ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

AUDITORÍA DE RIESGOS INFORMÁTICOS DEL DEPARTAMENTO DE SISTEMAS DE TELEAMAZONAS USANDO COBIT

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

MARCIA IVETH CORDERO CALDERÓN
marciveth@hotmail.com
MARÍA DEL CARMEN IBUJÉS RIVERA
carmmy_ibujes@hotmail.com

DIRECTOR: M.SC. ING. JAIME NARANJO
naranjojf@server.epn.edu.ec

Quito, Abril 2008

DECLARACIÓN

Nosotras, Marcia Iveth Cordero Calderón y María del Carmen Ibujés Rivera, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado por ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la siguiente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por su normativa institucional vigente.

Marcia Iveth Cordero Calderón

María del Carmen Ibujés Rivera

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por, Marcia Iveth Cordero Calderón y María del Carmen Ibujés Rivera bajo mi supervisión.

M.Sc. Ing. Jaime Naranjo
DIRECTOR DE PROYECTO

AGRADECIMIENTO

Primeramente a Dios por su infinita generosidad, al permitirme a mí y a todos mis seres queridos ver cumplida una de mis metas profesionales.

A mi amada hija Eliana Sarahí, mis queridos padres Humberto e Isolina y mis ñañitos bellos Byron y Alejandro; por toda su paciencia y apoyo incondicional en cada momento de mi vida.

A nuestro tutor de Tesis Ing. Jaime Naranjo, por brindarnos su paciencia, apoyo y asesoría, que permitieron realizar y concluir con satisfacción el presente proyecto.

A la empresa TELEAMAZONAS especialmente al Departamento de Sistemas, por su colaboración y apoyo al brindarnos la información necesaria para el desarrollo de nuestro trabajo.

A Carmy, compañera de tesis y amiga incondicional; gracias por tu comprensión y apoyo.

A Jorge, Daniel, Mary, Paty, Pato y todos mis buenos amigos que han confiado siempre en mí y me han brindado todo su apoyo, los quiero mucho.

A todos mis tíos, primos y demás familiares que me apoyaron incondicionalmente y siempre están dándome ánimos y fuerzas para seguir adelante.

A todas las personas que de una u otra manera aportaron de manera desinteresada para que esta tesis llegue a feliz término.

Marcy C.

AGRADECIMIENTO

A DIOS, por permitirme ver cada nuevo amanecer, por guiar mi camino, y darme la fe de que todo es posible.

A mi madre Gloria, por su ayuda en todos los momentos de mi vida, por su apoyo y sacrificio, porque sin ella no hubiese sido posible conseguir esta meta, porque en los momentos más difíciles siempre está ahí para pronunciar un Te quiero, y darme cuenta que tengo una madre maravillosa, Gracias por todo Mamita.

A Jackeline, Anita, Iván, Marco, Guillermo, Vinicio, Leonidas y toda mi familia, por su amor y apoyo incondicional, por depositar su confianza en mí y expresar palabras de aliento en los momentos más difíciles, pues ese fue el impulso para seguir luchando.

De manera especial al Ing. Jaime Naranjo, por brindarnos su apoyo e invalorable asesoría, permitiendo concluir satisfactoriamente el presente proyecto.

A TELEAMAZONAS especialmente al Departamento de Sistemas por su colaboración y apertura al brindarnos la información necesaria para el desarrollo de nuestro trabajo.

A mi Patito, por estar en todo momento a mi lado, siendo un apoyo incondicional, por comprender mis aciertos y desaciertos.

A mi compañera de tesis y amiga Marcy, por haber compartido esta etapa tan importante para las dos y aunque fue difícil, lo logramos!!. A mis amigos y compañeros por todos aquellos momentos que compartimos juntos.

A unas niñas muy especiales, porque con su espontaneidad y cariño han llegado a ocupar un lugar muy especial en mi corazón. Gracias hermanas.

Carmmy I.

DEDICATORIA

Este trabajo está dedicado con todo mi amor y cariño a mi hija adorada Eliana Sarahí, hijita de mi corazón TE AMO con toda mi alma, gracias Dios por enviarme un angelito que guíe mi camino.

A mis padres Humberto e Isolina, por todo el amor, cariño y apoyo que nos han brindado en cada momento de nuestras vidas a mis hermanos y a mí, tengan por seguro que todo su sacrificio por vernos superarnos será recompensado, los amamos mucho.

A mis hermanos Byron y Alejandro, para que sigan adelante y venzan todas las dificultades que se presenten en la vida y que sepan que siempre cuentan conmigo.

A mis abuelitos: Mamita Carmen, Papá Alejandro, Mamita Rosa y Papá Manuel†; gracias por darme sus bendiciones diarias desde donde estén.

A mis grandes amigos del alma: Jorge, Daniel, Mary, Carmy, Paty, Pato y todos aquellos que la vida me dio la oportunidad de conocer y que sean parte de mi vida, gracias por apoyarme en las buenas y en las malas.

A la Familia Cordero y a la Familia Calderón, con mucho cariño a todos mis tíos y primos.

Marcy C.

DEDICATORIA

Dedico este trabajo especialmente a mi fuente de inspiración, mi Madre por ser ejemplo de amor y constancia, porque siempre ha demostrado su entereza y que con esfuerzo y dedicación conseguimos todo lo que nos proponemos, quisiera que este sea uno más de sus logros para demostrarse que su dedicación valió la pena.

A mi hermano Vinicio, y familia por brindarme su apoyo y creer en mí.

A mi ángel de la guarda, mi abuelita †, porque en todo momento siento su cálida presencia para darme su bendición y guiar mi camino.

A Pato E. por su apoyo y comprensión porque cumplimos lo que un día nos prometimos, por brindarme su amor y por ser el amor de mi vida.

Carmmy I.

CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN

Ignorar las amenazas y riesgos que acechan a las unidades informáticas o trivializarlas, es como jugar a la ruleta rusa: se puede ser afortunado durante algún tiempo, pero tarde o temprano esa fortuna terminará. Desgraciadamente, la mayoría de las amenazas son invisibles hasta que es demasiado tarde, mucho más si se hace referencia a los sistemas de información, los mismos que manejan activos tan intangibles como los datos y la información que se obtiene de estos.

El presente trabajo tiene como objeto realizar la Auditoria de Riesgos Informáticos en el Departamento de Sistemas de Teleamazonas usando COBIT. A continuación presentamos un resumen de su contenido:

CAPÍTULO 1:

Justificación teórica del uso del marco referencial COBIT y las herramientas utilizadas para la realización del presente trabajo de auditoría.

CAPÍTULO 2:

Aplicamos COBIT para realizar la auditoría; esto se obtiene después de hacer un mapeo entre la Norma ISO 17799 y COBIT; así como hacer uso de los modelos de madurez y una metodología propuesta por COSO para modelar el impacto de los objetivos de control sobre los recursos y criterios de TI.

CAPÍTULO 3:

Tomando como base lo obtenido en el capítulo 2, se elabora el Informe Final de Auditoría.

CAPÍTULO 4:

Finalmente se presenta conclusiones y recomendaciones obtenidas en base a la Auditoría de Riesgos Informáticos del Departamento de Sistemas de Teleamazonas.

PRESENTACIÓN

La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente. Esto es especialmente importante en el ambiente comercial cada vez más interconectado. Como resultado de esta creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades

La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales.

La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos.

Los requerimientos de seguridad se identifican mediante una evaluación metódica de los riesgos de seguridad. El gasto en controles debe ser equilibrado con el daño comercial probable resultado de fallas en la seguridad.

Los resultados de la evaluación del riesgo ayudarán a guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de seguridad de la información, e implementar los controles seleccionados para protegerse contra esos riesgos.

La evaluación del riesgo se debe repetir periódicamente para tratar cualquier cambio que puede influir en los resultados de la evaluación del riesgo.

CAPITULO 1

JUSTIFICACION DEL USO DE COBIT Y HERRAMIENTAS

1.1 JUSTIFICACIÓN DEL USO DEL MARCO REFERENCIAL COBIT

COBIT es un marco de referencia y un juego de herramientas de soporte que permiten a la gerencia cerrar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los participantes. COBIT permite el desarrollo de políticas claras y de buenas prácticas para control de TI a través de las empresas. COBIT constantemente se actualiza y armoniza con otros estándares. Por lo tanto, COBIT se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios asociados con TI. La estructura de procesos de COBIT y su enfoque de alto nivel orientado al negocio brindan una visión completa de TI y de las decisiones a tomar acerca de TI.

Los beneficios de implementar COBIT como marco de referencia de gobierno sobre TI incluyen:

- Mejor alineación, con base en su enfoque de negocios
- Una visión, entendible para la gerencia, de lo que hace TI
- Propiedad y responsabilidades claras, con base en su orientación a procesos
- Aceptación general de terceros y reguladores
- Entendimiento compartido entre todos los participantes, con base en un lenguaje común
- Cumplimiento de los requerimientos COSO[1] para el ambiente de control de TI.

[1]COSO: Comité de organizaciones patrocinadoras de la comisión Treadway Estándar aceptado a nivel internacional para el gobierno corporativo. FUENTE: Documento COBIT 4.0

En la siguiente figura (Figura 1) se muestra el Marco de Trabajo General de COBIT, con el modelo de procesos de COBIT compuesto de cuatro dominios que contienen 34 procesos genéricos, administrando los recursos de TI para proporcionar información al negocio de acuerdo con los requerimientos del negocio y de gobierno.

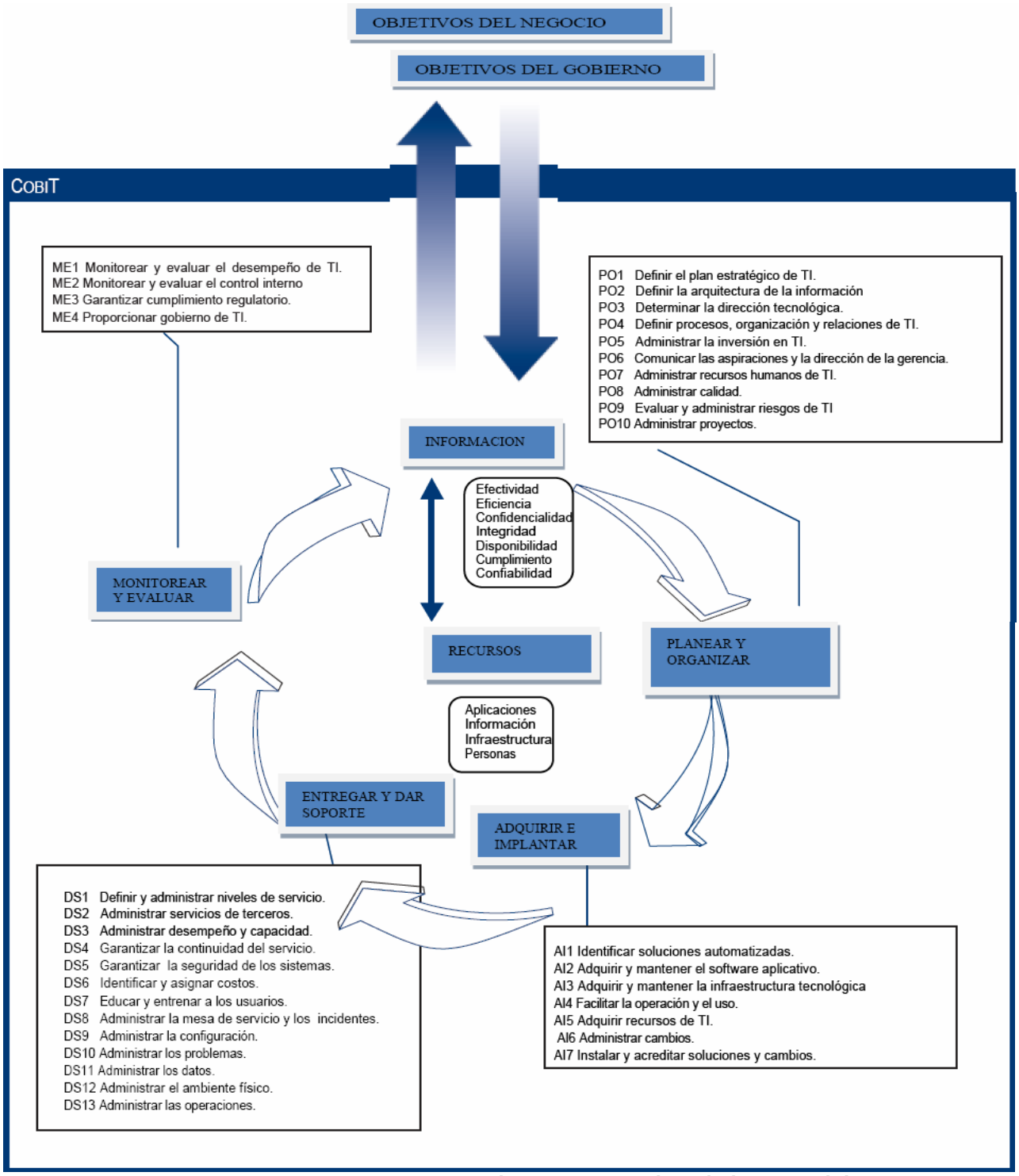

Figura 1: Marco de trabajo general de COBIT
Fuente: Documento COBIT 4.0

1.1.1 CRITERIOS DE INFORMACIÓN DE COBIT

Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio. Con base en los requerimientos de calidad, fiduciarios y de seguridad, se definieron los siguientes siete criterios de información:

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

- *Eficiencia* consiste en que la información sea generada optimizando los recursos (más productivo y económico).

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

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

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

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

- *Confiabilidad* significa proporcionar la información apropiada para que la gerencia administre la entidad y ejercite sus responsabilidades fiduciarias y de gobierno.

1.1.2 RECURSOS DE TI

La organización de TI se desempeña con respecto a estas metas como un conjunto de procesos definidos con claridad que utiliza las habilidades de las personas, y la infraestructura de tecnología para ejecutar aplicaciones automatizadas de negocio, mientras que al mismo tiempo toma ventaja de la información del negocio.

Para responder a los requerimientos que el negocio tiene hacia TI, la empresa debe invertir en los recursos requeridos para crear una capacidad técnica adecuada (Ej., un sistema de planeación de recursos empresariales) para dar soporte a la capacidad del negocio (Ej., implementando una cadena de suministro) que genere el resultado deseado (Ej., mayores ventas y beneficios financieros).

Los recursos de TI identificados en COBIT se pueden definir como sigue:

- *Aplicaciones* incluyen 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, en cualquier forma en que son 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 las aplicaciones.

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

En la siguiente tabla (Tabla 1) se muestra el impacto de los objetivos de control COBIT sobre los recursos y criterios de TI. En los recursos de TI una X significa que ese objetivo de control tiene impacto sobre el recurso y un espacio en blanco que no tiene impacto. En los criterios de información se identifica el grado de impacto; Primario (P), para indicar impacto directo sobre el criterio de información, Secundario (S) impacto indirecto o en menor medida y espacio en blanco o vacío, que no tiene impacto alguno.

OBJETIVOS DE CONTROL COBIT		Recursos TI de COBIT				Criterios de información de COBIT						
		PRESONAS	INFORMACION	APLICACIÓN	INFRAESTRUCTURA	EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO	CONFIABILIDAD
PLANEAR Y ORGANIZAR												
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	Definir la dirección tecnológica			X	X	P	P					
PO4	Definir los Procesos, Organización y Relaciones de TI	X				P	P					
PO5	Administrar la Inversión en TI	X		X	X	P	P					S
PO6	Comunicar las metas y la dirección de la gerencia	X	X			P					S	
PO7	Administrar los Recursos Humanos de TI	X				P	P					
PO8	Administrar la Calidad	X	X	X	X	P	P		S			S
PO9	Evaluar y Administrar los Riesgos de TI	X	X	X	X	S	S	P	P	P	S	S
PO10	Administrar los proyectos	X		X	X	P	P					
ADQUIRIR E IMPLANTAR												
AI1	Identificar las Soluciones Automatizadas			X	X	P	S					
AI2	Adquirir y Mantener 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	Procurar Recursos de TI	X	X	X	X	S	P				S	
AI6	Administrar los 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 los Niveles de Servicio	X	X	X	X	P	P	S	S	S	S	S
DS2	Administrar los Servicios de Terceros	X	X	X	X	P	P	S	S	S	S	S
DS3	Administrar el Desempeño y la Capacidad			X	X	P	P			S		
DS4	Asegurar el Servicio Continuo	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 el cumplimiento Regulatorio	X	X	X	X						P	S
ME4	Proporcionar Gobierno de TI	X	X	X	X	P	P	S	S	S	S	S

Tabla 1: Objetivos de Control COBIT, impacto en recursos TI y criterios de información

Fuente: Documento COBIT 4.0

1.2 JUSTIFICACIÓN DEL USO DE HERRAMIENTAS

1.2.1 NORMA ISO 17799 – 2005

Este Estándar Internacional establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos delineados en este Estándar Internacional proporcionan un lineamiento general sobre los objetivos de gestión de seguridad de la información generalmente aceptados.

Los objetivos de control y los controles de este estándar son diseñados para ser implementados para satisfacer los requerimientos identificados por una evaluación del riesgo. La norma puede servir como un lineamiento práctico para desarrollar estándares de seguridad organizacional y prácticas de gestión de seguridad efectivas y para ayudar a elaborar la confianza en las actividades inter-organizacionales.

1.2.2 MODELOS DE MADUREZ

Cada vez con más frecuencia, se les pide a los directivos de empresas corporativas y públicas que se considere qué tan bien se está administrando TI. Como respuesta a esto, se debe desarrollar un plan de negocio para mejorar y alcanzar el nivel apropiado de administración y control sobre la infraestructura de información.

Puede resultar difícil proporcionar respuestas significativas a estas preguntas. La gerencia de TI está buscando constantemente herramientas de evaluación por benchmarking[1] y herramientas de auto-evaluación como respuesta a la necesidad de saber qué hacer de manera eficiente. Comenzando con los procesos y los objetivos de control de alto nivel de COBIT, el propietario del proceso se debe poder evaluar de forma progresiva, contra los objetivos de control.

[1] Benchmarking: es una técnica utilizada para medir el rendimiento de un sistema o componente de un sistema, frecuentemente en comparación con el cual se refiere específicamente a la acción de ejecutar un benchmark. Fuente: http://es.wikipedia.org/wiki/Benchmark

Esto responde a tres necesidades:

1. Una medición relativa de dónde se encuentra la empresa
2. Una manera de decidir hacia dónde ir de forma eficiente
3. Una herramienta para medir el avance contra la meta

El modelado de la madurez para la administración y el control de los procesos de TI se basa en un método de evaluación de la organización, de tal forma que se pueda evaluar a sí misma desde un nivel de no-existente (0) hasta un nivel de optimizado (5). Este enfoque se deriva del modelo de madurez que el Software Engineering Institute definió para la madurez de la capacidad del desarrollo de software. Cualquiera que sea el modelo, las escalas no deben ser demasiado granulares, ya que eso haría que el sistema fuera difícil de usar y sugeriría una precisión que no es justificable debido a que en general, el fin es identificar dónde se encuentran los problemas y cómo fijar prioridades para las mejoras. El propósito no es avaluar el nivel de adherencia a los objetivos de control.

Los niveles de madurez están diseñados como perfiles de procesos de TI que una empresa reconocería como descripciones de estados posibles actuales y futuros. No están diseñados para ser usados como un modelo limitante, donde no se puede pasar al siguiente nivel superior sin haber cumplido todas las condiciones del nivel inferior. Si se usan los procesos de madurez desarrollados para cada uno de los 34 procesos TI de COBIT, la administración podrá identificar:

- El desempeño real de la empresa—Dónde se encuentra la empresa hoy
- El estatus actual de la industria—La comparación
- El objetivo de mejora de la empresa—Dónde desea estar la empresa

Se ha definido un modelo de madurez para cada uno de los 34 procesos de TI, con una escala de medición creciente a partir de 0, no existente, hasta 5, optimizado. El desarrollo se basó en las descripciones del modelo de madurez genérico descritas en la Tabla 2.

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 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.

Tabla 2: Modelo genérico de madurez
Fuente: Documento COBIT 4.0

CAPITULO 2 APLICACIÓN DE COBIT PARA LA AUDITORIA

2.1 CARACTERIZACIÓN DEL DEPARTAMENTO DE SISTEMAS

2.1.1 CARACTERIZACION DE LA EMPRESA

Identificación de la Empresa

Nombre : TELEAMAZONAS
Dirección : Calle Antonio Granda Centeno OE- 429 y Brasil.
Teléfono : 02 430313 / 2430350

Reseña Histórica

TELEAMAZONAS comenzó sus transmisiones el 22 de febrero de 1974, convirtiéndose en la primera red a color del Ecuador.

Desde sus inicios ha contado con la más avanzada tecnología: instaló la repetidora de microondas más potente del país, adquirió la primera unidad móvil del Ecuador, instaló en Guayaquil la antena auto soportada más grande del país.

Realiza coproducciones con importantes cadenas internacionales como Televisa de México y Canal 13 de Chile.

TELEAMAZONAS ha realizado importantes series y largometrajes de producción nacional como: Sucre, En un rincón del alma, Recuerdos en Paita, El gran retorno (ganadora del Festival de Cine Demetrio Aguilera Malta), J.J. El ruiseñor de América y El puente llevará su nombre, entre otras.

Es actualmente el canal con mayor cobertura a nivel nacional.

Actividad Principal

Misión[1]

> "Teleamazonas es la opción de televisión basada en valores, informa, educa y entretiene con una programación de la que se sienten orgullosos sus televidentes, anunciantes y empleados."

Visión[2]

> "Ser el primer canal en sintonía en Quito, y el segundo a nivel nacional, que aporta a la cultura y educación de los Ecuatorianos."

Valores[3]

- Ser el tercer canal a nivel nacional
- Tener 30 min. de programación nacional en el prime time (sin Noticias)
- Conseguir una operación auto-sustentable Dic. 2005
- Lograr la mejor señal a nivel nacional Dic. 2006

Factores Claves de Éxito[4]

- Rejilla de programación
- Cobertura
- Servicio al cliente
- Información de IBOPE
- Flexibilidad
- Tecnología
- Innovación
- Conocimiento de necesidades de anunciante

Planes

El Plan Informático general de Teleamazonas actualmente se encuentra en elaboración, no se cuenta con un Plan de Contingencias; en cuanto al Plan de

---

[1] FUENTE: http://www.teleamazonas.com/
[2] FUENTE: http://www.teleamazonas.com/
[3] FUENTE: http://www.teleamazonas.com/
[4] FUENTE: http://www.teleamazonas.com/

Capacitación del Personal no se lo tiene definido en forma específica sino que las capacitaciones se las realiza cuando sea necesario.

Los planes y políticas con los que cuenta Teleamazonas son los siguientes[1]:

- ✓ Políticas de Compras y Contratación
- ✓ Políticas de Registro de Activos Fijos
- ✓ Políticas y Procedimientos Vehículos
- ✓ Políticas Cajas Chicas
- ✓ Políticas de Gastos y Viajes
- ✓ Procedimientos de Teléfonos V2
- ✓ Procedimiento Beepers y Radios
- ✓ Procedimientos Seguros
- ✓ Procedimientos Seguridad Teleamazonas
- ✓ Formato Calificación Proveedor
- ✓ Formato Pagaré Directo
- ✓ Funciones Área Administrativa
- ✓ Funciones del Área Contabilidad – Administrativo
- ✓ Manual de Suministros y Materiales
- ✓ Manual Contable Cratel
- ✓ Manual de Taxis
- ✓ Gobierno Corporativo
- ✓ Manual Material Fílmico
- ✓ Modelo Conceptual de Gastos de Viaje

Estructura Organizacional[2]

La estructura organizacional de Teleamazonas está dividida en varios niveles en los cuales se encuentran tanto los órganos directivos como las diferentes direcciones o departamentos.

---

[1] Entregado por TELEAMAZONAS

[2] Realizado por: Marcia Cordero, María del Carmen Ibujés. Fuente: Entrevista con el Jefe del Departamento de Sistemas de TELEAMAZONAS.

En la siguiente figura (Figura 2) se muestra la estructura organizacional de TELEAMAZONAS:

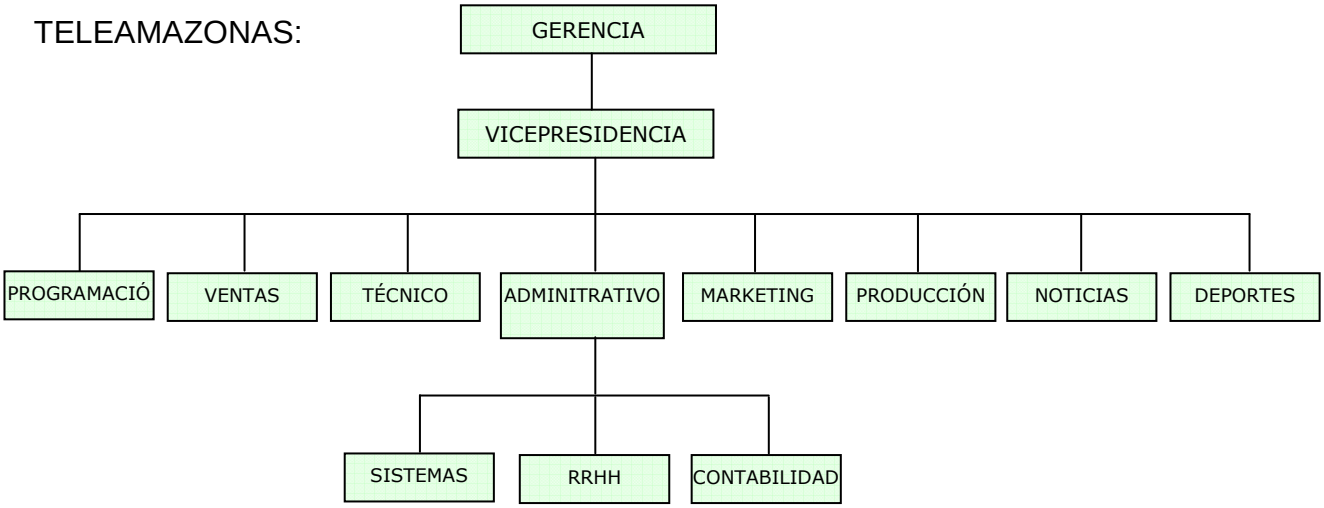

Figura 2: Estructura Organizacional de Teleamazonas
Fuente: Información otorgada por Teleamazonas.

Según la estructura organizacional de Teleamazonas nos podemos dar cuenta que el Área de Sistemas se encuentra bajo la dirección del Departamento Administrativo y Financiero, una recomendación es rediseñar esta organización y ubicarlo a un nivel asesor ya que el área de sistemas da soporte a todos los departamentos de la empresa además para tener un poder de decisión más independiente de otros departamentos.

2.1.2 PLAN ESTRATÉGICO Y ESTRUCTURA ORGANIZACIONAL DEL DEPARTAMENTO DE SISTEMAS

Misión[1]

La misión fundamental del Área de Sistemas es el diseño, implementación y mantenimiento de los elementos que constituyen la infraestructura informática de Teleamazonas, entendiendo por tal los elementos físicos, lógicos, configuraciones y procedimientos necesarios para proporcionar a toda la empresa los servicios informáticos necesarios para desarrollar sus actividades.

[1] Proporcionado por el Jefe del Departamento de Sistemas de TELEAMAZONAS

Visión[1]

- Cambio y actualización de Plataformas
- Migración de un ambiente de dos capas a uno de n capas. (Power Builder a .NET)
- Desarrollo de un Datawarehouse
- Basándose en el sistema gerencial que se tiene actualmente se han propuesto desarrollar un sistema para Teleamazonas.

Ubicación[2]

El área de Sistemas de Quito se encuentra en el tercer piso del edificio principal de las instalaciones de Teleamazonas, se ubica en un área adecuada para el personal existente, en caso de requerir más personal se requerirá de un espacio más amplio.

