ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

AUDITORÍA DE LA GESTIÓN DE LAS TIC'S PARA UNA EMPRESA DE AVIACIÓN

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

PRISCILA ROCIO CAJAMARCA ERAZO
priscila_cajamarca@hotmail.com

DIRECTOR: MSC. ING. JAIME FABIÁN NARANJO ANDA
jaime.naranjo@epn.edu.ec

Quito, Agosto 2013

DECLARACIÓN

Yo, Priscila Rocio Cajamarca Erazo, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Priscila Rocio Cajamarca Erazo

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Priscila Rocio Cajamarca Erazo, bajo mi supervisión.

Ing. Jaime Naranjo

DIRECTOR DEL PROYECTO

AGRADECIMIENTOS

A Dios por cada día de vida, por permitirme lograr mis sueños y por todas las bendiciones recibidas.

A mis padres por todo su apoyo, sus palabras y por haberme ayudado con lo necesario para seguir y alcanzar mi objetivo.

A mis hermanas y mi hermano por todos los momentos compartidos durante todo este tiempo.

Al Ing. Jaime Naranjo por haberme guiado y brindado las herramientas necesarias para el desarrollo de este trabajo.

A la Gerencia y el personal de área de Tecnologías de la Información de la empresa que me auspicio, por su apoyo, tiempo y colaboración en todo lo necesario para la realización de este trabajo.

A mi novio Diego, por todo el apoyo que me ha brindado y por estar ahí siempre alentándome para alcanzar mis objetivos.

A mis amigas que desde el colegio hemos conservado una buena amistad, y con quienes he compartido muchos momentos de mi vida.

A mis amistades de la Poli, quienes he conocido en las aulas, por los amigos de los amigos, por la música, es decir, por diferentes aspectos; con quienes hemos alcanzado una gran amistad. Apoyándonos en diferentes etapas y situaciones de la vida y compartiendo gratos momentos dentro y fuera de la Poli.

Gracias a todos.

Priscila C. E.

DEDICATORIA

A mis padres: Aida y Alberto porque gracias a su apoyo incondicional he podido alcanzar este logro.

A mis hermanos: Robinson, Myriam y Mayra.

Les quiero mucho, gracias por cada día compartido y por estar en todos los momentos buenos y malos de mi vida.

Priscila C. E.

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

En la actualidad las empresas presentan varios problemas en la Gestión de TIC'S, por esta razón, es necesario realizar un análisis del área de Sistemas con la finalidad de identificar posibles problemas y problemas existentes para buscar la mejor forma de proponer soluciones con procedimientos formales.

A continuación se detalla un resumen del contenido del presente trabajo:

El *Capítulo I* presenta la caracterización de la empresa, la cual incluye su actividad principal, descripción, cómo está organizada. Además se realiza un análisis de la situación actual de la empresa y finalmente se realiza la justificación de la metodología.

El *Capítulo II* muestra una caracterización del área de Sistemas de la empresa, también se detalla la selección de procesos del marco de trabajo COBIT 4.1 que fueron escogidos para la evaluación de los procesos. De igual forma se detalla la realización de la Auditoría de la Gestión de TIC'S para una Empresa de Aviación.

El Capítulo *III* contiene un análisis de los resultados obtenidos en la Auditoría. Además se presenta los siguientes informes: Informe Preliminar, informe Técnico e Informe Ejecutivo.

En el Capítulo *IV* se detallan las conclusiones y recomendaciones obtenidas en el trabajo realizado.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 CARACTERIZACIÓN DE LA EMPRESA

Por motivos de confidencialidad le denominaremos EA (Empresa Aérea) a la empresa de aviación donde se realizará la Auditoría de Gestión de TIC'S.

1.1.1 ACTIVIDAD PRINCIPAL

La empresa EA tiene como finalidad integrar y fomentar el desarrollo comercial turístico y cultural. Cientos de pasajeros se transportan diariamente en sus aviones a rutas nacionales e internacionales.

La adquisición de transportes modernos y de mayor capacidad les ha permitido ampliar el mercado comercial.

1.1.2 DESCRIPCIÓN DE LA EMPRESA

Los servicios de la empresa EA se rigen en estándares de seguridad, cuidado del medio ambiente para satisfacer las necesidades de sus clientes.

EA está conformada por más de 800 empleados, quienes reciben cursos de actualización dependiendo del área en el que se desempeñan para elevar su nivel técnico y profesional.

EA cuenta con diferentes certificaciones en las áreas de Gestión de Calidad, Gestión Ambiental, Sistemas de Gestión de Seguridad y Trabajo.

EA está enfocada en cumplir sus metas estratégicas teniendo en cuenta todos los recursos necesarios para brindar sus servicios y satisfacer a sus clientes.

1.1.3 ESTRUCTURA ORGANIZACIONAL DE LA EMPRESA

La Gerencia de Tecnologías de la Información se encuentra a Nivel Ejecutivo de Decisión, bajo la Vicepresidencia Ejecutiva, a este nivel se encuentran las áreas estratégicas como Recursos Humanos, Operaciones y Mantenimiento, como se muestra en la Figura 1-1.

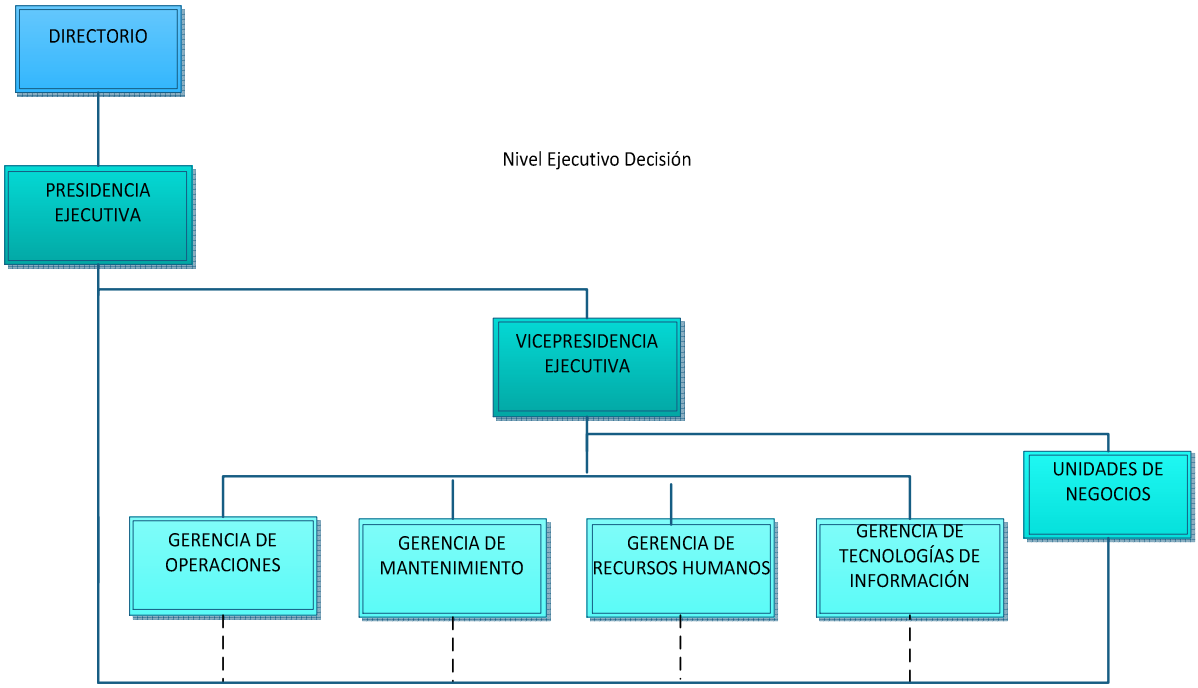

Figura 1-1 Extracto del Orgánico Funcional de la Empresa EA[1]

1.1.4 PLANIFICACIÓN ESTRATÉGICA[2]

La planificación estratégica de la empresa EA está constituida de la siguiente manera:

1.1.4.1 Plan Estratégico

En este documento se tiene las siguientes perspectivas: Finanzas, Clientes, Procesos y Capacidad Organizacional, donde para cada una de estas áreas se plantean Objetivos estratégicos a corto y largo plazo.

- **Interrelación de Objetivos y Acciones Estratégicas**

  Se tiene un mapa estratégico de la empresa EA, el mismo que permite visualizar la interrelación de los objetivos en las perspectivas antes mencionadas.

  Y se tiene adicionalmente los siguientes mapas estratégicos:

  - Mapa estratégico de la perspectiva Financiera: El mismo que está orientado a fortalecer el sistema de Gestión Financiera.

[1] Basado en documentación entregada por la empresa.
[2] Basado en el Plan Estratégico de la empresa.

- Mapa estratégico de la perspectiva del Cliente: El mismo que está orientado a fortalecer los procesos orientados al cliente.
- Mapa estratégico de la perspectiva de Procesos: Con el fin de fortalecer los procesos internos.
- Mapa estratégico perspectiva Capacidad Organizacional: Que está orientado a fortalecer la capacidad organizacional.

- **Políticas para el cumplimiento del Plan Estratégico**

  En este documento se detalla una serie de políticas y procedimientos para lograr cada uno de los objetivos estratégicos de la empresa.

  Donde también se toma en cuenta el cumplimiento de la normativa legal vigente.

- **Antecedentes[1]:**
  - ✓ Matriz FODA
  - ✓ FODA en las cuatro perspectivas
  - ✓ Deducción de objetivos centrales
  - ✓ Política y objetivos de calidad
  - ✓ Confrontación de los objetivos estratégicos con los de calidad

1.1.5 SERVICIOS

Los principales servicios que presenta la empresa EA son:

- ✓ Transporte aéreo nacional
- ✓ Transporte aéreo internacional
- ✓ Transporte aéreo de carga

1.1.5.1 Servicios WEB

- ✓ Consulta de Itinerarios de vuelos.
- ✓ Compra de pasajes aéreos con tarjetas de crédito.
- ✓ Consulta de estados de envíos.

1.1.5.2 Otros Servicios

- ✓ Socios VIP
- ✓ Acumulación de millas

[1] Basado en información entregada por la empresa.

- ✓ Reembolso de boletos
- ✓ Certificaciones

1.2 ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA EMPRESA

Para este análisis de la situación actual de la empresa EA, se toma como guía el marco de referencia ITIL v3.

La información que se presenta a continuación está basada en entrevistas (**Anexo 1**) realizadas a las Gerencia de TI y a los responsables de cada de una de las áreas de este departamento.

1.2.1 ESTRATEGIA DE SERVICIO

1.2.1.1 Gestión Financiera

Para los costos asociados con los productos y servicios de TI, la empresa EA toma en cuenta este aspecto en la Planificación Estratégica, además se considera los proyectos pendientes y nuevos proyectos.

Luego de esto se realiza un análisis de acuerdo a la importancia de los mismos y se asigna un presupuesto junto con el área Financiera para acordar los proyectos que se realizarán el en Plan Operativo Anual.

1.2.1.2 Gestión del Portafolio de Servicios

La Gestión de Portafolio de Servicios en la empresa EA tiene la finalidad de satisfacer las necesidades de los clientes, los servicios que ofrece han ido mejorando de acuerdos a las necesidades, falencias encontradas y nuevos requerimientos.

1.2.1.3 Gestión de la Demanda

La Empresa EA para la adquisición de Infraestructura de TI, esto lo realiza con un dimensionamiento planificadoa 5 años, con la finalidad de que soporte las necesidades y nuevos requerimientos del negocio.

Para el desarrollo de software la Empresa EA está realizando una reestructuración de QA (Aseguramiento de la calidad) con el fin de mejorar los niveles de calidad que ofrece.

1.2.2 DISEÑO DEL SERVICIO

1.2.2.1 Gestión del Catálogo de Servicios

Para el mantenimiento y actualización de los servicios se realiza una planificación de acuerdo al mercado que se desea enfocar y a las metas que se espera alcanzar, ya sean de tipo nacional, internacional, entre otros.

1.2.2.2 Gestión de Niveles de Servicio

El nivel de servicios está medido de acuerdo a la satisfacción de los clientes, cumpliendo con los requerimientos deseados y los beneficios esperados.

1.2.2.3 Gestión de la Capacidad

El tema de almacenamiento al momento lo realizan para algunos aspectos como *respaldos*en la nube.

Además tratan de aprovechar los recursos con los que disponen, es necesario tener en cuenta que algunos equipos tienen una capacidad sub-dimensionada.

1.2.2.4 Gestión de la Disponibilidad

La disponibilidad es un aspecto importante para la empresa EA debido a la naturaleza del negocio, por esta razón la empresa cuenta con personal encargado de monitorear este tipo de problemas.

1.2.2.5 Gestión de la Continuidad de servicios de TI

La empresa EA maneja redundancia en los equipos para mantener la disponibilidad de sus servicios en el caso que suceda algún desastre, pero no se tiene la suficiente documentación formal.

Se manejan políticas y procedimientos para respaldar la información y aplicaciones. Los respaldos se realizan de manera diaria, semanal y mensual.

1.2.2.6 Gestión de la Seguridad

Para el acceso a las aplicaciones, la empresa EA maneja un sistema de autenticación con perfiles de usuario, para que los usuarios accedan únicamente a las opciones que les corresponde.

La empresa EA tiene al momento políticas y procedimientos de seguridad a nivel perimetral, pero no todo está formalizado y documentado.

La detección de vulnerabilidades se manejamediante una consultoría de seguridad.

1.2.2.7 Gestión de Proveedores

Para la contratación de servicios se basan en leyes gubernamentales, y para casos específicos por ejemplo para la adquisición de software se toma en cuenta que sea de aerolínea y cumpla con estándares del mercado.

1.2.3 TRANSICIÓN DE LOS SERVICIOS DE TI

1.2.3.1 Gestión de Entregas y Despliegues

En la empresa EA existen aplicaciones desarrolladas *In House* y *adquiridas*.

Aplicaciones In House.- Se tiene un ambiente de desarrollo donde se realizan pruebas previas a la implementación del ambiente de producción. El software que desarrollan debe cumplir con QA (Aseguramiento de la calidad) de acuerdo a las políticas de la empresa.

Aplicaciones adquiridas.- Estas aplicaciones se basan en los requerimientos de la empresa, la misma que se asegura que las aplicaciones cumplan con lo establecido.

Además las empresas contratadas brindan soporte y mantenimiento.

1.2.3.2 Gestión de Cambios

La gestión de cambios se realiza a través de una planificación basada en ChangeRequest, pero que no está documentada como tal en todas las áreas de TI.

1.2.3.3 Gestión de la Configuración y Activos del Servicio

El área de HelpDesk tiene documentación de los procesos que manejan; en el área de Infraestructura Tecnológica el personal si está al tanto de la infraestructuraexistente perolos procedimientos necesitan ser formalizados por escrito.

1.2.3.4 Gestión del Conocimiento

En la empresa EA existen procesos que están documentados para tener un respaldo de las actividades que se realizan y en el caso que falte una persona, se pueda utilizar esa información como guía, pero no se encuentran documentados todos los procesos.

Para las capacitaciones del personal, en la mayoría de casos se toma en cuenta a más de una persona para no depender de recurso humano clave.

1.2.4 OPERACIÓN DE LOS SERVICIOS DE TI

1.2.4.1 Gestión de Eventos

No existen procedimientos formales.

1.2.4.2 Gestión de Incidencias

No existen procedimientos formales.

1.2.4.3 Gestión de Peticiones

El área de HelpDesk es la encargada de atender las peticiones de los usuarios proporcionándoles los recursos necesarios para el cumplimiento de sus actividades, y dan soporte en los casos que son necesarios.

1.2.4.4 Gestión de Problemas

Para la solución de ciertos problemas se realiza de manera reactiva. Pero si existen casos donde tratan de ser proactivos monitoreando los procesos para determinar soluciones.

1.2.4.5 Gestión de Acceso a los Servicios de TI

Para otorgar permisos se tiene un sistema de autenticación basado en perfiles de usuario.

1.3 JUSTIFICACIÓN DE LA METODOLOGÍA

Para la realización de esta Auditoría se toma como marco de referencia COBIT 4.1. COBIT (Control ObjectivesforInformation and RelatedTechnology - Objetivos de Control para la Información y Tecnologías relacionadas), es un marco de trabajo que define las razones de por qué se necesita el gobierno de TI y que se necesita cumplir en el gobierno de TI. Además este marco de trabajo tiene las siguientes características:

- Orientado a negocios
- Orientado a procesos
- Basado en controles
- Impulsado por mediciones.

Este marco de trabajo da soporte al gobierno de TI de manea que se garantice lo siguiente:

- TI está alineada con el negocio
- TI habilita al negocio y maximiza los beneficios
- Los recursos de TI se usan de manera responsable
- Los riesgos de TI se administran apropiadamente

En la Figura 1-2 se muestra las áreas de enfoque del Gobierno de TI establecidas por COBIT, donde se describen los tópicos en los que la dirección ejecutiva debe poner atención para gobernar la TI de sus empresas.

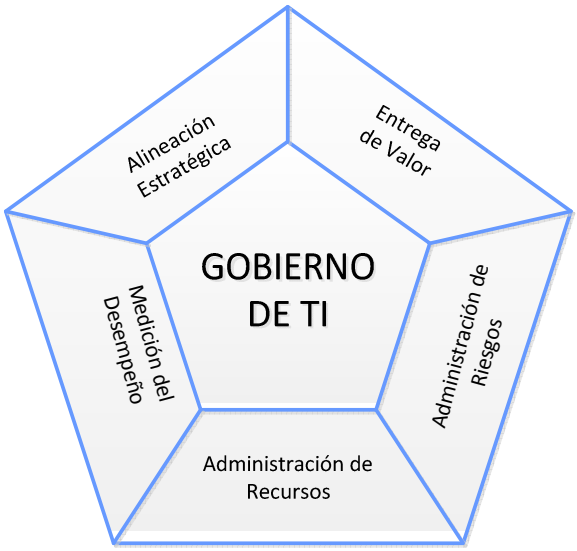

Figura 1-2 Áreas del Gobierno de TI[1]

Alineación Estratégica.- Consiste en la alineación entre los planes de negocio y de TI.

Entrega de Valor.- Está enfocada en la ejecución de la propuesta de valor con el fin de que la TI genere beneficios establecidos en la estrategia.

Administración de Riesgos.- Los altos ejecutivos deben tener en cuenta que riesgos están asociados a la empresa y asignar responsabilidades para la administración de los mismos.

Administración de Recursos.- Es la inversión óptima de los recursos críticos.

Medición del Desempeño.- Se refiere al rastreo y monitoreo de la estrategia de implementación, la terminación del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega de servicio.

En la Figura 1-3 se muestra el Marco de Trabajo Completo de COBIT, que está compuesto de cuatro dominios que contienen 34 procesos, administrando los recursos de TI para proporcionar información del negocio de acuerdo a los requerimientos del negocio y de gobierno.

[1] Documento COBIT 4.1

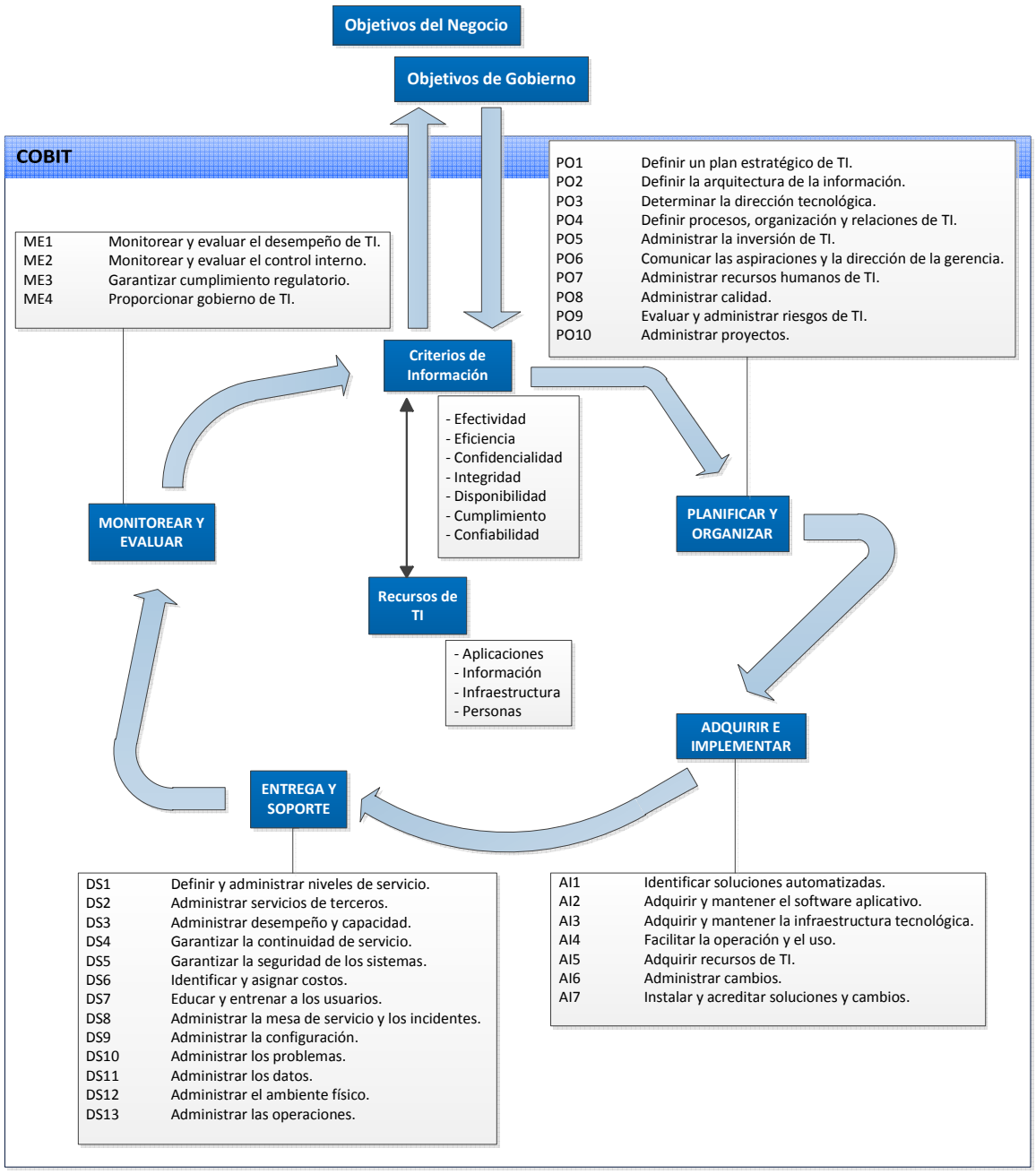

Figura 1-3 Marco de Trabajo de COBIT[1]

1.3.1 CRITERIOS DE INFORMACIÓN DE COBIT

Tomando en cuenta los requerimientos más amplios de calidad, fiduciarios y de seguridad, COBIT define los siguientes siete criterios de información[2]:

[1] Documento COBIT 4.1
[2] Basado en el documento de COBIT 4.1

Efectividad.- La información tiene que ser relevante y pertinente a los procesos del negocio y se debe proporcionar de manera oportuna, correcta, consistente y utilizable.

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

Confidencialidad.- Es la protección de información sensitiva contra revelación no autorizada.

Integridad.- Se refiere a que la información debe estar precisa, completa y su validez de acuerdo a los valores y expectativas del negocio.

Disponibilidad.- La información debe estar disponible cuando sea requerida por los procesos del negocio.

Cumplimiento.- Es acatar leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocio.

Confiabilidad.- Proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades.

1.3.2 MODELOS DE MADUREZ

El modelo de madurez está basado en un método de evaluación de la organización, con el fin de que se pueda evaluar así misma desde un nivel 0 ya que es posible que no existan procesos en lo absoluto.

La escala del 0-5 se basa en una escala de madurez simple que muestra como un proceso evoluciona desde una capacidad no existente hasta una capacidad optimizada.

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 se puede pasar al siguiente nivel superior sin haber cumplido todas las condiciones del nivel inferior.

Utilizando los modelos de madurez desarrollados para cada uno de los 34 procesos de COBIT, la gerencia podrá identificar: el desempeño de la empresa; el status actual de la industria; el objetivo de mejora de la empresa; el crecimiento requerido entre “cómo es” y “cómo será”.

El modelo de madurez es una forma de medir que tan bien están desarrollados los procesos administrativos, dependen principalmente de las metas de TI y de las necesidades del negocio subyacentes a las cuales sirven de base.

Las escalas del modelo de madurez ayudarán a los profesionales a explicarle a la gerencia dónde se encuentran los defectos en la administración de procesos de TI y establecer objetivos donde se requieran.

A continuación se detalla el *Modelo Genérico de Madurez de COBIT*[1].

0 No Existente.- Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.

1 Inicial.- Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

2 Repetible.- Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

3 Definido.- Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

4 Administrado.- Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de

[1] Basado en el documento de COBIT 4.1

forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

5 Optimizado.- Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

En la Tabla 1-1se muestra los Dominios y Procesos de TI, se tiene los Criterios de TI que afectan a los Objetivos de Control de alto nivel y los Recursos de TI que son aplicables.

Los Recursos de TI que están marcados con una (**X**), significa que ese objetivo de control tiene impacto sobre el recurso de TI. En los Criterios de Información de COBIT se identifica el grado de impacto: Primario (P), para indicar un impacto directo sobre el criterio de información.

Tabla 1-1Procesos definidos en los cuatro dominios[1]

OBJETIVOS DE CONTROL DE COBIT		Recursos TI de COBIT				Criterios de Información de COBIT						
PLANEAR Y ORGANIZAR		**Personas**	**Información**	**Aplicación**	**Infraestructura**	**Efectividad**	**Eficiencia**	**Confiabilidad**	**Integridad**	**Disponibilidad**	**Cumplimiento**	**Confiabilidad**
PO1	Definir un plan estratégico de TI.	X	X	X	X	P	S					
PO2	Definir la arquitectura de la información.		X	X		S	P	S	P			
PO3	Determinar la dirección tecnológica.			X	X	P	P					
PO4	Definir procesos, organización y relaciones de TI.	X				P	P					

[1]Documento de COBIT 4.1

PO5	Administrar la inversión de TI.	X		X	X	P	P					S
PO6	Comunicar las aspiraciones y la dirección de la gerencia.	X	X			P					S	
PO7	Administrar recursos humanos de TI.	X				P	P					
PO8	Administrar calidad.	X	X	X	X	P	P		S			S
PO9	Evaluar y administrar riesgos de TI.	X	X	X	X	S	S	P	P	P	S	S
PO10	Administrar proyectos.	X		X	X	P	P					
ADQUIRIR E IMPLEMENTAR												
AI1	Identificar soluciones automatizadas.			X	X	P	S					
AI2	Adquirir y mantener el software aplicativo.			X		P	P		S			S
AI3	Adquirir y mantener la infraestructura tecnológica.				X	S	P		S	S		
AI4	Facilitar la operación y el uso.	X		X	X	P	P		S	S	S	S
AI5	Adquirir recursos de TI.	X	X	X	X	S	P				S	
AI6	Administrar cambios.	X	X	X	X	P	P		P	P		S
AI7	Instalar y acreditar soluciones y cambios.	X	X	X	X	P	S		S	S		
ENTREGAR Y DAR SOPORTE												
DS1	Definir y administrar niveles de servicio.	X	X	X	X	P	P	S	S	S	S	S
DS2	Administrar servicios de terceros.	X	X	X	X	P	P	S	S	S	S	S
DS3	Administrar desempeño y capacidad.			X	X	P	P			S		
DS4	Garantizar la continuidad de servicio.	X	X	X	X	P	S			P		
DS5	Garantizar la seguridad de los sistemas.	X	X	X	X			P	P	S	S	S
DS6	Identificar y asignar costos.	X	X	X	X		P					P
DS7	Educar y entrenar a los usuarios.	X				P	S					
DS8	Administrar la mesa de servicio y los incidentes.	X		X		P	P					

DS9	Administrar la configuración.		X	X	X	P	S			S		S
DS10	Administrar los problemas.	X	X	X	X	P	P			S		
DS11	Administrar los datos.		X						P			P
DS12	Administrar el ambiente físico.			X					P	P		
DS13	Administrar las operaciones.	X	X	X	X	P	P		S	S		
MONITOREAR Y EVALUAR												
ME1	Monitorear y evaluar el desempeño de TI.	X	X	X	X	P	P	S	S	S	S	S
ME2	Monitorear y evaluar el control interno.	X	X	X	X	P	P	S	S	S	S	S
ME3	Garantizar cumplimiento regulatorio.	X	X	X	X						P	S
ME4	Proporcionar gobierno de TI.	X	X	X	X	P	P	S	S	S	S	S

(P) Primario; (S) Secundario

CAPÍTULO II

EJECUCIÓN DE LA AUDITORÍA DE GESTIÓN DE TIC'S

2.1 SITUACIÓN ACTUAL DEL ÁREA DE SISTEMAS

2.1.1 ESTRUCTURA ORGANIZACIONAL DEL ÁREA DE SISTEMAS

La unidad informática de la Empresa EA, se denomina Gerencia de TI (Tecnologías de Información), tiene una estructura organizacional como se representa en la Figura 2-1.

