UNIVERSIDAD DE CUENCA

FACULTAD DE INGENIERIA

Universidad de Cuenca

INGENIERIA EN SISTEMAS

VERONICA QUINTUÑA RODRIGUEZ

Dirigido por:
Ing. Pablo Vanegas Peralta, PhD.

AUDITORIA INFORMATICA A LA SUPERINTENDENCIA DE TELECOMUNICACIONES

UNIVERSIDAD DE CUENCA

FACULTAD DE INGENIERIA

AUDITORIA INFORMATICA A LA SUPERINTENDENCIA DE TELECOMUNICACIONES

VERONICA QUINTUÑA RODRIGUEZ

Universidad de Cuenca

INGENIERIA EN SISTEMAS

Un exhaustivo recorrido por los diversos estándares, técnicas y normas que rigen actualmente los procesos de auditoría informática, nos han llevado a determinar como marco de referencia para su ejecución, a COBIT.

Se define y aplica una estrategia basada en los objetivos de control de éste estándar, obteniendo como resultado indicadores que determinan el impacto, desempeño, madurez y cumplimiento de objetivos por cada proceso; los cuales fundamentan las recomendaciones y planes de acción, establecidos con miras a optimizar el desarrollo de las TIC'sen la SUPERTEL..

Auditoría Informática a la Superintendencia de Telecomunicaciones

Facultad de Ingeniería
Escuela de Informática

Auditoría Informática a la Superintendencia de Telecomunicaciones

Trabajo de titulación previo a la Obtención del Título de Ingeniero de Sistemas

Autor:

Verónica Karina Quitnuña Rodríguez

Director:
Pablo Fernando Vanegas Peralta

Cuenca – Ecuador

2012

Resumen:

El proyecto de tesis intitulado "Auditoría Informática a la Superintendencia de Telecomunicaciones", marca su inicio efectuando un análisis comparativo de la tecnología, normas y técnicas que estandarizan los procesos de auditoría informática en la actualidad, para posteriormente realizar un estudio del entorno a auditar, precisar una estrategia de auditoría, ejecutar los planes y programas puntualizados; y finalmente emitir un informe que determine si cada uno de los procesos de tecnología de la información colaboran eficazmente con la consecución de los objetivos institucionales, precisando un conjunto de recomendaciones en base a los resultados obtenidos

Palabras Clave:

Auditoría informática AI, tecnología de la información TI, COBIT, COSO, ITIL, procesos de TI, estándares, normas y técnicas de auditoría, modelos de madurez.

Indice General

Presentación:

El proyecto de tesis intitulado "Auditoría Informática a la Superintendencia de Telecomunicaciones", marca su inicio efectuando un análisis comparativo de la tecnología, normas y técnicas que estandarizan los procesos de auditoría informática en la actualidad, para posteriormente realizar un estudio del entorno a auditar, precisar una estrategia de auditoría, ejecutar los planes y programas puntualizados; y finalmente emitir un informe que determine si cada uno de los procesos de tecnología de la información colaboran eficazmente con la consecución de los objetivos institucionales, precisando un conjunto de recomendaciones en base a los resultados obtenidos.

Palabras Clave: auditoría informática AI, tecnología de la información TI, COBIT, COSO, ITIL, procesos de TI, estándares, normas y técnicas de auditoría, modelos de madurez.

Datos de catalogación bibliográfica

QUINTUÑA RODRÍGUEZ VERÓNICA KARINA
Auditoría Informática a la Superintendencia de Telecomunicaciones

Universidad de Cuenca, Cuenca – Ecuador, 2012
INGENIERÍA DE SISTEMAS

Formato A4 Páginas: 86

Breve reseña del autor e información de contacto:

Verónica Karina Quintuña Rodríguez

Egresada de la Escuela de Informática
Facultad de Ingeniería
Universidad de Cuenca, Ecuador.
Ingeniera Electrónica
Facultad de Ingenierías
Universidad Politécnica Salesiana, Ecuador, 2010
veronicakarinaq@hotmail.com

Dirigido por:

Pablo Vanegas Peralta

Ingeniero en Sistemas
Universidad de Cuenca, Ecuador, 1997.
Diplomado Superior en Formulación y Evaluación de Proyectos de Investigación
Universidad de Cuenca, Ecuador, 2004.
Master en Inteligencia Artificial
KatholiekeUniversiteitLeuven, Belgica, 2006.
PhD en Ingeniería Mecánica
KatholiekeUniversiteitLeuven, Bélgica, 2010.
pvanegas@ucuenca.edu.ec

Quintuña Rodríguez Verónica K.
Auditoría Informática a la Superintendencia de Telecomunicaciones

Edición y Producción:
Ing. Verónica Karina Quintuña Rodríguez

Diseño de la portada:
Ing. Verónica Karina Quintuña Rodríguez

IMPRESO EN ECUADOR

A Dios, Jesús y la Virgen.

DECLARACIÓN

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

Cuenca, Abril del 2012.

Verónica Quintuña Rodríguez

Ing. Pablo Vanegas Peralta, PhD.
Director de Tesis

CERTIFICO

Que la realización de la presente tesis ha cumplido con todos los objetivos planteados y se ha desarrollado acorde a las normas y estatutos que rigen la Facultad de Ingeniería, Escuela de Informática de la Universidad de Cuenca. Por lo

tanto autorizo su presentación para los fines consiguientes.

Cuenca, Abril del 2012

Ing. Pablo Vanegas

Prefacio

El presente documento ha sido elaborado como trabajo de tesis previa la obtención del título de Ingeniera en Sistemas en la Universidad de Cuenca. El proyecto fue establecido con el objetivo general de realizar una Auditoría

Informática a la Superintendencia de Telecomunicaciones, más concretamente a la Unidad de Tecnología de la Información.

De acuerdo a los objetivos específicos, el proyecto marca su inicio efectuando un análisis comparativo de la tecnología, normas y técnicas que estandarizan los procesos de AI en la actualidad, para posteriormente realizar un estudio del entorno a auditar, precisar una estrategia de auditoría, ejecutar los planes y programas puntualizados; y finalmente emitir un informe que determine si cada uno de los procesos de TI colaboran eficazmente con la consecución de los objetivos institucionales, precisando un conjunto de recomendaciones en base a los resultados obtenidos.

Prólogo

Las Tecnologías de Información y Comunicación constituyen actualmente, una herramienta estratégica para el desarrollo institucional global, y es precisamente de la importancia de su adecuada gestión y desempeño, de donde surge la necesidad de verificar que las políticas y procedimientos establecidos para su desarrollo, se lleven a cabo de manera oportuna y eficiente permitiendo un mejoramiento continuo.

La Superintendencia de Telecomunicaciones, SUPERTEL, consecuente con sus objetivos estratégicos institucionales se encuentra en una búsqueda continua, de fortalecimiento tecnológico, que brinde soporte efectivo a sus operaciones de control de los servicios de telecomunicaciones, y el uso del espectro radioeléctrico, para contribuir con el desarrollo del sector y del país.

La presente auditoría informática no ha tenido como fin detectar errores y señalar fallas, sino más bien ha sido un proceso que permitirá fortalecer debilidades y mejorar la aportación de las TICs a la consecución de los objetivos institucionales de la SUPERTEL, mediante recomendaciones y planes de acción emitidos con el objeto de que cada individuo y función de la institución opere de modo productivo y efectivo en sus actividades diarias.

Luego de haber realizado un estudio y análisis comparativo de las metodologías, normas, técnicas, y estándares que rigen los procesos de auditoría en la actualidad, además de examinar la legislación informática vigente en el Ecuador, se ha determinado como marco de referencia para la ejecución de la auditoría a COBIT(Control ObjectivesforInformation and relatedTecnology), por ser un estándar que asocia las mejores prácticas para el control de TI y para la implementación de Gobierno de TI; características que lo han posicionado como uno de los modelos más utilizados en el mundo por usuarios, directivos y auditores.

El proceso de auditoría inicia con un estudio exhaustivo del entorno a auditar, el cual ha permitido identificar las estructuras y procesos fundamentales de la SUPERTEL, así como también tener una visión completa de la Unidad de Tecnología de la Información.

El estudio preliminar ha permitido puntualizar un programa detallado fundamentado en la situación real, y definir una estrategia de auditoría adecuada que permita determinar el estado de los procesos, en base a tres dimensiones que incluyen desempeño, madurez y cumplimiento de objetivos de control de acuerdo a COBIT. Cada una de las dimensiones mencionadas, se sustentan bajo un modelo correspondiente que establece indicadores cuantitativos y/o cualitativos en base a la integración de un conjunto de matrices, que cubren cada uno de los aspectos considerados en el análisis.

Las matrices se encuentran estructuradas bajo treinta y cuatro objetivos de control determinados por COBIT. Cada matriz se determina a partir de la aplicación de diversas técnicas de auditoría que incluyen entre otros, procesos de observación, comparación, indagación, conciliación, revisión selectiva, y análisis. Posteriormente, las matrices se conjugan entre sí para determinar un indicador por cada dimensión, que conjuntamente con el indicador de impacto, permiten identificar la realidad de cada proceso, para finalmente proyectarse hacia un nivel de abstracción máximo que establece un calificador único del estado del proceso.

