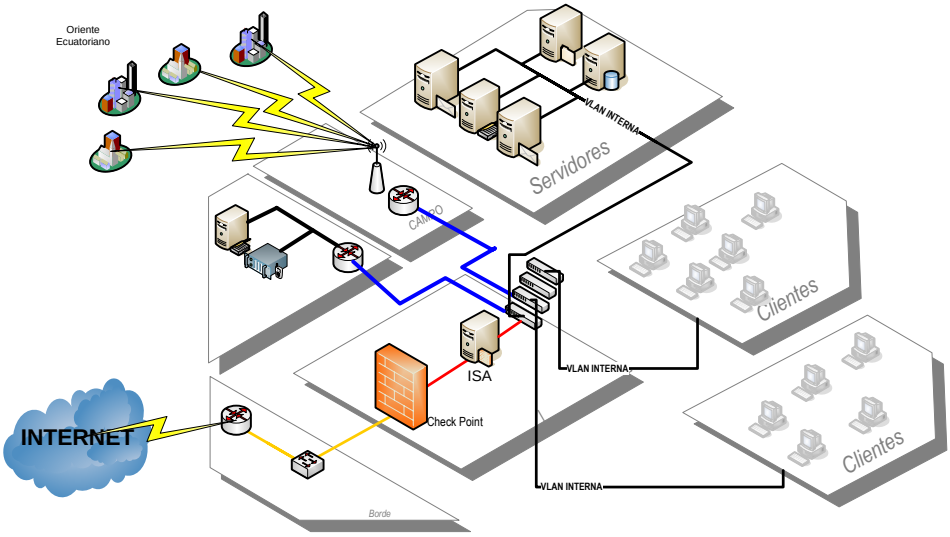


Figura 12 Infraestructura Tecnológica

La Tecnología actual provee un servicio de voz y datos para 120 usuarios, cuenta con enlaces de comunicaciones de fibra óptica y de microonda hacia las instalaciones de campo y una red WAN hacia casa matriz con servicios de datos hacia Argentina y Egipto desde donde se ejecutan aplicaciones propias del negocio.

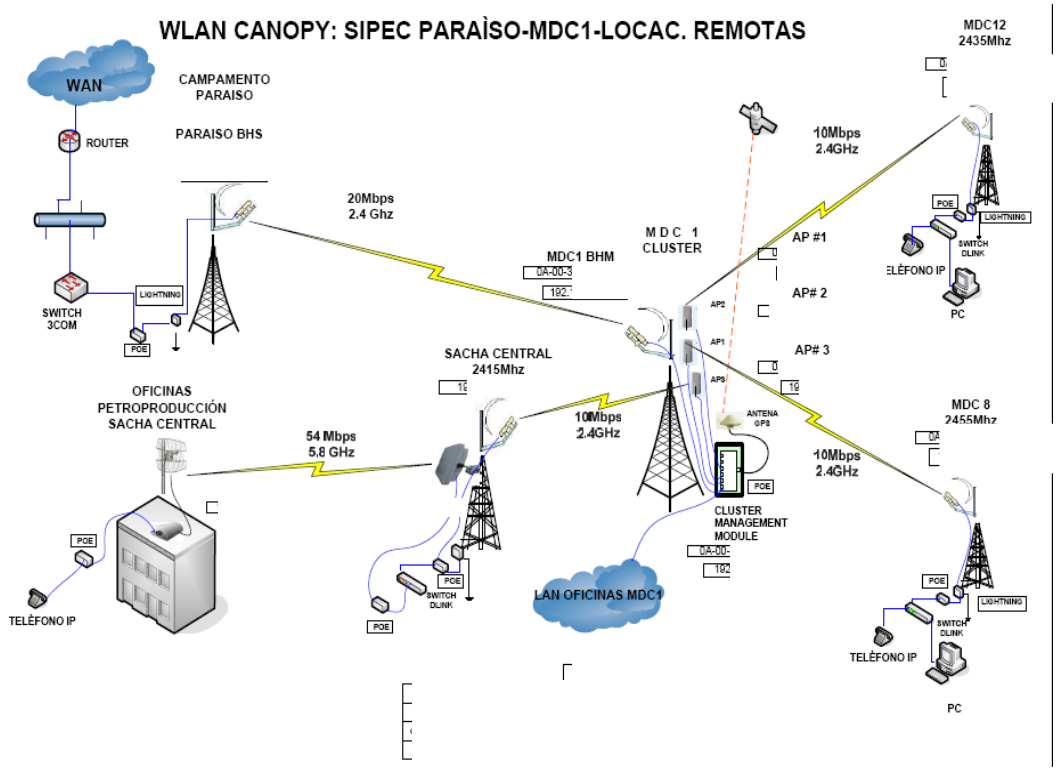


Figura 13 Sistemas de Voz y Datos

2.4.2.1 Detalle del Hardware

A continuación, se describe los elementos de tecnología con los que cuenta la compañía tanto en hardware y en software con la descripción de las aplicaciones propias del negocio:

Tabla 2

Detalle de hardware

Hardware	Software	Cantidad
Servidores	Windows Server 2003 / Exchange 2005 / SQL 2005 / ISA 2006/IIS/Sharepoint	10
Desktop	Windows XP Professional	50
Laptop	Windows XP Professional	70
Impresoras		10
Routers		2
Switches		10
Centrales de Voz/IP		2
Firewalls		2
Enlaces Inalámbricos		6

2.4.2.2 Detalle del Software

Tabla 3

Detalle de Software

AREA	APLICACIÓN	DESCRIPCION
Producción	Generados de Reportes para la DNH	Aplicación web que registra producción diaria de petróleo por pozo
	DIMS	Aplicación que registra eventos de perforación de cada pozo
	Zaphir/Topaze	Aplicación de comportamiento estadístico de producción de pozos
Finanzas/Compras	Maximise/SAP	Sistemas ERP´s Contable-Financiero
Legal	Lexis	Recopilación de leyes y registro oficial del gobierno
Exploración	Geografix	Sistema de interprestación de registros geológicos
	Petrel	Herramienta de análisis geológico
Nuevos Negocios	Global Economic Model	Aplicación de análisis de viabilidad de proyecto

2.4.2.3 Roles y Responsabilidades

A continuación se describe los roles y responsabilidades de TI, entre las principales funciones del área de sistemas se puede mencionar:

Tabla 4

Roles y Responsabilidades de TI

ROL	RESPONSABILIDADES
Gerente de Sistemas	-Gobernabilidad de TI -Análisis de implementación de nuevas tecnologías -Capacitación
Administrador de Seguridades	-Generación de Planes de Contingencia -implementación de Políticas de Seguridad
Administrador de Sistemas	-Administración de Información -Gestión de licencias -Gestión de versiones
Administrador de Redes	-Administración de redes -Administración de enlaces
Soporte a Usuarios	-Soporte a requerimientos de usuarios

Para que el negocio funcione adecuadamente se necesita de la siguiente información:

- Información Sísmica para determinar las nuevas reservas de los yacimientos.
- Bitácora de cada pozo perforado con el ciclo de vida.
- Reporte de producción diario.
- Información procesada en el sistema de monitoreo y control de producción.
- Información de maquinaria y equipos
- Información para el sistema administrativo – contable
- Correo electrónico e internet.

2.5 Selección de Procesos a Auditar

2.5.1 Criterios de Selección

El departamento de TI es el proveedor de servicios y recursos que permite cumplir las metas del negocio, por lo tanto, si se pretende que TI proporcione servicios de forma exitosa para dar soporte a la estrategia de la empresa, debe existir claridad y conocimiento de los requerimientos del negocio por parte de la Gerencia, cómo y qué debe entregar.

Es por ello, que el presente proyecto busca realizar una auditoría que evidencie hasta qué punto el departamento de tecnología puede dar soporte a las metas del negocio.

En la siguiente figura se indica como la estrategia de la empresa se debe traducir en objetivos del negocio para luego transformarse en metas del negocio para TI. Estas metas a su vez, deben conducir a una clara definición de los propios objetivos de TI, y luego éstas a su vez definir los recursos y capacidades de TI requeridos para ejecutar, de forma exitosa la parte que le corresponde a TI para cumplir con la estrategia empresarial.

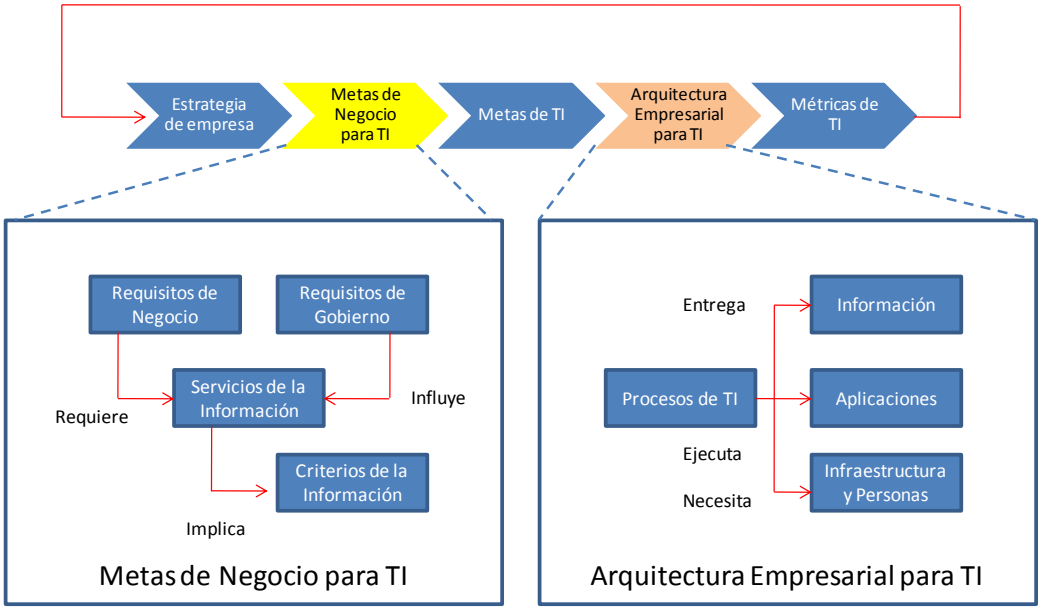


Figura 14 Definir las Metas de TI

Fuente: (IT Governance Institute, 2007), Pag.11, Estados Unidos

Para que la Dirección entienda las metas de TI, todos estos objetivos y sus métricas deben expresarse en términos del negocio y esto, combinado con una efectiva jerarquía de objetivos, se asegurará que la Dirección pueda confirmar que TI puede dar soporte a las metas del negocio.

Las siguientes tablas presentan los enlaces entre metas y procesos, proporciona una visión global de cómo las metas del negocio se relacionan con las metas de TI, los procesos de TI y los criterios de la información. Para poder elaborar las tablas resumen, se ha determinado una metodología para enlazar las metas del negocio vs las metas de TI:

- Evidenciar las metas del negocio, empleando para ello el BSC (Balanced Scorecard - Cuadro de Mando Integral) de la empresa.
- Recopilar los Objetivos de TI existentes.
- Evidenciar las Metas de TI.
- Con las metas de TI realizar el mapeo respectivo hacia los procesos de Cobit 4.1, determinando de esta manera cuáles son los procesos que efectivamente intervienen en la compañía.

2.5.2 Análisis de las Metas del Negocio

Para poder analizar las metas del negocio se ha empleado el BSC de la compañía que en sus cuatro perspectivas (Financiera, Cliente, Procesos Internos, Desarrollo de Capacidades) despliega los objetivos del negocio y sirve también como un mapa estratégico a ser cumplido por todas las áreas de la empresa.

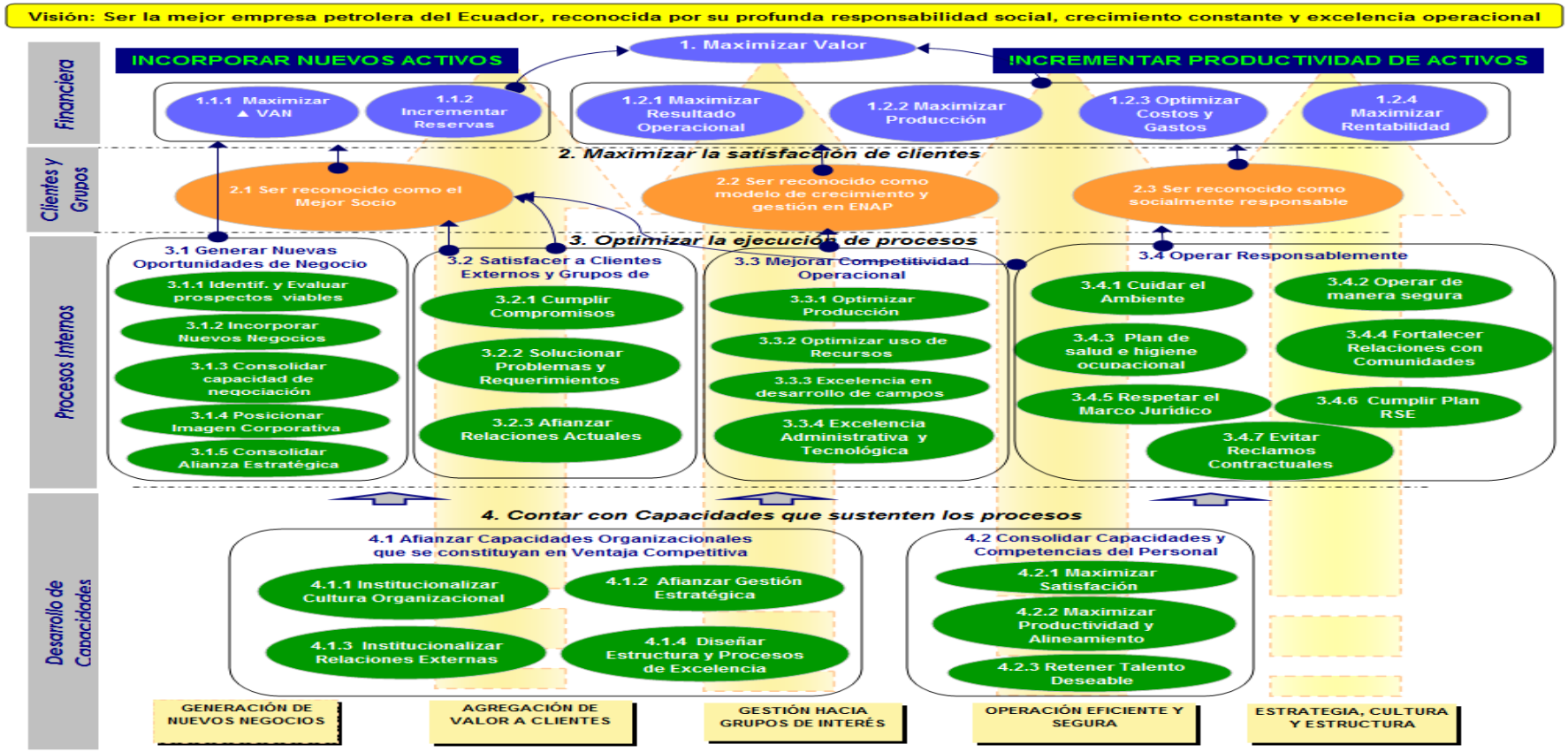


Figura 15 BSC ENAP-SIPETROL

2.5.3 Objetivos y Metas de TI

El departamento de tecnología dispone de 1 objetivo estratégico definido en el BSC, este es:

3.3.4 Excelencia Administrativa y Tecnológica

Para cumplir con este objetivo, se ha implementado un plan de trabajo anual en donde se establecen las tareas y los tiempos para determinar el cumplimiento del subproceso:

3.3.4.5 Disponer de Sistemas Adecuados

Lo anterior se describe a detalle en el Anexo 2.

Una vez establecidos los objetivos, el área de TI estableció las siguientes metas que permitan cumplir con los objetivos planteados, la siguiente figura despliega dicha información:

Tabla 5
Relación entre Objetivos y Metas TI

No.	OBJETIVOS DE TI	No.	METAS DE TI
1	Implementar aplicaciones bajo estándares de desarrollo de software	1	Contratar empresas certificadas en desarrollo de software
		2	Capacitar continuamente al personal de TI en nuevas herramientas de desarrollo
2	Mantener una plataforma actualizada y estandarizada	3	Reemplazar equipos de computación cada 3 años
		4	Adquirir equipos de una sola marca comercial
		5	Estandarizar software de equipos y servidores
		6	Adquirir un acuerdo de licenciamiento por volumen
		7	Utilizar los servicios de empresas certificadas
3	Cumplir con el presupuesto	8	Diseñar presupuesto anual de TI
		9	Implementar políticas de ahorro de recursos
		10	Gestionar alianzas a largo plazo con proveedores de tecnología
4	Analizar e Implementar nuevas tecnologías	11	Investigar nuevas tecnologías
		12	Determinar nuevos requerimientos del negocio
		13	Realizar estudios de factibilidad de implementación de nuevas tecnologías
5	Dar soporte adecuado a requerimientos del usuario	14	Mantener un registro de incidentes
		15	Generar una base de conocimiento
		16	Tener personal de TI capacitado
		17	Capacitar al usuario en el uso de herramientas
6	Asegurar la continuidad del negocio en caso de contingencia	18	Tener un plan de continuidad de negocio
		19	Realizar pruebas periódicas del plan de continuidad de negocio en TI
		20	Mantener actualizado el plan de continuidad de negocio
7	Asegurar la disponibilidad de los servicios de tecnología	21	Monitorear aplicaciones y generar alertas en caso de fallo de los servicios
		22	Realizar mantenimientos preventivos de equipos
		23	Realizar mantenimiento de aplicaciones
		24	Realizar upgrades a los sistemas
		25	Mantener un seguro sobre equipos de computación
		26	Cumplir con la legislación vigente
8	Mantener la seguridad de la información	27	Adquirir sistemas de protección
		28	Disponer de un sistema de control de accesos a la información
		29	Disponer de procedimientos de respaldos y recuperación de información
9	Gestionar Gobierno de TI	30	Crear políticas y procedimientos de TI
		31	Crear un plan estratégico de TI
		32	Analizar riesgos de TI
		33	Evaluar el desempeño de TI

A continuación se brinda una visión global de cómo se seleccionaron los procesos COBIT a ser auditados. Se utilizaron 3 tablas que permitieron establecer las relaciones entre metas del negocio, metas de TI y Procesos COBIT.

2.5.4 Relación entre las Metas del Negocio y Metas de TI

La primera tabla muestra las equivalencias de las metas del negocio, de acuerdo al Balanced Scorecard, con las metas de TI y con los criterios de información. Esto ayuda a mostrar, para una meta genérica de negocios determinada, las metas de TI que por lo general dan soporte a esta meta, y los criterios de información de COBIT que se relacionan con la meta del negocio.

Tabla 6
Relación entre Metas del Negocio y TI

																		CRITERIOS DE INFORMACION						
BALANCED SCORECARD	**No.**	**METAS DEL NEGOCIO - ENAP SIPEC**	**METAS TI - ENAP SIPEC**															*Efectividad*	*Eficiencia*	*Confidencialidad*	*Integridad*	*Disponibilidad*	*Cumplimiento*	*Confiabilidad*
PERSPECTIVA FINANCIERA	1	Maximizar VAN	9																√					
	2	Incrementar Reservas	12																	√	√	√		√
	3	Maximizar resultado Operacional	8	9	10	12												√	√					
	4	Maximizar Produccion	12															√	√					
	5	Optimizar Costos y Gastos	8	9	10	12	22	23											√					
	6	Maximizar rentabilidad de activos	3	6	22	26												√	√					
PERSPECTIVA DEL CLIENTE	7	Ser reconocido como el mejor socio																						
	8	Ser reconocido como modelo de crecimiento y gestión en ENAP	26	30	31													√	√					
	9	Ser reconocido como socialmente responsable	26															√						
PERSPECTIVA INTERNA	10	Generar nuevas oportunidades de negocio																						
	11	Satisfacer a clientes	12	14	15	17	23											√	√	√		√	√	√
	12	Mejorar competitividad Operacional	1	2	3	4	5	6	11	12	13	18	21	23	26	27	28	30	√	√				√	
	13	Operar responsablemente	6	7	12	18	19	20	21	22	23	24	25	26	27	28	29			√	√	√	√	√	√
PERSPECTIVA DE APRENDIZAJE Y CRECIMIENTO	14	Afianzar Capacidades Organizacionales que se constituyan en ventaja competitiva	3	4	6	11	12	14	16	17	31								√	√					
	15	Consolidar Capacidades y Competencias del personal	2	12	14	15	16	17											√	√					

Nota Fuente: (IT Governance Institute, 2007), Apéndice I

2.5.5 Relación entre Metas de TI y Procesos Cobit

La segunda tabla muestra las equivalencias de las metas de TI con los procesos de TI de COBIT, generando la siguiente matriz:

Tabla 7

Relación Metas de TI y Procesos Cobit 4.1

No	METAS DE TI - ENAP SIPEC	PROCESOS DE TI - COBIT							
1	Contratar empresas certificadas para el desarrollo de nuevas aplicaciones	P08	PO10	AI2	AI5	DS2			
2	Capacitar continuamente al personal de TI en nuevas herramientas de desarrollo	DS7							
3	Reemplazar equipos de computación cada 3 años	PO2	PO5	AI3	AI5				
4	Adquirir equipos de una sola marca comercial	PO5	AI3	AI5					
5	Estandarizar software de equipos y servidores	PO2	PO3	PO5	AI3	AI5			
6	Adquirir un acuerdo de licenciamiento por volumen	PO3	PO5	AI2	AI5	DS5	ME3		
7	Utilizar los servicios de empresas certificadas	DS2							
8	Diseñar presupuesto anual de TI	PO1	PO5						
9	Implementar políticas de ahorro de recursos	PO5							
10	Gestionar alianzas a largo plazo con proveedores de tecnología	PO1	DS2						
11	Investigar nuevas tecnologías	PO3							
12	Determinar nuevos requerimientos del negocio	PO1	PO3	PO5	PO7	PO9			
13	Realizar estudios de factibilidad de implementación de nuevas tecnologías	PO10	AI1						
14	Mantener un registro de incidentes	PO8	DS10	DS3	ME1				
15	Generar una base de conocimiento	PO8	DS10	DS3	ME1				
16	Tener personal de TI capacitado	PO7	AI5	DS2					
17	Capacitar al usuario en el uso de herramientas	AI5	DS2	DS7					
18	Tener un plan de continuidad de negocio	PO1	PO5	PO9	AI5	DS2	DS4	DS5	
19	Realizar pruebas periódicas del plan de continuidad de negocio en TI	PO1	PO5	PO9	AI5	DS2	DS4	DS5	ME1
20	Mantener actualizado el plan de continuidad de negocio	ME2							
21	Monitorear aplicaciones y generar alertas en caso de fallo de los servicios	DS4	ME1						
22	Realizar mantenimientos preventivos de equipos	PO5	AI5	DS2	DS4				
23	Realizar mantenimiento de aplicaciones	PO5	AI5	AI6	DS2	DS4			
24	Realizar upgrades a los sistemas	AI7	DS5						
25	Mantener un seguro sobre equipos de computación	PO5	AI5	DS2	DS4				
26	Cumplir con la legislación vigente	ME3							
27	Adquirir sistemas de protección	AI5	DS5						
28	Disponer de un sistema de control de accesos a la información	DS5	DS11						
29	Disponer de procedimientos de respaldos y recuperación de información	PO9	DS4	DS11	ME3				
30	Crear políticas y procedimientos de TI	PO1	PO4	DS1	DS4	DS5	DS13	ME4	
31	Crear un plan estratégico de TI	PO1	ME4						
32	Analizar riesgos de TI	PO9							
33	Evaluación del desempeño de TI	ME1							

2.5.6 Correlación entre Procesos Cobit vs Metas de TI

La tercera tabla proporciona un mapeo inverso que muestra para cada proceso de Cobit las metas de TI que son soportadas lo que determina el peso del proceso en la gestión de TI, se realizó una sumatoria de las metas por proceso determinando los 11 procesos de COBIT a ser auditados en el rango de 4 a 10.

Tabla 8

Matriz de Procesos Cobit 4.1 a Metas de TI de Enap-Sipetrol

	METAS TI - ENAP SIPETROL																																
	Contratar empresas certificadas para el desarrollo de nuevas aplicaciones	Capacitar continuamente al personal de TI en nuevas herramientas de desarrollo	Reemplazar equipos de computación cada 3 años	Adquirir equipos de una sola marca comercial	Estandarizar software de equipos y servidores	Adquirir un acuerdo de licenciamiento por volumen	Utilizar los servicios de empresas certificadas	Diseñar presupuesto anual de TI	Implementar políticas de ahorro de recursos	Gestionar alianzas a largo plazo con proveedores de tecnología	Investigar nuevas tecnologías	Determinar nuevos requerimientos del negocio	Realizar estudios de factibilidad de implementación de nuevas tecnologías	Mantener un registro de incidentes	Generar una base de conocimiento	Tener personal de TI capacitado	Capacitar al usuario en el uso de herramientas	Tener un plan de continuidad de negocio	Realizar pruebas periódicas del plan de continuidad de negocio en TI	Mantener actualizado el plan de continuidad de negocio	Monitorear aplicaciones y generar alertas en caso de fallo de los servicios	Realizar mantenimientos preventivos de equipos	Realizar mantenimiento de aplicaciones	Realizar upgrades a los sistemas	Mantener un seguro sobre equipos de computación	Cumplir con la legislación vigente	Adquirir sistemas de protección	Disponer de un sistema de control de accesos a la información	Disponer de procedimientos de respaldos y recuperación de infomación	Crear políticas y procedimientos de TI	Crear un plan estratégico de TI	Analizar riesgos de TI	Evaluación del desempeño de TI	SELECCIÓN DE PROCESOS COBIT
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	
PO1								1		1		1						1	1											1	1			7
PO2			1		1																													2
PO3					1						1	1																						3
PO4	1									1																				1	1			4
PO5								1	1																1									3
PO7												1				1																		2
PO8	1													1	1																			3
PO9												1						1	1										1			1		5
PO10	1												1																					2
AI1													1																					1
AI2	1					1																												2
AI3			1	1	1																													3
AI5	1		1	1	1	1										1	1	1	1			1	1		1		1							13
AI6																							1											1
AI7																								1										1
DS1																														1				1
DS2	1						1			1						1	1	1	1			1	1		1									10
DS3														1	1																			2
DS4																		1	1		1	1	1		1				1	1				8
DS5						1												1	1					1			1	1		1				7
DS7		1															1																	2
DS10														1	1																			2
DS11																												1	1					2
DS13	1	1			1																	1	1	1			1	1	1	1				10
ME1														1	1				1		1												1	5
ME2																				1														1
ME3						1																				1			1	1				4
ME4																														1	1	1	1	4

2.5.7 Resumen de Dominios y Procesos Cobit 4.1 a ser Auditados

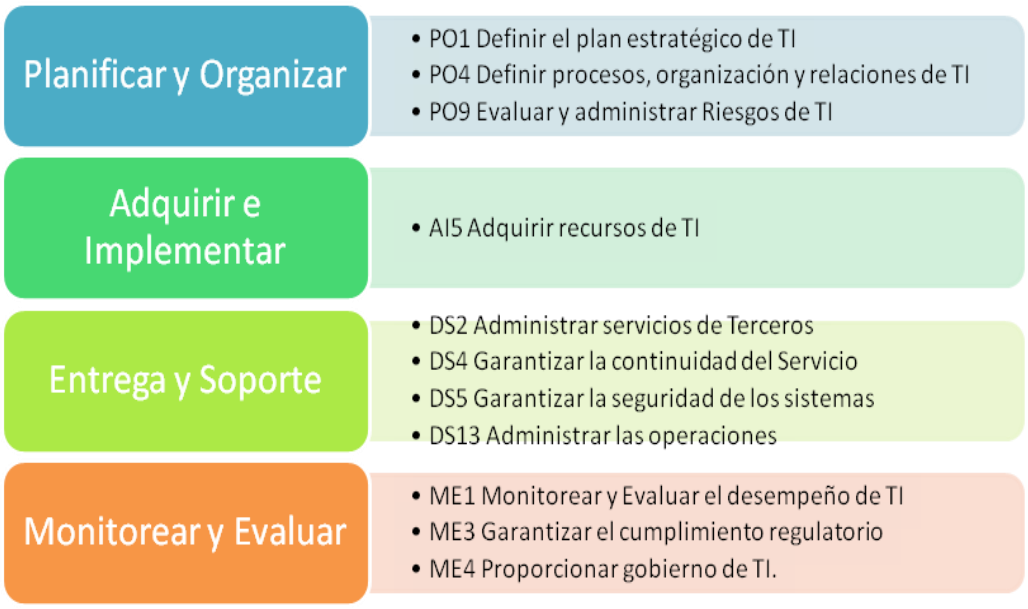


Figura 16 Resumen Procesos Cobit 4.1 a ser auditados

3 CAPITULO III

PLANIFICACION DE LA AUDITORIA

3.1 Introducción

En el capítulo anterior, "ALCANCE DE LA AUDITORIA", se definieron los procesos Cobit 4.1 a ser auditados en base a un análisis del Balanced Scorecard de la empresa ENAP-SIPETROL, los Objetivos y Metas de TI, y los dominios y procesos de Cobit 4.1, utilizando para ello matrices que permitieron visualizar de mejor manera la relación entre cada uno de ellos.

El objetivo del presente capítulo es planificar el proceso de auditoría[2] , para ello el equipo auditor preparará un plan que facilitará el establecimiento de los horarios y la coordinación de las actividades de auditoría. A continuación se describen los pasos a seguir para el desarrollo del plan de auditoría:

3.2 Preparación del Plan de Auditoría

El plan de auditoría incluirá los siguientes puntos:

- Los objetivos de la auditoría.
- Los criterios de auditoría y los documentos de referencia.
- El alcance de la auditoría, incluyendo la identificación de las unidades de la organización, unidades funcionales y los procesos que van a auditarse.
- Las fechas y lugares donde se va a realizar las actividades de la auditoría
- La hora y la duración estimadas de las actividades de la auditoría.
- Las funciones y responsabilidades de los miembros del equipo auditor
- La asignación de los recursos necesarios a las áreas críticas de la auditoría.
- Asuntos relacionados con la confidencialidad.

[2] (Mario G. Piattini, 2001)
(http://www.uaeh.edu.mx)
(http://fcasua.contad.unam.mx)

3.3 Asignación de las Tareas al Equipo Auditor

El líder del equipo, consultando con el equipo auditor, deberá asignar a cada miembro la responsabilidad para auditar procesos, funciones, lugares, áreas o actividades específicas. Se pueden realizar cambios en la asignación de tareas a medida que la auditoría se va llevando a cabo para asegurarse de que se cumplen los objetivos de la auditoría.

3.4 Preparación de los Documentos de Trabajo

Los miembros del equipo auditor deberán revisar la información pertinente a las tareas asignadas y preparar los documentos de trabajo que sean necesarios como referencia y registro del desarrollo de la auditoría. Tales documentos de trabajo pueden incluir:

- Listas de verificación y planes de muestreo de auditoría.
- Formularios para registrar información, tal como evidencia de apoyo, hallazgos de auditoría y registros de las reuniones.
- Aquellos documentos que contengan información confidencial o de propiedad privada deberán ser guardados con la seguridad apropiada en todo momento por los miembros del equipo auditor.

3.5 Plan de Auditoría

3.5.1 Objetivo de la Auditoría

- Establecer la situación actual del departamento de TI de Enap-Sipetrol S.A., en cuanto al cumplimiento de buenas prácticas de TI utilizando como marco de referencia Cobit 4.1.
- Proponer recomendaciones relativas a mejoras, tomando como base los resultados de la auditoría.
- Plantear nuevos proyectos que permitan mejorar la gestión del departamento de TI.

3.5.2 Alcance

El plan de auditoría se aplicará a todos los procesos seleccionados en el capítulo II de este proyecto.

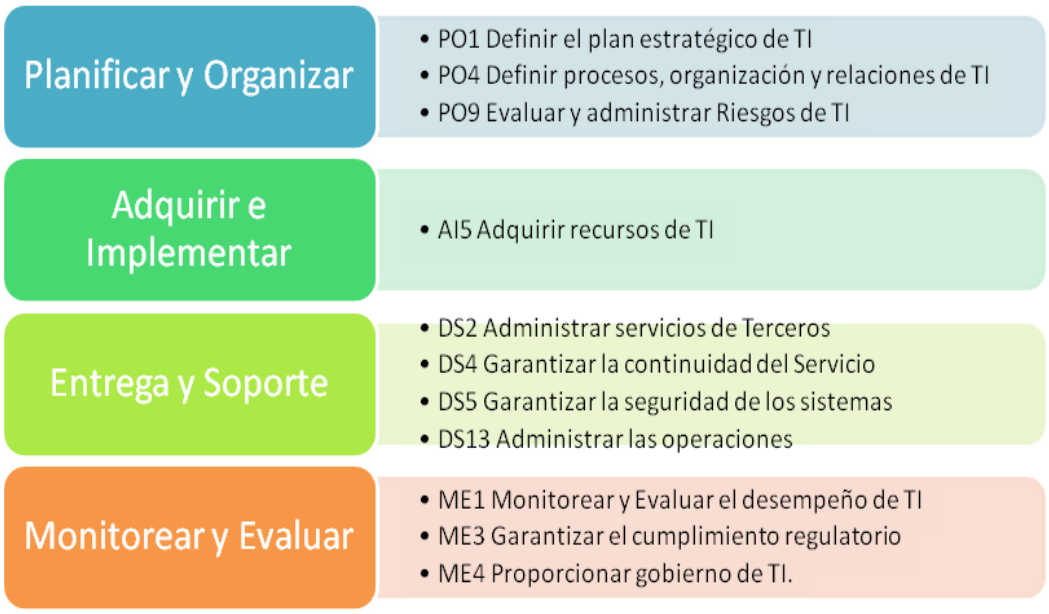


Figura 17 Resumen Procesos Cobit 4.1 a ser auditados

3.5.3 Criterios de Auditoría

El cumplimiento de buenas prácticas para el Gobierno de TI será verificado según los principios establecidos en el marco de referencia Cobit v4.1.

3.5.4 Equipo Auditor

Los miembros del equipo auditor son: Antonio Chuquimarca (Auditor líder) y Nelly Pérez (Auditor 2).

3.5.5 Responsabilidades:

Tabla 9

Responsabilidades del Equipo Auditor

AUDITOR	PROCESOS	
Nelly Perez	PO9	Evaluar y Administrar los Riesgos de TI
	DS4	Garantizar la continuidad del servicio
	DS13	Administracion de Operaciones
	ME1	Monitorear u Evaluar el Desempeño de TI
	ME3	Garantizar el cumplimiento con requerimientos externos
Antonio Chuquimarca	PO1	Definir un Plan Estratégico de TI
	PO4	Definir los Procesos, Organización y Relaciones de TI
	AI5	Adquirir Recursos de TI
	DS2	Administrar los servicios de terceros
	DS5	Garantizar la seguridad de los sistemas
	ME4	Proporcionar Gobierno de TI

3.5.6 Áreas a ser Auditadas

- Gerencia General
- Departamento de Sistemas
- Departamento de Recursos Humanos
- Departamento Legal
- Departamento de Planificación
- Departamento de Compras, Materiales y Logística

3.5.7 Proceso de Auditoría

La metodología a seguir se detalla a continuación:

- Realizar un estudio detallado de los procesos seleccionados en el capítulo "Alcance de la Auditoría", en donde se obtendrá un cuadro resumen que contiene: Procesos, Objetivos de Control y Factores de Riesgo.
- Definir la información que se va a solicitar en el proceso de Auditoría Informática, para ello se determinará los Elementos Auditables en base a los factores de riesgo de los procesos Cobit 4.1 para cada Objetivo de Control y se los resumirá en las hojas de trabajo de auditoría[3].

[3] (Institute, 2001)

- Establecer el cronograma de auditoría el cual permitirá dimensionar el tiempo utilizado en este proceso.
- Presentar un resumen de los hallazgos encontrados para cada uno de los procesos auditados y en base a ello determinar el nivel de madurez de los mismos.
- Elaborar el informe final de auditoría detallando las observaciones encontradas en la auditoría, el riesgo asociado a la observación, se emitirán las recomendaciones necesarias para mitigar el riesgo y se sugerirán nuevos proyectos en los casos que aplique, para mejorar la gestión de TI.