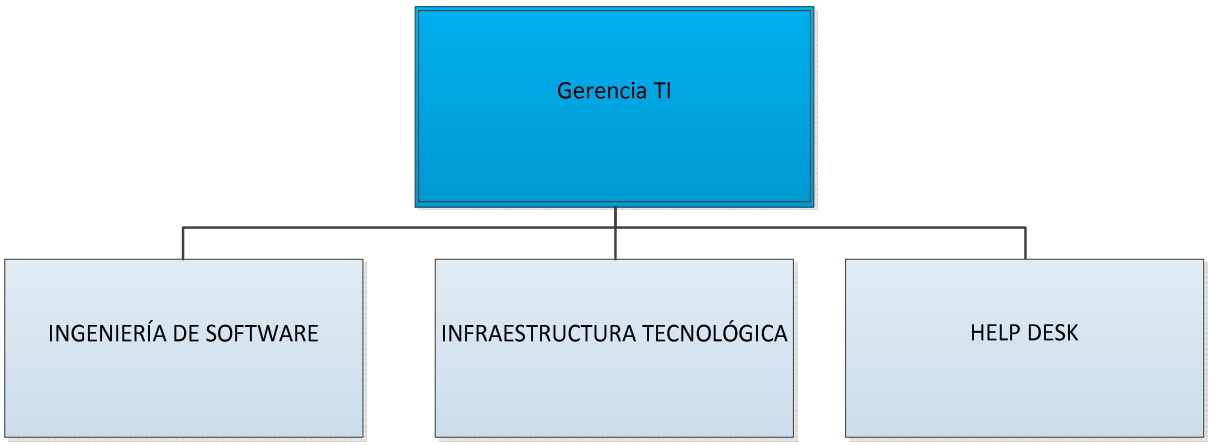

Figura 2-1 Orgánico Funcional de TI[1]

2.1.2 FUNCIONES DE LA GERENCIA DE TI[2]

La Gerencia de TI está dividida en tres áreas, y cumple las funcionesque se detallan a continuación:

2.1.2.1 Ingeniería de Software

Esta área está encargada del desarrollo y mantenimiento de software.

[1] Basado en información entregada por la empresa.
[2] Basado en documentación entregada por la empresa y entrevistas realizadas al personal de cada área de la Gerencia de TI.

2.1.2.1.1 Aplicaciones In House

Estas aplicaciones son desarrolladas de acuerdo a los requerimientos de la empresa, tienen como políticas desarrollar software que no haya en el mercado. De estas aplicaciones se tienen los respectivos manuales de usuario y manuales técnicos.

2.1.2.1.2 Aplicaciones Contratadas.

Para estas aplicaciones se hace un seguimiento con la finalidad que cumplan las especificaciones deseadas. De estas aplicaciones se tienen los manuales de usuario.

Además para el soporte del software las empresas con las que contratan satisfacen sus necesidades mediante los siguientes mecanismos:

- ✓ Correo electrónico
- ✓ Portal Web
- ✓ Telefonía

2.1.2.2 Infraestructura Tecnológica

En esta área se cumplen las siguientes funciones:

- ✓ Administración y operación de servidores
- ✓ Gestión de Redes
- ✓ Telefonía IP/ convencional
- ✓ Radiocomunicación
  - o VHF
  - o UHF
  - o HF

2.1.2.3 HelpDesk

- Mantener en óptimas condiciones todos los equipos informáticos.
- Atender nuevos requerimientos de configuraciones.
- Asignar perfiles de usuarios.
- Atender peticiones de usuarios
  - o Cambios y creación de contraseñas.
  - o Impresoras
  - o Cambios de equipos.
  - o Problemas de comunicación.

2.1.3 PLANESY PROCEDIMIENTOS DE LA EMPRESA

- Plan Informático.
- Plan operativo anual.
- Plan de respaldos.
- Plan de contratación.
- Planes de capacitación al personal
- Plan de vacaciones.

2.1.4 CARACTERIZACIÓN DE LA CARGA

En las entrevistas realizadas a los jefes de área, han determinado que las horas de mayor carga son entre las 10:00 a 12:30 y de 14:00 a 17:00.

2.1.4.1 Recurso Humano

Con relación al Recurso Humano, la Gerencia de TIcuenta con personal capacitado y experto en cada una de sus áreas donde se tiene Ingenieros en Sistemas, Ingenieros Electrónicos, Técnicos y Asistentes de TI.

La distribución de personal se tiene de la siguiente manera:

- Ingeniería de SW: 9 personas
- Infraestructura Tecnológica: 3 personas
- HelpDesk: 13 personas

2.1.4.2 Sistemas Operativos

2.1.4.2.1 Servidor

- Windows Server 2003
- Windows Server 2008
- Windows Server 2012
- Centos 5
- Red Hat 6

2.1.4.2.2 Escritorio

- Windows XP: 80%
- Windows 7: 15%
- Windows 8: 5%

2.1.5 SEGURIDAD DE LA EMPRESA

2.1.5.1 Seguridad Física

EA posee un servicio de guardianía privada mediante un sistema de relevos, mantiene una vigilancia de 24 horas.

El ingreso está controlado por el servicio de guardianía, quienes se encargan de verificar el ingreso con la cédula de identidad de los visitantes y entregándoles una tarjeta de visitante caracterizada por el número de piso, dirigiendo a cada persona a la dependencia apropiada para realizar el trámite pertinente.

En el caso que las personas ingresen mochilas se hace una revisión de pertenecías y al salir el personal de guardianía verifica que este lo ingresado, esto lo realizan por motivos de seguridad.

Además las dependencias del área de TI están protegidas por puertas que utilizan un sistema de tarjetas magnéticas.

En las tarjetas de visitante existen pasos a seguir en caso de emergencia la misma que será guiada con responsables en caso de emergencias o desastres naturales, pero no existe un plan específicamente detallado con este propósito.

También se tiene un sistema de video con cámaras instaladas en sitios estratégicos.

2.1.5.2 Seguridad del Personal

El personal de la Empresa EA posee un seguro del IESS, para el cual se realiza una aportación mensual y a partir del año los fondos de reserva.

La Empresa EA también cuenta con un seguro privado el mismo que es opcional y el empleado decide si desea o no adquirirlo.

La Empresa EA cumple con el Régimen Laboral vigente donde se detallan todos los beneficios decretados por ley para los empleados.

Los empleados tienen derecho a vacaciones por 15 días laborables hasta el quinto año de trabajo, a partir del quinto año los empleados tendrán un día adicional por año. Estas vacaciones se realiza con una planificación previa.

2.1.5.3 Seguridad Lógica

La Gerencia de TI ha descrito políticas de acceso a los servidores, únicamente tiene acceso el personal autorizado.

Las aplicaciones de la empresa EA cuentan con un sistema de autenticación que permite limitar el acceso a las opciones críticas, en función de las tareas asignadas a cada usuario.

2.1.5.4 Seguridad de Datos

- Se tiene mecanismos de respaldo diario, semanal y mensual.
- Se maneja información histórica.
- Se almacena en la nube:
    - Aplicaciones
    - Datos.
    - Respaldos de servidores

2.1.5.5 Seguridad Legal

Los servidores están asegurados y manejan SLAs preventivos y correctivos. Las máquinas de escritorio cuentan con garantías de fábrica que varían entre 1 y 3 años, adicionalmente se realiza mantenimiento a las PCs por parte del personal técnico de la empresa.

2.2 SELECCIÓN DE LOS PROCESOS Y DOMINIOS DE COBIT

La selección de dominios y procesos utilizados para la evaluación de la Unidad Informática de la Empresa EA,han sido escogidos conjuntamente con el Tutor de este trabajo y la Gerencia de Tecnologías de Información de dicha empresa. Debido al tamaño de la Unidad Informática no se han considerado la totalidad de procesos que presenta COBIT, sino únicamente los que se detallan a continuación.

2.2.1 DOMINIO: PLANEAR Y ORGANIZAR

PO1 Definir un Plan Estratégico de TI.

PO2 Definir la Arquitectura de la Información.

PO3 Determinar la Dirección Tecnológica.

PO4 Definir los procesos, organización y Relaciones de TI.

PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia.

PO7 Administrar los Recursos Humanos de TI.

PO9 Evaluar y Administrar los riesgos de TI.

PO10 Administrar Proyectos.

2.2.2 DOMINIO: ADQUIRIR E IMPLEMENTAR

AI2 Adquirir y mantener el software aplicativo.

AI3 Adquirir y mantener la infraestructura tecnológica.

AI4 Facilitar la operación y el uso.

AI5 Adquirir recursos de TI.

2.2.3 DOMINIO: ENTREGAR Y DAR SOPORTE

DS1 Definir y administrar niveles de servicio.

DS5 Garantizar la seguridad de los sistemas.

DS7 Educar y entrenar a los usuarios.

DS10 Administrar los problemas.

DS13 Administrar las operaciones.

2.2.4 DOMINIO: MONITOREAR Y EVALUAR

ME1 Monitorear y evaluar el desempeño de TI.

ME4 Proporcionar gobierno de TI.

2.3 SELECCIÓN DE LOS RECURSOS DE TI APLICABLES

De acuerdo a la selección de procesos realizada en el punto anterior, estos involucran todos los Recursos de TI que son:Aplicaciones, Infraestructura, Información yPersonas.

Según COBIT los *Recursos de TI*[1] se definen como se detalla continuación:

Aplicaciones.- Incluye tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.

Información.- Son los datos en todas sus formas, de entrada, procesados y generados por los sistemas de información, encualquier forma en que sean utilizados por el negocio.

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 lasaplicaciones.

Personas.- Se refiere al personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar lossistemas y los servicios de información. Estas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran.

[1] Basado en el Documento COBIT 4.1

2.4 REALIZACIÓN DE LA AUDITORÍA BASADA EN COBIT

Para la realización de este trabajo se ha utilizado la "Herramienta de Evaluación de Madurez de COBIT"[1] (**Anexo 2**) incluida en el kit de "Implementación y Mejora Continua del Gobierno de TI"[2], esta herramienta es presentada por COBIT para evaluar la madurez de los procesos de TI en una organización.

Se ha completado la información requerida por la herramienta antes mencionada, mediante entrevistas (**Anexo 1**) al personal de TI para obtener la información necesaria de cada uno de los procesos evaluados.

En el análisis de los procesos se debe tener las siguientes consideraciones que presenta la herramienta utilizada:

- En todos los procesos se analiza cada nivel de madurez (0 a 5).
- Existen sentencias para cada uno de los niveles. Se debe atribuir un factor de peso (1 a 10), este peso indica la importancia de cada una de las sentencias dentro de la organización y su ambiente externo. Por defecto, se tiene un peso de 5 para cada sentencia.
- Para las sentencias también debe indicarse en qué nivel se cumple (Está de acuerdo) con las siguientes escalas.
    - No se cumple.
    - Un poco.
    - En cierto grado.
    - Completamente.
- La multiplicación del peso por el nivel de cumplimiento de cada sentencia calcula la importancia relativa.
- Finalmente se obtiene la situación actual del proceso, debido a que esta herramienta calcula el nivel de cumplimiento, basándose en la importancia relativa y el peso de cada sentencia.

[1] COBIT Maturity Assessment Tool, ISACA, 2009
[2] Implementing and Continually Improving IT Governance, ISACA, 2009

2.4.1 PROCESOS DEL DOMINIO DE PLANEAR Y ORGANIZAR

2.4.1.1 PO1 Definir un Plan Estratégico de TI

Tabla 2-1 Resultado de evaluación del proceso PO1

PO1	Definir un Plan Estratégico de TI

Nivel	Cumplimiento	Contribución	Valor
0	1,00	0,00	0,00
1	0,81	1,00	0,81
2	0,85	1,00	0,85
3	0,87	1,00	0,87
4	0,90	1,00	0,90
5	0,58	1,00	0,58

Nivel de madurez=	**4,01**

Tabla 2-2Modelo de Madurez PO1

DOMINIO: PLANEACIÓN Y ORGANIZACIÓN					
PO1: Definición de un Plan Estratégico de Tecnología de Información					
NIVELES DE LOS MODELOS DE MADUREZ		CUMPLE	PARCIALMENTE	NO CUMPLE	OBSERVACIONES
NIVEL 0	No se lleva a cabo la planeación estratégica de TI. No existe conciencia por parte de la gerencia de que la planeación estratégica de TI es requerida para dar soporte a las metas del negocio.	X			
NIVEL 1	La gerencia de TI conoce la necesidad de una planeación estratégica de TI. La planeación de TI se realiza según se necesite como respuesta a un requerimiento de negocio específico. La alineación estratégica de TI se discute de forma ocasional en las reuniones de la gerencia de TI. La alineación de los requerimientos de las aplicaciones y tecnología del negocio se lleva a cabo de modo reactivo en lugar de hacerlo por medio de una estrategia organizacional. La posición de riesgo estratégico se identifica de manera informal proyecto por proyecto.	X			
NIVEL 2	La planeación estratégica de TI se comparte con la gerencia del negocio según se necesite. La actualización de los planes de TI ocurre como respuesta a las solicitudes de la dirección. Las decisiones estratégicas se toman proyecto por proyecto, sin ser consistentes con una estrategia global de la organización. Los riesgos ybeneficios al usuario, resultado de decisiones estratégicas importantes se reconocen de forma intuitiva.	X			

NIVEL 3	Una política define cómo y cuándo realizar la planeación estratégica de TI. La planeación estratégica de TI sigue un enfoqueestructurado, el cual se documenta y se da a conocer a todo el equipo. El proceso de planeación de TI es razonablemente sólido y garantiza que es factible realizar una planeación adecuada. Sin embargo, se otorga discrecionalidad a gerentesindividuales específicos con respecto a la implantación del proceso, y no existen procedimientos para analizar el proceso. La estrategia general de TI incluye una definición consistente de los riesgos que la organización está dispuesta a tomar como innovador o como seguidor. Las estrategias de recursos humanos, técnicos y financieros de TI influencian cada vez más la adquisición de nuevos productos y tecnologías. La planeación estratégica de TI se discute en reuniones de la dirección del negocio.	**X**			
NIVEL 4	La planeación estratégica de TI es una práctica estándar y las excepciones son advertidas por la dirección. La planeación estratégica de TI es una función administrativa definida conresponsabilidades de alto nivel. La dirección puede monitorear el proceso estratégicode TI, tomar decisiones informadas con base en el plan y medir su efectividad. La planeación de TI de corto y largo plazo sucede y se distribuye en forma de cascada hacia la organización, y las actualizaciones se realizan según sonnecesarias. La estrategia de TI y la estrategia organizacional se vuelven cada vez más coordinadas al abordar procesos de negocio y capacidades de valor agregado y al apalancar el uso de aplicaciones y tecnologías por medio de la re-ingeniería de procesos de negocio. Existen procesos bien definidos para determinar el uso de recursos internos y externos requeridos en el desarrollo y las operaciones de los sistemas.	**X**			
NIVEL 5	La planeación estratégica de TI es un proceso documentado y vivo, que cada vez más se toma en cuenta en el establecimiento de las metas del negocio y da como resultado un valor observable de negocios por medio de las inversiones en TI. Las consideraciones de riesgo y de valor agregado se actualizan de modo constante en el proceso de planeación estratégica de TI. Se desarrollan planes realistas a largo plazo de TI y se actualizan de manera constante para reflejar los cambiantes avances tecnológicos y el progreso relacionado al negocio. Se realizan evaluaciones por comparación contra normas industriales bien entendidas y confiables y se integran con el proceso de formulación de la estrategia. El plan estratégico especifica cómo los nuevos avances tecnológicos pueden impulsar creación de nuevas capacidades de negocio y mejorar la ventaja competitiva de la organización.			**X**	

COBIT define para el proceso PO1 los siguientes objetivos de control:

1. Administración del Valor de TI
2. Alineación de TI con el Negocio
3. Evaluación del Desempeño y la Capacidad Actual
4. Plan Estratégico de TI
5. Planes Tácticos de TI
6. Administración del Portafolio de TI

El objetivo esencial de un modelo de madurez es ascender a un grado de madurez superior, por esto, para que el proceso PO1 ascienda a un grado de madurez 5, como estrategia a corto plazo y conforme lo establece COBIT:

Se recomienda que la planeación estratégica considere que todas las metas del negocio estén en alineación con las metas de TI.

Se debe evaluar el cumplimiento del Plan Táctico (Plan Operativo Anual) para determinar si se está obteniendo los resultados esperados, que sería el cumplimiento de las metas estratégicas y tácticas.

Como estrategia a largo plazo se recomienda que se tome en consideración lo siguiente:

Se recomienda que la realización del Plan Estratégico y Táctico de TI se mantenga en mejora continua, tratando de cumplir normas bien definidas relacionadas al negocio.

2.4.1.2 PO2 Definir la Arquitectura de la Información

Tabla 2-3 Resultado de evaluación del proceso PO2

PO2	Definir la Arquitectura de la Información

Nivel	Cumplimiento	Contribución	Valor
0	0,83	0,00	0,00
1	0,65	1,00	0,65
2	0,89	1,00	0,89
3	0,73	1,00	0,73
4	0,61	1,00	0,61
5	0,52	1,00	0,52

Nivel de madurez =	**3,40**

Tabla 2-4Modelo de Madurez PO2

DOMINIO:PLANEACIÓN Y ORGANIZACIÓN					
PO2: Definir la Arquitectura de la Información					
	NIVELES DE LOS MODELOS DE MADUREZ	CUMPLE	PARCIALMENTE	NO CUMPLE	OBSERVACIONES
NIVEL 0	No existe conciencia de la importancia de la arquitectura de la información para la organización. El conocimiento, la experiencia y las responsabilidades necesarias para desarrollar esta arquitectura no existen en laorganización.	X			
NIVEL 1	La gerencia reconoce la necesidad de una arquitectura de información. El desarrollo de algunos componentes de una arquitectura de información ocurre de manera ad hoc. Las definiciones abarcan datos en lugar de información, y son impulsadas por ofertas de proveedores de software aplicativo. Existe una comunicación esporádica e inconsistente de la necesidad de una arquitectura de información.	X			
NIVEL 2	Surge un proceso de arquitectura de información y existen procedimientos similares, aunque intuitivos e informales, que se siguen por distintos individuos dentro de la organización. Las personas obtienen sushabilidades al construir la arquitectura de información por medio de experiencia práctica y la aplicación repetida de técnicas. Los requerimientos tácticos impulsan el desarrollo de los componentes de la arquitectura de la información por parte de los individuos.	X			

NIVEL 3	La importancia de la arquitectura de la información se entiende y se acepta, y la responsabilidad de su aplicación se asigna y se comunica de forma clara. Los procedimientos, herramientas y técnicas relacionados, aunque no son sofisticados, se han estandarizado y documentado y son parte de actividades informales de entrenamiento. Se han desarrollado políticas básicas de arquitectura de información, incluyendo algunos requerimientos estratégicos, aunque el cumplimiento de políticas, estándares y herramientas no se refuerza de manera consistente. Existe una función de administración de datos definida formalmente, que establece estándares para toda la organización, y empieza a reportar sobre la aplicación y uso de la arquitectura de la información. Las herramientas automatizadas se empiezan a utilizar, aunque los procesos y reglas son definidos por los proveedores de software de bases de datos. Un plan formal de entrenamiento ha sido desarrollado, pero el entrenamiento formal se basa en iniciativas individuales.	**X**			
NIVEL 4	Se da soporte completo al desarrollo e implantación de la arquitectura de información por medio de métodos y técnicas formales. La responsabilidad sobre el desempeño del proceso de desarrollo de la arquitectura se refuerza y se mide el éxito de la arquitectura de información. Las herramientas automatizadas de soporte están ampliamente generalizadas, pero todavía no están integradas. Se hanidentificado métricas básicas y existe un sistema de medición. El proceso de definición de la arquitectura de información es proactivo y se enfoca en resolver necesidades futuras del negocio. La organización de administración de datos está activamente involucrada en todos los esfuerzos de desarrollo de las aplicaciones, para garantizar la consistencia. Un repositorio automatizado está totalmenteimplementado. Se encuentran en implantación modelos de datos más complejos para aprovechar el contenido informativo de las bases de datos. Los sistemas de información ejecutiva y los sistemas de soporte a la toma de decisiones aprovechan la información existente.			**X**	
NIVEL 5	La arquitectura de información es reforzada de forma consistente a todos los niveles. El valor de la arquitectura de la información para el negocio se enfatiza de forma continua. El personal de TI cuenta con la experiencia y las habilidades necesarias para desarrollar y darmantenimiento a una arquitectura de información robusta y sensible que refleje todos los requerimientos del negocio. La información provista por la arquitectura se aplica de modo consistente y amplio. Se hace un uso amplio de las mejores prácticas de la industria en el desarrollo y mantenimiento de la arquitectura de información incluyendo un proceso de mejora continua. La estrategia para el aprovechamiento de la información por medio de tecnologías de bodega de datos y minería de datosestá bien definida. La arquitectura de la información se encuentra en mejora continua y toma en cuenta información no tradicional sobre los procesos, organizaciones y sistemas.			**X**	

COBIT define para el proceso PO2 los siguientes objetivos de control:

1. Modelo de Arquitectura de Información Empresarial
2. Diccionario de Datos Empresarial y Reglas de Sintaxis de Datos
3. Esquema de Clasificación de Datos
4. Administración de Integridad

El objetivo esencial de un modelo de madurez es ascender a un grado de madurez superior, por esto para que el proceso PO2 ascienda a un grado de madurez 4, como estrategia a corto plazo y conforme lo establece COBIT:

Se recomienda establecermetas y métricas parala evaluación del proceso de Desarrollo e Implementación de Arquitectura de la Información con el fin de mejorar el desempeño del mismo.

Se debe establecer procedimientos para que este proceso sea proactivo y logre resolver necesidades futuras del negocio.

El proceso de definición de Arquitectura de Información debe estar justificado formalmente, especificando las características y beneficios que se obtendrán con su implementación.

Como estrategia a largo plazo se recomienda que se tome en consideración lo siguiente:

Se recomienda que la Arquitectura de Información sea reforzada de manera consistente a todos los niveles para conseguir una mejor administración del proceso.

Se debe establecer tecnologías para la minería de datos.

Es necesario implementar procedimientos formales donde se incluya la mejora continua del proceso y se considere toda la información de los procesos organizacionales y sistemas.

2.4.1.3 PO3 Determinar la Dirección Tecnológica

Tabla 2-5 Resultado de evaluación del proceso PO3

PO3	Determinar la Dirección Tecnológica.

Nivel	Cumplimiento	Contribución	Valor
0	0,90	0,00	0,00
1	0,76	1,00	0,76
2	0,81	1,00	0,81
3	0,73	1,00	0,73
4	0,57	1,00	0,57
5	0,37	1,00	0,37

Nivel de madurez =	**3,25**

Tabla 2-6Modelo de Madurez PO3

DOMINIO: PLANEACIÓN Y ORGANIZACIÓN					
PO3: Determinar la Dirección Tecnológica					
	NIVELES DE LOS MODELOS DE MADUREZ	CUMPLE	PARCIALMENTE	NO CUMPLE	OBSERVACIONES
NIVEL 0	No existe conciencia sobre la importancia de la planeación de la infraestructura tecnológica para la entidad. El conocimiento y laexperiencia necesarios para desarrollar dicho plan de infraestructura tecnológica no existen. Hay una carencia de entendimiento deque la planeación del cambio tecnológico es crítica para asignar recursos de manera efectiva.	X			
NIVEL 1	La gerencia reconoce la necesidad de planear la infraestructura tecnológica. El desarrollo de componentes tecnológicos y laimplementación de tecnologías emergentes son ad hoc y aisladas. Existe un enfoque reactivo y con foco operativo hacia la planeaciónde la infraestructura. La dirección tecnológica está impulsada por los planes evolutivos, con frecuencia contradictorios, del hardware, del software de sistemas y de los proveedores de software aplicativo. La comunicación del impacto potencial de los cambios en latecnología es inconsistente.	X			

NIVEL 2	Se difunde la necesidad e importancia de la planeación tecnológica. La planeación es táctica y se enfoca en generar solucionestécnicas a problemas técnicos, en lugar de usar la tecnología para satisfacer las necesidades del negocio. La evaluación de loscambios tecnológicos se delega a individuos que siguen procesos intuitivos, aunque similares. Las personas obtienen sus habilidades sobre planeación tecnológica a través de un aprendizaje práctico y de una aplicación repetida de las técnicas. Están surgiendotécnicas y estándares comunes para el desarrollo de componentes de la infraestructura.	**X**			
NIVEL 3	La gerencia está consciente de la importancia del plan de infraestructura tecnológica. El proceso para el plan de infraestructuratecnológica es razonablemente sólido y está alineado con el plan estratégico de TI. Existe un plan de infraestructura tecnológicadefinido, documentado y bien difundido, aunque se aplica de forma inconsistente. La orientación de la infraestructura tecnológicaincluye el entendimiento de dónde la empresa desea ser líder y dónde desea rezagarse respecto al uso de tecnología, con base en losriesgos y en la alineación con la estrategia organizacional. Los proveedores clave se seleccionan con base en su entendimiento de latecnología a largo plazo y de los planes de desarrollo de productos, de forma consistente con la dirección de la organización.		**X**		**Objetivos no cumplidos:** No existe un plan de Infraestructura Tecnológica bien definido.
NIVEL 4	La dirección garantiza el desarrollo del plan de infraestructura tecnológica. El equipo de TI cuenta con la experiencia y las habilidadesnecesarias para desarrollar un plan de infraestructura tecnológica. El impacto potencial de las tecnologías cambiantes y emergentesse toma en cuenta. La dirección puede identificar las desviaciones respecto al plan y anticipar los problemas. La responsabilidad del desarrollo y mantenimiento del plan deinfraestructura tecnológica ha sido asignado. El proceso para desarrollar el plan deinfraestructura tecnológica es sofisticado y sensible a los cambios. Se han incluido buenas prácticas internas en el proceso. Laestrategia de recursos humanos está alineada con la dirección tecnológica, para garantizar que el equipo de TI pueda administrar loscambios tecnológicos. Los planes de migración para la introducción de nuevas tecnologías están definidos. Los recursos externos ylas asociaciones se aprovechan para tener acceso a la experiencia y a las habilidades necesarias. La dirección ha evaluado laaceptación del riesgo de usar la tecnología como líder, o rezagarse en su uso, para desarrollar nuevas oportunidades de negocio oeficiencias operativas.			**X**	
NIVEL 5	Existe una función de investigación que revisa las tecnologías emergentes y evolutivas y para evaluar la organización por comparacióncontra las normas industriales. La dirección del plan de infraestructura tecnológica está impulsada por los estándares y avancesindustriales e internacionales, en lugar de			**X**	

	estar orientada por los proveedores de tecnología. El impacto potencial de los cambiostecnológicos sobre el negocio se revisa al nivel de la alta dirección. Existe una aprobación ejecutiva formal para el cambio de ladirección tecnológica o para adoptar una nueva. La entidad cuenta con un plan robusto de infraestructura tecnológica que refleja los requerimientos del negocio, es sensible a los cambios en el ambiente del negocio y puede reflejar los cambios en éste. Existe unproceso continuo y reforzado para mejorar el plan de infraestructura tecnológica. Las mejores prácticas de la industria se usan deforma amplia para determinar la dirección técnica.				