En el quinto capitulo, se encuentra el informe final, en el cual se ven reflejadas todas las fases de la auditoría detallando para cada uno de los procesos COBIT, la situación actual, el calificador global, los indicadores tridimensionales del proceso y el impacto que representa en la consecución de los objetivos institucionales; argumentos que han permitido emitir recomendaciones fundamentadas para mejorar cada uno de los procesos, y proyectar planes de acción para fortalecer las debilidades y optimizar el desarrollo de las TICs en la SUPERTEL.

CAPITULO 1

GENERALIDADES DE LA AUDITORÍA INFORMÁTICA

Hoy en día los sistemas de información constituyen herramientas indispensables para el desarrollo empresarial general. Las Tecnologías de Información y Comunicación (TICs) se involucran directamente con la gestión integral de la empresa, por esta razón deben estar sujetas a lineamientos, normas y estándares que vayan de acuerdo con las políticas empresariales. De la importancia del adecuado funcionamiento de las TICs en una institución surge la Auditoría Informática.

Muchos autores coinciden en que la auditoría informática (AI) nació como una extensión de la auditoría general, sus investigaciones y desarrollos se originaron a comienzos de la década de los 60, siendo en el año de 1977 cuando realmente la AI adquiere las características que la identifican actualmente, luego de publicarse la primera edición de SystemsAuditability and Control (SAC), un trabajo conjunto del Institute of InternalAuditors (IIA), IBM y Stanford ResearchInstitute (SRI). (Lorenzo Gil, n.d.).

1.1 Conceptos de Auditoría y Auditoría Informática

En muchas ocasiones se relaciona a la auditoría como una rendición de cuentas en donde el fin último sería detectar errores, sin embargo, el concepto de auditoría va más allá de eso, es un procedimiento periódico, que debe realizarse con el objeto de evaluar la eficacia y eficiencia de una institución o de parte de ella.

Hernández sostiene que la auditoría es un proceso necesario para las organizaciones con el fin de asegurar que todos sus activos sean protegidos en forma adecuada. En donde, la alta dirección espera que de estos procesos de auditoría surjan recomendaciones necesarias para la mejora continua de las funciones de la organización. (Hernández, 1997).

Existen otros autores como Kell y Ziegler que orientan el concepto de auditoría a la obtención de resultados que deberán ser comunicados a la parte interesada,

definen a la auditoría como un proceso para obtener y evaluar evidencias. (Kell, Ziegler, n.d.).

Los conceptos anteriores hacen referencia a la auditoría de manera general, de los cuales se derivan las definiciones actuales de auditoría informática.

Según Piattini en su obra Auditoria Informática: Un Enfoque Práctico, la auditoría en informática se orienta a la verificación y aseguramiento de que las políticas y procedimientos establecidos para el manejo y uso adecuado de la tecnología de la información en la organización, se lleven a cabo de una manera oportuna y eficiente. (Piattini, Del Peso, 2003).

La auditoría informática es un proceso necesario que debe ser realizado por personal especializado para garantizar que todos los recursos tecnológicos operen en un ambiente de seguridad y control eficientes, de manera que la entidad tenga la seguridad de que opera con información verídica, integral, exacta y confiable. Además la auditoría deberá contener observaciones y recomendaciones para el mejoramiento continuo de la tecnología de la información en la institución.

1.2 Objetivos de la Auditoría Informática

Piattini sostiene que la auditoria informática confirma la consecución de los objetivos tradicionales de la auditoria: objetivos de protección de activos e integridad de datos; y objetivos de gestión, que abarcan no solamente los de protección de activos, sino también los de eficacia y eficiencia. (Piattini, Del Peso, 2003).

Caridad Simon en sus apuntes de Auditoría Informática (2006, p.15) cita a Ron Weber (1982) quien separa los objetivos de la AI en cuatro grupos: objetivos de salvaguarda de bienes; objetivos de integridad de datos; objetivos de efectividad del sistema y objetivos de eficiencia del sistema.(Caridad Simon, 2006)

1.3 Bases de la Auditoría Informática

Serafín Caridad Simón (2006), en su obra Auditoría Informática, considera a la Auditoría Informática (AI) como la intersección de cuatro disciplinas: Auditoría Tradicional, Ciencias del Comportamiento, Gestión de Sistemas de Información e Informática. Eso se muestra en la Figura 1.1

Figura 1.*1* *A.I. como intersección de otras disciplinas. Basado en Caridad Simón, (2006, p.18).*

1.4 Funciones de la Auditoría Informática

Dentro del proceso de auditoría es importante asegurar que se cumplan por lo menos los principios básicos de un proceso formal. Los elementos indispensables para cumplir este requisito son: la planeación, el control y el seguimiento del desempeño, que deberán garantizar lo siguiente:(Apuntes de Auditoría Informática, 2009).

- Que los recursos de informática sean orientados al logro de los objetivos y las estrategias de las organizaciones.
- La elaboración, difusión y cumplimiento de las políticas, controles y procedimientos inherentes a la AI.
- Que se den los resultados esperados por la institución mediante la coordinación y apoyo reciproco con: auditoría, asesores externos, informática, y la alta dirección.

1.5 Importancia del Control y la Auditoría Informática

Caridad Simon en sus apuntes de Auditoría Informática hace referencia a algunos factores críticos que atentan al bien más preciado de una organización en la actualidad, la información. Estos factores son: coste de la pérdida de datos, toma de decisiones incorrecta, abuso informático, y privacidad de los datos (Caridad Simon, 2006).

1.6 Metodología de desarrollo de la Auditoría Informática

Kuna en su Tesis de Magister: “Asistente para la realización de Autoría de Sistemas en Organismos Públicos o Privados”, enuncia una metodología de desarrollo de AI muy general, que coincide con varias propuestas de diferentes autores. Se contemplan las siguientes fases:

Fase 1. Identificar el alcance y los objetivos de la Auditoría Informática
En esta fase se determinan los límites y el entorno en que se realizará la auditoría, debe existir un acuerdo muy preciso entre autoridades y auditores. El éxito del proceso depende de una clara definición de esta etapa. (Kuna, 2006).

Fase 2. Realizar el estudio inicial del entorno a auditar
En esta fase es necesario examinar las funciones y actividades generales de la organización a auditar y en particular de las relacionadas con las tecnologías de la información. Se debe definir el organigrama, los departamentos, las relaciones funcionales y jerárquicas entre las distintas áreas de la organización, el flujo de información, el número de puestos de trabajo y personas por puesto de trabajo, la estructura organizativa del departamento de informática, características de hardware y software, las metodologías de desarrollo y mantenimiento de aplicaciones, y aspectos relacionados con la seguridad. (Kuna, 2006).

Fase 3. Determinación de los recursos necesarios para realizar la auditoría informática
Después de realizar el estudio preliminar se debe determinar los recursos materiales y humanos necesarios para implementar el plan de auditoría. (Kuna, 2006).

Fase 4. Elaborar el plan de trabajo
En esta fase se define el calendario de actividades a realizar, formalizando el mismo para la aprobación por parte de las autoridades. (Kuna, 2006).

Fase 5. Realizar las actividades de auditoría
Es el momento donde se efectivizan las actividades planificadas en la fase anterior, aplicando distintas técnicas y utilizando herramientas que garanticen el cumplimiento de los objetivos planteados. (Kuna, 2006).

Fase 6. Realizar el informe final
"La elaboración del Informe Final es la única referencia constatable de toda auditoría, y el exponente de su calidad." (Kuna, 2006, p. 25).
Kuna presenta un modelo estándar de la estructura del informe final para cada proceso evaluado, en el cual intervienen: definición de objetivos, situación actual, tendencias, puntos débiles, amenazas y recomendaciones. (Kuna, 2006).

Fase 7. Carta de Presentación
Es la última etapa de la auditoría consta de un resumen del contenido del informe final, dirigido a las autoridades de la institución. (Kuna, 2006).

CAPITULO 2

ESTUDIO DE LA NORMATIVA EXISTENTE PARA AUDITORÍAS INFORMÁTICAS

2.1 Normas, Técnicas, Estándares y Procedimientos de Auditoría

Actualmente el desarrollo de una auditoría informática se basa en la aplicación de normas, técnicas, estándares y procedimientos que garanticen el éxito del proceso.

La gran mayoría de documentación existente coincide en que las normas de auditoría son requisitos mínimos de calidad, relativos a las cualidades del auditor, a los métodos y procedimientos aplicados en la auditoría, y a los resultados. (Aguirre, n.d.a).

Las técnicas en cambio, son todos aquellos métodos que permiten al auditor evidenciar y fundamentar sus opiniones y conclusiones. La Figura 2.1 resume las técnicas aplicables más comunes en el campo de la auditoría. (Secretaría de la Función Pública – México, 2003).