3.5.8 Cronograma de Auditoría

La Auditoría Informática a la empresa Enap – Sipetrol S.A. será desarrollada según el cronograma descrito a continuación:

Tabla 10

Cronograma de Auditoría

			SEMANAS										
AUDITOR		PROCESOS	20-25 Ago	27-31 Ago	03-08 Sep	10-15 Sep	17-22-Sep	24-29 Sep	01-06 Oct	08-13 Oct	15-20 Oct	22-27 Oct	29-31 Oct
Nelly Perez	PO9	Evaluar y Administrar los Riesgos de TI											
	DS4	Garantizar la continuidad del servicio											
	DS13	Administracion de Operaciones											
	ME1	Monitorear y Evaluar el Desempeño de TI											
	ME3	Garantizar el cumplimiento con requerimientos externos											
Antonio Chuquimarca	PO1	Definir un Plan Estratégico de TI											
	PO4	Definir los Procesos, Organización y Relaciones de TI											
	AI5	Adquirir Recursos de TI											
	DS2	Administrar los servicios de terceros											
	DS5	Garantizar la seguridad de los sistemas											
	ME4	Proporcionar Gobierno de TI											
INFORME FINAL DE AUDITORIA													

3.6 Análisis de los Procesos Seleccionados

3.6.1 PO PLANEAR Y ORGANIZAR

3.6.1.1 PO1 Definir un Plan Estratégico de TI

3.6.1.1.1 Matriz RACI PO1

Tabla 11

Matriz RACI PO1

Actividades	Funciones		
	Gerente General	**Gerente de TI**	**Gerente de Planificación**
Relacionar las metas del negocio con las de TI	I	A	I
Identificar dependencias críticas y desempeño actual	I	A/R	I
Construir un plan estratégico de TI	A	C	C
Construir planes tácticos para TI	C	A	C
Analizar portafolio de programas	I	A/C	C

R Responsable, **A** Rinde cuentas, **C** Consultado, **I** Informado

Nota Fuente: (IT Governance Institute, 2007), Pag.31, Estados Unidos

Cuadro 1

Análisis Proceso PO1

PO1.1 Administración del Valor de IT			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Trabajar con el negocio para garantizar que el portafolio de inversiones de TI contenga casos de negocio sólidos. Los procesos de TI deben proporcionar una entrega efectiva y eficiente de los programas de TI y advertencias oportunas sobre las desviaciones del plan, incluyendo costo, cronograma o funcionalidad, que pudieran impactar los resultados esperados. Los servicios de TI se deben contemplar acuerdos de niveles de servicios adecuados.	-Poco valor de los proyectos de TI en el negocio -TI no alineado con el negocio -TI no cumpla con las directrices de administración de negocio -Inexistencia de responsables -Poco claro o no entendidos el costo-beneficio y los riesgos de TI	-Verificar si la empresa dispone de un proceso para la creación de casos de negocio. -Verificar que el proceso de casos de negocio tenga definidas las entradas/salidas, métricas, recursos y cuente con un proceso de administración de cambios. -Identificar si en el estudio del caso de negocio se han efectuado comparaciones con estándares técnicos, de la industria, SLA's. -Revisar casos de negocio anteriores para verificar desviaciones (costo, tiempo, personal)	Gerencia de TI
PO1.2 Alineación de TI con el Negocio			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Educar a los ejecutivos sobre las capacidades	-La misión de la empresa no está	-Evidenciar como se comunican los requerimientos del negocio hacia el área de TI.	Gerencia de

Continúa →

tecnológicas actuales y sobre el rumbo futuro, sobre las oportunidades que ofrece TI, y sobre qué debe hacer el negocio para capitalizar esas oportunidades. Las estrategias de negocio y de TI deben estar integradas, relacionando de manera clara las metas de la empresa y las metas de TI y reconociendo las oportunidades así como las limitaciones en la capacidad actual, y se deben comunicar de manera amplia.	soportada por TI. -Las decisiones de TI no se alinean con las del negocio. -Poca coordinación entre TI y el negocio generando inconvenientes con recursos y prioridades.- Oportunidades de mejora de TI no aprovechadas.	-Identificar cómo se involucra a la administración de TI en los objetivos del negocio -Evidenciar si se han definido los procesos críticos del negocio que dependen de TI.	Planificación Gerencia de TI
PO1.3 Evaluación de desempeño actual			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Evaluar el desempeño de los planes existentes y de los sistemas de información en términos de su contribución a los objetivos de negocio, su funcionalidad, su estabilidad, su complejidad, sus costos, sus fortalezas y debilidades.	-Las capacidades de TI no contribuyen a la misión de la organización y sus objetivos. -Decisiones de inversión tomadas muy tarde. -Uso no adecuado de recursos. -Requerimientos a futuro no	-¿Existe un sistema de evaluación de desempeño de la gestión de TI?, -¿Existe un plan de acción para desviaciones o variaciones de planes propuestos? -¿Existe una revisión de los objetivos para verificar su cumplimiento? -¿Están identificados procesos críticos de tecnología que soporten al negocio?	Gerencia de Planificación

Continúa →

	identificados.	-¿Se han analizado las fortalezas y debilidades de estos procesos, su funcionalidad, grado de automatización del negocio, estabilidad, complejidad, alineamiento tecnológico, requerimientos de soporte y mantenimiento? -¿Existe un comparativo de estándares de tecnología utilizado dentro del sector en el que se encuentra?	Gerencia de TI
PO1.4 Plan Estratégico de TI			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Crear un plan estratégico que defina cómo TI contribuirá a los objetivos estratégicos de la empresa (metas) así como los costos y riesgos relacionados. Incluye cómo TI dará soporte a los programas de inversión facilitados por TI y a la entrega de los servicios operativos. Define cómo se cumplirán y medirán los objetivos y recibirán una autorización formal de los interesados. El plan estratégico de TI debe incluir el	- Requerimientos del negocio no entendidos o manejados por la administración de TI. - Inexistencia de canales de consulta entre la administración de TI y la administración del negocio. - Planes de TI no alineadas con las necesidades del negocio.	Averiguar sobre el proceso de formulación de objetivos y metas de TI (definido, documentado y comunicado). Evidenciar logros y administración de riesgos de TI. -Evidenciar rendimiento actual y futuro de las expectativas del negocio. -Evidenciar la existencia de un plazo para el desarrollo de los planes estratégicos y tácticos.	Gerencia de Planificación Gerencia de TI

Continúa →

presupuesto de la inversión / operativo, las fuentes de financiamiento, la estrategia de obtención, la estrategia de adquisición, y los requerimientos legales y regulatorios. El plan estratégico debe ser lo suficientemente detallado para permitir la definición de planes tácticos de TI.	- Iniciativas e inversiones de TI innecesarias. - Planes de TI inconsistentes con las expectativas del negocio. - TI no enfocada en las prioridades del negocio.	-Evidenciar la existencia de métricas y que los objetivos de TI se relacionen con los objetivos del negocio. -Verificar que las políticas y procedimientos provean sustento al plan estratégico de TI.	
PO1.4 Plan Estratégico de TI			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Crear un plan estratégico que defina cómo TI contribuirá a los objetivos estratégicos de la empresa (metas) así como los costos y riesgos relacionados. Incluye cómo TI dará soporte a los programas de inversión facilitados por TI y a la entrega de los servicios operativos. Define cómo se cumplirán y medirán los objetivos y recibirán una autorización formal de los interesados. El	-Requerimientos del negocio no entendidos o manejados por la administración de TI. -Inexistencia de canales de consulta entre la administración de TI y la administración del negocio. -Planes de TI no alineadas con	Averiguar sobre el proceso de formulación de objetivos y metas de TI (definido, documentado y comunicado). -Evidenciar logros y administración de riesgos de TI. -Evidenciar rendimiento actual y futuro de las expectativas del negocio. -Evidenciar la existencia de un plazo para el desarrollo de los planes estratégicos y tácticos.	Gerencia de Planificación Gerencia de TI

Continúa →

plan estratégico de TI debe incluir el presupuesto de la inversión / operativo, las fuentes de financiamiento, la estrategia de obtención, la estrategia de adquisición, y los requerimientos legales y regulatorios. El plan estratégico debe ser bien detallado para permitir la definición de planes tácticos de TI.	las necesidades del negocio. - Iniciativas e inversiones de TI innecesarias. - Planes de TI inconsistentes con las expectativas del negocio. - TI no enfocada en las prioridades del negocio.	-Evidenciar la existencia de métricas y que los objetivos de TI se relacionen con los objetivos del negocio. -Verificar que las políticas y procedimientos provean sustento al plan estratégico de TI.	
PO1.5 Planes Tácticos de TI			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Crear planes tácticos de TI que se deriven del plan estratégico, estos deben describir las iniciativas y los requerimientos de recursos requeridos por TI, y cómo el uso de los recursos y el logro de los beneficios serán monitoreados y administrados. Los planes tácticos deben tener el detalle suficiente para permitir la definición de planes de proyectos. Administrar de forma activa los planes tácticos y las iniciativas de TI	- Planes de TI de largo plazo no alcanzados. -Recursos de TI no liberados. - Desviaciones en planes de TI no identificados. - Información para monitorear el área de TI no disponible.	-Verificar la existencia de un plan táctico de TI basado en un plan estratégico de TI. -Verificar que se lo lleve a cabo de una manera estructurada para evitar demoras en su ejecución. -Verificar las definiciones de proyectos, planificación de la información, los resultados y beneficios estimados.	Gerencia de TI

Continúa →

establecidas por medio del análisis de los portafolios de proyectos y servicios. Esto incluye el equilibrio de los requerimientos y recursos de forma regular, comparándolos con el logro de metas estratégicas y tácticas y con los beneficios esperados, y tomando las medidas necesarias en caso de desviaciones.			
PO1.6 Administración del Portafolio de TI			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Administrar, junto con el negocio, los programas de inversión de TI requerido para lograr objetivos de negocio estratégicos específicos por medio de la identificación, definición, evaluación, asignación de prioridades. Garantizar que los objetivos de los programas den soporte al logro de los resultados, entender el alcance para lograr los resultados, definir una rendición de cuentas clara, definir proyectos dentro del programa, asignar recursos y financiamiento y delegar autoridad.	-Recursos de TI no liberados. -Desviaciones de TI no identificadas.	-Evidenciar la formalización de un proceso de identificación y priorización de programas y proyectos de TI que soporten el plan táctico de TI. -Verificar si las metas de negocio y sus resultados están documentados y existen los recursos económicos y requeridos para llevarlos a cabo.	Gerencia de TI Gerencia de Planificación

Nota Fuente: (IT Governance Institute, 2007), Pag.30, Estados Unidos

Continúa →

3.6.1.2 PO4 Definir los Procesos, Organización y Relaciones de TI.

3.6.1.2.1 Matriz RACI PO4

Tabla 12

Matriz RACI PO4

Actividades	Funciones			
	Gerente General	**Gerente de TI**	**Gerente de Planificación**	**Gerente de RRHH**
Establecer estructura organizacional de TI incluyendo comités	A/R	C	C	C
Diseñar un marco de trabajo para el proceso de TI	I	A	C	C
Identificar dueños de sistemas	I	A	I	I
Identificar dueños de datos	I	A	I	I
Establecer e implementar roles y responsabilidades de TI	C		I	A

R Responsable, **A** Rinde cuentas, **C** Consultado, **I** Informado

Nota Fuente: (IT Governance Institute, 2007), Pág. 45, Estados Unidos

Cuadro 2

Análisis Proceso PO4

PO4.1 Marco de Trabajo de Procesos de TI			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Definir un marco de trabajo para el proceso de TI para ejecutar el plan estratégico de TI. Proporciona integración entre los procesos que son específicos para TI, administración del portafolio de la empresa, procesos de negocio y procesos de cambio del negocio.	-Organización de TI poco flexible -Superposición de actividades -Duplicación de procesos -Distanciamiento entre procesos	-Procesos de TI identificados y definidos en cuanto a responsables, recursos, controles. -Procesos del negocio identificados con entradas y salidas definidas. -Modelo de gestión de TI con metas definidas, control de metas, indicadores y modelo de madurez.	Gerencia de TI
PO4.2 Comité Estratégico de TI			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Establecer un comité estratégico de TI. Este comité deberá asegurar que el gobierno de TI, como parte del gobierno corporativo, se maneja de forma adecuada, asesora sobre la dirección estratégica y revisa las principales inversiones.	•TI no representada en el directorio •Riesgos y Valor de TI no reconocidos por el directorio. •Decisiones en inversiones y prioridades separas de TI y del	-Evidencia de la conformación de un comité de estrategia para TI. -Evidencia de la periodicidad de las reuniones del comité. -Evidencia de recomendaciones proporcionadas	Gerencia General Gerencia de RRHH

Continúa →

	Negocio. •Gobierno de TI no alineada al Gobierno del negocio.	a la organización. -Evidencia de las cualidades y capacidades de los miembros del comité.	
PO4.3 Comité Directivo de TI			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Establecer un comité directivo de TI (o su equivalente) compuesto por la gerencia ejecutiva, del negocio y de TI para: Determinar las prioridades de los programas de inversión de TI alineadas con la estrategia y prioridades de negocio de la empresa.	-Estrategia de TI no alineada con la estrategia del negocio. -Programas de inversión de TI poco alineadas al negocio. -	-Evidenciar la conformación de un comité de dirección de TI. -Averiguar por medio de actas de reuniones si los temas planteados aportan a la organización en cuanto al alineamiento de TI con el plan estratégico.	Gerencia General Gerencia Planificación
PO4.4 Ubicación Organizacional de la Función de TI			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**

Continúa →

Ubicar a la función de TI dentro de la estructura organizacional general con un modelo de negocios supeditado a la importancia de TI dentro de la empresa, en especial en función de qué tan crítica es para la estrategia del negocio y el nivel de dependencia operativa sobre TI. La línea de reporte del CIO es proporcional con la importancia de TI dentro de la empresa.	-Insuficiente involucramiento del grupo directivo en temas de TI. -TI no cuenta con una importancia adecuada en la estrategia de negocio. -Recursos de TI no proporcionados por el negocio. -Visión de TI separados del negocio y viceversa. -Vacío de comunicación entre logros de TI y dirección del negocio.	-Descripción de funciones del responsable de TI. -Evidenciar la independencia de funciones del área de TI del resto de áreas de la organización. -Asignación de recursos para el desempeño adecuado de las funciones de TI (presupuesto, personal, soporte, etc.).	Asistente de RRHH Gerente de TI

PO4.5 Estructura Organizacional			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Establecer una estructura organizacional de TI interna y externa que refleje las necesidades del negocio. Además, implementar un proceso para revisar la estructura organizacional de TI de forma periódica para ajustar los requerimientos de personal y las estrategias internas para	-Insuficiente soporte del negocio. -Poco personal de TI. -Rigidez de TI para soportar los cambios que el negocio requiere.	-Medición de capacidad de respuesta de acuerdo a cambios organizacionales y como estos cambios afectan a la organización. -Revisión de acuerdos con terceros y con servicios de TI de acuerdo a las necesidades del negocio.	Gerencia General, Gerencia de Contratos

Continúa →

satisfacer los objetivos de negocio esperados y las circunstancias cambiantes.			
PO4.6 Establecimiento de Roles y Responsabilidades			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Definir y comunicar los roles y las responsabilidades para el personal de TI y los usuarios que delimiten la autoridad entre el personal de TI y los usuarios finales y definían las responsabilidades y rendición de cuentas para alcanzar las necesidades del negocio.	-Incumplimiento de regulaciones. -Información confidencial -Personal incumpliendo sus funciones. -Uso fraudulento de datos -Organización de TI sin responsabilidades.	-Tareas de TI identificadas y formalizadas así como la existencia de actualizaciones. -Revisión anual de la política de sistemas. -Comunicación de las políticas para los empleados. -Registros de entrenamiento de los empleados. -Comprobar que todas las posiciones en la organización describan los roles de sistemas, control interno y seguridad de la información. -Definición de roles y funciones de TI de acuerdo a las tareas identificadas para el área de TI. - Verificar que se provea la adecuada difusión de los roles y responsabilidades asignados. -Verificar adecuadas delegaciones y responsabilidades que se han asignado y comunicado.	Gerencia de TI Gerencia de RRHH Gerencia de Planificación

Continúa →

		-En las evaluaciones de desempeño que los resultados de los objetivos y metas sean considerados.	

P.O.4.7 Responsabilidad de Aseguramiento de Calidad de TI

Objetivo de control	Factor de Riesgo	Elementos auditables	Auditado
Asignar la responsabilidad para el desempeño de la función de aseguramiento de calidad (QA) y proporcionar al grupo de QA sistemas de QA, los controles y la experiencia para comunicarlos. Asegurar que la ubicación organizacional, las responsabilidades y el tamaño del grupo de QA satisfacen los requerimientos de la organización.	-Riesgos de calidad no detectados que impactan en toda la organización. -Incremento en costos y retrasos debido a poco control de calidad. -Control de calidad no aplicado consistentemente o efectivamente. -Inconsistencia en calidad a través de la organización. -Reducción del rendimiento de la empresa.	-Vía de comunicación en temas de desvíos de los estándares de servicio definidos. -Un proceso definido y documentado para la identificación, el escalamiento y la resolución de inconvenientes identificados en el proceso de control de calidad,-Existencia de un proceso para el desarrollo de políticas y procedimientos, -Evidencia de empleo de las mejores prácticas y uso de estándares. -Proceso para reportar periódicamente los hallazgos y las recomendaciones.	Gerencia de TI

PO4.8 Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento

Objetivo de control	Factor de Riesgo	Elementos auditables	Auditado
Establecer la propiedad y la responsabilidad de los riesgos relacionados con TI. Definir y asignar	-Poca protección de los activos de	-Existencia de un staff que administre el riesgo y la seguridad de la información dentro de la	Gerencia

Continúa →

roles críticos para administrar los riesgos de TI, incluyendo la responsabilidad de la seguridad de la información, la seguridad física y el cumplimiento. Establecer responsabilidad sobre la administración del riesgo y la seguridad a nivel de toda la organización. Obtener orientación de la alta dirección con respecto al riesgo de TI y la aprobación de cualquier riesgo residual de TI.	información. -Pérdida de información confidencial. -Pérdidas Financieras. -Vacío en la dirección de lineamientos de seguridad. -Poca claridad sobre el apetito al riesgo de TI.	organización. -Definición de roles y responsabilidades para el staff que administra el riesgo y la seguridad de la información. -Administración de la seguridad de la información a cargo de un oficial de seguridad de la información. -Administración de la seguridad de la información a cargo de un oficial de seguridad de la información. -Consideraciones para que la mitigación del riesgo sea analizada y revisada de manera periódica.	de TI
PO4.9 Propiedad de Datos y Sistemas			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Proporcionar al negocio los procedimientos y herramientas que le permitan enfrentar sus responsabilidades de propiedad sobre los datos y los sistemas de información. Los dueños toman decisiones sobre la clasificación de la	-Inadecuada protección de activos de información. -Inadecuado aseguramiento de datos del negocio. -Inadecuadas medidas de seguridad	-Evidenciar la existencia de una política de clasificación de datos y propiedad de los sistemas, esté establecida y haya sido comunicada. -Validar que dicha política ha sido aplicada a la mayoría de los sistemas y a la arquitectura	Gerencia de TI

Continúa →

información y de los sistemas y sobre cómo protegerlos de acuerdo a esta clasificación.	para sistemas y datos. -Dueños de datos del negocio sin responsabilidad de sus datos.	empresarial tanto para las comunicaciones internas y externas. -Verificar que la política para clasificación de datos y propiedad del sistema soporta la protección de activos, permite la entrega eficiente y la utilización de aplicaciones del negocio facilitando la seguridad y apoyo en la toma de decisiones.	
PO4.10 Supervisión			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Implementar prácticas adecuadas de supervisión dentro de la función de TI para garantizar que los roles y las responsabilidades se ejerzan de forma apropiada, evaluar si el personal cuenta con la suficiente autoridad y recursos para ejecutar sus roles y responsabilidades y para revisar en general los indicadores clave de desempeño.	-Metas y Objetivos no alcanzados. -Inadecuado funcionamiento de TI y de los procesos de negocio. -Inadecuado monitoreo de controles y objetivos.-Roles principales y responsabilidades no realizadas.	-Verificar que existen procesos de supervisión. -Asegurar que dichos procesos de supervisión son revisados y ejecutados. -Verificar si las supervisiones disponen de un adecuado cumplimiento de las expectativas y de un adecuado rendimiento.	Gerencia de TI

Continúa →

PO4.11 Segregación de Funciones			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Implementar una división de roles y responsabilidades que reduzca la posibilidad de que un solo individuo afecte negativamente un proceso crítico. La gerencia también asegura que el personal realice sólo tareas autorizadas, relevantes a sus puestos y posiciones respectivas.	-Pérdida financiera y daño en imagen corporativa -Daños malintencionados. -Incumplimiento de regulaciones externas sobre división de funciones en sistemas y aplicaciones.	-Verificar la existencia de segregación de funciones. -Averiguar y confirmar si existe un proceso para identificar posiciones críticas y confirmar si existe segregación de funciones.	Gerencia de RRHH
PO4.12 Personal de TI			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Evaluar los requerimientos de personal de forma regular o cuando existan cambios importantes en el ambiente de negocios, operativo o de TI para garantizar que la función de TI cuente con un número suficiente de recursos para soportar adecuada y apropiadamente a las metas y objetivos del negocio.	-Personal de TI no cumple las necesidades del negocio. -Excesivo costo del personal de TI. -Bajo o sobredimensionado departamento de TI.	-Verificar que los conocimientos requeridos para el área de TI sean identificados y gestionados y su impacto en el personal de TI sean: analizados, escalados y resueltos de acuerdo a estas necesidades.-De existir cambios en el negocio o la operación verificar si existen impactos en las destrezas o competencias del personal de TI.-	RRHH

Continúa →

	-Carencia de adecuadas capacidades en el personal de TI.	Verificar las estrategias de soporte y verificar que están soportadas por las destrezas y competencias requeridas.	
PO4.13 Personal Clave de TI			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Definir e identificar al personal clave de TI y minimizar la dependencia en un solo individuo desempeñando una función de trabajo crítica.	-Capacidad insuficiente del personal clave de TI. -Poca transmisión de conocimientos e inexistencia de plan de sucesión. -Tareas críticas y roles no ejecutado.	Verificar la existencia de procesos formales para cubrir las posiciones en caso de ausencia del personal que administra los procesos claves de TI.-Verificar si la administración ha considerado la dependencia de personal de TI para casos de contingencia por medio de personal alterno, si existe documentación de temas críticos, delegación de funciones y personal entrenado para reemplazar al personal principal.	RRHH Gerencia de TI
PO4.14 Políticas y Procedimientos para Personal Contratado			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Asegurar que los consultores y el personal contratado que soporta la función de TI cumplan	-Dependencia de los recursos contratados.	-Solicitar las políticas que regulan cuándo, cómo y qué tipos de tareas pueden ser tercerizadas y si éstas	Jefe de Contratos

Continúa →

con las políticas organizacionales de protección de los activos de información de la empresa de tal manera que se logren los requerimientos contractuales acordados.	-Brechas entre requerimientos y capacidades del personal contratado. -Trabajo realizado no alineado con los requerimientos del negocio. -Conocimientos no registrados o capacidades no transferidas. -Fallas del personal contratado en cuanto al cumplimiento de las políticas de seguridad de datos.-Costos legales por desacuerdos.	tareas se las están realizando -Inspeccionar qué políticas y procedimientos para un efectivo control de seguridad hacia contratistas y asegurarse que están siendo empleadas. -Revisar las políticas y procedimientos para la selección de un proveedor y verificar si están siendo llevadas a cabo.	

PO4.15 Relaciones			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Establecer y mantener una estructura óptima de enlace, comunicación y coordinación entre la función de TI y otros interesados dentro y fuera de la función de TI, tales como ejecutivos, unidades de negocio, usuarios individuales, proveedores,etc.	-Inadecuada identificación de mejoras. -Brechas entre objetivos del negocio y las políticas de TI.	Niveles de comunicación hacia las partes interesadas han sido definidos.	Gerencia de TI

Nota Fuente: (IT Governance Institute, 2007), Pag.42, Estados Unidos

Continúa →

PO9. Evaluar y Administrar los Riesgos de TI

3.6.1.2.2 Matriz RACI PO9

Tabla 13

Matriz RACI PO9

Actividades	Funciones		
	Gerente General	**Gerente de TI**	**Gerente Planificación**
Determinar la alineación de la administración de riesgos.	A	C	I
Entender los objetivos de negocio estratégicos relevantes.		A/R	I
Identificar los objetivos internos de TI y establecer el contexto del riesgo.			I
Asesorar el riesgo con los eventos.		A/C	C
Evaluar y seleccionar respuestas a riesgos.	I	A/C	C
Aprobar y asegurar fondos para planes de acción de riesgos.			I
Mantener y monitorear un plan de acción de riesgos.	A	R	R

R Responsable, **A** Rinde cuentas, **C** Consultado, **I** Informado

Nota Fuente: (IT Governance Institute, 2007), Pag.65, Estados Unidos

Cuadro 3

Análisis Proceso PO9

PO9.1 Marco de Trabajo de Administración de Riesgos			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Establecer un marco de trabajo para la gestión de riesgos de TI que esté alineado con los riesgos de la organización.	-Los riesgos de TI y del negocio son manejados independientemente. -El impacto de un riesgo de TI en el negocio no es conocido. -Alto costo en la mitigación o control de un riesgo.	-Verificar que se tienen identificados y se gestionan apropiadamente los riegos del negocio y que estos son conocidos por la Gerencia de TI. -Verificar que se han identificado los riesgos de TI que afecten a las operaciones del negocio. -Verificar si existe una matriz de riesgos de TI donde se evalúen de acuerdo a su impacto y probabilidad.	Gerente General Gerente de TI
PO9.2 Establecimiento del Contexto del Riesgo			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Establecer el contexto en el cual el marco de trabajo de la evaluación de riesgos se aplica para garantizar resultados apropiados. Esto incluye la determinación del contexto interno y externo de cada evaluación de riesgos, la meta de la	- Riesgos irrelevantes son considerados importantes. - Riesgos significativos no tienen la apropiada atención. - Inapropiada evaluación de riesgos.	-Verificar el criterio que se emplea para clasificar los riegos. - Analizar la Matriz de riesgos de TI si existiera o la manera como se están evaluando los riesgos de TI.	Gerente de TI

Continúa →

evaluación y los criterios contra los cuales se evalúan los riesgos.		- Evidenciar riesgo para analizar la aplicación por gestión del riesgo en TI.	
PO9.3 Identificación de Eventos			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Identificar eventos (una amenaza importante y realista que ataca a una vulnerabilidad significativa) con un impacto potencial negativo sobre las metas o las operaciones de la empresa, incluyendo aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos. Determinar la naturaleza del impacto y mantener esta información. Registrar y mantener los riesgos relevantes en un registro de riesgos.	-Identificación y enfoque en los eventos de riesgos irrelevantes mientras que eventos de riesgos importantes no son evaluados.	-Verificar que se tengan registrados los eventos críticos de TI. -Evidenciar el análisis de los eventos ocurridos su impacto y las acciones implementadas. -Verificar si se realiza un seguimiento a los eventos ocurridos como resultado de falta de control a un riesgo. - Evidenciar la existencia de un registro de eventos.	Gerente de TI
PO9.4 Evaluación de Riesgos de TI			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Evaluar de forma recurrente la probabilidad e	-Incapacidad para explicar riesgos	-Evidenciar que la Gerencia General está enterada	Gerente

Continúa →

impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La probabilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio.	significativos a la Gerencia. -Pérdida de activos de TI. -Pérdida de la confidencialidad o integridad de los activos de TI.	o forma parte de la evaluación de los riesgos de TI. -Evidenciar que los riesgos están definidos y documentados. -Evidenciar el análisis de los riesgos de forma individual por categoría por su probabilidad e impacto.	General Gerente de TI
PO9.5 Respuesta a los Riesgos			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Desarrollar y mantener un proceso de respuesta a riesgos diseñado para asegurar que los controles son efectivos y mitigan al riesgo en forma continua. El proceso de respuesta debe incluir estrategias tales como evitar, reducir, compartir o aceptar riesgos, determinar responsabilidades y considerar los niveles de tolerancia de los riesgos.	-Respuesta no efectiva a los riesgos. -Mal uso de los recursos para responder a un riesgo. -Sobreestimación de controles ineficientes.	-Identificar y analizar los controles implementados a los riesgos de TI. -Identificar y analizar los recursos asignados para mitigación de riesgos. -Evidenciar si se documentan los resultados obtenidos luego de la ocurrencia de un riesgo y si se hace seguimientos de mejora. -Buscar evidencia de la aplicación de los resultados de la evaluación de los riesgos. Ejemplo en un BCP (Business Continuity Plan).	Gerente de TI

Continúa →

PO9.6 Mantenimiento y Monitoreo de un Plan de Acción de Riesgos			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Priorizar y planear las actividades para la implementación de los controles a los riesgos, incluyendo la identificación de costos, beneficios y responsables. Obtener la aprobación para las acciones recomendadas y la aceptación de cualquier riesgo residual, y asegurarse de que las acciones comprometidas están a cargo del dueño(s) de los procesos afectados. Monitorear la ejecución de los planes y reportar cualquier desviación a la alta dirección.	-Controles de mitigación de riesgos que no operan como deberían.	-Verificar la existencia de un Plan de acción para los riesgos identificados como principales. -Evidenciar el seguimiento a las actividades incluidas en los planes de acción para mitigación de riesgos. -Verificar que los Planes de acción sean conocidos y aprobados por la Gerencia General. -Evidenciar que los planes de acción sean actualizados de acuerdo a los cambios en los controles.	Gerente de TI

Nota Fuente: **(IT Governance Institute, 2007),** ***Pag.64, Estados Unidos***

Continúa →

3.6.2 DS ENTREGAR Y DAR SOPORTE

3.6.2.1 DS2 Administrar los Servicios de Terceros

3.6.2.1.1 Matriz RACI DS2

Tabla 14

Matriz RACI DS2

Actividades	Funciones		
	Gerente General	**Gerente de TI**	**Gerente Planificación**
Identificar y categorizar las relaciones de los servicios de terceros	I	I/C	A/R
Definir y documentar los procesos de administración del proveedor	I	C	A/R
Establecer políticas y procedimientos de evaluación y suspensión de proveedores	I	I/C	A/R
Identificar, valorar y mitigar los riesgos del proveedor	I	A/R	C
Monitorear la prestación del servicio del proveedor	I	A/R	I/C
Evaluar las metas de largo plazo de la relación del servicio para todos los interesados	I/C	***C***	A/R

R Responsable, **A** Rinde cuentas, **C** Consultado, **I** Informado

Nota Fuente: (IT Governance Institute, 2007), Pag.107, Estados Unidos

Cuadro 4

Análisis Proceso DS2

DS2.1 Identificación de todas la relaciones con proveedores			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Identificar todos los servicios de los proveedores y categorizarlos de acuerdo al tipo de proveedor, significado y criticidad. Mantener documentación formal de relaciones técnicas y organizacionales que cubren los roles y responsabilidades, metas, entregables esperados, y credenciales de los representantes de estos proveedores.	•Proveedores importantes y críticos no identificados. •Uso ineficiente e ineficaz de los recursos de administración de proveedores. •Roles y responsabilidades no definidas conducen a comunicaciones ineficientes, servicios deficientes y aumento de los costos.	-Pregunte si, y confirme que un registro de relaciones con los proveedores se mantiene. -Obtener e inspeccionar los criterios de relaciones con los proveedores de la razonabilidad y la integridad de clasificaciones por tipo de proveedor, la importancia y criticidad. -Determinar si el esquema de categorización del proveedor es lo suficientemente detallada para categorizar todas las relaciones con los proveedores sobre la base de la naturaleza de los servicios contratados. -Verificar si las historias del pasado en la selección de proveedores / rechazo son conservados y utilizados. -Inspeccionar el registro de relaciones con los	Jefe de Compras

Continúa →

		proveedores para asegurarse de que está al día, debidamente clasificado y suficientemente detallado para asegurarse de que proporciona una base para el monitoreo de los proveedores existentes.	
DS2.2 Gestión de Relaciones con Proveedores			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Formalizar el proceso de gestión de relaciones con proveedores para cada proveedor. Los dueños de las relaciones deben enlazar las cuestiones del cliente y proveedor y asegurar la calidad de las relaciones basadas en la confianza y transparencia. (Ej.: a través de SLA's).	•Proveedor no comprometido con la relación. •Problemas y asuntos no resueltos. •Calidad de servicio inadecuado.	-Inspeccionar la documentación de proveedores de servicios, de pruebas de los roles formales y responsabilidades y determinar si las funciones de gestión de proveedores han sido documentadas y comunicadas dentro de la organización. -Determinar si existen políticas para asegurar que los contratos se creen, mantengan, se den seguimiento y renegocien cuando sea necesario. -Evaluar si la asignación de funciones del proveedor es razonable y basada en el nivel y las habilidades técnicas necesarias para gestionar eficazmente la relación.	Jefe de Compras

Continúa →

DS2.3 Administración de Riesgos del Proveedor			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Identificar y mitigar los riesgos relacionados con la habilidad de los proveedores para mantener un efectivo servicio de forma segura y eficiente sobre una base de continuidad. Asegurar que los contratos están de acuerdo con los requerimientos legales y regulatorios. La administración del riesgo debe considerar además acuerdos de confidencialidad (NDAs), contratos de garantía, viabilidad de la continuidad del proveedor, conformidad con los requerimientos de seguridad, proveedores alternativos, penalizaciones e incentivos, etc.	•Incumplimiento de las obligaciones reglamentarias y legales. •Seguridad, así como otros incidentes. •Pérdidas económicas y daños en reputación debido a la interrupción del servicio.	-Pregunte si los riesgos asociados con la incapacidad para cumplir con los contratos con los proveedores se definen. -Pregunte si los recursos fueron considerados en la definición del contrato de abastecimiento -Inspeccionar la documentación del contrato para la evidencia de la revisión -Determinar si en las políticas se exigen la independencia entre el proveedor y el personal de gestión dentro de la organización	Jefe de Compras Asistente de Recursos Humanos

DS2.4 Monitoreo del Desempeño del Proveedor			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Establecer un proceso para monitorear la prestación del servicio para asegurar que el proveedor está cumpliendo con los requerimientos	•Degradación del servicio no detectada. •Incapacidad para afrontar cambios	-Seleccionar una muestra de facturas de proveedores, determinar si se identifican los cargos por los servicios contratados, según lo especificado	Gerencia de TI

Continúa →

del negocio actuales y que se adhiere continuamente a los acuerdos del contrato y a SLA's, y que el desempeño es competitivo con proveedores alternativos y las condiciones del mercado.	en precios y servicios. •Incapacidad para mejorar la competencia de otros proveedores.	en los contratos de servicios, y evaluar la razonabilidad de los gastos. -Inspeccionar una muestra de informes de servicio del proveedor para determinar si el proveedor informa regularmente sobre los criterios, reportes de desempeño y SLA´s acordados.	

Nota Fuente: (IT Governance Institute, 2007), Pag.106, Estados Unidos

Continúa →

3.6.2.2 DS4 Garantizar la Continuidad del Servicio

3.6.2.2.1 Matriz RACI DS4

Tabla 15

Matriz RACI DS4

Actividades	Funciones			
	Gerente General	**Gerente de TI**	**Analista de SS**	**Gerente de Planificación**
Desarrollar un análisis del impacto al negocio y valoración del riesgo.		A/R/C		C
Desarrollar y mantener planes de continuidad de TI.	I	A/R/C		C
Identificar y categorizar los recursos de TI con base en los objetivos de recuperación.		A/R/C		I
Desarrollar un plan de acción a seguir con base en los resultados de la pruebas.		A/R/C		I
Planear y llevar a cabo capacitación sobre los planes de continuidad de TI.		A/R/I		I
Planear la recuperación y reanudación de los servicios de TI.		A/R/C		C
Planear e implementar el almacenamiento y la protección de respaldos.		I	A/R	I

R Responsable, **A** Rinde cuentas, **C** Consultado, **I** Informado

Nota Fuente: (IT Governance Institute, 2007), Pag.115, Estados Unidos

Cuadro 5

Análisis Proceso DS4

DS4.1 Marco de Trabajo de Continuidad de TI			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Desarrollar un marco de trabajo que garantice un proceso consistente para la continuidad de TI y por ende del negocio. El objetivo del marco de trabajo es ayudar con la identificación de la infraestructura necesaria y los planes para la recuperación de desastres y de contingencias. El marco de trabajo debe tomar en cuenta la estructura organizacional para la gestión de la continuidad, tareas, roles y las responsabilidades de los proveedores de servicios internos y externos, clientes, así como las tareas para documentar, probar y ejecutar la recuperación de desastres y los planes de contingencia de TI. El	-Prácticas ineficientes de continuidad. -Servicios de continuidad de TI no manejados apropiadamente.	-Entender y evaluar la estrategia de continuidad del negocio. -Evaluar los planes de continuidad de TI que aseguren la continuidad del negocio. -Evidenciar si en el plan de continuidad están involucrados los usuarios, proveedores y clientes y se detalla los roles y responsabilidades de cada uno de ellos. -Evidenciar si en el plan de continuidad se encuentran todos los activos críticos de TI. -Verificar que el plan de continuidad sea conocido y aprobado por la Gerencia General y divulgado a todos los involucrados. - Verificar la vigencia del plan de continuidad y las actualizaciones cuando existan cambios.	Gerente General Gerente de TI

Continúa →

plan debe considerar la identificación de recursos críticos, el monitoreo y reporte de la disponibilidad, el procesamiento alternativo y los principios de respaldo y recuperación.			
DS4.2 Planes de Continuidad de TI			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio. Los planes deben considerar requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de todos los servicios críticos de TI. También deben cubrir los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas.	-Fallo en la recuperación de sistemas y servicios de TI. -Falta de recursos necesarios para la recuperación. -Problemas en la comunicación interna y externa.	- Verificar que se han identificado los procesos críticos de negocio. - Evaluar el Plan de continuidad para verificar que los procesos críticos están tomados en cuenta. - Evaluar la capacidad de recuperación y alternativas de procesamiento para garantizar la disponibilidad de los servicios. - Verificar que la mínima configuración de un recurso crítico está detallado en el procedimiento de recuperación. - Evidenciar que se ha realizado pruebas frecuentes al Plan de recuperación.	Gerente de TI

Continúa →

DS4.3 Recursos Críticos de TI			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Centrar la atención en los puntos más críticos en el plan de continuidad de TI, para establecer prioridades en situaciones de recuperación. Evitar recuperar los puntos menos críticos y asegurarse de que la recuperación está alineada con las necesidades prioritarias del negocio, verificar que los costos tengan un nivel aceptable y se cumple con los requerimientos regulatorios y contractuales.	-No disponibilidad de recursos críticos de TI. -Costos muy elevados para la ejecución del plan de continuidad. -Priorización de la recuperación de servicios no está basada en las necesidades del negocio.	-Verificar la estrategia para reemplazar los recursos críticos de TI en caso de un evento. -Verificar que la Gerencia de TI tenga identificadas a las funciones de negocio críticas: procesos y recursos. -Verificar que los planes de continuidad cumplan con requerimientos legales, contractuales y regulatorios. -Verificar si la priorización de la recuperación de los servicios y recursos críticos de TI establecidos en el plan son los requeridos por el negocio. -Evaluar el análisis de los costos en cada proceso de recuperación.	Gerente de TI
DS4.4 Mantenimiento del Plan de Continuidad de TI			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Exhortar a la Gerencia de TI a definir y ejecutar procedimientos de control de cambios, para	-Planes de recuperación desactualizados.	-Evidenciar que la Gerencia de TI haya desarrollado un procedimiento de control de	Gerente de TI

Continúa →

asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua los requerimientos actuales del negocio. Es esencial que los cambios en los procedimientos y las responsabilidades sean comunicados de forma clara y oportuna.	-Planes no reflejan cambios a las necesidades del negocio y tecnología. -Falta de procedimientos para el control de cambios.	cambios para el Plan de continuidad. -Evidenciar las actualizaciones al plan cuando se cambien recursos críticos. -Verificar que se lleva un registro de los cambios realizados a los Planes de continuidad, los responsables y que los cambios sean comunicados a los involucrados.	
DS4.5 Pruebas del Plan de Continuidad de TI			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Probar el plan de continuidad de TI de forma regular para asegurar que la recuperación será efectiva, que las deficiencias son atendidas y que el plan permanece aplicable. Esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas y, de acuerdo con los resultados, la implementación de un plan de acción. Considerar el alcance de las pruebas de	-Planes de recuperación incompletos. -Planes de recuperación desactualizados que no reflejan la actual arquitectura. -Pasos y procesos inapropiados para la recuperación. -Plan incapaz para recuperar	-Evidenciar programas frecuentes de pruebas para el plan de contingencia (cambios a recursos críticos). -Verificar que los planes de continuidad del negocio detallen secuencias lógicas y ordenadas para la ejecución de las pruebas. -Evaluar el almacenamiento en el sitio alterno si existiera. -Evaluar el sitio alterno para asegurar la presencia,	Gerente de TI Usuarios

Continúa →

recuperación en aplicaciones individuales, en escenarios de pruebas integrados, en pruebas de punta a punta y en pruebas integradas con el proveedor.	efectivamente si ocurriera un desastre real.	sincronización y vigencia de los medios y de la documentación. -Evaluar la capacidad del personal de TI y del usuario para responder con eficacia ante un desastre. -Evaluar los resultados de pruebas para determinar que se hayan incorporado al plan las acciones correctivas.	
DS4.6 Entrenamiento del Plan de Continuidad de TI			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Asegurarse de que todas las partes involucradas reciban capacitación de forma regular respecto a sus procesos, roles y responsabilidades en caso de incidente o desastre. Verificar e incrementar el entrenamiento de acuerdo con los resultados de las pruebas de contingencia.	-Programas de entrenamiento desactualizados. -Fallo en la recuperación como resultado de un entrenamiento inadecuado o desactualizado.	-Verificar la existencia de planes de capacitación a los involucrados. -Evaluar si los manuales y procedimientos de continuidad del negocio están escritos en una forma sencilla y fácil de entender por el usuario final. -Realizar entrevistas al personal para verificar si el Plan es apropiado, completo y entendible. -	Gerente de TI Usuarios

Continúa →

DS4.7 Distribución del Plan de Continuidad de TI			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Determinar que existe una estrategia de distribución definida y administrada para asegurar que los planes se distribuyan de manera apropiada y segura y que estén disponibles entre las partes involucradas y autorizadas cuando y donde se requiera. Se debe prestar atención en hacerlos accesibles bajo cualquier escenario de desastre.	-Información confidencial incluida en los planes. -Planes no accesibles por todas las partes involucradas. -Actualizaciones a los planes no ejecutados a tiempo.	-Evidenciar si el Plan de continuidad es distribuido al personal involucrado.-Verificar si existe un procedimiento de distribución. -Evidenciar que las copias del Plan de continuidad son protegidos adecuadamente y solo revisados por personal autorizado. -Evidenciar que en el Plan de continuidad no se incluya información confidencial que pueda ser leída por personal no autorizado.	Gerente de TI
DS4.8 Recuperación y Reanudación de los Servicios de TI			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Planear acciones a tomar durante TI está recuperando y reanudando los servicios. Activación de sitios de respaldo, inicio de	-Fallo en la recuperación de sistemas y servicios críticos del negocio a tiempo.	-Verificar que los procedimientos de recuperación y reanudación de los servicios sean completos, ordenados y lógicos.	Gerente de TI

Continúa →

procesamiento alternativo, la comunicación a clientes y a los interesados, realizar procedimientos de reanudación, etc. Asegurar que se entienden los tiempos de recuperación de TI y las inversiones necesarias en tecnología para soportar las necesidades de recuperación y reanudación del negocio.	-Desconocimiento de la Gerencia General y usuarios en cuanto al tiempo necesario para la recuperación.	-Verificar que la Gerencia General conoce el tiempo necesario para ejecutar la recuperación. -Verificar que la Gerencia General conoce el costo necesario para la recuperación.	
DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio. El contenido de los respaldos debe determinarse entre los responsables de los procesos y el personal de TI. Asegurarse de la compatibilidad del hardware y del software para recuperar los datos.	-Respaldo de datos y medios no funcionan adecuadamente. -Pérdida de datos debido a un desastre. -Destrucción accidental del backup de datos. -Incapacidad para localizar los medios de backup cuando se los necesita.	-Verificar la existencia de respaldos de los medios y documentación bien identificados. -Verificar que los respaldos se encuentre fuera de la oficina. -Evidenciar que se realizan pruebas de recuperación de información para validar backups. -Evidenciar registros de los procedimientos periódicos de copias de respaldo. -Evidenciar que se están respaldando la información detallada en el plan de continuidad del negocio.	Analista de TI

Continúa →

DS4.10 Revisión Post Reanudación			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Una vez lograda una exitosa reanudación de las funciones de TI después de un desastre, determinar si la Gerencia de TI ha establecido procedimientos para valorar lo adecuado del plan y realizar modificaciones si fuera el caso.	-Planes inapropiados de recuperación. -Planes de recuperación no ajustados a las necesidades del negocio. -Objetivos no tomados en cuenta.	-Evidenciar las mejoras al plan de continuidad luego de la recuperación a través de la creación de acciones correctivas. -Verificar que se mantiene informada a la Gerencia General luego de la reanudación de los servicios y que se aprueban los nuevos requerimientos.	Gerente de TI