Planes del Departamento de Sistemas[3]

El Departamento de Sistemas no tiene un Plan estratégico específico, tampoco un Plan de Contingencias; en cuanto al Plan Informático, este plan existe pero se lo tiene en borrador, se lo utiliza más como una agenda de actividades que se propone realizar a corto y largo plazo.

En cuanto a programas de capacitación, no se tiene un Plan de Capacitación establecido, se lo realiza cuando se requiera y en forma informal. Si se trata de una capacitación interna, ésta es impartida por el propio personal dependiendo del área de conocimiento. Para el caso en que se presentan proyectos que requieran de conocimientos con los que no cuenta el personal de la Unidad Informática, se realiza una capacitación externa bajo pedido de los usuarios.

---

[1] Proporcionado por el Jefe del Departamento de Sistemas de TELEAMAZONAS
[2] Realizado por: Marcia Cordero, María del Carmen Ibujés. Fuente: Entrevista con el Jefe del Departamento de Sistemas de TELEAMAZONAS
[3] Realizado por: Marcia Cordero, María del Carmen Ibujés. Fuente: Entrevista con el Jefe del Departamento de Sistemas de TELEAMAZONAS

Recursos Humanos[1]

El Departamento de Sistemas de Teleamazonas cuenta con cinco técnicos cuyos cargos se encuentran detallados en la Tabla 3.

CARGO	NÚMERO
Jefe de Sistemas.	1
Supervisor	1
Asistente	3

Tabla 3: Recurso Humano del Departamento de Sistemas
Fuente: Información otorgada por Teleamazonas

Estructura Organizacional del Departamento de Sistemas[2]

En la siguiente figura (Figura 3) se indica la estructura organizacional distribuida en el Departamento de Sistemas.

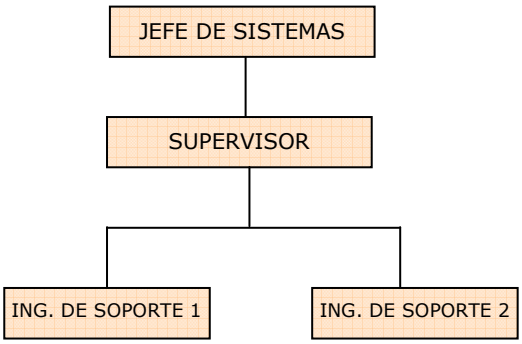

Figura3: Estructura Organizacional del Departamento de Sistemas.
Fuente: Creación de los autores

[1] Realizado por: Marcia Cordero, María del Carmen Ibujés. Fuente: Entrevista con el Jefe del Departamento de Sistemas de TELEAMAZONAS
[2] Realizado por: Marcia Cordero, María del Carmen Ibujés. Fuente: Entrevista con el Jefe del Departamento de Sistemas de TELEAMAZONAS

Diagrama Orgánico Funcional

En la siguiente figura (Figura 4) se muestra la distribución orgánico funcional del Departamento de Sistemas, obtenido por medio de entrevistas a los integrantes del mismo.

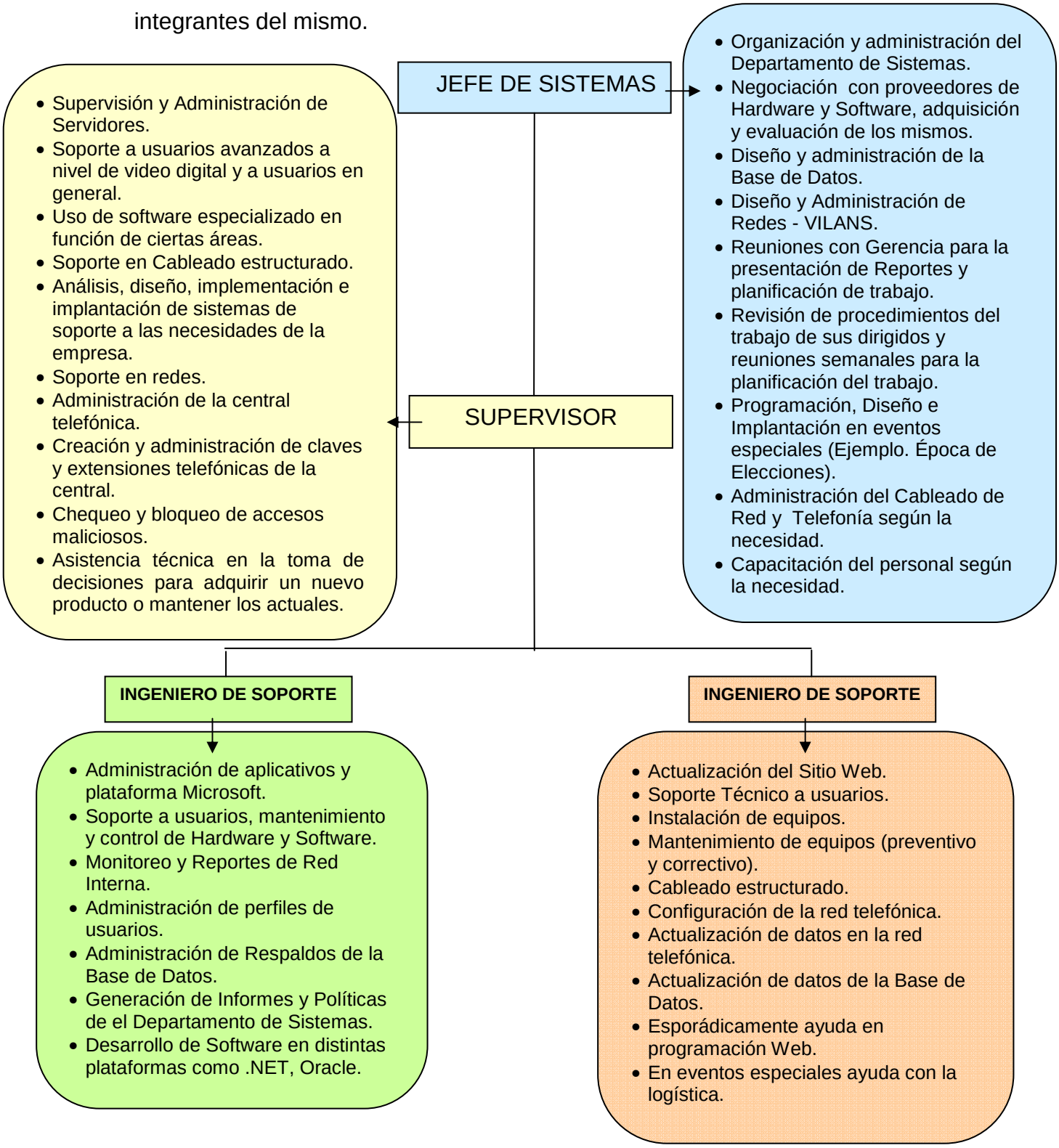

Figura 4: Diagrama Orgánico Funcional del Departamento de Sistemas.
Fuente: Creación de los autores

Funciones del Departamento de Sistemas.

A continuación se enumera las principales funciones del Departamento de Sistemas de Teleamazonas:

- Administrar los servidores de Quito y Guayaquil, realizar el monitoreo, respaldos y brindar el mantenimiento a los equipos y las aplicaciones (bases de datos, servidores Web, etc.), así como también verificar los aspectos relacionados con seguridad.
- Administrar la Red tanto de Quito como en Guayaquil; abarcando un amplio número de aspectos. En general, se tratan con muchos datos estadísticos e información sobre el estado de la red, y se realizan las acciones necesarias para ocuparse de fallos y otros cambios.
- Administrar la Base de Datos; definir y controlar las bases de datos corporativas, además proporcionar asesoría a los desarrolladores, usuarios y ejecutivos que la requieran.
- Desarrollar Aplicaciones para el canal utilizando herramientas de programación como Power Builder, Punto Net, Java, con Base de Datos Oracle. Las aplicaciones que se usan en el Departamento Administrativo Financiero son compradas y personalizadas para el caso de la empresa, la personalización de estos programas para que se adapten a las funcionalidades se las hace en un promedio del 50%.
- Negociar compras de equipos informáticos y software de diseño.
- Manejar Macintosh a nivel de administración y configuración.
- Se encarga de tareas puntuales, por ejemplo; en periodos electorales administran todo lo que se refiere a logística en cuanto a la información que se va a publicar y quien lo va a hacer.
- Mantenimiento Técnico del canal y Soporte Técnico.
- Administración y Publicación del Sitio Web de Teleamazonas.

Una descripción más detallada de las funciones del Departamento de Sistemas en encuentra en el *ANEXO 1*

2.1.3 PLATAFORMA, SISTEMAS, INTERCONECTIVIDAD Y SEGURIDAD DEL DEPARTAMENTO

Software

El Departamento de Sistemas de Teleamazonas cuenta con los siguientes tipos de software:

- Software de Sistema[1]
  Sistema Operativo Windows desde la versión 95 hasta XP Professional y para servidores, Windows Server 2003, además se tiene algunos equipos con sistema operativo Mac OS X.
- Software de Control
  Tantos los servidores de Correo, Dominio, Firewall, Archivos – Impresiones que son Windows 2003 cuentan con Performance Monitor la cual es una herramienta que permite medir el desempeño de los computadores de una red.
- Software de Aplicación[2]
  Las computadoras utilizadas en el área de sistemas como en toda la institución tienen generalmente las siguientes herramientas, Microsoft Office, Sistemas de Inventarios, sistemas de control y automatización para radio y televisión, Software de edición de video de imágenes y sonido, etc.

  Inventario de Software véase *ANEXO 2.*

Hardware

El Inventario Hardware así como la descripción de los servidores de Quito y Guayaquil se encuentra en el *ANEXO 3.*

---

[1] PLANETA CODIGO, glosario:software_de_sistema, http://www.planetacodigo.com/wiki/glosario:software_de_sistema, 2007[Software de Sistema.-Software diseñado para facilitar o permitir la operación y el mantenimiento de un sistema informático; por ejemplo los sistemas operativos]

[2] WIKIPEDIA, LA ENCICLOPEDIA LIBRE, Software, http://es.wikipedia.org/wiki/Software, 2007 [Software de Aplicación.- que permite a los usuarios llevar a cabo una o varias tareas más específicas, en cualquier campo de actividad susceptible de ser automatizado o asistido, con especial énfasis en los negocios.]

Topología de la Red

A continuación (Figura 5) se describe la Topología de la Red de Teleamazonas:

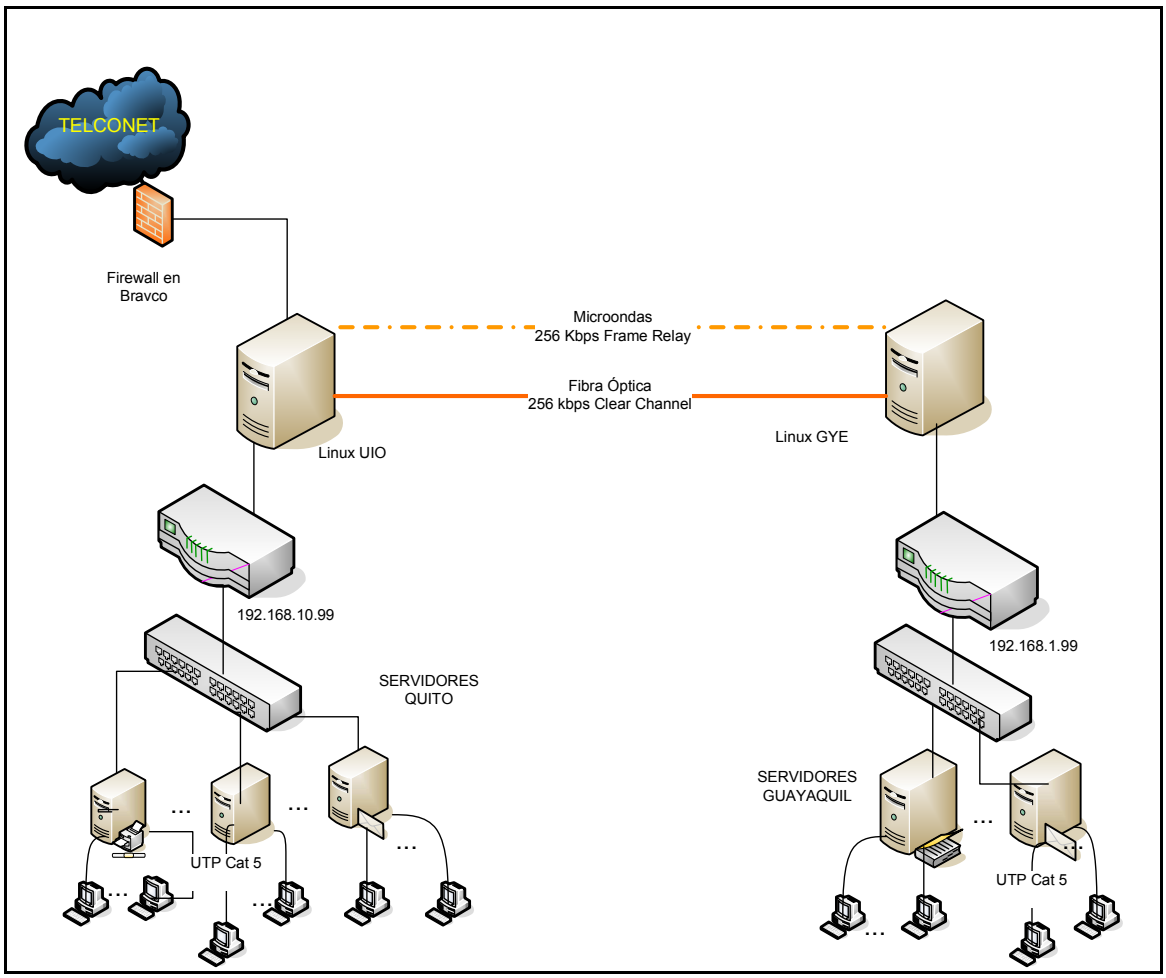

Figura 5: Topología de Red Teleamazonas
Fuente: Creación de los autores

Topología de Red de Quito y Guayaquil, están interconectadas con dos enlaces de 256 Kbps cada uno, mediante microondas para la tecnología Frame Relay y fibra óptica para Clear Channel; Bravco es el ISP[1] encargado de los enlaces entre Quito y Guayaquil.

[1] ISP: Internet Service Provider, son las empresas dedicadas a conectar los usuarios a **Internet**, y dar otras prestaciones relacionadas con redes venda de **dominios web**, etc. Fuente: http://gl.wikipedia.org/wiki/ISP

El servidor de Internet se encuentra en Quito desde el cual se envía la señal a Guayaquil; se tiene dos proveedores de Internet Telconet y Andinadatos.
En cuanto al medio de transmisión interno utilizan UTP categoría 5; y externamente fibra óptica y microondas.

2.1.4 ANALISIS DE SEGURIDAD BASADO EN ISO/IECE 17799.

El análisis de la seguridad en el Departamento de Sistemas de Teleamazonas está basado en el Estándar Internacional ISO/IECE 17799 - 2005[1] (Ver *ANEXO 4*), de acuerdo a las entrevistas escritas realizadas a los miembros del área (Ver *ANEXO 5*).

Este estándar contiene once cláusulas de control de seguridad, cada cláusula contiene un número de categorías de seguridad principales:

- Política de Seguridad
- Organización de la Seguridad de la Información
- Gestión de Activos
- Seguridad de Recursos Humanos
- Seguridad Física y Ambiental
- Gestión de Comunicaciones y Operaciones
- Control de Acceso
- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
- Gestión de Incidentes de Seguridad de la Información
- Gestión de la Continuidad Comercial
- Conformidad

Nota: La numeración que se ha utilizado para cada cláusula que a continuación están descritas, es la misma que corresponde a la norma ISO/IECE 17799 para efectos de mantener el formato de la misma.

[1] ANEXO 5: Estándar Internacional ISO/IEC 17799, Segunda Edición Junio 2005

Política de seguridad

5.1 Política de seguridad de la información

El Departamento de Sistemas no cuenta con una política de Seguridad de la Información definida.

Organización de la Seguridad de la Información

6.1 Organización interna

La gerencia está consciente que se debe elaborar una Política de Seguridad y difundirla a los integrantes del área, al momento se está diseñando políticas de seguridad específicas según las necesidades que se van presentando.

6.2 Grupos o personas externas

En cuanto al acceso físico de terceras personas[1] se mantiene un control de ingreso en las puertas principales y, dentro del Departamento de Sistemas lo que se practica es que sus integrantes estén pendientes de la presencia de las mismas.

El acceso lógico se maneja por medio de claves de ingreso a las bases de datos y sistemas de información.

Los controles no están claramente definidos, a pesar que manejan varios grupos externos; por ejemplo[2]:

- Proveedores de servicio; tal como ISPs, proveedores de redes, servicios telefónicos, Servicios de mantenimiento y soporte
- Servicios de seguridad manejados
- Clientes
- Gerencia y consultores comerciales, y auditores
- Diseñadores y proveedores; por ejemplo, productos de software y sistemas TI;
- Limpieza, abastecimiento de alimentos (catering) y otros servicios de soporte abastecido externamente

[1] Terceras personas: Físicamente no tienen nada que ver con la empresa
[2] FUENTE: Estándar Internacional ISO/IEC 17799, Segunda Edición Junio 2005, Pág. 14

- Personal temporal, colocación de estudiantes y otros nombramientos casuales de corto plazo.

Gestión de Activos

7.1 Responsabilidades sobre los activos.

Los inventarios de los activos ayudan a asegurar que se realice una protección efectiva de los mismos, y también puede requerir de otros propósitos comerciales; como planes de salud y seguridad, seguros o razones financieras (gestión de activos)[1].

En Teleamazonas se lleva un inventario de equipos y aplicaciones de software que se tiene instalado, llevan un inventario de switches de la red con sus respectivas configuraciones; los responsables de los equipos son quienes los usan, en caso de equipos que no estén asignados a ninguna persona el responsable es el administrador de red, y así para todos los activos con los que cuenta el Departamento de Sistemas.

Cabe recalcar que el inventario que se tiene no está realizado con ningún tipo de formato especificado por normas de manejo de seguridad.

Existen muchos tipos de activos que se deben respaldar dentro del Departamento de Sistemas como:

a) Información: bases de datos, contratos y acuerdos, documentación del sistema, información de investigaciones, manuales del usuario, material de capacitación, procedimientos operacionales o de soporte, planes de continuidad del negocio, acuerdos para contingencias, rastros de auditoria e información archivada.
b) Activos de software: software de aplicación, software del sistema, herramientas de desarrollo y utilidades.

[1] FUENTE: Estándar Internacional ISO/IEC 17799, Segunda Edición Junio 2005, Pág. 36

c) Activos físicos: equipo de cómputo, equipo de comunicación, medios removibles y otro equipo.
d) Servicios: servicios de computación y comunicación, servicios generales; por ejemplo, calefacción, iluminación, energía y aire acondicionado.
e) Personas, y sus calificaciones, capacidades y experiencia.
f) Intangibles, tales como la reputación y la imagen de la organización.

No se tiene documentado ni implementadas reglas para el uso aceptable de la información y los activos asociados con los medios del procesamiento de la información.

7.2 Clasificación de la Información

La información de la empresa no es clasificada. La información debe ser clasificada para indicar la necesidad, prioridades y grado de protección esperado cuando se maneja la información.

Seguridad de Recursos Humanos

8.1 Antes del empleo.

Se debe definir claramente el proceso de contratación de empleados con roles, responsabilidades, derechos y obligaciones definidos para los aspirantes, se debe hacer una verificación de antecedentes con la información que se registra en la hoja de vida.

8.2 Durante el desempeño de funciones.

En el Departamento de Sistemas de Teleamazonas no se tiene roles y responsabilidades definidos, realizan las actividades de acuerdo a las necesidades y conocimientos.

De las entrevistas realizadas se deduce que en ciertas ocasiones todo el equipo realiza las mismas actividades es decir se desempeñan de acuerdo a las necesidades.

No se tiene una adecuada capacitación con respecto a la seguridad de la información de la empresa, según la función laboral de cada empleado.

Seguridad Física y Ambiental

9.1 Áreas seguras

El objetivo es evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización.

Para mantener la seguridad física de Teleamazonas se ha contratado vigilancia privada por medio de una compañía dedicada a este fin, la misma que tiene sus correspondientes políticas de contratación.

En cuanto al Departamento de Sistemas la vigilancia del área se la realiza por los mismos integrantes, ya que no poseen ningún sistema de seguridad ni en el Departamento ni en el cuarto de servidores, lo que se tiene es una llave para entrar al mismo.

9.2 Equipo de seguridad

En el Departamento de Sistemas se cuenta con un extintor manual de fuego a base de gas, en caso de incendios; se realiza un control periódico del correcto funcionamiento de los extintores.

En el cuarto de servidores existe aire acondicionado que posee un sensor de temperatura que se activa automáticamente en caso de condiciones anormales del ambiente, en el edificio no se posee alarma para detectar fuego, calor, humo o fugas de agua.

El personal no está capacitado en caso de que suceda alguna emergencia, simplemente actuará por instinto o por lo que generalmente se conoce.

Existen normas generales en el Departamento de Sistemas para salvaguardar los equipos como:

- No fumar dentro de las instalaciones.
- No consumir alimentos dentro del cuarto de servidores.

- El cableado de la red, se tiene protegido mediante canaletas en el techo falso.
- No existe personal encargado o responsable del mantenimiento de los equipos, lo realiza todo el personal del Departamento de Sistemas.
- No se tiene una política definida para cuando haya necesidad de sacar los equipos de las instalaciones ya sea por realizar trabajos en casa o por presentaciones en otras áreas o locales.
- Cuando hay la necesidad de retirar un equipo a un usuario no se tiene definido un procedimiento, solo se verifica las razones del cambio, se respalda la información necesaria y se procede a realizar el cambio actualizando en inventario.

Gestión de las Comunicaciones y Operaciones

10.1 Procedimientos y responsabilidades operacionales

En el Departamento de Sistemas no se tiene un plan de procedimientos de operación de la información y de los equipos, los mismos que se deben documentar, mantener y poner a disposición de los usuarios que los necesiten.

Los procedimientos de operación deben especificar las instrucciones para la ejecución detallada de cada trabajo como:

a) Procesamiento y manejo de información.
b) Copia de seguridad o respaldo.
c) Requerimientos de programación de horarios, incluyendo las interdependencias con otros sistemas, los tiempos de culminación y horarios de los primeros y últimos trabajos.
d) Instrucciones para el manejo de errores u otras condiciones excepcionales, las cuales podrían surgir durante la ejecución del trabajo, incluyendo las restricciones sobre el uso de las utilidades del sistema.
e) Contactos de soporte en el evento de dificultades operacionales o técnicas inesperadas.
f) Procedimientos de reinicio y recuperación del sistema para su uso en el evento de una falla en el sistema.

g) La gestión de la información del rastro de auditoria y registro del sistema.

10.3 Planeación y aceptación del sistema

Con esto se trata de minimizar los riesgos en el sistema, se deben establecer, documentar y probar los requerimientos operacionales de los sistemas nuevos antes de su aceptación y uso.

En el Departamento de Sistemas no se tiene ni se realiza un monitoreo de los sistemas planificado, para evaluar el rendimiento del mismo, y no se hace un estudio debidamente documentado para la aceptación de sistemas que vayan a ser usados.

10.4 Protección contra el código malicioso y móvil

En el Departamento de Sistemas se protege de los códigos maliciosos[1] mediante el antivirus de Symantec Norton, y no se tiene una política de revisión de virus en dispositivos móviles[2] a ser ejecutados sino que se la realiza de manera informal; las personas que saben que deben revisar los dispositivos lo hacen, y los ejecutan de una manera que no afecte al sistema.

10.5 Respaldo o Back-Up

El Departamento de Sistemas de Teleamazonas cuenta con una política de respaldos (Ver *ANEXO 6*) recientemente implementada y se encuentra en la fase de pruebas e implantación.

Por el momento cada usuario está encargado de respaldar la información que utiliza y el Jefe de Departamento encargará a un miembro respaldar el Sistema Operativo, Bases de Datos, y Aplicaciones, los mismos que los realizan en Discos duros, Discos ópticos y DVDs, escogidos por costos y seguridad. No se tiene un lugar específico donde almacenarlos.

---

[1] Códigos maliciosos: virus cómputo, virus de red, caballos Troyanos y bombas lógicas

[2] Código móvil: código de software que transfiere de una computadora a otra computadora y luego ejecuta automáticamente y realiza un función específica con muy poca o ninguna interacción

10.6 Gestión de seguridad de la red

El administrador de la red realiza un control de la misma en cuanto a flujos de datos, monitoreo y protección; sin embargo no se cuenta con controles documentados para realizar estas tareas.

10.7 Gestión de medios

En el Departamento de Sistemas se controlan los medios y se los protege físicamente de acuerdo a la responsabilidad de cada unos de los integrantes del área; es decir cada uno tiene a su cargo algún medio y es responsable de su estado.

10.8 Intercambio de información

Para realizar el intercambio de la información no se tiene una política diseñada, sino que el Departamento tiene definido quien debe tener información para cada tarea específica, y cuando se trata de información confidencial se hace un registro de la persona a quien se entregó dicha información, para que quede constancia de haberla entregado.

Para la transmisión de información dentro de Teleamazonas se utiliza Microsoft Outlook, como gestor de correo electrónico, y de esta manera la persona encargada controla a quien, cuando, y que información ha sido enviada y recibida.

Para mantener la confidencialidad de la información se tiene restringido el uso de programas de mensajería como Windows Messenger, Yahoo Messenger, Skype, etc., No se tiene restringido el uso de celular dentro del Departamento de Sistemas de Teleamazonas lo que es un riesgo ya que se puede revelar información confidencial por este medio, en cuanto a la línea telefónica, se tiene una red telefónica de VOIP[1], en la que se puede controlar las llamadas entrantes y salientes, y los usuarios que las realizan.

---

[1] VOIP; también llamado **Voz sobre IP**, **VozIP**, **VoIP** , o **Telefonía IP**, es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Internet Protocol). Esto significa que se envía la señal de voz en forma digital en paquetes en lugar de enviarla (en forma digital o analógica) a través de circuitos utilizables solo para telefonía como una compañía telefónica convencional. Fuente : http://es.wikipedia.org/wiki/Voz_sobre_IP

10.10 Monitoreo

Es necesaria la utilización de procedimientos de monitoreo para asegurar que los usuarios sólo estén realizando actividades para las cuales han sido explícitamente autorizados; en el Departamento de Sistemas se usa pistas de auditoria para control de acceso a la base de datos.

Para acceder a los sistemas se tiene perfiles definidos para cada uno de los usuarios, con estos controles se puede administrar las fallas ocurridas en los sistemas para tomar acciones correctivas ante ellas.

Control de Acceso

11.1 Requerimiento del negocio para el control del acceso

El Departamento de Sistemas no cuenta con políticas para la divulgación, política de clasificación de la información y autorización de la información.

No se cuenta con una política de control de acceso (lógico y físico) totalmente definida; el control de la información se lo realiza en la práctica de la siguiente manera: el personal del Departamento es responsable del manejo de información específica y tiene a su cargo la administración de la misma siendo responsables de lo que ocurra con ella y de dar permisos de acceso.

11.2 Gestión de acceso del usuario

La manera como se asegura el acceso de usuarios autorizados y no autorizados a los sistemas de información es manejando perfiles, es decir login y passwords de acceso con sus respectivos permisos dentro de las aplicaciones.

Existe una persona encargada de la administración de usuarios, desde el registro de usuarios nuevos hasta la terminación final del registro de los mismos que ya no requieren acceso a los sistemas y servicios de información; pero este no es un procedimiento estrictamente formal.

El manejo de claves secretas no se controla a través de un proceso de gestión formal.