2.2 Organizaciones y Normas de AI más relevantes

Actualmente el Ecuador cuenta con un margo regulatorio y normativo reducido en materia informática, es por ello que se estudiarán las normas y organizaciones internacionales más relevantes en este ámbito. Las organizaciones más importantes son: *Institute of InternalAuditors (IIA), e InformationSystemAudit and Control Association (ISACA)*

Las organizaciones antes mencionadas, han desarrollado normas y estándares con el fin de establecer políticas y lineamientos que garanticen el proceso de auditoría. Algunos de los estándares más conocidos son:

- *COBIT:* Control Objectives for Information and related Technology. Desarrollado por InformationSystemsAudit and Control Association(ISACA). Centra su interés en la gobernabilidad, aseguramiento, control y auditoría para Tecnologías de la Información y Comunicación (TIC).

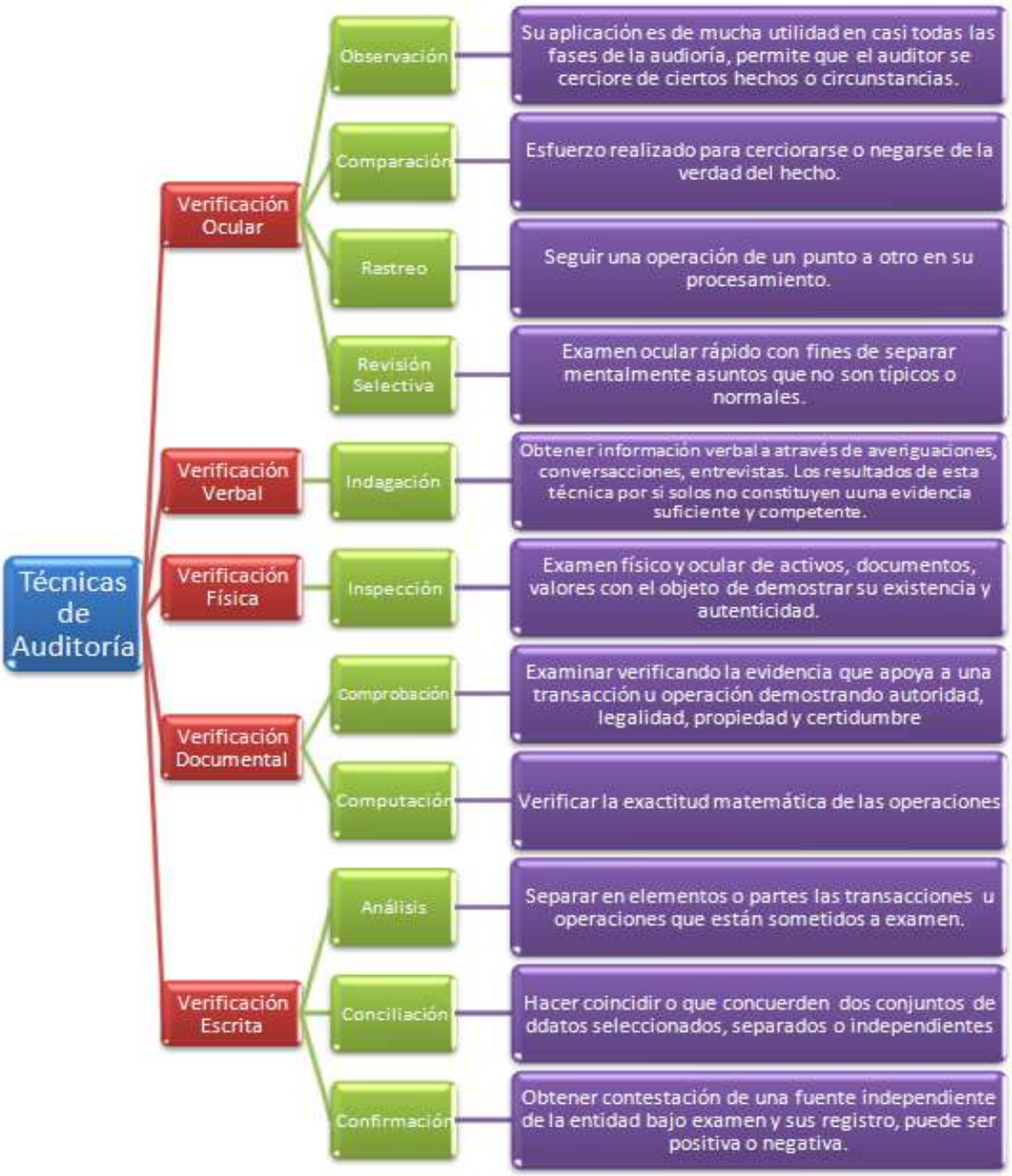

Figura 2.1*Técnicas de Auditoría.*

- *ITIL:*Information Technology Infrastructure Library. Recoge las mejores prácticas para administrar los servicios de Tecnología de la Información (TI).

- *COSO:*Committee of Sponsoring Organizations. Hace recomendaciones a los administradores de TI sobre cómo evaluar, informar e implementar sistemas de control, teniendo como objetivo la efectividad y eficiencia de las operaciones, la información financiera y el cumplimiento de las regulaciones, valoración de riesgos, actividades de control, información y comunicación y la verificación.

- *ISO Serie 27000:* Integra un conjunto de normas sobre Sistemas de Gestión de Seguridad de la Información (SGSI), que a través de su aplicación, permite administrar la información mediante el modelo Plan – Do – Check – Act(PDCA).

- *SAC:*SystemsAuditability and Control, ofrece una guía de estándares y controles a auditores internos sobre la forma de controlar y auditar los sistemas de información y tecnología

2.3Control Objetives for Information and Related Technology, COBIT

COBIT es uno de los estándares más utilizados actualmente, como base en la realización de una metodología de control interno en el ambiente de tecnología informática. COBIT es un marco de referencia y se fundamenta en los objetivos de control existentes de la InformationSystemsAudit and Control Foundation (ISACF), y se encuentra alineado con otros estándares de control y auditoria como COSO, IFAC, IIA, ISACA, AICPA[1]. Ver Figura 2.2.

El marco de referencia COBIT otorga especial importancia a los requerimientos de negocios en cuanto a efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad que deben ser satisfechos. El desarrollo de este marco de referencia ha sido limitado a objetivos de control de alto nivel en forma de necesidades de negocio dentro de un proceso de tecnología informática particular, cuyo logro es posible a través del establecimiento de controles, para el cual deben considerarse controles aplicables potenciales.

Figura 2.2*Orden procedimental de COBIT.*

Misión de COBIT. La misión COBIT es “Investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento”. (COBIT 4.1, 2007, p. 9).

Objetivos de Control. Un "Objetivo de Control", es una definición del resultado o propósito que se desea alcanzar implementando procedimientos de control específicos dentro de una actividad de tecnología informática. COBIT identifica un conjunto de 34 Objetivos de Control de alto nivel, uno para cada uno de los

[1] COSO, Comité de Organizaciones Patrocinadoras (*TreadwayCommission*).
IFAC, Federación Internacional de Contadores.
IIA, Instituto de Auditores Internos.
ISACA, Asociación de Auditoría y Control de Sistemas de Información.
AICPA, Instituto Americano de Contadores Públicos.

procesos de tecnología informática, agrupados en cuatro dominios: planeación y organización, adquisición e implementación, entrega (de servicio) y monitoreo.

Usuarios de COBIT. COBIT proporciona ventajas a gerentes, usuarios, e interventores, como se muestra en la Figura 2.3 Los gerentes se benefician de COBIT porque les provee un fundamento sobre el cual basar las decisiones. La toma de decisiones es más eficaz porque COBIT ayuda en la definición de un plan de TI estratégico, la definición de la arquitectura de la información, la adquisición del hardware necesario y el software para ejecutar una estrategia, la aseguración del servicio continuo, y la supervisión del funcionamiento del sistema TI. Los usuarios se benefician de COBIT debido al aseguramiento proporcionado a ellos en el tratamiento de la información. Finalmente los auditores o interventores se ven beneficiados porque COBIT permite identificar cuestiones de control de TI dentro de la infraestructura de una institución y a corroborar sus conclusiones de auditoría. (COBIT 4.1, 2007)

Figura 2.3*Usuarios COBIT.*

Modelo del Marco de Trabajo de COBIT

El marco de trabajo COBIT, relaciona los requerimientos de información y de gobierno TI a los objetivos de la función de servicios de TI. El modelo de procesos de COBIT permite que las actividades de TI y los recursos que los soportan sean administrados y controlados basados en los objetivos de control de COBIT, y alineados y monitoreados usando las metas y métricas de COBIT, como se ilustra en la Figura 2.4.