Nota Fuente: (IT Governance Institute, 2007), Pag.114, Estados Unidos

Continúa →

3.6.2.3 DS5 Garantizar la Seguridad de los Sistemas

3.6.2.3.1 Matriz RACI DS5

Tabla 16

Matriz RACI DS5

Actividades	Funciones		
	Gerente General	**Gerente de TI**	**Gerente Planificación**
Definir y mantener un plan de seguridad de TI	I	A/R	I
Definir, establecer y operar un proceso de administración de identidad (cuentas)		A/R	I
Monitorear incidentes de seguridad, reales y potenciales		A/R	I
Revisar y validar periódicamente los privilegios y derechos de accesos de los usuarios		A/R	I
Implementar y mantener controles técnicos y de procedimientos para proteger el flujo de información a través de la red	I	A/C	C
Realizar evaluaciones de vulnerabilidad de manera regular		A/C	C

R Responsable, **A** Rinde cuentas, **C** Consultado, **I** Informado

Nota Fuente: (IT Governance Institute, 2007), Pag.119, Estados Unidos

Cuadro 6

Análisis Proceso DS5

DS5.1 Administración de la Seguridad de TI			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Administrar la seguridad de TI apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.	-Ausencia de Gobierno de seguridad de TI. -Falta de alineación entre los objetivos de TI y los del negocio. -Activos de información y datos sin protección.	-Determinar si un comité de dirección de seguridad existe, con representación de las principales áreas funciónales, incluida la auditoría interna, recursos humanos, operaciones, seguridad informática y jurídica. -Determinar si existe un proceso para dar prioridad a las iniciativas, propuestas de seguridad, incluyendo los niveles requeridos de las políticas, normas y procedimientos. -Confirmar que una política de seguridad de la información existe. -Revisar y analizar la política de seguridad para verificar que se refiere a la protección frente al riesgo de la organización en relación con la seguridad de la información y que la misma incluya claramente: alcance, objetivos y responsabilidades de la seguridad. -Revisar la Política de seguridad de TI	Gerencia de TI

Continúa →

DS5.3 Administración de Identidad			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Asegurar que todos los usuarios y su actividad en sistemas de TI sean identificables de manera única. Permitir que el usuario se identifique a través de mecanismos de autenticación. Confirmar que los permisos de acceso del usuario al sistema y los datos están en línea con las necesidades del negocio definidas y documentadas y que los requerimientos de trabajo están adjuntos a las identidades del usuario. Asegurar que los derechos de acceso del usuario se solicitan por la gerencia de área, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad.	-Cambios no autorizados en hardware y software. -Fallas en la Administración de acceso incumpliendo los requerimientos del negocio y comprometiendo la seguridad de sistemas críticos para el negocio. -Requisitos de seguridad no especificadas para todos los sistemas. - Violación a la segregación de funciones. -Información comprometida.	-Determinar si las prácticas de seguridad requieren de una política de autenticación para conceder el acceso a los sistemas. -Si los roles predeterminados y con aprobación previa se utilizan para conceder acceso, determinar si delimitan las responsabilidades y verificar que estos roles sean aprobados por el dueño del proceso. -Determinar si los mecanismos de autenticación se utilizan para controlar el acceso lógico a través de todos los usuarios, los procesos del sistema, los recursos de TI y accesos remotos.	Gerencia de TI

Continúa →

DS5.4 Administración de Cuentas del Usuario			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Garantizar que la solicitud, emisión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por procedimientos de la gerencia. Estos procedimientos deben aplicarse a todos los usuarios, incluyendo administradores, usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relativos al acceso a los sistemas e información de la empresa deben acordarse contractualmente para todos los tipos de usuarios. Realizar revisiones regulares de la gestión de todas las cuentas y los privilegios asociados.	-Existencia de brechas de seguridad. -Existencia de usuarios que no cumplan con la política de seguridad. -Incidentes no resueltos de manera oportuna. -Falencias en cancelar cuentas no utilizadas de manera oportuna, impactando en la seguridad corporativa.	-Determinar si existen procedimientos para evaluar periódicamente y certificar el acceso a los sistemas y las aplicaciones. -Determinar si los procedimientos de control de acceso existen para controlar y gestionar los permisos a los sistemas y las aplicaciones. Los privilegios se basan a las políticas de seguridad de la organización, el cumplimiento y los requisitos reglamentarios. -Determinar si los sistemas, aplicaciones y datos han sido clasificados por niveles de importancia y riesgo, y si los propietarios del proceso han sido identificados y asignados. -	Gerencia de TI

Continúa →

DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa. La seguridad en TI debe ser reacreditada periódicamente para garantizar que se mantiene el nivel seguridad aprobado. Una función de ingreso al sistema y de monitoreo permite la detección oportuna de actividades inusuales o anormales que pueden requerir atención.	-Uso indebido de cuentas de usuario, comprometiendo la seguridad de la organización. -Brechas de seguridad no detectadas. -Los registros no confiables de seguridad.	-Pregunte si, y confirmar que un inventario de todos los dispositivos de red, servicios y aplicaciones existe y que cada componente se le ha asignado una calificación de riesgo de seguridad. -Determinar que exista una línea de base de seguridad para todos los recursos de TI utilizados por la organización. -Determinar si los activos de mayor riesgo de la red se controlan rutinariamente por los eventos de seguridad. -Determinar si la seguridad de TI se ha integrado dentro de las iniciativas de gestión de proyectos de la organización para garantizar que la seguridad está considerada en las necesidades de desarrollo, diseño y pruebas, para minimizar el riesgo de sistemas nuevos o existentes, que estén introduciendo vulnerabilidades en la seguridad.	Gerencia de TI

Continúa →

DS5.6 Definición de Incidente de Seguridad			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Definir claramente y comunicar las características de incidentes de seguridad potenciales para que puedan ser clasificados adecuadamente y tratados por el proceso de gestión de incidentes y problemas.	-Brechas de seguridad no detectadas. -Falta de información para realizar contra ataques. -Falta de clasificación de las infracciones de seguridad.	-El papel y las responsabilidades de los proveedores en la prevención de incidentes y el seguimiento, corrección de fallas de software y otras áreas. -Determine si el proceso de manejo de incidentes de seguridad emplea adecuadas relaciones con las funciones clave de la organización, como la mesa de ayuda, los proveedores de servicios externos y gestión de la red. -Evaluar si el proceso de gestión de incidentes incluye los siguientes elementos clave: •Detección de eventos, Correlación de eventos y la evaluación de la amenaza / incidente •Resolución de la amenaza o creación y orden de escalamiento, •Análisis post-implementación •Orden de trabajo / Cierre de incidente.	Gerencia de TI

Continúa →

DS5.7 Protección de la Tecnología de Seguridad			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Garantizar que la tecnología relacionada con la seguridad sea resistente al sabotaje y no revele documentación de seguridad innecesaria.	• Exposición de la información. • Abuso de confianza con otras organizaciones. • Violaciones de los requisitos legales y reglamentarios.	-Pregunte y confirme que políticas y procedimientos han sido establecidos para hacer frente a las consecuencias de violación de seguridad. -Inspeccionar los registros de control de acceso y registro de acceso de intentos fallidos. -Preguntar que existan reglas de contraseñas: longitud máxima, uso de letras y números, la expiración, reutilización de claves). -Pregunte si y confirmar que el control requiere de revisiones anuales de gestión de los elementos de seguridad para el acceso físico y lógico de archivos y datos. -Inspeccionar los informes de seguridad generados por las herramientas del sistema prevención de ataques de red, vulnerabilidad de la penetración.	Gerencia de TI

Continúa →

DS5.8 Administración de Llaves Criptográficas			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Determinar que las políticas y procedimientos para la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas.	-Claves indebidamente utilizadas por partes no autorizadas. -Registro de usuarios no verificados, comprometiendo la seguridad del sistema. -Acceso no autorizado a las claves criptográficas.	-Determine si existe un proceso del ciclo de vida de gestión que contenga: •Mínimo tamaño de caracteres en la clave para una contraseña segura. •Uso de algoritmos para generación de claves. •Métodos de distribución de claves. •Identificación de estándares para la generación de algoritmos •Respaldos de claves, archivo y destrucción. -Evaluar si los controles sobre las claves privadas existen para hacer cumplir su confidencialidad e integridad. Se debe considerar lo siguiente: Las claves privadas son respaldadas, almacenadas y recuperadas por personal autorizado con control dual en un medio ambiente protegido físicamente.	Gerencia de TI

Continúa →

DS5.9 Prevención, Detección y Corrección de Software Malicioso			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Poner medidas preventivas y correctivas (en especial contar con parches de seguridad y control de virus actualizados) en toda la organización para proteger los sistemas de la información y a la tecnología contra malware (virus, gusanos, spyware, correo basura).	-Exposición de la información. -Violaciones de los requisitos legales y reglamentarios. -Sistemas y datos que son propensos a ataques de virus. -Medidas ineficaces.	-Pregunte y confirme que una política de prevención sobre software malicioso está establecido, documentado, y comunicado a toda la organización. -Asegúrese de que controles automatizados han sido implementados para proporcionar protección contra virus y que las violaciones son comunicadas apropiadamente. -Infórmese de que los miembros del personal clave son conscientes de la política de prevención de software malintencionado y su responsabilidad para asegurar el cumplimiento. -A partir de una muestra de estaciones de trabajo, observar si una herramienta de protección contra virus se ha instalado e incluye los archivos de definiciones de virus y la última vez que las definiciones se han actualizado. -Pregunte y confirme que el software de protección es de distribución central (la versión y los parches de nivel) con una configuración centralizada y el proceso de gestión del cambio. -Revisar el proceso de distribución para determinar la efectividad de la	Gerencia de TI

Continúa →

		operación. -Pregunte si y confirme que la información sobre nuevas amenazas potenciales se revisa periódicamente y es evaluada y, de ser necesario, actualizar manualmente los archivos de definición de virus. -Pregunte y confirme que el correo electrónico entrante se filtra adecuadamente contra la información no solicitada. -Revisar el proceso de filtrado para determinar la eficacia de funcionamiento, o revisar el proceso automatizado establecido para fines de filtrado.	

DS5.10 Seguridad de la Red

Objetivo de control	Factor de Riesgo	Elementos auditables	Auditado
Uso de técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.	•Incumplimiento de reglas de firewall para reflejar la política de seguridad de la organización. •Modificaciones de reglas de firewall no detectadas ni autorizadas. •Arquitectura de seguridad global	-Pregunte y confirme que una política de seguridad de la red (por ejemplo, los servicios prestados, el tráfico permitido, los tipos de conexiones permitidas) ha sido establecida y se mantiene. -Pregunte y confirme que los procedimientos y directrices para la administración de todos los componentes críticos de la red (por ejemplo, routers principales, DMZ, switches VPN) son establecidos y	Gerencia de TI

Continúa →

	en peligro. •Infracciones de seguridad no detectadas de manera oportuna.	se actualizan periódicamente por el personal clave de la administración, y los cambios que se registran y conservan documentos históricos.	
DS5.11 Intercambio de Datos Sensitivos			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Transacciones de datos sensibles se intercambian solo a través de una ruta o medio con controles, para proporcionar autenticidad de contenido, prueba de envío, prueba de recepción y no repudio del origen.	-Información sensible expuesta. -Medidas de seguridad física inadecuadas. -Conexiones no autorizadas a sitios remotos externos. -Divulgación de activos corporativos e información sensible accesible para usuarios no autorizados.	-Pregunte y confirme que la transmisión de datos fuera de la organización se ha encriptado antes de la transmisión. -Pregunte si y confirme que los datos corporativos se clasifican de acuerdo al nivel de la exposición y el esquema de clasificación (por ejemplo, confidencial y sensible). Pregunte y confirme que el procesamiento de datos sensibles es controlado a través de controles de aplicación que valida la transacción antes de la transmisión. Revisar que existan los registros de aplicación para suspensiones de procesamiento para transacciones inválidas o incompletas.	Gerente de TI

Nota Fuente: (IT Governance Institute, 2007), Pag.118, Estados Unidos

Continúa →

DS13 Administración de Operaciones

Matriz RACI DS13

Tabla 17

Matriz RACI DS13

Actividades	Funciones		
	Gerente de TI	**Analista de SS**	**Gerente Planificación**
Crear, modificar procedimientos de operación (incluyendo manuales, planes de cambios, procedimientos de escalamientos)	A/R	I	I
Monitorear la infraestructura, procesar y resolver problemas.	I	A/R	I
Administrar y asegurar la salida física de información (reportes, medios, etc.)	A/R	I	C
Aplicar cambios o arreglos al programa y la infraestructura.	I	A/R	C
Implementar y establecer un proceso para salvaguardar los dispositivos	A/R	I	C
Programar y llevar a cabo mantenimiento preventivo.	A	R	

R Responsable, **A** Rinde cuentas, **C** Consultado, **I** Informado

Nota Fuente: IT Governance Institute, COBIT® 4.1, Pag.151, Estados Unidos

Cuadro 7

Análisis Proceso DS13

DS13.1 Procedimientos e Instrucciones de Operación			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Definir, implementar y mantener procedimientos estándar para operaciones de TI y garantizar que el personal de operaciones está familiarizado con todas las tareas de operación relativas a ellos. Los procedimientos de operación deben cubrir los procesos de entrega de turno (transferencia formal de la actividad, status, actualizaciones, problemas de operación, procedimientos de escalamiento, y reportes sobre las responsabilidades actuales) para garantizar la continuidad de las operaciones.	-Errores en las operaciones debido al desconocimiento de los procedimientos estándares. -Tareas informales y desordenadas debido a la falta de procedimientos estándares. -Incapacidad para responder rápidamente a problemas o cambios operacionales.	-Evidenciar la existencia de procedimientos estándares y su aplicación en las operaciones de TI. -Identificar un procedimiento operacional para analizar la claridad del contexto. -Evidenciar si la Gerencia de TI tiene identificadas las operaciones y responsabilidades. -Evaluar que en los procedimientos operacionales estén definidos los roles y responsabilidades. -Evidenciar que los procedimientos operacionales han sido difundidos a las personas implicadas.	Gerente de TI Analista RRHH

Continúa →

DS13.2 Programación de Tareas			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Organizar la programación de trabajos, procesos y tareas en la secuencia más eficiente, maximizando el desempeño y la utilización para cumplir con los requerimientos del negocio. Deben autorizarse los programas iniciales así como los cambios a estos programas. Los procedimientos deben implementarse para identificar, investigar y aprobar las salidas de los programas estándar.	-Picos de utilización de recursos. -Problemas con los trabajos programados. -Ejecución o reinicio de trabajos programados.	-Verificar que la Gerencia de TI mantenga un registro y programación de las tareas. - Verificar que la Gerencia de TI haga un seguimiento al resultado de las tareas programadas y reprogramación de las tareas no ejecutadas. - Verificar la metodología que la Gerencia de TI utiliza para el análisis del uso de recursos para el cumplimiento de las tareas programadas.	Gerente de TI

DS13.3 Monitoreo de la Infraestructura de TI			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Definir e implementar procedimientos para monitorear la infraestructura de TI y los eventos relacionados.	-Problemas de infraestructura no detectados a tiempo y ocurrencia de incidentes. -Problemas de infraestructura que	-Verificar las operaciones con hardware -Revisar los procedimientos de administración de la capacidad -Revisar el plan de adquisición de hardware -Revisar los criterios de adquisición de computadores -Revisar los controles de administración de cambios (hardware)	Gerente de TI Analista de

Continúa →

Garantizar que en los registros de operación se almacena suficiente información cronológica para permitir la reconstrucción, revisión y análisis de las operaciones y de otras actividades involucradas en dichas operaciones.	causan impactos operacionales y en el negocio que pudieron ser prevenidos o detectados antes de su ocurrencia. -Recursos de infraestructura subutilizados.	-Verificar las operaciones con Sistemas Operativos -Revisar los procedimientos de selección del software del sistema -Revisar las actividades del mantenimiento del software -Licenciamientos -Revisiones de control operativo de redes -Verificar Planes de implementación y de prueba para el hardware y los enlaces de comunicaciones de red -Analizar el diseño de la red para asegurar que una falla de servicio tendrá un efecto mínimo -Analizar los cambios realizados al software del sistema operativo utilizado por la red y verificar si estos están siendo controlados. -Las personas sólo tienen acceso a las aplicaciones definidas para su cargo, procesadores de transacciones y conjuntos de datos autorizados. - Se han implementado políticas y procedimientos de seguridad apropiados. -Revisión de logs - Determinar consistencia del cronograma para trabajos urgentes o	Sistemas

Continúa →

		que requieren ser repetidos. - Determinar si se han identificado las aplicaciones críticas. - Determinar si se emplean procedimientos para facilitar el uso óptimo de recursos. - Determinar si la cantidad de personal es adecuada.	

DS13.4 Documentos Sensitivos y Dispositivos de Salida			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Establecer lugares adecuados, prácticas de registro y administración de inventarios sobre los activos de TI más sensitivos tales como formas, instrumentos negociables, impresoras de uso especial o dispositivos de seguridad.	- Mal uso de activos de TI sensitivos, ocasionando pérdidas financieras y otros impactos en el negocio.	-Verificar que la Gerencia de TI tenga identificados a todos los activos críticos de TI. -Verificar que el lugar de almacenamiento de los activos críticos de TI sea el adecuado. -Verificar que registros de activos críticos de TI tal como inventarios, sean los vigentes y se mantenga actualizados.	Gerente de TI

DS13.5 Mantenimiento Preventivo del Hardware			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Definir e implementar procedimientos para garantizar el mantenimiento oportuno de la	-Problemas de infraestructura que pudieron haber sido evitados o	-Verificar la existencia de un Inventario de Hardware. -Verificar si la Gerencia de TI mantiene una Planificación	Gerente de

Continúa →

infraestructura para reducir la frecuencia y el impacto de las fallas o de la disminución del desempeño.	prevenidos. -Violación a las garantías debido al incumplimiento con los cronogramas de mantenimiento.	para el mantenimiento de Hardware. -Verificar el cumplimiento de los cronogramas de mantenimiento. -Verificar si los responsables del mantenimiento son los adecuados. -Verificar si existen contratos con terceros para la ejecución de los mantenimientos en el caso de ser necesario. -Evidenciar si existe una comunicación previa a usuarios finales y clientes afectados.	TI Analista de Sistemas

Nota Fuente: (IT Governance Institute, 2007), Pag,. Estados Unidos

Continúa →

3.6.3 AI ADQUIRIR E IMPLEMENTAR

3.6.3.1 AI5 Adquirir Recursos de TI

3.6.3.1.1 Matriz RACI AI5

Tabla 18

Matriz RACI AI5

Actividades	Funciones		
	Gerente General	**Gerente de TI**	**Jefe de compras**
Desarrollar políticas y procedimientos de adquisición de TI de acuerdo con las políticas de adquisiciones a nivel corporativo	C	C	A
Establecer/mantener una lista de proveedores acreditados	I	I	A
Evaluar y seleccionar proveedores a través de un proceso de solicitud de propuesta (RFP)	I	I	A
Desarrollar contratos que protejan los intereses de la organización	I	C	A
Realizar adquisiciones de conformidad con los procedimientos establecidos	I	I	A

R Responsable, **A** Rinde cuentas, **C** Consultado, **I** Informado

Nota Fuente: (IT Governance Institute, 2007), Pag.91, Estados Unidos

Cuadro 8

Análisis Proceso AI5

AI5.1 Control de Adquisición			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Desarrollar y seguir un conjunto de procedimientos y estándares consistente con el proceso general de adquisiciones de la organización y con la estrategia de adquisición para adquirir infraestructura relacionada con TI.	-Brechas en el cumplimiento de requisitos de los proveedores. -Automatizaciones no alineadas en los planes del corto o largo plazo. -Vacíos en controles de costo.	-Procedimiento de compras a nivel de empresa. -Cumplimiento del procedimiento de compras por parte de TI en las áreas de infraestructura, licenciamiento, renovaciones.	Jefe de Compras
AI5.2 Administración de Contratos con Proveedores			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Formular un procedimiento para establecer, modificar y concluir contratos para todos los proveedores. El procedimiento debe cubrir, como mínimo, responsabilidades y obligaciones legales, financieras, organizacionales, documentales, de desempeño, de seguridad, de propiedad intelectual y responsabilidades de conclusión, así como	-Brechas entre expectativas del negocio y las capacidades del proveedor. -Costos de servicio no determinado. -Ausencia de administración de costos. -Servicios no reflejan los	-Políticas y estándares de contratos para proveedores. -Inclusión de temas legales, financieros, organizacionales, documentales, de rendimiento, de seguridad, aspectos de responsabilidad. -Definición de responsabilidades por medio de SLA's.	Jefe de Compras Gerencia de TI

Continúa →

obligaciones (que incluyan cláusulas de penalización). Todos los contratos y las modificaciones a contratos las deben revisar asesores legales.	requerimientos del negocio.		
AI5.3 Selección de Proveedores			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Seleccionar proveedores de acuerdo a una práctica justa y formal para garantizar el mejor, según los requerimientos especificados. Los requerimientos deben estar optimizados con las entradas de los proveedores potenciales.	-Inadecuada selección de proveedores. -Apoyo insuficiente para el logro de los objetivos de la organización. -Brechas entre las capacidades y requisitos de proveedor.	-Existencia de proceso de selección de proveedores. -Criterios de pedido de compras definidos. -Para adquisición de software revisar los derechos y obligaciones en cuanto a garantías, mantenimientos, actualizaciones. -Para adquisición de hardware determinar la existencia de definiciones en SLA's, procedimientos de mantenimiento, controles de acceso, seguridad, rendimiento, condiciones de pago y procedimientos de arbitraje. -Determinar los términos legales en cuanto a licenciamiento y propiedad intelectual.	Jefe de Compras Gerencia de TI Legal

Continúa →

AI5.4 Adquisición de Recursos de TI			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Proteger y hacer cumplir los intereses de la organización en todo los contratos de adquisiciones, incluyendo los derechos y obligaciones de todas las partes en los términos contractuales para la adquisición de software, recursos de desarrollo, infraestructura y servicios.	-Actualizaciones de software no disponibles cuando se necesita. -Software incapaz de soportar los procesos de negocio. -Cambios en las aplicaciones no pueden ser aplicados como se esperaba. -Sistema propenso a problemas e incidentes, causando las interrupciones del servicio.	-Determinar si todos los acuerdos y procedimiento de compras son cumplidos. -Revisar un grupo representativo de procesos de compra de software, que contemple licenciamiento y propiedad intelectual, mantenimiento, garantías y actualización. -Revisar si los parámetros de calidad y recepción de compras se han establecido y son utilizados y determinar si el proceso se lleva a cabo antes de que se efectúen los pagos. -Verificar si todas las adquisiciones de hardware y software son registradas. -Realizar una revisión de los procedimientos para verificar su cumplimiento. -Evidenciar si las adquisiciones han sido revisadas y aprobadas por las instancias adecuadas y si cumplen con los términos legales.	Gerencia de TI Jefe de Compras Control Interno

Nota Fuente: (IT Governance Institute, 2007), Pag.90, Estados Unidos

Continúa →

3.6.4 ME MONITOREAR Y EVALUAR

3.6.4.1 ME1 Monitorear y Evaluar el desempeño de TI

3.6.4.2 Matriz RACI ME1

Tabla 19

Matriz RACI ME1

Actividades	Funciones		
	Gerente General	**Gerente de TI**	**Gerente Planificación**
Establecer el enfoque de monitoreo.	A	R	C
Identificar y recolectar objetivos medibles que apoyen a los objetivos del negocio.	C	A/R	
Crear cuadro de mandos.		A/R	
Evaluar el desempeño.		A/R	
Reportar el desempeño.	I	A/R	I
Identificar y monitorear las medidas de mejora del desempeño.		A/R	C

R Responsable, **A** Rinde cuentas, **C** Consultado, **I** Informado

Nota Fuente: (IT Governance Institute, 2007), Pag.155, Estados Unidos

Continúa →

Cuadro 9

Análisis *Proceso ME1*

ME1.1 Enfoque de Monitoreo			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Establecer un marco de trabajo de monitoreo y un enfoque que definan el alcance, la metodología y el proceso a seguir para medir la solución y la entrega de servicios de TI. Integrar el marco de trabajo con el sistema de gestión del desempeño corporativo.	-Reportes de rendimiento, basados en datos desactualizados, inadecuados o irreales. -Indicadores de rendimiento no alineados con requerimientos del negocio. -Identificación no adecuada de las necesidades del negocio y expectativas del cliente.	-Evidenciar que la Gerencia de TI haya definido un marco de trabajo para monitoreo del desempeño. -Evidenciar que se hayan diseñado y se estén utilizando reportes para medición del desempeño. -Analizar la información utilizada para emitir los reportes de desempeño de TI. -Evidenciar la existencia de indicadores de desempeño de TI y que estos se encuentran alineados con las necesidades de la Dirección. -Realizar una entrevista al cliente interno sobre el desempeño de TI.	Gerente General Gerente de TI Usuarios
ME1.2 Definición y recolección de datos de monitoreo			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Trabajar con el negocio para definir un conjunto balanceado de objetivos de desempeño y tenerlos aprobados por el negocio y otros interesados.	-Indicadores basados en objetivos que no están alineados con los del negocio.	-Evidenciar que se hayan definido los objetivos de desempeño y que estos sean conocidos y aprobados por la Gerencia General.	Gerente de TI

Continúa →

Medir los objetivos. Se deben establecer procesos para recolectar información oportuna y precisa para reportar el avance contra las metas.	-Indicadores basados en datos incompletos o erróneos	-Verificar que los indicadores mantengan relación con los objetivos de desempeño.	
ME1.3 Método de Monitoreo			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Garantizar que el proceso de monitoreo implante un método (Ej. Balanced Scorecard), que brinde una visión sucinta y desde todos los ángulos del desempeño de TI y que se adapte al sistema de monitoreo de la empresa.	-Necesidades y expectativas del negocio no son conocidas. -Decisiones incorrectas basadas en información de rendimiento no confiable.	-Evidenciar de que exista una relación entre procesos críticos de TI, sistemas de monitoreo y reportes de desempeño. -Reportes de desempeño completo y legible.	Gerente de TI
ME1.4 Evaluación del desempeño			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Comparar de forma periódica el desempeño contra las metas, realizar análisis de la causa raíz e iniciar medidas correctivas para resolver las causas subyacentes.	-Pérdida de oportunidades para mejora. -Rendimiento efectivo no reconocido, staff desmotivado.	-Realizar entrevista a usuarios finales para evidenciar si se han realizado recomendaciones de desempeño y estas han sido tomadas en cuenta. -Evidenciar que resultados negativos en los reportes de desempeño se gestionan por medio de acciones correctivas.	Gerente de TI Usuarios

Continúa →

ME1.5 Reportes al Consejo Directivo y a Ejecutivos			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Proporcionar reportes administrativos para ser revisados por la alta dirección sobre el avance de la organización hacia metas identificadas, niveles de servicio de programas individuales y la contribución de TI a ese desempeño	-Gerencia insatisfecha con el rendimiento de TI. -Desconexión entre Gerencia y TI. -Incapacidad para dirigir y controlar las principales actividades de TI.	-Evidenciar que los reportes ejecutivos de desempeño son diseñados de acuerdo a las necesidades de la Dirección y si son revisados frecuentemente por la misma. -Evidenciar que los reportes son aprobados por la Dirección.	Gerente General Gerente de TI
ME1.6 Acciones Correctivas			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Identificar e iniciar medidas correctivas basadas en el monitoreo del desempeño, evaluación y reportes. Esto incluye el seguimiento de todo el monitoreo, de los reportes y de las evaluaciones con: •Revisión, negociación y establecimiento de respuestas de administración.	-Incidentes debido a problemas no resueltos. -Bajo rendimiento de TI. -Medición del rendimiento no tomado seriamente.	-Evidenciar que existe un procedimiento para la gestión de acciones correctivas en lo que respecta al desvío de los objetivos de desempeño. -Evidenciar que se tienen asignados responsables para el cumplimiento de las acciones correctivas y que se establecen cronogramas de cumplimiento. -Evidenciar que se realizan seguimiento a los	Gerente de TI

Continúa →

•Asignación de responsabilidades por la corrección. •Rastreo de los resultados de las acciones comprometidas.		resultados de las acciones correctivas. -Evidenciar una acción correctiva implementada como resultado de un bajo rendimiento de desempeño.	

Nota Fuente: (IT Governance Institute, 2007), Pag.154, Estados Unidos

Continúa →

3.6.4.3 ME3 Garantizar el Cumplimiento con Requerimientos Externos

3.6.4.3.1 Matriz RACI ME3

Tabla 20

Matriz RACI ME3

Actividades	Funciones			
	Dpto. Legal	**Gerente General**	**Gerente de TI**	**Comité**
Definir y ejecutar un proceso para identificar los requerimientos legales, contractuales de políticas y regulatorios.	R	I	A	C
Evaluar el cumplimiento de actividades de TI con políticas, estándares y procedimientos de TI.			R/A	I
Brindar retroalimentación para alinear las políticas, estándares y procedimientos de TI con los requerimientos de cumplimiento.	C		A/R	I
Integrar los reportes de TI sobre requerimientos regulatorios con similares provenientes de otras funciones del negocio.	C		A/R	

R Responsable, **A** Rinde cuentas, **C** Consultado, **I** Informado

Nota Fuente: (IT Governance Institute, 2007), Pag.163, Estados Unidos

Continúa →

Cuadro 10

Análisis Proceso ME3

ME3.1 Identificar los Requerimientos de las Leyes, Regulaciones y Cumplimientos Contractuales			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Identificar, sobre una base continua, leyes locales e internacionales, regulaciones, y otros requerimientos externos que se deben cumplir para incorporar en las políticas, estándares, procedimientos y metodologías de TI de la organización.	-Incumplimiento de las leyes o regulaciones relevantes. -Potenciales riesgos de pérdidas financieras y penalidades no identificadas. -Pérdida de clientes e insatisfacción de los socios del negocio. -Disputas con clientes y proveedores. -Incremento del riesgo de continuidad del negocio por sanciones impuestas.	Evidenciar la existencia de un inventario de aspectos legales. -Evidenciar que en los procedimientos de TI se incluya el manejo de los requerimientos legales, regulatorios y contractuales. -Evidenciar una forma de priorización de los requerimientos de acuerdo a su importancia, frecuencia e impacto. -Evidenciar que se realiza una revisión frecuente de los incumplimientos y las sanciones.	Dpto. Legal Gerencia de TI

Continúa →

ME3.2 Optimizar la Respuesta a Requerimientos Externos			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Revisar y ajustar las políticas, estándares, procedimientos y metodologías de TI para garantizar que los requisitos legales, regulatorios y contractuales son direccionados y comunicados.	- Personal no comunicado en las prácticas y procedimientos para el cumplimiento con requerimientos legales y regulatorios.	- Evidenciar que en las políticas, procedimientos se definan hitos para el cumplimiento de las leyes, requerimientos regulatorios y contractuales.	Gerencia de TI Usuarios
ME3.3 Evaluación del Cumplimiento con Requerimientos Externos			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Confirmar el cumplimiento de políticas, estándares, procedimientos y metodologías de TI con requerimientos legales y regulatorios.	-Pérdidas financieras y sanciones -No cumplimiento genera incidentes graves impactando en el rendimiento y reputación de la empresa.	-Evidenciar que hayan existido sanciones o pérdidas financieras ocasionadas por el incumplimiento legal o regulatorio de TI, verificar que se hayan tomado medidas correctivas.	Gerencia General

Continúa →

ME3.4 Aseguramiento Positivo del Cumplimiento			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Obtener y reportar garantía de cumplimiento y adhesión a todas las políticas internas derivadas de directivas internas o requerimientos legales externos, regulatorios o contractuales, confirmando que se ha tomado cualquier acción correctiva para resolver cualquier brecha de cumplimiento por el dueño responsable del proceso de forma oportuna.	-Acciones correctivas no administradas a tiempo, impactando en el rendimiento de la organización.	-Evidenciar un inventario de requerimientos regulatorios y de cronogramas de revisión. -Evidenciar la existencia de un procedimiento para el cumplimiento de requerimientos legales y regulatorios por parte de terceros. -Evidenciar el cumplimiento de leyes y regulaciones por parte de proveedores. -Verificar la existencia de una base de datos que registre contratos y proveedores u otro medio de almacenamiento. -Evidenciar el monitoreo y reporte de no cumplimiento de leyes, regulaciones y compromisos contractuales.	Dpto. Legal Gerencia de TI

ME3.5 Reportes Integrados			
Objetivo de control	**Factores de riesgo**	**Elementos auditables**	**Auditado**
Integrar los reportes de TI sobre requerimientos legales, regulatorios y contractuales con las	- Otras funciones de negocio no conocen de los requerimientos de	- Analizar reportes corporativos para evidenciar que constan los requerimientos legales y regulatorios de	Gerente de TI

Continúa →

salidas similares provenientes de otras funciones del negocio.	cumplimiento de los procesos de TI	TI. - Evidenciar la consistencia de los reportes de TI con los reportes corporativos.	

Nota Fuente: (IT Governance Institute, 2007), Pag.162, Estados Unidos

Continúa →

3.6.4.4 ME4 Proporcionar Gobierno de TI

3.6.4.4.1 MATRIZ RACI ME4

Tabla 21

Matriz RACI ME4

Actividades	Funciones		
	Gerente General	**Gerente de TI**	**Gerente de Planificación**
Establecer visibilidad y facilitación del consejo y de los ejecutivos hacia las actividades de TI	R	C	A
Revisar, avalar, alinear y comunicar el desempeño de TI, la estrategia de TI, el manejo de recursos y riesgos de TI con respecto a la estrategia empresarial	R	C	A
Crear un cuadro de mando integral de TI		A/R	I
Resolver los hallazgos de las evaluaciones independientes y garantizar la implantación por parte de la gerencia de las recomendaciones acordadas	R	A/C	I
Generar un reporte de gobierno de TI	I	A/R	I

R Responsable, **A** Rinde cuentas, **C** Consultado, **I** Informado

Nota Fuente: (IT Governance Institute, 2007), Pag.167, Estados Unidos

Cuadro 11

Análisis Proceso ME4

ME4.1 Establecimiento de un Marco de Gobierno de TI			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Definir, establecer y alinear el marco de gobierno de TI con la visión completa del entorno de control y Gobierno Corporativo. Basar el marco de trabajo en un adecuado proceso de TI y modelo de control y proporcionar la rendición de cuentas y prácticas inequívocas para evitar una rotura en el control interno y la revisión. Confirmar que el marco de gobierno de TI asegura el cumplimiento con las leyes y regulaciones y que está alineado, y confirma la entrega de, la estrategia y objetivos empresariales. Informa del estado y cuestiones de gobierno de TI.	-Responsabilidades y rendición de cuentas ineficaces para los procesos de TI. -Los servicios de TI fallan en apoyar los objetivos y estrategias de la empresa. -Acciones correctivas para mantener y mejorar los procesos de TI no identificados ni implementados. -Los controles no funcionan como se esperaba.	Preguntar y confirmar que: -Un proceso acordado existe para alinear el marco de gobierno de TI con el gobierno de la empresa en general y control interno. -Exista una adecuada estructura de administración de gobierno, tales como el comité de estrategia de TI, comité directivo, consejo de la tecnología, la arquitectura y la junta de revisión del comité de auditoría de TI. Verificar que los términos de referencia existen para cada uno de estos.	Gerencia de TI

Continúa →

Objetivo de control	Factor de Riesgo	Elementos auditables	Auditado
Facilitar el entendimiento del consejo directivo y de los ejecutivos sobre temas estratégicos de TI tales como el rol de TI, características propias y capacidades de la tecnología. Trabajar con el consejo directivo para definir e implementar organismos de gobierno, tales como un comité estratégico de TI, para brindar una orientación estratégica a la gerencia respecto a TI, garantizando así que tanto la estrategia como los objetivos se distribuyan en cascada hacia las unidades de negocio y hacia las unidades de TI y que se desarrolle certidumbre y confianza entre el negocio y TI. Facilitar la alineación de TI con el negocio en lo referente a estrategia y operaciones.	-Asignación y gestión de las inversiones de TI ineficaces. -TI falla en apoyar los objetivos de la empresa. -Plan estratégico de TI no alineado con la estrategia global corporativa. -Direcciones de TI no definidas y no apoyan los objetivos del negocio.	-Inspeccionar la documentación estratégica de TI y evaluar si es compatible con la orientación proporcionada por la junta / alta dirección. Debe reflejar las estrategias de negocio y de TI la alineación adecuada de las operaciones comerciales. -Determinar si el proceso de planificación estratégica de TI incluye la participación de las operaciones comerciales y demuestra la alineación con las estrategias y objetivos de negocio. -Revisar los documentos de estrategia de TI y evaluar si se incluyen los principios rectores del negocio, cómo se monitorea la infraestructura y las aplicaciones de TI, cuál es la contribución potencial de TI con la estrategia general del negocio.	Gerencia de Planificación

Continúa →

ME 4.3 Entrega de Valor			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Administrar los programas de inversión, activos y servicios de TI, para asegurar que ofrecen el mayor valor posible para apoyar la estrategia y los objetivos empresariales. Asegurar que se generen casos de negocio integrales y consistentes, y que los aprueben los interesados, que los activos y las inversiones se administren a lo largo del ciclo de vida económico, y que se lleve a cabo una administración activa tal como: la contribución a nuevos servicios, ganancias de eficiencia y un mejor grado de reacción a los requerimientos de los clientes. Implementar un enfoque disciplinado de la administración del portafolio, programa y proyecto, enfatizando que el negocio asume la propiedad de todas las inversiones habilitadas con	-Inversiones de TI mal orientadas. -Valor no obtenido de los activos y servicios de TI. -Disminución de la satisfacción del cliente. -Beneficios esperados no realizados. -Aumento de los costos en las inversiones y operaciones. -Falta de alineación entre los objetivos del negocio y la arquitectura de TI	-Confirmar que existe la co-responsabilidad entre el negocio y TI para todas las inversiones en TI. -Determinar si existe un proceso para identificar y evaluar periódicamente la forma de aumentar la contribución del valor, gestionando las expectativas empresariales y de los ejecutivos con respecto a las tecnologías emergentes (por ejemplo, reuniones del comité directivo). -Determinar si existe una asociación entre la empresa y los proveedores de TI, con la responsabilidad compartida de las decisiones de aprovisionamiento. -Determinar si existe un proceso efectivo para asegurar que la arquitectura de TI está diseñada para obtener el máximo valor. -Determinar si existe un proceso eficaz para ajustar las inversiones sobre la base de un balance de riesgos,	Gerencia de Planificación Gerencia de TI

Continúa →

TI y que TI garantiza la optimización de los costos por la prestación de los servicios y capacidades.		costos y beneficios con los presupuestos y estos ajustes son aceptables obteniendo aspectos competitivos de las inversiones en TI. -Inspección de la documentación de TI para evaluar si la empresa ha establecido las expectativas sobre el contenido de las prestaciones de TI, incluyendo los requisitos de la reunión de negocios, la flexibilidad para adoptar las futuras necesidades, los tiempos de respuesta y, facilidad de uso, la seguridad y la integridad, exactitud y actualidad de la información. -Determinar que la administración de los activos de TI cuenta con un proceso de gestión y envía informes sobre los costos reales y el retorno de la inversión.	
ME 4.4 Administración de Recursos			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Revisar inversión, uso y asignación de los activos de TI por medio de evaluaciones periódicas de las	-Infraestructuras fragmentadas e ineficientes.	-Preguntar y confirmar que los recursos de TI son apropiados, los servicios e infraestructura están	Gerencia de Planificación

Continúa →

operaciones de TI para asegurar recursos y alineamiento apropiados con los objetivos estratégicos y los imperativos del negocio.	-Insuficientes recursos y capacidades para alcanzar las metas propuestas. -Objetivos estratégicos no alcanzados. -Prioridades inadecuadas empleadas para asignar recursos.	disponibles para satisfacer los objetivos estratégicos y que políticas se han establecido para permitir la disponibilidad de los servicios de TI. -Revisar las políticas, procedimientos y procesos establecidos para la gestión de recursos, y verificar que están operando de manera efectiva. -Establecer las prioridades del negocio para que los recursos se asignen para facilitar una eficaz desempeño de TI. -Preguntar y confirmar que la infraestructura de TI facilita la creación y el intercambio de información de negocios a un coste óptimo. -Rastrear elementos a través de las infraestructuras de TI y determinar si la creación y el intercambio de información se realizan con eficacia. -Preguntar y confirmar que las funciones críticas son asignadas y definidas para obtener el máximo valor de TI con personal y recursos apropiados. -Revisar la definición de roles y que estas sean	Gerencia de TI Gerencia de RRHH

Continúa →

		efectivamente asignadas y ejecutadas. -Preguntar y confirmar que los procedimientos para la evaluación de la capacidad se han establecido.	
ME 4.5 Administración de Riesgos			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Trabajar con el consejo directivo para definir el nivel de riesgo de TI aceptable por la empresa y obtener garantía razonable, que las prácticas de administración de riesgos de TI son apropiadas para asegurar que el riesgo actual de TI no excede el riesgo aceptable de la dirección. Introducir las responsabilidades de administración de riesgos en la organización, asegurando que el negocio y TI regularmente evalúan y reportan riesgos relacionados con TI y su impacto y que la posición de los riesgos de TI de la empresa es transparente a los interesados.	-Riesgos identificados o mal administrados. -Aumento de los gastos y costes para administrar riesgos imprevistos. -Falla de aplicaciones y servicios críticos de TI. -Falta de responsables sobre los riesgos de TI.	Confirmar que: -La gerencia general evalúa los riesgos de TI y costos asociados. -La gerencia general revisa los resultados de los controles implementados para mitigar los riesgos, teniendo en cuenta los controles de mitigación en el lugar. -Existe un proceso para incluir los riesgos de TI en la gestión de gobierno de TI.	Gerencia General

Continúa →

ME 4.6 Medición del Desempeño			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Confirmar que los objetivos de TI se han conseguido o que el progreso hacia las metas de TI cumple las expectativas. Donde los objetivos no se han alcanzado o el progreso no es el esperado, revisar las acciones correctivas de gerencia. Informar a la dirección los programas y desempeños de TI, soportados por informes para permitir a la alta dirección revisar el progreso de TI hacia las metas identificadas.	•Brechas de rendimiento no identificadas de manera oportuna. •Disminución de la confianza de los interesados. •Desviaciones y degradaciones de servicio no reconocido, resultando en inconvenientes de entrega a los requerimientos del negocio. •Fallos de rendimiento del servicio provocando riesgos de cumplimiento legal y normativo.	Preguntar y confirmar que: -El desempeño de TI se alinea correctamente con las medidas de Balanced Scorecard y se registra su medición. -Verificar que los informes incluyen la medida en que los objetivos previstos se han alcanzado y los resultados se han obtenido. -El Consejo evalúa las acciones correctivas en caso de problemas en el rendimiento y proporciona una dirección para corregir las causas.	Gerencia de Planificación
ME 4.7 Aseguramiento Independiente			
Objetivo de control	**Factor de Riesgo**	**Elementos auditables**	**Auditado**
Garantizar de forma independiente (interna o	-Daños en reputación debido al	-Verificar la existencia de un comité de auditoría. -Entrevista al comité de auditoría y evaluar su	Gerencia de

Continúa →

externa) la conformidad de TI con la legislación y regulación relevante; las políticas de la organización, estándares y procedimientos; practicas generalmente aceptadas; y la efectividad y eficiencia del desempeño de TI.	fracaso para detectar o prevenir fallas en el servicio. -Ineficaz control de TI, administración de riesgos y mecanismos de control interno. -Comportamientos antiético aprobado y aceptado.	conocimiento y conciencia de sus responsabilidades. -Pregunte si y confirme que se han realizado revisiones independientes, certificaciones o acreditaciones de cumplimiento de las políticas, normas y procedimientos. -Inspeccionar físicamente la adecuación de los documentos producidos por las revisiones independientes.	TI

Nota Fuente: (IT Governance Institute, 2007), Pag.166, Estados Unidos

Continúa →

4 CAPITULO IV

DESARROLLO DE LA AUDITORIA

4.1 Metodología

Una vez detallados los elementos auditables, se realizará una evaluación del cumplimiento de los mismos utilizando diferentes métodos de recopilación de información que incluyen: entrevistas, observaciones de actividades y revisión de documentos. Estas actividades se efectuarán en cada uno de los objetivos de control seleccionados en el capítulo II, permitiendo, al final, obtener el nivel de madurez actual de los procesos de TI.