COBIT define para el proceso PO3 los siguientes objetivos de control:

1. Planeación de la Dirección Tecnológica
2. Plan de Infraestructura Tecnológica
3. Monitoreo de Tendencias y Regulaciones Futuras
4. Estándares Tecnológicos
5. Consejo de Arquitectura de TI

El objetivo esencial de un modelo de madurez es ascender a un grado de madurez superior, por esto para que el proceso PO3 ascienda a un grado de madurez 4, como estrategia a corto plazo y conforme lo establece COBIT:

Se recomienda formalizar un Plan de Infraestructura Tecnológica donde se especifiquen claramente los objetivos, riesgos ya demás queeste alineado con las estrategias del negocio y pueda ser sujeto a cambios.

También se recomienda que se realicen evaluaciones acerca del uso de la tecnología para identificar los posibles riesgos.

Como estrategia a largo plazo se recomienda que se tome en consideración los siguientes puntos:

Se recomiendaque el Plan de Infraestructura Tecnológica este basado en estándares de la industria, para satisfacer las necesidades del negocio e implementar las mejores prácticas que sean relevantes para mejorar este proceso.

También es necesario que se implemente políticas y procedimientos formales para el desarrollo del Plan.

Acceder a recursos externos para los casos que sean necesarios con la finalidad de obtener mayor experiencia y las habilidades necesarias para cumplir con los objetivos del negocio y de TI.

2.4.1.4 PO4 Definir los procesos, organización y Relaciones de TI

Tabla 2-7Resultado de evaluación del proceso PO4

PO4	**Definir los Procesos, Organización y Relaciones de TI**

Nivel	Cumplimiento	Contribución	Valor
0	1,00	0,00	0,00
1	0,75	1,00	0,75
2	0,42	1,00	0,42
3	0,74	1,00	0,74
4	0,38	1,00	0,38
5	0,44	1,00	0,44

Nivel de Madurez =	**2,73**

Tabla 2-8Modelo de Madurez PO4

DOMINIO: PLANEACIÓN Y ORGANIZACIÓN					
PO4: Definir los procesos, organización y Relaciones de TI					
NIVELES DE LOS MODELOS DE MADUREZ		CUMPLE	PARCIALMENTE	NO CUMPLE	OBSERVACIONES
NIVEL 0	La organización de TI no está establecida de forma efectiva para enfocarse en el logro de los objetivos del negocio.	X			

NIVEL 1	Las actividades y funciones de TI son reactivas y se implantan de formainconsistente. TI se involucra en los proyectos solamente enlas etapas finales. La función de TI se considera como una función de soporte, sin una perspectiva organizacional general. Existe unentendimiento explícito de la necesidad de una organización de TI; sin embargo, los roles y las responsabilidades no están formalizados, ni reforzados.	**X**			
NIVEL 2	La función de TI está organizada para responder de forma táctica aunque de forma inconsistente, a las necesidades de los clientes ya las relaciones con los proveedores. La necesidad de contar con una organización estructurada y unaadministración de proveedoresse comunica, pero las decisiones todavía dependen del conocimiento y habilidades de individuos clave. Surgen técnicas comunespara administrar la organización de TI y las relaciones con los proveedores.	**X**			
NIVEL 3	Existen roles y responsabilidades definidos para la organización de TI y para terceros. La organización de TI se desarrolla, documenta, comunica y se alinea con la estrategia de TI. Se define el ambiente de control interno. Se formulan las relaciones con terceros, incluyendo los comités de dirección, auditoría interna y administración de proveedores. La organización de TI está funcionalmente completa. Existen definiciones de las funciones a ser realizadas por parte del personal de TI y las que deben realizar los usuarios. Losrequerimientos esenciales de personal de TI y experiencia están definidos y satisfechos. Existe una definición formal de las relacionescon los usuarios y con terceros. La división de roles y responsabilidades está definida e implantada.		**X**		**Objetivos no cumplidos:** Es En cierto grado hace falta formalizar las relaciones con terceros incluyendo los comités de la dirección, auditoría interna y administración de proveedores.
NIVEL 4	La organización de TI responde de forma proactiva al cambio e incluye todos los roles necesarios para satisfacer los requerimientos del negocio. La administración, la propiedad de procesos, la delegación y laresponsabilidad de TI están definidas y balanceadas. Sehan aplicado buenas prácticas internas en la organización de las funciones de TI. La gerencia de TI cuenta con la experiencia yhabilidades apropiadas para definir, implementar y monitorear la organización deseada y las relaciones. Las métricas medibles paradar soporte a los objetivos del negocio y los factores críticos de éxito definidos por el usuario siguen un estándar. Existen inventariosde habilidades para apoyar al personal de los proyectos y el desarrollo profesional. El equilibrio entre las habilidades y los recursosdisponibles internamente, y los			**X**	

	que se requieren de organizaciones externas están definidos y reforzados. La estructuraorganizacional de TI refleja de manera apropiada las necesidades del negocio proporcionando servicios alineados con los procesosestratégicos del negocio, en lugar de estar alineados con tecnologías aisladas.				
NIVEL 5	La estructura organizacional de TI es flexible y adaptable. Se ponen en funcionamiento las mejores prácticas de la industria. Existe un uso amplio de la tecnología para monitorear el desempeño de la organización y de los procesos de TI. La tecnología se aprovecha para apoyar la complejidad y distribución geográfica de la organización. Un proceso de mejora continua existe y está implantado.			**X**	

COBIT define para el proceso PO4 los siguientes objetivos de control:

1. Marco de Trabajo de Procesos de TI
2. Comité Estratégico de TI
3. Comité Directivo de TI
4. Ubicación Organizacional dela Función de TI
5. Estructura Organizacional
6. Establecimiento de Roles y Responsabilidades
7. Responsabilidad de Aseguramiento de Calidad de TI
8. Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento
9. Propiedad de Datos y de Sistemas
10. Supervisión
11. Segregación de Funciones
12. Personal de TI
13. Personal Clave de TI
14. Políticas y Procedimientos para Personal Contratado
15. Relaciones

El objetivo esencial de un modelo de madurez es ascender a un grado de madurez superior, por esto para que el proceso PO4 ascienda a un grado de madurez 4, como estrategia a corto plazo y conforme lo establece COBIT:

Se recomienda que se reforme la estructura organizacional de la empresa, donde la Gerencia de Tecnologías de Información se encuentre a un nivel asesor en la organización y de esta manera TIeste alineada con toda la organización.

Es necesario que se asignen roles y responsabilidades para fortalecer el manejo de Gestión de Riesgos y la Seguridad Informática.

Se debe fortalecer las relaciones con terceros involucrando a los comités de la dirección, auditoría interna y administración de proveedores.

Como estrategia a largo plazo se recomienda que se tome en consideración lo siguiente:

Se recomienda formalizar procedimientos para mejorar el desempeño y monitoreo de la organización y de los procesos de TI. Se mantenga en mejora continua y cumpla con los objetivos de la organización.

2.4.1.5 PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia

Tabla 2-9Resultado de evaluación del proceso PO6

PO6	**Comunicar las Aspiraciones y la Dirección de la Gerencia**		
Nivel	Cumplimiento	Contribución	Valor
0	1,00	0,00	0,00
1	0,54	1,00	0,54
2	0,84	1,00	0,84
3	0,56	1,00	0,56
4	0,51	1,00	0,51
5	0,46	1,00	0,46
	Nivel de madurez =		**2,92**

Tabla 2-10 Modelo de Madurez PO6

DOMINIO: PLANEACIÓN Y ORGANIZACIÓN					
PO6: Comunicar las Aspiraciones y la Dirección de la Gerencia					
NIVELES DE LOS MODELOS DE MADUREZ		CUMPLE	PARCIALMENTE	NO CUMPLE	OBSERVACIONES
NIVEL 0	La gerencia no ha establecido un ambiente positivo de control de información. No hay reconocimiento de la necesidad de establecer un conjunto de políticas, procedimientos, estándares y procesos de cumplimiento.	X			
NIVEL 1	La gerencia es reactiva al resolver los requerimientos del ambiente de control de información. Las políticas, procedimientos y estándares se elaboran y comunican de forma ad hoc de acuerdo a los temas. Los procesos de elaboración, comunicación ycumplimiento son informales e inconsistentes.	X			
NIVEL 2	La gerencia tiene un entendimiento implícito de las necesidades y de los requerimientos de un ambiente de control de informaciónefectivo, aunque las prácticas son en su mayoría informales. La gerencia ha comunicado la necesidad de políticas, procedimientos y estándares de control, pero la elaboración se delega a la discreción de gerentes y áreas de negocio individuales. La calidad sereconoce como una filosofía deseable a seguir, pero las prácticas se dejan a discreción de gerentes individuales. El entrenamiento serealiza de forma individual, según se requiera.	X			
NIVEL 3	La gerencia ha elaborado, documentado y comunicado un ambiente completo de administración de calidad y control de la información, que incluye un marco para las políticas, procedimientos y estándares. El proceso de elaboración de políticas es estructurado, mantenido y conocido por el personal, y las políticas, procedimientos y estándares existentes son razonablemente sólidos y cubren temas clave. La gerencia ha reconocido la importancia de la conciencia de la seguridad de TI y ha iniciado programas de concienciación. El entrenamiento formal está disponible para apoyar al ambiente de control de información, aunque no se aplica de forma rigurosa. Aunque existe un marco general de desarrollo para las políticas y estándares de control, el monitoreo del cumplimiento de estas políticas y estándares es inconsistente. Las técnicas para fomentar la conciencia de la seguridad estánestandarizadas y formalizadas.		X		**Objetivos no cumplidos:** Las técnicas para fomentar conciencia de la seguridad no están estandarizadas, ni formalizadas.

NIVEL 4	La gerencia asume la responsabilidad de comunicar las políticas de control interno y delega la responsabilidad y asigna suficientes recursos para mantener el ambiente en línea con los cambios significativos. Se ha establecido un ambiente de control de informaciónpositivo y proactivo. Se ha establecido un juego completo de políticas, procedimientos y estándares, los cuales se mantienen ycomunican, y forman un componente de buenas prácticas internas. Se ha establecido un marco de trabajo para la implantación y lasverificaciones subsiguientes de cumplimiento.			**X**	
NIVEL 5	El ambiente de control de la información está alineado con el marco administrativo estratégico y con la visión, y con frecuencia se revisa, actualiza y mejora. Se asignan expertos internos y externos para garantizar que se adoptan las mejores prácticas de la industria, con respecto a las guías de control y a las técnicas de comunicación. El monitoreo, la auto-evaluación y las verificaciones de cumplimiento están extendidas en la organización. La tecnología se usa para mantener bases de conocimiento de políticas y deconcienciación y para optimizar la comunicación, usando herramientas de automatización de oficina y de entrenamiento basado encomputadora.			**X**	

COBIT define para el proceso PO6 los siguientes objetivos de control:

1. Ambiente de Políticas y de Control
2. Riesgo Corporativo y Marco de Referencia de Control Interno de TI
3. Administración de Políticas para TI
4. Implantación de Políticas de TI
5. Comunicación de los Objetivos y la Dirección de TI

El objetivo esencial de un modelo de madurez es ascender a un grado de madurez superior, por esto para que el proceso PO6 ascienda a un grado de madurez 4, como estrategia a corto plazo y conforme lo establece COBIT:

Se recomienda reforzar los controles de información, las políticas de control interno, que todas las políticas y procedimientos acordados sean informados a todo el personal de TI.

Realizar un monitoreo para verificar que se cumpla todo lo establecido.

Formalizar y estandarizar las técnicas de concienciación de seguridad.

Como estrategia a largo plazo se recomienda que se tome en consideración los siguientes puntos:

Se recomienda implementar expertos internos y externos para garantizar que se adopten las mejores prácticas de la industria.

También se recomienda implementar bases de conocimientos de políticas y de concienciación con la finalidad de optimizar la comunicación mediante la implementación de herramientas de automatización.

2.4.1.6 PO7 Administrar los Recursos Humanos de TI

Tabla 2-11Resultado de evaluación del proceso PO7

PO7	**Administrar los Recursos Humanos de TI**		
Nivel	Cumplimiento	Contribución	Valor
0	1,00	0,00	0,00
1	0,92	1,00	0,92
2	0,82	1,00	0,82
3	0,77	1,00	0,77
4	0,29	1,00	0,29
5	0,46	1,00	0,46
		Nivel de madurez =	**3,25**

Tabla 2-12Modelo de Madurez PO7

DOMINIO: PLANEACIÓN Y ORGANIZACIÓN					
PO7: Administrar los Recursos Humanos de TI					
NIVELES DE LOS MODELOS DE MADUREZ		CUMPLE	PARCIALMENTE	NO CUMPLE	OBSERVACIONES
NIVEL 0	No existe conciencia sobre la importancia de alinear la administración de recursos humanos de TI con el proceso de planeación de la tecnología para la organización. No hay persona o grupo formalmente responsable de la administración de los recursos humanos de TI.	X			
NIVEL 1	La gerencia reconoce la necesidad de contar con administración de recursos humanos de TI. El proceso de administración derecursos humanos de TI es informal y reactivo. El proceso de recursos humanos de TI está enfocado de manera operacional en la contratación y administración del personal de TI. Se está desarrollando la conciencia con respecto al impacto que tienen los cambios rápidos de negocio y de tecnología, y las soluciones cada vez más complejas, sobre la necesidad de nuevos niveles de habilidades y de competencia.	X			
NIVEL 2	Existe un enfoque táctico para contratar y administrar al personal de TI, dirigido por necesidades específicas de proyectos, en lugar dehacerlo con base en un equilibrio entendido de disponibilidad interna y externa de personal calificado. Se imparte entrenamiento informal al personal nuevo, quienes después reciben entrenamiento según sea necesario.	X			
NIVEL 3	Existe un proceso definido y documentado para administrar los recursos humanos de TI. Existe un plan de administración de recursos humanos. Existe un enfoque estratégico para la contratación y la administración del personal de TI. El plan de entrenamiento formalestá diseñado para satisfacer las necesidades de los recursos humanos de TI. Está establecido un programa de rotación, diseñadopara expandir las habilidades gerenciales y de negocio.		X		**Objetivos no cumplidos:** No se ha establecido un programa de rotación, diseñado para expandir las habilidades gerenciales y de negocio, debido a que cada área cuenta con personal especializado en dicha área.

NIVEL 4	La responsabilidad de la elaboración y el mantenimiento de un plan de administración de recursos humanos para TI han sido asignados a un individuo o grupo con las habilidades y experiencia necesarias para elaborar y mantener el plan. El proceso para elaborar y mantener el plan de administración de recursos humanos de TI responde al cambio. La organización cuenta con métricasestandarizadas que le permiten identificar desviaciones respecto al plan de administración de recursos humanos de TI con énfasis especial en el manejo del crecimiento y rotación del personal. Las revisiones de compensación y de desempeño se estánestableciendo y se comparan con otras organizaciones de TI y con las mejores prácticas de la industria. La administración de recursoshumanos es proactiva, tomando en cuenta el desarrollo de un plan de carrera.			**X**	
NIVEL 5	El plan de administración de recursos humanos de TI se actualiza de forma constante para satisfacer los cambiantes requerimientos del negocio. La administración de recursos humanos de TI está integrada y responde a la dirección estratégica de la entidad. Los componentes de la administración de recursos humanos de TI son consistentes con las mejores prácticas de la industria, tales como compensación, revisiones de desempeño, participación en foros de la industria, transferencia de conocimiento, entrenamiento y adiestramiento. Los programas de entrenamiento se desarrollan para todos los nuevos estándares tecnológicos y productos antes desu implantación en la organización.			**X**	

COBIT define para el proceso PO7 los siguientes objetivos de control:

1. Reclutamiento y Retención del Personal
2. Competencias del Personal
3. Asignación de Roles
4. Entrenamiento del Personal de TI
5. Dependencia Sobre los Individuos
6. Procedimientos de Investigación del Personal
7. Evaluación del Desempeño del Empleado
8. Cambios y Terminación de Trabajo

El objetivo esencial de un modelo de madurez es ascender a un grado de madurez superior, por esto para que el proceso PO7 ascienda a un grado de madurez 4, como estrategia a corto plazo y conforme lo establece COBIT:

Se recomienda la elaboración y mantenimiento de un Plan de Administración de Recursos Humanos de TI, que permita realizar revisiones del desempeño del personal para satisfacer los requerimientos del negocio.

Implementar métricas estandarizadas que le permiten identificar desviaciones.

Como estrategia a largo plazo se recomienda que se tome en consideración lo siguiente:

Se recomienda que la Administración de Recursos Humanos de TI este integrada y responda a las estrategias del negocio.

El Plan de Administración de Recursos Humanos de TI se debe actualizar constantemente para cumplir con los cambiantes requerimientos del negocio.

2.4.1.7 PO9 Evaluar y Administrar los riesgos de TI

Tabla 2-13Resultado de evaluación del proceso PO9

PO9	**Evaluar y Administrar los Riesgos de TI**		
Nivel	Cumplimiento	Contribución	Valor
0	0,54	0,00	0,00
1	0,49	1,00	0,49
2	0,69	1,00	0,69
3	0,36	1,00	0,36
4	0,47	1,00	0,47
5	0,18	1,00	0,18
		Nivel de madurez =	**2,18**

Tabla 2-14Modelo de Madurez PO9

DOMINIO: PLANEACIÓN Y ORGANIZACIÓN
PO9: Evaluar y Administrar los riesgos de TI

NIVELES DE LOS MODELOS DE MADUREZ		CUMPLE	PARCIALMENTE	NO CUMPLE	OBSERVACIONES
NIVEL 0	La evaluación de riesgos para los procesos y las decisiones de negocio no ocurre. La organización no toma en cuenta los impactos enel negocio asociados a las vulnerabilidades de seguridad y a las incertidumbres del desarrollo de proyectos. La administración deriesgos no se ha identificado como algo relevante para adquirir soluciones de TI y para prestar servicios de TI.	X			
NIVEL 1	Los riesgos de TI se toman en cuenta de manera ad hoc. Se realizan evaluaciones informales de riesgos según lo determine cadaproyecto. En algunas ocasiones se identifican evaluaciones de riesgos en un plan de proyectos pero se asignan rara vez a gerentesespecíficos. Los riesgos específicos relacionados con TI tales como seguridad, disponibilidad e integridad se toman en cuentaocasionalmente proyecto porproyecto. Los riesgos relativos a TI que afectan las operaciones del día a día, son rara vez discutidas enreuniones gerenciales. Cuando se toman en cuenta los riesgos, la mitigación es inconsistente. Existe un entendimiento emergente deque los riesgos de TI son importantes y necesitan ser considerados.	X			
NIVEL 2	Existe un enfoque de evaluación de riesgos en desarrollo y se implementa a discreción de los gerentes de proyecto. La administración de riesgos se da por lo general a alto nivel y típicamente se aplica solo a proyectos grandes o como respuesta a problemas. Los procesos de mitigación de riesgos están empezando a ser implementados donde se identifican riesgos.	X			
NIVEL 3	Una política de administración de riesgos para toda la organización define cuándo y cómo realizar las evaluaciones de riesgos. La administración de riesgos sigue un proceso definido, el cual está documentado. El entrenamiento sobre administración de riesgosestá disponible para todo el personal. La decisión de seguir el proceso de administración de riesgos y de recibir entrenamiento sedeja a la discreción del individuo. La metodología para la evaluación de riesgos es convincente y sólida, y garantiza que los riesgosclaves para el negocio sean identificados. Un proceso para mitigar los riesgos clave por lo general se institucionaliza una vez que losriesgos se			X	

	identifican. Las descripciones de puestos consideran las responsabilidades de administración de riesgos.				
NIVEL 4	Una política de administración de riesgos para toda la organización define cuándo y cómo realizar las evaluaciones de riesgos. La administración de riesgos sigue un proceso definido, el cual está documentado. El entrenamiento sobre administración de riesgosestá disponible para todo el personal. La decisión de seguir el proceso de administración de riesgos y de recibir entrenamiento sedeja a la discreción del individuo. La metodología para la evaluación de riesgos es convincente y sólida, y garantiza que los riesgosclaves para el negocio sean identificados. Un proceso para mitigar los riesgos clave por lo general se institucionaliza una vez que losriesgos se identifican. Las descripciones de puestos consideran las responsabilidades de administración de riesgos.			**X**	
NIVEL 5	La administración de riesgos ha evolucionado al nivel en que un proceso estructurado está implantado en toda la organización y es bien administrado. Las buenas prácticas se aplican en toda la organización. La captura, análisis y reporte de los datos deadministración de riesgos están altamente automatizados. La orientación se toma de los líderes en el campo y la organización de TI participa en grupos de interés para intercambiar experiencias. La administración de riesgos está altamente integrada en todo elnegocio y en las operaciones de TI, está bien aceptada, y abarca a los usuarios de servicios de TI. La dirección detecta y actúa cuandose toman decisiones grandes de inversión o de operación de TI, sin considerar el plan de administración de riesgos. La direcciónevalúa las estrategias de mitigación de riesgos de manera continua.			**X**	

COBIT define para el proceso PO9 los siguientes objetivos de control:

1. Marco de Trabajo de Administración de Riesgos
2. Establecimiento del Contexto del Riesgo
3. Identificación de Eventos
4. Evaluación de Riesgos de TI
5. Respuesta a los Riesgos
6. Mantenimiento y Monitoreo de un Plan de Acción de Riesgos

El objetivo esencial de un modelo de madurez es ascender a un grado de madurez superior, por esto para que el proceso PO9ascienda a un grado de madurez 3, como estrategia a corto plazo y conforme lo establece COBIT:

Se recomienda que se implemente políticas y procedimientos formales para la Administración de Riesgos de toda la organización.

Asignar roles y responsables de cada proceso con el fin de que los riesgos del negocio sean identificados, evaluados y se obtenga soluciones inmediatas.

Como estrategia a largo plazo se recomienda que se tome en consideración los siguientes puntos:

Se recomienda que siga un proceso de Evaluación y Administración de Riesgos estandarizado.

Para la mitigación de riesgos es necesario monitorear y evaluar individualmente cada proyecto de manera continua.

2.4.1.8 PO10 Administrar Proyectos

Tabla 2-15Resultado de evaluación del proceso PO10

PO10	Administrar Proyectos		
Nivel	Cumplimiento	Contribución	Valor
0	0,66	0,00	0,00
1	0,63	1,00	0,63
2	0,70	1,00	0,70
3	0,79	1,00	0,79
4	0,61	1,00	0,61
5	0,61	1,00	0,61
		Nivel de madurez=	**3,35**

Tabla 2-16Modelo de Madurez PO10

DOMINIO: PLANEACIÓN Y ORGANIZACIÓN					
PO10: Administrar Proyectos					
NIVELES DE LOS MODELOS DE MADUREZ		CUMPLE	PARCIALMENTE	NO CUMPLE	OBSERVACIONES
NIVEL 0	Las técnicas de administración de proyectos no se usan y la organización no toma en cuenta los impactos al negocio asociados con lamala administración de los proyectos y con las fallas de desarrollo en el proyecto.	X			
NIVEL 1	El uso de técnicas y enfoques de administración de proyectos dentro de TI es una decisión individual que se deja a los gerentes de TI. Existe una carencia de compromiso por parte de la gerencia hacia la propiedad de proyectos y hacia la administración de proyectos. Las decisiones críticas sobre administración de proyectos se realizan sin la intervención de la gerencia usuaria ni del cliente. Hay poca o nula participación del cliente y del usuario para definir los proyectos de TI. No hay una organización clara dentro de TI para la administración de proyectos. Los roles y responsabilidades para la administración de proyectos no están definidas. Los proyectos, cronogramas y puntos clave están definidos pobremente, si es que lo están. No se hace seguimiento al tiempo y a los gastos del equipo del proyecto y no se comparan con el presupuesto	X			
NIVEL 2	La alta dirección ha obtenido y comunicado la conciencia de la necesidad de la administración de los proyectos de TI. La organización está en proceso de desarrollar y utilizar algunas técnicas y métodos proyecto por proyecto. Los proyectos de TI han definido objetivos técnicos y de negocio de manera informal. Hay participación limitada de los interesados en la administración de los proyectos de TI. Las directrices iniciales se han elaborado para muchos aspectos de la administración de proyectos. La aplicación a proyectos de las directrices administrativas se deja a discreción de cada gerente de proyecto.	X			

NIVEL 3	El proceso y la metodología de administración de proyectos de TI han sido establecidos y comunicados. Los proyectos de TI se definen con los objetivos técnicos y de negocio adecuados. La alta dirección del negocio y de TI, empiezan a comprometerse y a participar en la administración de los proyectos de TI. Se ha establecido una oficina de administración de proyectos dentro de TI, con roles yresponsabilidades iniciales definidas. Los proyectos de TI se monitorean, con puntos clave, cronogramas y mediciones de presupuesto y desempeño definidos y actualizados. Existe entrenamiento para la administración de proyectos. El entrenamiento enadministración de proyectos es un resultado principalmente de las iniciativas individuales del equipo. Los procedimientos deaseguramiento de calidad y las actividades de implantación post-sistema han sido definidos, pero no se aplican de manera amplia porparte de los gerentes de TI. Los proyectos se empiezan a administrar como portafolios.		**X**		**Objetivos no cumplidos:** En la administración de proyectos se hace un seguimiento que se cumpla con los objetivos esperados en tiempo, pero no en presupuesto. No se ha establecido una oficina de Administración de Proyectos de TI, con roles y responsabilidades definidas.
NIVEL 4	La gerencia requiere que se revisen métricas y lecciones aprendidas estandarizadas y formales después de terminar cada proyecto. La administración de proyectos se mide y evalúa a través de la organización y no sólo en TI. Las mejoras al proceso de administración de proyectos se formalizan y comunican y los miembros del equipo reciben entrenamiento sobre estas mejoras. La gerencia de TI implementa una estructura organizacional de proyectos con roles, responsabilidades y criterios de desempeño documentados. Los criterios para evaluar el éxito en cada punto clave se han establecido. El valor y el riesgo se miden y se administran, antes, durante y al final de los proyectos. Cada vez más, los proyectos abordan las metas organizacionales, en lugar de abordar solamente lasespecíficas a TI. Existe un apoyo fuerte y activo a los proyectos por parte de los patrocinadores de la alta dirección, así como de losinteresados. El entrenamiento relevante sobre administración de proyectos se planea para el equipo en la oficina de proyectos y a lolargo de la función de TI.			**X**	
NIVEL 5	Se encuentra implantada una metodología comprobada de ciclo de vida de proyectos, la cual se refuerza y se integra en la cultura de la organización completa. Se ha implantado una iniciativa continua para identificar e institucionalizar las mejores prácticas de administración de proyectos. Se ha definido e implantado una estrategia de TI para contratar el desarrollo y los proyectos operativos. Una oficina de administración de proyectos integrada es responsable de los proyectos y			**X**	

	programas desde su concepción hasta su post-implantación. La planeación de programas y proyectos en toda la organización garantiza que los recursos de TI y del usuario se utilizan de la mejor manera para apoyar las iniciativas estratégicas.				