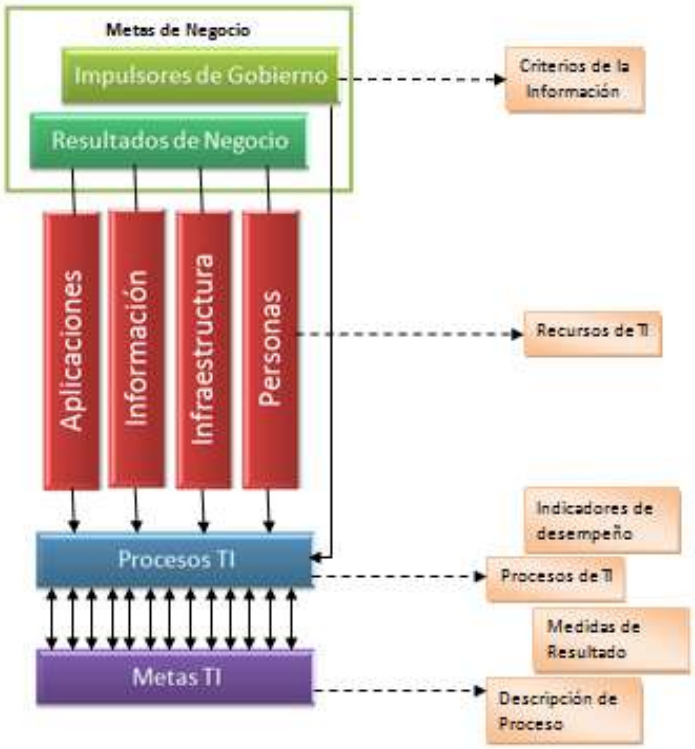

Figura 2.4*COBIT Gestión, Control, Alineamiento y Monitoreo. (COBIT 4.1, 2007, p. 24)*

Los recursos de TI son manejados por procesos de TI para lograr metas de TI que respondan a los requerimientos del negocio. Este es el principio básico del marco de trabajo COBIT, como se ilustra en el cubo COBIT, Figura 2.5.

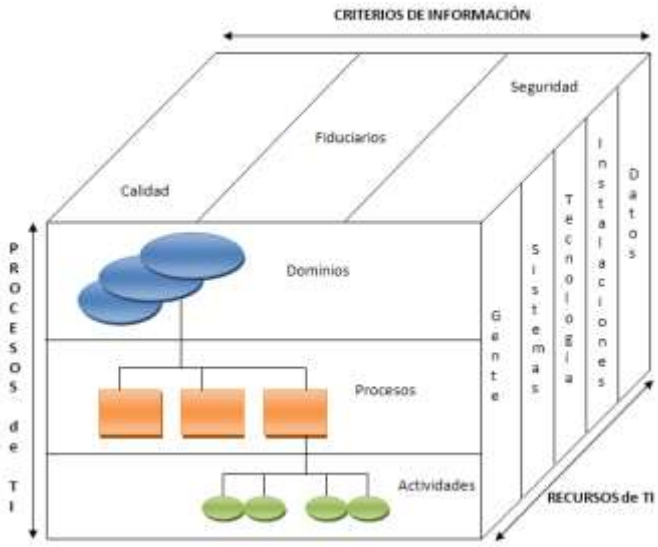

Figura 2.5*El Cubo de COBIT. (COBIT 4.1, 2007, pag. 25)*

*Criterios de Información.*Para alcanzar los requerimientos de negocio, la información necesita satisfacer ciertos criterios:

Requerimientos de Calidad: Calidad, costo y entrega.

Requerimientos Fiduciarios (COSO): Efectividad y eficiencia operacional, confiabilidad de los reportes financieros y cumplimiento de leyes y regulaciones.

Requerimientos de Seguridad: Confidencialidad, integridad y disponibilidad

*Recursos de TI.*En COBIT se establecen los siguientes recursos en TI necesarios para alcanzar los objetivos de negocio:datos, instalaciones, tecnología, sistemas, y recurso humano.

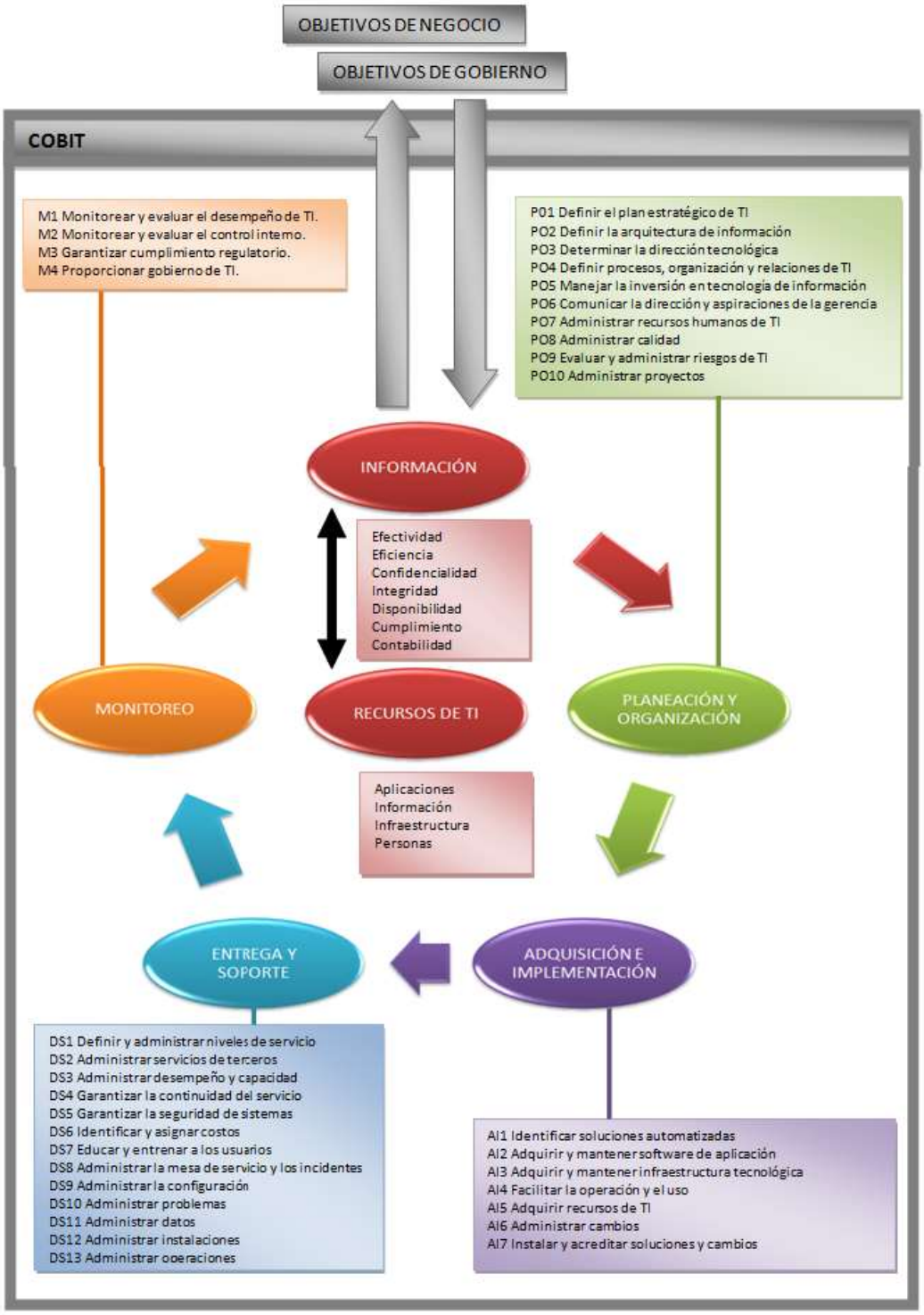

Figura 2.6 *Marco de Trabajo Completo de COBIT.* (COBIT 4.1, 2007, p. 26)

*Procesos de TI.*COBIT se divide en tres niveles:

Dominios: Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.

Procesos: Conjuntos o series de actividades unidas con delimitación o cortes de control.
Actividades: Acciones requeridas para lograr un resultado medible.

En detalle, el marco de trabajo general COBIT se muestra gráficamente en la Figura 2.6, 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.

2.4 Information Technology Infraestructure Library, ITIL

ITIL es un conjunto de las mejores prácticas para la gestión de servicios de TI que ha evolucionado desde 1987, comenzó como un conjunto de procesos que utilizaba el Gobierno Británico para mejorar la gestión de los servicios de TI. (Ramírez, 2006).

ITIL incluye cinco disciplinas que proporcionan a las empresas flexibilidad y estabilidad para ofrecer servicios de TI, estas son: Gestión de incidencias, Gestión de problemas, Gestión de cambios, Gestión de versiones, y Gestión de configuración. Incluye también cinco disciplinas que soportan los servicios TI de calidad y bajo costo de las empresas, estas son: Gestión del nivel de servicio, Gestión de la disponibilidad, Gestión de la capacidad, Gestión financiera para servicios TI, y Gestión de la continuidad de los servicios TI. (Cruz, 2009).

La versión 2.0 de ITIL mostrada en la Figura 2.7, tiene como una de sus metas principales alinear los objetivos de los servicios de la infraestructura de TI a los objetivos del negocio.Los servicios de TI no serían posibles sin su correspondiente soporte, ITIL trata de hacer una revisión y corrección de los procesos, de realizar una documentación apropiada para que de esta manera la información permita brindar un adecuado soporte a estos servicios.