11.3 Responsabilidades del usuario

El control de acceso de usuarios no autorizados para evitar poner en peligro la información y evitar el robo de la misma es manejado por cada uno de los miembros del Departamento de Sistemas quienes tienen la responsabilidad de salvaguardar los equipos y la información que se encuentran a cargo.

Cabe aclarar que no hay una política de escritorio y pantalla limpios estricta, pero existe una regla que cuando alguien tiene que dejar por cualquier motivo su lugar de trabajo es obligatorio que deje bloqueando su equipo y para desbloquearlo se necesita una clave personal secreta.

No existe una política de claves y contraseñas, el uso de las mismas es decidido por el usuario con consejo y consentimiento del personal de sistemas.

11.4 Control de acceso a la red

El control de acceso a los servicios de redes internas y externas lo realiza el administrador de la red o la persona encargada de esta función, no se tiene una política definida al respecto pero se controla mediante interfaces apropiadas y mecanismos de autenticación.

El control de acceso a los puertos de diagnostico y configuración remota está a cargo del administrador de la red y el Jefe del Departamento, se maneja protecciones adecuadas al administrar remotamente, por ejemplo en los equipos que se encuentran en Guayaquil; aunque no se cuenta con una política definida para el uso de los mismos.

Se realiza una segregación de redes dividiéndolas en dominios de red lógicos separados en dominios de red internos y dominios de red externos; además se tiene implementados Gateway para cada Vlan.

Hay restricción de los usuarios que se conectan a la red es decir aquellos que se encuentran fuera de la frontera de la organización, esto se lo realiza a través de Gateways.

Se restringe: correo electrónico, mensajería instantánea, transferencia de archivos y acceso a aplicaciones.

En cuanto a controles de routing no hay una reglamentación establecida ya que como se dijo anteriormente no existe una política de control de acceso.

11.5 Control del acceso al sistema operativo

Para evitar el acceso no autorizado a los sistemas operativos se autentifica a los usuarios autorizados pero no se registra los intentos exitosos y fallidos de autenticación del sistema. Mediante la aplicación Active Directory se da privilegios a los usuarios y se asigna las respectivas claves de acceso.

No se restringe el tiempo de conexión de los usuarios y se emite alarmas cuando se violan las políticas de seguridad del sistema.

Las sesiones inactivas se bloquean después de un periodo de inactividad, esto está definido como regla propia del sistema operativo, mas no como política del Departamento.

11.6 Control de acceso a la aplicación y la información

Para evitar el acceso no autorizado a la información en los sistemas de aplicación no existe una política de control de acceso definida; sin embargo el control se lo realiza por medio de claves de acceso a usuarios autorizados los cuales tienen perfiles definidos, con sus respectivos privilegios de acuerdo a las funciones que necesite, en los sistemas de aplicación.

11.7 Computación y tele-trabajo móvil

Para garantizar la seguridad de la información cuando se utiliza medios de computación y tele-trabajo móviles como notebooks el responsable del equipo debe tener especial cuidado.

No hay una política de computación móvil claramente establecida pero como regla general se tiene precaución en cuanto a respaldos, control de acceso, protección física, conexiones inalámbricas y protección contra virus.

Adquisición Desarrollo y Mantenimiento de los Sistemas de Información

12.1 Requerimientos de seguridad de los sistemas de información

En las aplicaciones que se desarrolla y se adquiere en el Departamento se define perfiles de usuario para manejar la seguridad de las mismas, así como también en las bases de datos de las aplicaciones.

No se define requerimientos de seguridad pero se los maneja en los diferentes sistemas, y cuando son aplicaciones adquiridas, siempre se hace una adecuada fase de pruebas.

12.2 Procesamiento correcto en las aplicaciones

Para prevenir errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones, se las realiza con las respectivas validaciones para el ingreso de información, y el procesamiento de dicha información es debidamente probado para evitar errores y riesgos de que se la use incorrectamente, se verifica que la salida de la información sea la que se esperaba, mas sin embargo; la validación, verificación y pruebas; y la salida no siempre será la correcta; es decir, aún los sistemas que han sido probados pueden producir output incorrecto en algunas circunstancias. Por esta razón se debe implementar mejores prácticas para un mejor resultado.

12.3 Controles criptográficos

Para proteger la confidencialidad, autenticidad e integridad a través de medios criptográficos. Se debe desarrollar una política sobre el uso de controles criptográficos.

En el Departamento de Sistemas se utiliza técnicas de criptografía que ofrecen los motores de bases de datos, no se tiene definidas políticas en particular para manejarla.

12.4 Seguridad de los archivos del sistema

El almacenamiento de código fuente e instalación de software es solo gestionado por las personas asignadas para el efecto, con el fin de garantizar la seguridad.

12.5 Seguridad en los procesos de desarrollo y soporte

Se debe documentar y hacer cumplir los procedimientos formales de control del cambio para minimizar la corrupción de los sistemas de información, en el Departamento de Sistemas para probar los cambios existe ambientes de prueba verificando que no comprometan a los procesos anteriores.

Cuando se adquiere software externo, el procedimiento de desarrollo y pruebas es debidamente controlado para que se adapte a sus necesidades y de esta manera disminuir riesgos cuando ya esté en producción.

Gestión de un incidente en la Seguridad de la Información

13.1 Reporte de los eventos y debilidades de la seguridad de la información

El Departamento no tiene una política de reporte de debilidades, sino que según sea el caso de emergencia se soluciona dichas eventualidades pero no con un procedimiento determinado, no se ha informado a los usuarios y terceros que se tome nota y se reporte cualquier debilidad de seguridad observada o sospechada en el sistema o los servicios.

13.2 Gestión de los incidentes y mejoras en la seguridad de la información

Además de establecer una política para reportar eventualidades posibles de riesgos de seguridad de los sistemas o servicios se debe establecer una política para el monitoreo de las mismas.

En Teleamazonas no se tiene un registro de eventualidades que han sido solucionadas, para su monitoreo y procurar que no vuelvan a suceder.

Gestión de la Continuidad del Negocio

14.1 Aspectos de la seguridad de la información de la gestión de la continuidad del Negocio

No existe un plan de contingencia donde se tome en cuenta aspectos de la seguridad de la información de la gestión de la continuidad del negocio.

Únicamente para salvaguardar la información se está implementando un plan de respaldos.

Cumplimiento

15.1 Cumplimiento de los requerimientos legales

Los sistemas de información del Departamento cumplen con los requerimientos legales correspondientes.

Todo el software cuenta con las licencias de uso respectivas y en regla.

No se cuenta con una política apropiada con respecto al uso de licencias y que garantice los derechos de propiedad intelectual de los sistemas que se han implementado así como con una política de protección y privacidad de los datos.

15.2 Cumplimiento de las políticas y estándares de seguridad, y cumplimiento técnico

La seguridad de los sistemas de información se revisa cada vez que es requerido, es decir, cuando se detecta algún error debido a la falta de seguridad.

El Jefe de Departamento verifica el cumplimiento de los procedimientos de seguridad dentro del área y en caso de un incumplimiento se pide rendición de cuentas a la persona encargada.

La detección de vulnerabilidades en los sistemas lo hacen las personas del Departamento de Sistemas y también los usuarios finales.

15.3 Consideraciones de auditoria de los sistemas de información

No se ha realizado auditoria de los sistemas de información, ni internamente ni externamente.

2.2 EJECUCIÓN DE LA AUDITORIA DE RIESGOS INFORMÁTICOS

2.2.1 ALCANCE DE LA AUDITORÍA DE RIESGOS INFORMÁTICOS

Teleamazonas es un canal de televisión, con visión a ser el mejor canal del Ecuador apoyando el desarrollo del país siendo una empresa sin fines de lucro. Por lo que es necesario que en todos sus departamentos se enfoquen a alcanzar esta meta dando lo mejor de sí, unos en mayor proporción que otros; en el caso del Departamento de Sistemas un punto importante que se debe tomar es la Gestión de Riesgos Informáticos, con el objetivo de salvaguardar los activos de la empresa y más aún la información.

De aquí partirá el análisis donde se identificarán los riesgos existentes y potenciales, se presentarán conclusiones sobre la situación actual así como recomendaciones para el mejoramiento de la gestión de riesgos.

El presente trabajo de auditoria aplicará COBIT como metodología para la evaluación y análisis de los diferentes procesos y controles que se aplican para la administración de Riesgos Informáticos en el Departamento de Sistemas.

2.2.2 OBJETIVOS DE LA AUDITORIA

- Analizar y Auditar la situación actual en cuanto a riesgos informáticos en el Departamento de Sistemas de Teleamazonas.

- Plantear las mejoras basándose en COBIT para una buena Administración de Riesgos en el Departamento.

- Elaborar el Informe de Auditoria con las directrices necesarias a ser implantadas en el Departamento, para de esta manera mejorar la gestión de riesgos informáticos.

2.2.3 INTEGRACIÓN ISO/IECE 17799 - COBIT

En la siguiente tabla (Tabla 4) se integra los objetivos de control de COBIT y la norma ISO/IECE 17799-2005; basado en el documento COBIT SECURITY BASELINE, en el cual se mapea los objetivos de control de COBIT con las cláusulas de control de seguridad de la norma ISO[1]. Para de esta manera seleccionar los objetivos de control concernientes a la evaluación de los riesgos fundamentándose en la norma. (Ver. CUADRO TOTAL DE INTEGRACION COBIT ISO ANEXO 7)

CLAUSULAS NORMA ISO/IECE 17799	OBJETIVOS DE CONTROL COBIT DETALLADOS
5. Política de seguridad 5.1 Política de seguridad de la información	PO3.1, PO5.3, PO5.4, PO6.1, PO6.2, PO6.3, PO6.4, PO7.4, PO9.4, DS4.1, DS5.5, DS5.6, DS7.1, ME2.1, ME2.4
6. Organización de la Seguridad de la Información 6.1 Organización interna 6.2 Grupos o personas externas	PO1.3, PO1.4, PO1.5, PO2.3, PO3.1, PO3.3, PO4.3, PO4.4, PO4.5, PO4.6, PO4.8, PO4.9, PO4.10, PO4.14 , PO4.15, PO6.1, PO6.3,PO6.4, PO6.5, PO7.2, PO7.4, PO7.5, PO9.3 , PO9.4, PO10.4, AI1.2, AI1.3, AI2.1, AI2.3, AI3.1, AI3.2, AI3.3, AI5.2, AI5.6, AI6.1, AI6.3, AI7.12, AI7.6, AI7.8, DS2.1, DS2.2, DS2.3, DS2.4, DS4.1, DS4.3, DS5.1, DS5.1, DS5.3, DS5.4, DS5.5, DS5.6, DS5.11, DS7.2, DS10.1, DS10.2, DS11.6, DS12.1, DS12.3, ME2.1, ME2.2, ME2.3, ME2.4, ME2.5.
7. Gestión de Activos 7.1 Responsabilidades sobre los activos. 7.2 Clasificación de la Información	PO2.3, PO3.1, PO4.9, PO4.10, PO6.3, PO6.4, PO6.5, PO9.3, AI2.2, AI6.5, AI7.8, DS9.1, DS9.2, DS9.3, DS11.2, DS11.3, DS11.6, DS13.4, ME3.1.
8. Seguridad de Recursos Humanos 8.1 Antes del empleo.	PO4.6, PO4.8, PO4.14, PO6.1, PO6.3 PO6.4, PO6.5, PO7.1, PO7.2, PO7.4, PO7. , PO7.7,

[1] Para realizar el paso de COBIT 3 a COBIT 4 se utilizó la Referencia Cruzada que se encuentra en le documento COBIT 4.0; y de la misma manera para pasar de la norma ISO 17799-2000 a ISO 17799-2005 utilizamos el documento COMPARISON BETWEEN OLD AND REVISED ISO 17799 STANDARD (ver ANEXO 8)

8.2 Durante el desempeño de funciones.	PO7.8, AI5.3, DS2.3, DS2.4, DS5.4, DS7.1, DS12.1.
9. Seguridad Física y Ambiental 9.1 Áreas seguras 9.2 Equipo de seguridad	PO4.14, PO6.3, PO6.4, PO6.5, PO9.3, AI6.3, AI7.11, DS4.1, DS4.7, DS4.8, DS4.9, DS5.3, DS5.4, DS5.7, DS9.3, DS10.2, DS11.4, DS12.1, DS12.2, DS12.3, DS12.4, DS12.5, DS13.2, DS13.5, ME3.1.
10. Gestión de las Comunicaciones y Operaciones 10.1 Procedimientos y responsabilidades operacionales 10.3 Planeación y aceptación del sistema 10.4 Protección contra el código malicioso y móvil 10.5 Respaldo o Back-Up 10.6 Gestión de seguridad de la red 10.7 Gestión de medios 10.8 Intercambio de información 10.10 Monitoreo	PO2.3, PO3.1, PO3.4, PO3.5, PO4.6, PO4.11, PO6.3, PO6.4, PO6.5, PO7.4, PO7.5, AI1.1, AI2.1, AI2.2, AI2.3, AI2.8, AI3.1, AI3.2, AI3.4, AI4.2, AI4.3, AI4.4, AI5.2, AI5.6, AI6.1, AI6.2, AI6.3, AI7.1, AI7.4, AI7.6, AI7.8, DS2.3, DS3.1, DS3.2 , DS3.3, DS3.4 , DS3.5, DS4.1, DS4.9, DS5.3, DS5.4, DS5.5, DS5.6, DS5.10, DS5.11, DS9.1, DS9.3, DS10.1, DS10.2, DS10.3, DS10.4, DS11.2 , DS11.3 , DS11.4, DS11.5, DS11.6, DS12.1, DS12.2, DS12.3, DS12.5, DS13.1, DS13.2, DS13.4 , ME2.1, ME2.2, ME2.3, ME2.4, ME3.1.
11. Control de Acceso 11.1 Requerimiento del negocio para el control del acceso 11.2 Gestión de acceso del usuario 11.3 Responsabilidades del usuario 11.4 Control de acceso a la red 11.5 Control del acceso al sistema operativo 11.6 Control de acceso a la aplicación y la información. 11.7 Computación y tele-trabajo móvil	PO2.3, PO3.4, PO3.5, PO6.3, PO6.4, PO6.5, PO7.4, PO7.5, PO7.8, PO9.3, AI1.1, AI1.2, AI3.1, AI3.2, AI6.3, DS4.1, DS5.3, DS5.4, DS5.5, DS5.6, S5.11, DS7.1, DS12.1, DS12.2, DS12.3.
12. Adquisición Desarrollo y Mantenimiento de los Sistemas de Información 12.1 Requerimientos de seguridad de los sistemas de información 12.2 Procesamiento correcto en las aplicaciones 12.3 Controles criptográficos 12.4 Seguridad de los archivos del sistema 12.5 Seguridad en los procesos de desarrollo y soporte	PO2.1, PO2.3, PO6.3, PO6.4, PO6.5, PO9.3, PO9.5, AI1.1, AI1.2, AI2.2, AI2.3, AI2.4, AI2.8, AI3.1, AI3.3, AI3.4, AI5.1, AI5.2, AI5.3, AI5.4, AI5.5, AI6.1, AI6.2, AI6.3, AI6.4, AI6.5, AI7.10, AI7.11, AI7.6, DS2.3, DS2.4, DS4.1, DS5.3, DS5.4, DS5.7, DS5.8, DS5.11, DS9.1, DS9.2, DS11.5, DS11.6, ME3.1.
13. Gestión de un incidente en la Seguridad de la Información 13.1 Reporte de los eventos y debilidades de la seguridad de la información	PO5.3, PO6.1, PO6.2, PO6.3, PO6.4, PO6.5, PO7.4, AI1.1, AI4.3, AI4.4, AI6.1, AI6.5, AI7.11, DS2.3, DS3.5, DS5.5, DS5.6, DS5.9, DS8.1,

13.2 Gestión de los incidentes y mejoras en la seguridad de la información	DS8.3, DS8.5, DS10.1, DS10.2, DS10.3, DS10.4, DS13.2, ME2.1, ME2.2, ME2.3, ME2.4.
14. Gestión de la Continuidad del Negocio 14.1 Aspectos de la seguridad de la información de la gestión de la continuidad del Negocio	PO3.1, PO7.5, AI1.1, AI1.2, AI6.5, DS2.1, DS4.1, DS4.2, DS4.3, DS4.4, DS4.5, DS4.6, DS4.8, DS10.1, DS8.3, DS10.2.
15. Cumplimiento 15.1 Cumplimiento de los requerimientos legales 15.2 Cumplimiento de las políticas y estándares de seguridad, y cumplimiento técnico 15.3 Consideraciones de auditoria de los sistemas de información	PO2.3, PO4.8, PO4.14, PO6.2, PO6.3, PO6.4, PO6.5, PO7.4, AI1.1, AI1.2, AI3.2, DS4.9, DS5.1, DS5.5, DS9.3, DS11.2, DS11.3, DS11.4, DS13.4, ME1.2, ME2.2, ME2.4, ME2.5, M3.1, M3.2, M3.7.

Tabla 4: Mapeo ISO 17799 y COBIT
Fuente: COBIT Security Baseline

2.2.4 DETERMINACIÓN DE LOS PROCESOS COBIT APLICABLES A LA AUDITORÍA.

La determinación de los procesos COBIT involucrados para realizar la auditoria de Riesgos Informáticos en el Departamento de Sistemas de Teleamazonas, fue realizada según el mapeo de los mismos con las normas ISO descritas anteriormente, los cuales se evaluarán estableciendo el grado de madurez de los procesos organizacionales. Dichos procesos se muestran a continuación (Tabla 5):

PLANEAR Y ORGANIZAR	
PO1	Definir el Plan Estratégico de TI
PO2	Definir la Arquitectura de la Información
PO3	Determinar la dirección tecnológica
PO4	Definir procesos, organización y relaciones de TI.
PO5	Administrar la inversión en TI.
PO6	Comunicar las aspiraciones y la dirección de la gerencia
PO7	Administrar recursos humanos de TI
PO9	Evaluar y Administrar Riesgos de TI
PO10	Administrar proyectos
ADQUIRIR E IMPLEMENTAR	
AI1	Identificar Soluciones Automatizadas
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
AI6	Administrar cambios
AI7	Instalar y Acreditar soluciones y cambios

ENTREGAR Y DAR SOPORTE	
DS2	Administrar servicios de terceros
DS3	Administrar desempeño y capacidad
DS4	Garantizar la Continuidad del Servicio
DS5	Garantizar la Seguridad de los Sistemas
DS7	Educar y entrenar a los usuarios
DS8	Administrar la mesa de servicio y los incidentes
DS9	Administrar la configuración
DS10	Administrar los problemas
DS11	Administrar los datos
DS12	Administrar el ambiente físico
DS13	Administrar las operaciones
MONITOREAR Y EVALUAR	
ME1	Monitorear y evaluar el Desempeño de TI
ME2	Monitorear y evaluar el control interno
ME3	Garantizar cumplimiento regulatorio

Tabla 5: Procesos aplicables a la auditoria de riesgos
Fuente: Creación de los autores

2.2.5 PLAN DE AUDITORÍA

A continuación se presentan las principales actividades para realizar este trabajo de Auditoria:

1. Recopilar y analizar información sobre COBIT aplicado a auditoria de riesgos informáticos
2. Recopilar y analizar las herramientas a utilizarse en la auditoria
3. Recopilar y analizar Información sobre el Departamento de Sistemas de TELEAMAZONAS
4. Recopilar y analizar información sobre Riesgos Informáticos
5. Analizar los riesgos existentes en el Departamento de Sistemas de TELEAMAZONAS
6. Ejecutar de la Auditoria de Riesgos Informáticos
7. Elaborar del Informe Final de Auditoria

Las personas responsables de la realización de la auditoria son:

- Marcia Cordero
- María del Carmen Ibujés

2.2.6 PUESTA EN MARCHA DEL PLAN DE AUDITORÍA

En la siguiente tabla (Tabla 6) se muestra los objetivos de control escogidos para realizar la auditoría y su impacto a los criterios de información y recursos de TI; la explicación de la misma ya se la realizó anteriormente.

OBJETIVOS DE CONTROL COBIT		Recursos TI de COBIT				Criterios de información de COBIT						
PLANEAR Y ORGANIZAR		PRESONAS	INFORMACION	APLICACIÓN	INFRAESTRUCTURA	EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	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	Definir la dirección tecnológica			X	X	P	P					
PO4	Definir los Procesos, Organización y Relaciones de TI	X				P	P					
PO5	Administrar la Inversión en TI	X		X	X	P	P					S
PO6	Comunicar las metas y la dirección de la gerencia	X	X			P					S	
PO7	Administrar los Recursos Humanos de TI	X				P	P					
PO9	Evaluar y Administrar los Riesgos de TI	X	X	X	X	S	S	P	P	P	S	S
PO10	Administrar los proyectos	X		X	X	P	P					
ADQUIRIR E IMPLANTAR												
AI1	Identificar las Soluciones Automatizadas			X	X	P	S					
AI2	Adquirir y Mantener 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	Procurar Recursos de TI	X	X	X	X	S	P				S	
AI6	Administrar los 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												
DS2	Administrar los Servicios de Terceros	X	X	X	X	P	P	S	S	S	S	S
DS3	Administrar el Desempeño y la Capacidad			X	X	P	P			S		
DS4	Asegurar el Servicio Continuo	X	X	X	X	P	S			P		
DS5	Garantizar la Seguridad de los Sistemas	X	X	X	X			P	P	S	S	S
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 el cumplimiento Regulatorio	X	X	X	X						P	S

Tabla 6: Impacto de los objetivos de control a aplicarse en la auditoria

Fuente: Creación de los autores

Para obtener los porcentajes de los criterios de información se asigna un valor al grado de impacto primario, secundario y blanco.

Para el análisis de resultados se toma como referencia el cuadro de interpretación (Tabla 7) según COSO (Sponsoring Organizations of the Treadway Commision) en cuanto al Nivel de Riesgo:

Calificación (%)		Grado de Confianza	Nivel de Riesgo
15%	50%	Bajo	Alto
51%	75%	Moderado	Moderado
76%	95%	Alto	Bajo
-	-	Vacío	Vacío

Tabla 7: Cuadro de Interpretación [1]
Fuente: COSO

Se genera una tabla de ponderación con el promedio de la calificación (Tabla 8) según la propuesta de COSO, con lo que se asigna un valor numérico al impacto de los criterios de información de cada proceso:

Nivel de Riesgo	Promedio	Grado de Confianza
Alto	32%	Bajo
Moderado	63%	Moderado
Bajo	86%	Alto

Tabla 8: Promedio de Nivel de Riesgo [2]
Fuente: COSO

Se coloca los valores propuestos en los criterios de Información que establece COBIT, dentro de cada uno de los procesos, utilizando la Tabla 8, especificando una calificación, como se puede ver en la Tabla 9; para el grado Primario se asigna el 86%, cuyo impacto es alto pero su nivel de riesgo es bajo; para el grado Secundario se asigna el 63% cuyo impacto y nivel de riesgo es moderado; y para

[1] Extraído de la tesis Análisis de la Gestión de las Tecnologías de la Información en la Unidad de Gestión de la Información de la EPN utilizando COBIT
[2] Extraído de la tesis Análisis de la Gestión de las Tecnologías de la Información en la Unidad de Gestión de la Información de la EPN utilizando COBIT

el caso vacío no se asigna ningún valor, ya que no impacta a los criterios de información y no tiene nivel de riesgo.

OBJETIVOS DE CONTROL COBIT		Criterios de información de COBIT						
PLANEAR Y ORGANIZAR		**EFECTIVIDAD**	**EFICIENCIA**	**CONFIDENCIALIDAD**	**INTEGRIDAD**	**DISPONIBILIDAD**	**CUMPLIMIENTO**	**CONFIABILIDAD**
PO1	Definir un plan estratégico de TI	0,86	0,63					
PO2	Definir la Arquitectura de la Información	0,63	0,86	0,63	0,86			
PO3	Definir la dirección tecnológica	0,86	0,86					
PO4	Definir los Procesos, Organización y Relaciones de TI	0,86	0,86					
PO5	Administrar la Inversión en TI	0,86	0,86					0,63
PO6	Comunicar las metas y la dirección de la gerencia	0,86					0,63	
PO7	Administrar los Recursos Humanos de TI	0,86	0,86					
PO9	Evaluar y Administrar los Riesgos de TI	0,63	0,63	0,86	0,86	0,86	0,63	0,63
PO10	Administrar los proyectos	0,86	0,86					
ADQUIRIR E IMPLANTAR								
AI1	Identificar las Soluciones Automatizadas	0,86	0,63					
AI2	Adquirir y Mantener Software Aplicativo	0,86	0,86		0,63			0,63
AI3	Adquirir y Mantener la Infraestructura Tecnológica	0,63	0,86		0,63	0,63		
AI4	Facilitar la operación y el uso	0,86	0,86		0,63	0,63	0,63	0,63
AI5	Procurar Recursos de TI	0,63	0,86				0,63	
AI6	Administrar los Cambios	0,86	0,86		0,86	0,86		0,63
AI7	Instalar y Acreditar soluciones y cambios	0,86	0,63		0,63	0,63		
ENTREGAR Y DAR SOPORTE								
DS2	Administrar los Servicios de Terceros	0,86	0,86	0,63	0,63	0,63	0,63	0,63
DS3	Administrar el Desempeño y la Capacidad	0,86	0,86			0,63		
DS4	Asegurar el Servicio Continuo	0,86	0,63			0,86		
DS5	Garantizar la Seguridad de los Sistemas			0,86	0,86	0,63	0,63	0,63
DS7	Educar y Entrenar a los Usuarios	0,86	0,63					
DS8	Administrar la mesa de Servicio y los Incidentes	0,86	0,86					
DS9	Administrar la Configuración	0,86	0,63			0,63		0,63
DS10	Administrar los Problemas	0,86	0,86			0,63		
DS11	Administrar los Datos				0,86			0,86
DS12	Administrar el Ambiente Físico				0,86	0,86		
DS13	Administrar las Operaciones	0,86	0,86		0,63	0,63		
MONITOREAR Y EVALUAR								
ME1	Monitorear y evaluar el desempeño de TI	0,86	0,86	0,63	0,63	0,63	0,63	0,63
ME2	Monitorear y evaluar el Control Interno	0,86	0,86	0,63	0,63	0,63	0,63	0,63
ME3	Garantizar el cumplimiento Regulatorio						0,86	0,63

Tabla 9: Resultados finales del impacto de los criterios de información

Fuente: COSO

MODELOS DE MADUREZ DE LOS PROCESOS

Se procede a la elaboración de cada una de las tablas de los modelos de madurez (Tabla 10 a Tabla 39), tomando en cuenta la situación del Departamento de Sistemas de Teleamazonas estudiada con la Norma ISO 17799 y luego respectivamente mapeado con COBIT; indicando con ello el grado de madurez y objetivos no cumplidos en cada uno de los procesos que establece COBIT.

DOMINIO: PLANEAR Y ORGANIZAR PO1: Definir el plan estratégico de TI			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando 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		**GRADO DE MADUREZ.** El proceso de definir el plan estratégico de TI se encuentra en el nivel 3
1 Inicial/Ad Hoc cuando 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 requisito de negocio específico. La planeación 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		
2 Repetible pero intuitiva cuando 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 y beneficios al usuario, resultado de decisiones estratégicas importantes se reconocen de forma intuitiva.	X		
3 Proceso definido cuando Una política define cómo y cuando realizar la planeación estratégica de TI. La planeación estratégica de TI sigue un enfoque estructurado, 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 gerentes individuales 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**	
4 Administrado y medible cuando 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 con responsabilidades de alto nivel. La dirección puede monitorear el proceso estratégico de 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 son necesarias. 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 aprovechar 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.			
5 Optimizado cuando 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 incluye cómo los nuevos avances tecnológicos pueden impulsar creación de nuevas capacidades de negocio y mejorar la ventaja competitiva de la organización.			