COBIT define para el proceso PO10 los siguientes objetivos de control:

1. Marco de Trabajo para la Administración de Programas
2. Marco de Trabajo para la Administración de Proyectos
3. Enfoque de Administración de Proyectos
4. Compromiso de los Interesados
5. Declaración de Alcance del Proyecto
6. Inicio de las Fases del Proyecto
7. Plan Integrado del Proyecto
8. Recursos del Proyecto
9. Administración de Riesgos del Proyecto
10. Plan de Calidad del Proyecto
11. Control de Cambios del Proyecto
12. Planeación del Proyecto y Métodos de Aseguramiento
13. Medición del Desempeño, Reporte y Monitoreo del Proyecto
14. Cierre del Proyecto

El objetivo esencial de un modelo de madurez es ascender a un grado de madurez superior, por esto para que el proceso PO10ascienda a un grado de madurez 4, como estrategia a corto plazo y conforme lo establece COBIT:

Se recomienda que se establezca una oficina de Administración de Proyectos dentro de TI con roles y responsabilidadessobre los proyectos y programas desde su inicio hasta después de su implementación.

Los proyectos necesitan ser monitoreados en puntos clave y se debe considerar métricas para verificar su cumplimiento.

La administración de proyectos debe ser evaluada por la organización, no únicamente por TI.

Como estrategia a largo plazo se recomienda que se tome en consideración los siguientes puntos:

Se recomienda que se implemente una metodología para el ciclo de vida de los proyectos con la finalidad de que se maneje las mejores prácticas para la Administración de Proyectos y de esta forma se pueda garantizar que los recursos de TI y del usuario son optimizados.

2.4.2 PROCESOS DEL DOMINIO DE ADQUIRIR E IMPLEMENTAR

2.4.2.1 AI2 Adquirir y mantener el software aplicativo

Tabla 2-17Resultado de evaluación del proceso AI2

AI2	Adquirir y Mantener Software Aplicativo		
Nivel	Cumplimiento	Contribución	Valor
0	1,00	0,00	0,00
1	0,89	1,00	0,89
2	0,92	1,00	0,92
3	0,94	1,00	0,94
4	0,78	1,00	0,78
5	0,57	1,00	0,57
		Nivel de madurez =	**4,10**

Tabla 2-18 Modelo de Madurez AI2

DOMINIO: ADQUIRIR E IMPLEMENTAR					
AI2: Adquirir y mantener el software aplicativo					
NIVELES DE LOS MODELOS DE MADUREZ		CUMPLE	PARCIALMENTE	NO CUMPLE	OBSERVACIONES
NIVEL 0	No existe un proceso de diseño y especificación de aplicaciones. Típicamente, las aplicaciones se obtienen con base en ofertas deproveedores, en el reconocimiento de la marca o en la familiaridad del personal de TI con productos específicos, considerando poco onada los requerimientos actuales.	X			
NIVEL 1	Existe conciencia de la necesidad de contar con un proceso de adquisición y mantenimiento de aplicaciones. Los enfoques para laadquisición y mantenimientos de software aplicativo varían de un proyecto a otro. Es probable que se hayan adquirido en forma independiente una variedad de soluciones individuales para requerimientos particulares del negocio, teniendo como resultadoineficiencias en elmantenimiento y soporte. Se tiene poca consideración hacia la seguridad y disponibilidad de la aplicación en el diseño o adquisición de softwareaplicativo.	X			
NIVEL 2	Existen procesos de adquisición y mantenimiento de aplicaciones, con diferencias pero similares, en base a la experiencia dentro dela operación de TI. El mantenimiento es a menudo problemático y se resiente cuando se pierde el conocimiento interno de la organización. Se tiene poca consideración hacia la seguridad y disponibilidad de la aplicación en el diseño o adquisición de softwareaplicativo	X			
NIVEL 3	Existe un proceso claro, definido y de comprensión general para la adquisición y mantenimiento de software aplicativo. Este procesova de acuerdo con la estrategia de TI y del negocio. Se intenta aplicar los procesos de manera consistente a través de diferentes aplicaciones y proyectos. Las metodologías son por lo general, inflexibles y difíciles de aplicar en todos los casos, por lo que es muyprobable que se salten pasos. Las actividades de	X			

	mantenimiento se planean, programan y coordinan.				
NIVEL 4	Existe una metodología formal y bien comprendida que incluye un proceso de diseño y especificación, un criterio de adquisición, unproceso de prueba y requerimientos para la documentación. Existen mecanismos de aprobación documentados y acordados, para garantizar que se sigan todos los pasos y se autoricen las excepciones. Han evolucionado prácticas y procedimientos para ajustarlos ala medida de la organización, los utilizan todo el personal y son apropiados para la mayoría de los requerimientos de aplicación.	**X**			
NIVEL 5	Las prácticas de adquisición ymantenimiento de software aplicativo se alinean con el proceso definido. El enfoque es con base encomponentes, con aplicaciones predefinidas y estandarizadas que corresponden a las necesidades del negocio. El enfoque se extiende para toda la empresa. La metodología de adquisición y mantenimiento presenta un buen avance y permite unposicionamiento estratégico rápido, que permite un alto grado de reacción y flexibilidad para responder a requerimientos cambiantesdel negocio. La metodología de adquisición e implantación de software aplicativo ha sido sujeta a mejora continua y se soporta conbases de datos internas y externas que contienen materiales de referencia y las mejores prácticas. La metodología producedocumentación dentro de una estructura predefinida que hace eficiente la producción y mantenimiento.			**X**	

COBIT define para el proceso AI2 los siguientes objetivos de control:

1. Diseño de Alto Nivel
2. Diseño Detallado
3. Control y Posibilidad de Auditar las Aplicaciones
4. Seguridad y Disponibilidad de las Aplicaciones
5. Configuración e Implantación de Software Aplicativo Adquirido
6. Actualizaciones Importantes en Sistemas Existentes
7. Desarrollo de Software Aplicativo
8. Aseguramiento de la Calidad del Software

9. Administración de los Requerimientos de Aplicaciones
10. Mantenimiento de Software Aplicativo

El objetivo esencial de un modelo de madurez es ascender a un grado de madurez superior, por esto para que el proceso AI2ascienda a un grado de madurez 5, como estrategia a corto plazo y conforme lo establece COBIT:

Se recomienda que las prácticas de adquisición y software aplicativo se extiendan para toda la empresa.

También se recomienda que la metodología de adquisición y mantenimiento sea reforzada para que se tenga un posicionamiento estratégico inmediato.

Como estrategia a largo plazo se recomienda que se tome en consideración lo siguiente:

Se recomienda que el proceso se mantenga en mejora continua con la finalidad de que soporte requerimientos cambiantes del negocio sin problema.

2.4.2.2 AI3Adquirir y mantener la infraestructura tecnológica

Tabla 2-19Resultado de evaluación del proceso AI3

AI3	**Adquirir y Mantener Infraestructura Tecnológica**		
Nivel	Cumplimiento	Contribución	Valor
0	0,66	0,00	0,00
1	0,74	1,00	0,74
2	0,87	1,00	0,87
3	0,68	1,00	0,68
4	0,76	1,00	0,76
5	0,34	1,00	0,34
	Nivel de madurez =		**3,38**

Tabla 2-20Modelo de Madurez AI3

DOMINIO:ADQUIRIR E IMPLEMENTAR					
AI3: Adquirir y mantener la infraestructura tecnológica					
NIVELES DE LOS MODELOS DE MADUREZ		CUMPLE	PARCIALMENTE	NO CUMPLE	OBSERVACIONES
NIVEL 0	No se reconoce la administración de la infraestructura de tecnología como un asunto importante al cual deba ser resuelto.	X			
NIVEL 1	Se realizan cambios a la infraestructura para cada nueva aplicación, sin ningún plan en conjunto. Aunque se tiene la percepción deque la infraestructura de TI es importante, no existe un enfoque general consistente. La actividad de mantenimiento reacciona anecesidades de corto plazo. El ambiente de producción es el ambiente de prueba.	X			
NIVEL 2	No hay consistencia entre enfoques tácticos al adquirir y dar mantenimiento a la infraestructura de TI. La adquisición y mantenimientode la infraestructura de TI no se basa en una estrategia definida y no considera las necesidades de las aplicaciones del negocio quese deben respaldar. Se tiene la noción de que la infraestructura de TI es importante, que se apoya en algunas prácticas formales. Algunos mantenimientos se programan, pero no se programa ni se coordina en su totalidad. Para algunos ambientes, existe unambiente de prueba por separado.	X			
NIVEL 3	Existe un claro, definido y generalmente entendido proceso para adquirir y dar mantenimiento a la infraestructura TI. El procesorespalda las necesidades de las aplicaciones críticas del negocio y concuerda con la estrategia de negocio de TI, pero no se aplica enforma consistente. Se planea, programa y coordina el mantenimiento. Existen ambientes separados para prueba y producción.	X			
NIVEL 4	Se desarrolla el proceso de adquisición y mantenimiento de la infraestructura de tecnología a tal punto que funciona bien para lamayoría de las situaciones, se le da un seguimiento consistente y un enfoque hacia la reutilización. La infraestructura de TI soportaadecuadamente lasaplicaciones del negocio. El proceso está bien organizado y es preventivo. Tanto el costo			X	

	como el tiempo derealización para alcanzar el nivel esperado de escalamiento, flexibilidad e integración se han optimizado parcialmente.				
NIVEL 5	El proceso de adquisición y mantenimiento de la infraestructura de tecnología es preventivo y está estrechamente en línea con lasaplicaciones críticas del negocio y con la arquitectura de la tecnología. Se siguen buenas prácticas respecto a las soluciones detecnología, y la organización tiene conciencia de las últimas plataformas desarrolladas y herramientas de administración. Se reducencostos al racionalizar y estandarizar loscomponentes de la infraestructura y con el uso de la automatización. Con un alto nivel deconciencia se pueden identificar los medios óptimos para mejorar eldesempeño en forma preventiva, incluyendo el considerar laopción de contratar servicios externos. La infraestructura de TI se entiende como el apoyo clave para impulsar el uso de TI.			**X**	

COBIT define para el proceso AI3 los siguientes objetivos de control:

1. Plan de Adquisición de Infraestructura Tecnológica
2. Protección y Disponibilidad del Recurso de Infraestructura
3. Mantenimiento de la Infraestructura
4. Ambiente de Prueba de Factibilidad

El objetivo esencial de un modelo de madurez es ascender a un grado de madurez superior, por esto para que el proceso AI3ascienda a un grado de madurez 4, como estrategia a corto plazo y conforme lo establece COBIT:

Se recomienda que se implemente un Plan de Adquisición y Mantenimiento de la Infraestructura de TI, donde se justifique el dimensionamiento de la arquitectura para el mejor aprovechamiento de los recursos adquiridos y disponibles.

Es necesario que el proceso esté bien organizado y llegue a ser proactivo.

Como estrategia a largo plazo se recomienda que se tome en consideración los siguientes puntos:

El proceso deAdquisición y Mantenimiento de la Infraestructura de TI este alineado con las aplicaciones críticas del negocio y la infraestructura tecnológica.

Se recomienda se implemente políticas y procedimientos que especifiquen que la Infraestructura de TI es un apoyo clave para el uso de TI dentro de la empresa.

2.4.2.3 AI4 Facilitar la operación y el uso

Tabla 2-21Resultado de evaluación del proceso AI4

AI4	Facilitar la Operación y el Uso		
Nivel	Cumplimiento	Contribución	Valor
0	0,81	0,00	0,00
1	0,57	1,00	0,57
2	0,60	1,00	0,60
3	0,65	1,00	0,65
4	0,49	1,00	0,49
5	0,16	1,00	0,16
		Nivel de madurez =	**2,46**

Tabla 2-22Modelo de Madurez AI4

DOMINIO: ADQUIRIR E IMPLEMENTAR					
AI4: Facilitar la operación y el uso					
NIVELES DE LOS MODELOS DE MADUREZ		CUMPLE	PARCIALMENTE	NO CUMPLE	OBSERVACIONES
NIVEL 0	No existe el proceso con respecto a la producción de documentación de usuario, manuales de operación y material de entrenamiento. Los únicos materiales existentes son aquellos que se suministran con los productos que se adquieren.	X			
NIVEL 1	Existe la percepción de que la documentación de proceso es necesaria. La documentación se genera ocasionalmente y se distribuyeen forma desigual a grupos limitados. Mucha de la documentación y muchos de los procedimientos ya caducaron. Los materiales deentrenamiento tienden a ser esquemas únicos con calidadvariable. Virtualmente no existen procedimientos	X			

	de integración a través de los diferentes sistemas y unidades de negocio. No hay aportes de las unidades de negocio en el diseño de programas de entrenamiento.				
NIVEL 2	Se utilizan enfoques similares para generar procedimientos y documentación, pero no se basan en un enfoque estructural o marco detrabajo. No hay un enfoque uniforme para el desarrollo de procedimientos de usuario y deoperación. Individuos o equipos de proyecto generan los materiales de entrenamiento, y la calidad depende de los individuos que se involucran. Los procedimientos y lacalidad del soporte al usuario van desde pobre a muy buena, con una consistencia e integración muy pequeña a lo largo de laorganización. Se proporcionan o facilitan programas de entrenamiento para el negocio y los usuarios, pero no hay un plan general para ofrecer o dar entrenamiento.	**X**			
NIVEL 3	Existe un esquema bien definido, aceptado y comprendido para documentación del usuario, manuales de operación y materiales deentrenamiento. Se guardan y se mantienen los procedimientos en una biblioteca formal y cualquiera que necesite saber tiene accesoa ella. Las correcciones a la documentación y a los procedimientos se realizan por reacción. Los procedimientos se encuentrandisponibles fuera de línea y se pueden acceder y mantener en caso de desastre. Existe un proceso que especifica las actualizacionesde procedimientos y los materiales de entrenamiento para que sea un entregable explícito de un proyecto de cambio. A pesar de laexistencia de enfoques definidos, el contenido actual varía debido a que no hay un control para reforzar el cumplimiento deestándares. Los usuarios se involucran en los procesos informalmente. Cada vez se utilizan más herramientas automatizadas en lageneración y distribución de procedimientos. Se planea y programa tanto el entrenamiento del negocio como de los usuario.			**X**	
NIVEL 4	Existe un esquema definido para los procedimientos de mantenimiento y para los materiales de entrenamiento que cuentan con elsoporte de laadministración de TI. El enfoque considerado para los procedimientos de mantenimiento y los manuales de entrenamiento cubren todos los sistemas			**X**	

	y las unidades de negocio, de manera que se pueden observar los procesos desde unaperspectiva de negocio. Los procedimientos y materiales de entrenamiento se integran para que contengan interdependencias e interfaces. Existen controles para garantizar que se adhieren losestándares y que se desarrollan y mantienen procedimientos para todos los procesos. La retroalimentación del negocio y del usuario sobre la documentación y el entrenamiento se recopila y evalúacomo parte de un proceso continuo de mejora. Los materiales de documentación y entrenamiento se encuentran generalmente a unbuen nivel, predecible, de confiabilidad y disponibilidad. Se implanta un proceso emergente para el uso de documentación yadministración automatizada de procedimiento. El desarrollo automatizado deprocedimientos se integra cada vez más con eldesarrollo de sistemas aplicativos, facilitando la consistencia y el acceso al usuario. El entrenamiento de negocio y usuario essensible a las necesidades del negocio. La administración de TI está desarrollando medidas para el desarrollo y la entrega dedocumentación,materiales y programas deentrenamiento.				
NIVEL 5	El proceso para la documentación de usuario y de operación se mejora constantemente con la adopción de nuevas herramientas ométodos. Los materiales de procedimiento y de entrenamiento se tratan como una base de conocimiento en evolución constante quese mantiene en forma electrónica, con el uso de administración de conocimiento actualizada, flujo de trabajo y tecnologías dedistribución, que los hacen accesibles y fáciles de mantener. El material de documentación y entrenamiento se actualiza para reflejar los cambios en la organización, en la operación y en el software. Tanto el desarrollo de materiales dedocumentación y entrenamiento como la entrega de programas de entrenamiento, se encuentran completamente integrados con el negocio y con las definiciones deproceso del negocio, siendo así un apoyo a los requerimientos de toda la organización y no tan sólo procedimientos orientados a TI.			**X**	

COBIT define para el proceso AI4 los siguientes objetivos de control:

1. Plan para Soluciones de Operación
2. Transferencia de Conocimiento a la Gerencia del Negocio
3. Transferencia de Conocimiento a Usuarios Finales
4. Transferencia de Conocimiento al Personal de Operaciones y Soporte

El objetivo esencial de un modelo de madurez es ascender a un grado de madurez superior, por esto para que el proceso AI4ascienda a un grado de madurez 3, como estrategia a corto plazo y conforme lo establece COBIT:

Se recomienda que se implemente un proceso donde se detalle actualizaciones de procedimientos y material de entrenamiento.

También es necesario se revise la documentación y los procedimientos con el fin de ser proactivos ante errores o problemas que puedan presentarse.

Como estrategia a largo plazo se recomienda que se tome en consideración los siguientes puntos:

Se recomienda que todos los procedimientos ya sea de mantenimiento o entrenamiento estén bien documentados para todos los sistemas y unidades del negocio.

La documentación debe estar a un buen nivel, de tal manera que sea predecible, confiable y disponible.

Se debe determinar controles y estándares para todos los procedimientos.

2.4.2.4 AI5 Adquirir recursos de TI

Tabla 2-23Resultado de evaluación del proceso AI5

AI5	Adquirir Recursos de TI

Nivel	Cumplimiento	Contribución	Valor
0	1,00	0,00	0,00
1	0,70	1,00	0,70
2	0,95	1,00	0,95
3	0,90	1,00	0,90
4	0,69	1,00	0,69
5	0,34	1,00	0,34

Nivel de madurez=	**3,59**

Tabla 2-24Modelo de Madurez AI5

DOMINIO:ADQUIRIR E IMPLEMENTAR					
AI5: Adquirir recursos de TI					
NIVELES DE LOS MODELOS DE MADUREZ		CUMPLE	PARCIALMENTE	NO CUMPLE	OBSERVACIONES
NIVEL 0	No existe un proceso definido de adquisición de recursos de TI. La organización no reconoce la necesidad de tener políticas yprocedimientos claros de adquisición para garantizar que todos los recursos de TI se encuentren disponibles y de forma oportuna yrentable.	X			
NIVEL 1	La organización ha reconocido la necesidad de tener políticas y procedimientos documentados que enlacen la adquisición de TI con el proceso general de adquisiciones de la organización. Los contratos para la adquisición de recursos de TI son elaborados yadministrados por gerentes de proyecto y otras personas que ejercen su juicio profesional más que seguir resultados deprocedimientos y políticas formales. Sólo existe un relación ad hoc entre los procesos de administración de adquisiciones y contratoscorporativos y TI. Los contratos de adquisición se administran a la terminación de los proyectos más que sobre una base continua.	X			

NIVEL 2	Existe conciencia organizacional de la necesidad de tener políticas y procedimientos básicos para la adquisición de TI. Las políticas y procedimientos se integran parcialmente con el proceso general de adquisición de la organización del negocio. Los procesos deadquisición se utilizan principalmente en proyectos mayores y bastante visibles. Se determinan responsabilidades y rendición decuentas para la administración de adquisición y contrato de TI según la experiencia particular del gerente de contrato. Se reconoce la importancia de administrar proveedores y las relaciones con ellos, pero se manejan con base en la iniciativa individual. Los procesosde contrato se utilizan principalmente en proyectos mayores o muy visibles.	**X**			
NIVEL 3	La administración establece políticas y procedimientos para la adquisición de TI. Las políticas y procedimientos toman como guía elproceso general de adquisición de la organización. La adquisición de TI se integra en gran parte con los sistemas generales deadquisición del negocio. Existen estándares de TI para la adquisición de recursos de TI. Los proveedores de recursos de TI se integrandentro de los mecanismos deadministración de proyectos de la organización desde una perspectiva de administración de contratos. La administración de TI comunica la necesidad de contar con una administración adecuada de adquisiciones y contratos en toda lafunción de TI.	**X**			
NIVEL 4	La adquisición de TI se integra totalmente con los sistemas generales de adquisición de la organización. Se utilizan los estándarespara la adquisición de recursos de TI en todos los procesos de adquisición. Se toman medidas para la administración de contratos y adquisiciones relevantes para los casos de negocio que requieran la adquisición de TI. Se dispone de reportes que sustentan losobjetivos de negocio. La administración está consciente por lo general, de las excepciones a las políticas y procedimientos para laadquisición de TI. Se está desarrollando unaadministración estratégica de relaciones. La administración de TI implanta el uso de procesos de administración para adquisición y contratos en todas las adquisiciones mediante la revisión de medición al desempeño		**X**		**Objetivos no cumplidos:** No se encuentra bien definida una Administración estratégica de relaciones.

NIVEL 5	La administración instituye y da recursos a procesos exhaustivos para la adquisición de TI. La administración impulsa el cumplimientode las políticas y procedimientos de adquisición de TI. Se toman las medidas en la administración de contratos y adquisiciones,relevantes en casos de negocio para adquisición de TI. Se establecen buenas relaciones con el tiempo con la mayoría de losproveedores y socios, y se mide y vigila la calidad de estas relaciones. Se manejan las relaciones en forma estratégica. Losestándares, políticas y procedimientos de TI para la adquisición de recursos TI se manejanestratégicamente y responden a lamedición del proceso. La administración de TI comunica la importancia estratégica de tener una administración apropiada de adquisiciones y contratos, a través de la función TI.			**X**	

COBIT define para el proceso AI5 los siguientes objetivos de control:

1. Control de Adquisición
2. Administración de Contratos con Proveedores
3. Selección de Proveedores
4. Adquisición de Recursos de TI

El objetivo esencial de un modelo de madurez es ascender a un grado de madurez superior, por esto para que el proceso AI5ascienda a un grado de madurez 5, como estrategia a corto plazo y conforme lo establece COBIT:

Se recomienda que se realicen reportes de los objetivos del negocio.

Cumplir y reforzar los estándares, políticas y procedimientos de adquisición de recursos de TI de manera continua.

Como estrategia a largo plazo se recomienda que se tome en consideración los siguientes puntos:

Se recomienda que exista una mejora continua en la administración de adquisiciones y contratos.

Manejar buenas relaciones estratégicas con los proveedores.

2.4.3 PROCESOS DEL DOMINIO DE ENTREGAR Y DAR SOPORTE

2.4.3.1 DS1 Definir y administrar niveles de servicio

Tabla 2-25Resultado de evaluación del proceso DS1

DS1	Definir y Administrar los Niveles de Servicio

Nivel	Cumplimiento	Contribución	Valor
0	1,00	0,00	0,00
1	0,59	1,00	0,59
2	0,38	1,00	0,38
3	0,32	1,00	0,32
4	0,51	1,00	0,51
5	0,29	1,00	0,29

Nivel de madurez =	**2,10**

Tabla 2-26 Modelo de Madurez DS1

DOMINIO: ENTREGAR Y DAR SOPORTE					
DS1: Definir y Administrar Niveles de Servicio					
	NIVELES DE LOS MODELOS DE MADUREZ	CUMPLE	PARCIALMENTE	NO CUMPLE	OBSERVACIONES
NIVEL 0	La gerencia no reconoce la necesidad de un proceso para definir los niveles de servicio. La responsabilidad y la rendición de cuentas sobre el monitoreo no está asignada.	X			
NIVEL 1	Hay conciencia de la necesidad de administrar los niveles de servicio, pero el proceso es informal y reactivo. La responsabilidad y la rendición de cuentas sobre para la definición y laadministración de servicios no está definida. Si existen las medidas para medir el desempeño son solamente cualitativas con metas definidas de forma imprecisa. La notificación es informal, infrecuente e inconsistente.	X			

NIVEL 2	Los niveles de servicio están acordados pero son informales y no están revisados. Los reportes de los niveles de servicio estánincompletos y pueden ser irrelevantes o engañosos para los clientes. Los reportes de los niveles de servicio dependen, en formaindividual, de las habilidades y la iniciativa de los administradores. Está designado un coordinador de niveles de servicio con responsabilidades definidas, pero con autoridad limitada. Si existe un proceso para el cumplimiento de los acuerdos de niveles deservicio es voluntario y no está implementado.		**X**		**Objetivos no cumplidos:** En la Empresa no se ha asignado un coordinador para los niveles de servicio, con responsabilidades definidas.
NIVEL 3	Las responsabilidades están bien definidas pero con autoridad discrecional. El proceso de desarrollo del acuerdo de niveles deservicio está en orden y cuenta con puntos de control para revalorar los niveles de servicio y la satisfacción de cliente. Los servicios ylos niveles de servicio están definidos, documentados y se ha acordado utilizar un proceso estándar. Las deficiencias en los nivelesde servicio están identificadas pero los procedimientos para resolver las deficiencias son informales. Hay un claro vínculo entre el cumplimiento del nivel de servicio esperado y el presupuesto contemplado. Los niveles de servicio están acordados pero pueden noresponder a las necesidades del negocio.			**X**	
NIVEL 4	Aumenta la definición de los niveles de servicio en la fase de definición de requerimientos del sistema y se incorporan en el diseño dela aplicación y de los ambientes de operación. La satisfacción del cliente es medida y valorada de forma rutinaria. Las medidas dedesempeño reflejan las necesidades del cliente, en lugar de las metas de TI. Las medidas para la valoración de los niveles de serviciose vuelven estandarizadas y reflejan los estándares de la industria. Los criterios para la definición de los niveles de servicio están basados en la criticidad del negocio e incluyen consideraciones de disponibilidad, confiabilidad, desempeño, capacidad decrecimiento, soporte al usuario, planeación de continuidad y seguridad. Cuando no se cumplen los niveles de servicio, se llevan acabos análisis causa-raíz de manera rutinaria. El proceso de reporte para monitorear los niveles de servicio se vuelve cada vez más automatizado. Los riesgos operativos y financieros asociados con la falta de cumplimiento de los niveles de servicio, están definidos yse entienden claramente. Se implementa y mantiene un sistema formal de medición de los KPIs y los KGIs.			**X**	

NIVEL 5	Los niveles de servicio son continuamente reevaluados para asegurar la alineación de TI y los objetivos del negocio, mientras se toma ventaja de la tecnología incluyendo le relación costo-beneficio. Todos los procesos de administración de niveles de servicio están sujetos a mejora continua. Los niveles de satisfacción del cliente son administrados y monitoreados de manera continua. Los niveles de servicio esperados reflejan metas estratégicas de las unidades de negocio y son evaluadas contra las normas de la industria. Laadministración de TI tiene los recursos y la asignación de responsabilidades necesarias para cumplir con los objetivos de niveles deservicio y la compensación está estructurada para brindar incentivos por cumplir con dichos objetivos. La alta gerencia monitorea losKPIs y los KGIs como parte de un proceso de mejora continua.			**X**	

COBIT define para el proceso DS1 los siguientes objetivos de control:

1. Marco de Trabajo de la Administración de los Niveles de Servicio
2. Definición de Servicios
3. Acuerdos de Niveles de Servicio
4. Acuerdos de Niveles de Operación
5. Monitoreo y Reporte del Cumplimento de los Niveles de Servicio
6. Revisión delos Acuerdos de Niveles de Servicio y delos Contratos

El objetivo esencial de un modelo de madurez es ascender a un grado de madurez superior, por esto para que el proceso DS1ascienda a un grado de madurez 3, como estrategia a corto plazo y conforme lo establece COBIT:

Se recomienda que se asigne un responsable para los niveles de servicio, con la finalidad de que se establezcan puntos de control para el cumplimiento de los mismos y de esta forma también satisfacer a los clientes.

Definir y documentar los niveles de servicio que se utilizarán a través de un proceso estándar.

Como estrategia a largo plazo se recomienda que se tome en consideración lo siguiente:

Se recomienda que para la administración de niveles de servicio las medidas tomadas se vayan estandarizando y se mantengan en mejora continua, teniendo en consideración que se incluya disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, soporte al usuario, planeación de continuidad y seguridad.