Figura 2.7 *ITIL Versión 2. (Cruz, 2009, p. 28)*

ITIL versión 2.0 sugiere para la gestión de servicios de TI, utilizar los libros de Entrega y Soporte de Servicios mediante un modelo de gestión de procesos que se muestra en la Figura 2.8.

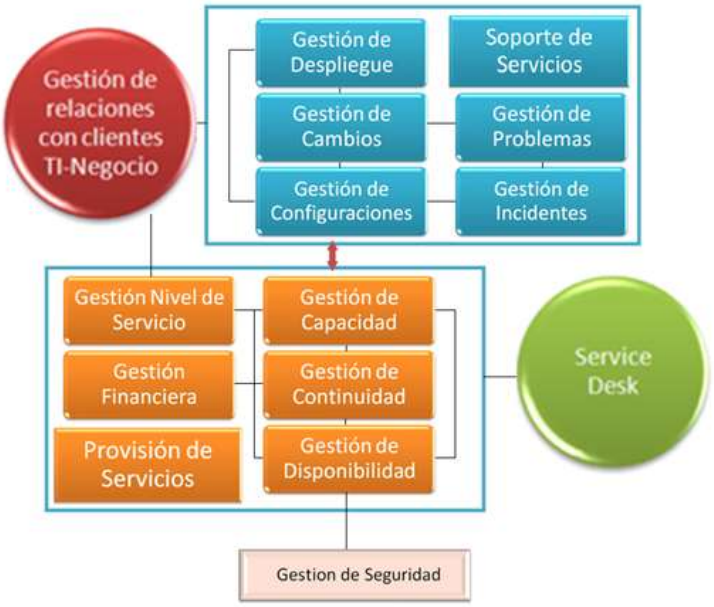

Figura 2.8*Modelo de Gestión de Servicios.*
(The ITIL fundation exam study guide 3rd edition citadopor Cruz, 2009, p. 30)

Gestión de Incidentes: Propone recuperar la operación de los servicios en el menor tiempo posible de manera que no se propicie una baja en los niveles de calidad y disponibilidad, minimizando así el impacto desfavorable a las operaciones de la institución. Los incidentes tanto de hardware como software son atendidos por el proceso de gestión de incidentes que requiere la detección del incidente, su registro, clasificación, soporte, investigación, diagnóstico, resolución, recuperación y cierre, finalmente es necesaria la asignación, supervisión, seguimiento y comunicación del proceso. El ciclo de vida de un incidente se muestra en la Figura 2.9.(ITIL V2.0)

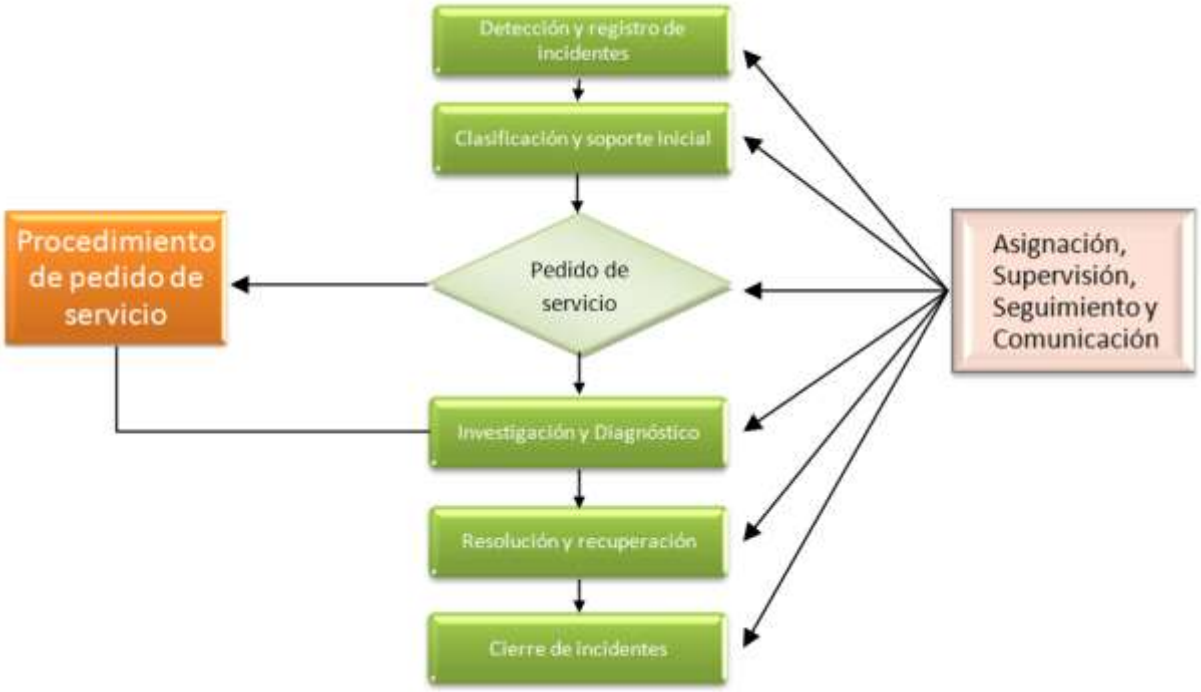

Figura 2.9 *Ciclo de vida de un incidente.*
(ITIL V2.0. Service Support, Incident Management citadopor Cruz, 2009, p. 31)

Gestión de Problemas: Intenta prevenir la abundancia de problemas e incidentes producidos por errores de la infraestructura de TI, encontrando sus causas, dándoles tratamiento e implementando sus soluciones. A diferencia de la gestión de incidentes que busca una solución temporal e inmediata, la gestión de problemas intenta hallar una solución permanente cuyo objetivo principal es identificar la causa raíz del incidente, darle solución y prevenirlo.El control de problemas trata de trasformar problemas en errores conocidos, mientras que el control de errores trata de resolver errores conocidos a partir del control de cambios como se muestra en la Figura 2.10. (ITIL V2.0)

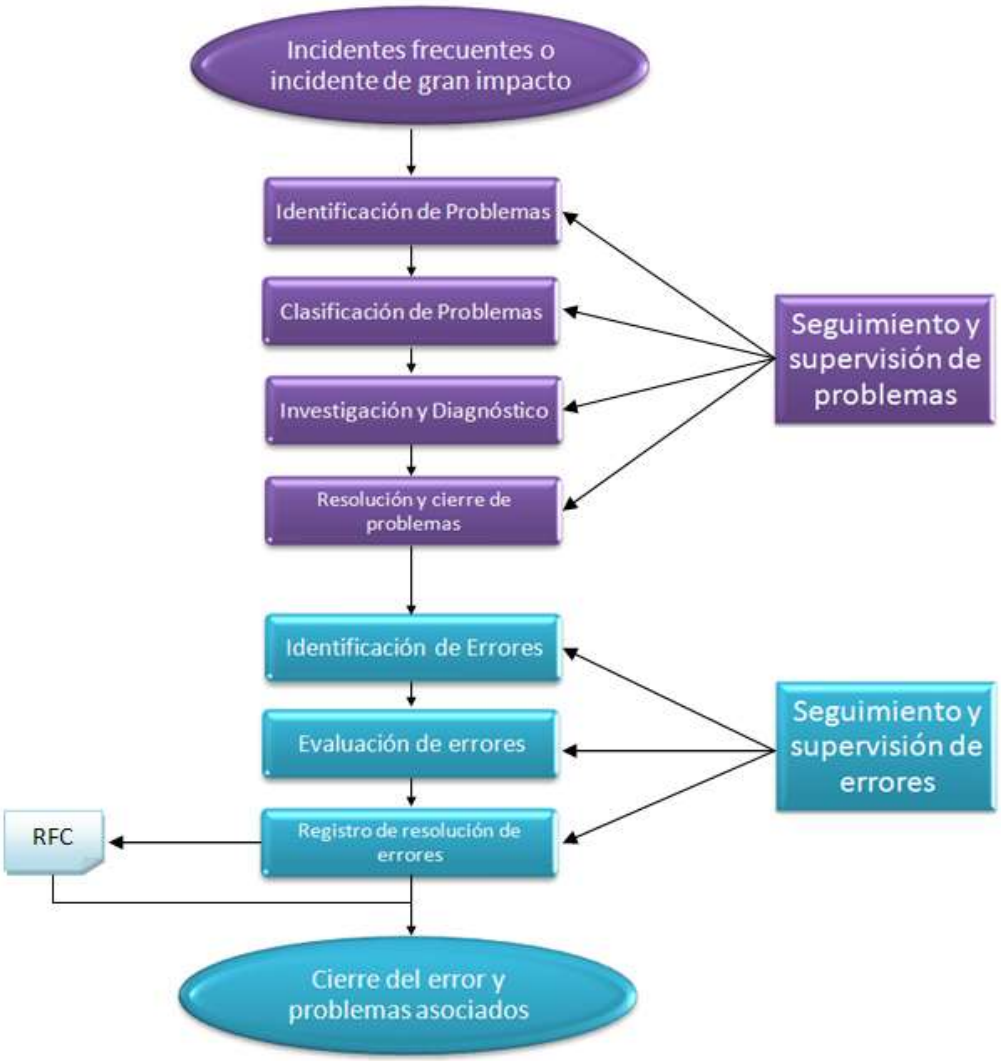

Figura 2.10 *Control de problemas y errores.*
(ITIL V2.0.Service Support, Problem Management citadopor Cruz, 2009, p. 32)