En base a esto se presentará un resumen con la información obtenida en la auditoría y seguidamente se analizará el nivel de madurez actual de la empresa para cada objetivo de control.

Adicionalmente, se establecerá el nivel de madurez de la industria para los procesos seleccionados en la auditoría, para ello se realizará una encuesta a las principales empresas petroleras y de servicios petroleros tales como:

Petroamazonas, Udss Specialized Services Ecuador S.A., Halliburton, Ivanhoe Energy Ecuador Inc, Qmax Ecuador.

Para el desarrollo de la auditoría se ha establecido una hoja de trabajo – "Guía de Verificación" que servirá de guía para el auditor en donde se registrarán los elementos auditables del proceso, el cargo de la persona a ser auditada, los documentos revisados, las observaciones del auditor y la fecha en que se realiza la auditoría.

4.2 Objetivos del Capítulo

- Auditar los procesos establecidos tomando en cuenta la metodología Cobit 4.1.

- Medir los procesos seleccionados a través de las métricas sugeridas por Cobit, con el objetivo de tener una valoración del desempeño de TI.
- Determinar el nivel de madurez de la industria.
- Determinar el nivel de madurez de los procesos analizados en base a la evidencia obtenida en el proceso de auditoría.

4.3 Resultado de la Auditoría

A continuación se presenta el resultado de la auditoría para cada uno de los procesos seleccionados:

4.3.1 PO PLANEAR Y ORGANIZAR

4.3.1.1 PO1 Definir un Plan Estratégico de TI

Cuadro 12

Análisis Proceso PO1

PO1.1 Administración del Valor de IT				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Verificar si la empresa dispone de un proceso para la creación de casos de negocio. -Verificar que el proceso de casos de negocio tenga definidas las entradas/salidas, métricas, recursos y cuente con un proceso de administración de cambios. -Revisar casos de negocio anteriores para verificar desviaciones (costo, tiempo, personal). -Identificar si en el estudio del caso de negocio se han efectuado comparaciones con	Gerencia de TI	-Documentos de casos de negocio. -Archivo de casos de negocio. -Casos de negocio anteriores.	-De la revisión de los procesos de tecnología se evidencia, la existencia de un proceso para la creación de casos de negocio en los proyectos de tecnología mayores a $10000. -El proceso contempla responsable, objetivo, alcance, presupuesto, cronograma y análisis de riesgos así como de versionamiento para control de cambios. -Para los casos de negocio revisados se determina que se emplean los estándares de acuerdo al proyecto sin incluir SLA's. -Existen 2 casos en fase de inicio y 1 caso ejecutándose con retrasos en cronograma y en recursos debido a cortes de	27/08/2012

Continúa →

estándares técnicos, de la industria, SLA's.			presupuestos y reformulación del alcance. -Se revisó los casos de negocio: Implementación de Solución Blade e Implementación de solución de Telefonía IP la correcta documentación y aprobación.	
PO1.2 Alineación de TI con el Negocio				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Evidenciar como se comunican los requerimientos del negocio hacia el área de TI. -Identificar cómo se involucra la administración de TI en los objetivos del negocio. - Evidenciar si se han definido los procesos críticos del negocio que dependen de TI.	Gerencia de Planificación. Gerencia de TI.	-Balanced Scorecard, Presupuesto Anual General, Documento de Hitos y cronogramas. -Documentos de procesos de la empresa.	-Se evidencia que en el Balanced Scorecard (Anexo 3) se involucra a TI en la estrategia negocio, con revisiones mensuales y evaluación anual. - Se evidencia la existencia de un Presupuesto Anual de TI (Anexo 4) detallando la inversión, mantenimientos y gastos operativos. - El documento de hitos y cronogramas (Anexo 2) detalla los proyectos a realizar en el año y el avance en porcentaje, permite un adecuado control de los proyectos asignados.	27/08/2012

Continúa →

PO1.3 Evaluación de Desempeño Actual				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Verificar si existe un sistema de evaluación de desempeño de la gestión de TI. -Verificar si existe un plan de acción para desviaciones o variaciones de planes propuestos. -Verificar si están identificados procesos críticos de tecnología que soporten al negocio. -Identificar si se han analizado las fortalezas y debilidades de estos procesos, su funcionalidad, grado de automatización del negocio, estabilidad, complejidad, alineamiento tecnológico, requerimientos de soporte y mantenimiento entre otros. -Verificar si existe una revisión de los objetivos para verificar su cumplimiento. -Verificar si existe un comparativo de	Gerencia de Planificación Gerencia de TI	-Documento de Hitos y cronogramas y BSC. -Documento de procesos de TI.	-Se evidencia la existencia de dos mecanismos de evaluación: Programas de Actividades de TI&C con Hitos y Cronogramas (Anexo 2) y la revisión del BSC. -Si existe un plan de acción de los proyectos del área de tecnología en el que se verifica el cumplimiento de los hitos y cronogramas y se revisa las causas de incumplimiento y de requerir ajustes en tiempo o en finanzas se procede a reajustarlos. -No se puede evidenciar la existencia de un análisis FODA de los procesos de TI ni del grado de automatización del negocio. -Si se encuentran identificados los procesos críticos de TI que soportan al negocio mediante la cadena de valor de Porter. -Se evidencia la revisión de los objetivos mensualmente debido al cumplimiento con el Balanced Scorecard y los	27/08/2012

Continúa →

estándares de tecnología utilizado dentro del sector en el que se encuentra.			resultados ingresados en el sistema Strategic para ser analizados por la dirección, se generan ajustes en casos necesarios luego de la aprobación de la dirección. -No se evidencia un análisis de los estándares utilizados en otras empresas dentro del sector.	
PO1.4 Plan Estratégico de TI				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Averiguar sobre el proceso de formulación de objetivos y metas de TI (definido, documentado y comunicado). -Evidenciar logros y administración de riesgos de TI. -Evidenciar rendimiento actual y futuro de las expectativas del negocio. -Verificar que las políticas y procedimientos provean sustento al plan estratégico de TI. -Evidenciar la existencia de métricas y que los objetivos de TI se relacionen con los objetivos	Gerencia de TI	-Presupuesto Anual General del año 2012. -Documento de riesgos. -Documento de hitos y cronogramas. -BSC -Política de TI	-El proceso de formulación de objetivos y metas se genera en la planificación del Presupuesto Anual General (PAG) que se realiza en septiembre de cada año y se enlaza con objetivos y metas del Balanced Scorecard en el mes de Febrero por lo que existe una brecha en el objetivo general creado por la planificación presupuestaria y la del negocio. -La administración de riesgos se maneja con la matriz de riesgos (Anexo 5) que los identifica y cuantifica y propone proyectos para eliminarlos, mitigarlos o mantenerlo. Como logros está la disminución de riesgos	27/08/2012

Continúa →

del negocio. -Evidenciar la existencia de un plazo para el desarrollo de los planes estratégicos y tácticos.			en sistemas de respaldos y en enlaces de comunicaciones mejorados y con redundancia. -Se revisaron 2 proyectos de infraestructura: Implementación de Solución Blade e Implementación de Telefonía IP, los que cumplieron con los cronogramas de implementación y cierres además existe seguimiento a los proyectos anuales y se han presentado proyectos para el próximo año. -Se evidencia los plazos para los planes tácticos en el documento Hitos y cronogramas. El plan estratégico de TI no está definido. -Se evidencia que el porcentaje de participación de TI en los objetivos del negocio es del 2% y se mide en el software Strategic. -Existen algunas políticas de TI, falta crear nuevas políticas y actualizar las existentes. -No se evidencia la existencia de procedimientos operacionales.	

Continúa →

PO1.5 Planes Tácticos de TI				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Verificar la existencia de un plan táctico de TI basado en un plan estratégico de TI. -Verificar que se lo lleve a cabo de una manera estructurada para evitar demoras en su ejecución. -Verificar las definiciones de proyectos, planificación, los resultados y beneficios estimados. -Revisar los riesgos asociados en TI.	Gerencia de TI	-Documento de hitos y cronogramas. -Matriz de riesgos.	-Existen planes tácticos actualizados que cubren áreas específicas de TI pero no existe un plan estratégico que englobe a los planes tácticos. -El plan táctico está detallado y estructurado con controles en la ejecución y ajustes en caso de requerirlo previa justificación -Los proyectos se han ejecutado sin una gestión adecuada de proyectos, por lo que la información está dispersa, sin controles ni responsable así como inexistencia de documentación. -Existe la evaluación de riesgos de TI que es un documento que debe ser actualizado anualmente pero en la revisión efectuada está desactualizado.	27/08/2012

Continúa →

PO1.6 Administración del Portafolio de TI				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Evidenciar la formalización de un proceso de identificación y priorización de programas y proyectos de TI que soporten el plan táctico de TI. -Verificar si las metas de negocio y sus resultados están documentados y existen los recursos económicos y requeridos para llevarlos a cabo. -Verificar que los programas / resultados de los proyectos se comuniquen debidamente a todas las partes interesadas.	Gerencia de TI Gerencia de Planificación	-Presupuesto Anual General. -Balanced Scorecard, sitio web de Strategic	-No se puede evidenciar la existencia de un proceso que genere la formalización de programas y proyectos pero se lo realiza de manera ad-hoc ya que la formulación de proyectos está asociado con la generación del presupuesto anual, pero no se enlaza con el de hitos y cronogramas que es un desglose de proyectos a nivel mensual y está desfasada en función del tiempo. -Las metas del negocio son definidas a inicios de año para integrarlas en el Balanced Scorecard e ingresadas en el sistema Strategic como resultado del plan estratégico, los recursos económicos y requeridos son gestionados por cada área y medidos por el presupuesto. -No se han comunicado los resultados de los proyectos a las partes interesadas por lo que no se ha visualizado el aporte de los proyectos a la organización.	27/08/2012

Continúa →

INDICADORES DE DESEMPEÑO

Tabla 22

Indicadores de Desempeño PO1

INDICADORES AÑO 2012	PORCENTAJE
% Cumplimiento BSC Enap Sipetrol / Hitos y Cronogramas	82%
% de objetivos de TI incorporados en el BSC	2%
% de proyectos de TI que cumplen con el Plan táctico del Negocio	30%
% de proyectos de TI incluidos en el plan táctico de TI	100%
% de cumplimiento en la actualización del BSC y planes tácticos de TI en el sistema Strategic	100 %
% de reuniones de planeación estratégica de TI con Directivos del Negocio	0%
% de proyectos de TI dirigidos por los Directivos del negocio	0%

Nota Fuente: (IT Governance Institute, 2007), Pag.31, Estados Unidos

Continúa →

4.3.1.2 PO4 Definir los Procesos, Organización y Relaciones de TI

Cuadro 13

Análisis *Proceso PO4*

PO4.1 Marco de Trabajo de Procesos de TI				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Evidenciar si existen procesos de TI identificados y definidos en cuanto a responsables, recursos, controles. -Evidenciar si existen procesos del negocio identificados con entradas y salidas definidas. -Modelo de gestión de TI con metas definidas, control de metas, indicadores y modelo de madurez.	Gerencia de TI	-Documento de procesos de TI. -Documento de los procesos de la empresa. -Documento de hitos y cronogramas.	-Se han identificado los procesos principales de tecnología, pero no existe detalle de responsables así como de los recursos necesarios para que se cumplan, ni de los controles adecuados. -Los procesos están identificados, no contienen las entradas ni las salidas lo cual no proporciona una información útil de que insumos emplea ni qué resultados proporciona. -El modelo de gestión de TI actualmente dispone de metas definidas a ser cumplidas de acuerdo a un cronograma definido con indicadores de cumplimiento pero no disponen de un nivel de madurez detectado.	03/09/2012

Continúa →

PO4.2 Comité Estratégico de TI				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Evidenciar la conformación de un comité de estrategia para TI. -Evidenciar las cualidades y capacidades de los miembros del comité. -Evidenciar la periodicidad de las reuniones del comité. -Evidenciar recomendaciones proporcionadas a la organización.	Gerencia General Gerencia de RRHH	-Cronograma -Documento de roles y funciones	-Existe un comité de estrategia a nivel de negocio pero no a nivel específico de TI, por lo que no está representada el área de TI en el directorio de la empresa. -No se han definido las características y conocimientos del personal para que integre este comité. -No existen actas de reuniones. -No se han generado recomendaciones a este nivel.	03/09/2012
PO4.3 Comité Directivo de TI				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Evidenciar la conformación de un comité de dirección de TI. -Averiguar por medio de actas de reuniones si los temas planteados aportan a la organización en cuanto al alineamiento de TI con el plan estratégico.	Gerencia General Gerencia de Planificación	-Integrantes del comité. -Actas de reuniones	-No existe un comité estratégico de TI y no está contemplado la generación de un comité de dirección de TI.	03/09/2012

Continúa →

PO4.4 Ubicación Organizacional de la Función de TI				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Verificar la existencia de descripción de funciones del responsable de TI. -Evidenciar la independencia de funciones del área de TI del resto de áreas de la organización. -Asignación de recursos para el desempeño adecuado de las funciones de TI (presupuesto, personal, soporte, etc.).	Asistente de RRHH Gerencia de TI	-Metodología Mercer (documentos confidenciales) -Organigrama General -Presupuesto Anual General	-La descripción de funciones de acuerdo a la herramienta Mercer excede el número de procesos recomendado para la posición llegando a 9 procesos cuando el estándar recomienda un máximo de 6 por lo que la posición esta con una carga de responsabilidades y obligaciones. -La asignación de recursos se la hace anualmente y en base al Presupuesto enviado por el jefe de área con un promedio de $600.000 dólares anuales. -En el organigrama general (Anexo 7) se evidencia que el área de TI está bajo el área de Proyectos, se encuentra completo y actualizado.	03/09/2012

PO4.5 Estructura Organizacional				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Verificar la capacidad de respuesta de acuerdo a cambios organizacionales y como estos cambios afectan a la organización.	Gerencia General Gerencia	-Organigrama y sus versiones -Revisión de	-No se ha contemplado un mecanismo de medición para la capacidad de repuesta en caso de cambios organizacionales. -Se evidencia la revisión de acuerdos con terceros para	03/09/2012

Continúa →

-Verificar los acuerdos con terceros y con servicios de TI alineados a las necesidades del negocio	de contratos	contratos (documentos confidenciales)	modificación de los servicios cuando el negocio lo requiere regulados dentro de los contratos por medio de la generación de anexos que amplían o modifican los servicios.	
PO4.6 Establecimiento de Roles y Responsabilidades				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Evidenciar si las áreas de TI se encuentran identificadas, formalizadas y son actualizadas ante un cambio. -Verificar si existe una definición de roles y funciones de TI de acuerdo a las tareas. -Verificar las adecuadas delegaciones y responsabilidades que se han asignado a dichos roles. -Verificar si los roles se han comunicado adecuadamente al personal de TI. -Verificar la existencia de una revisión periódica de los roles por parte de los directivos de la organización.	Gerencia de TI Gerencia de RRHH Gerencia de Planificación	-Documento de Hitos y Cronogramas. -Documento de roles y funciones -Documento de evaluación de desempeño -Organigrama y sus versiones -Política de sistemas. -Documento de	-Se evidencia la existencia de las tareas de TI en el documento Hitos y Cronogramas, bien definidas y actualizadas. -Se evidencia la definición de roles y funciones mediante los documentos: Descriptivo de funciones para el Gerente de área y Analista de TI, administrados y aprobados por Recursos Humanos (Anexo 8). -Recursos Humanos dispone de un plan anual de capacitaciones a nivel de toda la organización en el que se evidencia las capacitaciones del área de tecnología (Anexo 9). -No se evidencia la difusión de la política de TI a los empleados.	03/09/2012

Continúa →

-Verificar si en las evaluaciones de desempeño que los resultados de los objetivos y metas sean considerados. -Comprobar que todas las posiciones en la organización describan los roles de sistemas, control interno y seguridad de la información. -Verificar si existe revisión anual de la política de sistemas. -Verificar si existe la comunicación de las políticas de TI para los empleados. -Verificar si existe registros de entrenamiento de los empleados.		capacitación de los empleados.	-La política de Sistemas (Anexo 10) existe, pero no está actualizada, no se ha realizado la revisión desde el año 2009. -Debido a que está en fase de implementación y depuración por parte de RRHH no existe una comunicación sobre los roles y responsabilidades de manera formal, por lo que no se puede evidenciar una separación de funciones en este punto en la organización. -La herramienta Mercer apoyó a definir las responsabilidades de los roles identificando 9 procesos para el Coordinador de TI y 6 procesos para el Asistente de TI, proporcionando un mayor entendimiento de la carga de trabajo. -Se evidencia que en las evaluaciones de desempeño anuales se consideran las metas y objetivos propuestos. -No se evidencia la comunicación de los roles y responsabilidades a los involucrados.	

Continúa →

PO4.7 Responsabilidad de Aseguramiento de Calidad de TI				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Verificar si existe una vía de comunicación en temas de desvíos de los estándares de servicio definidos. -Evidenciar si existe un proceso definido y documentado para la identificación, el escalamiento y la resolución de incidentes en el proceso de control de calidad. -Evidenciar la existencia de un proceso para el desarrollo de políticas y procedimientos. -Evidenciar el empleo de las mejores prácticas y uso de estándares. -Evidenciar si existe un proceso para reportar periódicamente los hallazgos y las recomendaciones.	Gerencia de TI	-Política de TI y normas asociadas. -Correos y reportes de incidentes.	-No existe un procedimiento que permita el aseguramiento de calidad de TI. Un método de acuerdos de niveles de servicio (SLA) no ha sido establecido. -Los problemas se atienden conforme van apareciendo sin que exista un registro, seguimiento, cierre y evaluación del mismo por lo que no existe un proceso definido de tratamiento, considerándolos de manera informal. -No existe un proceso que regule la generación de políticas y procedimientos, pero existe de manera ad-hoc la actualización de la política de sistemas como documento que norme y enmarque el funcionamiento de TI en la organización. -No está definido un mecanismo de reporte sobre los problemas e inconvenientes generados en el área.	03/09/2012

Continúa →

PO4.8 Responsabilidad Sobre el Riesgo, la Seguridad y el Cumplimiento				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Evidenciar la existencia de un staff que administre el riesgo y la seguridad de la información dentro de la organización. -Definición de roles y responsabilidades para el staff que administra el riesgo y la seguridad de la información. -Administración de la seguridad de la información a cargo de un oficial de seguridad. -Consideraciones para que la mitigación del riesgo sea analizada y revisada de manera periódica.	Gerencia de TI	-Documento de análisis de riesgos. -Organigrama	-El personal de TI se encarga de la administración de riesgos debido al tamaño de la organización sin que exista separación de funciones o asignación de responsabilidades al respecto. -No se puede evidenciar separación de funciones para la administración del riesgo y la seguridad de la información. -Se evidencia que la administración de la seguridad lo realiza el departamento de sistemas. -La mitigación de los riesgos es a través de controles que no están actualizados, por lo que al momento no existe una mitigación de riesgos clara y definida.	03/09/2012
PO4.9 Propiedad de Datos y Sistemas				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Evidenciar la existencia de una política de clasificación de datos y propiedad de los	Gerencia de TI	-Configuración de servidor y políticas de	-No se evidencia una política para clasificación de datos. Sobre la propiedad de datos estos son propiedad	10/09/2012

Continúa →

sistemas, que esté establecida y haya sido comunicada. -Validar que dicha política ha sido aplicada a la mayoría de los sistemas y a la arquitectura empresarial tanto para las comunicaciones internas y externas. -Verificar si existe una aplicación adecuada del proceso de clasificación y propiedad de datos. -Verificar que la política para clasificación de datos y propiedad del sistema soporta la protección de activos, permite la entrega eficiente y la utilización de aplicaciones del negocio facilitando la seguridad y apoyo en la toma de decisiones.		accesos. -Revisión de permisos de acceso en servidor del dominio. -Configuración de accesos a los directorios de las áreas funcionales. -Política de Clasificación de datos.	de las áreas funcionales. -Solo se utiliza las restricciones de acceso de acuerdo al área y función. -Se protegen los datos por medio de permisos de acceso al dominio y aplicaciones (Anexo 11). -La clasificación de la información está realizada por medio de las áreas funcionales de la empresa generando silos de información y no está estructurada de acuerdo a una clasificación coherente ni de fácil identificación ya que está administrada por el criterio de cada área funcional.	

Continúa →

PO4.10 Supervisión				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Verificar que existen procesos de supervisión. -Verificar y asegurar que dichos procesos de supervisión son revisados y ejecutados. -Verificar si las supervisiones disponen de un adecuado cumplimiento de las expectativas y de un adecuado rendimiento.	Gerencia de TI	-Documento de hitos y cronogramas -Balanced Scorecard	-Como elemento de supervisión se evidencia la existencia de cronogramas de cumplimiento de tareas y proyectos así como una matriz para el cumplimiento de hitos de manera mensual, los dos elementos no están integrados y han sido generados en diferentes fechas por lo que el uno controla proyectos de TI inmediatos y el otro los generados como cumplimiento de la estrategia de negocio. -Los procesos de supervisión son realizados y revisados por la gerencia de planificación e incorporados con la herramienta Strategic. -Los porcentajes de cumplimiento alimentan al BSC que presenta de manera global el rendimiento del área y su impacto en la organización.	10/09/2012

Continúa →

PO4.11 Segregación de Funciones				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Verificar la existencia de segregación de funciones. -Averiguar y confirmar si existe un proceso para identificar posiciones críticas y confirmar si existen segregación de funciones	Gerencia de RRHH	-Documento de descripción de funciones -Documentos de consultora Mercer (confidenciales)	-Se evidencia que la segregación de funciones se ha establecido en la descripción de funciones del departamento. En la parte operativa no se evidencia una segregación de funciones. -Por medio de la herramienta Mercer se ha identificado las posiciones críticas pero por el tamaño de la organización no existe segregación de funciones que permita una adecuada responsabilidad de las tareas de TI.	10/09/2012
PO4.12 Personal de TI				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Verificar que los conocimientos requeridos para el área de TI sean identificados y gestionados y su impacto en el personal de TI sean analizados, escalados y resueltos de acuerdo a estas necesidades. -Verificar que de existir cambios en el	Gerencia de RRHH	-Documentos de cursos y capacitaciones recibidas. -Revisión de documentos de	-Se evidencia un análisis de necesidades de capacitación anual (Anexo 12) y se envía a recursos humanos para su ejecución, pero no existe un cumplimiento del 100%. -Se evidencia que cada vez que se cambia un recurso tecnológico se hace una capacitación tanto al personal de TI como a los usuarios.	10/09/2012

Continúa →

negocio o la operación, las destrezas o competencias del personal de TI son las adecuadas. -Verificar que las tareas de soporte dispongan de las destrezas y competencias adecuadas por parte del personal de TI.		proyectos recientes. -Revisión de documentos de capacitación recientes	-Se evidencia que el personal de soporte está capacitado con las herramientas necesarias para el negocio, con excepción de un entrenamiento adecuado para soportar el ERP.	
PO4.13 Personal Clave de TI				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Verificar la existencia de procesos formales para cubrir las posiciones en caso de ausencia del personal que administra los procesos claves de sistemas en el negocio. -Verificar si existen documentación de temas críticos, delegación de funciones y personal entrenado para reemplazar al personal principal.	Gerencia de RRHH Gerencia de TI	-Documentos de trabajo de temas críticos	-Se evidencia un procedimiento en caso de ausencia del personal de TI, para que otra persona asuma el rol. -La dependencia del personal es crítica ya que al ser dos personas la falta de una de ellas representa en una carga del 100% de las tareas a ser cubiertas. Para temas de contingencia no existe documentación de temas críticos ni delegación de funciones como tampoco personal externo que reemplace al personal principal.	10/09/2012

Continúa →

PO4.14 Políticas y Procedimientos para Personal Contratado				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Solicitar las políticas que regulan cuándo, cómo y qué tipo de tareas pueden ser tercerizadas y si estas tareas se las están realizando. -Inspeccionar políticas y procedimientos para un efectivo control de seguridad hacia contratistas y asegurarse que están siendo empleadas. -Revisar las políticas y procedimientos para la selección de un proveedor y verificar si están siendo llevadas a cabo.	Jefe de Contratos	-Revisión de documentos de contratos de los principales proveedores de servicios de tecnología (confidenciales) -Acuerdos de Nivel de Servicio.	-No existen políticas sobre los servicios a ser tercerizados, lo que existe son normativas legales que definen en los contratos los servicios que pueden ser considerados como tercerizados debido a la obligatoriedad de cumpliendo legal sobre servicios técnicos especializados. -Se evidencia que existen acuerdos con terceros en donde se estipulan cumplimientos y penalidades así como acuerdos de confidencialidad que están integrados en los contratos de proveedores de servicios. -Existen políticas y procedimientos para la selección de proveedores y al revisar su cumplimiento, se verifica que no se cumple, ya que en varios años no se han renovado, se ha obviado el proceso de calificación.	10/09/2012

Continúa →

PO4.15 Relaciones				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Verificar si existen niveles de comunicación hacia las partes interesadas. -Verificar si las partes interesadas están satisfechas con las comunicaciones de TI.	Gerencia de TI Gerencia General	-Documentos de contratos.	-Se evidencia que no están definidos niveles de comunicación hacia las partes interesadas. -No existe evidencia de registros que demuestre la comunicación y satisfacción de los clientes.	10/09/2012

INDICADORES DE DESEMPEÑO

Tabla 23

Indicadores de Desempeño PO4

INDICADORES AÑO 2012	PORCENTAJE
# de proyectos del negocio retrasados por no disponibilidad de TI	2 de 10=20%
# de procesos del negocio que no reciben soporte de TI	0/17=0%

Nota Fuente: (IT Governance Institute, 2007), Pag.45, Estados Unidos

Continúa →

4.3.1.3 PO9 Evaluar y Administrar los Riesgos de TI

Cuadro 14

Análisis Proceso PO9

PO9.1 Marco de Trabajo de Administración de Riesgos				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Verificar que se tienen identificados y se gestionan apropiadamente los riegos del negocio. -Verificar que se han identificado los riesgos de TI que afecten a las operaciones del negocio. -Verificar si existe una matriz de riesgos de TI en donde se valora el impacto y la ocurrencia de los riesgos.	Gerente General Gerente de TI	-Manual de Seguridad y Salud Ocupacional. -Matriz de sistemas y servicios críticos que gestiona TI. -Matriz de Riesgos de TI, Matriz de cumplimientos regulatorios	- Como requisito legal, la compañía dispone de un comité de Salud y Seguridad Ocupacional en donde se analiza los riesgos a los que están expuestos los trabajadores, este es el único análisis que realizan hasta el momento: Riesgos físicos, ergonómicos y de salud. - La Gerencia de TI no ha realizado un análisis de los riesgos que afecten a las operaciones del negocio, sin embargo ha realizado un análisis de los sistemas y servicios críticos que gestiona TI. No tiene una matriz de riesgos a nivel de la organización.	20/08/2012

Continúa →

PO9.2 Establecimiento del Contexto del Riesgo				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
- Analizar la definición de los riesgos de TI. - Evidenciar un riesgo para analizar la aplicación en la gestión del riesgo definida por TI. - Evidenciar la divulgación de los riesgos a la organización.	Gerente de TI	- Documento Plan Continuidad del Negocio - Matriz de sistemas y servicios críticos que gestiona TI	- Se tienen identificados algunos riesgos del departamento (Anexo 5) en base a los servicios y recursos críticos de TI y se encuentra en el documento Plan de Continuidad del Negocio (Anexo 13). - Se hace seguimiento al riesgo de "Daño total o parcial en el Controlador de dominio", se ha creado un servidor de dominio alterno pero no se ha realizado las pruebas de operación. Se hace seguimiento al riesgo de "Corte suministro de energía", se evidencia que la carga del ups era de 15 minutos en el 2010, para el año 2011 era de 20 minutos para el año 2012 era de 30 minutos. - El análisis de los recursos y servicios críticos que gestiona TI, se lo hizo mediante encuestas a los usuarios y Gerentes de área, y se la va a actualizando según existan cambios en los servicios y sistemas. (Anexo 14).	20/08/2012

Continúa →

PO9.3 Identificación de Eventos				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Verificar que se tengan registrados los eventos críticos de TI. -Evidenciar el análisis de los eventos ocurridos su impacto y las acciones implementadas. -Verificar si se realiza un seguimiento a los eventos ocurridos como resultado de falta de control a un riesgo. -Evidenciar la existencia de un registro de eventos.	Gerente de TI	-Registro de los últimos eventos críticos ocurridos en el área.	- La Gerencia de TI no mantiene un análisis de registro de los eventos críticos ocurridos en el área, el gerente explica que ante un evento se actúa con premura, se analiza la causa del evento, se buscan los responsables pero no se lo registra. - No se realiza un seguimiento a los eventos ocurridos. - La organización estaba comunicaba ante la ocurrencia de un evento de TI y la Gerencia General aprobaba las acciones correctivas que incluían un presupuesto para remediar el evento.	21/08/2012
PO9.4 Evaluación de Riesgos de TI				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Evidenciar que la Gerencia General está enterada o forma parte de la evaluación de los riesgos de TI. - Evidenciar que los riesgos están definidos y	Gerente General Gerente de TI	-Correos electrónicos o actas de reunión con la Gerencia.	- La Gerencia de TI comunicó a la Gerencia General el resultado de la encuesta de sistemas y servicios críticos de TI, pero no se pudo evidenciar debido a que no existe un documento de soporte o aprobación.	21/08/2012

Continúa →

documentados. - Evidenciar el análisis de los riesgos de forma individual por categoría por su probabilidad e impacto.		- Matriz de sistemas y servicios críticos que gestiona TI. -Matriz de probabilidad vs impacto en la pérdida de servicios críticos.	- La documentación está elaborada informalmente y no posee un formato estándar que contenga fechas de elaboración, fechas de actualización, aprobaciones o vigencia, no se ha especificado un sistema de archivos para este tipo de documentación. - En el análisis de los sistemas y servicios críticos de TI se evidencia una valoración de acuerdo a su importancia como resultado de la encuesta a los usuarios, además que se evidencia una valoración en cuanto a la probabilidad de perder el servicio o recurso crítico, estos valores fueron establecidos por el Gerente de TI. - Se evidencia que existe un análisis de riesgos por probabilidad versus impacto en el documento Plan de Continuidad del Negocio, pero el documento se encuentra en desarrollo.	

Continúa →

PO9.5 Respuesta a los Riesgos				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
- Identificar y analizar los controles implementados a los riesgos de TI. - Identificar y analizar los recursos asignados para mitigación de riesgos. - Evidenciar si se documentan los resultados obtenidos luego de la ocurrencia de un riesgo y si se hace seguimientos de mejora. - Buscar evidencia de la aplicación de los resultados de la evaluación de los riesgos. Ejemplo en un BCP (Business Continuity Plan).	Gerente de TI	- Documento Plan Continuidad del Negocio.	- Los controles que se han implementado se basan en la experiencia del Gerente de TI. Por ejemplo la compra de UPS, pararrayos, servidores de backup, etc. que permitan continuar con las operaciones en los sistemas y servicios que TI proporciona a los usuarios. - La Gerencia de TI no documenta los eventos ocasionados por un riesgo, se realiza seguimiento y se busca mejoras pero no se lo puede evidenciar ya que no está documentado. - La Gerencia de TI ha elaborado un Plan de Continuidad del Negocio (Anexo 13), en donde se encuentra descrito los recursos necesarios para controlar los riesgos; el documento se encuentra en desarrollo.	23/08/2012

Continúa →

PO9.6 Mantenimiento y Monitoreo de un Plan de Acción de Riesgos				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
- Verificar la existencia de un Plan de acción para los riesgos identificados como principales. -Evidenciar el seguimiento a las actividades incluidas en los planes de acción para mitigación de riesgos. - Verificar que los Planes de acción sean conocidos y aprobados por la Gerencia General. -Evidenciar que los planes de acción sean actualizados de acuerdo a los cambios en los controles.	Gerente de TI	- Planes de Acción para sistemas y servicios críticos. - Objetivos y Metas de TI.	- Se evidencia planes de acción (Anexo 15) para controlar los sistemas y servicios críticos que TI gestiona para años anteriores, el documento no está actualizado. - No existen cronogramas de implementación para los planes de acción por lo tanto no se ha medido la ejecución ni evidenciado desviaciones a los mismos. - Por cambios en la dirección del área de tecnología, se debe actualizar y aprobar los planes de acción de este año. - Los planes de acción deben ser aprobados por la Gerencia de Planificación, su formato es informal.	25/08/2012

Continúa →

INDICADORES DE DESEMPEÑO

Tabla 24

Indicadores de Desempeño PO9

INDICADORES AÑO 2012	PORCENTAJE
% de servicios críticos de TI cubiertos por la evaluación de riesgos	2 de 17 = 11%
% de riesgos de TI integrados en la evaluación de riesgos de TI	2 de 3 = 66%
% de eventos críticos de TI que han sido evaluados y documentados	0%
# de incidentes significativos causados por riesgos no identificados	0
% de riesgos críticos de TI identificados en un plan de acción	4 de 15 = 26%
Frecuencia de la revisión del proceso de administración de riesgos de TI	1 vez al año
% de planes de acción de administración de riesgos aprobados para su implementación	6 de 15 = 40%

Nota Fuente: (IT Governance Institute, 2007), Pag.65, Estados Unidos

4.3.2 DS ENTREGAR Y DAR SOPORTE

4.3.2.1 DS2 Administrar los Servicios de Terceros

Cuadro 15

Análisis Proceso DS2

DS2.1 Identificación de todas la relaciones con proveedores				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Preguntar y confirmar que un registro de relaciones con los proveedores se mantiene. -Obtener los criterios de relaciones con los proveedores por tipo de proveedor, la importancia y criticidad. -Inspeccionar el registro de relaciones con los proveedores para asegurarse de que está al día, debidamente clasificados y suficientemente detallada para asegurarse de que proporciona una base para el monitoreo de los proveedores existentes. -Verificar la existencia de históricos en la	Jefe de Compras	-Base de datos de proveedores. -Documento de registro de proveedores. -Revisión de contratos	-Se evidencia la existencia de un registro de proveedores con los recursos y servicios que este ofrece con una calificación y verificación de cumplimiento. -Se evidencia que existe una base de datos en donde se mantiene la calificación del proveedor (Anexo 16), esta calificación se la debe realizar como requisito de calificación y renovación cada 2 años. -La categorización se la realiza por medio de la empresa SGS, la misma que valora los aspectos del servicio o producto que proporciona, estados financieros y calidad, otorgando calificación en base al alfabeto siendo de la A a la C y la D lo descalifica.	24/09/2012

Continúa →

selección de proveedores / rechazo son conservados y utilizados. -Inspeccionar una muestra representativa de los contratos con proveedores, SLA's y otros documentos para asegurarse de que corresponden con el registro de proveedores.			-En la base de datos se mantiene un histórico y se registra los incumplimientos, sanciones y multas, considerando este histórico para el caso de nuevas contrataciones. -La base de datos se encuentra actualizada y forma parte del sistema ERP de la compañía. -Se toma una muestra de 3 contratos principales de TI (Anexo 17) y se evidencia el cumplimiento del 100% respecto a la documentación sustentada por el área de compras verificando calificación y actualización de los proveedores.	
DS2.2 Gestión de Relaciones con Proveedores				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Inspeccionar la documentación de proveedores de servicios y determinar si las funciones de gestión de proveedores han sido documentadas y comunicadas dentro de la organización. -Determinar si existen políticas para asegurar	Jefe de Compras	-Proceso de compras (confidencial)	-Dentro del proceso de calificación, toda la documentación de los proveedores es almacenada por la empresa SGS y están documentadas y comunicadas al área de compras. -Existen políticas por parte del área de contratos, se verifica que se están cumpliendo con los contratos	24/09/2012

Continúa →

que los contratos se creen, mantengan, se den seguimiento y renegocien cuando sea necesario. -Evaluar si la asignación de funciones del proveedor es razonable y basada en el nivel y las habilidades técnicas necesarias para gestionar eficazmente la relación.			actuales de tecnología y se verifica su cumplimiento y seguimiento. -Se evidencia que en el documento calificación de proveedores se registra las habilidades y capacidades de provisión de servicio.	