Tabla 10: MODELOS DE MADUREZ PO1

Fuente: Realizado por los autores

DOMINIO: PLANEAR Y ORGANIZAR PO2: Definir la arquitectura de la información			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando 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 la organización.	X		**GRADO DE MADUREZ.** El proceso de definir la arquitectura de la información se encuentra en el nivel 2
1 Inicial/Ad Hoc cuando 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		
2 Repetible pero intuitiva cuando 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 sus habilidades 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**	
3 Proceso definido cuando 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. Se definen, documentan y aplican actividades formales de entrenamiento de manera formal.			
4 Administrado y medible cuando 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 del 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 han identificado métricas básicas y existe un sistema de medición. El proceso de definición de la arquitectura de información es pro-activo 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 totalmente implantado. 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.			
5 Optimizado cuando 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 dar mantenimiento 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 un almacén de datos y tecnologías de minería de datos está 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.			

Tabla 11: MODELOS DE MADUREZ PO2

Fuente: Realizado por los autores

DOMINIO: PLANEAR Y ORGANIZAR PO3: Determinar la dirección tecnológica			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando No existe conciencia sobre la importancia de la planeación de la infraestructura tecnológica para la entidad. El conocimiento y la experiencia necesarios para desarrollar dicho plan de infraestructura tecnológica no existen. Hay una carencia de entendimiento de que la planeación del cambio tecnológico es crítica para asignar recursos de manera efectiva.	X		**GRADO DE MADUREZ.** El proceso de determinar la dirección tecnológica se encuentra en el nivel 3
1 Inicial/Ad Hoc cuando La gerencia reconoce la necesidad de planear la infraestructura tecnológica. El desarrollo de componentes tecnológicos y la implantación de tecnologías emergentes son ad hoc y aisladas. Existe un enfoque reactivo y con foco operativo hacia la planeación de 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 la tecnología es inconsistente.	X		
2 Repetible pero intuitiva cuando Se difunde la necesidad e importancia de la planeación tecnológica. La planeación es táctica y se enfoca en generar soluciones técnicas a problemas técnicos, en lugar de usar la tecnología para satisfacer las necesidades del negocio. La evaluación de los cambios 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 surgiendo técnicas y estándares comunes para el desarrollo de componentes de la infraestructura.	X		
3 Proceso definido cuando La gerencia está consciente de la importancia del plan de infraestructura tecnológica. El proceso para el plan de infraestructura tecnológica es razonablemente sólido y está alineado con el plan estratégico de TI. Existe un plan de infraestructura tecnológica definido, documentado y bien difundido, aunque se aplica de forma inconsistente. La orientación de la infraestructura tecnológica incluye el entendimiento de dónde la empresa desea ser líder y dónde desea rezagarse respecto al uso de tecnología, con base en los riesgos y en la alineación con la estrategia organizacional. Los proveedores clave se seleccionan con base en su entendimiento de la tecnología a largo plazo y de los planes de desarrollo de productos, de forma consistente con la dirección de la organización.		**X**	
4 Administrado y medible cuando La dirección garantiza el desarrollo del plan de infraestructura tecnológica. El equipo de TI cuenta con la experiencia y las habilidades necesarias para desarrollar un plan de infraestructura tecnológica. El impacto potencial de las tecnologías cambiantes y emergentes se toma en cuenta. La dirección puede identificar las desviaciones respecto al plan y anticipar los problemas. La responsabilidad del desarrollo y mantenimiento del plan de infraestructura tecnológica ha sido asignada. El proceso para desarrollar el plan de infraestructura tecnológica es sofisticado y sensible a los cambios. Se han incluido buenas prácticas internas en el proceso. La estrategia de recursos humanos está alineada con la dirección tecnológica, para garantizar que el equipo de TI pueda administrar los cambios tecnológicos. Los planes de migración para la introducción de nuevas tecnologías están definidos. Los recursos externos y las asociaciones se aprovechan para tener acceso a la experiencia y a las habilidades necesarias. La dirección ha evaluado la aceptación del riesgo de usar la tecnología como líder, o rezagarse en su uso, para desarrollar nuevas oportunidades de negocio o eficiencias operativas.			
5 Optimizado cuando Existe una función de investigación que revisa las tecnologías emergentes y evolutivas y para evaluar la organización por comparación contra las normas industriales. La dirección del plan de infraestructura tecnológica está impulsada por los estándares y avances industriales e internacionales, en lugar de estar orientada por los proveedores de tecnología. El impacto potencial de los cambios tecnológicos sobre el negocio se revisa al nivel de la alta dirección. Existe una aprobación ejecutiva formal para el cambio de la dirección 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 un proceso continuo y reforzado para mejorar el plan de infraestructura tecnológica. Las mejores prácticas de la industria se usan de forma amplia para determinar la dirección técnica.			

Tabla 12: MODELOS DE MADUREZ PO3

Fuente: Realizado por los autores

DOMINIO: PLANEAR Y ORGANIZAR PO4: Definir procesos, organización y relaciones de TI			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando La organización de TI no está establecida de forma efectiva para enfocarse en el logro de los objetivos del negocio.	X		**GRADO DE MADUREZ.** El proceso de definir el plan estratégico de TI se encuentra en el nivel 3
1 Inicial/Ad Hoc cuando Las actividades y funciones de TI son reactivas y se implantan de forma inconsistente. IT se involucra en los proyectos solamente en las etapas finales. La función de TI se considera como una función de soporte, sin una perspectiva organizacional general. Existe un entendimiento explícito de la necesidad de una organización de TI; sin embargo, los roles y las responsabilidades no están formalizadas ni reforzadas.	X		
2 Repetible pero intuitiva cuando La función de TI está organizada para responder de forma táctica aunque de forma inconsistente, a las necesidades de los clientes y a las relaciones con los proveedores. La necesidad de contar con una organización estructurada y una administración de proveedores se comunica, pero las decisiones todavía dependen del conocimiento y habilidades de individuos clave. Surgen técnicas comunes para administrar la organización de TI y las relaciones con los proveedores.	X		
3 Proceso definido cuando 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, auditoria 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. Los requerimientos esenciales de personal de TI y experiencia están definidos y satisfechos. Existe una definición formal de las relaciones con los usuarios y con terceros. La división de roles y responsabilidades está definida e implantada.		**X**	
4 Administrado y medible cuando La organización de TI responde de forma pro-activa al cambio e incluye todos los roles necesarios para satisfacer los requerimientos del negocio. La administración, la propiedad de procesos, la delegación y la responsabilidad de TI están definidas y balanceadas. Se han aplicado buenas prácticas internas en la organización de las funciones de TI. La gerencia de TI cuenta con la experiencia y habilidades apropiadas para definir, implantar y monitorear la organización deseada y las relaciones. Las métricas medibles para dar soporte a los objetivos del negocio y los factores críticos de éxito definidos por el usuario siguen un estándar. Existen inventarios de habilidades para apoyar al personal de los proyectos y el desarrollo profesional. El equilibrio entre las habilidades y los recursos disponibles internamente, y los que se requieren de organizaciones externas están definidos y reforzados. La estructura organizacional de TI refleja de manera apropiada las necesidades del negocio proporcionando servicios alineados con los procesos estratégicos del negocio, en lugar de estar alineados con tecnologías aisladas.			
5 Optimizado cuando 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.			

Tabla 13: MODELOS DE MADUREZ PO4

Fuente: Realizado por los autores

DOMINIO: PLANEAR Y ORGANIZAR PO5: Administrar la inversión en TI			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando No existe conciencia de la importancia de la selección y presupuesto de las inversiones en TI. No existe seguimiento o monitoreo de las inversiones y gastos de TI	X		**GRADO DE MADUREZ.** El proceso de Administrar la inversión de TI se encuentra en el nivel 1
1 Inicial/Ad Hoc cuando La organización reconoce la necesidad de administrar la inversión en TI, aunque esta necesidad se comunica de manera inconsistente. La asignación de responsabilidades de selección de inversiones en TI y de desarrollo de presupuestos se hace de una forma ad hoc. Existen implantaciones aisladas de selección y presupuesto de inversiones en TI, con documentación informal. Las inversiones en TI se justifican de una forma ad hoc. Se toman decisiones presupuestales enfocadas de modo reactivo y operativo.		**X**	
2 Repetible pero intuitiva cuando Existe un entendimiento implícito de la necesidad de seleccionar y presupuestar las inversiones en TI. La necesidad de un proceso de selección y presupuesto se comunica. El cumplimiento depende de la iniciativa de individuos dentro de la organización. Surgen técnicas comunes para desarrollar componentes del presupuesto de TI. Se toman decisiones presupuestales reactivas y tácticas.			
3 Proceso definido cuando Las políticas y los procesos para inversiones y presupuestos están definidas, documentadas y comunicadas y cubren temas clave de negocio y de tecnología. El presupuesto de TI está alineado con los planes estratégicos de TI y con los planes del negocio. Los procesos de selección de inversiones en TI y de presupuestos están formalizados, documentados y comunicados. Surge el entrenamiento formal aunque todavía se basa de modo principal en iniciativas individuales. Ocurre la aprobación formal de la selección de inversiones en TI y presupuestos. El personal de TI cuenta con la experiencia y habilidades necesarias para desarrollar el presupuesto de TI y recomendar inversiones apropiadas en TI.			
4 Administrado y medible cuando La responsabilidad y la rendición de cuentas por la selección y presupuestos de inversiones se asignan a un individuo específico. Las diferencias en el presupuesto se identifican y se resuelven. Se realizan análisis formales de costos que cubren los costos directos e indirectos de las operaciones existentes, así como propuestas de inversiones, considerando todos los costos a lo largo del ciclo completo de vida. Se usa un proceso de presupuestos pro-activo y estándar. El impacto en los costos operativos y de desarrollo debidos a cambios en hardware y software, hasta cambios en integración de sistemas y recursos humanos de TI, se reconoce en los planes de inversión. Los beneficios y los retornos se calculan en términos financieros y no financieros.			
5 Optimizado cuando Se utilizan las mejores prácticas de la industria para evaluar los costos por comparación e identificar la efectividad de las inversiones. Se utiliza el análisis de los avances tecnológicos en el proceso de selección y presupuesto de inversiones. El proceso de administración de inversiones se mejora de forma continua con base en las lecciones aprendidas provenientes del análisis del desempeño real de las inversiones. Las decisiones de inversiones incluyen las tendencias de mejora de precio/desempeño. Se investigan y evalúan formalmente las alternativas de financiamiento dentro del contexto de la estructura de capital existente en la organización, mediante el uso de métodos formales de evaluación. Existe la identificación pro-activa de varianzas. Se incluye un análisis de los costos y beneficios a largo plazo del ciclo de vida total en la toma de decisiones de inversión.			

Tabla 14: MODELOS DE MADUREZ PO5

Fuente: Realizado por los autores

DOMINIO: PLANEAR Y ORGANIZAR PO6: Comunicar las aspiraciones y la dirección de la gerencia			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando 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		**GRADO DE MADUREZ.** El proceso de comunicar las aspiraciones y la dirección de la gerencia se encuentra en el nivel 3
1 Inicial/Ad Hoc cuando La gerencia es reactiva al resolver los requerimientos del ambiente de control de información. Las políticas, procedimientos estándares se elaboran y comunican de forma ad hoc de acuerdo a los temas. Los procesos de elaboración, comunicación y cumplimiento son informales e inconsistentes.	X		
2 Repetible pero intuitiva cuando La gerencia tiene un entendimiento implícito de las necesidades y de los requerimientos de un ambiente de control de información efectivo, 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 se reconoce como una filosofía deseable a seguir, pero las prácticas se dejan a discreción de gerentes individuales. El entrenamiento se realiza de forma individual, según se requiera.	X		
3 Proceso definido cuando 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 están estandarizadas y formalizadas.		**X**	
4 Administrado y medible cuando 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 información positivo y proactivo. Se ha establecido un juego completo de políticas, procedimientos y estándares, los cuales se mantienen y comunican, y forman un componente de buenas prácticas internas. Se ha establecido un marco de trabajo para la implantación y las verificaciones subsiguientes de cumplimiento.			
5 Optimizado cuando 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 de concienciación y para optimizar la comunicación, usando herramientas de automatización de oficina y de entrenamiento basado en computadora.			

Tabla 15: MODELOS DE MADUREZ PO6

Fuente: Realizado por los autores

DOMINIO: PLANEAR Y ORGANIZAR PO7: Administrar recursos humanos de TI			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando 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		**GRADO DE MADUREZ.** El proceso de administrar recursos humanos de TI se encuentra en el nivel 3
1 Inicial/Ad Hoc cuando La gerencia reconoce la necesidad de contar con administración de recursos humanos de TI. El proceso de administración de recursos 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		
2 Repetible pero intuitiva cuando Existe un enfoque táctico para contratar y administrar al personal de TI, dirigido por necesidades específicas de proyectos, en lugar de hacerlo 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		
3 Proceso definido cuando 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 formal está diseñado para satisfacer las necesidades de los recursos humanos de TI. Está establecido un programa de rotación, diseñado para expandir las habilidades gerenciales y de negocio.		**X**	
4 Administrado y medible cuando La responsabilidad de la elaboración y el mantenimiento de un plan de administración de recursos humanos para TI ha sido asignado 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 métricas estandarizadas 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 están estableciendo y se comparan con otras organizaciones de TI y con las mejores prácticas de la industria. La administración de recursos humanos es proactiva, tomando en cuenta el desarrollo de un plan de carrera.			
5 Optimizado cuando 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 de su implantación en la organización.			

Tabla 16: MODELOS DE MADUREZ PO7

Fuente: Realizado por los autores

DOMINIO: PLANEAR Y ORGANIZAR PO9: Evaluar y administrar riesgos de TI			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando La evaluación de riesgos para los procesos y las decisiones de negocio no ocurre. La organización no toma en cuenta los impactos en el negocio asociados a las vulnerabilidades de seguridad y a las incertidumbres del desarrollo de proyectos. La administración de riesgos no se ha identificado como algo relevante para adquirir soluciones de TI y para prestar servicios de TI	X		**GRADO DE MADUREZ.** El proceso de evaluar y administrar riesgos de TI se encuentra en el nivel 2.
1 Inicial/Ad Hoc cuando Los riesgos de TI se toman en cuenta de manera ad hoc. Se realizan evaluaciones informales de riesgos según lo determine cada proyecto. En algunas ocasiones se identifican evaluaciones de riesgos en un plan de proyectos pero se asignan a gerentes específicos con poca frecuencia. Los riesgos específicos relacionados con TI tales como seguridad, disponibilidad e integridad se toman en cuenta ocasionalmente proyecto por proyecto. Los riesgos relativos a TI que afectan las operaciones del día con día, son rara vez discutidas en reuniones gerenciales. Cuando se toman en cuenta los riesgos, la mitigación es inconsistente. Existe un entendimiento emergente de que los riesgos de TI son importantes y necesitan ser considerados.	X		
2 Repetible pero intuitiva cuando Existe un enfoque de evaluación de riesgos inmaduro y en evolución y se implanta a discreción de los gerentes de proyecto. La administración de riesgos se da por lo general a altos niveles y se aplica de manera típica solo a proyectos grandes o como respuesta a problemas. Los procesos de mitigación de riesgos están en implantación donde se identifican riesgos.		**X**	
3 Proceso definido cuando 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 riesgos está disponible para todo el personal. La decisión de seguir el proceso de administración de riesgos y de recibir entrenamiento se delega a la discreción del individuo. La metodología para la evaluación de riesgos es convincente y sólida, y garantiza que los riesgos claves sean identificados. Un proceso para mitigar los riesgos clave por lo general se institucionaliza una vez que los riesgos se identifican. Las descripciones de puestos toman en cuenta las responsabilidades de administración de riesgos.			
4 Administrado y medible cuando 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 riesgos está disponible para todo el personal. La decisión de seguir el proceso de administración de riesgos y de recibir entrenamiento se delega a la discreción del individuo. La metodología para la evaluación de riesgos es convincente y sólida, y garantiza que los riesgos claves sean identificados. Un proceso para mitigar los riesgos clave por lo general se institucionaliza una vez que los riesgos se identifican. Las descripciones de puestos toman en cuenta las responsabilidades de administración de riesgos.			
5 Optimizado cuando 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 de administración 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 el negocio y en las operaciones de TI está bien aceptada, y abarca a los usuarios de servicios de TI. La dirección detectará y actuará cuando se realicen decisiones grandes de inversión, operación o de TI, sin tomar en cuenta el plan de administración de riesgos. La dirección evalúa las estrategias de mitigación de riesgos de manera continua.			

Tabla 17: MODELOS DE MADUREZ PO9

Fuente: Realizado por los autores

DOMINIO: PLANEAR Y ORGANIZAR PO10: Administrar proyectos			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando Las técnicas de administración de proyectos no se usan y la organización no toma en cuenta los impactos al negocio asociados con la mala administración de los proyectos y con las fallas de desarrollo en el proyecto.	X		**GRADO DE MADUREZ.** El proceso de administrar proyectos se encuentra en el nivel 2.
1 Inicial/Ad Hoc cuando 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, calendarios 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		
2 Repetible pero intuitiva cuando La alta dirección ha obtenido y comunicado la conciencia de la necesidad de una administración de los proyectos de TI. La organización está en proceso de desarrollar y utilizar algunas técnicas y métodos de proyecto a 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 del gerente de proyecto.		**X**	
3 Proceso definido cuando 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 y responsabilidades iniciales definidas. Los proyectos de TI se monitorean, con puntos clave, calendarios y mediciones de presupuesto y desempeño definidos y actualizados. Existe entrenamiento para la administración de proyectos. El entrenamiento en administración de proyectos es un resultado principalmente de las iniciativas individuales del equipo. Los procedimientos de aseguramiento de calidad y las actividades de implantación post-sistema han sido definidos, pero no se aplican de manera amplia por parte de los gerentes de TI. Los proyectos se empiezan a administrar como portafolios.			
4 Administrado y medible cuando 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 solo 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 ha implantado 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 las específicas a TI. Existe un apoyo fuerte y activo a los proyectos por parte de los patrocinadores de la alta dirección, así como de los interesados. El entrenamiento relevante sobre administración de proyectos se planea para el equipo en la oficina de proyectos y a lo largo de la función de TI.			
5 Optimizado cuando 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. La oficina integrada de administración de proyectos es responsable de los proyectos y 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.			

Tabla 18: MODELOS DE MADUREZ PO10

Fuente: Realizado por los autores

DOMINIO: ADQUIRIR E IMPLANTAR AI1: Identificar soluciones automatizadas			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando La organización no requiere de la identificación de los requerimientos funcionales y operativos para el desarrollo, implantación o modificación de soluciones, tales como sistemas, servicios, infraestructura y datos. La organización no está consciente de las soluciones tecnológicas disponibles que son potencialmente relevantes para su negocio.	X		**GRADO DE MADUREZ.** El proceso de identificar soluciones automatizadas se encuentra en el nivel 3
1 Inicial/Ad Hoc cuando Existe conciencia de la necesidad de definir requerimientos y de identificar soluciones tecnológicas. Grupos individuales se reúnen para analizar las necesidades de manera informal y los requerimientos se documentan algunas veces. Los individuos identifican soluciones con base en una conciencia limitada de mercado o como respuesta a ofertas de proveedores. Existe una investigación o análisis estructurado mínimo de la tecnología disponible.	X		
2 Repetible pero intuitiva cuando Existen algunos enfoques intuitivos para identificar que existen soluciones de TI y éstos varían a lo largo del negocio. Las soluciones se identifican de manera informal con base en la experiencia interna y en el conocimiento de la función de TI. El éxito de cada proyecto depende de la experiencia de unos cuantos individuos clave. La calidad de la documentación y de la toma de decisiones varía de forma considerable. Se usan enfoques no estructurados para definir los requerimientos e identificar las soluciones tecnológicas.	X		
3 Proceso definido cuando Existen enfoques claros y estructurados para determinar las soluciones de TI. El enfoque para la determinación de las soluciones de TI requiere la consideración de alternativas evaluadas contra los requerimientos del negocio o del usuario, las oportunidades tecnológicas, la factibilidad económica, las evaluaciones de riesgo y otros factores. El proceso para determinar las soluciones de TI se aplica para algunos proyectos con base en factores tales como las decisiones tomadas por el personal involucrado, la cantidad de tiempo administrativo dedicado, y el tamaño y prioridad del requerimiento de negocio original. Se usan enfoques estructurados para definir requerimientos e identificar soluciones de TI.		**X**	
4 Administrado y medible cuando Existe una metodología establecida para la identificación y la evaluación de las soluciones de TI y se usa para la mayoría de los proyectos. La documentación de los proyectos es de buena calidad y cada etapa se aprueba adecuadamente. Los requerimientos están bien articulados y de acuerdo con las estructuras predefinidas. Se consideran soluciones alternativas, incluyendo el análisis de costos y beneficios. La metodología es clara, definida, generalmente entendida y medible. Existe una interfaz definida de forma clara entre la gerencia de TI y la del negocio para la identificación y evaluación de las soluciones de TI.			
5 Optimizado cuando La metodología para la identificación y evaluación de las soluciones de TI está sujeta a una mejora continua. La metodología de adquisición e implantación tiene la flexibilidad para proyectos de grande y de pequeña escala. La metodología está soportada en bases de datos de conocimiento internas y externas que contienen material de referencia sobre soluciones tecnológicas. La metodología en sí misma genera documentación en una estructura predefinida que hace que la producción y el mantenimiento sean eficientes. Con frecuencia, se identifican nuevas oportunidades de uso de la tecnología para ganar una ventaja competitiva, ejercer influencia en la re-ingeniería de los procesos de negocio y mejorar la eficiencia en general. La gerencia detecta y toma medidas si las soluciones de TI se aprueban sin considerar tecnologías alternativas o los requerimientos funcionales del negocio.			

Tabla 19: MODELOS DE MADUREZ AI1

Fuente: Realizado por los autores

DOMINIO: ADQUIRIR E IMPLANTAR AI2: Adquirir y mantener el software aplicativo			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando No existe un proceso de diseño y especificación de aplicaciones. Típicamente, las aplicaciones se obtienen con base en ofertas de proveedores, en el reconocimiento de la marca o en la familiaridad del personal de TI con productos específicos, considerando poco o nada los requerimientos actuales.	X		**GRADO DE MADUREZ.** El proceso de adquirir y mantener el software aplicativo se encuentra en el nivel 3
1 Inicial/Ad Hoc cuando Existe conciencia de la necesidad de contar con un proceso de adquisición y mantenimiento de aplicaciones. Los enfoques para la adquisición 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 resultado ineficiencias en el mantenimiento y soporte. Se tiene poca consideración hacia la seguridad y disponibilidad de la aplicación en el diseño o adquisición de software aplicativo.	X		
2 Repetible pero intuitiva cuando Existen procesos de adquisición y mantenimiento de aplicaciones, con diferencias pero similares, en base a la experiencia dentro de la 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 software aplicativo.	X		
3 Proceso definido cuando Existe un proceso claro, definido y de comprensión general para la adquisición y mantenimiento de software aplicativo. Este proceso va 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 muy probable que se salten pasos. Las actividades de mantenimiento se planean, programan y coordinan.		**X**	
4 Administrado y medible cuando Existe una metodología formal y bien comprendida que incluye un proceso de diseño y especificación, un criterio de adquisición, un proceso 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 a la medida de la organización, los utilizan todo el personal y son apropiados para la mayoría de los requerimientos de aplicación.			
5 Optimizado cuando Las prácticas de adquisición y mantenimiento de software aplicativo se alinean con el proceso definido. El enfoque es con base en componentes, 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 un posicionamiento estratégico rápido, que permite un alto grado de reacción y flexibilidad para responder a requerimientos cambiantes del negocio. La metodología de adquisición e implantación de software aplicativo ha sido sujeta a mejora continua y se soporta con bases de datos internas y externas que contienen materiales de referencia y las mejores prácticas. La metodología produce documentación dentro de una estructura predefinida que hace eficiente la producción y mantenimiento.			

Tabla 20: MODELOS DE MADUREZ AI2

Fuente: Realizado por los autores

DOMINIO: ADQUIRIR E IMPLANTAR AI3: Adquirir y mantener la infraestructura tecnológica			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando No se reconoce la administración de la infraestructura de tecnología como un asunto importante al cual deba ser resuelto.	X		**GRADO DE MADUREZ.** El proceso de adquirir y mantener la infraestructura tecnológica se encuentra en el nivel 3.
1 Inicial/Ad Hoc cuando Se realizan cambios a la infraestructura para cada nueva aplicación, sin ningún plan en conjunto. Aunque se tiene la percepción de que la infraestructura de TI es importante, no existe un enfoque general consistente. La actividad de mantenimiento reacciona a necesidades de corto plazo. El ambiente de producción es el ambiente de prueba.	X		
2 Repetible pero intuitiva cuando No hay consistencia entre enfoques tácticos al adquirir y dar mantenimiento a la infraestructura de TI. La adquisición y mantenimiento de la infraestructura de TI no se basa en una estrategia definida y no considera las necesidades de las aplicaciones del negocio que se 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 un ambiente de prueba por separado.	X		
3 Proceso definido cuando Existe un claro, definido y generalmente entendido proceso para adquirir y dar mantenimiento a la infraestructura TI. El proceso respalda las necesidades de las aplicaciones críticas del negocio y concuerda con la estrategia de negocio de TI, pero no se aplica en forma consistente. Se planea, programa y coordina el mantenimiento. Existen ambientes separados para prueba y producción.		**X**	
4 Administrado y medible cuando Se desarrolla el proceso de adquisición y mantenimiento de la infraestructura de tecnología a tal punto que funciona bien para la mayoría de las situaciones, se le da un seguimiento consistente y un enfoque hacia la reutilización. La infraestructura de TI soporta adecuadamente las aplicaciones del negocio. El proceso está bien organizado y es preventivo. Tanto el costo como el tiempo de realización para alcanzar el nivel esperado de escalamiento, flexibilidad e integración se han optimizado parcialmente.			
5 Optimizado cuando El proceso de adquisición y mantenimiento de la infraestructura de tecnología es preventivo y está estrechamente en línea con las aplicaciones críticas del negocio y con la arquitectura de la tecnología. Se siguen buenas prácticas respecto a las soluciones de tecnología, y la organización tiene conciencia de las últimas plataformas desarrolladas y herramientas de administración. Se reducen costos al racionalizar y estandarizar los componentes de la infraestructura y con el uso de la automatización. Con un alto nivel de conciencia se pueden identificar los medios óptimos para mejorar el desempeño en forma preventiva, incluyendo el considerar la opción de contratar servicios externos. La infraestructura de TI se entiende como el apoyo clave para impulsar el uso de TI			

Tabla 21: MODELOS DE MADUREZ AI3

Fuente: Realizado por los autores

DOMINIO: ADQUIRIR E IMPLANTAR AI4: Facilitar la operación y el uso			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando 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		**GRADO DE MADUREZ.** El proceso de facilitar la operación y el uso se encuentra en el nivel 3.
1 Inicial/Ad Hoc cuando Existe la percepción de que la documentación de proceso es necesaria. La documentación se genera ocasionalmente y se distribuye en forma desigual a grupos limitados. Mucha de la documentación y muchos de los procedimientos ya caducaron. Los materiales de entrenamiento tienden a ser esquemas únicos con calidad variable. Virtualmente no existen procedimientos 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.	X		
2 Repetible pero intuitiva cuando Se utilizan enfoques similares para generar procedimientos y documentación, pero no se basan en un enfoque estructural o marco de trabajo. No hay un enfoque uniforme para el desarrollo de procedimientos de usuario y de operación. Individuos o equipos de proyecto generan los materiales de entrenamiento, y la calidad depende de los individuos que se involucran. Los procedimientos y la calidad del soporte al usuario van desde pobre a muy buena, con una consistencia e integración muy pequeña a lo largo de la organización. 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		
3 Proceso definido cuando Existe un esquema bien definido, aceptado y comprendido para documentación del usuario, manuales de operación y materiales de entrenamiento. Se guardan y se mantienen los procedimientos en una biblioteca formal y cualquiera que necesite saber tiene acceso a ella. Las correcciones a la documentación y a los procedimientos se realizan por reacción. Los procedimientos se encuentran disponibles fuera de línea y se pueden acceder y mantener en caso de desastre. Existe un proceso que especifica las actualizaciones de procedimientos y los materiales de entrenamiento para que sea un entregable explícito de un proyecto de cambio. A pesar de la existencia de enfoques definidos, el contenido actual varía debido a que no hay un control para reforzar el cumplimiento de estándares. Los usuarios se involucran en los procesos informalmente. Cada vez se utilizan más herramientas automatizadas en la generación y distribución de procedimientos. Se planea y programa tanto el entrenamiento del negocio como de los usuario.		**X**	
4 Administrado y medible cuando Existe un esquema definido para los procedimientos de mantenimiento y para los materiales de entrenamiento que cuentan con el soporte de la administración de TI. El enfoque considerado para los procedimientos de mantenimiento y los manuales de entrenamiento cubren todos los sistemas y las unidades de negocio, de manera que se pueden observar los procesos desde una perspectiva de negocio. Los procedimientos y materiales de entrenamiento se integran para que contengan interdependencias e interfases. Existen controles para garantizar que se adhieren los estándares 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 evalúa como parte de un proceso continuo de mejora. Los materiales de documentación y entrenamiento se encuentran generalmente a un buen nivel, predecible, de confiabilidad y disponibilidad. Se implanta un proceso emergente para el uso de documentación y administración automatizada de procedimiento. El desarrollo automatizado de procedimientos se integra cada vez más con el desarrollo de sistemas aplicativos, facilitando la consistencia y el acceso al usuario. El entrenamiento de negocio y usuario es sensible a las necesidades del negocio. La administración de TI está desarrollando medidas para el desarrollo y la entrega de documentación, materiales y programas de entrenamiento.			
5 Optimizado cuando El proceso para la documentación de usuario y de operación se mejora constantemente con la adopción de nuevas herramientas o métodos. Los materiales de procedimiento y de entrenamiento se tratan como una base de conocimiento en evolución constante que se mantiene en forma electrónica, con el uso de administración de conocimiento actualizada, workflow y tecnologías de distribución, 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 de documentación y entrenamiento como la entrega de programas de entrenamiento, se encuentran completamente integrados con el negocio y con las definiciones de proceso del negocio, siendo así un apoyo a los requerimientos de toda la organización y no tan sólo procedimientos orientados a TI.			