Gestión de la Configuración: Pretende proveer la información y documentación que permita que se conozcan todos los bienes de la infraestructura de TI, su software, configuraciones y servicios, de manera que proporcione una base sólida para la gestión de incidentes, problemas, cambios y versiones. Para facilitar el manejo de esta información debe existir una base de datos de configuración, Configuration Management Database (CMDB). La CMDB está íntimamente relacionada con otros procesos, como se detalla en la Figura 2.11, pues proporciona información que está relacionada con la mejora de la gestión de los mismos.(ITIL V2.0)

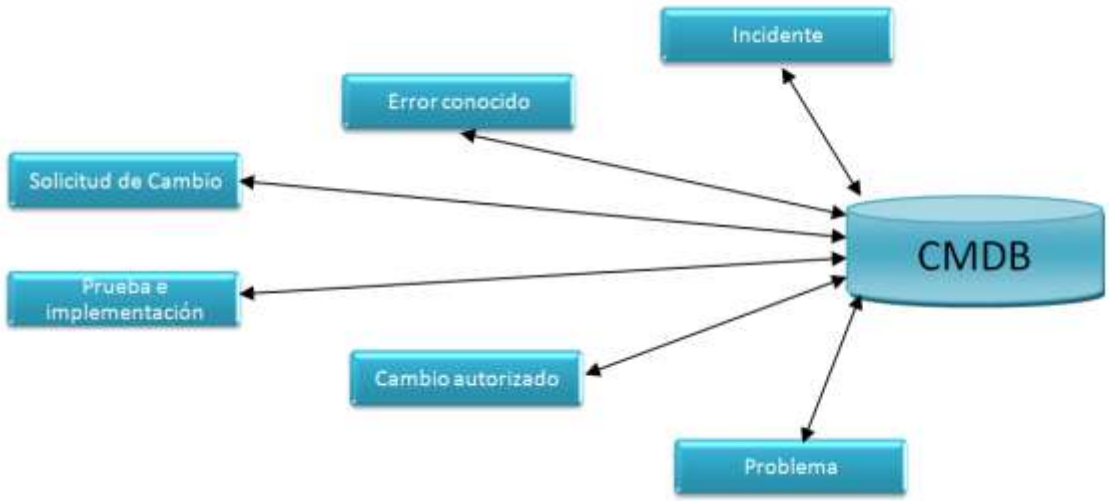

Figura 2.11*Relación con otros procesos.*
(ITIL V2.0. Service Support, Configuration Management, citadopor Cruz, 2009, p. 34)

Gestión de Cambios: Aspira brindar garantía en los métodos y procedimientos que se utilizan a la hora de realizar cambios, permite minimizar el impacto que producen los incidentes y problemas en la infraestructura, relacionados con cambios en las operaciones de la institución, en su búsqueda de beneficios, reducción de costos o mejora del servicio. Para tener una buena gestión de cambios es necesario tomar en cuenta la evaluación del riesgo, la continuidad del negocio, los requerimientos de recursos y su aprobación. El procedimiento genérico de cambio se muestra en la Figura 2.12.(ITIL V2.0)

Figura 2.12*Procedimiento de cambio.*
(ITIL V2.0. Service Support, Change Management citadopor Cruz, 2009, p. 35)

Gestión de Versiones: Su función es proteger el ambiente de producción y servicios, cuidando del software, hardware y los elementos relacionados, asegurando que estén en uso solamente las versiones correctas, probadas y autorizadas, garantizando que los componentes utilizados en determinado lugar sean los adecuados y estén disponibles en el momento oportuno.
La gestión de versiones incluye un escenario de planificación, uno de preparación, uno de pruebas y uno de construcción y distribución. Durante éste último escenario, los registros de la gestión de configuraciones deben ser actualizados para asegurar versiones confiables que puedan ser revertidas en caso de problemas, es claro entonces que intervienen directamente la base de datos de configuraciones (CMDB), la Librería de Software definitivo, Definitive Software Library (DSL) y el

depósito de hardware definitivo, Definitive Hardware Store (DHS), como se muestra en la Figura 2.13.(ITIL V2.0)

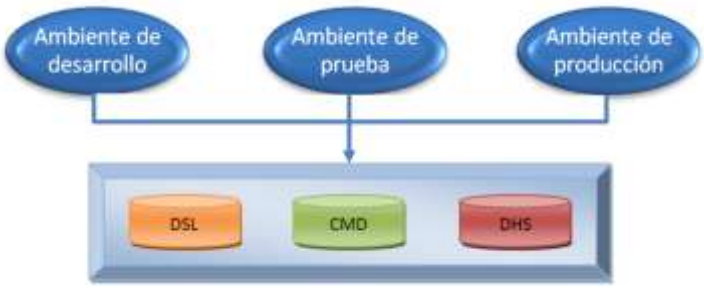

Figura 2.13*Ambientes Principales de Gestión de Versiones.*
(ITIL V2.0. Service Support, Release Management citadopor Cruz, 2009, p. 36)

Gestión de Niveles de Servicios: Pretende mantener y mejorar la calidad de los servicios de TI. La gestión del nivel de servicio plantea las necesidades de los clientes, las traslada a una planificación de la operación, alcance y funcionamiento, hace una negociación concisa con respecto a lo requerido, en los estándares de calidad solicitados, posteriormente realiza el monitoreo e informes de los logros del servicio que serán medidos a través de indicadores convenientes y finalmente se busca mantener los SLA's(*ServiceLevelAgreement*) que aseguren la satisfacción de todos los implicados. (Figura 2.14).(ITIL V2.0)

Figura 2.14*Alcance de los SLA's.*
(ITIL V2.0. ServiceDelivery, ServiceLevel Management citado por Cruz, 2009, p. 37)

Gestión Financiera: Su misión es proveer información de los costos de los activos de TI y de los recursos que colaboran con la provisión de los servicios cuando la organización es pequeña, mientras que debe proveer la contabilidad de todos los gastos de los servicios de TI y asistir en la decisiones de inversión en lo que a recursos tecnológicos se refiere, en caso de tratarse de una organización grande. Para una organización los servicios de TI significan casi siempre un punto crítico, ya que los costos que genera ésta área en ocasiones no parecen justificar el dinero gastado, pues su valor resulta ser no tan evidente. (Figura 2.15).(ITIL V2.0)

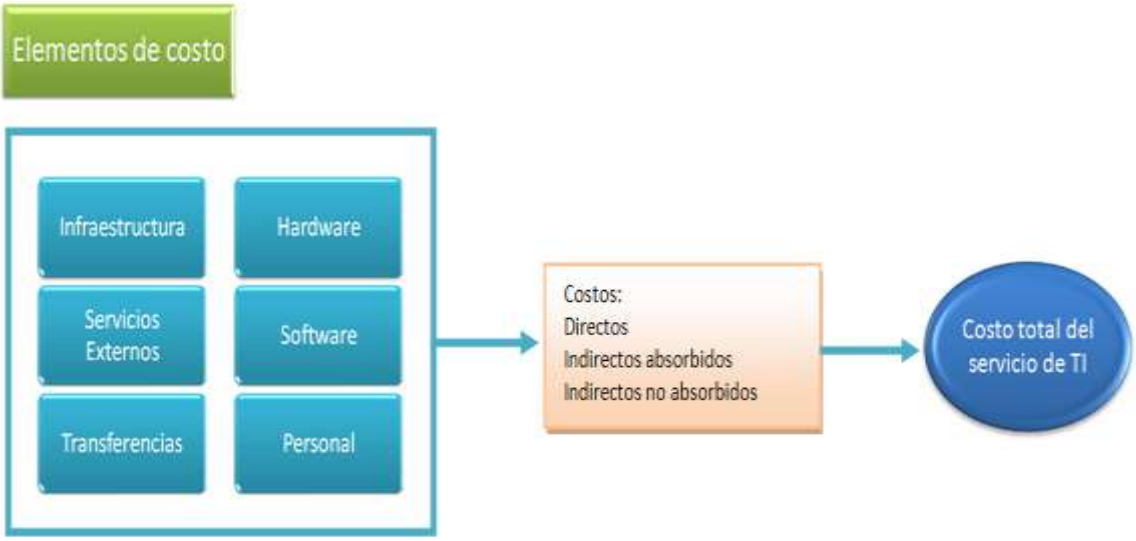

Figura 2.15*Modelo de costos "Por Servicio".*
(ITIL V2.0. ServiceDelivery, Financial Management citado por Cruz, 2009, p. 38)

Gestión de Capacidad: Su propósito es determinar y asegurar que la capacidad actual de la infraestructura de TI sea provista oportunamente, a un costo eficiente y con los aspectos de rendimiento requeridos por la institución.