2.4.3.2 DS5 Garantizar la seguridad de los sistemas

Tabla 2-27Resultado de evaluación del proceso DS5

DS5	Garantizar la Seguridad de los Sistemas

Nivel	Cumplimiento	Contribución	Valor
0	0,68	0,00	0,00
1	0,74	1,00	0,74
2	0,58	1,00	0,58
3	0,70	1,00	0,70
4	0,56	1,00	0,56
5	0,27	1,00	0,27

Nivel de madurez =	**2,85**

Tabla 2-28 Modelo de Madurez DS5

DOMINIO: ENTREGAR Y DAR SOPORTE					
DS5: Garantizar la seguridad de los sistemas					
	NIVELES DE LOS MODELOS DE MADUREZ	CUMPLE	PARCIALMENTE	NO CUMPLE	OBSERVACIONES
NIVEL 0	La organización no reconoce la necesidad de la seguridad para TI. Las responsabilidades y la rendición de cuentas no estánasignadas para garantizar la seguridad. Las medidas para soportar la administrar la seguridad de TI no están implementadas. No hayreportes de seguridad de TI ni un proceso de respuesta para resolver brechas de seguridad de TI. Hay una total falta de procesosreconocibles de administración de seguridad de sistemas.	X			

NIVEL 1	La organización reconoce la necesidad de seguridad para TI. La conciencia de la necesidad de seguridad dependeprincipalmente delindividuo. La seguridad de TI se lleva a cabo de forma reactiva. No se mide la seguridad de TI. Las brechas de seguridad de TIocasionan respuestas con acusaciones personales, debido a que las responsabilidades no son claras. Las respuestas a las brechas de seguridad de TI son impredecibles.	**X**			
NIVEL 2	Las responsabilidades y la rendición de cuentas sobre la seguridad, están asignadas a un coordinador de seguridad de TI, pero la autoridad gerencial del coordinador es limitada. La conciencia sobre la necesidad de la seguridad esta fraccionada y limitada. Aunque los sistemas producen información relevante respecto a la seguridad, ésta no se analiza. Los servicios de terceros pueden no cumplir con los requerimientos específicos de seguridad de la empresa. Las políticas de seguridad se han estado desarrollando, pero lasherramientas y las habilidades son inadecuadas. Los reportes de la seguridad de TI son incompletos, engañosos o no aplicables. Elentrenamiento sobre seguridad está disponible pero depende principalmente de la iniciativa del individuo. La seguridad de TI es vistaprimordialmente como responsabilidad y disciplina de TI, y el negocio no ve la seguridad de TI como parte de su propia disciplina.	**X**			
NIVEL 3	Existe conciencia sobre la seguridad y ésta es promovida por la gerencia. Los procedimientos de seguridad de TI están definidos yalineados con la política de seguridad de TI. Las responsabilidades de la seguridad de TI están asignadas y entendidas, pero nocontinuamente implementadas. Existe un plan de seguridad de TI y existen soluciones de seguridad motivadas por un análisis deriesgo. Los reportes no contienen un enfoque claro de negocio. Se realizan pruebas de seguridad adecuadas (por ejemplo, pruebascontra intrusos). Existe entrenamiento en seguridad para TI y para el negocio, pero se programa y se comunica de manera informal.		**X**		**Objetivos no cumplidos:** No existe formalmente un Plan de Seguridad de TI, se necesita reforzar las políticas y procedimientos, asignación de responsables para mejorar este proceso.
NIVEL 4	Las responsabilidades sobre la seguridad de TI son asignadas, administradas e implementadas de forma clara. Regularmente se llevaa cabo un análisis de impacto y de riesgos de seguridad. Las políticas y prácticas de seguridad se complementan con referencias de seguridad específicas. El contacto con métodos para promover la conciencia de la seguridad es obligatorio. La identificación,autenticación y autorización de los usuarios estáestandarizada. La certificación en seguridad es buscada por parte del personal quees responsable de la auditoría y la administración de la seguridad.			**X**	

	Las pruebas de seguridad se hacen utilizando procesos estándaresy formales que llevan a mejorar los niveles de seguridad. Los procesos de seguridad de TI están coordinados con la función deseguridad de toda la organización. Los reportes de seguridad están ligados con los objetivos del negocio. El entrenamiento sobreseguridad se imparte tanto para TI como para el negocio. El entrenamiento sobre seguridad de TI se planea y se administra demanera que responda a las necesidades del negocio y a los perfiles de riesgo de seguridad. Los KGIs y KPIs ya están definidos perono se miden aún.				
NIVEL 5	La seguridad en TI es una responsabilidad conjunta del negocio y de la gerencia de TI y está integrada con los objetivos de seguridad del negocio en la corporación. Los requerimientos de seguridad de TI están definidos de forma clara, optimizados e incluidos en unplan de seguridad aprobado. Los usuarios y los clientes se responsabilizan cada vez más de definir requerimientos de seguridad, y lasfunciones de seguridad están integradas con las aplicaciones en la fase de diseño. Los incidentes de seguridad son atendidos deforma inmediata con procedimientos formales de respuesta soportados por herramientas automatizadas. Se llevan a cabovaloraciones de seguridad de forma periódica para evaluar la efectividad de la implementación del plan de seguridad. La informaciónsobre amenazas y vulnerabilidades se recolecta y analiza de manera sistemática. Se recolectan e implementan de forma oportunacontroles adecuados para mitigar riesgos. Se llevan a cabo pruebas de seguridad, análisis de causa-efecto e identificación pro-activade riesgos para la mejora continua de procesos. Los procesos de seguridad y la tecnología están integrados a lo largo de toda laorganización. Los KGIs y KPIs para administración de seguridad son recopilados y comunicados. La gerencia utiliza los KGIs y KPIspara ajustar el plan de seguridad en un proceso de mejora continua			**X**	

COBIT define para el proceso DS5 los siguientes objetivos de control:

1. Administración de la Seguridad de TI
2. Plan de Seguridad de TI
3. Administración de Identidad
4. Administración de Cuentas del Usuario

5. Pruebas, Vigilancia y Monitoreo de la Seguridad
6. Definición de Incidente de Seguridad
7. Protección de la Tecnología de Seguridad
8. Administración de Llaves Criptográficas
9. Prevención, Detección y Corrección de Software Malicioso
10. Seguridad de la Red
11. Intercambio de Datos Sensitivos

El objetivo esencial de un modelo de madurez es ascender a un grado de madurez superior, por esto para que el proceso DS5ascienda a un grado de madurez 4, como estrategia a corto plazo y conforme lo establece COBIT:

Se recomienda que se implemente un Plan de Seguridad de TI, donde se asigne responsables para su cumplimiento.

Realizar periódicamente unanálisisde impacto y de riesgos de seguridad de TI.

Aplicar pruebas de seguridad con el fin de encontrar y solucionar posibles problemas.

Evaluar regularmente la implementación del Plan de Seguridad para determinar si cumple o no lo establecido, y además en el caso de tener nuevos requerimientos puedan ser implementados.

Como estrategia a largo plazo se recomienda que se tome en consideración lo siguiente:

Se recomienda establecer políticas y procedimientos para fortalecer la seguridad de TI en la empresa.

Obtener certificaciones de seguridad con la finalidad de cumplir con estándares y mantener un alto nivel de seguridad.

2.4.3.3 DS7 Educar y entrenar a los usuarios

Tabla 2-29Resultado de evaluación del proceso DS7

DS7	Educar y Entrenar a los Usuarios

Nivel	Cumplimiento	Contribución	Valor
0	1,00	0,00	0,00
1	0,60	1,00	0,60
2	0,76	1,00	0,76
3	0,76	1,00	0,76
4	0,80	1,00	0,80
5	0,60	1,00	0,60

Nivel de madurez=	**3,51**

Tabla 2-30 Modelo de Madurez DS7

DOMINIO: ENTREGAR Y DAR SOPORTE					
DS7: Educar y entrenar a los usuarios					
	NIVELES DE LOS MODELOS DE MADUREZ	CUMPLE	PARCIALMENTE	NO CUMPLE	OBSERVACIONES
NIVEL 0	Hay una total falta de programas deentrenamiento y educación. La organización no reconoce que hay un problema a ser atendido respecto al entrenamiento y no hay comunicación sobre el problema.	X			
NIVEL 1	Hay evidencia de que la organización ha reconocido la necesidad de contar con un programa de entrenamiento y educación, pero no hay procedimientos estandarizados. A falta de un proceso organizado, los empleados han buscado y asistido a cursos deentrenamiento por su cuenta. Algunos de estos cursos de entrenamiento abordan los temas de conducta ética, conciencia sobre laseguridad en los sistemas y prácticas de seguridad. El enfoque global de la gerencia carece de cohesión y sólo hay comunicaciónesporádica e inconsistente respecto a los problemas y enfoques para hacerse cargo del entrenamiento y la educación.	X			
NIVEL 2	Hay conciencia sobre la necesidad de un programa de entrenamiento y educación, y sobre los procesos asociados a lo largo de toda la organización. El entrenamiento está comenzando a identificarse en los planes de desempeño individuales de los empleados. Los procesos se han desarrollado hasta la fase en la cual se imparte entrenamiento informal por parte de diferentes instructores,cubriendo los mismos	X			

	temas de materias con diferentes puntos de vista. Algunas de las clases abordan los temas de conducta ética yde conciencia sobre prácticas y actividades de seguridad en los sistemas. Hay una gran dependencia del conocimiento de los individuos. Sin embargo, hay comunicación consistente sobre los problemas globales y sobre la necesidad de atenderlos.				
NIVEL 3	El programa de entrenamiento y educación se institucionaliza y comunica, y los empleados y gerentes identifican y documentan las necesidades de entrenamiento. Los procesos de entrenamiento y educación se estandarizan y documentan. Para soportar elprograma de entrenamiento y educación, se establecen presupuestos, recursos, instructores e instalaciones. Se imparten clasesformales sobre conducta ética y sobre conciencia y prácticas de seguridad en los sistemas. La mayoría de los procesos deentrenamiento y educación son monitoreados, pero no todas las desviaciones son susceptibles de detección por parte de la gerencia. El análisis sobre problemas de entrenamiento y educación solo se aplica de forma ocasional.	**X**			
NIVEL 4	Hay un programa completo de entrenamiento y educación que produce resultados medibles. Las responsabilidades son claras y seestablece la propiedad sobre los procesos. El entrenamiento y la educación son componentes de los planes de carrera de losempleados. La gerencia apoya y asiste a sesiones de entrenamiento y de educación. Todos los empleados reciben entrenamientosobre conducta ética y sobre conciencia y prácticas de seguridad en los sistemas. Todos los empleados reciben el nivel apropiado deentrenamiento sobre prácticas de seguridad en los sistemas para proteger contra daños originados por fallas que afecten la disponibilidad, la confidencialidad y la integridad. La gerencia monitorea el cumplimiento por medio de revisión constante yactualización del programa y de los procesos de entrenamiento. Los procesos están en vía de mejora y fomentan las mejoresprácticas internas.		**X**		**Objetivos no cumplidos:** En la Empresa EA, los empleados reciben entrenamiento sobre conducta, concienciación y prácticas de seguridad de en los sistemas pero de manera informal.
NIVEL 5	El entrenamiento y la educación dan como resultado la mejora del desempeño individual. El entrenamiento y la educación soncomponentes críticos de los planes de carrera de los empleados. Se asignan suficientes presupuestos, recursos, instalaciones einstructores para los programas de entrenamiento y educación. Los procesos se afinan y están en continua mejora, tomando ventajade las mejores prácticas externas y de modelos de madurez de otras organizaciones. Todos los problemas y desviaciones se analizanpara identificar las causas de raíz, se identifican y llevan a cabo acciones de forma expedita. Hay una actitud			**X**	

	positiva con respecto ala conducta ética y respecto a los principios de seguridad en los sistemas. TI se utiliza de manera amplia, integral y óptima paraautomatizar y brindar herramientas para los programas de entrenamiento y educación. Se utilizan expertos externos en entrenamiento y se utilizan benchmarks del mercado como orientación.				

COBIT define para el proceso DS7 los siguientes objetivos de control:

1. Identificación de Necesidades de Entrenamiento y Educación
2. Impartición de Entrenamiento y Educación
3. Evaluación del Entrenamiento Recibido

El objetivo esencial de un modelo de madurez es ascender a un grado de madurez superior, por esto para que el proceso DS7ascienda a un grado de madurez 5, como estrategia a corto plazo y conforme lo establece COBIT:

Se recomienda que se formalice y documente las prácticas y procedimientos de entrenamiento a los empleados.

Además investigar técnicas y estrategias que faciliten el entrenamiento y educación de los usuarios, con la finalidad de que alcanzar los objetivos de la organización.

Como estrategia a largo plazo se recomienda que se tome en consideración lo siguiente:

Se recomienda que los procesos se afinen y se mantengan en mejora continua basándose en las mejores prácticas y estándares de la industria.

Analizar los problemas para identificar las causas y tomar acciones correctivas al respecto.

2.4.3.4 DS10 Administrar los problemas

Tabla 2-31Resultado de evaluación del proceso DS10

DS10	Administración de Problemas

Nivel	Cumplimiento	Contribución	Valor
0	1,00	0,00	0,00
1	0,88	1,00	0,88
2	0,72	1,00	0,72
3	0,46	1,00	0,46
4	0,38	1,00	0,38
5	0,19	1,00	0,19

Nivel de madurez =	**2,63**

Tabla 2-32 Modelo de Madurez DS10

DOMINIO: ENTREGAR Y DAR SOPORTE					
DS10: Administrar los problemas					
NIVELES DE LOS MODELOS DE MADUREZ		CUMPLE	PARCIALMENTE	NO CUMPLE	OBSERVACIONES
NIVEL 0	No hay conciencia sobre la necesidad de administrar problemas, y no hay diferencia entre problemas e incidentes. Por lo tanto, no sehan hecho intentos por identificar la causa raíz de los incidentes.	X			
NIVEL 1	Los individuos reconocen la necesidad de administrar los problemas y de revolver las causas de fondo. Algunos individuos expertos clave brindan asesoría sobre problemas relacionados a su área de experiencia, pero no está asignada la responsabilidad para la administración de problemas. La información no se comparte, resultando en la creación de nuevos problemas y la pérdida de tiempo productivo mientras se buscan respuestas.	X			
NIVEL 2	Hay una amplia conciencia sobre la necesidad y los beneficios de administrar los problemas relacionados con TI, tanto dentro de las áreas de negocio como en la función de servicios de información. El proceso de resolución ha evolucionado un punto en el que unoscuantos individuos clave sonresponsables de identificar y resolver los problemas. La información se comparte entre el personal demanera informal y reactiva. El nivel de servicio hacia la comunidad usuaria varía y es obstaculizado por la falta de conocimientoestructurado a disposición del administrador de problemas.	X			

NIVEL 3	Se acepta la necesidad de un sistema integrado de administración de problemas y se evidencia con el apoyo de la gerencia y la asignación de presupuesto para personal y entrenamiento. Se estandarizan los procesos de escalamiento y resolución de problemas. El registro y rastreo de problemas y de sus soluciones se dividen dentro del equipo de respuesta, utilizando las herramientas disponibles sin centralizar. Es poco probable detectar las desviaciones de los estándares y de las normas establecidas. Lainformación se comparte entre el personal de manera formal y proactiva. La revisión de incidentes y los análisis de identificación yresolución de problemas son limitados e informales.		**X**		**Objetivos no cumplidos:** No se estandarizan los procesos de escalamiento y resolución de problemas.
NIVEL 4	El proceso de administración de problemas se entiende a todos los niveles de la organización. Las responsabilidades y la propiedad de los problemas están claramenteestablecidas. Los métodos y losprocedimientos son documentados, comunicados y medidos paraevaluar su efectividad. La mayoría de los problemas están identificados, registrados y reportados, y su solución ha iniciado. Elconocimiento y la experiencia se cultivan, mantienen y desarrollan hacia un nivel más alto a medida que la función es vista como unactivo y una gran contribución al logro de las metas de TI y a la mejora de los servicios de TI. La administración de problemas estábien integrada con los procesos interrelacionados, tales como administración de incidentes, de cambios, y de configuración, y ayuda a los clientes para administrar información, instalaciones y operaciones. Se han acordado los KPIs y KGIs para el proceso de administración de problemas.			**X**	
NIVEL 5	El proceso de administración de problemas ha evolucionado a un proceso proactivo y preventivo, que contribuye con los objetivos de TI. Los problemas se anticipan y previenen. El conocimiento respecto a patrones deproblemas pasados y futuros se mantiene a través de contactos regulares con proveedores y expertos. El registro, reporte y análisis de problemas y soluciones está integrado por completo con la administración de datos de configuración. Los KPIs y KGIs son medidos de manera consistente. La mayoría de los sistemas están equipados con mecanismos automáticos de advertencia y detección, los cuales son rastreados y evaluados demanera continua. El proceso de administración de problemas se analiza para buscar la mejora continua con base en los KPIs y KGIs yse reporta a los interesados.			**X**	

COBIT define para el proceso DS10 los siguientes objetivos de control:

1. Identificación y Clasificación de Problemas
2. Rastreo y Resolución de Problemas
3. Cierre de Problemas
4. Integración de las Administraciones de Cambios, Configuración y Problemas

El objetivo esencial de un modelo de madurez es ascender a un grado de madurez superior, por esto para que el proceso DS10ascienda a un grado de madurez 4, como estrategia a corto plazo y conforme lo establece COBIT:

Se recomienda la implementación de un Plan de Administración de Problemas tomando en cuenta todos los aspectos clave de la organización.

También se recomienda estandarizar los procesos de escalamiento y resolución de problemas.

Como estrategia a largo plazo se recomienda que se tome en consideración lo siguiente:

Se recomienda que la Administración de Problemas evolucione a un nivel en el que se convierta en un proceso proactivo y preventivo, contribuyendo así son los objetivos del negocio.

Establecer indicadores clave de metas y desempeño sean medidos de manera consistente para el mejoramiento continuo del proceso.

2.4.3.5 DS13 Administrar las operaciones

Tabla 2-33Resultado de evaluación del proceso DS13

DS13	Administración de Operaciones

Nivel	Cumplimiento	Contribución	Valor
0	1,00	0,00	0,00
1	0,75	1,00	0,75
2	0,73	1,00	0,73
3	0,55	1,00	0,55
4	0,58	1,00	0,58
5	0,70	1,00	0,70

Nivel de madurez=	**3,31**

Tabla 2-34 Modelo de Madurez DS13

DOMINIO: ENTREGAR Y DAR SOPORTE					
DS13: Administrar las operaciones					
NIVELES DE LOS MODELOS DE MADUREZ		CUMPLE	PARCIALMENTE	NO CUMPLE	OBSERVACIONES
NIVEL 0	La organización no dedica tiempo y recursos al establecimiento de soporte básico de TI y a actividades operativas.	X			
NIVEL 1	La organización reconoce la necesidad de estructurar las funciones de soporte de TI. Se establecen algunos procedimientos estándar y las actividades de operaciones son de naturaleza reactiva. La mayoría de los procesos de operación son programados de manerainformal y el procesamiento de peticiones se acepta sin validación previa. Las computadoras, sistemas y aplicaciones que soportanlos procesos del negocio con frecuencia no están disponibles, se interrumpen o retrasan. Se pierde tiempo mientras los empleadosesperan recursos. Los medios de salida aparecen ocasionalmente en lugares inesperados o no aparecen	X			
NIVEL 2	La organización esta consiente del rol clave que las actividades de operaciones de TI juegan en brindar funciones de soporte de TI. Seasignan presupuestos para herramientas con un criterio de caso por caso. Las operaciones de soporte de TI son informales e intuitivas. Hay una alta dependencia sobre las habilidades de los individuos. Lasinstrucciones de qué hacer, cuándo y en qué ordenno están	X			

	documentadas. Existe algo de entrenamiento para el operador y hay algunos estándares de operación formales.				
NIVEL 3	Se entiende y acepta dentro de la organización la necesidad de administrar las operaciones de cómputo. Se han asignado recursos yse lleva a cabo algúnentrenamiento durante el trabajo. Las funciones repetitivas están definidas, estandarizadas, documentadas ycomunicadas de manera formal. Los resultados de las tareas completadas y de los eventos se registran, con reportes limitados hacia la gerencia. Se introduce el uso de herramientas de programación automatizadas y de otras herramientas para limitar la intervencióndel operador. Se introducen controles para colocar nuevos trabajos en operación. Se desarrolla una política formal para reducir elnúmero de eventos no programados. Los acuerdos de servicio y mantenimiento con proveedores siguen siendo de naturalezainformal.		**X**		**Objetivos no cumplidos:** No se desarrolla una política formal para reducir en número de eventos noprogramados.
NIVEL 4	Las operaciones de cómputo y las responsabilidades de soporte están definidas de forma clara y la propiedad está asignada. Lasoperaciones se soportan a través de presupuestos de recursos para gastos de capital y de recursos humanos. El entrenamiento seformaliza y está en proceso. Las programaciones y las tareas se documentan y comunican, tanto a la función interna de TI como a losclientes del negocio. Es posible medir y monitorear las actividades diarias con acuerdos estandarizados de desempeño y de niveles deservicio establecidos. Cualquier desviación de las normas establecidas es atendida y corregida de forma rápida. La gerenciamonitorea el uso de los recursos de cómputo y la terminación del trabajo o de las tareas asignadas. Existe un esfuerzo permanentepara incrementar el nivel de automatización de procesos como un medio de mejora continua. Se establecen convenios formales demantenimiento y servicio con los proveedores. Hay una completa alineación con los procesos de administración de problemas,capacidad y disponibilidad, soportados por un análisis de causas de errores y fallas.			**X**	
NIVEL 5	Las operaciones de soporte de TI son efectivas, eficientes y suficientemente flexibles para cumplir con las necesidades de niveles deservicio con una pérdida de productividad mínima. Los procesos de administración de operaciones de TI están estandarizados y documentados en una base de conocimiento, y están sujetos a una mejora continua. Los procesos automatizados que soportan los			**X**	

	sistemas contribuyen a un ambiente estable. Todos los problemas y fallas se analizan para identificar la causa que los originó. Las reuniones periódicas con los responsables de administración del cambio garantizan la inclusión oportuna de cambios en las programaciones de producción. En colaboración con los proveedores, el equipo se analiza respecto a posibles síntomas de obsolescencia y fallas, y el mantenimiento es principalmente de naturaleza preventiva.				

COBIT define para el proceso DS13 los siguientes objetivos de control:

1. Procedimientos e Instrucciones de Operación
2. Programación de Tareas
3. Monitoreo de la Infraestructura de TI
4. Documentos Sensitivos y Dispositivos de Salida
5. Mantenimiento Preventivo del Hardware

El objetivo esencial de un modelo de madurez es ascender a un grado de madurez superior, por esto para que el proceso DS13ascienda a un grado de madurez 4, como estrategia a corto plazo y conforme lo establece COBIT:

Se recomienda desarrollar una política formal para reducir el número de eventos no programados.

Programar tareas y responsabilidades que sean documentadas y comunicadas a la función interna de TI e interesados.

Es necesario se monitoree las actividades diarias con acuerdos estandarizados con el fin de cumplir los niveles de servicio que se establezcan.

Como estrategia a largo plazo se recomienda que se tome en consideración lo siguiente:

Se recomienda la alineación de los procesos de administración de problemas, capacidad y disponibilidad.

Todos los problemas y fallas deben ser analizados con el fin de identificar las causas de su origen.

2.4.4 PROCESOS DEL DOMINIO DE MONITOREAR Y EVALUAR

2.4.4.1 ME1 Monitorear y evaluar el desempeño de TI

Tabla 2-35Resultado de evaluación del proceso ME1

ME1	Monitorear y Evaluar el Desempeño de TI

Nivel	Cumplimiento	Contribución	Valor
0	0,92	0,00	0,00
1	0,68	1,00	0,68
2	0,77	1,00	0,77
3	0,34	1,00	0,34
4	0,47	1,00	0,47
5	0,14	1,00	0,14
	Nivel de madurez=		**2,39**

Tabla 2-36 Modelo de Madurez ME1

DOMINIO: MONITOREAR Y EVALUAR					
ME1: Monitorear y evaluar el desempeño de TI					
NIVELES DE LOS MODELOS DE MADUREZ		CUMPLE	PARCIALMENTE	NO CUMPLE	OBSERVACIONES
NIVEL 0	La organización no cuenta con un proceso implantado de monitoreo. TI no lleva a cabo monitoreo de proyectos o procesos de formaindependiente. No se cuenta con reportes útiles, oportunos y precisos. La necesidad de entender de forma clara los objetivos de losprocesos no se reconoce.	X			
NIVEL 1	La gerencia reconoce una necesidad de recolectar y evaluar información sobre los procesos de monitoreo. No se han identificadoprocesos estándar de recolección y evaluación. El monitoreo se implanta y las métricas se seleccionan de acuerdo a cada caso, deacuerdo a las necesidades de proyectos y procesos de TI específicos. El monitoreo por lo general se implanta de forma reactiva aalgún incidente que ha ocasionado alguna perdida o vergüenza a la organización. La función de contabilidad monitorea medicionesfinancieras básicas para TI.	X			

NIVEL 2	Se han identificado algunas mediciones básicas a ser monitoreadas. Los métodos y las técnicas de recolección y evaluación existen,pero los procesos no se han adoptado en toda la organización. La interpretación de los resultados del monitoreo se basa en laexperiencia de individuos clave. Herramientas limitadas son seleccionadas y se implantan para recolectar información, pero esta recolección no se basa en un enfoque planeado.	X			
NIVEL 3	La gerencia ha comunicado einstitucionalizado un procesos estándar de monitoreo. Se han implantado programas educacionales yde entrenamiento para el monitoreo. Se ha desarrollado una base de conocimiento formalizada del desempeño histórico. Lasevaluaciones todavía se realizan al nivel de procesos y proyectos individuales de TI y no están integradas a través de todos losprocesos. Se han definido herramientas para monitorear los procesos y los niveles de servicio de TI. Las mediciones de lacontribución de la función de servicios de información al desempeño de la organización se han definido, usando criterios financieros y operativos tradicionales. Las mediciones del desempeño específicas de TI, las mediciones no financieras, lasestratégicas, las desatisfacción del cliente y los niveles de servicio están definidas. Se ha definido un marco de trabajo para medir el desempeño.			X	
NIVEL 4	La gerencia ha definido las tolerancias bajo las cuales los procesos deben operar. Los reportes de los resultados del monitoreo estánen proceso de estandarizarse y normalizarse. Hay una integración de métricas a lo largo de todos los proyectos y procesos de TI. Lossistemas de reporte de la administración de TI están formalizados. Las herramientas automatizadas están integradas y se aprovechanen toda la organización para recolectar y monitorear la información operativa de lasaplicaciones, sistemas y procesos. La gerenciapuede evaluar el desempeño con base en criterios acordados y aprobados por las terceras partes interesadas. Las mediciones de lafunción de TI están alienadas con las metas de toda la organización.			X	

NIVEL 5	Un proceso de mejora continua de la calidad se ha desarrollado para actualizar los estándares y las políticas de monitoreo a nivelorganizacional incorporando mejores prácticas de la industria. Todos los procesos de monitoreo están optimizados y dan soporte a losobjetivos de toda la organización. Las métricas impulsadas por el negocio se usan de forma rutinaria para medir el desempeño, yestán integradas en los marcos de trabajo estratégicos, tales como el BalancedScorecard. El monitoreo de los procesos y el rediseñocontinuo son consistentes con los planes de mejora de los procesos de negocio en toda la organización. Benchmarks contra la industria y los competidores clave se han formalizado, con criterios de comparación bien entendidos.			**X**	

COBIT define para el proceso ME1 los siguientes objetivos de control:

1. Enfoque del Monitoreo
2. Definición y Recolección de Datos de Monitoreo
3. Método de Monitoreo
4. Evaluación del Desempeño
5. Reportes al Consejo Directivo y a Ejecutivos
6. Acciones Correctivas

El objetivo esencial de un modelo de madurez es ascender a un grado de madurez superior, por esto para que el proceso ME1ascienda a un grado de madurez 3, como estrategia a corto plazo y conforme lo establece COBIT:

Se recomienda que se implemente un proceso estándar de monitoreo y se defina herramientas para el monitoreo de los procesos y los niveles de servicio.

Efectuar regularmente una comparación entre el desempeño de TI con las metas del negocio.