Tabla 22: MODELOS DE MADUREZ AI4

Fuente: Realizado por los autores

DOMINIO: ADQUIRIR E IMPLANTAR AI5: Adquirir recursos de TI			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando No existe un proceso definido de adquisición de recursos de TI. La organización no reconoce la necesidad de tener políticas y procedimientos claros de adquisición para garantizar que todos los recursos de TI se encuentren disponibles y de forma oportuna y rentable.	X		**GRADO DE MADUREZ.** El proceso de Adquirir recursos de TI se encuentra en el nivel 1.
1 Inicial/Ad Hoc cuando 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 y administrados por gerentes de proyecto y otras personas que ejercen su juicio profesional más que seguir resultados de procedimientos y políticas formales. Sólo existe un relación *ad hoc* entre los procesos de administración de adquisiciones y contratos corporativos y TI. Los contratos de adquisición se administran a la terminación de los proyectos más que sobre una base continua.		**X**	
2 Repetible pero intuitiva cuando 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 de adquisición se utilizan principalmente en proyectos mayores y bastante visibles. Se determinan responsabilidades y rendición de cuentas 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 procesos de contrato se utilizan principalmente en proyectos mayores o muy visibles.			
3 Proceso definido cuando La administración establece políticas y procedimientos para la adquisición de TI. Las políticas y procedimientos toman como guía el proceso general de adquisición de la organización. La adquisición de TI se integra en gran parte con los sistemas generales de adquisición del negocio. Existen estándares de TI para la adquisición de recursos de TI. Los proveedores de recursos de TI se integran dentro de los mecanismos de administración 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 la función de TI.			
4 Administrado y medible cuando La adquisición de TI se integra totalmente con los sistemas generales de adquisición de la organización. Se utilizan los estándares para 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 los objetivos de negocio. La administración está consciente por lo general, de las excepciones a las políticas y procedimientos para la adquisición de TI. Se está desarrollando una administración 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.			
5 Optimizado cuando La administración instituye y da recursos a procesos exhaustivos para la adquisición de TI. La administración impulsa el cumplimiento de 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 los proveedores y socios, y se mide y vigila la calidad de estas relaciones. Se manejan las relaciones en forma estratégica. Los estándares, políticas y procedimientos de TI para la adquisición de recursos TI se manejan estratégicamente y responden a la medición 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.			

Tabla 23: MODELOS DE MADUREZ AI5

Fuente: Realizado por los autores

DOMINIO: ADQUIRIR E IMPLANTAR AI6: Administrar cambios			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando No existe un proceso definido de administración de cambio y los cambios se pueden realizar virtualmente sin control. No hay conciencia de que el cambio puede causar una interrupción para TI y las operaciones del negocio y no hay conciencia de los beneficios de la buena administración de cambio.	X		**GRADO DE MADUREZ.** El proceso de administrar cambios se encuentra en el nivel 1.
1 Inicial/Ad Hoc cuando Se reconoce que los cambios se deben administrar y controlar. Las prácticas varían y es muy probable que se puedan dar cambios sin autorización. Hay documentación de cambio pobre o no existente y la documentación de configuración es incompleta y no confiable. Es posible que ocurran errores junto con interrupciones al ambiente de producción, provocados por una pobre administración de cambios.		**X**	
2 Repetible pero intuitiva cuando Existe un proceso de administración de cambio informal y la mayoría de los cambios siguen este enfoque; sin embargo, el proceso no está estructurado, es rudimentario y propenso a errores. La exactitud de la documentación de la configuración es inconsistente y de planeación limitada y la evaluación de impacto se da previa al cambio.			
3 Proceso definido cuando Existe un proceso formal definido para la administración del cambio, que incluye la categorización, asignación de prioridades, procedimientos de emergencia, autorización del cambio y administración de liberación, y va surgiendo el cumplimiento. Se dan soluciones temporales a los problemas y los procesos a menudo se omiten o se hacen a un lado. Aún pueden ocurrir errores y los cambios no autorizados ocurren ocasionalmente. El análisis de impacto de los cambios de TI en operaciones de negocio se está volviendo formal, para apoyar la implantación planeada de nuevas aplicaciones y tecnologías.			
4 Administrado y medible cuando El proceso de administración de cambio se desarrolla bien y es consistente para todos los cambios, y la gerencia confía que hay excepciones mínimas. El proceso es eficiente y efectivo, pero se basa en manuales de procedimientos y controles considerables para garantizar el logro de la calidad. Todos los cambios están sujetos a una planeación minuciosa y a la evaluación del impacto para minimizar la probabilidad de tener problemas de post-producción. Se da un proceso de aprobación para cambios. La documentación de administración de cambios es vigente y correcta, con seguimiento formal a los cambios. La documentación de configuración es generalmente exacta. La planeación e implantación de la administración de cambios en TI se van integrando con los cambios en los procesos de negocio, para asegurar que se resuelven los asuntos referentes al entrenamiento, cambio organizacional y continuidad del negocio. Existe una coordinación creciente entre la administración de cambio de TI y el rediseño del proceso de negocio. Hay un proceso consistente para monitorear la calidad y el desempeño del proceso de administración de cambios.			
5 Optimizado cuando El proceso de administración de cambios se revisa con regularidad y se actualiza para permanecer en línea con las buenas prácticas. El proceso de revisión refleja los resultados del monitoreo. La información de la configuración es computarizada y proporciona un control de versión. El rastreo del cambio es sofisticado e incluye herramientas para detectar software no autorizado y sin licencia. La administración de cambio de TI se integra con la administración de cambio del negocio para garantizar que TI sea un factor que hace posible el incremento de productividad y la creación de nuevas oportunidades de negocio para la organización.			

Tabla 24: MODELOS DE MADUREZ AI6

Fuente: Realizado por los autores

DOMINIO: ADQUIRIR E IMPLANTAR AI7: Instalar y acreditar soluciones y cambios			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando Hay una ausencia completa de procesos formales de instalación o acreditación y ni la gerencia senior ni el personal de TI reconocen la necesidad de verificar que las soluciones se ajustan para el propósito deseado.	X		**GRADO DE MADUREZ.** El proceso de instalar y acreditar soluciones y cambios se encuentra en el nivel 3.
1 Inicial/Ad Hoc cuando Existe la percepción de la necesidad de verificar y confirmar que las soluciones implantadas sirven para el propósito esperado. Las pruebas se realizan para algunos proyectos, pero la iniciativa de pruebas se deja a los equipos de proyectos particulares y los enfoques que se toman varían. La acreditación formal y la autorización son raras o no existentes.	X		
2 Repetible pero intuitiva cuando Existe cierta consistencia entre los enfoques de prueba y acreditación, pero por lo regular no se basan en ninguna metodología. Los equipos individuales de desarrollo deciden normalmente el enfoque de prueba y casi siempre hay ausencia de pruebas de integración. Hay un proceso de aprobación informal.	X		
3 Proceso definido cuando Se cuenta con una metodología formal en relación con la instalación, migración, conversión y aceptación. Los procesos de TI para instalación y acreditación están integrados dentro del ciclo de vida del sistema y están automatizados hasta cierto punto. El entrenamiento, pruebas y transición y acreditación a producción tienen muy probablemente variaciones respecto al proceso definido, con base en las decisiones individuales. La calidad de los sistemas que pasan a producción es inconsistente, y los nuevos sistemas a menudo generan un nivel significativo de problemas posteriores a la implantación.		**X**	
4 Administrado y medible cuando Los procedimientos son formales y se desarrollan para ser organizados y prácticos con ambientes de prueba definidos y con procedimientos de acreditación. En la práctica, todos los cambios mayores de sistemas siguen este enfoque formal. La evaluación de la satisfacción a los requerimientos del usuario es estándar y medible, y produce mediciones que la gerencia puede revisar y analizar de forma efectiva. La calidad de los sistemas que entran en producción es satisfactoria para la gerencia, aún con niveles razonables de problemas posteriores a la implantación. La automatización del proceso es *ad hoc* y depende del proyecto. Es posible que la gerencia esté satisfecha con el nivel actual de eficiencia a pesar de la ausencia de una evaluación posterior a la implantación. El sistema de prueba refleja adecuadamente el ambiente de producción. La prueba de stress para los nuevos sistemas y la prueba de regresión para sistemas existentes se aplican para proyectos mayores.			
5 Optimizado cuando Los procesos de instalación y acreditación se han refinado a un nivel de buena práctica, con base en los resultados de mejora continua y refinamiento. Los procesos de TI para la instalación y acreditación están totalmente integrados dentro del ciclo de vida del sistema y se automatizan cuando es apropiado, arrojando el estatus más eficiente de entrenamiento, pruebas y transición a producción para los nuevos sistemas. Los ambientes de prueba bien desarrollados, los registros de problemas y los procesos de resolución de fallas aseguran la transición eficiente y efectiva al ambiente de producción. La acreditación toma lugar regularmente sin repetición de trabajos, y los problemas posteriores a la implantación se limitan normalmente a correcciones menores. Las revisiones posteriores a la implantación son estándar, y las lecciones aprendidas se canalizan nuevamente hacia el proceso para asegurar el mejoramiento continuo de la calidad. Las pruebas de stress para los nuevos sistemas y las pruebas de regresión para sistemas modificados se aplican en forma consistente.			

Tabla 25: MODELOS DE MADUREZ AI7

Fuente: Realizado por los autores

DOMINIO: ENTREGAR Y DAR SOPORTE DS2: Administrar los servicios de terceros			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando Las responsabilidades y la rendición de cuentas no están definidas. No hay políticas y procedimientos formales respecto a la contratación con terceros. Los servicios de terceros no son ni aprobados ni revisados por la gerencia. No hay actividades de medición y los terceros no reportan. A falta de una obligación contractual de reportar, la alta gerencia no está al tanto de la calidad del servicio prestado.	X		**GRADO DE MADUREZ.** El proceso de Administrar los servicios de terceros se encuentra en el nivel 3.
1 Inicial/Ad Hoc cuando La gerencia está conciente de la importancia de la necesidad de tener políticas y procedimientos documentados para la administración de los servicios de terceros, incluyendo la firma de contratos. No hay condiciones estandarizadas para los convenios con los prestadores de servicios. La medición de los servicios prestados es informal y reactiva. Las prácticas dependen de la experiencia de los individuos y del proveedor (por ejemplo, por demanda).	X		
2 Repetible pero intuitiva cuando El proceso de supervisión de los proveedores de servicios de terceros, de los riesgos asociados y de la prestación de servicios es informal. Se utiliza un contrato pro-forma con términos y condiciones estándares del proveedor (por ejemplo, la descripción de servicios que se prestarán). Los reportes sobre los servicios existen, pero no apoyan los objetivos del negocio.	X		
3 Proceso definido cuando Hay procedimientos bien documentados para controlar los servicios de terceros con procesos claros para tratar y negociar con los proveedores. Cuando se hace un acuerdo de prestación de servicios, la relación con el tercero es meramente contractual. La naturaleza de los servicios a prestar se detalla en el contrato e incluye requerimientos legales, operacionales y de control. Se asigna la responsabilidad de supervisar los servicios de terceros. Los términos contractuales se basan en formatos estandarizados. El riesgo del negocio asociado con los servicios del tercero esta valorado y reportado.		**X**	
4 Administrado y medible cuando Se establecen criterios formales y estandarizados para definir los términos de un acuerdo, incluyendo alcance del trabajo, servicios/entregables a suministrar, suposiciones, calendario, costos, acuerdos de facturación y responsabilidades. Se asignan las responsabilidades para la administración del contrato y del proveedor. Las aptitudes, capacidades y riesgos del proveedor son verificadas de forma continua. Los requerimientos del servicio están definidos y alineados con los objetivos del negocio. Existe un proceso para comparar el desempeño contra los términos contractuales, lo cual proporciona información para evaluar los servicios actuales y futuros del tercero. Se utilizan modelos de fijación de precios de transferencia en el proceso de adquisición. Todas las partes involucradas tienen conocimiento de las expectativas del servicio, de los costos y de las etapas. Se acordaron los KPIs y KGIs para la supervisión del servicio.			
5 Optimizado cuando Los contratos firmados con los terceros son revisados de forma periódica en intervalos predefinidos. La responsabilidad de administrar a los proveedores y la calidad de los servicios prestados está asignada. Se monitorea el cumplimiento de las condiciones operacionales, legales y de control y se implantan acciones correctivas. El tercero está sujeto a revisiones periódicas independientes y se le retroalimenta sobre su desempeño para mejorar la prestación del servicio. Las mediciones varían como respuesta a los cambios en las condiciones del negocio. Las mediciones ayudan a la detección temprana de problemas potenciales con los servicios de terceros. La notificación completa y bien definida del cumplimiento de los niveles de servicio, está asociada con la compensación del tercero. La gerencia ajusta el proceso de adquisición y monitoreo de servicios de terceros con base en los resultados de los KPIs y KGIs.			

Tabla 26: MODELOS DE MADUREZ DS2

Fuente: Realizado por los autores

DOMINIO: ENTREGAR Y DAR SOPORTE DS3: Administrar el desempeño y la capacidad			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando La gerencia no reconoce que los procesos clave del negocio pueden requerir altos niveles de desempeño de TI o que el total de los requerimientos de servicios de TI del negocio pueden exceder la capacidad. No se lleva cabo un proceso de planeación de la capacidad.	X		**GRADO DE MADUREZ.** El proceso de administrar el desempeño y la capacidad se encuentra en el nivel 2.
1 Inicial/Ad Hoc cuando Los usuarios, con frecuencia, tienen que llevar acabo soluciones alternas para resolver las limitaciones de desempeño y capacidad. Los responsables de los procesos del negocio valoran poco la necesidad de llevar a cabo una planeación de la capacidad y del desempeño. Las acciones para administrar el desempeño y la capacidad son típicamente reactivas. El proceso de planeación de la capacidad y el desempeño es informal. El entendimiento sobre la capacidad y el desempeño de TI, actual y futuro, es limitado.	X		
2 Repetible pero intuitiva cuando Los responsables del negocio y la gerencia de TI están concientes del impacto de no administrar el desempeño y la capacidad. Las necesidades de desempeño se logran por lo general con base en evaluaciones de sistemas individuales y el conocimiento y soporte de equipos de proyecto. Algunas herramientas individuales pueden utilizarse para diagnosticar problemas de desempeño y de capacidad, pero la consistencia de los resultados depende de la experiencia de individuos clave. No hay una evaluación general de la capacidad de desempeño de TI o consideración sobre situaciones de carga pico y peor-escenario. Los problemas de disponibilidad son susceptibles de ocurrir de manera inesperada y aleatoria y toma mucho tiempo diagnosticarlos y corregirlos. Cualquier medición de desempeño se basa primordialmente en las necesidades de TI y no en las necesidades del cliente.		**X**	
3 Proceso definido cuando Los requerimientos de desempeño y capacidad están definidos a lo largo del ciclo de vida del sistema. Hay métricas y requerimientos de niveles de servicio bien definidos, que pueden utilizarse para medir el desempeño operacional. Los pronósticos de la capacidad y el desempeño se modelan por medio de un proceso definido. Los reportes se generan con estadísticas de desempeño. Los problemas relacionados al desempeño y a la capacidad siguen siendo susceptibles a ocurrir y su resolución sigue consumiendo tiempo. A pesar de los niveles de servicio publicados, los usuarios y los clientes pueden sentirse escépticos acerca de la capacidad del servicio.			
4 Administrado y medible cuando Los requerimientos de desempeño y capacidad están definidos a lo largo del ciclo de vida del sistema. Hay métricas y requerimientos de niveles de servicio bien definidos, que pueden utilizarse para medir el desempeño operacional. Los pronósticos de la capacidad y el desempeño se modelan por medio de un proceso definido. Los reportes se generan con estadísticas de desempeño. Los problemas relacionados al desempeño y a la capacidad siguen siendo susceptibles a ocurrir y su resolución sigue consumiendo tiempo. A pesar de los niveles de servicio publicados, los usuarios y los clientes pueden sentirse escépticos acerca de la capacidad del servicio.			
5 Optimizado cuando Los planes de desempeño y capacidad están completamente sincronizados con las proyecciones de demanda del negocio. La infraestructura de TI y la demanda del negocio están sujetas a revisiones regulares para asegurar que se logre una capacidad óptima con el menor costo posible. Las herramientas para monitorear recursos críticos de TI han sido estandarizadas y usadas a través de diferentes plataformas y vinculadas a un sistema de administración de incidentes a lo largo de toda la organización. Las herramientas de monitoreo detectan y pueden corregir automáticamente problemas relacionados con la capacidad y el desempeño. Se llevan a cabo análisis de tendencias, los cuales muestran problemas de desempeño inminentes causados por incrementos en los volúmenes de negocio, lo que permite planear y evitar problemas inesperados. Las métricas para medir el desempeño y la capacidad de TI han sido bien afinadas dentro de los KGIs y KPIs para todos los procesos de negocio críticos y se miden de forma regular. La gerencia ajusta la planeación del desempeño y la capacidad siguiendo los análisis de los KGIs y KPIs.			

Tabla 27: MODELOS DE MADUREZ DS3

Fuente: Realizado por los autores

DOMINIO: ENTREGAR Y DAR SOPORTE DS4: Garantizar la continuidad del servicio			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando No hay entendimiento de los riesgos, vulnerabilidades y amenazas a las operaciones de TI o del impacto en el negocio por la pérdida de los servicios de TI. No se considera que la continuidad en los servicios deba tener atención de la gerencia.	X		**GRADO DE MADUREZ.** El proceso de garantizar la continuidad del servicio se encuentra en el nivel 2.
1 Inicial/Ad Hoc cuando Las responsabilidades sobre la continuidad de los servicios son informales y la autoridad para ejecutar responsabilidades es limitada. La gerencia comienza a darse cuenta de los riesgos relacionados y de la necesidad de mantener continuidad en los servicios. El enfoque de la gerencia sobre la continuidad del servicio radica en los recursos de infraestructura, en vez de radicar en los servicios de TI. Los usuarios utilizan soluciones alternas como respuesta a la interrupción de los servicios. La respuesta de TI a las interrupciones mayores es reactiva y sin preparación. Las pérdidas de energía planeadas están programadas para cumplir con las necesidades de TI pero no consideran los requerimientos del negocio.	X		
2 Repetible pero intuitiva cuando Se asigna la responsabilidad para mantener la continuidad del servicio. Los enfoques para asegurar la continuidad están fragmentados. Los reportes sobre la disponibilidad son esporádicos, pueden estar incompletos y no toman en cuenta el impacto en el negocio. No hay un plan de continuidad de TI documentado, aunque hay compromiso para mantener disponible la continuidad del servicio y sus principios más importantes se conocen. Existe un inventario de sistemas y componentes críticos, pero puede no ser confiable. Las prácticas de continuidad en los servicios emergen, pero el éxito depende de los individuos.		**X**	
3 Proceso definido cuando La responsabilidad sobre la administración de la continuidad del servicio es clara. Las responsabilidades de la planeación y de las pruebas de la continuidad de los servicios están claramente asignadas y definidas. El plan de continuidad de TI está documentado y basado en la criticidad de los sistemas y el impacto al negocio. Hay reportes periódicos de las pruebas de continuidad. Los individuos toman la iniciativa para seguir estándares y recibir capacitación para enfrentarse con incidentes mayores o desastres. La gerencia comunica de forma regular la necesidad de planear el aseguramiento de la continuidad del servicio. Se han aplicado componentes de alta disponibilidad y redundancia. Se mantiene un inventario de sistemas y componentes críticos.			
4 Administrado y medible cuando La responsabilidad sobre la administración de la continuidad del servicio es clara. Las responsabilidades de la planeación y de las pruebas de la continuidad de los servicios están claramente asignadas y definidas. El plan de continuidad de TI está documentado y basado en la criticidad de los sistemas y el impacto al negocio. Hay reportes periódicos de las pruebas de continuidad. Los individuos toman la iniciativa para seguir estándares y recibir capacitación para enfrentarse con incidentes mayores o desastres. La gerencia comunica de forma regular la necesidad de planear el aseguramiento de la continuidad del servicio. Se han aplicado componentes de alta disponibilidad y redundancia. Se mantiene un inventario de sistemas y componentes críticos.			
5 Optimizado cuando Se hacen cumplir las responsabilidades y los estándares para la continuidad de los servicios. Se asigna la responsabilidad de mantener un plan de continuidad de servicios. Las actividades de mantenimiento están basadas en los resultados de las pruebas de continuidad, en las buenas prácticas internas y en los cambios en el ambiente del negocio y de TI. Se recopila, analiza y reporta documentación estructurada sobre la continuidad en los servicios y se actúa en consecuencia. Se brinda capacitación formal y obligatoria sobre los procesos de continuidad. Se implementan regularmente buenas prácticas de disponibilidad de los sistemas. Las prácticas de disponibilidad y la planeación de la continuidad de los servicios tienen influencia una sobre la otra. Se clasifican los incidentes de discontinuidad y la ruta de escalamiento es bien conocida por todos los involucrados. Se han desarrollado y acordado KGIs y KPIs para la continuidad de los servicios, aunque pueden ser medidos de manera inconsistente.			

Tabla 28: MODELOS DE MADUREZ DS4

Fuente: Realizado por los autores

DOMINIO: ENTREGAR Y DAR SOPORTE DS5: Garantizar la seguridad de los sistemas			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando La organización no reconoce la necesidad de la seguridad para TI. Las responsabilidades y la rendición de cuentas no están asignadas para garantizar la seguridad. Las medidas para soportar la administrar la seguridad de TI no están implementadas. No hay reportes de seguridad de TI ni un proceso de respuesta para resolver brechas de seguridad de TI. Hay una total falta de procesos reconocibles de administración de seguridad de sistemas.	X		**GRADO DE MADUREZ.** El proceso de garantizar la seguridad de los sistemas se encuentra en el nivel 2.
1 Inicial/Ad Hoc cuando La organización reconoce la necesidad de seguridad para TI. La conciencia de la necesidad de seguridad depende principalmente del individuo. La seguridad de TI se lleva a cabo de forma reactiva. No se mide la seguridad de TI. Las brechas de seguridad de TI ocasionan respuestas con acusaciones personales, debido a que las responsabilidades no son claras. Las respuestas a las brechas de seguridad de TI son impredecibles.	X		
2 Repetible pero intuitiva cuando 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 las herramientas y las habilidades son inadecuadas. Los reportes de la seguridad de TI son incompletos, engañosos o no aplicables. La capacitación sobre seguridad está disponible pero depende principalmente de la iniciativa del individuo. La seguridad de TI es vista primordialmente como responsabilidad y disciplina de TI, y el negocio no ve la seguridad de TI como parte de su propia disciplina.		**X**	
3 Proceso definido cuando Existe conciencia sobre la seguridad y ésta es promovida por la gerencia. Los procedimientos de seguridad de TI están definidos y alineados con la política de seguridad de TI. Las responsabilidades de la seguridad de TI están asignadas y entendidas, pero no continuamente implementadas. Existe un plan de seguridad de TI y existen soluciones de seguridad motivadas por un análisis de riesgo. Los reportes no contienen un enfoque claro de negocio. Se realizan pruebas de seguridad adecuadas (por ejemplo, pruebas contra intrusos). Existe capacitación en seguridad para TI y para el negocio, pero se programa y se comunica de manera informal.			
4 Administrado y medible cuando Las responsabilidades sobre la seguridad de TI son asignadas, administradas e implementadas de forma clara. Regularmente se lleva a 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 está estandarizada. La certificación en seguridad es buscada por parte del personal que es responsable de la auditoria y la administración de la seguridad. Las pruebas de seguridad se hacen utilizando procesos estándares y formales que llevan a mejorar los niveles de seguridad. Los procesos de seguridad de TI están coordinados con la función de seguridad de toda la organización. Los reportes de seguridad están ligados con los objetivos del negocio. La capacitación sobre seguridad se imparte tanto para TI como para el negocio. La capacitación sobre seguridad de TI se planea y se administra de manera que responda a las necesidades del negocio y a los perfiles de riesgo de seguridad. Los KGIs y KPIs ya están definidos pero no se miden aún.			
5 Optimizado cuando Las responsabilidades sobre la seguridad de TI son asignadas, administradas e implementadas de forma clara. Regularmente se lleva a 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 está estandarizada. La certificación en seguridad es buscada por parte del personal que es responsable de la auditoria y la administración de la seguridad. Las pruebas de seguridad se hacen utilizando procesos estándares y formales que llevan a mejorar los niveles de seguridad. Los procesos de seguridad de TI están coordinados con la función de seguridad de toda la organización. Los reportes de seguridad están ligados con los objetivos del negocio. La capacitación sobre seguridad se imparte tanto para TI como para el negocio. La capacitación sobre seguridad de TI se planea y se administra de manera que responda a las necesidades del negocio y a los perfiles de riesgo de seguridad. Los KGIs y KPIs ya están definidos pero no se miden aún.			