DS2.3 Administración de Riesgos del Proveedor				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Preguntar si los riesgos asociados con la incapacidad para cumplir con los contratos con los proveedores se definen. -Preguntar si los recursos fueron considerados en la definición del contrato de abastecimiento. -Inspeccionar la documentación del contrato para la evidencia de la revisión. -Determinar si en las políticas se exigen la	Jefe de Compras. Asistente de Recursos Humanos	-Contratos individuales de proveedores (confidencial)	-Se evidencia que en los contratos están definidos los riesgos por incumplimiento, las sanciones, multas y penalizaciones. -Se evidencia que en los contratos están definidos los recursos económicos, técnicos y humanos en la prestación del servicio. -Se evidencia que los contratos están revisados con sello y firma del área jurídica, sumilla del jefe de compras, sumilla del área de tecnología y sumilla del	24/09/2012

Continúa →

independencia entre el proveedor y el personal de gestión dentro de la organización.			proveedor. -Se evidencia la existencia de un hito dentro del Reglamento interno de trabajo de que no puede existir relación directa entre los proveedores y el personal de compras de la organización y la sanción al incumplimiento.	
DS2.4 Monitoreo del Desempeño del Proveedor				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Seleccionar una muestra de facturas de proveedores, identificar los cargos por los servicios contratados, según lo especificado en los contratos, evaluar la razonabilidad de los gastos. -Determinar si el proveedor cumple los niveles de desempeño acordados y el contrato de proveedor.	Gerencia de TI	-Facturas de los 3 proveedores principales -SLA's -Informe Técnico del proveedor	-Se evidencia que la factura del proveedor del enlace internacional corresponde a lo descrito en el contrato, en el área de telecomunicaciones. Al verificar las facturas de los enlaces existe un valor que sobrepasa el valor promedio de mercado en 8 veces para este tipo de enlaces siendo la justificación la contratación directa por parte de la casa matriz. -No se evidencia revisión de los acuerdos de servicio.	24/09/2012

Continúa →

INDICADORES DE DESEMPEÑO

Tabla de Indicadores de Desempeño DS2

INDICADORES AÑO 2012	**PORCENTAJE**
% del gasto dedicado a la provisión de servicios con terceros	313.240 / 644.654 = 49%
% de los principales proveedores que cumplen claramente los requerimientos definidos y los niveles de servicio	100%
# de controversias con los proveedores	0=100%
% de facturas del proveedor en controversia	0=100%
% de los principales proveedores sujetos a una clara definición de requerimientos	100%
# de incidentes significativos por incumplimiento del proveedor en un periodo de tiempo	0=100%

Nota Fuente: (IT Governance Institute, 2007), Pag.107, Estados Unidos

4.3.2.2 DS4 Garantizar la Continuidad del Servicio

Cuadro 16

Análisis Proceso DS4

DS4.1 Marco de Trabajo de Continuidad de TI				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
- Entender y evaluar la estrategia de continuidad del negocio. - Evaluar los planes de continuidad de TI que aseguren la continuidad del negocio. - Evidenciar si en el plan de continuidad están involucrados los usuarios, proveedores y clientes y se detalla los roles y responsabilidades de cada uno de ellos. - Evidenciar si en el plan de continuidad se encuentran todos los activos críticos de TI. - Verificar que el plan de continuidad sea conocido y aprobado por la Gerencia General y divulgado a todos los involucrados.	Gerente General Gerente de TI	-Documento Plan Continuidad del Negocio.	- La Gerencia General tiene claro cuáles son las estrategias a nivel de la compañía en lo que respecta a continuidad del negocio, pero éstas no han sido divulgadas a la organización, por lo tanto la Gerencia de TI no ha podido establecer una relación entre las estrategias de TI y del negocio. -La Gerencia de TI se encuentra elaborando el plan de continuidad del negocio – BCP (Anexo 13), no se evidenció la existencia de un cronograma de elaboración y por lo tanto una fecha de entrega para aprobaciones de la Gerencia General. - En el plan de continuidad se evidencia la descripción de recursos y servicios a proteger pero no se los ha	27/08/2012

Continúa →

- Verificar la vigencia del plan de continuidad y las actualizaciones cuando existan cambios.			identificado como activos críticos de TI. - En el plan de continuidad de TI si se encuentran involucrados los usuarios con sus roles y responsabilidades, pero los proveedores no constan en el plan.	
DS4.2 Planes de Continuidad de TI				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Verificar que se han identificado los procesos críticos de negocio. -Evaluar el Plan de continuidad para verificar que los procesos críticos están tomados en cuenta. -Evaluar la capacidad de recuperación y alternativas de procesamiento para garantizar la disponibilidad de los servicios. -Verificar que la mínima configuración de un recurso crítico está detallado en el procedimiento de recuperación.	Gerente de TI	-Matriz de sistemas y servicios críticos que gestiona TI -Documento Plan Continuidad del Negocio -Pruebas de funcionamiento del UPS - Configuración del PDC	- El Gerente de TI, menciona que los procesos críticos del negocio serán tomados en cuenta en la elaboración del Plan de Continuidad, pero no se pudo evidenciar. - Para garantizar la disponibilidad de los servicios la Gerencia de TI, realizó el análisis de los sistemas críticos y servicios que TI presta a los usuarios (Anexo 14), no se evidencia que se realicen pruebas frecuentes a los controles implementados. - En el Plan de Continuidad de TI se tienen procedimientos de recuperación para algunos de los recursos como servidores, firewalls, centrales telefónicas,	27/08/2012

Continúa →

-Evidenciar que se ha realizado pruebas frecuentes al plan de recuperación. -Evidenciar que existe una revisión al resultado de las pruebas y se realiza seguimiento a las acciones correctivas.		- Configuración del Firewall	routers, etc. pero no se los ha definido como activos críticos. - Se realizó una prueba para verificar el buen funcionamiento del UPS, se desconectó la corriente de luz primaria, entrando a funcionar el UPS y dotando de energía alterna a servidores, equipos de comunicaciones, equipos de computación y teléfonos. - Se revisó el recursos crítico Firewall, en el Plan de Continuidad no consta la configuración del equipo, pero está documentado que existe un backup diario de la configuración y es recibida por el Gerente de Sistemas por correo electrónico, ésta se almacena en las cintas de backup, se detalla el procedimiento para restaurar la copia de seguridad, el procedimiento toma alrededor de 5 minutos. - Se revisó el recurso crítico PDC, en el Plan de Continuidad no consta la configuración, pero se evidencia la existencia de un servidor PDC alterno.	

Continúa →

DS4.3 Recursos Críticos de TI				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
- Verificar la estrategia para reemplazar los recursos críticos de TI en caso de un evento. - Verificar que la Gerencia de TI tenga identificadas a las funciones de negocio críticas: procesos y recursos. - Verificar que los planes de continuidad cumplan con requerimientos legales, contractuales y regulatorios. - Verificar si la priorización de la recuperación de los servicios y recursos críticos de TI establecidos en el plan son los requeridos por el negocio. - Evaluar el análisis de los costos en cada proceso de recuperación.	Gerente de TI	- Registro de los últimos eventos críticos ocurridos en el área.	- Se evidencia que en el plan de continuidad de TI a nivel de servidores, según sea el caso, primero se adquirirán partes y piezas de servidores o en su defecto se realizará el cambio total del equipo, no se ha definido en el documento el proveedor sugerido. - Se tiene identificado los sistemas y servicios críticos de TI, la Gerencia de TI conoce cuáles son las funciones de negocio críticas, el proceso y los recursos asignados a ellas, pero no se lo ha documentado. - La Gerencia de TI tomará en cuenta los requerimientos legales, contractuales y regulatorios para incluirlos en el Plan de Continuidad del Negocio, actualmente no constan en el documento. - La priorización para la recuperación de los servicios y recursos de TI está dada por la encuesta que se realizó a los usuarios.	29/08/2012

Continúa →

DS4.4 Mantenimiento del Plan de Continuidad de TI				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
- Evidenciar que la Gerencia de TI haya desarrollado un procedimiento de control de cambios para el Plan de continuidad. - Evidenciar las actualizaciones al plan cuando se cambien recursos críticos. - Verificar que se lleva un registro de los cambios realizados a los Planes de continuidad, los responsables y que los cambios sean comunicados a los involucrados.	Gerente de TI	- Documento Plan de Continuidad	- Se evidencia que la Gerencia de TI no ha establecido un procedimiento para el control de cambios, los cambios son realizados por el Gerente de TI. - Se evidencia que las actualizaciones al documento se realizan cuando cambian los recursos críticos. - No se lleva un registro de los cambios realizados al documento, el responsable ni tampoco el motivo del cambio.	30/08/2012
DS4.5 Pruebas del Plan de Continuidad de TI				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
- Evidenciar programas frecuentes de pruebas para el plan de contingencia (cambios a recursos críticos). - Verificar que los planes de continuidad del	Gerente de TI Usuarios	- Documento Plan Continuidad del Negocio.	- Se toma como muestra los sistemas y servicios críticos que están desarrollados en el Plan de Contingencia debido a que éste se encuentra en desarrollo, con relación a esto, la Gerencia de TI ha realizado pruebas de los	30/08/2012

Continúa →

negocio detallen secuencias lógicas y ordenadas para la ejecución de las pruebas. - Evaluar el almacenamiento en el sitio alterno si existiera. - Evaluar el sitio alterno para asegurar la presencia, sincronización y vigencia de los medios y de la documentación. - Evaluar la capacidad del personal de TI y del usuario para responder con eficacia ante un desastre.			sistemas y servicios críticos pero no las ha documentado. - No se evidencia la existencia de un procedimiento de pruebas de los sistemas y servicios críticos TI, tampoco existe un registro con los resultados de las pruebas realizadas. - Se evidencia que la organización no cuenta con un sitio alterno en caso de un desastre. - No se ha establecido un procedimiento para el personal de TI ni para los usuarios en el caso de ocurrir un desastre. - La Gerencia de TI mantiene un registro de acciones correctivas, pero estas no están actualizadas.	
DS4.6 Entrenamiento del Plan de Continuidad de TI				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
- Verificar la existencia de planes de capacitación a los involucrados. - Evaluar si los manuales y procedimientos de continuidad del negocio están escritos en	Gerente de TI Usuarios	- Documento Plan Continuidad del Negocio	-La Gerencia de TI ha realizado capacitaciones que tienen que ver con seguridad de los sistemas y servicios críticos, pero no se puede evidenciar debido a que no existen actas ni listas de asistentes.	31/08/2012

Continúa →

una forma sencilla y fácil de entender por el usuario final. - Realizar entrevistas al personal para verificar si el Plan es apropiado, completo y entendible. - Realizar entrevistas al personal clave para evaluar el entendimiento de las responsabilidades que se le ha asignado.			-No se han desarrollado manuales ni procedimientos de Continuidad del Negocio, ya que se encuentra en desarrollo. -La Gerencia de TI informa que se están manteniendo reuniones frecuentes con usuarios clave para la elaboración del Plan de Continuidad, no se puede evidenciar ya que no existen actas o listas de asistentes.	
DS4.7 Distribución del Plan de Continuidad de TI				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
- Evidenciar si el Plan de continuidad es distribuido al personal involucrado. - Verificar si existe un procedimiento de distribución. - Evidenciar que las copias del Plan de continuidad son protegidos adecuadamente y accesados por personal autorizado. - Evidenciar que en el Plan de continuidad no	Gerente de TI	- Documento Plan de Continuidad del Negocio	- No aplica debido a que el Plan de Continuidad se está desarrollando. - El Plan de Continuidad de TI que se está desarrollando solo lo administra el Gerente de TI hasta que esté culminado.	31/08/2012

Continúa →

se incluya información confidencial que pueda ser leída por personal no autorizado.				
DS4.8 Recuperación y Reanudación de los Servicios de TI				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
- Verificar que los procedimientos de recuperación y reanudación de los servicios sean completos, ordenados y lógicos. - Verificar que la Gerencia General conoce el tiempo necesario para ejecutar la recuperación. - Verificar que la Gerencia General conoce el costo necesario para la recuperación.	Gerente General Gerente de TI	- Documento Plan de Continuidad del Negocio	- Los procedimientos para la recuperación y reanudación de los sistemas y servicios críticos, están en desarrollo. - La Gerencia General y la Gerencia de TI no tienen conocimientos del costo y tiempo que tomaría reanudar todas las operaciones del negocio en caso de un desastre porque aún no se lo ha puesto en marcha ni se ha realizado pruebas.	01/09/2012
DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
- Verificar la existencia de respaldos de información, bien identificados. - Verificar que los respaldos se encuentren fuera de la oficina. - Evidenciar que se realizan pruebas de	Analista de TI	-Software Dataprotector - Cintas de Respaldo -Registro de Backups - Registro de Envío	-Se evidencia que se utiliza el software Dataprotector de HP para la realización de backups, el software se encuentra debidamente licenciado y funcionando. -Se evidencia la existencia de 20 cintas para los backups diarios de la información crítica.	01/09/2012

Continúa →

recuperación de información para validar backups. - Evidenciar registros de los procedimientos periódicos de copias de respaldo. - Evidenciar que se está respaldando la información detallada en el plan de continuidad del negocio. - Verificar procedimientos de backups y recuperación de datos. - Verificar que la frecuencia de rotación de medios sea la adecuada.		fuera de oficinas - Registro de pruebas de recuperación - Procedimiento de Backups y Recuperación	-Se evidencia la existencia de 4 cintas para los backups mensuales. -Se evidencia que se realizan backups diarios de la información a través del Registro Diario de Backups (Anexo 18) de los servidores (data), no se tiene clasificada la información, por lo tanto el backup es total. -No se está realizando copia de seguridad de las configuraciones de los servidores, se evidencia que las etiquetas de los medios están codificadas, el Analista de Sistemas es el único que conoce la definición de las codificaciones. -Se evidencia que los medios de backup son almacenados fuera de la oficina en la empresa G4S y se mantiene un registro del envío diario. -Se evidencia que no se están realizando pruebas frecuentes de los medios y copias de seguridad para verificar el buen funcionamiento. -Se evidencia la automatización del proceso de backup no	

Continúa →

			se necesita un procedimiento, en el caso de alguna falla en el servidor o en la herramienta de backup se deberá volver a configurarla, no existen procedimientos de recuperación, los medios rotan cada mes. -La política para comunicar a los usuarios de la responsabilidad que tienen para que se realice backups de sus documentos está realizada pero no aprobada.	
DS4.10 Revisión Post Reanudación				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
- Evidenciar las mejoras al plan de continuidad luego de la recuperación a través de la creación de acciones correctivas. - Verificar que se mantiene informada a la Gerencia General luego de la reanudación de los servicios y que se aprueban los nuevos requerimientos.	Gerente de TI	-Documento Plan de Continuidad del Negocio -Correos electrónicos a la Gerencia informando de la reanudación de los servicios y acciones implementadas.	- La Gerencia de TI informa que aún no se ha realizado acciones correctivas por cuanto no se ha realizado las pruebas al Plan de Continuidad de TI. - Cuando un servicio falla la Gerencia General está informada pero es una comunicación informal por lo tanto no se la puede evidenciar.	01/09/2012

Continúa →

INDICADORES DE DESEMPEÑO

Tabla 25

Indicadores de Desempeño DS4

INDICADORES AÑO 2012	**PORCENTAJE**
# de horas perdidas debido a interrupciones no planeadas	16 horas (Enlaces)
# de procesos críticos del negocio que dependen de TI, no cubiertos por un plan de continuidad	2 de 2
% de pruebas para lograr los objetivos de recuperación	0
Frecuencia en la interrupción de servicios de sistemas críticos	1 vez al año
% de componentes de infraestructura críticos con monitoreo de disponibilidad automatizado	0
Frecuencia de revisión del plan de continuidad de TI	n/a

Nota Fuente: (IT Governance Institute, 2007), Pag.119, Estados Unidos

4.3.2.3 DS5 Garantizar la Seguridad de los Sistemas

Cuadro 17

Análisis Proceso DS5

DS5.1 Administración de la Seguridad de TI				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Determinar si un comité de dirección de seguridad existe, con representación de las principales áreas funcionales, incluida la auditoría interna, recursos humanos, operaciones, seguridad informática y jurídica. -Determinar si existe un proceso para dar prioridad a las iniciativas, propuestas de seguridad, incluyendo los niveles requeridos de las políticas, normas y procedimiento	Gerencia de TI	-Organigrama -Política de Seguridad de TI	-No se evidencia la existencia de un comité de dirección de seguridad. -No existe un proceso definido para iniciativas de seguridad. -Existe una política de sistemas (Anexo 10) en donde consta un hito para la seguridad de la información pero no existe una política de seguridad específica. -Existe una política de sistemas, no se especifica el alcance, objetivos y responsabilidades de la función de gestión de seguridad. -La responsabilidad dentro de la política de sistemas sólo hace referencia a los usuarios. -No existe una Política de seguridad.	01/10/2012

Continúa →

DS5.2 Plan de Seguridad de TI				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
Determinar la eficacia del plan general de seguridad de TI que responda a las necesidades cambiantes de la organización. -Verificar que el plan de seguridad considera planes tácticos, la clasificación de datos, los estándares de tecnología, políticas de seguridad y control, gestión de riesgos y el cumplimiento de los requisitos externos. -Determinar si existe un proceso para actualizar periódicamente el plan de seguridad de TI, y si el proceso requiere de niveles adecuados de revisión de la gestión y aprobación de los cambios.	Gerencia de TI	Política y normativa de TI	-No existe un plan general de seguridad, existiendo de manera aislada planes tácticos, estándares de tecnología, política de sistemas, lo cual no permite verificar un plan de seguridad coherente. -No existe una definición para una línea base sobre seguridad. -No se evidencia la existencia de un proceso de actualización de un plan de seguridad. -Se evidencia la existencia de una política de sistemas, la misma que está desactualizada, en funciones y responsabilidades. -No existe presupuesto para el ámbito de seguridad.	01/10/2012

Continúa →

DS5.3 Administración de Identidad				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Determinar si las prácticas de seguridad requieren de una política de autenticación para conceder el acceso a los sistemas. -Si los roles predeterminados y con aprobación previa se utilizan para conceder acceso, determinar si delimitan las responsabilidades y verificar que estos roles son aprobados por el dueño del proceso. -Determinar si los mecanismos de autenticación se utilizan para controlar el acceso lógico a través de todos los usuarios, los procesos del sistema, los recursos de TI y accesos remotos.	Gerencia de TI	-Revisión de política y normativa de TI	-Se evidencia una política de accesos (Anexo 11) mediante usuario y contraseña a los sistemas críticos de la compañía. Todo usuario debe contar con al menos acceso de red y código telefónico y aquellos con uso a SAP debe contar con la respectiva clave. -Se evidencia que se implementan perfiles de usuario (Anexo 19) para cada aplicación y que el dueño del proceso es quien solicita a TI la creación y asignación de los perfiles a los usuarios. -Se evidencia que todo acceso a un recurso lógico, a los principales sistemas de la organización así como a los recursos de TI incluyendo accesos remotos, cumplen con mecanismos de autenticación previo al uso de estos recursos.	01/10/2012

Continúa →

DS5.4 Administración de Cuentas del Usuario				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Determinar si existen procedimientos para evaluar periódicamente y certificar el acceso a los sistemas y a las aplicaciones. -Determinar si los procedimientos de control de acceso existen para controlar y gestionar los derechos del sistema y la aplicación y los privilegios de acuerdo a las políticas de seguridad de la organización y el cumplimiento y los requisitos reglamentarios. -Determinar si los sistemas, aplicaciones y datos han sido clasificados por niveles de importancia y riesgo, y si los propietarios del proceso han sido identificados y asignados.	Gerencia de TI	-Políticas del servidor. -Contratos	-No existe un procedimiento que evalúe periódicamente el acceso de usuarios a los sistemas y aplicaciones. -Se evidencia que los controles de acceso están bien definidos y asignados a los usuarios. -No existe una clasificación de datos, sistemas y aplicaciones por niveles de importancia y riesgo. -Se evidencia que en los contratos existe una cláusula de confidencialidad de la información y para usuarios internos consta en el Reglamento interno de trabajo, las normas y procedimientos son comunicados a terceros.	01/10/2012

Continúa →

DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Preguntar y confirmar que un inventario de todos los dispositivos de red, servicios y aplicaciones existe y que cada componente se le ha asignado una calificación de riesgo de seguridad. -Determinar que exista una línea base de seguridad para todos los recursos de TI utilizados por la organización. -Determinar si los activos de mayor riesgo de la red se controlan rutinariamente por los eventos de seguridad. -Determinar si la función de la administración de seguridad informática se ha integrado dentro de las iniciativas de gestión de proyectos de la organización.	Gerencia de TI	-Inventario de equipos. -Documentos de relevamiento de riesgos.	-Existe un inventario de hardware, software, aplicaciones (Anexo 20) pero no se le ha asignado una calificación del riesgo de seguridad. -Se evidencia un análisis de riesgos (Anexo 5) de los servicios de TI críticos del negocio. No se ha realizado un análisis global de los recursos de TI y sus riesgos asociados, por lo que no se ha establecido una línea base de seguridad para los recursos utilizados en la organización. -Se evidencia que se realiza una revisión mensual del log del servidor firewall pero no de los otros activos de mayor riesgo de la red. -No se ha creado la integración entre la seguridad informática y la gestión de proyectos, se han implementado las seguridades propias de las aplicaciones adquiridas.	01/10/2012

Continúa →

DS5.6 Definición de Incidente de Seguridad				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-El papel y las responsabilidades de los proveedores en la prevención de incidentes y el seguimiento, corrección de fallas de software, y otras áreas. -Determine si el proceso de manejo de incidentes emplea adecuadas relaciones con las funciones clave de la organización, como la mesa de ayuda, los proveedores de servicios externos y gestión de la red. -Evaluar si el proceso de gestión de incidentes incluye los siguientes elementos clave: - Detección de eventos - Evaluación de la amenaza / incidente - Resolución de la amenaza o creación y orden de escalamiento - Análisis post-implementación - Orden de trabajo / Cierre de incidente	Gerencia de TI	-Contratos de proveedores.	-Se evidencia que se han definido los proveedores y responsables para el área de comunicaciones y telefonía, aplicaciones críticas, sistemas operativos. No se ha establecido para hardware. -No se ha establecido un proceso para el manejo de incidentes de seguridad.	01/10/2012

Continúa →

DS5.7 Protección de la Tecnología de Seguridad				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Preguntar y confirmar que políticas y procedimientos han sido establecidos para hacer frente a los ataques a la seguridad de la información. -Inspeccionar los registros de control de acceso y registro de acceso intentos fallidos, acceso no autorizado a archivos confidenciales y / o datos, y el acceso físico a las instalaciones. -Preguntar y confirmar que las características de seguridad implementadas facilitan las reglas de contraseñas (por ejemplo, la longitud máxima, uso de letras y números, la expiración, reutilización de claves).	Gerencia de TI	-Política de TI y de las normativas asociadas. -Logs del servidor de archivos. -Políticas del servidor. -Reportes del firewall de manera mensual.	-En la política general de sistemas existe un hito para seguridad de la información el cual es muy general y no están considerados los nuevos servicios que presta TI. -Se evidencia que el acceso físico se encuentra monitoreado constantemente por un sistema de control de accesos. No se evidencia un log donde se visualice los intentos fallidos a aplicaciones y archivos. -Se evidencia la implementación de una política de creación de contraseñas (Anexo 21) la cual incluye como mínimo 6 caracteres, expira a los 90 días y no acepta 3 claves anteriores a la actual. -No se evidencia la existencia de revisiones anuales a los elementos de seguridad. -Se evidencia la existencia de un reporte generado por el sistema Fortinet (Anexo 22).	01/10/2012

Continúa →

DS5.8 Administración de Llaves Criptográficas				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Determinar si existe un proceso para la gestión de llaves que contenga: Mínimo tamaño de caracteres en la clave para una contraseña segura. Uso de algoritmos para generación de claves. Métodos de distribución de claves. Identificación de estándares para la generación de algoritmos Respaldos de claves, archivo y destrucción. -Evaluar si los controles sobre las claves privadas existen para hacer cumplir su confidencialidad e integridad. Las claves privadas son respaldadas, almacenadas y recuperadas por personal autorizado con control dual en un medio ambiente protegido físicamente.	Gerencia de TI	-Revisión de políticas en servidor. -Certificados de Seguridad	-No se evidencia la existencia de un proceso que regule la gestión de claves criptográficas y seguridad asociada. -No se evidencia clasificación de la información de acuerdo a parámetros de propiedad de activos de datos. Está clasificada de acuerdo a las áreas de la organización. -No existen procedimientos que regulen la clasificación de la información. -No se evidencia el uso e implementación de métodos criptográficos.	01/10/2012

Continúa →

DS5.9 Prevención, Detección y Corrección de Software Malicioso				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Preguntar y confirmar que una política de prevención sobre software malicioso está establecido, documentado, y comunicado a toda la organización. -Asegurar que controles automatizados han sido implementados para proporcionar protección contra virus y que las violaciones son comunicadas apropiadamente. -Evidenciar que los miembros del personal clave son conscientes de la política de prevención de software malintencionado y su responsabilidad para asegurar el cumplimiento. -A partir de una muestra de estaciones de trabajo, observar si una herramienta de protección contra virus se ha instalado e	Gerencia de TI	-Revisión de la existencia de antivirus actualizado por computador. -Revisión de la consola de administración del antivirus. -Licencias	-Se evidencia que en la política general de sistemas existe un hito para la prevención de uso no adecuado de software, está documentada pero no se evidencia que los usuarios están comunicados. -Se evidencia la existencia de Trend Micro como antivirus corporativo, se ha evidenciado que está licenciado, actualizado y parametrizado para enviar alertas en caso de detectar incidentes al administrador de sistemas. No se evidencia que los miembros del personal clave están al tanto de la política de prevención de virus. El antivirus reside en un servidor central y en la consola de administración se encuentran las políticas y reglas de actualizaciones automáticas, escaneo y limpieza de archivos infectados. -Se evidencia que el proceso funciona adecuadamente.	01/10/2012

Continúa →

incluye los archivos de definiciones de virus y la última vez que las definiciones se han actualizado. -Preguntar y confirmar que el software de protección es de distribución central (la versión y los parches de nivel) con una configuración centralizada. -Preguntar si y confirmar que la información sobre nuevas amenazas potenciales se revisa periódicamente y es evaluada. -Preguntar y confirmar que el correo electrónico entrante se filtra adecuadamente contra la información no solicitada. -Revisar el proceso de filtrado para determinar la eficacia de funcionamiento, o revisar el proceso automatizado establecido para fines de filtrado.			De la muestra de equipos revisados el 100% está cubierto. -No existe un procedimiento para la revisión periódica de nuevas amenazas, como mecanismo de prevención está la actualización automática de las definiciones de virus en el antivirus. -Se evidencia que el primer filtro para antispam es el servidor proxy ISA Server 2006, como segundo filtro está configurado un antivirus y antispam en el servidor de correo Exchange 2008. Se evidencia que el proceso de filtrado funciona adecuadamente. -Se revisan 10 equipos cumpliendo todos con la actualización del antivirus.	

Continúa →

DS5.10 Seguridad de la Red				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Preguntar y confirmar que una política de seguridad de la red (por ejemplo, los servicios prestados, el tráfico permitido, los tipos de conexiones permitidas) ha sido establecida y se mantiene. -Preguntar y confirmar que los procedimientos y directrices para la administración de todos los componentes críticos de la red (por ejemplo, routers principales, DMZ, switches VPN) son establecidos y se actualizan periódicamente por el personal clave de la administración, los cambios que se registran y si conservan documentos históricos.	Gerencia de TI	-Revisión de políticas en servidor.	-Se evidencia que existen reglas configuradas en el servidor Proxy para el filtro de paquetes de acuerdo a los permisos definidos. -No se ha establecido una clasificación para los elementos de la red que permitan detectar los elementos críticos, por lo que no se han establecido procedimientos para la administración de dichos elementos.	01/10/2012

Continúa →

DS5.11 Intercambio de Datos Sensitivos				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Preguntar y confirmar que la transmisión de datos fuera de la organización se ha encriptado. -Preguntar y confirmar que los datos corporativos se clasifican de acuerdo al nivel de la exposición y el esquema de clasificación (por ejemplo, confidencial, público y privado). -Preguntar y confirmar que el procesamiento de datos sensibles valida la transacción antes de la transmisión.	Gerencia de TI	-Mecanismos de encriptación -Clasificación de la información -Información transmitida de un sitio a otro.	No se ha establecido un mecanismo de encriptación. La información no está clasificada.	01/10/2012

Continúa →

INDICADORES DE DESEMPEÑO

Tabla 26

Indicadores de Desempeño DS5

INDICADORES AÑO 2012	PORCENTAJE
# de incidentes con impacto al negocio	0/0 =100%
# de sistemas que no cumplen con los requerimientos de seguridad	0/0 =100%
% de cumplimiento para otorgar, cambiar o eliminar privilegios de acceso	100%
# de bloqueos a intentos de acceso externo no permitido	200/200 =100%
# de incidentes de accesos bloqueados por segregación de funciones	3/3 =100%
% de usuarios que cumplen con los estándares de contraseñas	100%
# y tipo de código malicioso prevenido	400/400 virus =100%
% cumplimiento en la frecuencia y revisión del tipo de eventos de seguridad a ser monitoreados	100%
# y tipo de cuentas obsoletas	0/0=100%
# de direcciones IP no autorizadas, puertos y tipos de tráfico denegados	41/41=100%, 2/2 puertos 25 smtp y 80, http
# de llaves criptográficas comprometidas y revocadas	0/0 = 100%
% de derechos de acceso autorizados, revocados, restaurados o cambiados	100%

Nota Fuente: (IT Governance Institute, 2007), Pag.123, Estados Unidos

4.3.2.4 DS13 Administración de Operaciones

Cuadro 18

Análisis Proceso DS13

DS13.1 Procedimientos e Instrucciones de Operación				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Evidenciar la existencia de procedimientos estándares y su aplicación en las operaciones de TI. -Identificar un procedimiento operacional para analizar la claridad del contexto. -Evidenciar si la Gerencia de TI tiene identificadas las operaciones y responsabilidades. -Evaluar que en los procedimientos operacionales estén definidos los roles y responsabilidades.	Gerente de TI Analista RRHH	-Procedimientos operacionales -Matriz de funciones y responsabilidades -Cronogramas mensuales de trabajo -Perfil de cargo	-La Gerencia de TI comunica que no se han documentado procedimientos operacionales, todas las tareas se las realiza de acuerdo a la experiencia del personal. -Se evidencia que la Gerencia de TI si tiene identificadas las operaciones y responsabilidades sin embargo estas no están documentadas. -Se ha evidenciado que recursos humanos si tiene establecido el perfil de cargo y la descripción de funciones (Anexo 8) para los integrantes del área de TI, sin embargo no han sido difundidos.	05/09/2012

Continúa →

DS13.2 Programación de Tareas				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
- Verificar que la Gerencia de TI mantenga un registro y programación de las tareas. - Verificar que la Gerencia de TI haga un seguimiento al resultado de las tareas programadas y reprogramación de las tareas no ejecutadas. - Verificar la metodología que la Gerencia de TI utiliza para el análisis del uso de recursos para el cumplimiento de las tareas programadas.	Gerente de TI	-Cronogramas mensuales de trabajo -Documento Hitos y Cronogramas -Programación de Actividades TI&C -Documento Implementación Servidores Blade -Documento Implementación SAP	- La Gerencia de TI realiza reuniones mensuales de trabajo con el personal a su cargo, se establecen responsables y se definen cronogramas, los cronogramas son enviados por correo electrónico a los responsables. - Se evidencia que la Gerencia de TI si realiza un seguimiento a las tareas y registra los resultados utiliza dos registros: Hitos y Cronogramas y Programación de Actividades TI&C (Anexo 2). - Se verifica que la Gerencia de TI crea proyectos tecnológicos en base a la metodología aprobada por la Gerencia para todas las áreas, especificando, el Problema Actual, Objetivo, Alcance, Costos, Responsables y Cronogramas de implementación, esta metodología se evidencia en los documentos analizados: Implementación Servidores Blade e Implementación SAP.	06/09/2012

Continúa →

DS13.3 Monitoreo de la Infraestructura de TI				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Verificar las operaciones con hardware --Revisar los procedimientos de administración de la capacidad --Revisar el plan de adquisición de hardware --Revisar los criterios de adquisición de computadores --Revisar los controles de administración de cambios (hardware) -Verificar las operaciones con Sistemas Operativos --Revisar los procedimientos de selección del software del sistema --Revisar las actividades del mantenimiento del software --Licenciamientos	Gerente de TI Analista de Sistemas	-Registro Mantenimientos de Hardware -Plan de adquisición de Hardware -Política de reposición de equipos de computación -Inventario de Hardware -Licenciamiento -Inventario de Software -Contratos con	- Se evidencia la existencia de contratos con proveedores para el mantenimiento de ups, copiadoras, aires acondicionados, impresoras. - Se evidencia el análisis de capacidad de los servidores pero no se ha establecido un procedimiento. - El plan de adquisición es anual y sujeto al presupuesto aprobado por la Gerencia General a inicios de año. - Se evidencia la existencia de una política para reposición de equipos cada 3 años y de acuerdo a los proyectos presentados por cada área. - Se realiza el registro de cambios de componentes de hardware en el inventario general. - Se evidencia la política que establece el uso de software Microsoft a nivel corporativo y para software del negocio los establecidos por la industria.	07/09/2012 y 08/09/2012

Continúa →

-Revisiones de control operativo de redes --Verificar Planes de implementación y de prueba para el hardware y los enlaces de comunicaciones de red --Analizar el diseño de la red para asegurar que una falla de servicio tendrá un efecto mínimo -- Analizar los cambios realizados al software del sistema operativo utilizado por la red y verificar si estos están siendo controlados.		terceros para servicios de Software -Mantenimiento de usuarios en el PDC -Aplicación de parches de seguridad	- Se evidencia que los mantenimientos de software se los realiza mediante los contratos de mantenimiento con los proveedores, en la aplicación crítica del negocio existe un cronograma de renovación de licencias, con tiempos, cronogramas, costo y contactos. - No se evidencia las versiones de software y aplicaciones en el inventario. - Se evidencia el cumplimiento en cuanto a licencias de software Microsoft, Trend Micro, Geographics, Petrel, OFM, Ecrin, Data Protector, Fortinet, Strategic. -Se evidencia los planes de implementación de nuevo hardware como proyectos presentados y aprobados por la gerencia, análisis de riesgos y resultado de las pruebas respectivas. -Los parches de servidores se los aplica manualmente pero no se los registra, el parche de equipos clientes se lo administra por medio del servidor WSUS y registra el versionamiento.	

Continúa →

-Revisar que los usuarios sólo tienen acceso a las aplicaciones, procesadores de transacciones y conjuntos de datos autorizados. --Se han implementado políticas y procedimientos de seguridad apropiados.		-Usuarios y accesos al Sistema ERP SAP -Política cambio de contraseñas en los sistemas Listado de servicios críticos - proveedores.	- Se evidencia el registro de usuarios activos e inactivos, se utiliza Active Directory para el acceso de los usuarios a la red y se evidencia que 3 de 3 usuarios despedidos han sido dados de baja en el sistema. Los accesos al sistema ERP son administrados por casa matriz. - Las Políticas de seguridad no están actualizadas, mantienen fecha del año 2009. - No se está cumpliendo con la política en cuanto al uso de formatos. No existe un procedimiento definido en caso de que las personas de TI no se encuentren y existiera fallos. No se han definido una lista de contactos de los proveedores de servicio que ayuden a resolver problemas de TI. - No se evidencia la divulgación de la política de seguridad a los usuarios.	10/09/2012
-Revisión de logs en servidores -Determinar consistencia del cronograma para trabajos urgentes o que requieren ser repetidos.		-Logs de Aplicación, Seguridad y	- No se ha establecido un cronograma para revisión de logs de servidores, se envía al mes un reporte de los logs emitidos por el firewall.	11/09/2012 y 12/09/2012

Continúa →

--Determinar si se han identificado las aplicaciones críticas. --Determinar si se emplean procedimientos para facilitar el uso óptimo de recursos --Determinar si la cantidad de personal es adecuada. --Revisar los procedimientos para recolectar, reportar y analizar indicadores clave de desempeño (KPI). -Revisar reportes de gestión de problemas --Revisar los procedimientos usados para registrar, evaluar y resolver o escalar cualquier problema. --Determinar que los problemas significativos y recurrentes han sido identificados y se están tomando acciones al respecto. --Revisar documentación de las operaciones. --Revisar los registros de llamadas al Service Desk.		Sistema en servidores. - Visor de Eventos. - Administrador de Tareas. -Políticas de seguridad -Indicadores del desempeño del área	- No se ha determinado las aplicaciones críticas. -No está formalizado el procedimiento de uso de recursos aunque si están implementadas algunas medidas. - No se ha establecido una herramienta que permita medir la capacidad del proceso del área de TI, se está consciente de la necesidad de contratar nuevo personal. - No se ha establecido procedimientos para recolectar, reportar, analizar indicadores que permitan evaluar el desempeño del analista de sistemas. - No se evidencia un procedimiento formal para la gestión de problemas. - La solución de problemas o incidentes no se los documenta se resuelven conforme ocurren. - No existe documentación de la gestión de operaciones. -No existen registros de las llamadas al departamento de soporte.	

Continúa →

DS13.4 Documentos Sensitivos y Dispositivos de Salida				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
- Verificar que la Gerencia de TI tenga identificados a todos los activos críticos de TI. - Verificar que el lugar de almacenamiento de los activos críticos de TI sea el adecuado. - Verificar que los registros de los activos críticos de TI tal como inventarios, sean los vigentes y se mantengan actualizados.	Analista de Sistemas	- Inventario de activos críticos de TI - Evidencia del cuarto de servidores - Registro de temperatura - Registro de acceso del personal al cuarto de servidores.	- Se evidencia que la Gerencia de TI conoce cuales son los activos críticos de TI, estos se encuentran identificados en el Plan de Continuidad del Negocio pero la información está incompleta. - Se evidencia que los activos críticos de TI tales como servidores se encuentran en lugares adecuados con la seguridad, temperatura necesaria, los activos de software críticos como Active Directory, aplicaciones de perforación, extracción se encuentran en servidores adecuados y la seguridad de que solo personal autorizado puede ingresar a ellas. -El área de servidores se encuentra debidamente restringida y su acceso es sólo a personal autorizado a través de tarjetas magnéticas, posee un registro del personal (Anexo 23) que ingresa al área.	13/09/2012

Continúa →

DS13.5 Mantenimiento Preventivo del Hardware				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Verificar la existencia de un Inventario de Hardware. -Verificar si la Gerencia de TI mantiene una Planificación para el mantenimiento de Hardware. -Verificar el cumplimiento de los cronogramas de mantenimiento. -Verificar si los responsables del mantenimiento son los adecuados. -Evidenciar si existe una comunicación previa a usuarios finales y clientes afectados.	Gerente de TI Analista de Sistemas Analista de Compras	- Inventario de Hardware - Planes de mantenimiento - Calificación de proveedores - Contratos con terceros - Correos electrónicos indicando cronograma de mantenimientos - Registro de mantenimientos realizados.	- Se evidencia la existencia de inventario de Hardware actualizado y completo. - Se evidencia el plan de mantenimiento para ups, copiadoras, impresora pero no para computadoras. - Se ha evidenciado los cronogramas de mantenimiento: copiadoras 2 meses, ups 3 meses, impresoras 6 meses. - Se evidencia la existencia de contratos vigentes con terceros, servicio de comunicaciones TELCONET, soporte Microsoft con la empresa DOS (Anexo 17). - El mantenimiento de computadoras se lo hace internamente sin la necesidad de contratar a terceros, se evidencia el registro de mantenimiento del año 2012 firmado por el usuario (Anexo 24)	13/09/2012

Continúa →

INDICADORES DE DESEMPEÑO

Tabla 27

Indicadores de Desempeño DS13

INDICADORES AÑO 2012	**PORCENTAJE**
# de niveles de servicio impactados por incidentes operativos	0=100%
# horas sin servicio, no planeadas, causadas por incidentes en las operaciones en el año 2012	16/8760=0.18%
# de incidentes, de tiempo sin servicio, causados por la desviación de los procedimientos de operaciones	1
# de incidentes de tiempo sin servicio y de retrasos causados por procedimientos inadecuados	0
% de peticiones y trabajos programados que no se cumplen a tiempo	2/10=20%
% de activos de hardware incluidos en los programas de mantenimiento preventivo	100 %
% de cumplimiento en la frecuencia de actualización de los procedimientos operativos	0%

Nota Fuente: (IT Governance Institute, 2007), Pag.151, Estados Unidos

4.3.3 AI ADQUIRIR E IMPLEMENTAR

4.3.3.1 AI5 Adquirir Recursos de TI

Cuadro 19

Análisis Proceso AI5

AI5.1 Control de Adquisición				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Revisar un procedimiento de compras a nivel de empresa. -Verificar el cumplimiento del procedimiento de compras por parte de TI en las áreas de infraestructura, licenciamiento, renovaciones.	Jefe de Compras	Manual de compras y contrataciones	Se verifica la existencia del procedimiento de compras-contrataciones hasta el año 2009. En el documento Manual de compras y contrataciones no se han realizado revisiones al documento y el mismo no refleja lo que sucede en el proceso de adquisiciones debido a que no está integrado con la incorporación de SAP que modificó dicho proceso. -No se cumple con el procedimiento de compras debido a que está desactualizado y no hace referencia al sistema SAP implementado desde enero 2011.	17/09/2012

Continúa →

AI5.2 Administración de Contratos con Proveedores				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Revisar Políticas y estándares de contratos para proveedores. -Revisar la definición de responsabilidades por medio de SLA's. -Revisar inclusión de temas legales, financieros, organizacionales, documentales, de rendimiento, de seguridad, aspectos de responsabilidad.	Jefe de Compras. Gerencia de TI.	Formato de solicitud de contratos. Contratos varios	Si se tiene definido un procedimiento para la generación de contratos el documento es Formato de Solicitud de Contratos (Anexo 25). -No se ha evidenciado los documentos de Acuerdo de nivel de servicio en los contratos auditados. Se ha evidenciado los requerimientos legales, financieros, organizacionales, documentales, de rendimiento y seguridad en los contratos auditados, los contratos son revisados y aprobados por el departamento legal.	17/09/2012
AI5.3 Selección de Proveedores				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Evidenciar la existencia del proceso de selección de proveedores. -Revisar los criterios de pedido definidos. -Para adquisición de software revisar los	Jefe de Compras. Gerencia de TI.	-Proceso de calificación de proveedores. -Formatos de	Sí existe un proceso de selección de proveedores por medio de la empresa SGS quien lo hace de acuerdo a parámetros como precio, tiempo de entrega, calidad etc., son categorizados e ingresados a la base de datos de	17/09/2012

Continúa →

derechos y obligaciones en cuanto a garantías, mantenimientos, actualizaciones. -Averiguar los términos legales en cuanto a licenciamiento y propiedad intelectual. -Para adquisición de hardware determinar la existencia de definiciones en SLA´s, procedimientos de mantenimiento, controles de acceso, seguridad, rendimiento, condiciones de pago y procedimientos de arbitraje. -Evidenciar que la documentación se mantiene.	Legal	requisición. -Formato de orden de compra. -Ley de comercio electrónico. -Inventario de aplicaciones críticas. -Contratos de adquisición. -Revisión de contratos del área.	proveedores que posteriormente son utilizados por el área de compras para solicitar productos o servicios de acuerdo a la clasificación generada. Sobre el software que utiliza la organización existe un inventario de aplicaciones críticas con condiciones de renovación, garantía y valores de mantenimiento así como los términos de las actualizaciones. -Existe un procedimiento que establece el uso de los formatos de pedido llamado Requisición y también del formato de Orden de Compra (Anexo 26) que incluye parámetros de uso y control así como de aprobación contra un presupuesto que permite disponer de un control y seguimiento de lo solicitado. -No se logra evidenciar que el área legal tenga claro los parámetros en los que se enmarca el uso del software, ni de la renovación o las condiciones de propiedad intelectual de lo desarrollado en la empresa. Se evidencia que la documentación está bien mantenida y en orden.	