Como estrategia a mediano plazo se recomienda que se tome en consideración lo siguiente:

Es necesario que se realicen reportes de los resultados obtenidos para que la Gerencia esté informada del cumplimiento de las metas.

Las herramientas automatizadas deben estar integradas y ser de ayuda para toda la organización en la recolección y monitoreo de la información.

2.4.4.2 ME4 Proporcionar gobierno de TI

Tabla 2-37Resultado de evaluación del proceso ME4

ME4	Proporcionar Gobierno de TI

Nivel	Cumplimiento	Contribución	Valor
0	0,91	0,00	0,00
1	0,65	1,00	0,65
2	0,68	1,00	0,68
3	0,60	1,00	0,60
4	0,73	1,00	0,73
5	0,57	1,00	0,57

Nivel de madurez =	**3,23**

Tabla 2-38 Modelo de Madurez ME4

DOMINIO: MONITOREAR Y EVALUAR					
ME4: Proporcionar gobierno de TI					
	NIVELES DE LOS MODELOS DE MADUREZ	CUMPLE	PARCIALMENTE	NO CUMPLE	OBSERVACIONES
NIVEL 0	Existe una carencia completa de cualquier proceso reconocible de gobierno de TI. La organización ni siquiera ha reconocido que existe un problema a resolver; por lo tanto, no existe comunicación respecto al tema.	X			
NIVEL 1	Se reconoce que el tema del gobierno de TI existe y que debe ser resuelto. Existen enfoques ad hoc aplicados individualmente o casopor caso. El enfoque de la gerencia es reactivo y solamente existe una comunicación esporádica e inconsistente sobre los temas y losenfoques para resolverlos. La gerencia solo cuenta con una indicación aproximada de cómo TI contribuye al desempeño del negocio. La gerencia solo responde de forma reactiva a los incidentes que hayan causado pérdidas o vergüenza a la organización.	X			

NIVEL 2	Existe una conciencia sobre los temas de gobierno de TI. Las actividades y los indicadores de desempeño del gobierno de TI, loscuales incluyen procesos planeación, entrega y supervisión de TI, están en desarrollo. Los procesos de TI seleccionados se identifican para ser mejorados con base en decisiones individuales. La gerencia ha identificado mediciones básicas para el gobierno de TI, así como métodos de evaluación y técnicas; sin embargo, el proceso no ha sido adoptado a lo largo de la organización. La comunicación respecto a los estándares y responsabilidades de gobierno se deja a los individuos. Los individuos impulsan los procesos de gobiernoen varios proyectos y procesos de TI. Los procesos, herramientas y métricas para medir el gobierno de TI están limitadas y pueden nousarse a toda su capacidad debido a la falta de experiencia en su funcionalidad.	**X**			
NIVEL 3	La importancia y la necesidad de un gobierno de TI se reconocen por parte de la gerencia y se comunican a la organización. Unconjunto de indicadores base de gobierno de TI se elaboran donde se definen y documentan los vínculos entre las mediciones deresultados y los impulsores del desempeño. Los procedimientos se han estandarizado y documentado. La gerencia ha comunicado losprocedimientos estandarizados y el entrenamiento está establecido. Se han identificado herramientas para apoyar a la supervisióndel gobierno de TI. Se han definido tableros de control como parte de los BalancedScorecard de TI. Sin embargo, se delega alindividuo su entrenamiento, el seguimiento de los estándares y su aplicación. Puede ser que se monitoreen los procesos sin embargola mayoría de desviaciones, se resuelven con iniciativa individual y es poco probable que se detecten por parte de la gerencia.		**X**		**Objetivos no cumplidos:** La Empresa no ha definido tableros de control como parte de los BSC. Todos los procedimientos no están documentados y estandarizados.
NIVEL 4	Existe un entendimiento completo de los temas de gobierno a todos los niveles. Hay un entendimiento claro de quién es el cliente y se definen y supervisan las responsabilidades por medio de acuerdos de niveles de servicio. Las responsabilidades son claras y lapropiedad de procesos está establecida. Los procesos de TI y el gobierno de TI están alineados e integrados con la estrategiacorporativa de TI. La mejora de los procesos de TI se basa principalmente en un entendimiento cuantitativo y es posiblemonitorear ymedir el cumplimiento con procedimientos y métricas de procesos. Todos los interesados en los procesos están conscientes de losriesgos, de la importancia de TI, y de las oportunidades que ésta puede ofrecer. La gerencia ha definido niveles de tolerancia bajo loscuales los procesos pueden operar. Existe un uso limitado,			**X**	

	principalmente táctico, de la tecnología con base en técnicas maduras yherramientas estándar ya implantadas. El gobierno de TI ha sido integrado a los procesos de planeación estratégica y operativa, asícomo a los procesos de monitoreo. Los indicadores de desempeño de todas las actividades de gobierno de TI se registran y siguen, yesto lidera mejoras a nivel de toda la empresa. La rendición general de cuentas del desempeño de los procesos clave es clara, y la gerencia recibe recompensas con base en las mediciones clave de desempeño.				
NIVEL 5	Existe un entendimiento avanzado y a fututo de los temas y soluciones del gobierno de TI. El entrenamiento y la comunicación sebasan en conceptos y técnicas de vanguardia. Los procesos se han refinado hasta un nivel de mejor práctica de la industria, con baseen los resultados de las mejoras continuas y en el modelo de madurez con respecto a otras organizaciones. La implantación de laspolíticas de TI ha resultado en una organización, personas y procesos que se adaptan rápidamente, y que dan soporte completo a losrequisitos de gobierno de TI. Todos los problemas y desviaciones se analizan por medio de la técnica de causa raíz y se identifican eimplementan medidas eficientes de forma rápida. TI se utiliza de forma amplia, integrada y optimizada para automatizar el flujo detrabajo y brindar herramientas para mejorar la calidad y efectividad. Los riesgos y los retornos de los procesos de TI están definidos,balanceados y comunicados en toda la empresa. Se aprovechan a los expertos externos y se usan evaluaciones por comparaciónpara orientarse. El monitoreo, la auto-evaluación y la comunicación respecto a las expectativas de gobierno están en toda laorganización y se dé un uso óptimo a la tecnología para apoyar las mediciones, el análisis, la comunicación y el entrenamiento. El Gobierno Corporativo y el gobierno de TI están vinculados de forma estratégica, aprovechando la tecnología y los recursos humanos yfinancieros para mejorar la ventaja competitiva de la empresa. Las actividades de gobierno de TI están integradas al proceso deGobierno Corporativo.			**X**	

COBIT define para el proceso ME4 los siguientes objetivos de control:

1. Establecimiento de un Marco de Gobierno de TI
2. Alineamiento Estratégico
3. Entrega de Valor

4. Administración de Recursos
5. Administración de Riesgos
6. Medición del Desempeño
7. Aseguramiento Independiente

El objetivo esencial de un modelo de madurez es ascender a un grado de madurez superior, por esto para que el proceso ME4ascienda a un grado de madurez 4, como estrategia a corto plazo y conforme lo establece COBIT:

Se recomienda que se implemente y se registre indicadores de desempeño de todas las actividades de gobierno de TI.

Definir tableros de control como parte del BSC.

Como estrategia a largo plazo se recomienda que se tome en consideración lo siguiente:

Se debe establecer acuerdos de nivel de servicio donde se defina y supervise las responsabilidades con el cliente.

Reforzar temas de Gobierno de TI a todos los niveles y todo el personal debe estar al tanto para que se tome medidas en la mejora del proceso.

CAPÍTULO III

ANÁLISIS DE LOS RESULTADOS

3.1 ANALISIS DE LOS RESULTADOS

A continuación se detalla el *Informe Preliminar, Informe Técnico* e *Informe Ejecutivo*, los cuales estarán dirigidos al Gerente de Tecnologías de la Información de la Empresa EA y personal que esté interesado en los resultados obtenidos en la auditoría basada en COBIT 4.1.

En estos informes se incluirá observaciones, conclusiones y recomendaciones basadas en la auditoría y evaluación de cada uno de los procesos de COBIT que fueron seleccionados en la sección 2.2.

En la tabla 3-1 se muestra el reporte de niveles de madurez de cada uno de los procesos que han sido evaluados en la Empresa EA.

Tabla 3-1 Reporte General de los Niveles de Madurez

DOMINIO	PROCESO		NIVEL DE MADUREZ
PLANEAR Y ORGANIZAR	**PO1**	Definir un plan estratégico de TI.	4
	PO2	Definir la arquitectura de la información.	3
	PO3	Determinar la dirección tecnológica.	3
	PO4	Definir procesos, organización y relaciones de TI.	3
	PO6	Comunicar las aspiraciones y la dirección de la gerencia.	3
	PO7	Administrar recursos humanos de TI.	3
	PO9	Evaluar y administrar riesgos de TI.	2
	PO10	Administrar proyectos.	3
ADQUIRIR E IMPLEMENTAR	**AI2**	Adquirir y mantener el software aplicativo.	4
	AI3	Adquirir y mantener la infraestructura tecnológica.	3
	AI4	Facilitar la operación y el uso.	2
	AI5	Adquirir recursos de TI.	4
ENTREGAR Y DAR SOPORTE	**DS1**	Definir y administrar niveles de servicio.	2
	DS5	Garantizar la seguridad de los sistemas.	3
	DS7	Educar y entrenar a los usuarios.	4
	DS10	Administrar los problemas.	3
	DS13	Administrar las operaciones.	3
MONITOREAR Y EVALUAR	**ME1**	Monitorear y evaluar el desempeño de TI.	2
	ME4	Proporcionar gobierno de TI.	3

En la Figura 3-1se muestra los niveles de madurez actuales como se indica en la Tabla 3-1 y los niveles de madurez futuros que se han que se han definido luego de la evaluación de cada proceso.

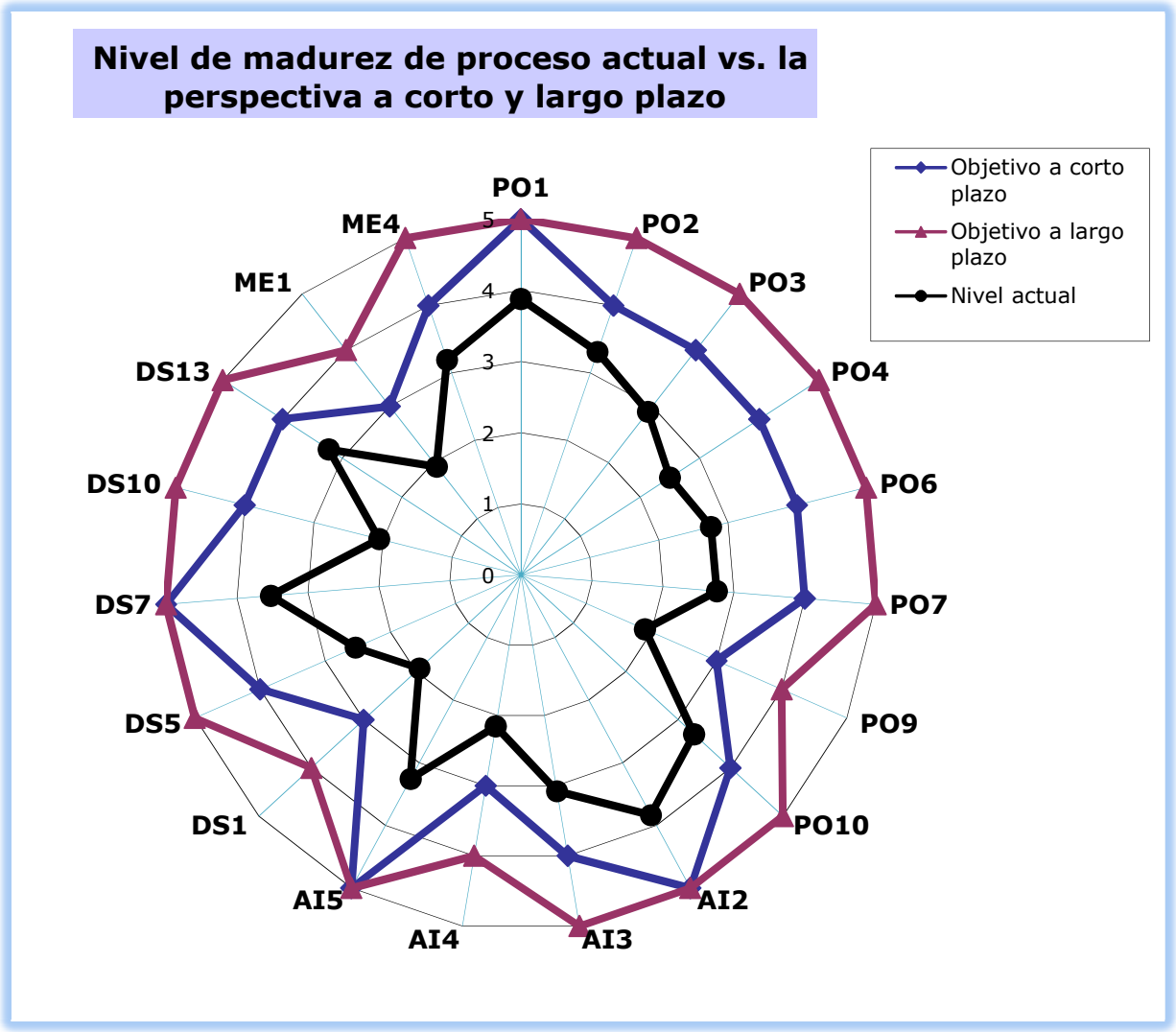

Figura 3-1 Nivel de madurez de los procesos Actual vs. Futuro

Los resultados obtenidos nos permiten conocer el nivel en el que se encuentra cada dominio, para obtener el nivel del dominio se tomará en cuenta el nivel de madurez más bajo de los procesos que se encuentran dentro de este.

Considerando el nivel más bajo de los procesos, se ha obtenido el nivel en que se encuentran los cuatro dominios como se detalla a continuación:

- Planificar y Organizar: Nivel 2
- Adquirir e Implementar: Nivel 2
- Entregar y Dar Soporte: Nivel 2
- Monitorear y Evaluar: Nivel 2

Luego de haber identificado el nivel más bajo obtenido en los cuatro dominios, se puede establecer que la Empresa EA en general se encuentra en un *nivel 2 (Repetible pero Intuitivo).*

La Empresa EA según lo establece COBIT, en este nivel se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

Como plan de mejoramiento de los procesos a corto plazo se debe empezar subiendo todos los procesos que se encuentran en un *nivel 2* a un *nivel 3(Definido)*con el uso de las estrategias presentadas en este trabajo,terminado este plan se debe trabajar para alcanzar el siguiente nivel superior con la finalidad que se llegue a estandarizar todos los procesos de la empresa.

3.2 INFORME PRELIMINAR

Este Informe se lo realiza con el objetivo de recolectar las observaciones necesarias como retroalimentación de la Gerencia de Tecnologías de la Información de la empresa EA, en este informe se da a conocer los resultados obtenidos en la práctica realizada.

El documento entregado a la empresa se encuentra en el **Anexo3.**

En la carta entregada por la empresa, el criterio de la Gerencia de Tecnologías de TI menciona que se ha realizado este trabajo de forma satisfactoria y que los resultados obtenidos muestra la situación en la que se encuentra la empresa.

Luego de esta revisión de resultados la empresa ahora cuenta con una herramienta adicional para optimizar sus procesos y procedimientos internos, como parte de la mejora continua,que es algo esencial dentro de esta empresa.

3.3 INFORME TÉCNICO

ALCANCE

Mediante este proyecto se desea realizar la auditoría del área de Tecnologías de la Información de una empresa de aviación.

El proyecto empieza con la caracterización de la empresa, análisis de la documentación. Luego se realizará un análisis del estado de las TIC'S en la empresa. Se seleccionarán los procesos, dominios y recursos de TI donde se aplicará la auditoría, basada en COBIT. Luego se realizará la auditoría y finalmente se realizarán los informes con los resultados obtenidos.

OBJETIVOS

OBJETIVO GENERAL

- Auditar la Gestión de las TIC'S para una empresa de aviación.

OBJETIVOS ESPECIFICOS

- Analizar la situación actual de la empresa.
- Recopilar y analizar la información de la empresa.
- Analizar los procesos que realiza la empresa para identificar posibles problemas de la empresa.

Metodología

Para la realización de esta Auditoría se toma como marco de referencia COBIT 4.1. COBIT (Control ObjectivesforInformation and RelatedTechnology - Objetivos de Control para la Información y Tecnologías relacionadas), es un marco de trabajo que define las razones de por qué se necesita el gobierno de TI y que se necesita cumplir en el gobierno de TI. Además este marco de trabajo tiene las siguientes características:

- Orientado a negocios

- Orientado a procesos
- Basado en controles
- Impulsado por mediciones.

Este marco de trabajo da soporte al gobierno de TI de manea que se garantice lo siguiente:

- TI está alineada con el negocio
- TI habilita al negocio y maximiza los beneficios
- Los recursos de TI se usan de manera responsable
- Los riesgos de TI se administran apropiadamente

COBIT permite evaluar los procesos mediante el modelo de madurez, este modelo está basado en un método de evaluación de la organización, con el fin de que se pueda evaluar así misma desde un nivel 0 ya que es posible que no existan procesos en lo absoluto.

La escala del 0-5 se basa en una escala de madurez simple que muestra como un proceso evoluciona desde una capacidad no existente hasta una capacidad optimizada.

RESULTADOS DE LA AUDITORÍA

Tabla 3-2 Resumen de resultados PO1

PO1 Definir un Plan Estratégico de TI	**Grado de Madurez** *CUATRO*
CONCLUSIÓN FINAL:	
• La planificación estratégica de TI no considera riesgos, evaluaciones en comparación con normas y estándares de la industria, con el fin de comparar como se lleva este proceso en otras empresas de la misma naturaleza y mejorar.	
RECOMENDACIONES FINALES:	
• En la planificación estratégica debe considerarse que todas las metas del negocio estén en alineación con las metas de TI. • Evaluar el cumplimiento del Plan Táctico (Plan Anual) para determinar si se está obteniendo los resultados esperados, que sería el cumplimiento de las metas estratégicas y tácticas. • Establecer que el Plan Estratégico y Táctico de TI se mantengan en mejora	

continua, tratando de cumplir normas bien definidas relacionadas al negocio.

Tabla 3-3 Resumen de resultados PO2

PO2 Definir la Arquitectura de la Información.	**Grado de Madurez** *TRES*
CONCLUSIÓN FINAL:	
• Este proceso se realiza de forma reactiva, lo cual no permite que se resuelvan posibles problemas que pudieran estarse presentando. Además no se mide el éxito de la arquitectura de la información implementada para ser reforzada.	
RECOMENDACIONES FINALES:	
• Establecer metas y métricas para la evaluación del proceso de Desarrollo e Implementación de Arquitectura de la Información con el fin de mejorar el desempeño del mismo. • Determinar procedimientos para que este proceso sea proactivo y logre resolver necesidades futuras del negocio. • El proceso de definición de Arquitectura de Información debe estar justificado formalmente, especificando las características y beneficios que se obtendrán con su implementación. • La Arquitectura de Información debe ser reforzada de manera consistente a todos los niveles para conseguir una mejor administración del proceso. • Establecer tecnologías para la minería de datos. • Implementar procedimientos formales donde se incluya la mejora continua del proceso y se considere toda la información de los procesos organizacionales y sistemas.	

Tabla 3-4Resumen de resultados PO3

PO3 Determinar la Dirección Tecnológica	**Grado de Madurez** *TRES*
CONCLUSIÓN FINAL:	
• No existe un plan de Infraestructura Tecnológica bien definido, tampoco están bien definidos los riesgos que involucran a este proceso.	
RECOMENDACIONES FINALES:	
• Formalizar un Plan de Infraestructura Tecnológica donde se especifiquen claramente los objetivos, riesgos. Este plan debe estar alineado con las estrategias del negocio y pueda ser sujeto a cambios. • Realizar evaluaciones acerca del uso de la tecnología para identificar los posibles	

riesgos.

- El Plan de Infraestructura Tecnológica debe implementar estándares de la industria para satisfacer las necesidades del negocio e implementar las mejores prácticas que sean relevantes para mejorar este proceso.
- Implementar políticas y procedimientos formales para el desarrollo del Plan.
- Acceder a recursos externos para los casos que sean necesarios, con la finalidad de tener mayor experiencia y las habilidades necesarias para cumplir con los objetivos del negocio y de TI.

Tabla 3-5Resumen de resultados PO4

PO4 Definir procesos, organización y relaciones de TI	**Grado de Madurez** *TRES*
CONCLUSIÓN FINAL:	
• En cierto grado hace falta formalizar las relaciones con los usuarios y terceros. • La estructura organizacional de TI no refleja de manera apropiada las necesidades del negocio, ya que se encuentra al mismo nivel de otras áreas estratégicas.	
RECOMENDACIONES FINALES:	
• Reformar la estructura organizacional de la empresa, donde la Gerencia de Tecnologías de Información se encuentre a un nivel asesor y de esta manera TI este alineada con toda la organización. • Asignar roles y responsabilidades para fortalecer el manejo de Gestión de Riesgos y la Seguridad Informática. • Fortalecer las relaciones con terceros involucrando a los comités de la dirección, auditoría interna y administración de proveedores. • Formalizar procedimientos para mejorar el desempeño y monitoreo de la organización y de los procesos de TI para que se mantengan en mejora continua y cumplan con los objetivos de la organización.	

Tabla 3-6Resumen de resultados PO6

PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia	**Grado de Madurez** *TRES*
CONCLUSIÓN FINAL:	
• Las técnicas para fomentar conciencia de la seguridad no están estandarizadas, ni formalizadas. • Hace falta formalizar técnicas de concienciación de seguridad.	
RECOMENDACIONES FINALES:	
• Reforzar los controles de información, las políticas de control interno y que todas	

las políticas y procedimientos acordados sean informados a todo el personal de TI. • Monitorear el proceso para verificar que se cumpla todo lo establecido. • Formalizar y estandarizar las técnicas de concienciación de seguridad. • Considerar expertos internos y externos para garantizar que se adopten las mejores prácticas de la industria. • Implementar bases de conocimiento de políticas y de concienciación con la finalidad de optimizar la comunicación mediante la implementación de herramientas de automatización.

Tabla 3-7Resumen de resultados PO7

PO7 Administrar Recursos Humanos de TI	**Grado de Madurez** *TRES*
CONCLUSIÓN FINAL:	
• No se ha establecido un programa de rotación, diseñado para expandir las habilidades gerenciales y de negocio, debido a que cada área cuenta con personal especializado en dicha área.	
RECOMENDACIONES FINALES:	
• Elaborar y Mantener un Plan de Administración de Recursos Humanos de TI, que permita realizar revisiones del desempeño del personal para satisfacer los requerimientos del negocio. • Implementar métricas estandarizadas que le permiten identificar desviaciones. • La Administración de Recursos Humanos de TI debe estar integrada y responder a las estrategias del negocio. • El Plan de Administración de Recursos Humanos de TI se debe actualizar constantemente para cumplir con los cambiantes requerimientos del negocio	

Tabla 3-8Resumen de resultados PO9

PO9 Evaluar y administrar riesgos de TI	**Grado de Madurez** *DOS*
CONCLUSIÓN FINAL:	
• No existe un proceso bien definido, ni documentado para la Administración de Riesgos. • No se han identificado los riesgos claves para el negocio.	
RECOMENDACIONES FINALES:	
• Implementar políticas y procedimientos formales para la Administración de Riesgos de toda la organización. • Asignar roles y responsables de cada proceso con el fin de que los riesgos del	

negocio sean identificados, evaluados y se obtenga soluciones inmediatas. • Seguir un proceso de Evaluación y Administración de Riesgos estandarizado. • Para la mitigación de riesgos es necesario monitorear y evaluar individualmente cada proyecto de manera continua.

Tabla 3-9 Resumen de resultados PO10

PO10 Administrar Proyectos	**Grado de Madurez** *TRES*
CONCLUSIÓN FINAL:	
• En la administración de proyectos se hace un seguimiento para que se cumpla con los objetivos esperados en tiempo, pero no en el presupuesto. • No se tiene bien definido una administración de proyectos dentro de TI con roles y responsabilidades.	
RECOMENDACIONES FINALES:	
• Asignar una oficina de Administración de Proyectos dentro de TI con roles y responsabilidades sobre los proyectos y programas desde su inicio hasta después de su implementación. • Los proyectos necesitan ser monitoreados en puntos clave y se debe considerar métricas para verificar su cumplimiento. • La administración de proyectos debe ser evaluada por la organización, no únicamente por TI. • Implementar una metodología para el ciclo de vida de los proyectos con la finalidad de que se maneje las mejores prácticas para la Administración de Proyectos y de esta forma se pueda garantizar que los recursos de TI y del usuario son optimizados.	

Tabla 3-10 Resumen de resultados AI2

AI2 Adquirir y Mantener el Software Aplicativo	**Grado de Madurez** *CUATRO*
CONCLUSIÓN FINAL:	
• Las prácticas de adquisición y software aplicativo no están reforzadas a nivel de toda la empresa. • La metodología para este proceso no está completamente enfocada a la mejora continua,	
RECOMENDACIONES FINALES:	
• Las prácticas de adquisición y software aplicativo se extiendan para toda la empresa, además debe ser reforzada para que se tenga un posicionamiento estratégico inmediato.	

• Mantener el proceso en mejora continua con la finalidad de que soporte requerimientos cambiantes del negocio sin problema.

Tabla 3-11Resumen de resultados AI3

AI3 Adquirir y Mantener la Infraestructura Tecnológica	**Grado de Madurez** *TRES*
CONCLUSIÓN FINAL:	
• El Plan de adquisición y Mantenimiento de Infraestructura de TI no está implementado.	
RECOMENDACIONES FINALES:	
• Implementar un Plan de Adquisición y Mantenimiento de la Infraestructura de TI, donde se justifique el dimensionamiento de la arquitectura para el mejor aprovechamiento de los recursos adquiridos y disponibles. • Es necesario que el proceso esté bien organizado y llegue a ser proactivo. • El proceso de Adquisición y Mantenimiento de la Infraestructura de TI debe estar alineado con las aplicaciones críticas del negocio y la infraestructura tecnológica. • Establecer políticas y procedimientos que especifiquen que la Infraestructura de TI es un apoyo clave para el uso de TI dentro de la empresa.	

Tabla 3-12Resumen de resultados AI4

AI4 Facilitar la Operación y el Uso	**Grado de Madurez** *DOS*
CONCLUSIÓN FINAL:	
• No están formalizados ni documentados los procedimientos y la calidad de soporte al usuario. • No existe bien definido un plan de entrenamiento general.	
RECOMENDACIONES FINALES:	
• Implementar un proceso donde se detalle actualizaciones de procedimientos y material de entrenamiento. • Revisar la documentación y los procedimientos con el fin de ser proactivos ante errores o problemas que puedan presentarse. • Todos los procedimientos ya sean de mantenimiento o entrenamiento estén bien documentados para todos los sistemas y unidades del negocio. • La documentación debe estar a un buen nivel, de tal manera que sea predecible, confiable y disponible.	

• Se debe determinar controles y estándares para todos los procedimientos.

Tabla 3-13Resumen de resultados AI5

AI5 Adquirir Recursos de TI	**Grado de Madurez** *CUATRO*
CONCLUSIÓN FINAL:	
• No se encuentra bien definida una Administración estratégica de relaciones. • No existen reportes donde se evidencie los objetivos de la empresa.	
RECOMENDACIONES FINALES:	
• Realizar reportes de los objetivos del negocio. • Cumplir y reforzar los estándares, políticas y procedimientos de adquisición de recursos de TI. • Mejoramiento continuo en la administración de adquisiciones y contratos. • Manejar las relaciones estratégicas con los proveedores.	