Tabla 29: MODELOS DE MADUREZ DS5

Fuente: Realizado por los autores

DOMINIO: ENTREGAR Y DAR SOPORTE DS7: Educar y entrenar a los usuarios			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando Hay una total falta de programas de entrenamiento y educación. La organización no reconoce que hay un problema a ser atendido respecto al entrenamiento y no hay comunicación sobre el problema.	X		**GRADO DE MADUREZ.** El proceso de educar y entrenar a los usuarios se encuentra en el nivel 2.
1 Inicial/Ad Hoc cuando 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 de entrenamiento por su cuenta. Algunos de estos cursos de entrenamiento abordan los temas de conducta ética, conciencia sobre la seguridad en los sistemas y prácticas de seguridad. El enfoque global de la gerencia carece de cohesión y sólo hay comunicación esporádica e inconsistente respecto a los problemas y enfoques para hacerse cargo del entrenamiento y la educación.	X		
2 Repetible pero intuitiva cuando 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 temas de materias con diferentes puntos de vista. Algunas de las clases abordan los temas de conducta ética y de 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.		**X**	
3 Proceso definido cuando 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 el programa de entrenamiento y educación, se establecen presupuestos, recursos, instructores e instalaciones. Se imparten clases formales sobre conducta ética y sobre conciencia y prácticas de seguridad en los sistemas. La mayoría de los procesos de entrenamiento 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.			
4 Administrado y medible cuando 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 el programa de entrenamiento y educación, se establecen presupuestos, recursos, instructores e instalaciones. Se imparten clases formales sobre conducta ética y sobre conciencia y prácticas de seguridad en los sistemas. La mayoría de los procesos de entrenamiento 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.			
5 Optimizado cuando Hay un programa completo de entrenamiento y educación que produce resultados medibles. Las responsabilidades son claras y se establece la propiedad sobre los procesos. El entrenamiento y la educación son componentes de los planes de carrera de los empleados. La gerencia apoya y asiste a sesiones de entrenamiento y de educación. Todos los empleados reciben entrenamiento sobre conducta ética y sobre conciencia y prácticas de seguridad en los sistemas. Todos los empleados reciben el nivel apropiado de entrenamiento 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 y actualización del programa y de los procesos de entrenamiento. Los procesos están en vía de mejora y fomentan las mejores prácticas internas.			

Tabla 30: MODELOS DE MADUREZ DS7

Fuente: Realizado por los autores

DOMINIO: ENTREGAR Y DAR SOPORTE DS8: Administrar la mesa de servicio y los incidentes			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando No hay soporte para resolver problemas y preguntas de los usuarios. Hay una completa falta de procesos para la administración de incidentes. La organización no reconoce que hay un problema que atender.	X		**GRADO DE MADUREZ.** El proceso de administrar la mesa de servicio y los incidentes se encuentra en el nivel 2.
1 Inicial/Ad Hoc cuando La gerencia reconoce que requiere un proceso soportado por herramientas y personal para responder a las consultas de los usuarios y administrar la resolución de incidentes. Sin embargo, se trata de un proceso no estandarizado y sólo se brinda soporte reactivo. La gerencia no monitorea las consultas de los usuarios, los incidentes o las tendencias. No existe un proceso de escalamiento para garantizar que los problemas se resuelvan.	X		
2 Repetible pero intuitiva cuando Hay conciencia organizacional de la necesidad de una función de mesa de servicio y de un proceso de administración de incidentes. Existe ayuda disponible de manera informal a través de una red de individuos expertos. Estos individuos tienen a su disposición algunas herramientas comunes para ayudar en la resolución de incidentes. No hay entrenamiento formal y la comunicación obre procedimientos estándar y la responsabilidad es delegada al individuo.		**X**	
3 Proceso definido cuando Hay conciencia organizacional de la necesidad de una función de mesa de servicio y de un proceso de administración de incidentes. Existe ayuda disponible de manera informal a través de una red de individuos expertos. Estos individuos tienen a su disposición algunas herramientas comunes para ayudar en la resolución de incidentes. No hay entrenamiento formal y la comunicación obre procedimientos estándar y la responsabilidad es delegada al individuo.			
4 Administrado y medible cuando En todos los niveles de la organización hay un total entendimiento de los beneficios de un proceso de administración de incidentes y la función de mesa de servicio se ha establecido en las unidades organizacionales apropiadas. Las herramientas y técnicas están automatizadas con una base de conocimientos centralizada. El personal de la mesa de servicio interactúa muy de cerca con el personal de administración de problemas. Las responsabilidades son claras y se monitorea su efectividad. Los procedimientos para comunicar, escalar y resolver incidentes han sido establecidos y comunicados. El personal de la mesa de servicio está capacitado y los procesos se mejoran a través del uso de software para tareas específicas. La gerencia ha desarrollado los KPIs y KGIs para el desempeño de la mesa de servicio.			
5 Optimizado cuando En todos los niveles de la organización hay un total entendimiento de los beneficios de un proceso de administración de incidentes y la función de mesa de servicio se ha establecido en las unidades organizacionales apropiadas. Las herramientas y técnicas están automatizadas con una base de conocimientos centralizada. El personal de la mesa de servicio interactúa muy de cerca con el personal de administración de problemas. Las responsabilidades son claras y se monitorea su efectividad. Los procedimientos para comunicar, escalar y resolver incidentes han sido establecidos y comunicados. El personal de la mesa de servicio está capacitado y los procesos se mejoran a través del uso de software para tareas específicas. La gerencia ha desarrollado los KPIs y KGIs para el desempeño de la mesa de servicio.			

Tabla 31: MODELOS DE MADUREZ DS8

Fuente: Realizado por los autores

DOMINIO: ENTREGAR Y DAR SOPORTE DS9: Administrar la configuración			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando La gerencia no valora los beneficios de tener un proceso implementado que sea capaz de reportar y administrar las configuraciones de la infraestructura de TI, tanto para configuraciones de hardware como de software.	X		**GRADO DE MADUREZ.** El proceso de administrar la configuración se encuentra en el nivel 2.
1 Inicial/Ad Hoc cuando Se reconoce la necesidad de contar con una administración de configuración. Se llevan a cabo tareas básicas de administración de configuraciones, tales como mantener inventarios de hardware y software pero de manera individual. No están definidas prácticas estandarizadas.	X		
2 Repetible pero intuitiva cuando La gerencia esta conciente de la necesidad de controlar la configuración de TI y entiende los beneficios de mantener información completa y precisa sobre las configuraciones, pero hay una dependencia implícita del conocimiento y experiencia del personal técnico. Las herramientas para la administración de configuraciones se utilizan hasta cierto grado, pero difieren entre plataformas. Además no se han definido prácticas estandarizadas de trabajo. El contenido de la información de la configuración es limitado y no lo utilizan los procesos interrelacionados, tales como administración de cambios y administración de problemas.		**X**	
3 Proceso definido cuando Los procedimientos y las prácticas de trabajo se han documentado, estandarizado y comunicado, pero la capacitación y la aplicación de estándares dependen del individuo. Además se han implementado herramientas similares de administración de configuración entre plataformas. Es poco probable detectar las desviaciones de los procedimientos y las verificaciones físicas se realizan de manera inconsistente. Se lleva a cabo algún tipo de automatización para ayudar a rastrear cambios en el software o en el hardware. La información de la configuración es utilizada por los procesos interrelacionados.			
4 Administrado y medible cuando En todos los niveles de la organización se reconoce la necesidad de administrar la configuración y las buenas prácticas siguen evolucionando. Los procedimientos y los estándares se comunican e incorporan a la capacitación y las desviaciones son monitoreadas, rastreadas y reportadas. Se utilizan herramientas automatizadas para fomentar el uso de estándares y mejorar la estabilidad. Los sistemas de administración de configuraciones cubren la mayoría de los activos de TI y permiten una adecuada administración de liberaciones y control de distribución. Los análisis de excepciones, así como las verificaciones físicas, se aplican de manera consistente y se investigan las causas desde su raíz.			
5 Optimizado cuando Todos los activos de TI se administran en un sistema central de configuraciones que contiene toda la información necesaria acerca de los componentes, sus interrelaciones y eventos. La información de las configuraciones está alineada con los catálogos de los proveedores. Hay una completa integración de los procesos interrelacionados, y estos utilizan y actualizan la información de la configuración de manera automática. Los reportes de auditoria de los puntos de referencia, brindan información esencial sobre el software y hardware con respecto a reparaciones, servicios, garantías, actualizaciones y evaluaciones técnicas de cada unidad individual. Se fomentan las reglas para limitar la instalación de software no autorizado. La gerencia proyecta las reparaciones y las actualizaciones utilizando reportes de análisis que proporcionan funciones de programación de actualizaciones y de renovación de tecnología. El rastreo de activos y el monitoreo de activos individuales de TI los protege y previene de robo, de mal uso y de abusos.			

Tabla 32: MODELOS DE MADUREZ DS9

Fuente: Realizado por los autores

DOMINIO: ENTREGAR Y DAR SOPORTE DS10: Administración de problemas			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando No hay conciencia sobre la necesidad de administrar problemas, y no hay diferencia entre problemas e incidentes. Por lo tanto, no se han hecho intentos por identificar la causa raíz de los incidentes.	X		**GRADO DE MADUREZ.** El proceso de administración de problemas se encuentra en el nivel 3.
1 Inicial/Ad Hoc cuando 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		
2 Repetible pero intuitiva cuando 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 unos cuantos individuos clave son responsables de identificar y resolver los problemas. La información se comparte entre el personal de manera informal y reactiva. El nivel de servicio hacia la comunidad usuaria varía y es obstaculizado por la falta de conocimiento estructurado a disposición del administrador de problemas.	X		
3 Proceso definido cuando 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 capacitación. 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. La información se comparte entre el personal de manera formal y proactiva. La revisión de incidentes y los análisis de identificación y resolución de problemas son limitados e informales.		**X**	
4 Administrado y medible cuando 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 capacitación. 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. La información se comparte entre el personal de manera formal y proactiva. La revisión de incidentes y los análisis de identificación y resolución de problemas son limitados e informales.			
5 Optimizado cuando 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 de problemas 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 de manera continua. El proceso de administración de problemas se analiza para buscar la mejora continua con base en los KPIs y KGIs y se reporta a los interesados.			

Tabla 33: MODELOS DE MADUREZ DS10

Fuente: Realizado por los autores

DOMINIO: ENTREGAR Y DAR SOPORTE DS11: Administración de datos			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando Los datos no son reconocidos como parte de los recursos y los activos de la empresa. No está asignada la propiedad sobre los datos o sobre la rendición de cuentas individual sobre la administración de los datos. La calidad y la seguridad de los datos son deficientes o inexistentes.	X		**GRADO DE MADUREZ.** El proceso de administración de datos se encuentra en el nivel 2.
1 Inicial/Ad Hoc cuando La organización reconoce la necesidad de una correcta administración de los datos. Hay un método adecuado para especificar requerimientos de seguridad en la administración de datos, pero no hay procedimientos implementados de comunicación formal. No se lleva a cabo capacitación específica sobre administración de los datos. La responsabilidad sobre la administración de los datos no es clara. Los procedimientos de respaldo y recuperación y los acuerdos sobre desechos están en orden.	X		
2 Repetible pero intuitiva cuando A lo largo de toda la organización existe conciencia sobre la necesidad de una adecuada administración de los datos. A un alto nivel empieza a observarse la propiedad o responsabilidad sobre los datos. Los requerimientos de seguridad para la administración de datos son documentados por individuos clave. Se lleva a cabo algún tipo de monitoreo dentro de TI sobre algunas actividades clave de la administración de datos (respaldos, recuperación y desecho). Las responsabilidades para la administración de datos son asignadas de manera informal a personal clave de TI.		**X**	
3 Proceso definido cuando Se entiende y acepta la necesidad de la administración de datos, tanto dentro de TI como a lo largo de toda la organización. Se establece la responsabilidad sobre la administración de los datos. Se asigna la propiedad sobre los datos a la parte responsable que controla la integridad y la seguridad. Los procedimientos de administración de datos se formalizan dentro de TI y se utilizan algunas herramientas para respaldos / recuperación y desecho de equipo. Se lleva a cabo algún tipo de monitoreo sobre la administración de datos. Se definen métricas básicas de desempeño. Comienza a aparecer el entrenamiento sobre administración de información.			
4 Administrado y medible cuando Se entiende la necesidad de la administración de los datos y las acciones requeridas son aceptadas a lo largo de toda la organización. La responsabilidad de la propiedad y la administración de los datos están definidas, asignada y comunicada de forma clara en la organización. Los procedimientos se formalizan y son ampliamente conocidos, el conocimiento se comparte. Comienza a aparecer el uso de herramientas. Se acuerdan con los clientes los indicadores de desempeño y meta y se monitorean por medio de un proceso bien definido. Se lleva a cabo entrenamiento formal para el personal de administración de los datos.			
5 Optimizado cuando Se entiende y acepta dentro de la organización la necesidad de realizar todas las actividades requeridas para la administración de datos. Las necesidades y los requerimientos futuros son explorados de manera proactiva. Las responsabilidades sobre la propiedad de los datos y la administración de los mismos están establecidas de forma clara, se conocen ampliamente a lo largo de la organización y se actualizan periódicamente. Los procedimientos se formalizan y se conocen ampliamente, la compartición del conocimiento es una práctica estándar. Se utilizan herramientas sofisticadas con un máximo de automatización de la administración de los datos. Se acuerdan con los clientes los indicadores de desempeño y meta, se ligan con los objetivos del negocio y se monitorean de manera regular utilizando un proceso bien definido. Se exploran constantemente oportunidades de mejora. El entrenamiento para el personal de administración de datos se institucionaliza.			

Tabla 34: MODELOS DE MADUREZ DS11

Fuente: Realizado por los autores

DOMINIO: ENTREGAR Y DAR SOPORTE DS12: Administración del ambiente físico			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando No hay conciencia sobre la necesidad de proteger las instalaciones o la inversión en recursos de cómputo. Los factores ambientales tales como protección contra fuego, polvo, tierra y exceso de calor y humedad no se controlan ni se monitorean.	X		**GRADO DE MADUREZ.** El proceso de administración del ambiente físico se encuentra en el nivel 3.
1 Inicial/Ad Hoc cuando La organización reconoce la necesidad de contar con un ambiente físico que proteja los recursos y el personal contra peligros naturales y causados por el hombre. La administración de instalaciones y de equipo depende de las habilidades de individuos clave. El personal se puede mover dentro de las instalaciones sin restricción. La gerencia no monitorea los controles ambientales de las instalaciones o el movimiento del personal.	X		
2 Repetible pero intuitiva cuando Los controles ambientales se implementan y monitorean por parte del personal de operaciones. La seguridad física es un proceso informal, realizado por un pequeño grupo de empleados con alto nivel de preocupación por asegurar las instalaciones físicas. Los procedimientos de mantenimiento de instalaciones no están bien documentados y dependen de las buenas prácticas de unos cuantos individuos. Las metas de seguridad física no se basan en estándares formales y la gerencia no se asegura de que se cumplan los objetivos de seguridad.	X		
3 Proceso definido cuando Se entiende y acepta a lo largo de toda la organización la necesidad de mantener un ambiente de cómputo controlado. Los controles ambientales, el mantenimiento preventivo y la seguridad física cuentan con presupuesto autorizado y rastreado por la gerencia. Se aplican restricciones de acceso, permitiendo el ingreso a las instalaciones de cómputo sólo al personal aprobado. Los visitantes se registran y acompañan dependiendo del individuo. Las instalaciones físicas mantienen un perfil bajo y no son reconocibles de manera fácil. Las autoridades civiles monitorean al cumplimiento con los reglamentos de salud y seguridad. Los riesgos se aseguran con el mínimo esfuerzo para optimizar los costos del seguro.		**X**	
4 Administrado y medible cuando Se entiende y acepta a lo largo de toda la organización la necesidad de mantener un ambiente de cómputo controlado. Los controles ambientales, el mantenimiento preventivo y la seguridad física cuentan con presupuesto autorizado y rastreado por la gerencia. Se aplican restricciones de acceso, permitiendo el ingreso a las instalaciones de cómputo sólo al personal aprobado. Los visitantes se registran y acompañan dependiendo del individuo. Las instalaciones físicas mantienen un perfil bajo y no son reconocibles de manera fácil. Las autoridades civiles monitorean al cumplimiento con los reglamentos de salud y seguridad. Los riesgos se aseguran con el mínimo esfuerzo para optimizar los costos del seguro.			
5 Optimizado cuando Se entiende por completo la necesidad de mantener un ambiente de cómputo controlado y se evidencia en la estructura organizacional y en la distribución del presupuesto. Los requerimientos de seguridad físicos y ambientales están documentados y el acceso se monitorea y controla estrictamente. Se establecen y comunican las responsabilidades. El personal de las instalaciones ha sido entrenado por completo respecto a situaciones de emergencia, así como en prácticas de salud y seguridad. Están implementados mecanismos de control estandarizados para la restricción de accesos a instalaciones y para contrarrestar los factores ambientales y de seguridad. La gerencia monitorea la efectividad de los controles y el cumplimiento de los estándares establecidos. La gerencia ha establecido KPIs y KGIs para medir la administración del ambiente de cómputo. La capacidad de recuperación de los recursos de cómputo se incorpora en un proceso organizacional de administración de riesgos. La información integrada se usa para optimizar la cobertura de los seguros y de los costos asociados.			

Tabla 35: MODELOS DE MADUREZ DS12

Fuente: Realizado por los autores

DOMINIO: ENTREGAR Y DAR SOPORTE DS13: Administración de operaciones			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando La organización no dedica tiempo y recursos al establecimiento de soporte básico de TI y a actividades operativas.	**X**		**GRADO DE MADUREZ.** El proceso de administración de operaciones se encuentra en el nivel 2.
1 Inicial/Ad Hoc cuando 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 manera informal y el procesamiento de peticiones se acepta sin validación previa. Las computadoras, sistemas y aplicaciones que soportan los procesos del negocio con frecuencia no están disponibles, se interrumpen o retrasan. Se pierde tiempo mientras los empleados esperan recursos. Los medios de salida aparecen ocasionalmente en lugares inesperados o no aparecen.	**X**		
2 Repetible pero intuitiva cuando La organización esta conciente del rol clave que las actividades de operaciones de TI juegan en brindar funciones de soporte de TI. Se asignan 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. Las instrucciones de qué hacer, cuándo y en qué orden no están documentadas. Existe algo de capacitación para el operador y hay algunos estándares de operación formales.		X	
3 Proceso definido cuando Se entiende y acepta dentro de la organización la necesidad de administrar las operaciones de cómputo. Se han asignado recursos y se lleva a cabo alguna capacitación durante el trabajo. Las funciones repetitivas están definidas, estandarizadas, documentadas y comunicadas 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 intervención del operador. Se introducen controles para colocar nuevos trabajos en operación. Se desarrolla una política formal para reducir el número de eventos no programados. Los acuerdos de servicio y mantenimiento con proveedores siguen siendo de naturaleza informal.			
4 Administrado y medible cuando Se entiende y acepta dentro de la organización la necesidad de administrar las operaciones de cómputo. Se han asignado recursos y se lleva a cabo alguna capacitación durante el trabajo. Las funciones repetitivas están definidas, estandarizadas, documentadas y comunicadas 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 intervención del operador. Se introducen controles para colocar nuevos trabajos en operación. Se desarrolla una política formal para reducir el número de eventos no programados. Los acuerdos de servicio y mantenimiento con proveedores siguen siendo de naturaleza informal.			
5 Optimizado cuando Las operaciones de soporte de TI son efectivas, eficientes y suficientemente flexibles para cumplir con las necesidades de niveles de servicio 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 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.			

Tabla 36: MODELOS DE MADUREZ DS13

Fuente: Realizado por los autores

DOMINIO: MONITOREAR Y EVALUAR ME1: Monitorear y evaluar el desempeño de TI			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando La organización no cuenta con un proceso implantado de monitoreo. TI no lleva a cabo monitoreo de proyectos o procesos de forma independiente. No se cuenta con reportes útiles, oportunos y precisos. La necesidad de entender de forma clara los objetivos de los procesos no se reconoce.	X		**GRADO DE MADUREZ.** El proceso de Monitorear y evaluar el desempeño de TI se encuentra en el nivel 3.
1 Inicial/Ad Hoc cuando La gerencia reconoce una necesidad de recolectar y evaluar información sobre los procesos de monitoreo. No se han identificado procesos estándar de recolección y evaluación. El monitoreo se implanta y las métricas se seleccionan de acuerdo a cada caso, de acuerdo a las necesidades de proyectos y procesos de TI específicos. El monitoreo por lo general se implanta de forma reactiva a algún incidente que ha ocasionado alguna perdida o vergüenza a la organización. La función de contabilidad monitorea mediciones financieras básicas para TI.	X		
2 Repetible pero intuitiva cuando 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 la experiencia de individuos clave. Herramientas limitadas son seleccionadas y se implantan para recolectar información, pero esta recolección no se basa en un enfoque planeado.	X		
3 Proceso definido cuando La gerencia ha comunicado e institucionalizado un procesos estándar de monitoreo. Se han implantado programas educacionales y de entrenamiento para el monitoreo. Se ha desarrollado una base de conocimiento formalizada del desempeño histórico. Las evaluaciones todavía se realizan al nivel de procesos y proyectos individuales de TI y no están integradas a través de todos los procesos. Se han definido herramientas para monitorear los procesos y los niveles de servicio de TI. Las mediciones de la contribución 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, las estratégicas, las de satisfacción del cliente y los niveles de servicio están definidas. Se ha definido un marco de trabajo para medir el desempeño.		**X**	
4 Administrado y medible cuando La gerencia ha definido las tolerancias bajo las cuales los procesos deben operar. Los reportes de los resultados del monitoreo están en proceso de estandarizarse y normalizarse. Hay una integración de métricas a lo largo de todos los proyectos y procesos de TI. Los sistemas de reporte de la administración de TI están formalizados. Las herramientas automatizadas están integradas y se aprovechan en toda la organización para recolectar y monitorear la información operativa de las aplicaciones, sistemas y procesos. La gerencia puede evaluar el desempeño con base en criterios acordados y aprobados por las terceras partes interesadas. Las mediciones de la función de TI están alienadas con las metas de toda la organización.			
5 Optimizado cuando Un proceso de mejora continua de la calidad se ha desarrollado para actualizar los estándares y las políticas de monitoreo a nivel organizacional incorporando mejores prácticas de la industria. Todos los procesos de monitoreo están optimizados y dan soporte a los objetivos de toda la organización. Las métricas impulsadas por el negocio se usan de forma rutinaria para medir el desempeño, y están integradas en los marcos de trabajo estratégicos, tales como el Balanced Scorecard. El monitoreo de los procesos y el rediseño continuo 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.			

Tabla 37: MODELOS DE MADUREZ ME1

Fuente: Realizado por los autores

DOMINIO: MONITOREAR Y EVALUAR ME2: Monitorear y evaluar el control interno			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando La organización carece de procedimientos para monitorear la efectividad de los controles internos. Los métodos de reporte de control interno gerenciales no existen. Existe una falta generalizada de conciencia sobre la seguridad operativa y el aseguramiento del control interno de TI. La gerencia y los empleados no tienen conciencia general sobre el control interno.	X		**GRADO DE MADUREZ.** El proceso de monitorear y evaluar el control interno se encuentra en el nivel 2.
1 Inicial/Ad Hoc cuando La gerencia reconoce la necesidad de administrar y asegurar el control de TI de forma regular. La experiencia individual para evaluar la suficiencia del control interno se aplica de forma ad hoc. La gerencia de TI no ha asignado de manera formal las responsabilidades para monitorear la efectividad de los controles internos. Las evaluaciones de control interno de TI se realizan como parte de las auditorias financieras tradicionales, con metodologías y habilidades que no reflejan las necesidades de la función de los servicios de información.	X		
2 Repetible pero intuitiva cuando La organización utiliza reportes de control informales para comenzar iniciativas de acción correctiva. La evaluación del control interno depende de las habilidades de individuos clave. La organización tiene una mayor conciencia sobre el monitoreo de los controles internos. La gerencia de servicios de información realiza monitoreo periódico sobre la efectividad de lo que considera controles internos críticos. Se están empezando a usar metodologías y herramientas para monitorear los controles internos, aunque no se basan en un plan. Los factores de riesgo específicos del ambiente de TI se identifican con base en las habilidades de individuos.		**X**	
3 Proceso definido cuando La gerencia apoya y ha institucionalizado el monitoreo del control interno. Se han desarrollado políticas y procedimientos para evaluar y reportar las actividades de monitoreo del control interno. Se ha definido un programa de educación y entrenamiento para el monitoreo del control interno. Se ha definido también un proceso para auto-evaluaciones y revisiones de aseguramiento del control interno, con roles definidos para los responsables de la administración del negocio y de TI. Se usan herramientas, aunque no necesariamente están integradas en todos los procesos. Las políticas de evaluación de riesgos de los procesos de TI se utilizan dentro de los marcos de trabajo desarrollados de manera específica para la función de TI. Se han definido políticas para el manejo y mitigación de riesgos específicos de procesos.			
4 Administrado y medible cuando La gerencia tiene implantado un marco de trabajo para el monitoreo del control interno de TI. La organización ha establecido niveles de tolerancia para el proceso de monitoreo del control interno. Se han implantado herramientas para estandarizar evaluaciones y para detectar de forma automática las excepciones de control. Se ha establecido una función formal para el control interno de TI, con profesionales especializados y certificados que utilizan un marco de trabajo de control formal avalado por la alta dirección. Un equipo calificado de TI participa de forma rutinaria en las evaluaciones de control interno. Se ha establecido una base de datos de métricas para información histórica sobre el monitoreo del control interno. Se realizan revisiones entre pares para verificar el monitoreo del control interno.			
5 Optimizado cuando La gerencia ha implantado un programa de mejora continua en toda la organización que toma en cuenta las lecciones aprendidas y las mejores prácticas de la industria para monitorear el control interno. La organización utiliza herramientas integradas y actualizadas, donde es apropiado, que permiten una evaluación efectiva de los controles críticos de TI y una detección rápida de incidentes de control de TI. La compartición del conocimiento, específico de la función de servicios de información, se encuentra implantada de manera formal. El benchmarking con los estándares de la industria y las mejores prácticas está formalizado.			

Tabla 38: MODELOS DE MADUREZ ME2

Fuente: Realizado por los autores

DOMINIO: MONITOREAR Y EVALUAR ME3: Garantizar el cumplimiento regulatorio			
NIVELES DE LOS MODELOS DE MADUREZ	**CUMPLE**		**OBSERVACIONES**
	SI	**NO**	
0 No existente cuando Existe poca conciencia respecto a los requerimientos externos que afectan a TI, sin procesos referentes al cumplimiento de requisitos regulatorios, legales y contractuales.	X		**GRADO DE MADUREZ.** El proceso de garantizar el cumplimiento regulatorio se encuentra en el nivel 3.
1 Inicial/Ad Hoc cuando Existe conciencia de los requisitos de cumplimiento regulatorio, contractual y legal que tienen impacto en la organización. Se siguen procesos informales para mantener el cumplimiento, pero solo si la necesidad surge en nuevos proyectos o como respuesta a auditorias o revisiones.	X		
2 Repetible pero intuitiva cuando Existe el entendimiento de la necesidad de cumplir con los requerimientos externos y la necesidad se comunica. En los casos en que el cumplimiento se ha convertido en un requerimiento recurrente., como en los reglamentos regulatorios o en la legislación de privacidad, se han desarrollado procedimientos individuales de cumplimiento y se siguen año con año. No existe, sin embargo, un enfoque estándar. Hay mucha confianza en el conocimiento y responsabilidad de los individuos, y los errores son posibles. Se brinda entrenamiento informal respecto a los requerimientos externos y a los temas de cumplimiento.	X		
3 Proceso definido cuando Se han desarrollado, documentado y comunicado políticas, procedimientos y procesos, .para garantizar el cumplimiento de los reglamentos y de las obligaciones contractuales y legales, pero algunas quizá no se sigan y algunas quizá estén desactualizadas o sean poco prácticas de implantar. Se realiza poco monitoreo y existen requisitos de cumplimiento que no han sido resueltos. Se brinda entrenamiento sobre requisitos legales y regulatorios externos que afectan a la organización y se instruye respecto a los procesos de cumplimiento definidos. Existen contratos pro forma y procesos legales estándar para minimizar los riesgos asociados con las obligaciones contractuales		**X**	
4 Administrado y medible cuando Existe un entendimiento completo de los eventos y de la exposición a requerimientos externos, y la necesidad de asegurar el cumplimiento a todos los niveles. Existe un esquema formal de entrenamiento que asegura que todo el equipo esté consciente de sus obligaciones de cumplimiento. Las responsabilidades son claras y el empoderamiento de los procesos es entendido. El proceso incluye una revisión del entorno para identificar requerimientos externos y cambios recurrentes. Existe un mecanismo implantado para monitorear el no cumplimiento de los requisitos externos, reforzar las prácticas internas e implantar acciones correctivas. Los eventos de no cumplimiento se analizan de forma estándar en busca de las causas raíz, con el objetivo de identificar soluciones sostenibles. Buenas prácticas internas estandarizadas se usan para necesidades específicas tales como reglamentos vigentes y contratos recurrentes de servicio.			
5 Optimizado cuando Existe un proceso bien organizado, eficiente e implantado para cumplir con los requerimientos externos, basado en una sola función central que brinda orientación y coordinación a toda la organización. Hay un amplio conocimiento de los requerimientos externos aplicables, incluyendo sus tendencias futuras y cambios anticipados, así como la necesidad de nuevas soluciones. La organización participa en discusiones externas con grupos regulatorios y de la industria para entender e influenciar los requerimientos externos que la puedan afectar. Se han desarrollado mejores prácticas que aseguran el cumplimiento de los requisitos externos, y esto ocasiona que haya muy pocos casos de excepciones de cumplimiento. Existe un sistema central de rastreo para toda la organización, que permite a la gerencia documentar el flujo de trabajo, medir y mejorar la calidad y efectividad del proceso de monitoreo del cumplimiento. Un proceso externo de auto-evaluación de requerimientos existe y se ha refinado hasta alcanzar el nivel de buena práctica. El estilo y la cultura administrativa de la organización referente al cumplimiento es suficientemente fuerte, y se elaboran los procesos suficientemente bien para que el entrenamiento se limite al nuevo personal y siempre que ocurra un cambio significativo.			