Continúa →

AI5.4 Adquisición de Recursos de TI				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Determinar si todos los acuerdos y procedimiento de compras son cumplidos. -Evidenciar si las adquisiciones han sido revisadas y aprobadas por las instancias adecuadas y si cumplen con los términos legales. Inspeccionar que los contratos han sido revisados y aprobados. Averiguar si los procesos han sido establecidos y se utilizan para la adquisición de software e infraestructura. -Realizar una revisión de los procedimientos para verificar su cumplimiento. .Verificar si todas las adquisiciones de hardware y software son registradas.	Gerente de TI Control Interno Jefe de Compras	Manual de compras y contrataciones. -Revisión de reportes de SAP. -Revisión de contratos principales. -Registro de control de gastos de SAP -Manual de compras y contrataciones -Revisión de contratos de software. -Documentos de órdenes de compra.	-Se cumple con los procedimientos que compras ha establecido pero estos no están actualizados. -El proceso de compras con sus respectivas aprobaciones se cumple en todos los procesos desde los de menor cuantía hasta los de proyectos debido a la utilización de SAP que regula montos y aprobaciones. -Se evidencia que explícitamente para la adquisición de software e infraestructura no se tiene un proceso definido, forma parte del proceso general de compras. -Se evidencia la existencia de contratos de licenciamiento con Microsoft y Software de Exploración bien definidos y mantenidos por más de 5 años (Anexo 27). -Se evidencia que las compras de software y hardware están registrados en el área financiera y las compras mayores a 1000 usd son registrados como activos fijos.	17/09/2012

Continúa →

INDICADORES DE DESEMPEÑO

Tabla 28

Indicadores de Desempeño AI5

INDICADORES AÑO 2012	**PORCENTAJE**
# de inconvenientes en los contratos de compra	0/0=100%
% de adquisiciones que cumplen con las políticas y procedimientos de compras	100%
# de solicitudes de adquisición que se cierran a tiempo	100%
# de modificaciones del proveedor para la misma clase de bienes y servicios adquiridos	0

Nota Fuente: (IT Governance Institute, 2007), Pag.91, Estados Unidos

4.3.4 ME MONITOREAR Y EVALUAR

4.3.4.1 ME1 Monitorear y Evaluar el Desempeño de TI

Cuadro 20

Análisis Proceso ME1

ME1.1 Enfoque de Monitoreo				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Evidenciar que la Gerencia de TI haya definido un marco de trabajo para monitoreo del desempeño. -Evidenciar que se hayan diseñado y se estén utilizando reportes para medición del desempeño. -Analizar la información utilizada para emitir los reportes de desempeño de TI. -Evidenciar la existencia de indicadores de desempeño de TI y que estos se encuentran alineados con las necesidades de la Dirección.	Gerente General Gerente de TI Usuarios	-Documento Hitos y Cronogramas - Programación de Actividades TI&C -Revisión Software Strategic	- Se evidencia que el marco de trabajo se denomina Hitos y Cronogramas y define los objetivos a ser alcanzados en un año, también se evidencia otro formato denominado programación de actividades TI&C (Anexo 2). - Se evidencia que el reporte de desempeño se denomina Hitos y Cronogramas. - Se evidencia que el análisis de indicadores de desempeño a nivel corporativo se realiza a través del software Strategic (Anexo 28) en donde se registra la medición del desempeño del área tecnológica. - Se evidencia que la Dirección aprueba las actividades a	18/09/2012

Continúa →

-Realizar una entrevista al cliente interno sobre el desempeño de TI.			monitorear de cada departamento para asegurar que los procesos monitoreados son los requeridos por el negocio. - Se evidencia que el alcance de los procesos a ser monitoreados están definidos a inicios de año con reuniones entre la Dirección y las Gerencias de áreas.	
ME1.2 Definición y Recolección de Datos de Monitoreo				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Evidenciar que se hayan definido los objetivos de desempeño y que estos sean conocidos y aprobados por la Gerencia General. -Verificar que los indicadores mantengan relación con los objetivos de desempeño.	Gerente de TI	-Revisión Software Strategic	- Se evidencia que la definición de los objetivos de desempeño se hace de acuerdo a los objetivos del área de TI y su cumplimiento, estos objetivos son aprobados por la Gerencia General. - Se evidencia que existen reuniones mensuales con el área de planificación en donde se ingresa la información de cumplimiento al sistema Strategic. La recolección de datos es mensual y obligatoria para cada área. El software Strategic genera un resumen con los datos obtenidos.	18/09/2012

Continúa →

ME1.3 Método de Monitoreo				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
- Evidenciar que exista una relación entre procesos críticos de TI, sistemas de monitoreo y reportes de desempeño. - Análisis de los reportes de desempeño para determinar si están completos y legibles.	Gerente de TI	-Procesos Críticos de TI -Reportes de Desempeño -Sistemas de Monitoreo -Sistema Strategic	- No se han definido los procesos críticos de TI, sólo son conocidos por el Gerente de TI, en base a esto no se han establecido sistemas de monitoreo y reportes de desempeño que mantengan relación unos con otros. - El sistema Strategic se lo utiliza también para generar los reportes de desempeño en base a tareas establecidas, son más cumplimiento de tareas que oportunidades de mejora.	19/09/2012
ME1.4 Evaluación del Desempeño				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
- Realizar entrevista a usuarios finales para evidenciar si se han realizado recomendaciones de desempeño y estas han sido tomadas en cuenta. - Evidenciar que resultados negativos en los reportes de desempeño se gestionan por	Gerente de TI Usuarios	- Registro de acciones correctivas	- Se evidencia que el levantamiento de acciones correctivas no está formalizado, no se gestionan acciones correctivas como tal, sino que se generan como proyectos o nuevas adquisiciones de acuerdo a las necesidades. - Se evidencia que la Gerencia de TI está evaluando el desempeño del analista de sistemas en base al	19/09/2012

Continúa →

medio de acciones correctivas.			cronograma de trabajo mensual, no se han creado indicadores dentro del departamento de TI.	
ME1.5 Reportes al Consejo Directivo y a Ejecutivos				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
- Evidenciar que los reportes ejecutivos de desempeño son diseñados de acuerdo a las necesidades de la Dirección y si son revisados frecuentemente por la misma. - Evidenciar que los reportes son aprobados por la Dirección. - Evidenciar que la Dirección aprueba los cambios a los métodos de desempeño cuando estos se desvían de los objetivos.	Gerente General Gerente de TI	-Sistema Strategic -Reportes de Desempeño	- Se evidencia que el sistema Strategic contiene los formatos de reportes de desempeño de acuerdo a las necesidades de la Dirección. - Se evidencia que los reportes son emitidos mensualmente para el análisis y aprobados por la Dirección. - En este caso no es necesario una gestión de versiones por cuanto la información siempre está actualizada y con el formato de reporte vigente. -Se evidencia que cuando el desempeño no es el adecuado se toman medidas pero éstas no son formalizadas.	22/09/2012

Continúa →

ME1.6 Acciones Correctivas				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Evidenciar que existe un procedimiento para la gestión de acciones correctivas en lo que respecta al desvío de los objetivos de desempeño. -Evidenciar que se tienen asignados responsables para el cumplimiento de las acciones correctivas y que se establecen cronogramas de cumplimiento. -Evidenciar que se realizan seguimiento a los resultados de las acciones correctivas.	Gerente de TI	- Procedimiento de acciones correctivas	- No se ha implementado un procedimiento para la gestión de acciones correctivas. - Se evidencia que no se realiza gestión de acciones correctivas pero se asignan tareas cuando el objetivo no ha sido cumplido y el seguimiento lo hace cada Gerente de área en base a cronogramas.	22/09/2012

Continúa →

INDICADORES DE DESEMPEÑO

Tabla 29

Indicadores de Desempeño ME1

INDICADORES AÑO 2012	**PORCENTAJE**
# de cambios a las metas de TI en el año 2012	1/31=4%
% de procesos críticos de TI monitoreados en el desempeño	100%
# de acciones de mejoramiento impulsadas por las actividades de monitoreo	100%
# de metas de TI cumplidas en el año 2012	90%

Nota Fuente: (IT Governance Institute, 2007), Pag.155, Estados Unidos

4.3.4.2 ME3 Garantizar el Cumplimiento con Requerimientos Externos

Cuadro 21

Análisis Proceso ME3

ME3.1 Identificar los Requerimientos de las Leyes, Regulaciones y Cumplimientos Contractuales				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Evidenciar la existencia de un inventario de aspectos legales. -Evidenciar que en los procedimientos de TI se incluya el manejo de los requerimientos legales, regulatorios y contractuales. -Evidenciar una forma de priorización de los requerimientos de acuerdo a su importancia, frecuencia e impacto, -Evidenciar que se realiza una revisión frecuente de los incumplimientos y las sanciones.	Dpto. Legal Gerencia de TI	- Matriz de aspectos legales	- Se evidencia la existencia de una matriz de aspectos legales (Anexo 29), la cual es actualizada por el Departamento Legal. - TI no ha formalizado aún procedimientos en donde se pueda evidenciar la inclusión de requerimientos legales, regulatorios y contractuales. - Se evidencia que en la matriz de aspectos legales se visualiza por importancia y por tema es decir se encuentra bien categorizada.	26/09/2012

Continúa →

ME3.2 Optimizar la Respuesta a Requerimientos Externos				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
- Evidenciar que en las políticas y procedimientos se definan hitos para el cumplimiento de las leyes, requerimientos regulatorios y contractuales. - Realizar una entrevista a los clientes internos para evidenciar si ellos conocen y entienden los requerimientos legales y regulatorios de TI de los que forman parte.	Gerencia de TI Usuarios Analista de RRHH	- Política de confidencialidad de información - Licenciamiento - Contratos de trabajo.	- Se evidencia que en el contrato de trabajo de los empleados se ha añadido una cláusula de confidencialidad de información y la penalidad que conlleva el incumplimiento a esta norma, 3 de 3 usuarios entrevistados conocen este antecedente. - La Gerencia de TI mantiene una política de uso de software legal, la sanción al incumplimiento de la política. 3 de 3 usuarios entrevistados conocen este antecedente.	26/09/2012
ME3.3 Evaluación del Cumplimiento con Requerimientos Externos				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
- Evidenciar que hayan existido sanciones o pérdidas financieras ocasionadas por el incumplimiento legal o regulatorio de TI, verificar que se hayan tomado medidas correctivas.	Gerencia General	- Ley de comercio electrónico - Ley de propiedad intelectual	- Se evidencia que no han existido sanciones o pérdidas económicas por el incumplimiento de leyes o regulaciones de TI, las leyes que aplican son: La ley de comercio electrónico y de propiedad intelectual.	28/09/2012

Continúa →

ME3.4 Aseguramiento positivo del cumplimiento				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
- Evidenciar un inventario de requerimientos regulatorios y de cronogramas de revisión. - Evidenciar la existencia de un procedimiento para el cumplimiento de requerimientos legales y regulatorios por parte de terceros. - Evidenciar el cumplimiento de leyes y regulaciones por parte de proveedores. - Verificar la existencia de una base de datos que registre contratos y proveedores u otro medio de almacenamiento.	Dpto. Legal Gerencia de TI	- Inventario de requerimientos legales y regulatorios - Contratos con proveedores	- Si existe un inventario de los requerimientos legales y regulatorios (Anexo 29), se encuentra actualizado y lo mantiene el departamento legal. - Se evidencia que en los contratos con terceros se estipula cláusulas de cumplimiento legal, regulatorio y contractual y las sanciones en caso de incumplimiento. - Se evidencia que en el file server se encuentran registrados los contratos con proveedores. - Se evidencia que el área de compras realiza el monitoreo del cumplimiento y no cumplimiento de los compromisos contractuales y ellos son los que ejecutan sanciones y multas.	28/09/2012
ME3.5 Reportes integrados				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
- Analizar reportes corporativos para evidenciar	Gerente de	-Contratos de	- Se evidencia que en los reportes corporativos los requerimientos legales y regulatorios del área de TI no	28/09/2012

Continúa →

que constan los requerimientos legales y regulatorios de TI. - Evidenciar la consistencia de los reportes de TI con los reportes corporativos.	TI	Trabajo -Contratos con terceros	están presentes. - Se evidencia que los reportes corporativos legales y los reportes legales de TI no mantienen una consistencia en cuanto a la forma de distribución, frecuencia de revisión, contenido y formato.	

Continúa →

INDICADORES DE DESEMPEÑO

Tabla 30

Indicadores de Desempeño ME3

INDICADORES AÑO 2012	**PORCENTAJE**
Costo del no cumplimiento de leyes, reglamentos, acuerdos contractuales de TI, incluyendo arreglos y multas	0/0=100%
# de problemas de no cumplimiento reportados a la Gerencia General, o que hayan causado comentarios o vergüenza pública	0/0=100%
# de problemas críticos de no cumplimiento identificados en el año 2012	0/0=100%
% cumplimiento en la frecuencia de revisiones de contratos	1/1=100%
# de eventos por no cumplimiento de contratos	0=100%
Días de entrenamiento por año, referentes al cumplimiento	0%

Nota Fuente: (IT Governance Institute, 2007), Pag.163, Estados Unidos

4.3.4.3 ME4 Proporcionar Gobierno de TI

Cuadro 22

Análisis Proceso ME4

ME4.1 Establecimiento de un Marco de Gobierno de TI				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
Preguntar y confirmar que: -Un proceso existe para alinear el marco de gobierno de TI con el gobierno de la empresa. -El marco de gobierno se basa en un completo modelo de TI y control de procesos y define el liderazgo, la rendición de cuentas clara, roles y responsabilidades, requerimientos de información, estructuras organizativas y prácticas para evitar la ruptura en el control interno y la supervisión. -Exista una adecuada estructura de administración, tales como el comité de	Gerencia de TI	Balanced Scorecard, pagina web de software Strategic. -Política de sistemas, documento de roles y funciones. -Organigrama. -Documentos de hitos y cronogramas, Presupuesto Anual General. -Procedimiento de comunicación de	-Se evidencia la revisión anual del sistema de gestión BSC de la organización (Balanced Scorecard) el cual alinea la estrategia del negocio con todas las áreas incluyendo a TI, pero por medio de un solo indicador. -No existe un marco de gobierno estructurado e implantado, existen elementos de gobierno de TI aislados como política de sistemas, seguridades de acceso, control de respaldos. No se evidencia definición en roles y funciones ni tampoco cumplimiento en procesos de control. -No existe ninguna definición a nivel de estructura de administración de gobierno con lo cual ninguno de los comités, consejos o junta se han establecido, existiendo	08/10/2012

Continúa →

estrategia de TI, comité directivo, consejo de la tecnología, la arquitectura y la junta de revisión del comité de auditoría de TI. -El marco de gobierno de TI se centra en la alineación estratégica, la entrega de valor, gestión de recursos, gestión de riesgos y medición de los resultados. -Existe un proceso para medir y evaluar la prestación de TI, las estrategias y objetivos, y agregar los problemas de gobierno y acciones correctivas en un repositorio de gestión. -Las condiciones de gobierno de TI y los problemas se reportan al órgano de gobierno de supervisión corporativa.		incidentes	un vacío a nivel directivo. -Ciertos elementos de gobierno de TI como política, rendición de cuentas a través de BSC y presupuesto cumple con parámetros de gestión de valor, recursos y riesgos. -En el sistema Strategic se encuentran definidos los objetivos a alcanzar alineados con los objetivos del negocio, que permite evaluar y medir los resultados. No se evidencia un repositorio para problemas ni acciones correctivas. -Se evidencia la comunicación de problemas de TI a la Dirección de la organización sólo en casos de mayor afectación o interrupción de servicios.	

Continúa →

ME4.2 Alineamiento Estratégico				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Inspeccionar la documentación estratégica de TI y evaluar si es compatible con la orientación proporcionada por la junta / alta dirección. Debe reflejar las estrategias de negocio y de TI la alineación adecuada de las operaciones comerciales. -Determinar si el proceso de planificación estratégica de TI incluye la participación de las operaciones comerciales y demuestra la alineación con las estrategias y objetivos de negocio.	Gerencia de Planificación	Documentos de hitos y cronogramas, Presupuesto Anual General, Balanced Scorecard. -Página web de software de Strategic.	-Existe información de elementos de seguridad, riesgos, proyectos, presupuesto que regulan las estrategias de TI pero no están alineadas con la estrategia del negocio. -Están enfocado a las áreas funcionales por lo que no existe una alineación con el negocio. -Los documentos de estrategia de TI reflejan el desarrollo de elementos y tecnología pero sin una alineación de apoyo al negocio ni tampoco un análisis de valor de los proyectos ya implementados.	08/10/2012
ME 4.3 Entrega de Valor				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Confirmar que existe la co-responsabilidad entre el negocio y TI para todas las inversiones en TI.	-Gerencia de Planificación -Gerencia de	-Documento de Hitos y cronogramas.	-Se generan iniciativas de tecnología en todas las áreas y se consolidan en TI. -Existe la documentación por proyectos, áreas y	10/10/2012

Continúa →

-Determinar si existe un proceso efectivo para asegurar que la arquitectura de TI está diseñada para obtener el máximo valor. -Determinar si existe un proceso eficaz para ajustar las inversiones sobre la base de un balance de riesgos, costos y beneficios con los presupuestos y estos ajustes son aceptables. -Inspección de la documentación de TI para evaluar si la empresa ha establecido las prestaciones de TI, incluyendo la flexibilidad para adoptar las futuras necesidades, los tiempos de respuesta y facilidad de uso, la seguridad y la integridad, exactitud y actualidad de la información.	TI	-Diagrama lógico del área de tecnología. -PAG anual y casos de negocio de últimos proyectos. -Control de presupuestos.	presupuesto a nivel mensual. -Para la evaluación del cumplimiento del área de tecnología se lo realiza por medio del cumplimiento de hitos y cronogramas (Anexo 2) el mismo que a su vez alimenta el BSC, pero al ser solamente un elemento dentro de todas las perspectivas no refleja el verdadero valor de tecnología en la organización. -Existen alianzas estratégicas con los proveedores de comunicaciones que aportan mejoras año a año, con los proveedores de hardware se evidencia sesiones informativas de los productos utilizados. -No existe un proceso definido de contribución de valor de TI. -Existe un presupuesto anual (Anexo 4) para ajustar inversiones y la generación de casos de negocio con costos, beneficios y riesgos mejorando las inversiones de TI. -Existen cronogramas para las prestaciones de TI. -Existe rendición de cuentas de presupuesto y	

Continúa →

			cumplimiento de manera mensual. -Existe el informe de costos reales pero no se evidencia la generación de ROI de las inversiones.	
ME 4.4 Administración de Recursos				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Preguntar y confirmar que los recursos de TI son apropiados, los servicios e infraestructura están disponibles para satisfacer los objetivos estratégicos y qué políticas se han establecido para permitir la disponibilidad de los servicios de TI. -Preguntar y confirmar que la infraestructura de TI facilita la creación y el intercambio de información de negocios a un coste óptimo. -Revisar las políticas, procedimientos y procesos establecidos para la gestión de recursos, y verificar que están operando de manera efectiva.	-Gerencia de Planificación. -Gerencia de TI. -Gerencia de RRHH	-Documentos de proyectos. -PAG anual. -Revisión de contrato de comunicaciones. -Revisiones de cumplimiento de presupuesto. -Revisión de enlaces de datos.	-Existen actas para contratos mayores a $10000 dólares. -Los recursos de TI mantienen la operación de la empresa y tienen un nivel de disponibilidad del 98%. No se evidencia políticas que determinen acuerdos internos para disponibilidad de servicios de TI. -La infraestructura permite el intercambio de información a un coste alto hacia casa matriz y a un nivel medio hacia la sucursal del campo. Las políticas de la empresa regulan la prestación de bienes y servicios de acuerdo a los montos definidos por casa matriz. Como fuentes de información y conocimiento se evidencia el desarrollo de la Intranet de la empresa (Anexo 30) que está en una fase inicial.	10/10/2012

Continúa →

-Rastrear elementos a través de las infraestructuras de TI y determinar si la creación y el intercambio de información se facilita con eficacia. -Preguntar y confirmar que las funciones críticas son asignadas y definidas para obtener el máximo valor de TI con personal y recursos apropiados.			Se evidencia la asignación de recursos de manera anual (Anexo 4) con revisiones mensuales de cumplimiento. -Se evidencia una conexión adecuada de recursos entre la unidad administrativa y la unidad de operación con un intercambio de información con limitantes debido al ancho de banda entre las dos unidades. -No existe un detalle de las funciones críticas. -Si existe una definición de roles y funciones (Anexo 8). -No existe procedimiento para la evaluación de la capacidad.	
ME 4.4 Administración de Recursos				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Preguntar y confirmar que los recursos de TI son apropiados, los servicios e infraestructura están disponibles para satisfacer los objetivos estratégicos y qué políticas se han establecido para permitir la disponibilidad de los servicios de TI.	-Gerencia de Planificación. -Gerencia de TI. -Gerencia de RRHH	-Documentos de proyectos. -PAG anual. -Revisión de contrato de comunicaciones.	-Existen actas para contratos mayores a $10000 dólares. -Los recursos de TI mantienen la operación de la empresa y tienen un nivel de disponibilidad del 98%. No se evidencia políticas que determinen acuerdos internos para disponibilidad de servicios de TI. -La infraestructura permite el intercambio de información	10/10/2012

Continúa →

-Preguntar y confirmar que la infraestructura de TI facilita la creación y el intercambio de información de negocios a un coste óptimo. -Revisar las políticas, procedimientos y procesos establecidos para la gestión de recursos, y verificar que están operando de manera efectiva. -Rastrear elementos a través de las infraestructuras de TI y determinar si la creación y el intercambio de información se facilita con eficacia. -Preguntar y confirmar que las funciones críticas son asignadas y definidas para obtener el máximo valor de TI con personal y recursos apropiados. -Revisar la definición de roles y que éstas sean efectivamente asignadas y ejecutadas.		-Revisiones de cumplimiento de presupuesto. -Revisión de enlaces de datos.	a un coste alto hacia casa matriz y a un nivel medio hacia la sucursal del campo. Las políticas de la empresa regulan la prestación de bienes y servicios de acuerdo a los montos definidos por casa matriz. Como fuentes de información y conocimiento se evidencia el desarrollo de la Intranet de la empresa (Anexo 30) que está en una fase inicial. Se evidencia la asignación de recursos de manera anual (Anexo 4) con revisiones mensuales de cumplimiento. -Se evidencia una conexión adecuada de recursos entre la unidad administrativa y la unidad de operación con un intercambio de información con limitantes debido al ancho de banda entre las dos unidades. -No existe un detalle de las funciones críticas. -Si existe una definición de roles y funciones (Anexo 8). -No existe procedimiento para la evaluación de la capacidad.	

Continúa →

ME 4.5 Administración de Riesgos				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Verificar que la gerencia general evalúa los riesgos de TI y costos asociados. -La gerencia general revisa los resultados de los controles implementados para mitigar los riesgos. -Existe un proceso para incluir los riesgos de TI en la gestión de gobierno de TI.	Gerencia General	-Matriz de riesgos	Se presenta una evaluación de riesgos anual (Anexo 5) y proyectos de mitigación de riesgo con valores asociados los mismos que son aprobados o rechazados. La gerencia no revisa los controles implementados. No existe un proceso formal de inclusión de riesgos dentro del gobierno de TI.	10/10/2012
ME 4.6 Medición del Desempeño				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Preguntar y confirmar que: El desempeño de TI se alinea correctamente con las medidas de Balanced Scorecard y se registra su medición. Verificar que los informes incluyen la medida en que los objetivos previstos se han alcanzado y los resultados se han obtenido.	Gerencia de Planificación	Balanced Scorecard, página web de software Strategic.	Se evidencia que en el sistema Strategic (Anexo 31) se registran las puntuaciones a los objetivos del desempeño. La gerencia evalúa mensualmente y aprueba los resultados. El sistema genera reportes mensuales y existen comités ampliados cada trimestre para el análisis de	11/10/2012

Continúa →

El Consejo evalúa las acciones correctivas en caso de problemas en el rendimiento y proporciona una dirección para corregir las causas.			los resultados y toma de medidas correctivas.	

ME 4.7 Aseguramiento Independiente				
Elementos auditables	**Auditado**	**Documentación revisada**	**Observaciones del auditor**	**Fecha**
-Verificar la existencia de un comité de auditoría. -Entrevistar al comité de auditoría y evaluar su conocimiento y conciencia de sus responsabilidades. -Preguntar y confirmar que se han realizado revisiones independientes, certificaciones o acreditaciones de cumplimiento de las políticas, normas y procedimientos. -Inspeccionar físicamente la adecuación de los documentos producidos por las auditorías.	Gerencia de TI	Resultados de auditorías anteriores.	No existe un comité de auditoría debido a que la organización no tiene una cultura de revisión de temas de tecnología. No existe un comité de auditoría. No se evidencia auditorías anteriores.	11/10/2012

Continúa →

INDICADORES DE DESEMPEÑO

Tabla 31

Indicadores de Desempeño ME4

INDICADORES AÑO 2012	**PORCENTAJE**
# de veces que TI se encuentra en la agenda del consejo directivo de manera proactiva	0%
Frecuencia de reportes del consejo directivo sobre TI a las terceras partes interesadas	0%
# de eventos recurrentes de TI en las agendas del consejo directivo	0%
Frecuencia de reportes provenientes de TI hacia el consejo directivo	Mensual 100%
Frecuencia de auditorías de cumplimiento de TI	0%
% del equipo entrenado en gobierno	1 / 2= 50%
Frecuencia en que el gobierno de TI es un punto de la agenda en las reuniones estratégicas/de comité de TI	100%
% de miembros del consejo directivo con entrenamiento o experiencia en gobierno de TI	0
Frecuencia de reportes al consejo directivo sobre encuestas de satisfacción	0

Nota Fuente: (IT Governance Institute, 2007), Pag.167, Estados Unidos

4.4 ESTABLECIMIENTO DEL NIVEL DE MADUREZ DE LA INDUSTRIA

Para determinar el nivel de madurez de la industria de los procesos analizados en este proyecto, se utilizó la encuesta: "**MODELOS DE MADUREZ PARA PROCESOS DE TI EN LA INDUSTRIA PETROLERA**", en donde se detalla cada uno de los niveles de madurez desde 0 No existente, 1 Inicial/Adhoc, 2 Repetible pero intuitivo, 3 Definido, 4 Administrable y Medible y 5 Optimizado, según la metodología COBIT 4.1, el modelo de encuesta se puede evidenciar en el Anexo No. 32 de este documento.

Dicha encuesta fue enviada al responsable del departamento de Tecnología de las principales empresas petroleras y empresas de servicios petroleros, residentes en el Ecuador, para conocer el nivel de madurez de cada proceso seleccionado. Las empresas a las cuales se envió la encuesta fueron:

- Andes Petroleum
- Halliburton
- Ivanhoe del Ecuador
- Schlumberger
- Petroamazonas
- Petrosud
- Qmax
- UDSS Specialized Services Ecuador S.A.

No todas las empresas seleccionadas aceptaron ayudar con el desarrollo de la encuesta debido a políticas internas, de las 8 empresas 3 no enviaron los resultados: Andes Petroleum, Schlumberger y Petrosud, por lo que el universo de empresas se redujo a 5, esto representa a la mitad más uno por lo tanto se procedió a tabular las encuesta con este número de empresas.

Los resultados de la encuesta se detallan a continuación:

Tabla 32

Análisis Resultados Encuesta

	PO 1	**PO 4**	**PO 9**	**AI 5**	**DS 2**	**DS 4**	**DS 5**	**DS1 3**	**ME 1**	**ME 3**	**ME 4**
UDSS Specialized Services Ecuador S.A.	2	1	2	1	0	1	1	2	1	1	1
Halliburton	2	3	2	4	4	3	3	4	3	3	4
Ivanhoe Energy Ecuador Inc.	3	3	4	4	3	3	3	4	3	3	2
Petroamazonas	4	3	4	3	5	3	2	5	5	4	3
Qmax Ecuador	2	2	1	1	2	2	1	1	0	1	1
Promedio de la Industria	**3**	**2**	**3**	**3**	**3**	**2**	**2**	**3**	**2**	**2**	**2**

ANALISIS DE LOS RESULTADOS

Una vez analizada la información se puede generar la siguiente lectura del resultado obtenido:

Las 2 empresas dedicadas a la extracción de crudo como Petroamazonas e Ivanhoe evidencian niveles de madurez 3 Definido, 4 Administrable-Medible y 5 Optimizado.

En el caso de Petroamazonas estos niveles Optimizados se deben a dos factores importantes que corresponden a la madurez de la institución del estado en cuanto su experiencia y trayectoria en el mercado petrolero de 42 años, además de haber incorporado las mejores prácticas de una empresa transnacional como Occidental luego de su salida del país y por tanto operar el bloque 15 del cual la empresa americana estaba a cargo absorbiendo tecnología y mano de obra calificada, con estándares de la industria americana.

En el caso de Ivanhoe los niveles de madurez representan un nivel estandarizado y mejorado con la consideración de que es una empresa de energía nueva en el país con apenas 5 años pero sus prácticas corresponden a un modelo canadiense que es

gestionado desde la casa matriz y replicado en el país siguiendo las guías y prácticas de una transnacional anglosajona.

Las empresas de servicios petroleros la más importante es Halliburton con presencia a nivel mundial y sede en Estados Unidos, que evidencia procesos estandarizados con necesidad de mejoras en la planificación y administración de riesgos.

Las 2 empresas de servicios petroleros restantes UDSS SPECIALIZED SERVICES ECUADOR S.A. y QMAX del Ecuador son empresas de origen canadiense con una presencia en el mercado petrolero menor a 5 años, se puede establecer que sus procesos están aún consolidándose ya que las casas matrices son administrativas lo cual se refleja en el manejo inicial en temas de tecnología.

4.5 ESTABLECIMIENTO DEL NIVEL DE MADUREZ PARA CADA PROCESO

4.5.1 PO PLANEAR Y ORGANIZAR

4.5.1.1 PROCESO: PO1 Definir un Plan Estratégico de TI

Luego de realizar el análisis de los resultados de la auditoría para el proceso DE DEFINIR UN PLAN ESTRATEGICO DE TI, se considera que la empresa ENAP-SIPETROL se encuentra en el nivel 2 de madurez.

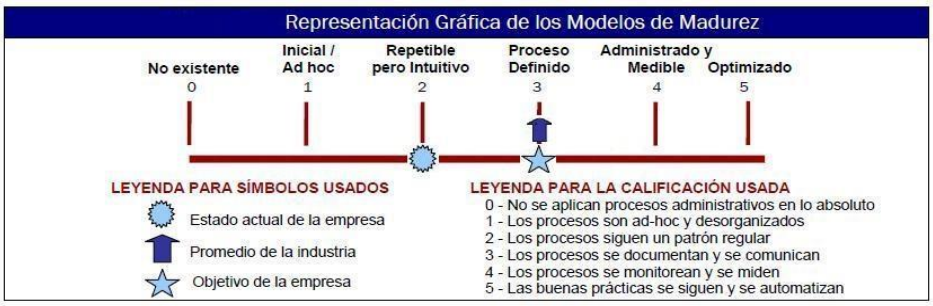


Figura 18 Modelo de Madurez Proceso PO1

Fuente: (IT Governance Institute, 2007), Pag.32, Estados Unidos

Las razones por las que se ha establecido en el nivel 2 de madurez (Repetible pero Intuitivo) son las siguientes:

Solamente se generan casos de negocio para proyectos mayores a $10000 dólares, no existe un control para proyectos menores.

La planificación se realiza anualmente en temas de presupuesto y objetivos empresariales incorporados en el BSC de la empresa, además existe un cronograma de actividades con responsables y seguimiento lo cual se complementa con objetivos y metas, los riesgos no están actualizados, se debe actualizar las políticas (No existe un plan estratégico formalizado).

Los planes tácticos se actualizan en el tiempo, los proyectos se ejecutan sin formalizar ni documentar, no se ha conseguido que exista una alineación entre presupuesto y los planes tácticos de TI.

4.5.1.2 PROCESO: PO4 Definir los Procesos, Organización y Relaciones de TI

Del análisis de los resultados de la auditoría para el proceso de: DEFINIR LOS PROCESOS, ORGANIZACIÓN Y RELACIONES DE TI, se considera que la empresa ENAP-SIPETROL se encuentra en el nivel 1 de madurez.

Figura 19 Modelo de Madurez Proceso PO4

Fuente: (IT Governance Institute, 2007), Pag.46, Estados Unidos

Las razones por las que se ha establecido en el nivel 1 de madurez (Inicial-Ad Hoc) son las siguientes:

Los procesos de TI son conocidos por el gerente de área, no existe un detalle de los procesos de TI, documentación, ni se han definido indicadores para los diferentes procesos.

Por la estructura organizacional, no existe un comité estratégico de TI ni tampoco un comité Directivo de TI, que dirija el rumbo de tecnología en la organización.

Dentro de la organización, el área de TI depende del área de Proyectos e internamente se tiene una estructura dependiente de personal de TI y sin una capacidad de respuesta adecuada para crecimiento futuro debido a que no existe una definición de funciones con roles y responsabilidades.

La política de sistemas que está vigente, data del año 2005 por lo que debe ser actualizada para incluir los tópicos de control en todas las áreas de tecnología, no se ha difundido en la organización, no existe un sistema de Aseguramiento de la calidad ni un sistema que permita el registro de incidentes para evaluar los problemas del área, ni su seguimiento, cierre y posterior valoración.

El tema de riesgos y de seguridad existe a un nivel básico, sin una administración formal, ni responsabilidad definida dentro de la organización, no existe una clasificación de datos solo protección de accesos por medio de permisos de acuerdo a la función.

4.5.1.3 PROCESO: PO9 Evaluar y Administrar los Riesgos de TI

Luego de realizar el análisis de los resultados de la auditoría para el proceso de EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI se considera que la empresa ENAP-SIPETROL se encuentra en el nivel 2 de madurez.

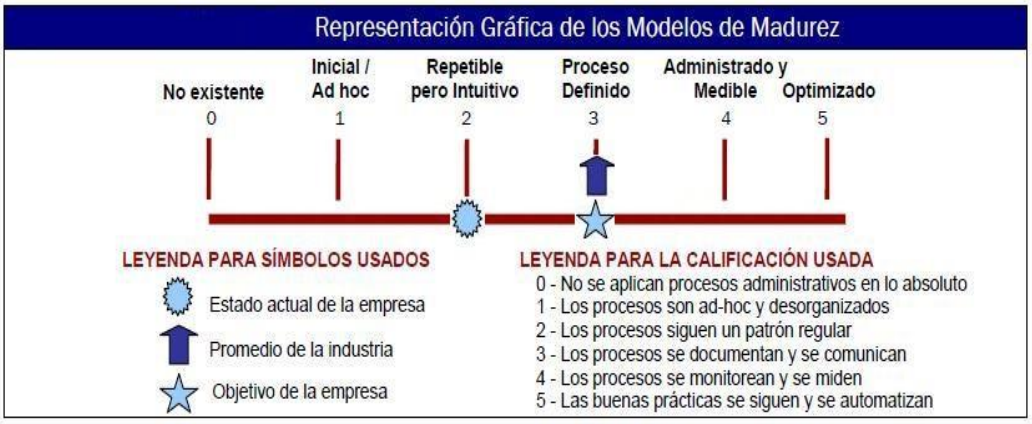


Figura 20 Modelo de Madurez Proceso PO9

Fuente: (IT Governance Institute, 2007), Pag.66, Estados Unidos

Las razones por las que se ha establecido en el nivel 2 de madurez (Los procesos siguen un patrón regular) son las siguientes:

La Gerencia de TI y Gerencias de área de la organización, están conscientes de que los riesgos de TI son importantes y necesitan ser considerados. La Gerencia de TI ha realizado un análisis de los riesgos a los que los servicios y recursos críticos de TI están sujetos y detalla los controles que se deben implementar para mitigar los riesgos. Este análisis se encuentra en el Plan de Continuidad de TI, pero no está completo ni actualizado.

Los riesgos de TI y del negocio son manejados independientemente.

La gestión de riesgos no es un proceso definido en el área de TI, por lo tanto no se han establecido roles y responsabilidades en la evaluación de los riesgos. La documentación está elaborada informalmente, no contiene fechas de elaboración, fechas de actualización, aprobaciones o vigencia, no se ha especificado un sistema de archivos para guardar este tipo de información.

El análisis de riesgos se aplica a proyectos grandes o para resolver problemas. No se analiza periódicamente si los controles implementados han mitigado los riesgos identificados.

4.5.2 DS - ENTREGAR Y DAR SOPORTE

4.5.2.1 PROCESO: DS2 Identificación de Todas la Relaciones con Proveedores

Del análisis de los resultados de la auditoría para el proceso: IDENTIFICACIÓN DE TODAS LAS RELACIONES CON PROVEEDORES, se considera que la empresa ENAP-SIPETROL se encuentra en el nivel 3 de madurez.

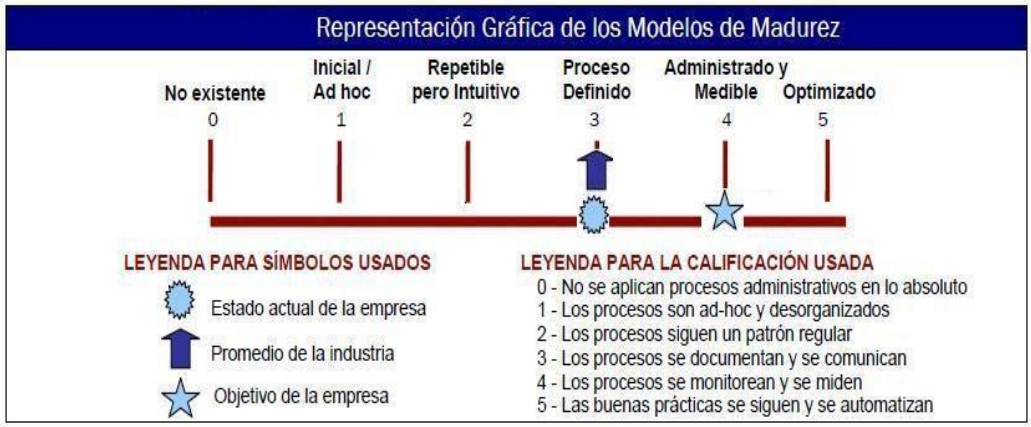


Figura 21 Modelo de Madurez Proceso DS2

Fuente: (IT Governance Institute, 2007), Pag.108, Estados Unidos

razones por las que se ha establecido en el nivel 3 de madurez (Definido) son las siguientes:

La organización dispone de una política de adquisiciones y se cumple en cuanto a los términos y condiciones establecidas con los proveedores a fin de evitar conflicto de intereses.