Tabla 3-14Resumen de resultados DS1

DS1 Definir y Administrar Niveles de Servicio	**Grado de Madurez** *DOS*
CONCLUSIÓN FINAL:	
• En la Empresa EA no se ha asignado un coordinador para los niveles de servicio, con responsabilidades definidas.	
RECOMENDACIONES FINALES:	
• Asignar un responsable para los niveles de servicio, con la finalidad de que se establezcan puntos de control para el cumplimiento de los mismos y de esta forma también satisfacer a los clientes. • Definir y documentar los niveles de servicio que se utilizarán a través de un proceso estándar. • En la administración de niveles de servicio las medidas tomadas deben estandarizarse y se mantenerse en mejora continua, teniendo en consideración que se incluya disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, soporte al usuario, planeación de continuidad y seguridad.	

Tabla 3-15Resumen de resultados DS5

DS5 Garantizar la Seguridad de los Sistemas	Grado de Madurez *TRES*
CONCLUSIÓN FINAL:	
• No existe formalmente un Plan de Seguridad de TI, se necesita reforzar las políticas, procedimientos y asignación de responsables para mejorar este proceso.	
RECOMENDACIONES FINALES:	
• Implementar un Plan de Seguridad de TI, donde se asigne responsables para su cumplimiento. • Realizar periódicamente un análisis de impacto y de riesgos de seguridad de TI. • Aplicar pruebas de seguridad con el fin de encontrar y solucionar posibles problemas. • Evaluar regularmente la implementación del Plan de Seguridad para determinar si cumple o no establecido, y además en el caso de tener nuevos requerimientos puedan ser implementados. • Establecer políticas y procedimientos para fortalecer la seguridad de TI en la empresa. • Obtener certificaciones de seguridad con la finalidad de cumplir con estándares y mantener un alto nivel de seguridad.	

Tabla 3-16Resumen de resultados DS7

DS7 Educar y Entrenar a los Usuarios	Grado de Madurez *CUATRO*
CONCLUSIÓN FINAL:	
• El personal de la empresa recibe entrenamiento sobre conducta, concienciación y prácticas de seguridad de en los sistemas pero de manera informal.	
RECOMENDACIONES FINALES:	
• Formalizar y documentar las prácticas y procedimientos de entrenamiento a los	

empleados.
- Investigar técnicas y estrategias que faciliten el entrenamiento y educación de los usuarios.
- Analizar los problemas para identificar las causas y tomar acciones correctivas al respecto.
- Los procesos se deben afinar y mantener en mejora continua basándose en las mejores prácticas y estándares de la industria.

Tabla 3-17Resumen de resultados DS10

DS10 Administrar los Problemas	Grado de Madurez *TRES*
CONCLUSIÓN FINAL:	
• No se estandarizan los procesos de escalamiento y resolución de problemas.	
RECOMENDACIONES FINALES:	
• Implementar un Plan de Administración de Problemas tomando en cuenta todos los aspectos clave de la organización. • Estandarizar los procesos de escalamiento y resolución de problemas. • La Administración de Problemas necesita alcanzar un nivel en el que se convierta en un proceso proactivo y preventivo, contribuyendo así son los objetivos del negocio. • Establecer indicadores clave de metas y desempeño sean medidos de manera consistente para el mejoramiento continuo del proceso.	

Tabla 3-18Resumen de resultados DS13

DS13 Administrar las Operaciones	Grado de Madurez *TRES*
CONCLUSIÓN FINAL:	
• No se desarrolla una política formal para reducir en número de eventos no programados.	
RECOMENDACIONES FINALES:	
• Desarrollar una política formal para reducir el número de eventos no programados. • Programar tareas y responsabilidades que sean documentadas y comunicadas a la función interna de TI e interesados. • Monitorear las actividades diarias con acuerdos estandarizados con el fin de	

cumplir los niveles de servicio que se establezcan.

- Alineación de los procesos de administración de problemas, capacidad y disponibilidad.
- Todos los problemas y fallas deben ser analizados con el fin de identificar las causas de su origen.

Tabla 3-19Resumen de resultados ME1

ME1 Monitorear y Evaluar el Desempeño de TI	**Grado de Madurez** *DOS*
CONCLUSIÓN FINAL:	
• Los procedimientos de monitoreo son ad hoc, al momento se usan herramientas disponibles para los sistemas e infraestructura pero no ha sido un proceso formalizado y considere métricas y aspectos clave para monitoreo.	
RECOMENDACIONES FINALES:	
• Implementar un proceso estándar y herramientas de monitoreo para los procesos y niveles de servicio. • Realizar de manera regular una comparación entre el desempeño de TI y las metas del negocio. • Realizar reportes de los resultados obtenidos para que la Gerencia de TI esté informada del cumplimiento de las metas. • Las herramientas automatizadas deben estar integradas y ser de ayuda para toda la organización en la recolección y monitoreo de la información.	

Tabla 3-20Resumen de resultados ME4

ME4 Proporcionar Gobierno de TI	**Grado de Madurez** *TRES*
CONCLUSIÓN FINAL:	
• La Empresa EA no ha definido tableros de control como parte de los BSC. • Todos los procedimientos no están documentados y estandarizados. • No está bien definido y documentado un conjunto de indicadores para medir el desempeño y evaluar sus resultados.	

RECOMENDACIONES FINALES:
• Implementar y registrar indicadores de desempeño de todas las actividades de gobierno de TI. • Definir tableros de control como parte del BSC. • Establecer acuerdos de nivel de servicio donde se defina y supervise las responsabilidades con el cliente.

3.4 INFORME EJECUTIVO

El presente informe muestra los resultados de la evaluación de los procesos obtenidos en la Auditoría de Gestión de TIC'S basada en la metodología COBIT 4.1.

En la Tabla 3-21 se detalla el nivel de madurez en el que se encuentra cada uno de los procesos.

Tabla 3-21 Resumen de los Niveles de Madurez de los procesos evaluados.

PROCESO		NIVEL DE MADUREZ
PO1	Definir un plan estratégico de TI.	4
PO2	Definir la arquitectura de la información.	3
PO3	Determinar la dirección tecnológica.	3
PO4	Definir procesos, organización y relaciones de TI.	3
PO6	Comunicar las aspiraciones y la dirección de la gerencia.	3
PO7	Administrar recursos humanos de TI.	3
PO9	Evaluar y administrar riesgos de TI.	2
PO10	Administrar proyectos.	3
AI2	Adquirir y mantener el software aplicativo.	4
AI3	Adquirir y mantener la infraestructura tecnológica.	3
AI4	Facilitar la operación y el uso.	2
AI5	Adquirir recursos de TI.	4
DS1	Definir y administrar niveles de servicio.	2
DS5	Garantizar la seguridad de los sistemas.	3
DS7	Educar y entrenar a los usuarios.	4
DS10	Administrar los problemas.	3
DS13	Administrar las operaciones.	3

ME1	Monitorear y evaluar el desempeño de TI.	2
ME4	Proporcionar gobierno de TI.	3

Los niveles de madurez tomados como referencia son:

0 No Existente.- No se ha reconocido la necesidad de implementar un proceso.

1 Inicial.- Se ha reconocido los problemas pero se los maneja de manera ad hoc.

2 Repetible.- Se han desarrollado los procesos y se siguen procedimientos similares, además no hay procedimientos formales.

3 Definido.- Los procedimientos han sido estandarizados y documentados, estos procedimientos formalizan las prácticas existentes.

4 Administrado.- Los procesos son monitoreados y se mide su cumplimiento.

5 Optimizado.- Los procesos se han refinado hasta un nivel de mejor práctica.

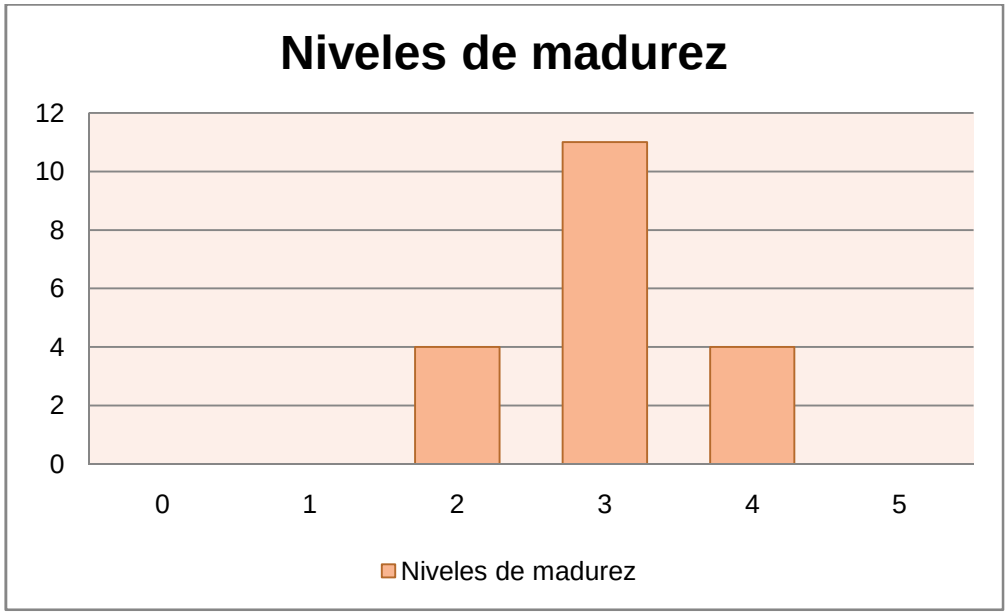

Figura 3-2 Resultados obtenidos de los Niveles de Madurez

En la figura 3-2 se puede visualizar que en su mayoría los procesos evaluados se encuentran en el nivel *3 Definido*.

Los resultados obtenidos nos permiten conocer el nivel en el que se encuentra cada dominio, para obtener el nivel del dominio se tomará en cuenta el nivel de madurez más bajo de los procesos que se encuentran dentro de este.

Luego de haber identificado el nivel más bajo obtenido en los cuatro dominios, se puede establecer que la Empresa EA en general se encuentra en un *nivel 2 (Repetible pero Intuitivo).*

La Empresa EA según lo establece COBIT, en este nivel se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

Como plan de mejoramiento de los procesos a corto plazo se debe empezar subiendo todos los procesos que se encuentran en un *nivel 2* a un *nivel 3(Definido)*con el uso de las estrategias presentadas en este trabajo,terminado este plan se debe trabajar para alcanzar el siguiente nivel superior con la finalidad que se lleguen a estandarizar todos los procesos de la empresa.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- El marco de referencia COBIT 4.1 me permitió desarrollar este trabajo satisfactoriamente ya que presenta el material necesario para entender, evaluar y tomar medidas para mejorar el desempeño de los procesos; para esto fue necesario identificar el nivel de madurez en que se encuentra cada proceso y mediante los objetivos de control que presenta COBIT,dar recomendaciones para que la empresa auditada tome esto en consideración y de esta manera los procesos estén en el nivel inmediato superior.

- Esta auditoría permite a la empresa tomar medidas correctivas en los procesos que necesitan ser atendidos con mayor brevedad para el mejor funcionamiento de los mismos.

- Con el uso de esta herramienta, las guías de auditoría que presenta COBIT y la colaboración del área de Tecnologías de la Información de la empresa

auditada, se ha obtenido el nivel de madurez de los procesos evaluados, lo cual ha permitido definir conclusiones y recomendaciones para mejorar el desempeño de los procesos de la empresa de aviación.

- Esta auditoría ha dado como resultado que los procesos evaluados en el área de TI de la empresa de aviación se encuentran en un nivel de madurez entre 2 y 4, lo que demuestra que los procesos han sido identificados, pero en su mayoría no siguen procedimientos formales y no se maneja la administración de procesos importantes, por esta razón es necesario tomar en cuenta el *Análisis de los Resultados* presentado, con el fin de obtener un mejor manejo de los procesos.

- Los resultados obtenidos en esta auditoría fueron entregadosen el informe preliminar a la empresa de aviación, los mismos que han sido de ayuda para que la empresa identifique los procesos que necesitan ser atendidos a corto y largo plazo, por tal motivo la empresa ha decidido utilizar herramientas con el fin de optimizar los procesos.

- En la realización de esta auditoría también se ha identificado la falta de documentación y formalización de procesos en las áreas de Ingeniería de Software e Infraestructura Tecnológica.

- La empresa no ha identificado la necesidad de la Administración de diferentes procesos, para lo cual es necesario revisar las recomendaciones que han sido basadas en el marco de trabajo COBIT 4.1, las mismas que se presentan en el *Informe Técnico* con el fin de que se tomen medidas para el mejoramiento de los procesos.

- La realización de este trabajo ha sido posible gracias a las entrevistas realizadas, la colaboración de la empresa entregando información necesaria y en otros casos con explicaciones del personal para conocer y entender cómo se manejan los procesos de la empresa.

4.2 RECOMENDACIONES

- Se recomienda tomar en consideración los Objetivos de control presentados por COBIT ya que este marco de trabajo nos permite tener una mejor administración y manejo de los procesos

- Es necesario que la Gerencia de TI tome en consideración las sugerencias entregadas en este trabajo para cada proceso evaluado, con la finalidad de que los procesos obtengan cambios significativos.

- Luego de la implementación de controles para cada proceso es necesario que se realice una Auditoría cada cierto tiempo, con el fin de volver a evaluar los procesos y esto permita que los procesos obtengan un mejor desempeño y se estandaricen.

- Se recomienda que los procesos se mantengan monitoreados y en mejora continua para tomar medias a tiempo en el caso de que existan nuevas necesidades.

- Se recomienda tomar como guía este trabajo para futuras auditorías que puedan realizarse a empresas de la misma naturaleza.

BIBLIOGRAFÍA

- LLUMIHUASI Juan. Auditoría de la Gestión de las Tecnologías de la Información en el Gobierno Municipal de San Miguel de Urcuquí utilizando como modelo de referencia COBIT 4.0. Escuela Politécnica Nacional, Facultad de Ingeniería de Sistemas. 2010.
- CARRIÓN Mayra del Cisne, CORONADO Luz. Auditoría de Gestión de TIC'S para la empresa DIPAC utilizando COBIT. Escuela Politécnica Nacional, Facultad de Ingeniería de Sistemas. 2008.
- CILIO Pablo, MUÑOZ Javier. Evaluación y Propuesta de Mejora de los Procesos TI pertenecientes al dominio de Entrega y Soporte del Modelo COBIT 4.1 en el Departamento de Tecnologías de la Información de una Empresa Comercial. Escuela Politécnica Nacional, Facultad de Ingeniería de Sistemas. 2012.
- DEL HIERRO Pablo, TRUJILLO Freddy. Auditoría del Sistema Informático del Hospital del Sur "Enrique Garcés". Escuela Politécnica Nacional. Facultad de Ingeniería de Sistemas. 2012.
- JARA Sayuri. Auditoría Informática de la Gestión de TI para la Empresa "AdvanceConsulting" utilizando el Modelo COBIT. Ponificia Universidad Católica del Ecuador, Facultad de Ingeniería, Escuela de Sistemas. 2012.
- IT GovernanceInstitute. COBIT 4.1. 2007.

- ITGovernance Institute.Cobit Control Practices. Guidance to Achieve Control Objectives for Successful IT Governance. 2nd Edition. 2007.
- COBITSteering Committee, IT Governance Institute. Cobit Audit Guidelines. 3rd Edition. July 2000
- OSIATIS. ITIL V3. http://itilv3.osiatis.es/.
- SAÁ Diego. Glosario de Términos de Gestión de TIs. September1, 2011.

GLOSARIO

Los siguientes Conceptos han sido tomados del *Documento de COBIT 4.1*[1] y del *Glosario de Términos de Gestión de TIs*[2].

- **Actividad.-** Las medidas principales tomadas para operar el proceso COBIT.
- **Administración de la configuración.-** El control de cambios realizados a un conjunto de componentes de la configuración a lo largo del ciclo de vida del sistema.
- **Administración del desempeño.-** La capacidad de administrar cualquier tipo de medición incluyendo mediciones de empleados, equipo, proceso, operativas o financieras. El término denota un control de ciclo cerrado y la vigilancia periódica de la medición.
- **Alineamiento de objetivos.-** Se define como el balance entre los objetivos de la Organización y los objetivos planteados por el área de TI.
- **Arquitectura de TI.-** Un marco integrado para evolucionar o dar mantenimiento a TI existente y adquirir nueva TI para alcanzar las metas estratégicas y de negocio de la empresa.

[1] Documento de COBIT 4.1, APÉNDICE VII, GLOSARIO
[2] SAÁ Diego, Glosario de Términos de Gestión de TIs. September 1, 2011.

- **Autenticación.-** El acto de verificar la identidad de un usuario y su elegibilidad para acceder a la información computarizada. La autenticación está diseñada para proteger contra conexiones de acceso fraudulentas.
- **BalancedScorecard.-** Un método para medir las actividades de una empresa en términos de su visión y estrategias, proporcionando una vista rápida e integral del desempeño del negocio a la gerencia. Es una herramienta administrativa cuyo fin es medir un negocio desde las siguientes perspectivas: financiera, del cliente, del negocio y del aprendizaje.
- **Capacidad.-** Contar con los atributos necesarios para realizar o lograr.
- **Cliente.-** Una persona o entidad externa o interna que recibe los servicios empresariales de TI.
- **COBIT**(Control OBjectivesforInformation and RelatedTechnology).- Objetivos de Control para Información y Tecnologías Relacionadas. Es un estándar abierto producido por ISACA (TheInformationSystemAudit and Control Association and Foundation) cuyo enfoque se centra en el Gobierno de TI tomando en cuenta aspectos de Auditoría y operaciones de TI. Se basa en tres dimensiones básicas: Requerimientos del Negocio, Recursos de TI y Procesos de TI.
- **Continuidad.-** Prevenir, mitigar y recuperarse de una interrupción. Los términos “planear la reanudación del negocio”, “planear la recuperación después de un desastre” y “planear contingencias” también se pueden usar en este contexto; todos se concentran en los aspectos de recuperación de la continuidad.
- **Control Interno.-** Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una garantía razonable de que los objetivos del negocio se alcanzarán y de que los eventos indeseables serán prevenidos o detectados y corregidos.
- **Desempeño.-**La implantación real o el logro de un proceso.
- **Diccionario de datos.-**Un conjunto de meta-datos que contiene definiciones y representaciones de elementos de datos.
- **Dominio.-**Agrupación de objetivos de control en etapas lógicas en el ciclo de vida de inversión en TI.

- **Empresa.-** Un grupo de individuos que trabajan juntos para un fin común, por lo general dentro del contexto de una forma organizacional, como una corporación agencia pública, entidad de caridad o fondo.
- **Estándar.-** Una práctica de negocio o producto tecnológico que es una práctica aceptada, avalada por la empresa o por el equipo gerencial de TI. Los estándares se pueden Implementar para dar soporte a una política o a un proceso, o como respuesta a una necesidad operativa. Así como las políticas, los estándares deben incluir una descripción de la forma en que se detectará el incumplimiento.
- **Gestión de Disponibilidad.-** Es responsable de optimizar y monitorizar los servicios de TI para que estos funcionen ininterrumpidamente y de manera fiable, cumpliendo los SLAs y todo ello a un costo razonable.
- **Gestión de Nivel de Servicio.-** Es el proceso por el cual se define, negocia y supervisa la calidad de los servicios de TI ofrecidos. Es responsable de buscar un compromiso realista entre las necesidades y expectativas del cliente y los costes de los servicios asociados, de forma que estos sean asumibles tanto por el cliente como por la organización de TI. Además debe velar por la calidad de los servicios de TI, alineando tecnología con procesos del negocio y todo ello a unos costes razonable.
- **Gestión de Riesgos**.- Es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias para manejarlo y mitigación del riesgo utilizando recursos gerenciales.
- **Gobierno.-** El método por medio del cual una organización es dirigida, administrada o controlada.
- **Gobierno de TI.-** Es el conjunto de acciones que realiza el área de TI en coordinación con la alta dirección para movilizar sus recursos de la forma más eficiente en respuesta a requisitos regulatorios, operativos o del negocio.
- **Incidente.-** Cualquier evento que no sea parte de la operación estándar de un servicio que ocasione, o pueda ocasionar, una interrupción o una reducción de la calidad de ese servicio (alineado a ITIL).

- **Infraestructura.-** La tecnología, los recursos humanos y las instalaciones que permiten el procesamiento de las aplicaciones.
- **ITIL**.- (Information Technology Infrastructure Library). Conjunto de conceptos y prácticas para la gestión de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general.
- **KGI (Key GoalIndicators).-** Son los indicadores clave de metas, los cuales representan mediciones para informar a la dirección general si un determinado proceso de TIC ha alcanzado sus requisitos de negocio.
- **KPI(Key Performance Indicators).-** Son los indicadores clave de rendimiento, los cuales determinan el rango ´óptimo de rendimiento que la empresa debe procurar alcanzar para cumplir sus objetivos.
- **Madurez.-** Indica el grado de confiabilidad o dependencia que el negocio puede tener en un proceso, al alcanzar las metas y objetivos deseados.
- **Métrica.-**Un estándar para medir el desempeño contra la meta.
- **Objetivo de control.-** Una declaración del resultado o propósito que se desea alcanzar al Implementar procedimientos de control en un proceso en particular.
- **Organización.-** La manera en que una empresa está estructurada.
- **Plan de infraestructura tecnológica.-** Un plan para el mantenimiento y desarrollo de la infraestructura tecnológica.
- **Plan estratégico de TI.-** Un plan a largo plazo, Ej., con un horizonte de tres a cinco años, en el cual la gerencia del negocio y de TI describen de forma cooperativa cómo los recursos de TI contribuirán a los objetivos estratégicos empresariales (metas).
- **Plan táctico de TI.-** Un plan a mediano plazo, Ej., con un horizonte de seis a dieciocho meses, que traduzca la dirección del plan estratégico de TI en las iniciativas requeridas, requisitos de recursos y formas en las que los recursos y los beneficios serán supervisados y administrados.
- **Política.-** Por lo general, un documento que ofrece un principio de alto nivel o una estrategia a seguir. El propósito de una política es influenciar y guiar la toma de decisiones presente y futura, haciendo que estén de acuerdo a la filosofía, objetivos y planes estratégicos establecidos por los equipos

gerenciales de la empresa. Además del contenido de la política, esta debe describir las consecuencias de la falta de cumplimiento de la misma, el mecanismo para manejo de excepciones y la manera en que se verificará y medirá el cumplimiento de la política.

- **Portafolio.-** Una agrupación de programas, proyectos, servicios o activos seleccionados, administrados y vigilados para optimizar el retorno sobre la inversión.
- **Problema.-** Causa subyacente desconocida de uno o más incidentes
- Procedimiento.-Una descripción de una manera particular de lograr algo; una forma establecida de hacer las cosas; una serie de pasos que se siguen en un orden regular definido, garantizando un enfoque consistente y repetitivo hacia las actividades.
- **Proceso.-** Por lo general, un conjunto de procedimientos influenciados por las políticas y estándares de la organización, que toma las entradas provenientes de un número de fuentes, incluyendo otros procesos, manipula las entradas, y genera salidas, incluyendo a otros procesos, para los clientes de los procesos. Los procesos tienen razones claras de negocio para existir, dueños responsables, roles claros y responsabilidades alrededor de la ejecución del proceso, así como los medios para medir el desempeño.
- **Programa.-** Una agrupación estructurada de proyectos independientes que incluye el alcance completo del negocio, del proceso, de las personas, de la tecnología y las actividades organizacionales que se requieren (tanto necesarias como suficientes) para lograr un resultado de negocios claramente especificado.
- **Proveedor de servicios.-** Organización externa que presta servicios a la organización.
- **Proyecto.-** Un conjunto estructurado de actividades relacionadas con la entrega de una capacidad definida a la organización (la cual es necesaria, aunque no suficiente para lograr un resultado de negocios requerido) con base en un cronograma y presupuesto acordado.

- **Recursos.-** Son los insumos de la empresa, además de ser necesarios para alcanzar los objetivos de las TI. Según COBIT se clasifican en: aplicaciones, información, infraestructura y personal.
- **Requerimientos del Negocio.-** Consisten en Efectividad, Eficiencia, Confidencialidad, Integridad, Disponibilidad, Cumplimiento y Confiabilidad. Estos requerimientos deben estar debidamente alcanzados a través de los Objetivos de TI.
- **Riesgo.-** El potencial de que una amenaza específica explote las debilidades de un activo o grupo de activos para ocasionar pérdida y/o daño a los activos. Por lo general se mide por medio de una combinación del impacto y la probabilidad de ocurrencia.
- **SLA.-** Acuerdo de nivel de servicio. Acuerdo por escrito entre un proveedor de servicios y los usuarios del cliente, el cual documenta los niveles de servicio acordados para un servicio prestado.
- **Tablero de control.-** Una herramienta para establecer las expectativas de una organización en cada nivel y para comparar de forma continua el desempeño contra las metas establecidas.
- **TI.-** Tecnología de información.
- **Usuario.-** Una persona que utiliza los sistemas empresariales.

ANEXOS

Anexo1: Entrevistas realizadas al personal de la empresa

Entrevista 1

Gerencia de TI

1. ¿Qué servicios brinda la empresa?
2. ¿Cómo está estructurada el área de tecnologías de la Información?
3. ¿Existe una planificación estratégica?
4. ¿Cómo se realiza el Plan Estratégico? ¿Quiénes son los involucrados? ¿Cómo se comunica al personal?
5. ¿La planificación estratégica de TI se comparte con la gerencia del negocio según se necesite?
6. ¿Cada cuánto tiempo se reestructura la planificación estratégica?
7. ¿Para la contratación de personal interviene el área de TI?
8. ¿Cuántas personas conforman el área de TI?
9. ¿El personal recibe capacitaciones? ¿Cada qué tiempo?

10. ¿Cómo se manejan las vacaciones del personal?
11. ¿Cómo se maneja la seguridad personal, física, legal, lógica y de datos en la empresa?
12. ¿A qué problemas se ha enfrentado el área de TI?

Entrevista 2

Infraestructura TI

1. ¿Qué funciones cumple el área de Infraestructura de TI?
2. ¿Cómo es la Topología de la red o un esquema?
3. ¿Qué políticas de seguridad se manejan?
4. ¿Existe seguridad al acceso a servidores?
5. ¿Qué sistemas operativos que usan para servidor/usuario?
6. ¿El software es licenciado?
7. ¿Existe detección de vulnerabilidades?
8. ¿Existe restricción de usuarios que se conectan a la red, fuera de la frontera de la organización?
9. ¿Cuál es la hora de mayor carga?
10. ¿Qué problemas que han sido afrontados por esta área?
11. ¿Cuántas personas trabajan en el área?
12. ¿Existen planes de adquisición y mantenimiento de la Arquitectura de TI?

Entrevista 3

Ingeniería de SW

1. ¿Qué funciones desempeña esta área?
2. ¿Cuántas personas trabajan en el área?
3. De qué tipo son las aplicaciones que presentan:desarrolladas aquí o adquiridas.
4. A las tienen: soporte, mantenimiento, tienen el código fuente, manuales de usuario.
5. ¿Qué seguridad en los sistemas existe?
6. ¿Qué problemas que han sido afrontados por esta área?
7. ¿Existe personal clave?
8. ¿Se da capacitación a los usuarios para el uso de las aplicaciones?
9. ¿Cómo se manejan los cambios de requerimientos?
10. ¿Se satisface los requisitos del usuario?
11. ¿Existe documentación de todas las aplicaciones?
12. ¿Existen políticas para la adquisición de SW?
13. ¿Cómo se seleccionan los proveedores de SW?
14. ¿Existe una administración de contratos con los proveedores?

15. ¿Se realiza pruebas para probar que se soporta la carga?
16. ¿Cuál es el horario donde existe mayor carga?
17. ¿En qué lenguajes de programación se desarrolla y que metodologías de desarrollo de usan?

Entrevista 4

HelpDesk

1. ¿Qué funciones desempeña esta área?
2. ¿Cuántas personas trabajan en el área?
3. ¿Qué problemas que han sido afrontados por esta área?