Tabla 39: MODELOS DE MADUREZ ME3

Fuente: Realizado por los autores

REPORTE GENERAL DE MODELOS DE MADUREZ

La siguiente tabla (Tabla 40) se muestra el reporte del grado de madurez de cada proceso evaluado, se puede observar que hay procesos con grado de madurez 1 o inicial que deben ser motivo de especial atención por parte del Departamento de Sistemas de Teleamazonas, como plan a corto plazo.

DOMINIO	PROCESO		GRADO DE MADUREZ
Planear y Organizar	PO1	Definir un plan estratégico de TI	3
	PO2	Definir la Arquitectura de la Información	2
	PO3	Definir la dirección tecnológica	3
	PO4	Definir los Procesos, Organización y Relaciones de TI	3
	PO5	Administrar la Inversión en TI	1
	PO6	Comunicar las metas y la dirección de la gerencia	3
	PO7	Administrar los Recursos Humanos de TI	3
	PO9	Evaluar y Administrar los Riesgos de TI	2
	PO10	Administrar los proyectos	2
Adquirir e Implantar	AI1	Identificar las Soluciones Automatizadas	3
	AI2	Adquirir y Mantener Software Aplicativo	3
	AI3	Adquirir y Mantener la Infraestructura Tecnológica	3
	AI4	Facilitar la operación y el uso	3
	AI5	Procurar Recursos de TI	1
	AI6	Administrar los Cambios	1
	AI7	Instalar y Acreditar soluciones y cambios	3
Entregar y Dar Soporte	DS2	Administrar los Servicios de Terceros	3
	DS3	Administrar el Desempeño y la Capacidad	2
	DS4	Asegurar el Servicio Continuo	2
	DS5	Garantizar la Seguridad de los Sistemas	2
	DS7	Educar y Entrenar a los Usuarios	2
	DS8	Administrar la mesa de Servicio y los Incidentes	2
	DS9	Administrar la Configuración	2
	DS10	Administrar los Problemas	3
	DS11	Administrar los Datos	2
	DS12	Administrar el Ambiente Físico	3
	DS13	Administrar las Operaciones	2
Monitorear y Evaluar	ME1	Monitorear y evaluar el desempeño de TI	3
	ME2	Monitorear y evaluar el Control Interno	2
	ME3	Garantizar el cumplimiento Regulatorio	3

Tabla 40: Reporte general de modelos de madurez

Fuente: Creación de Autores

RESULTADOS FINALES DEL IMPACTO SOBRE LOS CRITERIOS DE INFORMACIÓN

Los resultados presentados en la siguiente tabla (Tabla 41) resultan de la multiplicación entre el valor propuesto por COSO (Tabla 9) para cada criterio y el valor obtenido del grado de madurez (Tabla 40) en que se encuentra cada proceso relacionado con la situación actual del Departamento de Sistemas de Teleamazonas. Se obtiene el total real haciendo una sumatoria por cada columna de criterios; el cual se lo compara con el total ideal que resulta de la suma por columna si se considera que el grado de madurez de cada criterio es óptimo (5).Posteriormente se realiza el cálculo del porcentaje dividiendo el total real para el total ideal y multiplicando por 100. Finalmente se obtiene el promedio de los porcentajes de los criterios de información.

DOMINIO	PROCESO		EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO	CONFIABILIDAD
Planear y Organizar	PO1	Definir un plan estratégico de TI	2.58	1.89	0.00	0.00	0.00	0.00	0.00
	PO2	Definir la Arquitectura de la Información	1.89	1.72	0.40	0.74	0.00	0.00	0.00
	PO3	Definir la dirección tecnológica	2.58	2.58	0.00	0.00	0.00	0.00	0.00
	PO4	Definir los Procesos, Organización y Relaciones de TI	2.58	2.58	0.00	0.00	0.00	0.00	0.00
	PO5	Administrar la Inversión en TI	2.58	0.86	0.00	0.00	0.00	0.00	0.00
	PO6	Comunicar las metas y la dirección de la gerencia	2.58	0.00	0.00	0.00	0.00	0.00	0.00
	PO7	Administrar los Recursos Humanos de TI	2.58	2.58	0.00	0.00	0.00	0.00	0.00
	PO9	Evaluar y Administrar los Riesgos de TI	1.89	1.26	0.54	0.54	0.74	0.54	0.54

	PO10	Administrar los proyectos	2.58	1.72	0.00	0.00	0.00	0.00	0.00
Adquirir e Implantar	AI1	Identificar las Soluciones Automatizadas	2.58	1.89	0.00	0.00	0.00	0.00	0.00
	AI2	Adquirir y Mantener Software Aplicativo	2.58	2.58	0.00	0.54	0.00	0.00	0.00
	AI3	Adquirir y Mantener la Infraestructura Tecnológica	1.89	2.58	0.00	0.54	0.00	0.00	0.00
	AI4	Facilitar la operación y el uso	2.58	2.58	0.00	0.54	0.00	0.40	0.40
	AI5	Procurar Recursos de TI	1.89	0.86	0.00	0.00	0.00	0.00	0.00
	AI6	Administrar los Cambios	2.58	0.86	0.00	0.74	0.00	0.00	0.54
	AI7	Instalar y Acreditar soluciones y cambios	2.58	1.89	0.00	0.40	0.00	0.00	0.00
Entregar y Dar Soporte	DS2	Administrar los Servicios de Terceros	2.58	2.58	0.54	0.54	0.40	0.40	0.40
	DS3	Administrar el Desempeño y la Capacidad	2.58	1.72	0.00	0.00	0.00	0.00	0.00
	DS4	Asegurar el Servicio Continuo	2.58	1.26	0.00	0.00	0.00	0.00	0.00
	DS5	Garantizar la Seguridad de los Sistemas	0.00	0.00	0.00	0.00	0.54	0.54	0.40
	DS7	Educar y Entrenar a los Usuarios	2.58	1.26	0.00	0.00	0.00	0.00	0.00
	DS8	Administrar la mesa de Servicio y los Incidentes	2.58	1.72	0.00	0.00	0.00	0.00	0.00
	DS9	Administrar la Configuración	2.58	1.26	0.00	0.00	0.00	0.00	0.40
	DS10	Administrar los Problemas	2.58	2.58	0.00	0.00	0.00	0.00	0.00
	DS11	Administrar los Datos	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	DS12	Administrar el Ambiente Físico	0.00	0.00	0.00	0.00	0.00	0.00	0.00
	DS13	Administrar las Operaciones	2.58	1.72	0.00	0.54	0.00	0.00	0.00
Monitorear y Evaluar	ME1	Monitorear y evaluar el desempeño de TI	2.58	2.58	0.54	0.54	0.40	0.40	0.40
	ME2	Monitorear y evaluar el Control Interno	2.58	1.72	0.54	0.54	0.40	0.40	0.40
	ME3	Garantizar el cumplimiento Regulatorio	0.00	0.00	0.00	0.00	0.00	0.00	0.00
		TOTAL REAL	**64.32**	**46.83**	**2.56**	**6.21**	**2.47**	**2.67**	**3.47**
		TOTAL IDEAL	**107.20**	**99.45**	**21.20**	**51.00**	**51.85**	**29.50**	**38.95**
		PORCENTAJE	**60.00%**	**47.09%**	**12.09%**	**12.18%**	**4.77%**	**9.05%**	**8.90%**
		PROMEDIO DE CRITERIOS DE INFORMACION	22.01%						

Tabla 41: Resumen de procesos y criterios de información por impacto.

FUENTE: Realizado por los autores

GRAFICA REPRESENTATIVA DEL IMPACTO DE LOS CRITERIOS DE INFORMACIÓN

En la siguiente gráfica (Figura 6) se observa el resultado de los porcentajes obtenidos en la Tabla 41, que da una idea de cómo en el Departamento de Sistemas de Teleamazonas los procesos impactan a cada uno de los criterios de información.

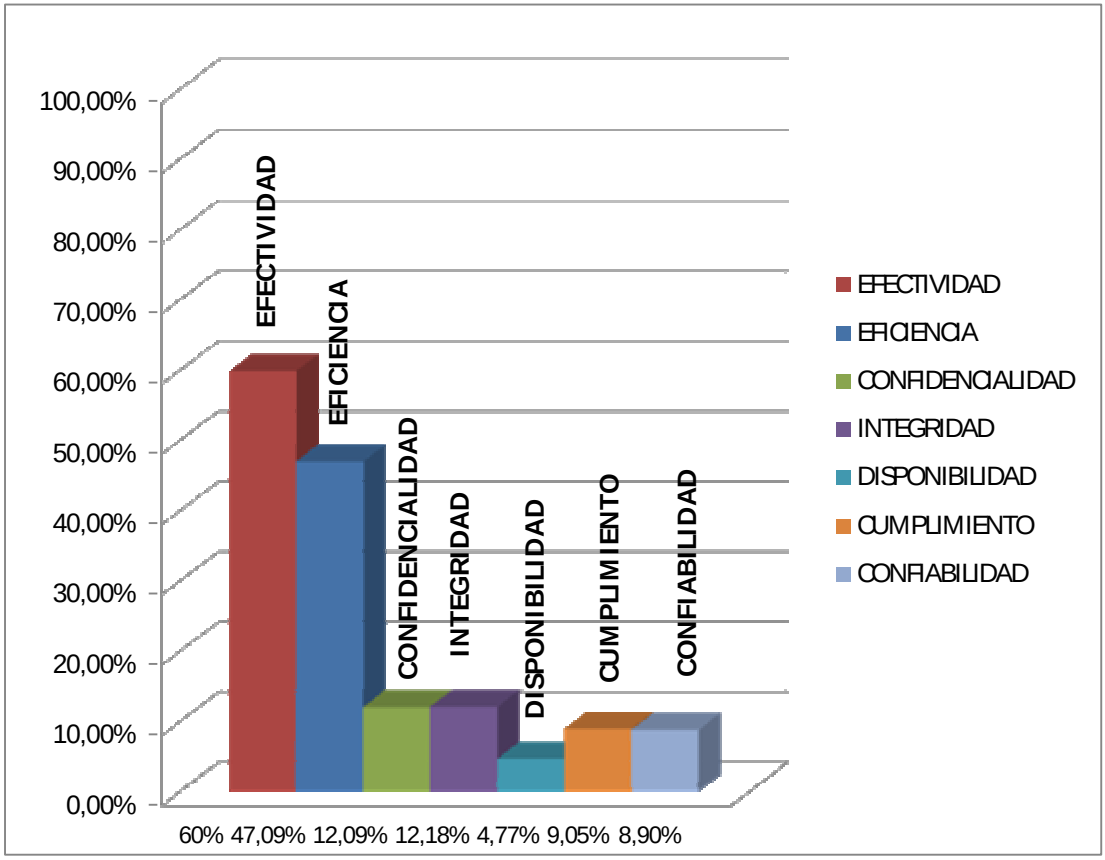

Figura 6: Representación del impacto de los criterios de información.
Fuente: Creación de los autores

CAPITULO 3

PRESENTACIÓN DE RESULTADOS DE LA AUDITORIA

3.1 ELABORACIÓN DEL INFORME FINAL DE AUDITORIA

A continuación se presenta el Informe de la Auditoría de los procesos establecidos por COBIT (Tabla 42 a Tabla 71) aplicados al Departamento de Sistemas de Teleamazonas, presentando para cada uno el factor de riesgo y las recomendaciones respectivas.

PO1: Definir el plan estratégico de TI	Grado de Madurez 3
FACTOR DE RIESGO: No hay una política que defina como y cuando realizar la planeación estratégica de TI. La planeación estratégica de TI no sigue un enfoque estructurado, en el que se documente y se de a conocer a todo el equipo. El proceso de planeación de TI no es sólido y no garantiza que es factible realizar una planeación adecuada. La estrategia general de TI no incluye una definición consistente de los riesgos que la organización está dispuesta a tomar como innovador[1] o como seguidor[2]. Las estrategias de recursos humanos, técnicos y financieros de TI no influencian la adquisición de nuevos productos y tecnologías.	
RECOMENDACIONES COBIT: • Elaborar el Plan Estratégico de TI con la intervención de las gerencias y teniendo en cuenta las necesidades actuales y futuras del Departamento de Sistemas de Teleamazonas. • Analizar y entender las capacidades actuales del Departamento de TI. • Aplicar un esquema de prioridades para los objetivos del negocio que cuantifique los requerimientos del Departamento de Sistemas de Teleamazonas.	

Tabla 42: Resumen de resultados PO1
Fuente: Creación de Autores

[1] Innovador: Es decir que se proponga el plan estratégico como nuevas tendencias a seguir en la empresa. Fuente: Los autores.
[2] Seguidor: Que se fomente seguir el Plan Estratégico para mejorar la situación de la empresa. Fuente: Los autores.

PO2: Definir la arquitectura de la información	Grado de Madurez 2
FACTOR DE RIESGO: No hay un proceso de arquitectura de información ni procedimientos similares, ni intuitivos o informales. Las personas obtienen sus habilidades al construir la arquitectura de información por medio de experiencia práctica y la aplicación repetida de técnicas.	
RECOMENDACIONES COBIT: • Elaborar la arquitectura de la información y datos asignando la propiedad de los mismos para garantizar el correcto uso y seguridad de la información del Departamento de Sistemas de Teleamazonas. • Usar un esquema de clasificación de la información acordado.	

Tabla 43: Resumen de resultados PO2
Fuente: Creación de Autores

PO3: Determinar la dirección tecnológica	Grado de Madurez 3
FACTOR DE RIESGO: La gerencia no está totalmente consciente de la importancia del plan de infraestructura tecnológica. No hay un plan de infraestructura tecnológica definido, documentado y difundido. Los proveedores clave no se seleccionan con base en su entendimiento de la tecnología a largo plazo y de los planes de desarrollo de productos.	
RECOMENDACIONES COBIT: • Establecer la arquitectura de la información estableciendo un foro para dirigir la arquitectura y verificar el cumplimiento • Establecer un Plan de Infraestructura tecnológica equilibrando costos, riesgos y requerimientos y basándose en las necesidades de la arquitectura de la información.	

Tabla 44: Resumen de resultados PO3
Fuente: Creación de Autores

PO4: Definir procesos, organización y relaciones de TI	Grado de Madurez 3
FACTOR DE RIESGO: Existen roles y responsabilidades definidos para la organización de TI. La organización de TI no desarrolla, documenta, comunica y se alinea con la estrategia de TI. No se formulan las relaciones con terceros, incluyendo los comités de dirección, auditoria interna y administración de proveedores. La organización de TI no está funcionalmente completa. Existen definiciones de las funciones a ser realizadas por parte del personal de TI y las que deben realizar los usuarios pero no están bien definidos ya que en ciertas ocasiones todos realizan las mismas funciones por la falta de personal para cubrir las necesidades del momento. No hay una definición formal de las relaciones con los usuarios y con terceros. La división de roles y responsabilidades no está bien definida e implantada.	
RECOMENDACIONES COBIT: • Establecer los procesos de TI y de la empresa en general y establecer roles y responsabilidades de las personas que intervienen o intervendrán en la ejecución de dichos propósitos. • Establecer una estructura organizacional apropiada colocando al Departamento de TI en el nivel que le corresponde por las actividades que realiza, que es nivel asesor para que el mismo tenga poder de decisión dentro de Teleamazonas.	

Tabla 45: Resumen de resultados PO4
Fuente: Creación de Autores

PO5: Administrar la inversión en TI	Grado de Madurez 1
FACTOR DE RIESGO: La organización no reconoce en su totalidad la necesidad de administrar la inversión en TI, y lo poco que reconoce se comunica de manera inconsistente. La asignación de responsabilidades de selección de inversiones en TI y de desarrollo de presupuestos se hace de una forma inicial. Existen implantaciones aisladas de selección y presupuesto de inversiones en TI, con	

documentación informal. Las inversiones en TI se justifican de manera informal. Se toman decisiones presupuestales enfocadas de modo reactivo y operativo.
RECOMENDACIONES COBIT: • Tomar consciencia de que la información o datos del Departamento de Sistemas de Teleamazonas son un activo más, para la adecuada asignación de presupuesto. • Definir criterios formales de inversión. • Medir y evaluar constantemente el valor del negocio con respecto al pronóstico para verificar que el presupuesto ha sido correctamente utilizado.

Tabla 46: Resumen de resultados PO5
Fuente: Creación de Autores

PO6: Comunicar las aspiraciones y la dirección de la gerencia	Grado de Madurez 3
FACTOR DE RIESGO: La gerencia no ha elaborado, documentado y comunicado un ambiente completo de administración de calidad y control de la información. El proceso de elaboración de políticas no es estructurado, mantenido y conocido por el personal, y las políticas, procedimientos y estándares existentes no son sólidos. La gerencia no ha reconocido totalmente la importancia de la conciencia de seguridad de TI y no ha iniciado programas de concienciación formales. El entrenamiento formal no está disponible para apoyar al ambiente de control de información, y 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 no están estandarizadas y formalizadas.	
RECOMENDACIONES COBIT: • Elaborar e implantar Políticas para TI, difundiendo a todo el personal de la empresa, para que tengan en cuenta que deben hacer para apoyar a los	

mismos y sepan a donde quieren llegar. • Monitorear el cumplimiento de las mismas para que no queden solo en papeles.

Tabla 47: Resumen de resultados PO6
Fuente: Creación de Autores

PO7: Administrar recursos humanos de TI	Grado de Madurez 3
FACTOR DE RIESGO: No hay un proceso definido y documentado para administrar los recursos humanos de TI. No hay un plan de administración de recursos humanos. No hay un enfoque estratégico para la contratación y la administración del personal de TI. No está establecido un programa de rotación, diseñado para expandir las habilidades gerenciales y de negocio.	
RECOMENDACIONES COBIT: • Administrar los recursos humanos de TI y elaborar planes de contratación y entrenamiento adecuados. • Evitar la sobre-dependencia de recursos clave para evitar problemas en caso de que los mismos no estén en algún momento • Verificar con roles y responsabilidades si el personal es necesario y suficiente para las tareas del Departamento.	

Tabla 48: Resumen de resultados PO7
Fuente: Creación de Autores

PO9: Evaluar y administrar riesgos de TI	Grado de Madurez 2
FACTOR DE RIESGO: Existe un enfoque de evaluación de riesgos inmaduro y en evolución. La administración de riesgos se da por lo general a altos niveles y se aplica de manera típica solo a proyectos grandes o como respuesta a problemas. Los procesos de mitigación de riesgos están en implementación.	
RECOMENDACIONES COBIT: • Elaborar de forma especifica un Plan de Seguridad teniendo en cuenta todas las áreas de la empresa tanto interna como externamente.	

• Aplicar los planes de seguridad de forma consciente • Realizar permanentes evaluaciones de riesgo • Recomendar y comunicar planes de acción para mitigar riesgos a todo el personal de la empresa.

Tabla 49: Resumen de resultados PO9
Fuente: Creación de Autores

PO10: Administrar proyectos	Grado de Madurez 2
FACTOR DE RIESGO: Los proyectos de TI definen 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 elaboran para muchos aspectos de la administración de proyectos pero no para todos. La aplicación a proyectos de las directrices administrativas se deja a discreción del gerente de proyecto.	
RECOMENDACIONES COBIT: • Definir e implantar marcos y enfoques de programas y de proyectos • Emitir directrices administrativas para proyectos • Hacer la planeación para todos los proyectos incluidos en el portafolio de proyectos.	

Tabla 50: Resumen de resultados PO10
Fuente: Creación de Autores

AI1: Identificar soluciones automatizadas	Grado de Madurez 3
FACTOR DE RIESGO: No hay enfoques claros y estructurados para determinar las soluciones de TI. El enfoque para la determinación de las soluciones de TI requiere la consideración de alternativas evaluadas contra los requerimientos del negocio o del usuario, las oportunidades tecnológicas, la factibilidad económica, las evaluaciones de riesgo y otros factores. El proceso para determinar las soluciones de TI se aplica para algunos proyectos con base en factores tales como las decisiones tomadas por el personal involucrado, la cantidad de	

tiempo administrativo dedicado, y el tamaño y prioridad del requerimiento de negocio original. No se usan enfoques estructurados para definir requerimientos e identificar soluciones de TI.
RECOMENDACIONES COBIT: • Definir requerimientos técnicos y de negocio • Realizar estudios de factibilidad económica, oportunidades tecnológicas para escoger la mejor solución. • Aprobar (o rechazar) los requerimientos y los resultados de los estudios de factibilidad.

Tabla 51: Resumen de resultados AI1
Fuente: Creación de Autores

AI2: Adquirir y mantener el software aplicativo	Grado de Madurez 3
FACTOR DE RIESGO: No hay un proceso claro, definido y de comprensión general para la adquisición y mantenimiento de software aplicativo. 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 muy probable que se salten pasos.	
RECOMENDACIONES COBIT: • Elaborar un plan de adquisición y mantenimiento de Software que garantice tomar la mejor decisión. • Definir estándares de desarrollo para todas las modificaciones • Separar actividades de desarrollo, de pruebas y operativas	

Tabla 52: Resumen de resultados AI2
Fuente: Creación de Autores

AI3: Adquirir y mantener la infraestructura tecnológica	Grado de Madurez 3
FACTOR DE RIESGO: No hay un claro, definido y entendido proceso para adquirir y dar mantenimiento a la infraestructura TI. El proceso existente no respalda las necesidades de las aplicaciones críticas del negocio y no concuerda con la estrategia de negocio de TI. No se planea, programa y coordina el	

mantenimiento.
RECOMENDACIONES COBIT: • Establecer un plan de adquisición de tecnología que se alinee con el plan de infraestructura tecnológica • Implantar medidas de control interno, seguridad y auditabilidad.

Tabla 53: Resumen de resultados AI3
Fuente: Creación de Autores

AI4: Facilitar la operación y el uso	Grado de Madurez 3
FACTOR DE RIESGO: No hay un esquema bien definido, aceptado y comprendido para documentación del usuario, manuales de operación y materiales de entrenamiento. No se guarda y mantiene los procedimientos en una biblioteca formal y cualquiera que necesite saber no tiene acceso a ella. Las correcciones a la documentación y a los procedimientos se realizan por reacción. No hay un proceso que especifica las actualizaciones de procedimientos y los materiales de entrenamiento para que sea un entregable explícito de un proyecto de cambio. A pesar de la existencia de enfoques definidos, el contenido actual varía debido a que no hay un control para reforzar el cumplimiento de estándares. Los usuarios se involucran en los procesos informalmente. No se planea y programa tanto el entrenamiento del negocio como de los usuarios.	
RECOMENDACIONES COBIT: • Implantar una política de documentación de tareas a todos los empleados del Departamento de Sistemas de Teleamazonas para transferir el conocimiento y de esta manera apoyar al control y evaluación. • Comunicar y entrenar a usuarios, a la gerencia del negocio, personal de apoyo y personal de operación	

Tabla 54: Resumen de resultados AI4
Fuente: Creación de Autores

AI5: Adquirir recursos de TI	Grado de Madurez 1
FACTOR DE RIESGO: La organización no 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 y administrados por gerentes de proyecto u otras personas que ejercen su juicio profesional más que seguir resultados de procedimientos y políticas formales. Sólo existe una relación *ad hoc* entre los procesos de administración de adquisiciones y contratos corporativos de TI. Los contratos de adquisición se administran a la terminación de los proyectos más que sobre una base continua.	
RECOMENDACIONES COBIT: • Asesorarse profesional, legal y contractualmente para adquirir algún recurso de TI. • Definir procedimientos y estándares de adquisición • Adquirir hardware, software y servicios requeridos de acuerdo con los procedimientos definidos	

Tabla 55: Resumen de resultados AI5
Fuente: Creación de Autores

AI6: Administrar cambios	Grado de Madurez 1
FACTOR DE RIESGO: No se reconoce que los cambios se deben administrar y controlar. Las prácticas varían y es muy probable que se puedan dar cambios sin autorización. Hay documentación de cambio pobre o no existente y la documentación de configuración es incompleta y no confiable. Es posible que ocurran errores junto con interrupciones al ambiente de producción, provocados por una pobre administración de cambios.	
RECOMENDACIONES COBIT: • Evaluación, asignar prioridad y autorizar cambios • Seguir el procedimiento y reporte de cambios	

Tabla 56: Resumen de resultados AI6
Fuente: Creación de Autores

AI7: Instalar y acreditar soluciones y cambios	Grado de Madurez 3
FACTOR DE RIESGO: No se cuenta con una metodología formal en relación con la instalación, migración, conversión y aceptación. Los procesos de TI para instalación y acreditación no están integrados dentro del ciclo de vida del sistema y no están automatizados. El entrenamiento, pruebas, transición y acreditación a producción tienen variaciones respecto al proceso definido, con base en las decisiones individuales.	
RECOMENDACIONES COBIT: • Establecer una metodología de prueba a los cambios realizados. • Evaluar y aprobar los resultados de las pruebas por parte de la gerencia del negocio • Ejecutar revisiones posteriores a la implantación	

Tabla 57: Resumen de resultados AI7
Fuente: Creación de Autores

DS2: Administrar los servicios de terceros	Grado de Madurez 3
FACTOR DE RIESGO: No hay procedimientos bien documentados para controlar los servicios de terceros con procesos claros para tratar y negociar con los proveedores. Cuando se hace un acuerdo de prestación de servicios, la relación con el tercero no es meramente contractual. La naturaleza de los servicios a prestar no se detalla en el contrato y no incluye requerimientos legales, operacionales y de control. No se asigna la responsabilidad a algún miembro del departamento de supervisar los servicios de terceros. Los términos contractuales no se basan en formatos estandarizados. El riesgo del negocio asociado con los servicios del tercero no está valorado y reportado.	
RECOMENDACIONES COBIT: • Establecer un procedimiento de contratación de servicios por terceros que	

garantice que estos cumplan a cabalidad con su trabajo y para tener un mejor control del uso de recursos del Departamento de Sistemas de Teleamazonas.