Debido a los requerimientos del área de compras, existe un registro y control sobre proveedores, pero no se han definido SLA’s con los mismos afectando por tanto el compromiso en cuanto a tiempos de respuesta.

No se mantiene una base de datos de proveedores y servicios críticos, no se ha registrado datos del contacto de los proveedores para localizarlos fácilmente en el caso de presentarse un incidente, sólo los conoce el Gerente de TI.

4.5.2.2 PROCESO: DS4 Garantizar la Continuidad del Servicio

Luego de realizar el análisis de los resultados de la auditoría para el proceso de GARANTIZAR LA CONTINUIDAD DEL SERVICIO se considera que la empresa ENAP-SIPETROL se encuentra en el nivel 1 de madurez.

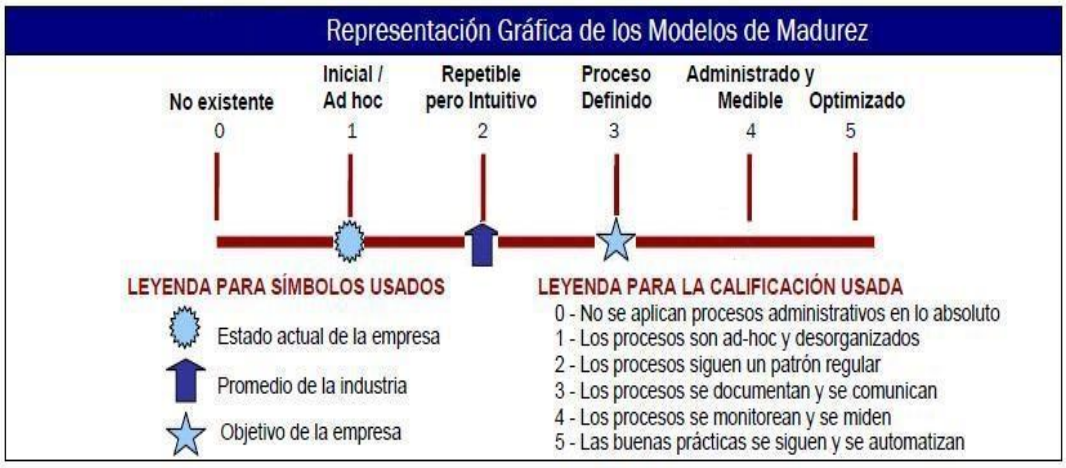


Figura 22 Modelo de Madurez Proceso DS4

Fuente: (IT Governance Institute, 2007), Pag.116, Estados Unidos

Las razones por las que se ha establecido en el nivel 1 de madurez (Los procesos son ad-hoc y desorganizados) son las siguientes:

La Gerencia de TI conoce la necesidad de mantener la continuidad de los servicios, está desarrollando el Plan de Continuidad de TI en base a los servicios y recursos que TI brinda a la organización, aún no se han definido responsables, tampoco se tiene una fecha de culminación del documento o una fecha para aprobación por la Gerencia General.

No existen reportes de disponibilidad de servicios.

Se debe actualizar el inventario de los servicios y recursos críticos de TI.

La elaboración del Plan no se encuentra formalizada, ni mantiene una estructura y secuencia lógica, no se ha identificado una metodología apropiada. Es un documento informal.

4.5.2.3 PROCESO: DS5 Garantizar la Seguridad de los Sistemas

Del análisis de los resultados de la auditoría para el proceso: GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS, se considera que la empresa ENAP-SIPETROL se encuentra en el nivel 1 de madurez.

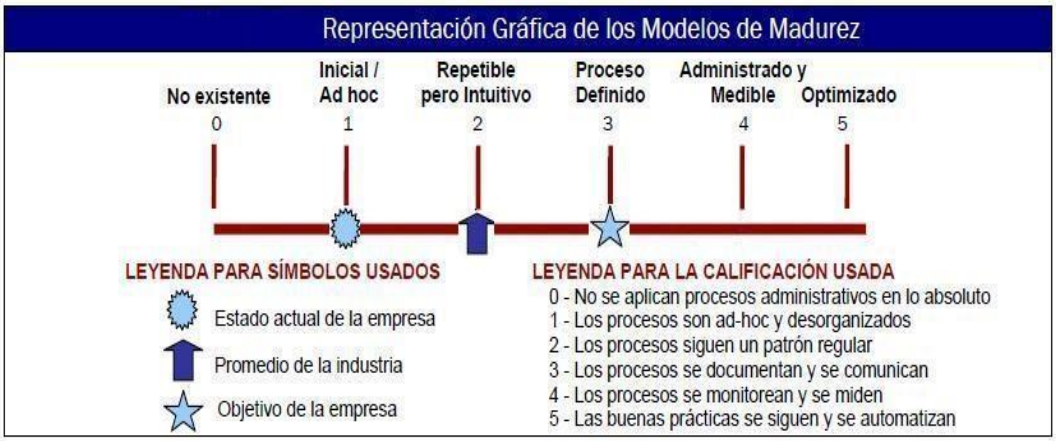


Figura 23 Modelo de Madurez Proceso DS5

Fuente: (IT Governance Institute, 2007), Pag.120, Estados Unidos

Las razones por las que se ha establecido en el nivel 1 de madurez (Inicial/Ad-hoc) son las siguientes:

La organización no dispone de un tratamiento adecuado sobre los riesgos y sobre temas de seguridad, además no existe la conciencia de su importancia y la necesidad de contar con un comité que administre la seguridad informática.

Debido a lo anterior, no existe una visión de seguridad en temas de manejo de información ni de manejo de tecnologías. Se cumple en cuanto al control de accesos por medio de una identificación única para el usuario así como un cumplimiento en cuanto al acceso a los sitios de información de manera consistente y estructurada.

En lo que concierne al control de la información, este es mínimo y no existe conciencia de su importancia ya que el nivel de protección de datos es básico, la administración de riesgos mínimo y no es repetible con controles.

En cuanto a definiciones no existe un sistema que maneje incidentes de seguridad, no están identificados proveedores o servicios clave, ni los puntos de contacto, ni se dispone de un proceso para manejo de incidentes de seguridad.

El control en cuanto a virus está definido instalado y actualizado en un 100%, existe un control para el tráfico de datos en la red pero no existe una identificación de elementos críticos y no existe un proceso de protección de la información por medio de encriptación.

4.5.2.4 PROCESO: DS13 Administración de Operaciones

Luego de realizar el análisis de los resultados de la auditoría para el proceso de ADMINISTRACION DE OPERACIONES se considera que la empresa ENAP-SIPETROL se encuentra en el nivel 2 de madurez.

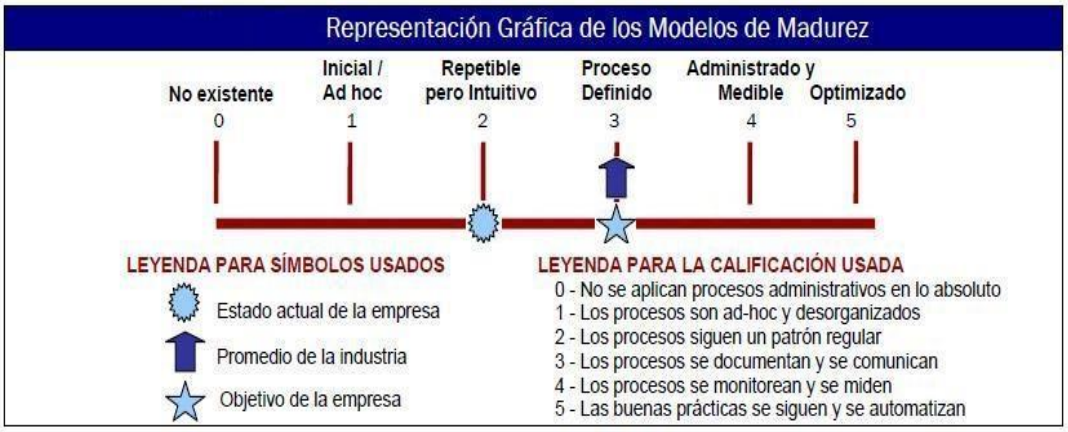


Figura 24 Modelo de Madurez Proceso DS13

Fuente: (IT Governance Institute, 2007), Pag.152, Estados Unidos

Las razones por las que se ha establecido en el nivel 2 de madurez (Los procesos siguen un patrón regular) son las siguientes:

La organización conoce las actividades de soporte que brinda TI y aprueba los presupuestos anuales presentados por la Gerencia de TI. Las operaciones de soporte son conocidas tanto por el Gerente de TI como por el Analista de Sistemas, ambos están en la capacidad de solucionar los problemas de soporte, las operaciones son informales y de acuerdo a la experiencia de quien las atiende. No se han documentado procedimientos operacionales que describan qué hacer, cuándo y en qué orden.

4.5.3 AI ADQUIRIR E IMPLEMENTAR

4.5.3.1 PROCESO: AI5 Adquirir Recursos de TI

Del análisis de los resultados de la auditoría para el proceso: Adquirir recursos de TI, se considera que la empresa ENAP-SIPETROL se encuentra en el nivel 1 de madurez.

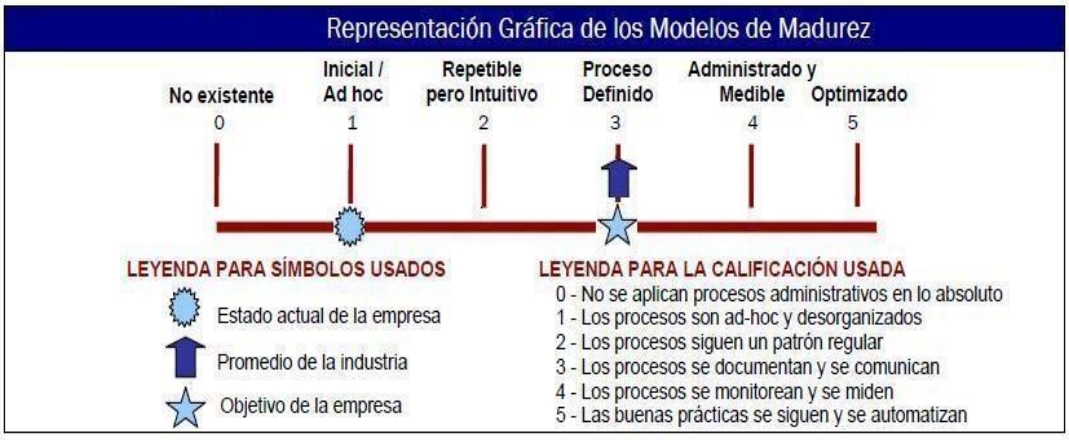


Figura 25 Modelo de Madurez Proceso AI5

Fuente: (IT Governance Institute, 2007), Pago. 92, Estados Unidos

Las razones por las que se ha establecido en el nivel 1 de madurez (Inicial / Ad Hoc) son las siguientes:

La gerencia de TI conoce la necesidad de crear políticas y procedimientos en lo que respecta a la adquisición de recursos de TI, esta necesidad no es conocida por la

gerencia general, tampoco se ha considerado en el proceso de adquisiciones de la organización.

Los contratos de TI con los proveedores se cumplen con todos los términos legales y tienen asignados responsables para algunos servicios de TI, falta mayor formalidad en realizar contratos con todos los proveedores.

Los procesos de adquisición se utilizan principalmente en proyectos donde la inversión es mayor a $10000 usd.

Se ha estandarizado el uso de software Microsoft en la organización, no se ha estandarizado el uso de hardware.

4.5.4 ME MONITOREAR Y EVALUAR

4.5.4.1 PROCESO: ME1 Monitorear y Evaluar el Desempeño de TI

Luego de realizar el análisis de los resultados de la auditoría para el proceso de MONITOREAR Y EVALUAR EL DESEMPEÑO DE TI se considera que la empresa ENAP-SIPETROL se encuentra en el nivel 3 de madurez.

Figura 26 Modelo de Madurez Proceso ME1

Fuente: (IT Governance Institute, 2007), pág. 156, Estados Unidos

Las razones por las que se ha establecido en el nivel 3 de madurez (Los procesos se documentan y comunican) son las siguientes:

Enap-Sipetrol ha definido un marco de trabajo para evaluar y medir el desempeño a todas las áreas de la organización, ha implementado un sistema informático en línea "STRATEGIC", en donde cada Gerente de Área tiene definidos los objetivos a alcanzar mensualmente. El Gerente de TI puede ingresar los resultados del departamento hasta 5 días después del siguiente mes. El sistema STRATEGIC presenta los resultados a través de reportes diseñados en base a los requerimientos de la Gerencia General. El sistema mantiene datos históricos. Los criterios utilizados para medir el desempeño de TI se basan en el ámbito financiero, de estrategias, de satisfacción del cliente y nuevos proyectos.

La Gerencia de TI evalúa el desempeño del Analista de Sistema en base al cronograma de trabajo mensual asignado a él, no se tienen creados indicadores de desempeño dentro del departamento de TI.

4.5.4.2 PROCESO: ME3 Garantizar el Cumplimiento con Requerimientos Externos

Luego de realizar el análisis de los resultados de la auditoría para el proceso de MONITOREAR Y EVALUAR EL DESEMPEÑO DE TI se considera que la empresa ENAP-SIPETROL se encuentra en el nivel 3 de madurez.

Figura 27 Modelo de Madurez Proceso ME3

Fuente: (IT Governance Institute, 2007), Pag.164, Estados Unidos

Las razones por las que se ha establecido en el nivel 3 de madurez (Los procesos se documentan y comunican) son las siguientes:

El proceso está definido y conocido por todos en la organización, se han establecido responsables para cada tarea.

Enap-Sipetrol tiene un Departamento Legal, que gestiona los procesos legales de la compañía. Existe un Área de Contratos que define las condiciones bajo el cual los proveedores deben prestar sus servicios: esquemas de contratos, pólizas, seguros, tiempo del contrato, cláusulas de penalización, cláusulas de responsabilidad, cláusulas de confidencialidad.

La Gerencia de TI gestiona la compra y almacenamiento de nuevas licencias para aplicaciones locales, Casa Matriz gestiona la compra y renovación de software Microsoft. En el contrato de trabajo de los empleados, no se establece la cláusula de confidencialidad de la información, uso y propiedad de la información

4.5.4.3 PROCESO: ME4 Proporcionar Gobierno de TI

Del análisis de los resultados de la auditoría para el proceso: Proporcionar Gobierno de TI, se considera que la empresa Enap-Sipetrol se encuentra en el nivel 0 de madurez.

Figura 28 Modelo de Madurez Proceso ME4

Fuente: (IT Governance Institute, 2007), Pág.168, Estados Unidos

Las razones por las que se ha establecido en el nivel 0 de madurez (No existente) son las siguientes:

A nivel general, se puede determinar que el área de TI no está alineada con el negocio, además, los elementos de gobierno de TI no están estructurados, no se han revisado los pocos existentes y no son repetibles en el tiempo.

En los temas de la inversión en activos y servicios, está adecuadamente gestionado con seguimiento y controles desde el área de compras y financiera.

Hay que considerar que las inversiones son gestionadas de acuerdo a criterios de TI y no bajo la alineación a la estrategia del negocio. Al no estar bien definidos los roles y funciones, se diluye la responsabilidad.

En cuanto a la valoración de riesgos se lo hace únicamente a nivel de TI y no está integrado en un sistema de riesgos de la organización.

Los objetivos establecidos por el negocio no reflejan los objetivos planteados y alcanzados por TI por lo que no existe un objetivo común.

No se evidencia la realización de revisiones del área de TI, ni internas ni externas, ni tampoco existen planes para su cumplimiento.

5 CAPITULO V

5.1 INFORME FINAL DE AUDITORIA[4]

Información sobre la Organización			
Nombre de la Organización	**ENAP – SIPETROL S.A.**		
Dirección	Av. República de El Salvador N34-229 y Moscú Edif. San Salvador, piso 10, Quito – Ecuador		
No. Teléfono	(593) (2) 396 8400	**No. Fax**	(593) (2) 227 1026
Página Web	www.enap.cl		
Descripción de la Organización	ENAP SIPETROL S.A., es una empresa dedicada a la exploración y explotación de petróleo en el oriente ecuatoriano en los bloques de MDC (Mauricio Dávalos Cordero) y PBH (Paraíso, Biguno y Huachito) con una producción promedio de 15.000 barriles al día. En el año 2003, inició sus operaciones en el Ecuador como socio de Petroecuador. La utilidad en el año 2012 fue de 70.8 millones de dólares, y la inversión en el área tecnológica fue de 450.000 usd.		

Información de la Auditoría			
Metodología	Cobit versión 4.1		
Tipo de Auditoria	Auditoría de Evaluación		
Fecha inicio Auditoria	20/08/2012	**Fecha fin de Auditoria**	11/10/2012
Objetivos de la Auditoría	-Evaluar la gestión y el desempeño actual del Departamento de TI. -Evidenciar si los objetivos de TI se encuentran alineados con el negocio. -Determinar el nivel de madurez de los procesos de TI evaluados. -Determinar los riesgos de TI que afecten al negocio. -Generar un informe final que sirva de guía para el mejoramiento del área de Tecnología. -Agregar valor al proceso de auditoría, generando soluciones y		

[4] (http://www.slideshare.net)
(http://www.docstoc.com)

	recomendaciones a la Gerencia de TI sobre los hallazgos encontrados.	
Alcance de la Auditoría	Analizar la situación actual de la empresa ENAP-SIPETROL auditando 11 procesos (PO1, PO4, PO9, DS2, DS4, DS5, DS13, AI5, ME1, ME3, ME4) bajo el estándar COBIT versión 4.1. Continúa→	
Procesos Asignados	Antonio Chuquimarca	PO1 – Definir el plan estratégico de TI PO4 – Definir procesos, organización y relaciones de TI DS2 – Adquirir recursos de TI DS5 – Garantizar la continuidad del servicio AI5 – Administrar las operaciones ME4 – Proporcionar gobierno de TI
	Nelly Pérez	PO9 – Evaluar y administrar riesgos de TI DS4 – Administrar servicios de terceros DS13 – Garantizar la seguridad de los sistemas ME1 – Monitorear y evaluar el desempeño de TI ME3 – Garantizar el cumplimiento regulatorio
Resultados de Auditorías previas		No se ha realizado una auditoría informática en Enap Sipetrol, por lo tanto no existen hallazgos de auditorías anteriores

Información sobre el Auditor	
Auditor Líder:	Antonio Chuquimarca
Auditor 1	Nelly Pérez
Horario	Lunes a Viernes de 15:00 – 17:30

Recomendación del Equipo Auditor

El equipo auditor recomienda realizar auditorías internas con el fin de verificar que se establezcan acciones correctivas a los hallazgos encontrados.

Resumen de los Hallazgos de la Auditoría

Los auditores han realizado una auditoría basada en los procesos COBIT versión 4.1, seleccionados en base a los objetivos que TI desea cumplir, se analizaron los elementos auditables en cada proceso y los riesgos que se desea mitigar. La metodología de auditoría empleada ha consistido en entrevistas, observación de las actividades y revisión de documentos y registros, cumpliendo en todo momento, con el acuerdo de confidencialidad de la información.

PO PLANEAR Y ORGANIZAR PO1 Definir un plan estratégico de TI			
No	**Observación**	**Riesgo**	**Recomendación**
1	No se evidencia la existencia de un plan estratégico de TI.	Planes estratégicos de TI inconsistentes con los requerimientos del negocio.	Crear un plan estratégico de TI que incluya el presupuesto de inversión, operativo, fuentes de financiamiento, la estrategia de adquisición, y los requerimientos legales y regulatorios. El plan estratégico debe ser lo suficientemente detallado para permitir la definición de planes tácticos de TI.
2	El objetivo estratégico de Excelencia Administrativa definido en el BSC es muy subjetivo para poder medir el desempeño de TI.	No medir adecuadamente el desempeño de TI en base al objetivo estratégico planteado en el BSC.	Plantear los objetivos estratégicos del BSC de forma que sean específicos, medibles, alcanzables, con responsables y que se los pueda medir en el tiempo.
3	Los proyectos mayores a $10000 dólares se manejan con análisis de proyectos, riesgos y recursos necesarios, no incluyen acuerdos de niveles de servicio.	La inadecuada gestión de proyectos de TI ocasiona pérdidas en los recursos asignados.	Se recomienda que todos los proyectos incluyan una adecuada gestión utilizando metodología PMP.
Nivel de madurez actual: 2			
P04. Definir los Procesos, Organización y Relaciones de TI.			
No	**Observación**	**Riesgo**	**Recomendación**
4	Los procesos principales del negocio y de TI están identificados, pero no está definida la interrelación entre ellos, ni el aporte de TI a los procesos críticos del negocio.	Inadecuada asignación de los recursos y servicios de TI a los procesos críticos del negocio.	Se recomienda realizar un relevamiento de procesos no solo del área de tecnología sino de toda la organización.
5	Existe un comité de estrategia a nivel de la organización, pero no existe un comité de	No existe alineación del área de TI con el negocio generando decisiones	Crear un Comité de Estrategia de TI conformado por personal de distintas áreas para definir los lineamientos

Continúa→

	estrategia de TI.	erróneas.	de TI.
6	Existe sobrecarga de trabajo asignado al personal de TI y no se ha realizado una segregación de funciones.	Incumplimiento de los objetivos y metas de TI.	Redefinición de las funciones del personal de TI de acuerdo a la situación actual del negocio.
Nivel de madurez actual: 1			
PROCESO P09. Evaluar y Administrar los Riesgos de TI			
No	**Observación**	**Riesgo**	**Recomendación**
7	La Dirección de ENAP-SIPETROL no ha realizado un análisis de los potenciales riesgos asociados al negocio, por lo tanto, el área de TI ha identificado sus riesgos sin conocer si son los que la organización necesita controlar o mitigar.	Los riesgos de TI y del negocio son manejados independientemente, por lo tanto el impacto de un riesgo de TI en el negocio no es conocido o puede ser minimizado. Puede existir un alto costo en la mitigación o control de un riesgo de TI que el negocio no lo requiere.	Establecer un proceso formal que permita gestionar los riesgos, esto es: identificar, analizar, evaluar el impacto versus la probabilidad de ocurrencia, implementar controles para reducir o mitigar los eventos, elaborar presupuestos, asignar responsables y capacitar al personal.
8	La encuesta realizada por la Gerencia de TI para determinar los recursos y servicios críticos fue realizada en el año 2008, en base a esto se analizaron los posibles riesgos a los que están expuestos, en estos años se han implementado nuevos recursos y servicios que no están considerados.	Recursos y servicios críticos de TI no considerados en el análisis de riesgos.	Actualizar la encuesta que permite identificar servicios y recursos críticos de TI añadiendo los nuevos recursos y servicios implementados, incluir en los encuestados a la Dirección y divulgar los resultados de la encuesta a todos los miembros de la organización.

Continúa→

9	Los planes de acción para gestión de riesgos de los sistemas y servicios críticos de TI están realizados hasta el año 2011, el documento no está actualizado.	No implementar los controles a los riesgos oportunamente por falta de cronogramas, presupuesto o responsables.	Actualizar los planes de acción para la gestión de riesgos, desarrollar cronogramas de implementación para el año 2013, incluir costos, beneficios y responsables. Pedir la aprobación de los planes de acción a la Gerencia General.
10	No se evidencia una política para clasificación de la información. No se ha establecido una propiedad de datos.	El principal riesgo es una inadecuada protección de los activos de información.	Se recomienda realizar la clasificación de información de acuerdo a su confidencialidad.
Nivel de madurez actual: 2			
AI – ADQUIRIR E IMPLEMENTAR AI5 - Adquirir recursos de TI			
No	**Observación**	**Riesgo**	**Recomendación**
11	No se cumple con el procedimiento de compras debido a que está desactualizado y no hace referencia al sistema SAP implementado desde enero 2011.	Las adquisiciones no siguen un procedimiento definido que cumplan con los requisitos del negocio.	Actualizar el procedimiento de compras, incorporando las nuevas políticas en cuanto a montos de aprobación, aprobaciones de funcionarios por áreas, asignación de cuentas contables, distribución por porcentajes de acuerdo al contrato y ajuste a los presupuestos anuales aprobados.
12	No se evidencia la definición de SLA's para todos los servicios críticos proporcionados por terceros.	No establecer la responsabilidad y tolerancia de los servicios brindados por terceros.	Definir SLA's para todos los servicios críticos brindados por terceros que permitan establecer los niveles de disponibilidad, eficiencia, integridad, seguridad y responsabilidad de cada uno.
13	Se evidencia que para la adquisición de software	Sistema propenso a problemas e	Se recomienda la generación de un

Continúa→

	e infraestructura no se tiene un proceso definido, forma parte del proceso general de compras.	incidentes, causando las interrupciones del negocio.	procedimiento que regule la adquisición de hardware y software y que solamente el área de tecnología pueda realizar dichas adquisiciones.
Nivel de madurez actual: 1			
DS - ENTREGAR Y DAR SOPORTE **DS2 Administrar los Servicios de Terceros**			
No	**Observación**	**Riesgo**	**Recomendación**
14	Se cumple con el registro de proveedores pero no se han definido SLA's	La no existencia de Acuerdo de Niveles de Servicio afecte la calidad del servicio.	Todo contrato de servicio debe incorporar la definición de Acuerdos de Servicio.
15	Se evidencia que la factura del proveedor del enlace internacional corresponde a lo descrito en el contrato, en el área de telecomunicaciones. Al verificar las facturas de los enlaces existe un valor que sobrepasa el valor promedio de mercado en 8 veces para este tipo de enlaces siendo la justificación la contratación directa por parte de la casa matriz.	El riesgo corresponde a la incapacidad de ajustar los valores de los precios y servicios de telecomunicaciones a tarifas que reflejen el ajuste del mercado quedando dicho servicio sobrevalorado	Para los contratos de comunicaciones se recomienda realizar contratos máximo por un lapso de dos años ya que el valor de dichos servicios es variable en el tiempo y con tendencia a la baja así como la presencia de varias empresas que compiten por un servicio adecuado por lo que se puede seleccionar en el mercado soluciones que permitan un adecuado servicio a un costo menor cada año.
Nivel de madurez actual: 3			
DS4 - Garantizar la Continuidad del Servicio			
No	**Observación**	**Riesgo**	**Recomendación**
16	No se evidencia un Plan de Continuidad de TI, completo, actualizado y alineado a los	El Plan de Continuidad de TI podría estar incompleto,	Desarrollar un Plan de Continuidad de TI alineado a los requerimientos actuales del negocio, que

	requerimientos del negocio.	desactualizado y no reflejar la arquitectura actual, podría contener procedimientos inapropiados para la recuperación o planes incapaces de recuperar efectivamente las operaciones si ocurriera un desastre.	permita recuperar los servicios y recursos críticos de TI ante un desastre. El plan deberá contener procedimientos y planes de pruebas, entrenamiento, control de cambios, distribución, análisis de tiempos y costos de recuperación.
17	No se evidencia la existencia de procedimientos de recuperación, no se realizan pruebas frecuentes de los medios y copias de seguridad para verificar el buen funcionamiento.	No se puede recuperar la información almacenada en las cintas de backups.	Establecer un procedimiento que permita realizar pruebas periódicas para la recuperación de la información almacenadas en las cintas de backups con el fin de verificar su buen funcionamiento.
Nivel de madurez actual: 1			
DS5 - Garantizar la Seguridad de los Sistemas			
No	**Observación**	**Riesgo**	**Recomendación**
18	No se evidencia la existencia de un Comité para la gestión de la seguridad.	No delegación de responsabilidades en los temas de seguridad.	Crear un Comité de Seguridad con integrantes de diferentes áreas para que en conjunto propongan los lineamientos que garanticen la seguridad de los sistemas.
19	No se evidencia políticas, normas o procedimientos que garanticen la seguridad de los sistemas y de la información.	Activos de información y datos sin protección.	Crear una política de seguridad que incluya: alcance y objetivos, responsabilidades de todos los integrantes de la organización, debe incluir normas de seguridad y procedimientos detallados.
20	No se evidencia la existencia de un Plan de	No reaccionar efectivamente ante	Crear un Plan de Seguridad de TI que permita

Continúa→

	Seguridad de TI	un incidente de seguridad.	reaccionar rápidamente ante un incidente de seguridad, tomando en cuenta los requerimientos del negocio, riesgos, la infraestructura de TI. Asegurar que el plan está basado en las políticas y procedimientos de seguridad junto con las inversiones apropiadas en los servicios, personal, software y hardware. Comunicar las políticas y procedimientos de seguridad a los interesados y a los usuarios.
21	No existe un proceso definido para la gestión de incidentes y problemas	Incidentes y problemas graves no son atendidos.	Establecer un proceso para la gestión de incidentes y problemas que incluya: -Detección de eventos -Evaluación de la amenaza / incidente -Resolución de la amenaza o creación y orden de escalamiento -Análisis post implementación -Orden de trabajo -Cierre del incidente
Nivel de madurez actual: 1			
DS13 Administración de Operaciones			
No	**Observación**	**Riesgo**	**Recomendación**
22	La Gerencia de TI comunica que no se han establecido procedimientos o instrucciones de operación, todas las tareas son conocidas por la Gerencia de TI y el Analista de Sistemas.	Errores en las operaciones debido al desconocimiento de los procedimientos estándares. Tareas informales y desordenadas debido a la falta de procedimientos estándares.	Adquirir la cultura de desarrollar procedimientos para estandarizar, formalizar y organizar las operaciones realizadas por el departamento de TI. Almacenarlos en un lugar que puedan ser fácilmente localizables por el personal de TI.

Continúa→

		Incapacidad para responder rápidamente a problemas o cambios operacionales.	
23	La documentación de procedimientos, manuales, políticas son informales no posee un formato estándar que contenga fechas de elaboración, fechas de actualización, aprobaciones o vigencia, no se ha especificado un sistema de archivos para este tipo de documentación.	La documentación no mantiene un formato estándar que sea fácil de entender, no mantiene fechas de creación, modificación o aprobaciones por lo que es difícil reconocer si el documento es actual. Los documentos difícilmente son encontrados con rapidez.	Crear formatos estándar para la documentación de información importante para la organización como políticas, procedimientos, manuales, etc. Almacenar la información en directorios establecidos para ello que sean fácilmente localizables y con las seguridades necesarias para ser leídos solamente por las personas autorizadas.
24	No se ha definido una lista de Contactos en caso de emergencia, detallando los proveedores de servicio, nombre del técnico, teléfono o correo electrónico.	Imposible localizar a los proveedores de servicios contratados en caso de emergencia.	Registrar una lista de Contactos en caso de emergencia, detallando los proveedores de servicio, nombre del técnico, teléfono o correo electrónico, permitiendo localizar inmediatamente al proveedor en caso de emergencias.
25	La solución a problemas o incidentes no se encuentra documentada, es decir no se mantiene una base de conocimiento que permita identificar los problemas y buscar la solución rápidamente. No se evidencia un procedimiento formal para la gestión de problemas e incidentes.	La solución de problemas conocidos toma mucho tiempo.	Crear una base de conocimiento que permita identificar los problemas y buscar la solución rápidamente. Este registro es de gran ayuda para solucionar problemas frecuentes. Analizar la adquisición de un sistema para el manejo de incidentes que permita gestionar de mejor manera los problemas diarios.

Continúa→

Nivel de madurez actual: 2			
ME - MONITOREAR Y EVALUAR **ME1 - Monitorear y Evaluar el desempeño de TI**			
No	**Observación**	**Riesgo**	**Recomendación**
26	No se han establecido indicadores de desempeño dentro del departamento de TI.	Desconocimiento del desempeño de TI, imposibilidad para implementar acciones de mejora.	Utilizar los indicadores de Cobit que permitan medir el desempeño del departamento de TI.
Nivel de madurez actual: 3			
ME3 - Garantizar el cumplimiento con requerimientos externos			
No	**Observación**	**Riesgo**	**Recomendación**
27	En las políticas y procedimientos de TI no existen hitos para referenciar el cumplimiento de leyes, requerimientos regulatorios o contractuales. La Gerencia de TI no ha divulgado los requerimientos legales y regulatorios de TI a los usuarios, tampoco ha establecido responsables.	Desconocimiento del personal involucrado en las prácticas y procedimientos para el cumplimiento con requerimientos legales y regulatorios.	Verificar que los requisitos legales, regulatorios y contractuales están presentes en las políticas y procedimientos de TI y que estos son comunicados al personal involucrado.
Nivel de madurez actual: 3			
ME4 Proporcionar Gobierno de TI			
No	**Observación**	**Riesgo**	**Recomendación**
28	No existe un marco de gobierno estructurado e implantado, existen elementos de gobierno de TI aislados como	Responsabilidades y rendición de cuentas ineficaces para los procesos de TI.	Implementación de la Guía rápida de despliegue de COBIT para la gestión del Gobierno de TI.

Continúa→

	política de sistemas, seguridades de acceso, control de respaldos. No se evidencia definición en roles y funciones ni tampoco cumplimiento en procesos de control.		
Nivel de madurez actual: 0			

6 CAPITULO VI

6.1 PROYECTOS ASOCIADOS A LAS RECOMENDACIONES

En el Capítulo V se presentó el informe final de la Auditoría Informática a la empresa ENAP-SIPETROL en donde se realizó un resumen de las observaciones encontradas en el proceso de auditoría, se analizaron los riesgos asociados a las observaciones y se presentaron recomendaciones a los hallazgos encontrados.

En el presente capítulo, el equipo auditor analizará cada recomendación y presentarán proyectos que permitan elevar el nivel de madurez de los procesos evaluados. A continuación se muestra un cuadro en donde se visualiza los niveles de madurez definidos en base a los hallazgos encontramos en el proceso de auditoría:

Tabla 33

Resumen Niveles de Madurez

PROCESOS	Nivel de Madurez
PO1 - Definir un Plan Estratégico de TI	2
PO4 - Definir los Procesos, Organización y Relaciones de TI	1
P09 - Evaluar y Administrar los Riesgos de TI	2
AI5 - Adquirir Recursos de TI	1
DS2 - Administrar los servicios de terceros	3
DS4 - Garantizar la Continuidad del Servicio	1
DS5 - Garantizar la seguridad de los sistemas	1
DS13 - Administración de Operaciones	2
ME1 - Monitorear y Evaluar el desempeño de TI	3
ME3 - Garantizar el cumplimiento con requerimientos externos	3
ME4 - Proporcionar Gobierno de TI	0

Los niveles de madurez establecidos en los 11 procesos auditados, determinan la situación actual de TI: el 9% corresponde al nivel 0 “No existente”, el 37% corresponde al nivel 1 “Inicial-Ad hoc”, el 27% corresponde al nivel 2 “Repetible pero intuitivo”, el 27% corresponde al nivel 3 “Proceso Definido”.

El 73 % de los procesos auditados se encuentran entre los niveles de madurez 0 y 2 y el 27 % se encuentran en un nivel de madurez 3.

La organización debe enfocarse en el mejoramiento de los procesos que forman parte del 73% ya que por son procesos informales, sin un enfoque estándar ocasionando que la administración de los mismos sean de una manera desorganizada, delegando la responsabilidad al individuo y por lo tanto lo errores son muy probables.

Con el objetivo de mejorar tanto los procesos de operaciones como los procesos de gestión se recomienda alcanzar un nivel de madurez 3 "Proceso Definido" para asegurar la estandarización de los procesos, la documentación y la comunicación a la organización. El alcanzar el nivel de madurez 3 no implica un alto presupuesto, en su lugar está enfocado al levantamiento y mejora de los procesos.

Para llegar a un nivel de madurez 3 Cobit recomienda cumplir con los siguientes elementos:

PO1 - Definir un Plan Estratégico de TI

1. Definición de una Política de planeación estratégica
    - Fechas de creación y actualización del Plan
    - Definición de los Integrantes
    - Definición de los Responsables del Plan
    - Asignación de Recursos (humanos, técnicos y financieros)
    - Definición de la frecuencia de revisiones
    - Difusión de la política
2. Crear un plan estratégico basado en la metodología PETI

PO4 - Definir los Procesos, Organización y Relaciones de TI

1. Descripción de procesos de TI y sus relaciones
2. Definir la organización de TI
    - Establecer los recursos de TI (humanos, técnicos y financieros)

- Establecer políticas y reglamentos que se deben cumplir alineados a la estrategia de TI.
- Establecer roles y responsabilidades en TI y las asignadas a usuarios y a terceros.

3. Documentar y comunicar la organización de TI.

P09 - Evaluar y Administrar los Riesgos de TI

1. Definición de una Política para la administración de Riesgos
   - Fechas de creación y actualización de la Política
   - Definición de los Integrantes
   - Definición de los Responsables
   - Asignación de Recursos (humanos, técnicos y financieros)
   - Definición de la frecuencia de revisiones
   - Difusión de la política
2. Entrenamiento de la gestión de riesgos a todo el personal
3. Establecer una metodología para la evaluación de riesgos
4. Identificación de riesgos claves
5. Establecer responsables para la administración de riesgos en la descripción de funciones.

AI5 - Adquirir Recursos de TI

- Establecer políticas y procedimientos para adquisiciones de TI
- Identificación del uso de estándares
- Administración de contratos con proveedores
- Comunicar al área de adquisiciones el uso obligatorio de contratos
- Establecer Acuerdos de Niveles de Servicio en los contratos.

DS4 - Garantizar la Continuidad del Servicio

- Crear un plan de continuidad de TI, documentado y basado en los recursos y servicios críticos de TI y su impacto en el negocio.

- Mantener un inventario de sistemas y componentes críticos de TI
- Instalar componentes de alta disponibilidad y redundancia
- Involucrar a la Dirección en el plan de continuidad
- Realizar pruebas de continuidad y documentarlas

DS5 - Garantizar la seguridad de los sistemas

- Involucramiento de la Dirección en los temas de seguridad
- Creación de una política de seguridad de TI basada en riesgos críticos
- Creación de procedimientos de seguridad de TI
- Asignación de Responsables en los temas de seguridad
- Realizar pruebas de seguridad
- Difusión de las políticas y procedimientos al personal

DS13 - Administración de Operaciones

- Formalizar las funciones repetitivas, estandarizarlas, documentarlas y comunicarlas.
- Seguimiento al cumplimiento de las tareas asignadas
- Uso de aplicaciones para minimizar las tareas operativas
- Asignación de recursos para la ejecución de las tareas
- El equipo auditor considera que no se puede implementar los niveles de madurez 4 (Administrado) o 5 (Optimizado) por cuanto es necesario, primeramente, estandarizar los procesos, definirlos adecuadamente y hacer que sean aceptados por toda la organización.
- En base al detalle de los procesos en el nivel de madurez 3, el equipo auditor sugiere los siguientes proyectos como mejora a los procesos auditados:

Tabla 34

Proyectos Sugeridos

Proyectos	Actividades
Plan Estratégico de TI	Esquema de Plan Estratégico de TI
	Esquema de Desarrollo de Proyectos
	Análisis de Procesos de TI
	Análisis de Funciones de TI
Gestión de Riesgos de TI	Esquema de Gestión de Riesgos de TI
	Clasificación de la Información
Plan de Continuidad de TI	Esquema de un Plan de Continuidad de TI
	Esquema de una Política de Seguridad
	Esquema de un Plan de Seguridad
	Definición de Acuerdos de Niveles de Servicio
Control de la Documentación	Esquema de un formato de Poes
	Formato para el Control de la Documentación de TI

6.2 PRINCIPALES ACCIONES PROPUESTAS

6.2.1 Esquema de un Plan Estratégico de TI

El equipo auditor sugiere utilizar la metodología PETI (Plan Estratégico de TI) el cual es un plan de acción, hoja de ruta o pasos ordenados y estructurados que permiten en un cierto horizonte de tiempo implementar una arquitectura de TI deseada para soportar los objetivos estratégicos de la organización[5].