Entrevista 5

1. ¿Existe una administración de datos definida formalmente?
2. ¿Existe planeación de la infraestructura tecnológica?
3. Antes de realizar una compra la gerencia está totalmente de acuerdo.
4. ¿Existe gestión de riesgos/ cambios?
5. ¿Las actividades de TI son reactivas o proactivas?
6. ¿Se define un ambiente de control interno?
7. ¿La división de roles y responsabilidades está definida formalmente?
8. ¿Existen políticas, procedimientos, estándares y procesos de cumplimiento?
9. ¿Se cubren temas clave para la empresa?
10. ¿Existe manejo de inventarios?
11. ¿Para los proyectos que se realizan se hace alguna evaluación de riegos o se implementa cuando se identifican los riegos?¿Existe un proceso definido?
12. ¿Existe gestión de proyectos? ¿Se toma en cuenta el impacto?
13. ¿Se define roles y responsabilidades para proyectos?

14. ¿Se hace un seguimiento al tiempo, gastos en equipo y presupuestos para proyectos?

Entrevista 6

Adquirir y mantener software aplicativo

1. ¿Existe un diseño y especificación de aplicaciones?
2. ¿Existe conciencia de la necesidad de contar con un proceso de adquisición y mantenimiento de aplicaciones?
3. ¿El mantenimiento es problemático?
4. ¿Se tiene consideración para la seguridad y disponibilidad de aplicaciones?
5. ¿Existe un proceso claro y definido para la adquisición y mantenimiento de software aplicativo?
6. ¿Este proceso va de acuerdo a la estrategia de TI y del negocio?
7. ¿Las actividades de mantenimiento se planean, programan y coordinan?
8. ¿Qué metodologías de desarrollo utilizan?¿Son flexibles?
9. ¿Existe un proceso de documentación?
10. ¿Las prácticas de adquisición y mantenimiento de software aplicativo se alinean con el proceso definido?

Adquirir y mantener Infraestructura Tecnológica

1. ¿Se realizan cambios en la infraestructura para cada nueva aplicación de acuerdo a un plan conjunto?
2. ¿Existe un ambiente diferente de producción y ambiente de prueba?
3. ¿Se considera la adquisición y mantenimiento de la infraestructura de TI como una estrategia definida para satisfacer las necesidades de las aplicaciones del negocio? ¿En qué porcentaje se lo realiza?
4. ¿Se maneja procedimientos formales?

Entrevista 7

Proceso DS1: Definir y Administrar los Niveles de Servicio

1. ¿Se tiene administración de los niveles de servicio?
2. ¿Existen reportes sobre los niveles de servicio?
3. ¿Existen puntos de control para determinar los niveles de servicio?
4. ¿Existen acuerdos para el cumplimiento de los niveles de servicio?
5. ¿Existe algún vínculo entre el nivel de servicio esperado y el contemplado?
6. ¿Los niveles de servicio están en la fase de definición de requerimientos del sistema y se incorporan en el diseño de la aplicación?
7. ¿Cuándo no se llevan a cabo los niveles de servicio se realiza un análisis causa-raíz?
8. ¿Los niveles de satisfacción del cliente son administrados y monitoreados?

Proceso DS5: Garantizar la seguridad de los sistemas

1. ¿Las responsabilidades y la rendición de cuentas están asignadas?
2. ¿Qué medidas están implementadas para soportar la administración de seguridad de TI?
3. ¿Existen reportes de seguridad de TI?
4. ¿Qué medidas o implementaciones se han realizado para mejorar la seguridad de la empresa?
5. ¿Existe monitoreo de los eventos? ¿Con qué frecuencia?
6. ¿La seguridad se lleva acabo de forma reactiva?
7. ¿Los sistemas producen información relevante respecto a seguridad? ¿Esta información es analizada?
8. ¿Existe un plan de seguridad de TI? ¿Qué aspectos están considerados?
9. ¿Se desarrolla pruebas de seguridad?

Proceso DS7: Educar y entrenar a los usuarios

1. ¿Se imparte clases formales acerca de temas como conducta ética, concienciación y prácticas de seguridad en los sistemas?

Entrevista 8

Proceso DS10: Administración de problemas

1. ¿Existe conciencia de administrar problemas?
2. ¿Se considera a los problemas e incidentes diferentes?
3. ¿La resolución de problemas son formales o informales?
4. ¿La administración de problemas se maneja en todos los niveles de la organización?
5. ¿Las responsabilidades sobre los problemas están claramente establecidas?
6. ¿Los métodos y procedimientos son documentados, comunicados y medidos para evaluar su efectividad?
7. ¿La mayoría de problemas están identificados, registrados? ¿Se ha iniciado la solución a esos problemas?

8. ¿Se han acordado metas y métricas para el proceso de administración de problemas?
9. ¿La administración de problemas es proactiva o reactiva t en qué casos?
10. ¿Existen reportes sobre los problemas, estos son analizados?
11. ¿La mayoría de los sistemas están equipados con mecanismos automáticos de advertencia y detección, los cuales son rastreados y evaluados de manera continua?
12. ¿Cómo se administra los niveles de servicio?
13. ¿Se realiza acuerdos de servicio con los clientes?
14. ¿Se cumplen los acuerdos de servicio?
15. ¿Existen medidas para garantizar la seguridad de TI implementadas?
16. ¿Hay reportes de seguridad de TI?
17. ¿La seguridad de TI es una responsabilidad conjunta con el negocio y gerencia de TI?

Entrevista 9

Proceso DS13: Administración de Operaciones

1. ¿La infraestructura de TI puede resistir y recuperarse a errores?
2. ¿Los procesos de operación son programados de manera formal o informal?
3. ¿Existe dependencia de las habilidades de los individuos?
4. ¿La programación de tareas se documenta, comunican tanto a la función interna de TI como a los clientes del negocio?
5. ¿Las operaciones de soporte de Ti son efectivas, eficientes y suficientemente flexibles para cumplir con las necesidades de niveles de servicio sin pérdida de productividad?
6. ¿Los procesos automatizados que soportan los sistemas contribuyen a tener un ambiente estable?

Anexo 2: Herramienta de Evaluación de Madurez de COBIT con la evaluación de los procesos realizado en la Empresa EA (anexo digital).

Anexo3: Informe Preliminar

Quito, 24 de junio de 2013

Ing. _ _ _ _ _ _ _ _ _ _ _ _ _
GERENTE DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA EMPRESA _ _ _ _
Presente.-

Me dirijo a usted con la finalidad de poner en consideración el trabajo de Auditoría de Gestión de TIC'S (Tecnologías de la Información y Comunicación) usando como modelo de referencia COBIT 4.1 (Control ObjectivesforInformation and RelatedTechnology) practicadas desde Enero de 2013 hasta Junio del 2013.

Auditora.
Priscila RocioCajamarca Erazo

El presente informe tiene la finalidad de dar a conocer los resultados de la Auditoría practicada a la empresa _ _ _ _ _ _ _ _, que en la Auditoría por razones de confidencialidad se la denominado EA(Empresa Aérea).

También se desea recolectar las observaciones que se puedan realizar al presente trabajo, por tal motivo se pone en consideración al equipo de TI de la empresa el presente informe.

REALIZACIÓN DE LA AUDITORÍA BASADA EN COBIT

Para la realización de este trabajo se ha utilizado la "Herramienta de Evaluación de Madurez de COBIT"[1] incluida en el kit de "Implementación y Mejora Continua del Gobierno de TI"[2], esta herramienta es presentada por COBIT para evaluar la madurez de los procesos de TI en una organización.

Se ha completado la información requerida por la herramienta antes mencionada, mediante entrevistas al personal de TI para obtener la información necesaria de cada uno de los procesos evaluados.

En el análisis de los procesos se debe tener las siguientes consideraciones que presenta la herramienta utilizada:

- En todos los procesos se analiza cada nivel de madurez (0 a 5).
- Existen sentencias para cada uno de los niveles. Se debe atribuir un factor de peso (1 a 10), este peso indica la importancia de cada una de las

[1] COBIT Maturity Assessment Tool, ISACA, 2009
[2] Implementing and Continually Improving IT Governance, ISACA, 2009

sentencias dentro de la organización y su ambiente externo. Por defecto, se tiene un peso de 5 para cada sentencia.

- Para las sentencias también debe indicarse en qué nivel se cumple (Está de acuerdo) con las siguientes escalas.
  - No se cumple.
  - Un poco.
  - En cierto grado.
  - Completamente.
- La multiplicación del peso por el nivel de cumplimiento de cada sentencia calcula la importancia relativa.
- Finalmente se obtiene la situación actual del proceso, debido a que esta herramienta calcula el nivel de cumplimiento, basándose en la importancia relativa y el peso de cada sentencia.

PO1: Definición de un Plan Estratégico de Tecnología de Información	***Grado de Madurez*** CUATRO
Estrategias a corto plazo: • Se recomienda que la planeación estratégica considere que todas las metas del negocio estén en alineación con las metas de TI. • Se debe evaluar el cumplimiento del Plan Táctico (Plan Anual) para determinar si se está obteniendo los resultados esperados, que sería el cumplimiento de las metas estratégicas y tácticas.	
Estrategias a largo plazo: • Se recomienda que la realización del Plan Estratégico y Táctico de TI se mantenga en mejora continua, tratando de cumplir normas bien definidas relacionadas al negocio.	

PO2: Definir la Arquitectura de la Información	***Grado de Madurez*** TRES

Estrategias a corto plazo:

- Se recomienda establecer metas y métricas para la evaluación del proceso de Desarrollo e Implementación de Arquitectura de la Información con el fin de mejorar el desempeño del mismo.

- Se debe establecer procedimientos para que este proceso sea proactivo y logre resolver necesidades futuras del negocio.

- El proceso de definición de Arquitectura de Información debe estar justificado formalmente, especificando las características y beneficios que se obtendrán con su implementación.

Estrategias a largo plazo:

- Se recomienda que la Arquitectura de Información sea reforzada de manera consistente a todos los niveles para conseguir una mejor administración del proceso.

- Se debe establecer tecnologías para la minería de datos.

- Es necesario implementar procedimientos formales donde se incluya la mejora continua del proceso y se considere toda la información de los procesos organizacionales y sistemas.

PO3: Determinar la Dirección Tecnológica	***Grado de Madurez*** TRES

Estrategias a corto plazo:

- Se recomienda formalizar un Plan de Infraestructura Tecnológica donde se especifiquen claramente los objetivos, riesgos, que este alineado con las estrategias del negocio y pueda ser sujeto a cambios.

- También se recomienda que se realicen evaluaciones acerca del uso de la tecnología para identificar los posibles riesgos.

Estrategias a largo plazo:

- Se recomienda que el Plan de Infraestructura Tecnológica este basado en estándares de la industria, para satisfacer las necesidades del negocio e implementar las mejores prácticas que sean relevantes para mejorar este proceso.

- También es necesario que se implemente políticas y procedimientos formales

para el desarrollo del Plan.

- Acceder a recursos externos para los casos que sean necesarios con la finalidad de tener mayor experiencia y las habilidades necesarias para cumplir con los objetivos del negocio y de TI.

PO4: Definir los procesos, organización y Relaciones de TI	***Grado de Madurez*** TRES

Estrategias a corto plazo:

- Se recomienda que se reforme la estructura organizacional de la empresa, donde la Gerencia de Tecnologías de Información se encuentre a un nivel asesor en la organización y de esta manera TI este alineada con toda la organización.
- Es necesario que se asignen roles y responsabilidades para fortalecer el manejo de Gestión de Riesgos y la Seguridad Informática.
- Se debe fortalecer las relaciones con terceros involucrando a los comités de la dirección, auditoría interna y administración de proveedores.

Estrategias a largo plazo:

- Se recomienda formalizar procedimientos para mejorar el desempeño y monitoreo de la organización y de los procesos de TI para que se mantenga en mejora continua y cumpla con los objetivos de la organización.

PO6: Comunicar las Aspiraciones y la Dirección de la Gerencia	***Grado de Madurez*** TRES

Estrategias a corto plazo:

- Se recomienda reforzar los controles de información, las políticas de control interno y que todas las políticas y procedimientos acordados sean informados a todo el personal de TI.
- Realizar un monitoreo para verificar que se cumpla todo lo establecido.
- Formalizar y estandarizar las técnicas de concienciación de seguridad.

Estrategias a largo plazo:

- Se recomienda implementar expertos internos y externos para garantizar que se adopten las mejores prácticas de la industria.

- También se recomienda implementar bases de conocimientos de políticas y de concienciación con la finalidad de optimizar la comunicación mediante la implementación de herramientas de automatización.

PO7: Administrar los Recursos Humanos de TI	***Grado de Madurez*** TRES
Estrategias a corto plazo: • Se recomienda la elaboración y mantenimiento de un Plan de Administración de Recursos Humanos de TI, que permita realizar revisiones del desempeño del personal para satisfacer los requerimientos del negocio. • Implementar métricas estandarizadas que le permiten identificar desviaciones.	
Estrategias a largo plazo: • Se recomienda que la Administración de Recursos Humanos de TI este integrada y responda a las estrategias del negocio. • El Plan de Administración de Recursos Humanos de TI se debe actualizar constantemente para cumplir con los cambiantes requerimientos del negocio.	

PO9: Evaluar y Administrar los Riesgos de TI	***Grado de Madurez*** DOS
Estrategias a corto plazo: • Se recomienda que se implemente políticas y procedimientos formales para la Administración de Riesgos de toda la organización. • Asignar roles y responsables de cada proceso con el fin de que los riesgos del negocio sean identificados, evaluados y se obtenga soluciones inmediatas.	
Estrategias a largo plazo: • Se recomienda que siga un proceso de Evaluación y Administración de Riesgos	

estandarizado.

- Para la mitigación de riesgos es necesario monitorear y evaluar individualmente cada proyecto de manera continua.

PO10: Administrar Proyectos	***Grado de Madurez*** TRES

Estrategias a corto plazo:

- Se recomienda que se establezca una oficina de Administración de Proyectos dentro de TI con roles y responsabilidades sobre los proyectos y programas desde su inicio hasta después de su implementación.
- Los proyectos necesitan ser monitoreados en puntos clave y se debe considerar métricas para verificar su cumplimiento.
- La administración de proyectos debe ser evaluada por la organización, no únicamente por TI.

Estrategias a largo plazo:

- Se recomienda que se implemente una metodología para el ciclo de vida de los proyectos con la finalidad de que se maneje las mejores prácticas para la Administración de Proyectos y de esta forma se pueda garantizar que los recursos de TI y del usuario son optimizados.

AI2: Adquirir y Mantener el Software Aplicativo	***Grado de Madurez*** CUATRO

Estrategias a corto plazo:

- Se recomienda que las prácticas de adquisición y software aplicativo se extiendan para toda la empresa.
- También se recomienda que la metodología de adquisición y mantenimiento sea reforzada para que se tenga un posicionamiento estratégico inmediato.

Estrategias a largo plazo: • Se recomienda que el proceso se mantenga en mejora continua con la finalidad de que soporte requerimientos cambiantes del negocio sin problema.

AI3: Adquirir y Mantener la Infraestructura Tecnológica	***Grado de Madurez*** TRES
Estrategias a corto plazo: • Se recomienda que se implemente un Plan de Adquisición y Mantenimiento de la Infraestructura de TI, donde se justifique el dimensionamiento de la arquitectura para el mejor aprovechamiento de los recursos adquiridos y disponibles. • Es necesario que el proceso esté bien organizado y llegue a ser proactivo.	
Estrategias a largo plazo: • El proceso de Adquisición y Mantenimiento de la Infraestructura de TI este alineado con las aplicaciones críticas del negocio y la infraestructura tecnológica. • Se recomienda se implemente políticas y procedimientos que especifiquen que la Infraestructura de TI es un apoyo clave para el uso de TI dentro de la empresa.	

AI4: Facilitar la Operación y el Uso	***Grado de Madurez*** DOS
Estrategias a corto plazo: • Se recomienda que se implemente un proceso donde se detalle actualizaciones de procedimientos y material de entrenamiento.	

• También es necesario se revise la documentación y los procedimientos con el fin de ser proactivos ante errores o problemas que puedan presentarse.
Estrategias a largo plazo: • Se recomienda que todos los procedimientos ya sea de mantenimiento o entrenamiento estén bien documentados para todos los sistemas y unidades del negocio. • La documentación debe estar a un buen nivel, de tal manera que sea predecible, confiable y disponible. • Se debe determinar controles y estándares para todos los procedimientos.

AI5: Adquirir Recursos de TI	***Grado de Madurez*** TRES
Estrategias a corto plazo: • Se recomienda que se realicen reportes de los objetivos del negocio. • Cumplir y reforzar los estándares, políticas y procedimientos de adquisición de recursos de TI de manera continua.	
Estrategias a largo plazo: • Se recomienda que exista una mejora continua en la administración de adquisiciones y contratos. • Manejar buenas relaciones estratégicas con los proveedores.	

DS1: Definir y Administrar Niveles de Servicio	***Grado de Madurez*** DOS
Estrategias a corto plazo: • Se recomienda que se asigne un responsable para los niveles de servicio con la	

finalidad de que se establezcan puntos de control para el cumplimiento de los mismos y de esta forma también satisfacer a los clientes. • Definir y documentar los niveles de servicio que se utilizarán a través de un proceso estándar.
Estrategias a largo plazo: • Se recomienda que para la administración de niveles de servicio las medidas tomadas se vayan estandarizando y se mantengan en mejora continua, teniendo en consideración que se incluya disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, soporte al usuario, planeación de continuidad y seguridad.

DS5: Garantizar la Seguridad de los Sistemas	***Grado de Madurez*** TRES
Estrategias a corto plazo: • Se recomienda que se implemente un Plan de Seguridad de TI, donde se asigne responsables para su cumplimiento. • Realizar periódicamente un análisis de impacto y de riesgos de seguridad de TI. • Aplicar pruebas de seguridad con el fin de encontrar y solucionar posibles problemas. • Evaluar regularmente la implementación del Plan de Seguridad para determinar si cumple o no establecido, y además en el caso de tener nuevos requerimientos puedan ser implementados.	
Estrategias a largo plazo: • Se recomienda establecer políticas y procedimientos para fortalecer la seguridad de TI en la empresa. • Obtener certificaciones de seguridad con la finalidad de cumplir con estándares y mantener un alto nivel de seguridad.	

DS7: Educar y Entrenar a los Usuarios	***Grado de Madurez*** CUATRO
Estrategias a corto plazo:	

- Se recomienda que se formalice y documente las prácticas y procedimientos de entrenamiento a los empleados.

- Investigar técnicas y estrategias que faciliten el entrenamiento y educación de los usuarios, con la finalidad de que alcanzar los objetivos de la organización.

Estrategias a largo plazo:

- Se recomienda que los procesos se afinen y se mantengan en mejora continua basándose en las mejores prácticas y estándares de la industria.

- Analizar los problemas para identificar las causas y tomar acciones correctivas al respecto.

DS10: Administrar los Problemas	***Grado de Madurez*** TRES

Estrategias a corto plazo:

- Se recomienda la implementación de un Plan de Administración de Problemas tomando en cuenta todos los aspectos clave de la organización.

- También se recomienda estandarizar los procesos de escalamiento y resolución de problemas.

Estrategias a largo plazo:

- Se recomienda que la Administración de Problemas evolucione a un nivel en el que se convierta en un proceso proactivo y preventivo, contribuyendo así son los objetivos del negocio.

- Establecer indicadores clave de metas y desempeño sean medidos de manera consistente para el mejoramiento continuo del proceso.

DS13: Administrar las Operaciones	***Grado de Madurez*** TRES

Estrategias a corto plazo: • Se recomienda desarrollar una política formal para reducir el número de eventos no programados. • Programar tareas y responsabilidades que sean documentadas y comunicadas a la función interna de TI e interesados. • Es necesario se monitoree las actividades diarias con acuerdos estandarizados con el fin de cumplir los niveles de servicio que se establezcan.	
Estrategias a largo plazo: • Se recomienda la alineación de los procesos de administración de problemas, capacidad y disponibilidad. • Todos los problemas y fallas deben ser analizados con el fin de identificar las causas de su origen.	

ME1: Monitorear y Evaluar el Desempeño de TI	***Grado de Madurez*** DOS
Estrategias a corto plazo: • Se recomienda que se implemente un proceso estándar de monitoreo y se defina herramientas para el monitoreo de los procesos y los niveles de servicio. • Efectuar regularmente una comparación entre el desempeño de TI con las metas del negocio.	
Estrategias a largo plazo: • Es necesario que se realicen reportes de los resultados obtenidos para que la Gerencia esté informada del cumplimiento de las metas. • Las herramientas automatizadas deben estar integradas y ser de ayuda para toda la organización en la recolección y monitoreo de la información.	

ME4: Proporcionar Gobierno de TI	***Grado de Madurez*** TRES
Estrategias a corto plazo: • Se recomienda que se implemente y se registre indicadores de desempeño de todas las actividades de gobierno de TI. • Definir tableros de control como parte del BSC.	
Estrategias a largo plazo: • Se debe establecer acuerdos de nivel de servicio donde se defina y supervise las responsabilidades con el cliente. • Reforzar temas de Gobierno de TI a todos los niveles y todo el personal debe estar al tanto para que se tome medidas en la mejora del proceso.	

ANÁLISIS DE LOS RESULTADOS

A continuación se realiza un análisis de los resultados obtenidos en la Auditoría de Gestión de TIC'S basada en la metodología COBIT 4.1.

En la tabla A-1 se muestra el reporte de niveles de madurez de cada uno de los procesos que han sido evaluados en la Empresa EA.

Tabla A-1 Reporte General de los Niveles de Madurez

DOMINIO	PROCESO		NIVEL DE MADUREZ
PLANEAR Y ORGANIZAR	**PO1**	Definir un plan estratégico de TI.	4
	PO2	Definir la arquitectura de la información.	3
	PO3	Determinar la dirección tecnológica.	3
	PO4	Definir procesos, organización y relaciones de TI.	3
	PO6	Comunicar las aspiraciones y la dirección de la gerencia.	3
	PO7	Administrar recursos humanos de TI.	3
	PO9	Evaluar y administrar riesgos de TI.	2
	PO10	Administrar proyectos.	3
ADQUIRIR E IMPLEMENTAR	**AI2**	Adquirir y mantener el software aplicativo.	4
	AI3	Adquirir y mantener la infraestructura tecnológica.	3
	AI4	Facilitar la operación y el uso.	2
	AI5	Adquirir recursos de TI.	4
ENTREGAR Y DAR SOPORTE	**DS1**	Definir y administrar niveles de servicio.	2
	DS5	Garantizar la seguridad de los sistemas.	3
	DS7	Educar y entrenar a los usuarios.	4
	DS10	Administrar los problemas.	3
	DS13	Administrar las operaciones.	3
MONITOREAR Y EVALUAR	**ME1**	Monitorear y evaluar el desempeño de TI.	2
	ME4	Proporcionar gobierno de TI.	3

En la Figura A-1se muestra los niveles de madurez actuales como se indica en la Tabla A-1 y los niveles de madurez futuros que se han que se han definido luego de la evaluación de cada proceso.

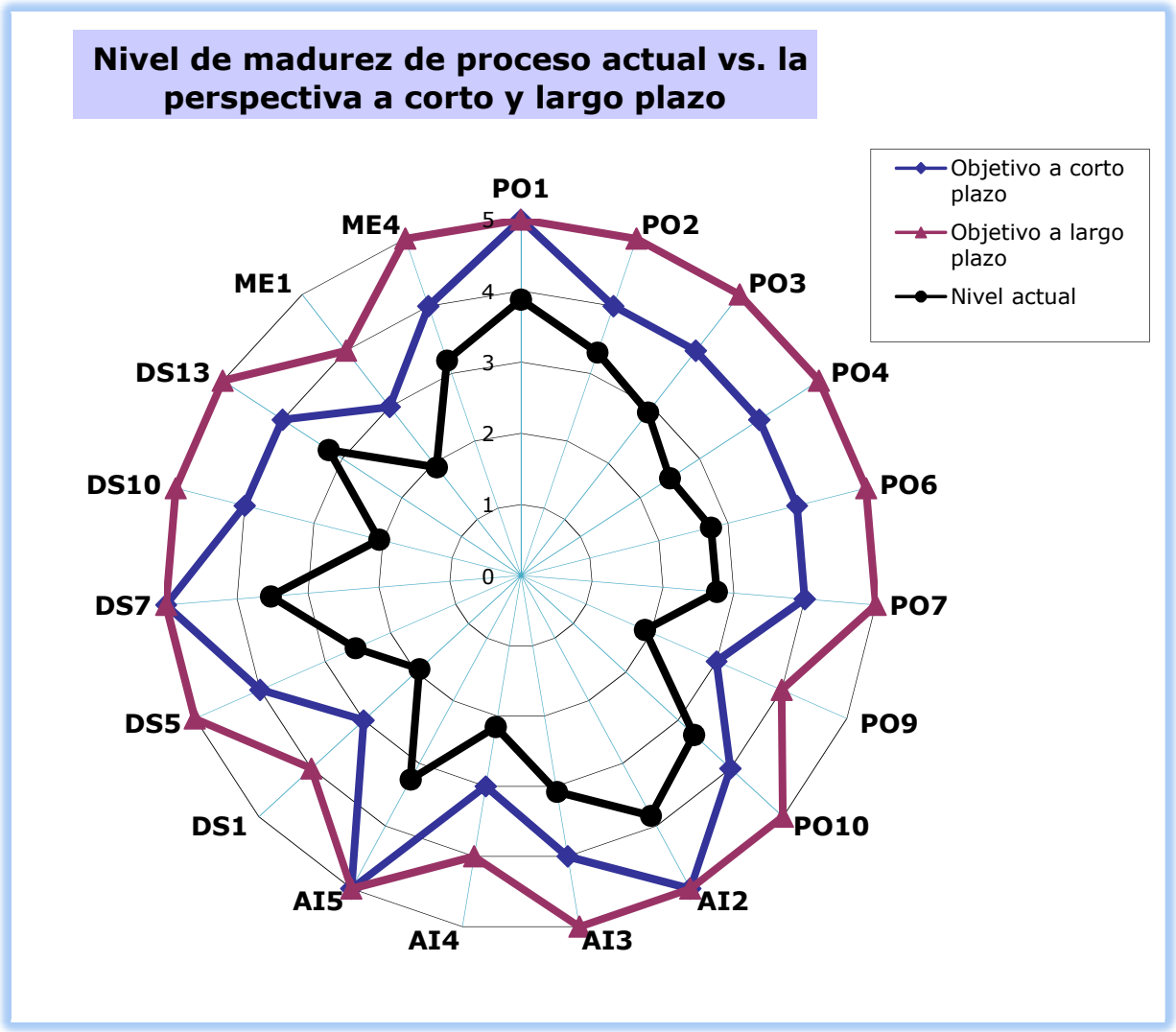

Figura A-1 Nivel de madurez de los procesos Actual vs. Futuro

Los resultados obtenidos nos permiten conocer el nivel en el que se encuentra cada dominio, para obtener el nivel del dominio se tomará en cuenta el nivel de madurez más bajo de los procesos que se encuentran dentro de este.

Considerando el nivel más bajo de los procesos, se ha obtenido el nivel en que se encuentran los cuatro dominios como se detalla a continuación:

- Planificar y Organizar: Nivel 2
- Adquirir e Implementar: Nivel 2
- Entregar y Dar Soporte: Nivel 2
- Monitorear y Evaluar: Nivel 2

Luego de haber identificado el nivel más bajo obtenido en los cuatro dominios, se puede establecer que la Empresa EA en general se encuentra en un *nivel 2 (Repetible pero Intuitivo).*

La Empresa EA según lo establece COBIT, en este nivel se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

Como plan de mejoramiento de los procesos a corto plazo se debe empezar subiendo todos los procesos que se encuentran en un *nivel 2* a un *nivel 3(Definido)*con el uso de las estrategias presentadas en este trabajo,terminado este plan se debe trabajar para alcanzar el siguiente nivel superior con la finalidad que se llegue a estandarizar todos los procesos de la empresa.