El proceso de gestión de la capacidad como se muestra en la Figura 2.16, comprende un monitoreo continuo que garantice la utilización óptima de los recursos, el cumplimiento de los SLA's y los volúmenes de negocio esperados; un análisis de los datos con el fin de identificar condiciones de excepción, tendencias y predicciones en cuanto al uso de los recursos; un ajuste basado en la localización de las áreas y servicios que requieren perfeccionar su rendimiento; y la implementación que introduce los cambios y mejoras descubiertos en el ambiente operacional.

Todos los datos relacionados con esta gestión se almacenan en la Base de Datos de la Capacidad (CDB) en la que se guarda información técnica, de negocios, servicios, finanzas y estadísticas de utilización, la que contribuye con generación de pronósticos de capacidad y la planificación de requerimientos futuros. (ITIL V2.0)

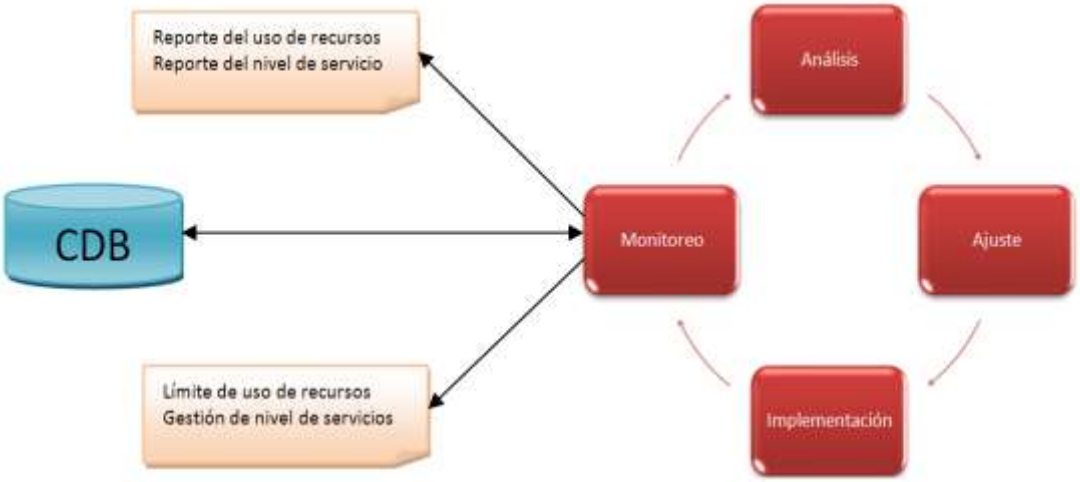

Figura 2.16*Proceso de Gestión de la Capacidad.*
(ITIL V2.0.ServiceDelivery, Capacity Management citadopor Cruz, 2009, p. 39)

Gestión de Continuidad del Servicio: Procura asegurar que los servicios de TI requeridos sean recuperados en los tiempos negociados y con la calidad acordada. Es necesario medir el nivel de dependencia tecnológica que tiene la organización, conocer los servicios otorgados, y la actitud de la institución frente a riesgos.

Se debe identificar los procesos críticos, los riesgos, las medidas que los reduzcan y los mecanismos de recuperación de los servicios. En la gestión de riesgos se trata de identificar los activos que son componentes de TI que soportan los procesos del negocio, las amenazas que son la acción o evento que pone en riesgo el funcionamiento de los procesos, la vulnerabilidad que es la debilidad interna que puede producir fallas al estar expuesta a amenazas, las contramedidas que son el control efectivo de costos para reducir riesgos excedentes y sus relaciones que se pueden apreciar en la Figura 2.17.(ITIL V2.0)

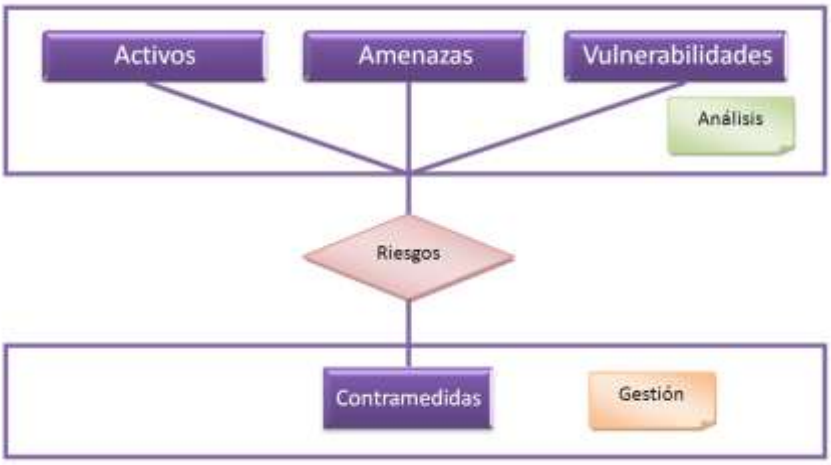

Figura 2.17*Evaluación de riesgos.*
(ITIL V2.0. Service Delivery, IT Service Continuity Management citadopor Cruz, 2009, p. 41)

Gestión de Disponibilidad: Trata de planificar, medir, supervisar y mejorar de forma continua los niveles de servicio y soporte que permitan la disponibilidad que la institución pretende obtener de la infraestructura de TI, para llegar a satisfacer sus requerimientos.

En el proceso de gestión de disponibilidad, es necesario tener claros los requerimientos de disponibilidad del negocio, hacer una evaluación del impacto de los mismos, comprender los requerimientos de disponibilidad, confiabilidad y mantenimiento de las TI, tener datos de los incidentes, problemas y SLA's, con el propósito de diseñar un plan basado en criterios que permitan cumplir los objetivos de disponibilidad establecidos y la capacidad de recuperarse frente a fallos. (Figura 2.18).(ITIL V2.0)

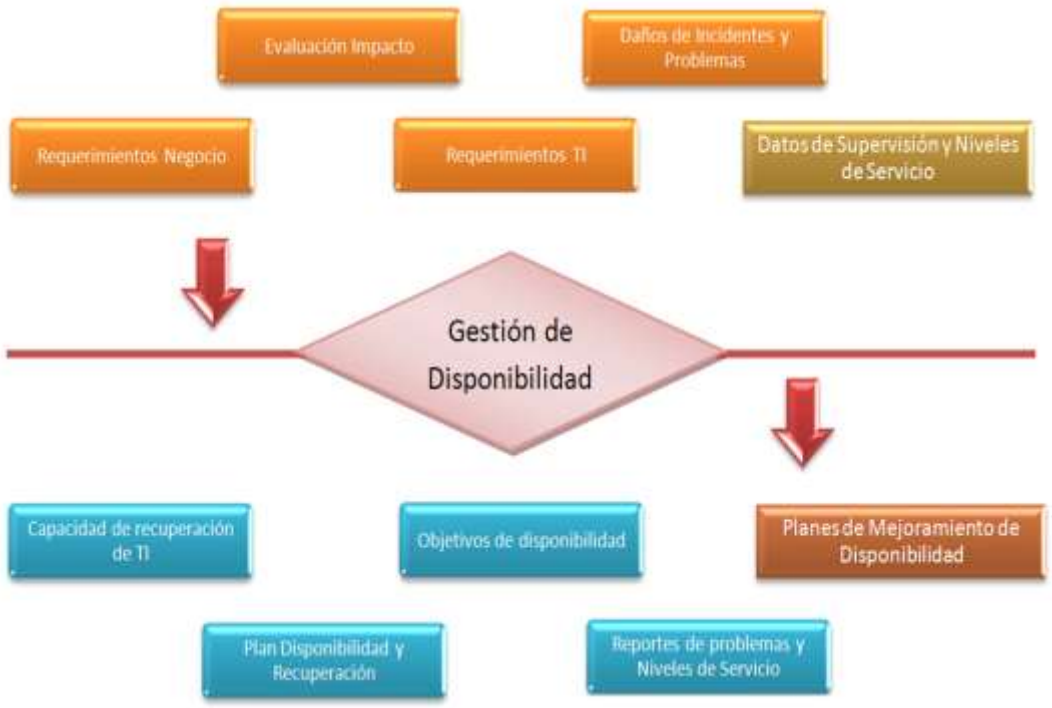

Figura 2.18*Proceso de gestión de Disponibilidad.*
(ITIL V2.0. Service Delivery, Availability Management citadopor Cruz, 2009, p. 42)

Gestión de Seguridad: Su propósito es proveer un nivel de seguridad apropiado para un servicio que incluye la reacción a incidentes provocados por eventos de inseguridad. La gestión de seguridad intenta controlar la provisión de información de los procesos del negocio y prevenir su uso sin autorización, de forma que se proteja el valor de la información relacionada con hardware, software, documentación y procedimientos, esta validez, como se muestra en la Figura 2.19, se mide en términos de confidencialidad que cerciora que la información sea accedida solo por quien debe, integridad que garantiza que la información sea exacta, total y correcta, y disponibilidad que asegura que la información y servicios estén a disposición del usuario.(ITIL V2.0)

Figura 2.19*Aspectos para gestión de seguridad.*
(Mafla – Apuntes de Seguridad en Redes, citado por Cruz, 2009, p. 43)

La versión 3.0 de ITIL fortalece la visión del negocio y está orientada al ciclo de vida del servicio, asegurando calidad en los servicios, integrando más estrechamente las estrategias de servicio comerciales y las de TI, proporcionando modelos de transición de acuerdo a la utilidad, describiendo la provisión de servicios y la búsqueda de los mismos, facilitando la implementación y administración de

servicios en un entorno variable, mejorando la medición y demostración del valor, identificando disparadores para la mejora del servicio y tratando las insuficiencias surgidas en la versión anterior. (ITIL V3.0, ServiceStrategy citado por Cruz, 2009)

Ciclo de vida del servicio: El ciclo de vida del servicio está basado en la arquitectura de ITIL, en este diagrama no existe punto de partida porque puede ser inusual que una organización inicie desde cero, además que tampoco existe un punto de salida fácil de la rueda, debido a que el trayecto nunca termina. El diagrama del ciclo se muestra en la Figura 2.20.