Cuadro 23

Esquema para desarrollar un Plan Estratégico de TI

Plan Estratégico de TI – PETI			
Fase	**Tareas**	**Entregable**	**Tiempo**
Fase I: Organización del Trabajo	-Definición de acciones y recursos necesarios	Plan de Trabajo	2 días
Fase II: Diagnóstico de la	-Revisión de la situación actual	Diagnóstico de la situación	5 días

[5] (IT Governance Institute, 2008)

Continúa→

situación actual de TI	-Plataformas tecnológicas utilizadas -Situación actual de la operatividad de la infraestructura	actual de TI	
Fase III: Definición de componentes estratégicos de TI	-Lineamientos estratégicos de TI -Definición de objetivos y estrategias de TI	Componentes estratégicos de TI	5 días
Fase IV: Diseños de Modelos de Arquitectura de TIC	-Transformación de estrategia de negocios a estrategia de TI Construcción de la arquitectura de sistemas -Definición de los elementos clave de arquitectura tecnológica (hardware, software y comunicaciones) -Diseño de los modelos operativos de TI -Definición de la estructura de la organización de TI	Arquitectura de Datos Propuesta Arquitectura de sistemas Arquitectura tecnológica propuesta	10 días
Fase V: Elaboración de la cartera de proyectos de TI	Establecimiento de las diferencias entre la Fase III y Fase IV	Cartera de Proyectos de TI	2 días
Fase VI: Diseño de mecanismos para la gestión de TI	Elaboración de procedimientos para el control y seguimiento de proyectos Capacitación en la gestión de proyectos, seguimiento e implementación, Actualización del Plan.	Metodología para la gestión de proyectos de TI	7 días

Empresa	**Ubicación**	**Costo**	**Recursos**
PALMSTORE	Alpallana E7-123 Telf.: 3530-130	$12.000	1 consultor Senior, 1 consultor Junior, 1 Responsable Directivo de la Organización.

Nota Fuente: Información del Proveedor

6.2.2 Esquema de Desarrollo de Proyectos

El equipo auditor sugiere utilizar la metodología de desarrollo de proyectos según la guía del PMBOOK, la cual proporciona y promueve un vocabulario común en el ámbito de la dirección de proyectos. La metodología propuesta contempla un conjunto de procedimientos y formatos que facilitarán la definición, aprobación, planificación, ejecución, seguimiento/control y cierre de un proyecto.

Cuadro 24

Esquema para el Desarrollo de Proyectos

Fase	**Tareas**	**Entregable**
Fase I: Inicio del proyecto	Gestión de iniciativas de proyectos Priorización de proyectos	Listado de proyectos
Fase II: Análisis y planificación del Proyecto	Elaboración de estudios técnicos, costos y de mercado. Diseño del proyecto Plan de ejecución del proyecto. Aprobación del proyecto	Estudio de Factibilidad Diseño del proyecto Plan de ejecución del proyecto
Fase III: Ejecución y control del proyecto	Cumplimiento del plan de ejecución del proyecto Control en base a reuniones quincenales de trabajo Supervisión en la entrega y calidad de los productos o servicios Documentación del proyecto	Actas de reuniones Formatos Generales
Fase IV: Cierre del proyecto	Verificación del producto o servicio entregado Transferencia del producto final Formalización del cierre	Formatos Generales

Nota Fuente: (PMBOK 3 ediciónPMP)

6.2.3 Análisis de procesos de TI

Para el análisis de los procesos se recomienda contratar una empresa de consultoría local que permita realizar el relevamiento respectivo dentro de la organización abarcando todas las áreas de la misma y con el apoyo de la Gerencia General.

Cuadro 25

Análisis de Procesos de TI

Fases	**Tareas**	**Entregables**	**Tiempo**
Fase I: Planificación del proyecto	-Definición de los objetivos -Alcance -Estimación de recursos	Documento de Planificación	2 días
Fase II: Levantamiento de Procesos de Negocio.	-Relevamiento de: Entradas, recursos, controles, responsables, salidas e interrelaciones.	-Mapa de Procesos. Mapa de interrelación de procesos	20 días
Fase III: Diagnóstico del alineamiento de las estrategias de negocio y la de procesos de TI	-Revisión de la Estrategia de la organización. -Definición de los requerimientos del negocio con respecto a TI -Revisión de los servicios actuales de TI	-Matriz de Interrelación entre requerimientos de TI del negocio y servicios actuales de TI	5 días
Fase IV: Rediseño de Procesos definiendo cambios/mejoras en el flujo de proceso.	-Análisis GAP de procesos -Rediseño en los flujos de procesos. -Mejora de los procesos -Revisión de responsables, recursos, controles y salidas.	-Mapa de procesos mejorados. -Modificación de responsables -Redistribución de recursos	5 días

Continúa →

Fase V: Diseño de Indicadores de Gestión y finalización de proyecto	-Generar indicadores acorde al rediseño de procesos.	-Indicadores de gestión por proceso. Informe Final.	5 días
Empresa	**Ubicación**	**Costo**	**Recursos**
ERNST&YOUNG ECUADOR	Andalucía y Cordero. Edif. Cyede Telf.: 593-2-2555-553	$8000	1 consultor Senior, 1 Responsable Directivo de la Organización.

Nota Fuente: Información del Proveedor

6.2.4 Análisis de funciones de TI

Para el análisis de las funciones del personal, se recomienda contratar una empresa de consultoría que permita realizar el relevamiento respectivo dentro de la organización abarcando todas las áreas de la misma y con el apoyo de la Gerencia General, utilizando una metodología de clase mundial y que permita obtener resultados en el menor tiempo posible.

Cuadro 26

Análisis de Funciones de TI

Fases	**Tareas**	**Entregables**	**Tiempo**
Fase I: Capacitación en la utilización de la herramienta.	-Capacitación a todo el personal en la utilización del formato de relevamiento de información proporcionado por Mercer en la versión 3.0	-Registro de capacitación del Personal	2 días
Fase II: Relevamiento de la información por empleado	-Evaluación de las funciones del empleado -Evaluaciones de las tareas del empleado. -Determinar la capacidad de la posición	-Formato Mercer llenado y revisado por la Gerencia respectiva.	2 días
Fase III: Resultado de la medición de la posición	-Comparación con las funciones estándar de la posición de acuerdo a las categorías definidas por la consultora Mercer. -Medición de la posición.	Definición de funciones de la posición Medición de la capacidad de la posición de acuerdo a las funciones realizadas. Redefinición de funciones Recomendación de incorporación de personal de requerirlo.	3 días
Empresa	**Ubicación**	**Recursos**	**Costo**
Mercer	Bogotá-Colombia Cra 69 No 25B - 44 - Piso 2 Edificio World Business Port Tel: +57 1 742 1000 Fax: +57 1 742 1099	1 Consultor Senior 1 Consultor Junior 1 Responsable de RRHH de la empresa.	$15000

Nota Fuente: Información del Proveedor

6.2.5 Proyecto de Análisis de Gestión de Riesgos de TI

Cuadro 27

Esquema para la Gestión de Riesgos de TI

Fases	**Tareas**	**Entregables**	**Tiempo**
Fase I: Planificación del proyecto	-Definición de los objetivos -Alcance -Estimación de recursos	Documento de Planificación del Proyecto	15 días
Fase II: Análisis de Riesgos	-Identificación de Activos (Inventario de activos de TI, selección de activos críticos) -Identificación de Amenazas (tomando en cuenta la integridad, disponibilidad, confidencialidad para cada activo) -Identificación de las vulnerabilidades -Estimación de la probabilidad de ocurrencia (baja, media, alta, muy alta) -Estimación de la vulnerabilidad de cada activo (baja, media, alta) -Estado del riesgo (Calcular el nivel del riesgo: impacto vs ocurrencia)	Documento de Análisis del Proyecto	30 días
Fase III: Gestión de riesgos	-Toma de decisiones respecto al riesgo (prevenir, impedir, reducir o controlar) -Elaborar el Plan de seguridad -Plan de acción para reducir las vulnerabilidad (quién, cómo, cuándo, qué) -Plan de acción durante la emergencia -Plan de acción después de la emergencia -Ejecución del plan, - Pruebas del plan	Plan de Seguridad	30 días
Empresa	**Ubicación**	**Recursos**	**Costo**
PALMSTORE	Alpallana E7-123 Telf.: 3530-130	1 consultor Senior, 1 consultor Junior, 1 Resp.de la Organización.	$16000

Nota Fuente: (ISACA, 2008)

6.2.6 Clasificación de la información

Cuadro 28

Clasificación de la Información

Clasificación de la Información				
INTERNA	**TIPO**	**PROPIETARIO DEL DATO**	**TIPO DE ACCESO**	**CRITERIO DE CLASIFICACIÓN**
De valor para la organización	Reservada	Gerente	Único	-Documentación de negociaciones o acuerdos con otras empresas que requieran reserva. -Los expedientes judiciales o procedimientos administrativos -Informes y comunicaciones de casa matriz reservados sobre el resultado del negocio. -Informes provenientes de Recursos Humanos sobre el rendimiento de empleados. -Los procedimientos de responsabilidad de los empleados de la organización provenientes de Recursos Humanos.
	Confidencial	Gerencias	Solo Gerentes	-Documentos de Planificación de cada Gerencia. -Resultados consolidados de Gestión de la organización. -Informes de resultados de proyectos. -Comunicados de casa matriz a nivel gerencial -Actas de sesiones de Comité
	Privada	Gerencia Asociada	Gerencia y personal del área	-Formatos propios de cada área -Proyectos/Estudios Técnicos -Informes/Reportes, Procedimientos -Bases de Datos, -Aplicaciones -Planos, -Presentaciones
	Pública	Todas las áreas	General	-Informes/reportes interdepartamentales -Planos, -Estudios técnicos -Presentaciones, Archivos de Instaladores
Externa	Pública	Gerencia General	General vía web	-Información General -Resumen de resultados -Datos de Contacto

Nota Fuente: Autores de la Tesis

6.2.7 Definición de Acuerdos de Niveles de Servicio (SLA's)

Para facilitar la elaboración de Acuerdos de Niveles de Servicios se considera la utilización de plantillas que contengan los siguientes elementos:

- Descripción general del servicio entregado.
- Designación de responsables del acuerdo del lado del cliente como del proveedor.
- Definición de los plazos para la provisión del servicio.
- Definición de la duración del acuerdo y condiciones para su renovación y/o terminación.
- Determinación de las condiciones de disponibilidad del servicio.
- Definición del tipo de soporte y actividades de mantenimiento asociadas.
- Establecimiento de tiempos de respuesta en condiciones de soporte.
- Definición de tiempos de recuperación en casos de incidentes.
- Determinación de niveles de escalamiento, determinando tiempos, responsables y gestión de problemas.
- Planes de contingencia y responsables de su inicio.
- Definición de facturación y cobro, en condiciones normales y en caso de sanciones
- Criterios de evaluación y periodicidad de la calidad del servicio, reportes e informes.

6.2.8 Esquema de un Plan de Continuidad de TI

Cuadro 29

Esquema de un Plan de Continuidad

FASES		**ACTIVIDADES**
1.Dirección del Proyecto		1.1 Plan del Proyecto
		1.2 Lanzamiento del Proyecto
		1.3 Control de Avance, seguimiento y Riesgos
		1.4 Cierre del Proyecto
2.Implementación del proceso de Gestión de Continuidad		2.1 Definición de Políticas de Continuidad
		2.2 Diseño y Construcción del proceso
		2.3 Publicación y puesta en marcha del proceso
3.Definición de requerimientos		3.1 Identificación de procesos críticos de TI
		3.2 Identificación de funciones vitales de TI
		3.3 Análisis del impacto al negocio
		3.4 Análisis de Riesgos de TI
		3.5Identificación y selección de estrategias de continuidad
4.Implementación de Continuidad de servicios de TI	4.1Plan de Continuidad de servicios de TI	4.1.1 Plan de respuesta ante la emergencia
		4.1.2 Planes de notificación
		4.1.3 Plan de evaluación del daño
		4.1.4 Planes de declaración
		4.1.5 Plan de recuperación
		4.1.6 Plan de operación en contingencia
		4.1.7 Plan de restauración
		4.1.8 Plan Financiero
		4.1.9 Plan de recursos humanos
		4.1.10 Definición de roles y responsabilidades
	4.2Organización de Continuidad	4.2.1 Comité de dirección de continuidad de Servicios de TI
		4.2.2 Equipos de Recuperación de negocio
		4.2.3 Equipos de recuperación de TI
	4.3Medidas de mitigación y contingencia	4.3.1 Medidas de mitigación de amenazas
		4.3.2 Medidas de contingencia
		4.3.3 Planes y procedimientos de recuperación
		4.3.4 Planes y procedimientos de restauración

Continúa →

		4.3.5 Acuerdos stand-by
	4.4Comunicación y Capacitación	4.4.1 Plan de concientización
		4.4.2 Material de concientización
		4.4.3 Plan de capacitación
		4.4.4 Material de capacitación
5.Concientización y prueba inicial		5.1 Ejecución de los talleres de concientización
		5.2 Dictado de los cursos de capacitación
		5.3 Definición del alcance de la prueba
		5.4 Planificación de la prueba
		5.5 Ejecución de la prueba
		5.6 Informe de análisis de resultados

Empresa	**Ubicación**	**Costo**	**Recursos**
PALMSTORE	Alpallana E7-123 Telf.: 3530-130	$30.000	2 Consultor Senior, 3 Consultor Junior, 1 Responsable de la organización por área.

Nota Fuente: (ISACA, ITAFTM, 2008)

Los principales entregables son:

- Plan del Proyecto
- Políticas de Gestión de Continuidad de Servicios de TI
- Proceso de Gestión de Continuidad de Servicios de IT
- Análisis de Impacto al Negocio
- Análisis de Riesgos de los Servicios de TI
- Análisis de Estrategias de Continuidad
- Plan de Continuidad de Servicios de IT
- Organización de Continuidad de Servicios de IT

- Medidas de Mitigación y Contingencia
- Material de Comunicación y Concientización
- Material de Capacitación y Entrenamiento
- Prueba Inicial del Plan de Continuidad de Servicios de IT

6.2.9 Esquema de una Política de Seguridad

Cuadro 30

Esquema de una Política de Seguridad

Contenido de la Política de Seguridad	**Responsable**	**Período revisión**
Política General	Coordinador de Sistemas	Anual
Normas		
-Tratamiento de la Información	Coordinador de Sistemas	Anual
-Responsabilidades de Seguridad	CSI / CIO	Anual
-Administración de usuarios	TI	Anual
-Licencias Legales de Software	TI	Anual
-Copias de respaldo	TI	Anual
-Correo electrónico y uso de Internet	TI	Anual
-Ambientes de Procesamiento	TI	Anual
-Comunicaciones	TI	Anual
-Antivirus	TI	Anual
-Protección Física de Recursos de TI	TI / Seguridad	Anual
-Continuidad del Procesamiento	TI	Anual
-Computadoras portables	TI	Anual
Procedimientos		
-Definición de Dueños de Datos	CIO usuarios	Semestral
-Clasificación de la Información	CIO	Semestral
-Alta, Baja y Modificación de Usuarios	CIO / TI	Semestral

Continúa →

Contenido de la Política de Seguridad	Responsable	Período revisión
-Alta, Baja y Modificación de Puestos / Perfiles / Grupos	CIO / TI	Semestral
-Generación de Copias de Respaldo y Restauración	TI / Operaciones	Semestral
-Traspaso de software a ambientes Productivos	TI / Desarrollo	Semestral
-Administración de Incidentes	CIO / TI	Semestral
-Acciones ante Situaciones de Emergencias	TI / Operaciones	Semestral
Glosario de Términos	TI	Semestral
Sanciones por Incumplimientos	TI / RRHH	Semestral

Nota Fuente: Autores de la Tesis

6.2.10 Esquema de un plan de seguridad

Un Plan de Seguridad de la información incluye todos los procesos/servicios involucrados en la administración de la seguridad de la información.

La finalidad del Plan es proteger la información y los activos de la organización, tratando de conseguir confidencialidad, integridad y disponibilidad de los datos, y responsabilidades que debe asumir cada uno de los empleados mientras permanezcan en la organización. Todo este análisis se detalla en la sección Gestión de Riesgos de TI, en donde se encuentra el esquema del Plan de Seguridad de TI.

6.2.6.3 Gestión de Incidentes y Problemas

El equipo auditor recomienda la utilización de un software para la gestión de incidentes y problemas, actualmente en el mercado existen varias empresas que prestan el servicio de venta e implementación de estos sistemas o existe software de tipo open source que se lo puede descargar gratuitamente del internet, algunos recomendados son:

Cuadro 31

Software Libre para Gestión de Incidentes

Software	Descripción		Link para descarga
GMF	Es una implementación de las recomendaciones **ITIL** para la gestión de servicios de TI. Es un producto de software libre que incluye módulos de gestión de incidencias, gestión de inventario, gestión del cambio y reportes.		http://www.genos.org
OTRS	(Open-source Ticket Request System). Su versatilidad y capacidad de adaptación permiten realizar de forma sencilla el seguimiento y manejo de incidencias.		https://www.otrs.com
osTikect	Integra consultas creadas a través de formularios de correo electrónico, teléfono y web basados en una interfaz web multi-usuario.		http://osticket.com/
Empresa	**Ubicación**	**Costo**	**Recursos**
PALMSTORE	Alpallana E7-123 Telf.: 3530-130	$2.000	1 Consultor Senior.

Nota Fuente: (http://itilv3.osiatis.es)

Nota Fuente: (http://www.itil-officialsite.com/)

6.2.7 Administración de Operaciones

En este punto se ha definido formatos estándares para el manejo de la documentación de TI tanto para políticas, procedimientos y manuales con el fin de que las aprobaciones y control de versiones sean de fácil administración. Los formatos están descritos en el Anexo No. 32 de este documento.

6.3 Plan de Implementación

Para definir la implementación de los proyectos, el grupo auditor, ha generado una guía más que una metodología, la misma que pretende apoyar al área de tecnología y a la organización en la toma de decisiones considerando que la ruta de implementación de proyectos se convierte en el resumen a ser considerado por la Gerencia General de la organización.

Sobre los proyectos planteados estos tienen objetivos a ser cubiertos y lo que se pretende con cada uno de ellos es generar un servicio o un resultado único con un efecto duradero.

Para el despliegue de los proyectos el principal criterio que se debe considerar es que estos deben cumplir con el Plan Estratégico de la organización definido en el Balanced Scorecard de Enap-Sipetrol, cuyos pilares fundamentales son:

- Estrategia, Cultura y Estructura
- Operación eficiente y Segura

Definida la clasificación de los proyectos por las directrices del Plan Estratégico su implementación se la deberá realizar por fases considerando aquellos proyectos que cumplan con la estrategia, disminuyan el riesgo y mantengan la operación de la organización. Los proyectos definidos son:

Tabla 35

Proyectos Asociados a las Recomendaciones

Procesos COBIT	Proyectos
PO1	Plan Estratégico de TI
PO1	Modelo de Desarrollo de Proyectos
PO4	Análisis de Procesos de TI
PO4	Análisis de Funciones de TI
PO9	Gestión de Riesgos de TI
PO9	Clasificación de la Información
AI5	Acuerdos de Niveles de Servicio
DS4	Plan de Continuidad de TI
DS5	Política de Seguridad
DS5	Plan de Seguridad
DS5	Gestión de Incidentes y Problemas
DS13	Control de la Documentación de TI

Nota Fuente: Autores de la Tesis

Los proyectos se agrupan por afinidad dentro de los pilares del BSC de la siguiente manera:

Tabla 36

Proyectos por Afinidad en el BSC

Pilares BSC de la Organización	Proyectos
Estrategia, Cultura y Estructura	Plan Estratégico de TI
	Análisis de Procesos de TI
	Análisis de Funciones de TI
	Modelo de Desarrollo de Proyectos
Operación Eficiente y Segura	Política de Seguridad
	Gestión de Riesgos de TI
	Plan de Seguridad
	Plan de Continuidad de TI
	Acuerdos de Niveles de Servicio
	Gestión de Incidentes y Problemas
	Clasificación de la Información
	Control de la Documentación de TI

Nota Fuente: Autores de la Tesis

A los 12 proyectos los agrupamos en 4 proyectos generales en base a su relación, los proyectos son: Plan Estratégico, Gestión de Riesgos, Plan de Continuidad y Control de la documentación.

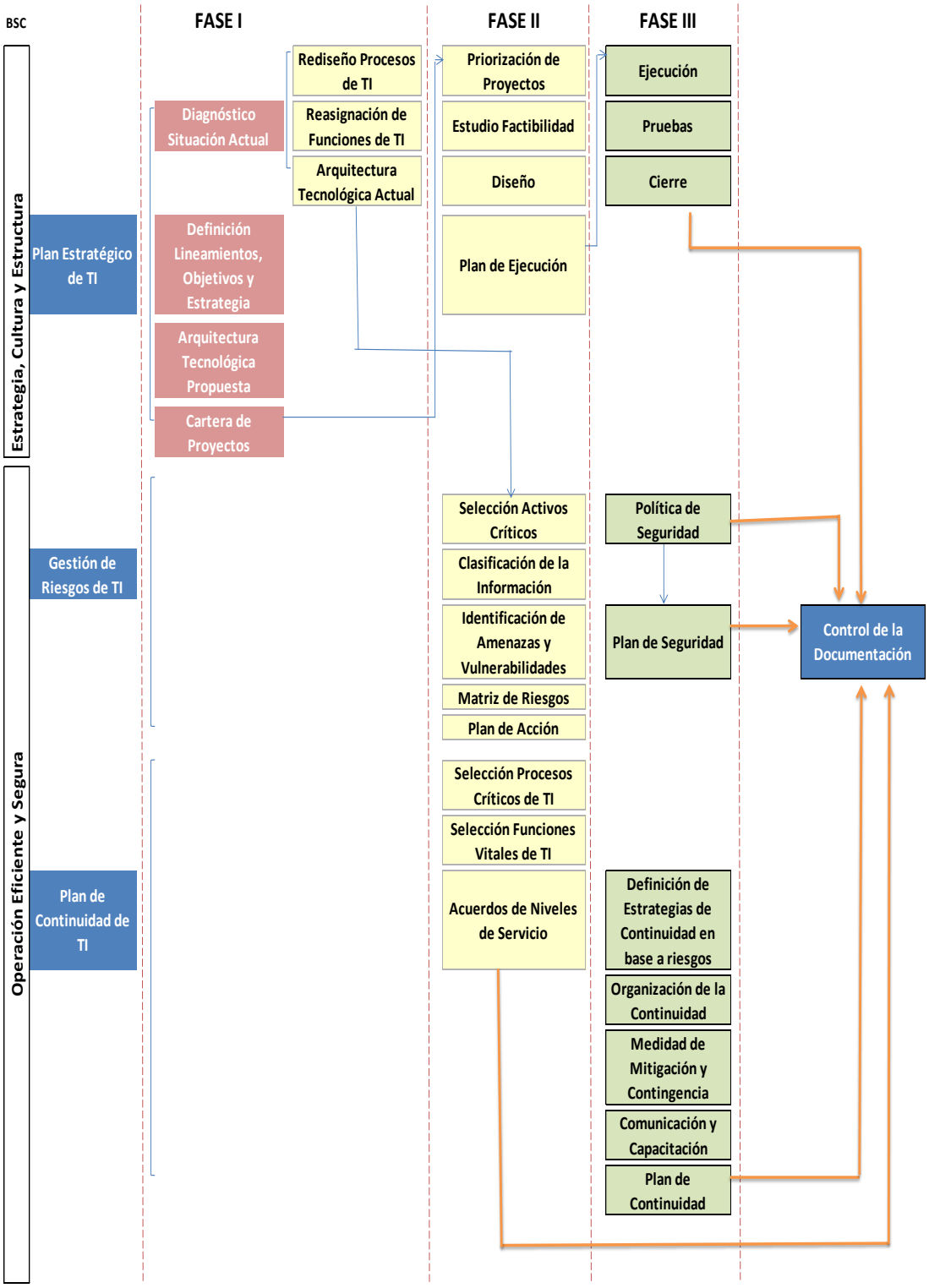
El Plan Estratégico y la Gestión de Riesgos ayudan a cumplir con uno de los pilares del Balance Scorecard de Enap-Sipetrol: Estrategia, Cultura y Estructura.

El Plan de Continuidad y Control de la documentación ayudan a cumplir con otro pilar del Balance Scorecard: Operación Eficiente y Segura.

Para cumplir con cada una de estas etapas las actividades se han divido en 3 Fases, en el siguiente gráfico se detallan las actividades a realizar en cada una de las fases:

Figura 29 Fases para la Implementación de Proyectos Sugeridos

Fuente: Autores de la Tesis


BSC
FASE I
FASE II
FASE III
Estrategia, Cultura y Estructura
Operación Eficiente y Segura
Plan Estratégico de TI
Gestión de Riesgos de TI
Plan de Continuidad de TI
Diagnóstico Situación Actual
Definición Lineamientos, Objetivos y Estrategia
Arquitectura Tecnológica Propuesta
Cartera de Proyectos
Rediseño Procesos de TI
Reasignación de Funciones de TI
Arquitectura Tecnológica Actual
Priorización de Proyectos
Estudio Factibilidad
Diseño
Plan de Ejecución
Ejecución
Pruebas
Cierre
Selección Activos Críticos
Clasificación de la Información
Identificación de Amenazas y Vulnerabilidades
Matriz de Riesgos
Plan de Acción
Selección Procesos Críticos de TI
Selección Funciones Vitales de TI
Acuerdos de Niveles de Servicio
Política de Seguridad
Plan de Seguridad
Definición de Estrategias de Continuidad en base a riesgos
Organización de la Continuidad
Medidad de Mitigación y Contingencia
Comunicación y Capacitación
Plan de Continuidad
Control de la Documentación

6.3.1 FASE I

En la fase de inicio, los proyectos seleccionados son los que apoyan las principales definiciones del Plan Estratégico, entre las principales actividades a desarrollar en esta etapa están:

- Realizar un Diagnóstico de la Situación Actual, para ello se deberán rediseñar los procesos, las funciones y analizar la tecnología actual del departamento de TI.
- Definir los Lineamientos, Objetivos y la Estrategia de TI.
- Proponer una Arquitectura Tecnológica adecuada, tomando en cuenta el análisis realizado en las actividades anteriores, de acuerdo a las necesidades actuales del negocio.
- Establecer una Cartera de Proyectos, en donde se detallarán las diferencias entre la arquitectura tecnológica actual y la arquitectura tecnológica propuesta con el fin de plantear mejoras en el departamento de TI.

Las salidas de esta fase son: La arquitectura tecnológica actual y una cartera de proyectos los cuales son la entrada de la fase II.

6.3.2 FASE II

Las siguientes actividades, permiten continuar con las actividades de la FASE I:

En lo que respecta al Plan Estratégico, una vez creada la Cartera de Proyectos se continuarán con las siguientes actividades que forman parte de la Gestión de Proyectos:

1. Priorización de Proyectos
2. Estudio de Factibilidad
3. Diseño
4. Plan de Ejecución

Para cubrir la Gestión de Riesgos, las actividades que se deberán realizar en la Fase II son:

1. Selección de Activos Críticos, tomando como referencia el Inventario de Activos de TI realizados en la Fase I.
2. Clasificación de la Información
3. Identificación de amenazas y vulnerabilidades
4. Generación de la Matriz de Riesgos
5. Plan de Acción

En lo que respecta al Plan de Continuidad las actividades a realizar en la Fase II son:

1. Selección de Procesos Críticos de TI, tomando como referencia el análisis de los Procesos de TI realizados en la Fase I.
2. Selección de las Funciones Principales de TI, tomando como referencia el análisis de las funciones realizadas en la Fase I.
3. Verificar los Acuerdos de Niveles de Servicio para los servicios prestados por terceros.

6.3.3 FASE III

En esta fase se continúa con las actividades de Gestión de Proyectos:

1. Ejecución
2. Pruebas
3. Cierre
4. Documentación del Proyecto

En lo que respecta a la Gestión de Riesgos, en esta fase se culmina realizando una Política de Seguridad y generando el Documento del Plan de Seguridad en base a toda la información recopilada en las actividades de la Fase II. El plan de Seguridad permitirá generar varios proyectos asociados a cubrir los temas de seguridad por cuanto esta actividad se enlaza con la actividad de Cartera de Proyectos en el Plan Estratégico de TI.

En lo que respecta al Plan de Continuidad las actividades que se deben realizar en esta Fase son:

1. Selección de Estrategias de Continuidad, tomando como referencia el análisis de los riesgos realizados en la Fase II de la Gestión de Riesgos
2. Organización de la Continuidad
3. Medidas de Mitigación y Contingencia
4. Comunicación y Capacitación
5. Documento del Plan de Continuidad

Por último, para asegurar el correcto manejo de la documentación se debe cumplir con la actividad de Control de la Documentación durante todo el ciclo de actividades: mantener formatos estándares, cumplir con fechas de vigencia, realizar aprobaciones y registrar el envío de copias, permitirá formalizar la siguiente documentación:

1. Documento de Proyectos
2. Documento de Plan de Seguridad
3. Política de Seguridad
4. Política de Continuidad
5. Documento Plan de Continuidad.
6. Documento de Acuerdos de Niveles de Servicio

7 Capitulo VII

CONCLUSIONES Y RECOMENDACIONES

7.1 CONCLUSIONES

1. Cobit versión 4.1, como herramienta de auditoría, permitió evaluar de una manera objetiva la situación actual del área de Tecnología de ENAP SIPETROL Ecuador, la metodología es explícita, entendible y de fácil uso. Los objetivos de control permitieron definir los elementos auditables en cada proceso proporcionando un punto de referencia en el cumplimiento del desempeño de TI.

2. El alcance de la metodología Cobit es muy amplio, debido a que abarca a todos los procesos de Tecnología, es muy importante saber seleccionar los procesos a ser auditados en base a las necesidades de la organización, en este proyecto, los procesos fueron seleccionados tomando en cuenta la alineación de los objetivos de TI con los objetivos del Negocio.

3. La metodología utilizada para seleccionar los procesos a ser auditados se basaron en el Apéndice 1 del libro Cobit 4.1, tomando como referencia las metas del negocio definidas en el Balanced Scorecard, identificando el objetivo estratégico en el que TI forma parte; para cumplir con este objetivo se establecieron metas de TI las cuales se identificaron en los procesos definidos en la metodología Cobit. Por último para priorizar los procesos Cobit a ser auditados se identificaron los procesos que permitían cumplir con la mayoría de las metas de TI.

4. La mayoría de los procesos evaluados en el departamento de TI tienen un nivel 2, siendo 5 el máximo valor dentro de la escala de niveles de madurez que presenta Cobit, esto se debe a que la organización integra a TI en un solo proceso definido en el Balanced Scorecard, por lo tanto, los objetivos de TI si se encuentran alineados a los objetivos del negocio en la ponderación asignada en el Balanced Scorecard.

5. Cobit permitió evaluar la parte técnica dándonos a conocer si las tareas son ejecutadas de una manera estándar, se pudo evidenciar que los procesos de operaciones se encuentran en un nivel de madurez 1 “Inicial-Ad hoc”, adicionalmente, se realizó una auditoría de gestión determinando si la administración de TI es adecuada, dándonos como resultado un nivel de madurez 2 “Repetible pero intuitivo”.

6. Los niveles de madurez establecidos en los 11 procesos auditados, determinan la situación actual de TI: el 9% corresponde al nivel 0 “No existente”, el 37% corresponde al nivel 1 “Inicial-Ad hoc”, el 27% corresponde al nivel 2 “Repetible pero intuitivo”, el 27% corresponde al nivel 3 “Proceso Definido”, concluyendo que el 73 % de los procesos deben ser mejorados.

7. Se determinó que el mayor riesgo que afecta al negocio es la falta de corresponsabilidad e involucramiento de la Dirección General en la toma de decisiones que conciernen a tecnología, delegando toda la responsabilidad en la Gerencia de TI.

8. Los procesos que tienen relación con la seguridad y continuidad del negocio no contemplan un plan de acción, asignación de recursos y responsables ya que no forman parte del plan estratégico del negocio, por lo tanto, no se han establecido controles para mitigar o eliminar los incidentes de seguridad constituyendo un grave riesgo para la organización.

9. No se ha realizado un análisis de los perfiles de cargo y descripción de funciones del área de Tecnología en base al crecimiento de la organización y nuevos servicios, esto conlleva a que exista una sobrecarga de trabajo.

10. La recopilación de la documentación que permite evidenciar los puntos auditables no estuvo disponible en su totalidad, debido a una falta de cultura de generación de documentos importantes como políticas, procedimientos,

cronogramas; la generación de este tipo de documentación es informal y no sigue un estándar, generando un retraso en la duración de la auditoría.

11. La Gestión del Área de TI, relacionada con: Administración de Proyectos, Gestión de Incidentes, Planes de Contingencia, Planes de Seguridad de la Información, no siguen una metodología que guíen adecuadamente estos aspectos dentro de la organización.

12. Los Objetivos de TI ayudan a cumplir un solo objetivo estratégico dentro del Balanced Scorecard de la organización "Excelencia Administrativa y Tecnológica", se considera este objetivo muy amplio y subjetivo ya que no permite evidenciar la responsabilidad del Área de TI en el ámbito del negocio.

13. El Informe Final de Auditoría se presenta en el capítulo V, el cual consta de un resumen Gerencial de todo el trabajo de auditoría describiendo los hallazgos encontrados y las recomendaciones sugeridas.

14. Se analizó el nivel de madurez de 5 empresas petroleras y de servicios petroleros, 3 de 5 empresas encuestadas poseen altos niveles de madurez entre 3 "Definido" y 5 "Optimizado" debido a la experiencia y trayectoria de más de 40 años de servicio y de haber adoptado las mejores prácticas de empresas transnacionales con estándares de la industria Americana.

15. En el Capítulo V, se presentan proyectos asociados a las recomendaciones, para ello se han tomado en cuenta los factores de riesgo en cada objetivo de control. Los proyectos sugeridos se los ha priorizado en base a dos pilares del Balanced Scorecard de Enap-Sipetrol: Estrategia, Cultura y Estructura – Operación Eficiente y Segura. Los proyectos cubren las áreas de Planificación Estratégica, Gestión de Proyectos, Gestión de Riesgos, Plan de Continuidad y Acuerdos de Niveles de Servicio.

16. La obtención del nivel de madurez de la industria por medio de encuestas enviadas a los responsables de tecnología, tuvo poca colaboración y requirió de insistencia para contar con la respuesta requerida.

17. De los proyectos obtenidos como resultado de la auditoria el 54% tienen un costo cero asociado a su implementación pero el 46% restante tienen un costo total de $91000 que representa un 16% en el presupuesto anual de tecnología.

18. Los proyectos asociados pretenden generar una mejora y un alineamiento del área de tecnología con la organización en el menor tiempo posible y al incorporar un componente económico representativo esta mejora dependerá de la asignación de presupuesto previa aprobación gerencial.

19. La generación de una implementación de proyectos por parte del grupo auditor no necesariamente debe ser tomada como una regla sino más bien como una guía de implementación para obtener beneficios al corto plazo con la menor inversión económica de inicio.

7.2 RECOMENDACIONES

1. Se recomienda utilizar a la Metodología Cobit no sólo como una herramienta de auditoría sino como una herramienta de Gestión de TI, debido a que permite establecer el nivel de madurez de los procesos por medio de sus objetivos de control.

2. Con el objetivo de mejorar tanto los procesos de operaciones como los procesos de gestión se recomienda alcanzar un nivel de madurez 3 "Proceso Definido", para asegurar la estandarización de los procesos, la documentación y la comunicación a la organización. El alcanzar el nivel de madurez 3 no implica un alto presupuesto, en su lugar está enfocado al levantamiento y mejora de los procesos.

3. Crear un Comité de Tecnología que permita definir los lineamientos de tecnología y ser corresponsables en la toma de decisiones importantes que afecten directamente al negocio.

4. Se sugiere realizar revisiones anuales a los procesos auditados en este proyecto, que permita hacer seguimiento a las recomendaciones generadas y ver la posibilidad de realizar una nueva evaluación para los procesos que no fueron considerados en el presente trabajo.

5. Se recomienda poner especial énfasis en los procesos referentes a la seguridad y continuidad del negocio, estos procesos deben ser parte del plan estratégico de la organización.

6. Realizar un análisis de los perfiles de cargo y descripción de funciones del área de Tecnología en base al crecimiento de la organización y la prestación de nuevos servicios.

7. La documentación importante de la empresa tal como: políticas, procedimientos, cronogramas, organigramas, manuales, etc., deben ser documentadas en formatos estándares que permitan evidenciar de una mejor manera la información.

8. Se recomienda a la Gerencia de TI, la adopción de metodologías que ayuden a la correcta Gestión de Proyectos - PMP, a la Gestión de TI - Cobit v5, a la Gestión de Servicio – ITIL, para asegurar una adecuada administración de los recursos tecnológicos y el cumplimiento de los objetivos y metas de TI.

9. Se recomienda a la Gerencia General establecer Objetivos Estratégicos de tipo SMART (específicos, medibles, alcanzables y que se puedan medir en el tiempo), para que los objetivos departamentales puedan alinearse de mejor manera con los objetivos del negocio.

10. En el Balanced Scorecard, la participación del departamento de Tecnología es de un 2% ya que solamente está presente en un solo objetivo estratégico, esto no corresponde a la realidad de la empresa ya que se evidencia la participación de TI en todos los procesos del negocio, se recomienda ampliar los objetivos estratégicos que involucren al departamento de Tecnología.

11. Se recomienda implementar los proyectos sugeridos, mencionados en el capítulo VI, ya que ellos mitigan o eliminan los riesgos encontrados en la auditoría. Se pone a consideración del Gerente de TI, un plan de implementación, pero se los puede implementar de acuerdo a la necesidad del negocio.

12. Se recomienda utilizar este trabajo como una guía para los estudiantes y profesionales que deseen involucrarse en el amplio mundo de la Auditoría Informática, y como una herramienta que permita establecer los niveles de desempeño del Área de TI.

13. Se recomienda que el personal de tecnología reciba capacitación en COBIT 4.1 para que pueda comprender y alinear la organización con este marco de referencia.

14. Para la implementación de los proyectos se recomienda el realizarlos con empresas multinacionales de consultoría para un resultado garantizado.

15. Se recomienda el gestionar los proyectos con costos mayores a $10000 dólares directamente con la Gerencia General para acelerar su aprobación.

8 BIBLIOGRAFÍA

EKOS. (15 de Enero de 2013). *www.ekosnegocios.com*. Obtenido de EKOS, Portal de Negocios: http://www.ekosnegocios.com/empresas/Empresas.aspx?idE=146&nombre=ENAP%20SIPETROL%20S.%20A.&b=1

http://auditoriasistemas.com. (s.f.). Obtenido de http://auditoriasistemas.com: http://auditoriasistemas.com/auditoria-de-sistemas-informaticos/

http://fcasua.contad.unam.mx. (s.f.). Obtenido de http://fcasua.contad.unam.mx: http://fcasua.contad.unam.mx/apuntes/interiores/docs/98/8/audi_infor.pdf

http://itilv3.osiatis.es. (s.f.). Obtenido de http://itilv3.osiatis.es: http://itilv3.osiatis.es/ciclo_vida_servicios_TI.php

http://www.docstoc.com. (s.f.). Obtenido de http://www.docstoc.com: http://www.docstoc.com/docs/76828904/Ejemplo-de-un-Informe-de-Auditor%C3%ADa-Inform%C3%A1tica-%28PDF%29

http://www.itil-officialsite.com/ . (s.f.). Obtenido de http://www.itil-officialsite.com/ : http://www.itil-officialsite.com/

http://www.slideshare.net. (s.f.). Obtenido de http://www.slideshare.net: http://www.slideshare.net/AmdCdmas/informe-final-de-auditoria-informatica

http://www.uaeh.edu.mx. (s.f.). Obtenido de http://www.uaeh.edu.mx: http://www.uaeh.edu.mx/docencia/P_Presentaciones/huejutla/sistemas/auditoria_informatica/auditoria.pdf

(2001). IT Assurance Guide: Using COBIT®. En I. G. Institute, *IT Assurance Guide: Using COBIT®*. Estados Unidos.

ISACA. (2008). *The Risk IT Framework*. Estados Unidos.

ISACA, ITAFTM. (2008). *A Professional Practices Framework for IT Assurance*. Estados Unidos.

IT Governance Institute. (2007). Cobit 4.1. En I. G. Institute, *Cobit 4.1* (pág. 211). Rolling Meadows, Illinois, United States: IT Governance Institute.

IT Governance Institute. (2007). *Cobit 4.1*. Estados Unidos.

IT Governance Institute. (2007). COBIT 4.1. En I. G. Institute, *COBIT 4.1* (pág. 211). Rolling Meadows: IT Governance Institute.

IT Governance Institute. (2008). *Enterprise Value: Governance of IT Investments.* Estados Unidos.

Mario G. Piattini, E. D. (2001). *Auditoria Informática un enfoque práctico* (2da. Edición ed.). México: Editorial Alfa Omega.

PMBOK 3 ediciónPMP. (s.f.). *Programa de Certificación.*