Tabla 58: Resumen de resultados DS2
Fuente: Creación de Autores

DS3: Administrar el desempeño y la capacidad	Grado de Madurez 2
FACTOR DE RIESGO: Los responsables del negocio y la gerencia de TI no están concientes del impacto de no administrar el desempeño y la capacidad. Las necesidades de desempeño se logran por lo general con base en evaluaciones de sistemas individuales, el conocimiento y soporte de equipos de proyecto. Algunas herramientas individuales pueden utilizarse para diagnosticar problemas de desempeño y de capacidad, pero la consistencia de los resultados depende de la experiencia de individuos clave. No hay una evaluación general de la capacidad de desempeño de TI. Los problemas de disponibilidad son susceptibles de ocurrir de manera inesperada y aleatoria y toma mucho tiempo diagnosticarlos y corregirlos. Cualquier medición de desempeño se basa primordialmente en las necesidades de TI y no en las necesidades del cliente.	
RECOMENDACIONES COBIT: • Administrar el desempeño capacidad y disponibilidad de los sistemas de la empresa.	

Tabla 59: Resumen de resultados DS3
Fuente: Creación de Autores

DS4: Garantizar la continuidad del servicio	Grado de Madurez 2
FACTOR DE RIESGO: No se asigna la responsabilidad a alguno de los miembros del departamento para mantener la continuidad del servicio. Los enfoques para asegurar la continuidad están fragmentados. Los reportes sobre la disponibilidad son esporádicos, pueden estar incompletos y no toman en cuenta el impacto en el negocio. No hay un plan de continuidad de TI documentado, aunque hay compromiso para mantener disponible la continuidad del servicio y sus	

principios más importantes se conocen. Existe un inventario de sistemas y componentes críticos, pero puede no ser confiable.
RECOMENDACIONES COBIT: • Desarrollar y mantener planes de contingencia de TI • Difundir los planes de contingencia con entrenamiento y pruebas de los mismos. • Guardar copias de los planes de contingencia y de los datos fuera de las instalaciones.

Tabla 60: Resumen de resultados DS4
Fuente: Creación de Autores

DS5: Garantizar la seguridad de los sistemas	Grado de Madurez 2
FACTOR DE RIESGO: Las responsabilidades y la rendición de cuentas sobre la seguridad, no están asignadas a un coordinador de seguridad de TI. 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 no cumplen con los requerimientos específicos de seguridad del Departamento de Sistemas de Teleamazonas. Las políticas de seguridad se están desarrollando, pero las herramientas y las habilidades son inadecuadas. Los reportes de la seguridad de TI son incompletos. La capacitación sobre seguridad está disponible pero depende principalmente de la iniciativa del individuo. La seguridad de TI es vista primordialmente como responsabilidad y disciplina de TI, y el negocio no ve la seguridad de TI como parte de su propia disciplina.	
RECOMENDACIONES COBIT: • Entender los requerimientos, vulnerabilidades y amenazas de seguridad. • Administrar autorizaciones a los usuarios de forma estandarizada. • Probar la seguridad de forma regular.	

Tabla 61: Resumen de resultados DS5
Fuente: Creación de Autores

DS7: Educar y entrenar a los usuarios	Grado de Madurez 2
FACTOR DE RIESGO: El programa de entrenamiento y educación, y los procesos asociados a lo largo de toda la organización está comenzando a identificarse en los planes de desempeño individuales de los empleados. Los procesos se desarrollan hasta la fase en la cual se imparte entrenamiento informal por parte de diferentes instructores. Sin embargo, hay comunicación consistente sobre los problemas globales y sobre la necesidad de atenderlos.	
RECOMENDACIONES COBIT: • Establecer un plan de entrenamiento a usuarios • Monitorear y reportar la efectividad del entrenamiento.	

Tabla 62: Resumen de resultados DS7
Fuente: Creación de Autores

DS8: Administrar la mesa de servicio y los incidentes	Grado de Madurez 2
FACTOR DE RIESGO: No hay conciencia organizacional de la necesidad de una función de mesa de servicio y de un proceso de administración de incidentes. Existe ayuda disponible de manera informal a través de una red de individuos expertos. Estos individuos tienen a su disposición algunas herramientas comunes para ayudar en la resolución de incidentes. No hay entrenamiento formal y la comunicación sobre procedimientos estándar y la responsabilidad es delegada al usuario.	
RECOMENDACIONES COBIT: • Crear el servicio de una mesa de servicios • Monitorear y reportar tendencias	

Tabla 63: Resumen de resultados DS8
Fuente: Creación de Autores

DS9: Administrar la configuración	Grado de Madurez 2
FACTOR DE RIESGO: La gerencia no esta conciente de la necesidad de controlar la configuración de TI y no entiende los beneficios de mantener información completa y precisa sobre las configuraciones. Las herramientas para la administración de configuraciones se utilizan hasta cierto grado, pero difieren entre plataformas. Además no se definen prácticas estandarizadas de trabajo. El contenido de la información de la configuración es limitado y no utilizan procesos interrelacionados, tales como administración de cambios y administración de problemas.	
RECOMENDACIONES COBIT: • Establecer un repositorio central de todos los elementos de la configuración • Identificar los elementos de configuración y su mantenimiento • Revisar la integridad de los datos de configuración.	

Tabla 64: Resumen de resultados DS9
Fuente: Creación de Autores

DS10: Administración de problemas	Grado de Madurez 3
FACTOR DE RIESGO: No se acepta la necesidad de un sistema integrado de administración de problemas y no se evidencia con el apoyo de la gerencia y la asignación de presupuesto para personal y capacitación. El registro y rastreo de problemas y soluciones se dividen dentro del equipo de respuesta, utilizando las herramientas disponibles. Es poco probable detectar las desviaciones de los estándares y de las normas establecidas. La información no se comparte entre el personal de manera formal y proactiva. La revisión de incidentes y los análisis de identificación y resolución de problemas son limitados e informales.	
RECOMENDACIONES COBIT: • Administrar y analizar causas raíz de los problemas reportados • Tomar propiedad de los problemas y una resolución de problemas progresiva.	

Tabla 65: Resumen de resultados DS10
Fuente: Creación de Autores

DS11: Administración de datos	Grado de Madurez 2
FACTOR DE RIESGO: No hay conciencia sobre la necesidad de una adecuada administración de los datos. No se observa la propiedad y responsabilidad sobre los datos. Los requerimientos de seguridad para la administración de datos no son documentados por individuos clave. No se lleva a cabo algún tipo de monitoreo dentro de TI sobre algunas actividades clave de la administración de datos (respaldos, recuperación y desecho). Las responsabilidades para la administración de datos son asignadas de manera informal a personal clave de TI.	
RECOMENDACIONES COBIT: • Realizar un plan de Respaldos más específico que el que ya se tiene en el Departamento de Sistemas, administrando el almacenamiento de datos en sitio y fuera de sitio • Probar la restauración de la información • Desechar de manera segura los datos y el equipo para que no puedan tener acceso personas que pueden hacer mal uso de la información.	

Tabla 66: Resumen de resultados DS11
Fuente: Creación de Autores

DS12: Administración del ambiente físico	Grado de Madurez 3
FACTOR DE RIESGO: Los controles ambientales, el mantenimiento preventivo y la seguridad física no cuentan con presupuesto autorizado y rastreado por la gerencia. No se aplican restricciones de acceso, permitiendo el ingreso a las instalaciones de cómputo sólo al personal aprobado. Los visitantes se registran a la entrada de la organización. Las instalaciones físicas mantienen un perfil bajo y son reconocibles de manera fácil. Las autoridades civiles no monitorean al cumplimiento con los reglamentos de salud y seguridad. Los riesgos se aseguran con el mínimo esfuerzo para optimizar los costos del seguro.	

RECOMENDACIONES COBIT:
• Implementar medidas de seguridad físicas. • Administrar las instalaciones físicas de manera que se garantice la seguridad de los activos del Departamento de Sistemas de Teleamazonas.

Tabla 67: Resumen de resultados DS12
Fuente: Creación de Autores

DS13: Administración de operaciones	Grado de Madurez 2
FACTOR DE RIESGO: La organización no está conciente del rol clave que las actividades de operaciones de TI juegan en brindar funciones de soporte de TI. No se asignan 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. Las instrucciones de qué hacer, cuándo y en qué orden no están documentadas.	
RECOMENDACIONES COBIT: • Administrar las operaciones del ambiente de TI en línea con los niveles de servicio acordados y con las instrucciones definidas.	

Tabla 68: Resumen de resultados DS13
Fuente: Creación de Autores

ME1: Monitorear y evaluar el desempeño de TI	Grado de Madurez 3
FACTOR DE RIESGO: La gerencia no ha comunicado e institucionalizado un proceso estándar de monitoreo. No se implantan programas educacionales y de entrenamiento para el monitoreo. Las evaluaciones todavía se realizan al nivel de procesos y proyectos individuales de TI y no están integradas a través de todos los procesos. No se definen herramientas para monitorear los procesos y los niveles de servicio de TI. Las mediciones de la contribución de la función de servicios de información al desempeño de la organización se definen, usando criterios financieros y operativos tradicionales. Las mediciones del desempeño específicas de TI, las mediciones no financieras, las estratégicas, las de	

satisfacción del cliente y los niveles de servicio no están definidas. No se ha definido un marco de trabajo para medir el desempeño.
RECOMENDACIONES COBIT: • Establecer programas de reportes de desempeño de proceso a reportes gerenciales • Comparar el desempeño contra las metas acordadas e iniciar las medidas correctivas necesarias

Tabla 69: Resumen de resultados ME1
Fuente: Creación de Autores

ME2: Monitorear y evaluar el control interno	Grado de Madurez 2
FACTOR DE RIESGO: La organización no utiliza reportes de control para comenzar iniciativas de acción correctiva. La evaluación del control interno depende de las habilidades de individuos clave. La organización no tiene mayor conciencia sobre el monitoreo de los controles internos. Se están empezando a usar metodologías y herramientas para monitorear los controles internos, aunque no se basan en un plan. Los factores de riesgo específicos del ambiente de TI se identifican con base en las habilidades de individuos.	
RECOMENDACIONES COBIT: • Definir un sistema de controles interno integrado en el marco de trabajo de los procesos de TI • Monitorear y reportar la efectividad de los controles internos sobre TI • Reportar las excepciones de control a la gerencia para tomar acciones	

Tabla 70: Resumen de resultados ME2
Fuente: Creación de Autores

ME3: Garantizar el cumplimiento regulatorio	Grado de Madurez 3
FACTOR DE RIESGO: No se desarrollan, documentado y comunicado políticas, procedimientos y procesos, para garantizar el cumplimiento de los reglamentos y de las obligaciones contractuales legales. Se realiza poco monitoreo y existen	

requisitos de cumplimiento que no están resueltos. No se brinda entrenamiento sobre requisitos legales y regulatorios externos que afectan a la organización y no se instruye respecto a los procesos de cumplimiento definidos.
RECOMENDACIONES COBIT: • Establecer políticas y procedimientos para cumplir con requisitos legales y regulatorios relacionados con la TI

Tabla 71: Resumen de resultados ME3
Fuente: Creación de Autores

IMPACTO DE LOS CRITERIOS DE INFORMACIÓN EN EL DEPARTEMENTO DE SISTEMAS DE TELEAMAZONAS

A continuación se presenta el informe del impacto de los criterios de información en TELEAMAZONAS (Tabla 72 a Tabla 78).

CRITERIO DE INFORMACIÓN	**Porcentaje**
Efectividad	60%
RECOMENDACIÓN COBIT: Para que exista una alta efectividad en el Departamento de Sistemas y llegue al 100% se recomienda que la información importante y referente a los procesos del negocio sea oportuna, correcta, consistente y utilizable.	

Tabla 72: Resumen de resultados criterio: Efectividad
Fuente: Creación de Autores

CRITERIO DE INFORMACIÓN	**Porcentaje**
Eficiencia	47,09%
RECOMENDACIÓN COBIT: Para que exista una alta eficiencia en el Departamento de Sistemas y llegue al 100% se recomienda que la información que se obtenga sea optimizando los recursos de TI.	

Tabla 73: Resumen de resultados criterio: Eficiencia
Fuente: Creación de Autores

CRITERIO DE INFORMACIÓN	Porcentaje
Confidencialidad	12,09%
RECOMENDACIÓN COBIT: Para que exista una alta confidencialidad en el Departamento de Sistemas de Teleamazonas y llegue al 100% se recomienda que la información sensible contra divulgación no autorizada del Departamento de Sistemas se le otorgue una debida protección contra intrusos o extraños al departamento.	

Tabla 74: Resumen de resultados criterio: Confidencialidad
Fuente: Creación de Autores

CRITERIO DE INFORMACIÓN	Porcentaje
Integridad	12,08%
RECOMENDACIÓN COBIT: Para que exista una alta integridad en el Departamento de Sistemas y llegue al 100% se recomienda que la información entregada al mismo mantenga su validez de acuerdo con los valores y expectativas del negocio, así como también exista precisión y suficiencia de la información.	

Tabla 75: Resumen de resultados criterio: Integridad
Fuente: Creación de Autores

CRITERIO DE INFORMACIÓN	Porcentaje
Disponibilidad	4,77%
RECOMENDACIÓN COBIT: Para que exista una alta disponibilidad en el Departamento de Sistemas y llegue al 100% se recomienda que la información cuando es requerida por el proceso del negocio ahora y en el futuro se encuentre disponible, así como también se debe tomar en cuenta la protección de los recursos de TI y las capacidades asociadas.	

Tabla 76: Resumen de resultados criterio: Disponibilidad
Fuente: Creación de Autores

CRITERIO DE INFORMACIÓN	Porcentaje
Cumplimiento	9,05%
RECOMENDACIÓN COBIT: Para que exista un alto cumplimiento en el Departamento de Sistemas y llegue al 100% se recomienda que se lleve un adecuado cumplimiento de las leyes, regulaciones, y acuerdos contractuales a los que el proceso del negocio esta sujeto.	

Tabla 77: Resumen de resultados criterio: Cumplimiento
Fuente: Creación de Autores

CRITERIO DE INFORMACIÓN	Porcentaje
Confiabilidad	8,90%
RECOMENDACIÓN COBIT: Para que exista una alta confiabilidad en el Departamento de Sistemas y llegue al 100% se recomienda que se entregue una información adecuada para que la gerencia administre la entidad y ejerza sus responsabilidades de reportes financieros y de cumplimiento.	

Tabla 78: Resumen de resultados criterio: Confiabilidad
Fuente: Creación de Autores

Como promedio total del impacto de los criterios de información se obtuvo el valor de 22,01%, lo que en comparación con el 100% es bajo en su impacto.

3.2 PRESENTACIÓN DEL INFORME FINAL DE AUDITORIA

Informe ejecutivo

El presente informe muestra los resultados de la evaluación de los procesos que establece COBIT, practicada al Departamento de Sistemas de Teleamazonas, en base a los grados de madurez.

A continuación (Tabla 79) se presentan un resumen de los resultados obtenidos, con los cuales la empresa y la dirección de TI pueden darse cuenta en el nivel que están ubicados para analizar y poner en práctica las recomendaciones enunciadas en la anterior sección.

PO1: Definir el plan estratégico de TI	Grado de Madurez 3
PO2: Definir la arquitectura de la información	Grado de Madurez 2
PO3: Determinar la dirección tecnológica	Grado de Madurez 3
PO4: Definir procesos, organización y relaciones de TI	Grado de Madurez 3
PO5: Administrar la inversión en TI	Grado de Madurez 1
PO6: Comunicar las aspiraciones y la dirección de la gerencia	Grado de Madurez 3
PO7: Administrar recursos humanos de TI	Grado de Madurez 3
PO9: Evaluar y administrar riesgos de TI	Grado de Madurez 2
PO10: Administrar proyectos	Grado de Madurez 2
AI1: Identificar soluciones automatizadas	Grado de Madurez 3
AI2: Adquirir y mantener el software aplicativo	Grado de Madurez 3
AI3: Adquirir y mantener la infraestructura tecnológica	Grado de Madurez 3
AI4: Facilitar la operación y el uso	Grado de Madurez 3
AI5: Adquirir recursos de TI	Grado de Madurez 1
AI6: Administrar cambios	Grado de Madurez 1
AI7: Instalar y acreditar soluciones y cambios	Grado de Madurez 3
DS2: Administrar los servicios de terceros	Grado de Madurez 3
DS3: Administrar el desempeño y la capacidad	Grado de Madurez 2
DS4: Garantizar la continuidad del servicio	Grado de Madurez 2
DS5: Garantizar la seguridad de los sistemas	Grado de Madurez 2
DS7: Educar y entrenar a los usuarios	Grado de Madurez 2
DS8: Administrar la mesa de servicio y los incidentes	Grado de Madurez 2
DS9: Administrar la configuración	Grado de Madurez 2
DS10: Administración de problemas	Grado de Madurez 3

DS11: Administración de datos	Grado de Madurez 2
DS12: Administración del ambiente físico	Grado de Madurez 3
DS13: Administración de operaciones	Grado de Madurez 2
ME1: Monitorear y evaluar el desempeño de TI	Grado de Madurez 3
ME2: Monitorear y evaluar el control interno	Grado de Madurez 2
ME3: Garantizar el cumplimiento regulatorio	Grado de Madurez 3

Tabla 79: Grados de madurez en los que se encuentra el Departamento de Sistemas de Teleamazonas.
Fuente: Creación de Autores

A continuación (Tabla 80) se presenta los grados de madurez tomados como referencia:

0	No existe	No se aplican procesos administrativos en lo absoluto.
1	Inicial	Los procesos son iniciales y desorganizados.
2	Repetible	Los procesos siguen un patrón regular.
3	Definido	Los procesos se documentan y se comunican.
4	Administrado	Los procesos se monitorean y se miden.
5	Optimizado	Las buenas prácticas se siguen y se automatizan.

Tabla 80: Referencia del valor del modelo de madurez
Fuente: Creación de Autores

El cálculo de porcentaje de los criterios de información se presenta a continuación (Tabla 81):

Efectividad	**60 %**
Eficiencia	**47.09 %**
Confidencialidad	**12.09 %**
Integridad	**12.08 %**
Disponibilidad	**4.77 %**
Cumplimiento	**9.05 %**
Confiabilidad	**8.90 %**
Promedio de los criterios de información	**22.01 %**

Tabla 81: Resumen de Resultados
Fuente: Creación de Autores

A continuación se presenta gráficamente (Figura 7) el porcentaje obtenido por cada uno de los criterios de la información, para tener una visión mas clara del estado que se encuentra el Departamento de Sistemas de Teleamazonas:

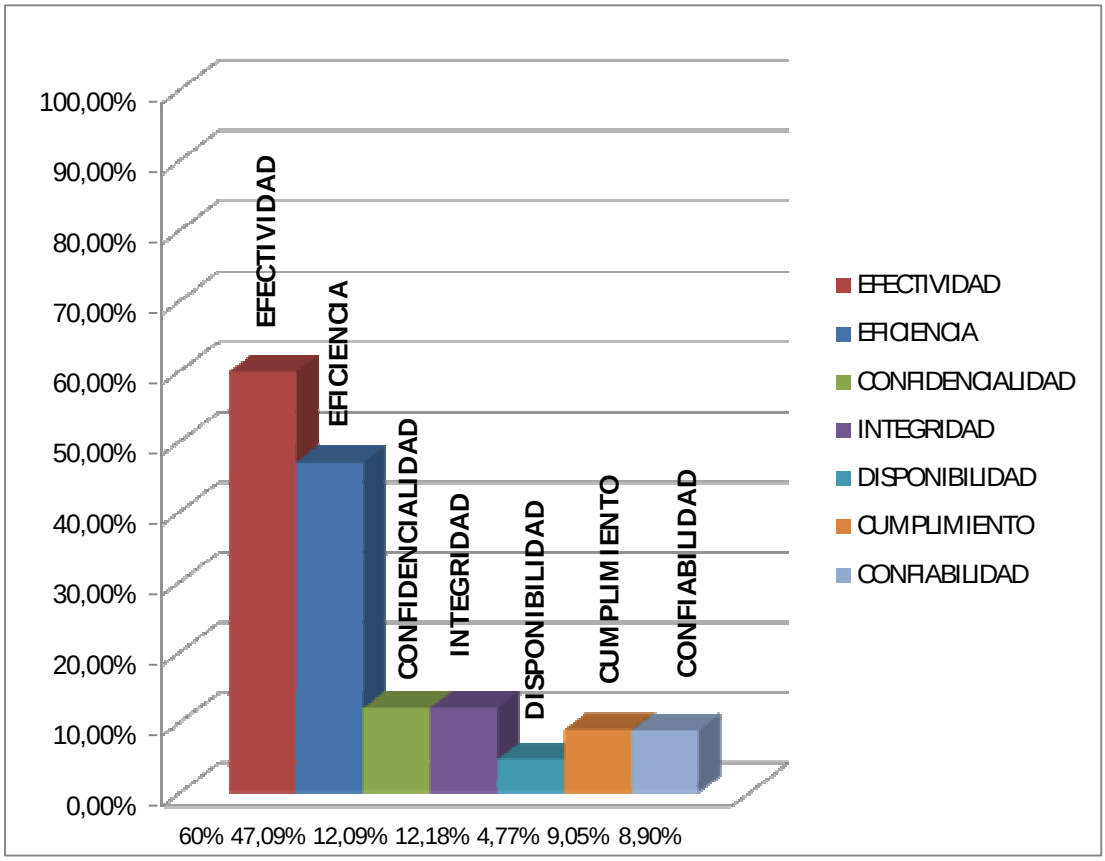

Figura 7: Impacto de los criterios de información en el Departamento de Sistemas de Teleamazonas.
Fuente: Creación de los autores

El Promedio general obtenido de los criterios de la información es del 21,01%.

CAPITULO 4
CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- Los objetivos de control planteados por COBIT se relacionan de manera directa con el ambiente de manejo y evaluación de riesgos, los mismos que pueden ser entendidos tanto por el departamento administrativo como por el Departamento de Sistemas.
- El Jefe del Departamento de Sistemas de Teleamazonas puede asegurar que proporciona un sistema de control de riesgos adecuado para el ambiente de TI si administra adecuadamente los Objetivos de Control de alto nivel que se encuentran distribuidos en los Dominios de COBIT.
- Los Modelos de Madurez de COBIT para el control sobre los procesos de TI dan un punto claro de donde la organización está actualmente y son un punto de partida para fijar una meta futura de ascenso hasta llegar al nivel óptimo.
- La utilización de una norma internacional como lo es la ISO 17799 para el manejo de la seguridad dentro de un área de TI, previa la elaboración de la Auditoria nos ayudó a conocer la situación actual de la organización para luego seleccionar los objetivos de control de COBT indicados para evaluarlos.
- En el Departamento de Sistemas de Teleamazonas se encontró procesos con grado de madurez 1, lo que quiere decir que estos son iniciales y desorganizados.
- Se determinó el impacto de los procesos de TI sobre la efectividad (60%), eficiencia (47,09%), confidencialidad (12,09%), integridad (12,08%), disponibilidad (4,77%), cumplimiento (9,05%) y confiabilidad (8,90%) del Departamento de Sistemas de Teleamazonas, dando un promedio de 22,01%; lo que nos indica que la organización se encuentra en un nivel bajo en cuanto a gestión de riesgos de TI.

4.2 RECOMENDACIONES

- Se recomienda documentar todos los procesos de TI en forma gráfica y escrita, para establecer controles de seguridad de la información y de esta manera evitar que la misma sea vulnerable ante errores, fallas, etc. Además TELEAMAZONAS debe tener un Plan Estratégico actualizado que sirva como guía y ayuda al Departamento de Sistemas, y este pueda elaborar su propio Plan Estratégico conjuntamente ligado al general.
- Tomar en cuenta los factores de riesgos y recomendaciones dadas por esta Auditoria, ya que va a ser de gran aporte para mejorar el desempeño del Departamento de Sistemas de Teleamazonas y así orientar su trabajo y esfuerzo al desarrollo de toda la organización.
- Se recomienda al Departamento de Sistemas de Teleamazonas que inicie un proceso de implementación de un modelo de control que puede ser COBIT, ya que esta metodología es fruto de un compendio de experiencias y recomendaciones de profesionales a nivel mundial.
- La Gerencia de TI del Departamento de Sistemas de Teleamazonas debe tomar en consideración los procesos que se encuentran en un grado de madurez 1; ya que los mismos están en un estado crítico y requieren atención inmediata.
- Tomar en consideración los porcentajes obtenidos acerca de los criterios de información que tiene que ver con efectividad, eficiencia, confiabilidad, integridad, disponibilidad, confidencialidad y cumplimiento, para que de esta manera el Departamento de Sistemas de Teleamazonas cubra las debilidades que tenga y lograr así un mejor desempeño.

REFERENCIAS BIBLIOGRÁFICAS

Tesis

- CARRIÓN Mayra, CORONADO Luz, Auditoria de la Gestión de las TIC'S para la empresa DIPAC utilizando COBIT, 2007
- MATUTE María Del Carmen, QUISPE Transito, Auditoria de la Gestión de la Seguridad en la red de datos del SWISSOTEL basado en COBIT, Escuela Politécnica Nacional, Facultad de Sistemas, 2006
- VELÁSTEGUI Talina, Análisis de la Gestión de las Tecnologías de la Información de la Escuela Politécnica Nacional utilizando COBIT, 2007

Fuente Bibliográfica

- Avaya Communications Proprietary and Confidential Information Reference: - BG Issue: 1.0 06/05/2008
- Comité Directivo de COBIT, COBIT 4.0 Marco de Trabajo, año 2006
- Documentación facilitada por Teleamazonas
- Estándar Internacional ISO/IEC 17799, Segunda Edición Junio 2005
- NARANJO, Jaime. Documentación de Auditoria y Evaluación de Sistemas.

Fuentes de Internet

- Information Systems Audit and Control Association. http://www.isaca.org/Template.cfm?Section=Downloads3&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=63&ContentID=13742, 2008
- Teleamazonas junto a ti. http://www.teleamazonas.com, 2008
- Wikipedia, la enciclopedia libre. http://es.wikipedia.org/wiki/Teleamazonas, 2007

GLOSARIO:

Ad Hoc: porque sí, por costumbre, sin costo.

Auditoría: La auditoria es el control de los controles cuyo objetivo es evaluar la eficiencia y eficacias con que se está operando para que se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación.

COBIT: Control Objetives Information Technologies, es un modelo de referencia, empleado en la administración y control de las tecnologías de la información.

COSO: Comité de organizaciones patrocinadoras de la comisión Treadway Estándar aceptado a nivel internacional para el gobierno corporativo.

Dominio: Agrupación de objetivos de control en las etapas lógicas en el ciclo de vida de inversión en TI.

Estándar: Es un conjunto de reglas y especificaciones a seguir, mismas que son desarrolladas de común acuerdo para su uso permanente por las empresas, instituciones o personas que representan cualquier sector y tiene como fin cubrir una necesidad vigente.

Gobierno (governance): Sistema de alta gerencia para asegurar la consecución de los objetivos de una organización.

KGI: Indicador clave de meta. Definen las medidas que indican a la administración – después del hecho- si un proceso de TI ha satisfecho sus requerimientos de negocio.

KPI: Indicador clave de desempeño. Define mediada para determinar que también se está desempeñando el proceso de TI para permitir que se alcance el objetivo; son indicadores guía de que un objetivo probablemente se alcanzará o no; y son buenos indicadores de capacidades, prácticas y habilidades.

Objetivo de Control: Es el propósito que se desea alcanzar al implantar los procedimientos de control en un proceso en particular.

Riesgo: Es la probabilidad de obtener un resultado desfavorable como resultad de la exposición de un evento dado.

TIC'S: Tecnologías de la Información y Comunicación; son aquellos sistemas informáticos ya se hardware o software que permiten desarrollar, convertir, almacenar y administrar la información.