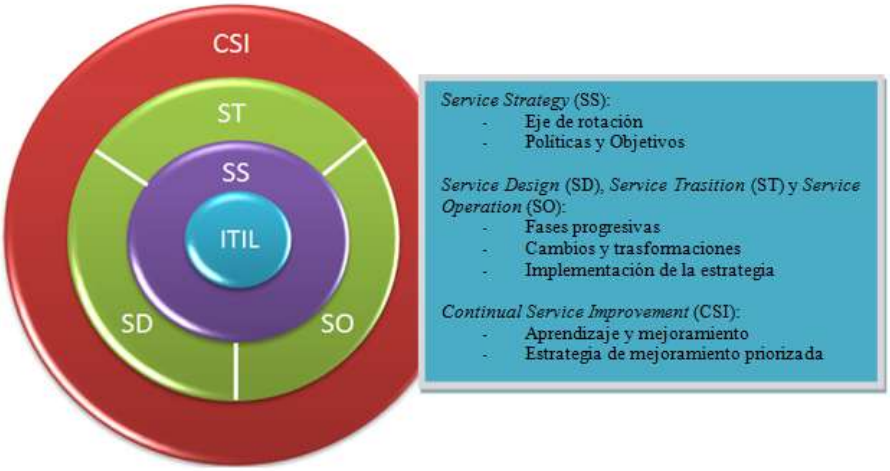

Figura 2.20*Diagrama de la Rueda. (ITIL V3.0. ServiceStrategy, citado por Cruz, 2009, p. 53)*

ITIL versión 3.0 crea una integración de procesos de TI, personas y herramientas dentro de la estrategia de negocios a través de los servicios de TI. Su estructura describe cómo los procesos están conectados, determina su comportamiento, organiza la infraestructura diseñada para un rendimiento sustentable, como se muestra en la Figura 2.21.

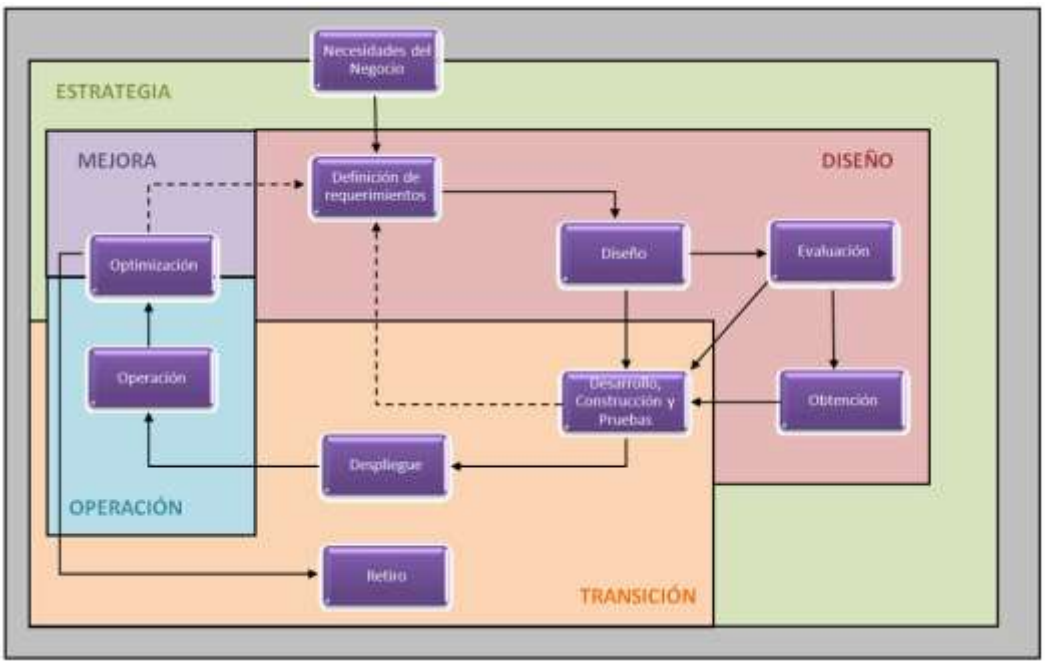

Figura 2.21*ITIL versión 3.0. (Cruz, 2009, p.54)*

2.5 COSO, Committee Of Sponsoring Organizations Of The Treadway Commission

COSO Report o COSO I fue un informe sobre control interno elaborado en 1992 por el Committee of SponsoringOrganizations of theTreadwayCommission de los EEUU., con el objetivo fundamental de especificar un marco conceptual de control interno de las organizaciones, capaz de integrar las diferentes políticas y lineamientos que permitan a la alta dirección mejorar sus sistemas de control interno. De acuerdo a COSO I, el control interno se basa en los siguientes componentes: ambiente de control, evaluación de riesgos, actividades de control, información y comunicación, y supervisión.

El COSO II O COSO ERM (Enterprise Risk Management) fue formulado en el 2004, su enfoque es el mismo que el de COSO Report pero basado en el riesgo.

Este nuevo enfoque no sustituye el marco de control interno, sino que lo incorpora como parte de él, permitiendo a las organizaciones mejorar sus prácticas de control interno o decidir encaminarse hacia un proceso más completo de gestión de riesgo.

Marco del Control Interno (COSO-ERM: La definición del marco del control interno se entiende como el proceso que ejecuta la administración con el fin de evaluar operaciones específicas con seguridad razonable en tres principales categorías: Efectividad y eficiencia operacional, confiabilidad de la información financiera y cumplimiento de políticas, leyes y normas. (COSO, 2004)

La comprensión del control interno puede así ayudar a cualquier entidad pública o privada a obtener logros significativos en su desempeño con eficiencia, eficacia y economía, indicadores indispensables para el análisis, toma de decisiones y cumplimiento de metas. (COSO, 2004)

El marco integrado de control que plantea el COSO-ERM consta de ocho componentes interrelacionados, derivados del estilo de la dirección, e integrados al proceso de gestión, siendo estos componentes siguientes: ambiente interno, establecimiento de objetivos, identificación de eventos, evaluación de riesgos, respuesta al riesgo, actividades de control, información y comunicación, y supervisión.

La gestión de riesgos empresariales no constituye estrictamente un proceso en serie, donde cada componente afecta sólo al siguiente, sino un proceso multidireccional e iterativo en que casi cualquier componente puede influir en otro.

Existe también una relación directa entre los objetivos y los ocho componentes referenciados, la que se manifiesta permanentemente en el campo de la gestión: las unidades operativas y cada agente de la organización conforman secuencialmente un esquema orientado a los resultados que se buscan. Un cadro de las componentes se muestra en la Figura 2.22(COSO, 2004)

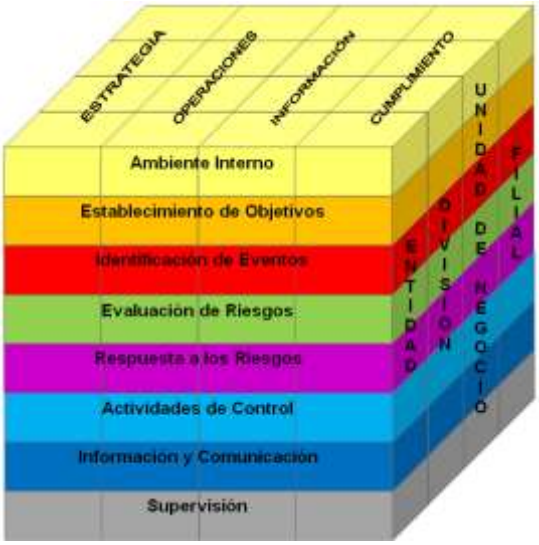

Figura 2.22*Componentes de COSO-ERM. (NASAudit, 2009, p. 2)*

Debe existir una circulación multidireccional de la información: ascendente, descendente y transversal, además de líneas abiertas de comunicación y una clara voluntad de escuchar por parte de los directivos. La Figura 2.23 Expone los flujos de información entre actividades inherentes a la gestión de riesgos empresariales de forma conceptual.

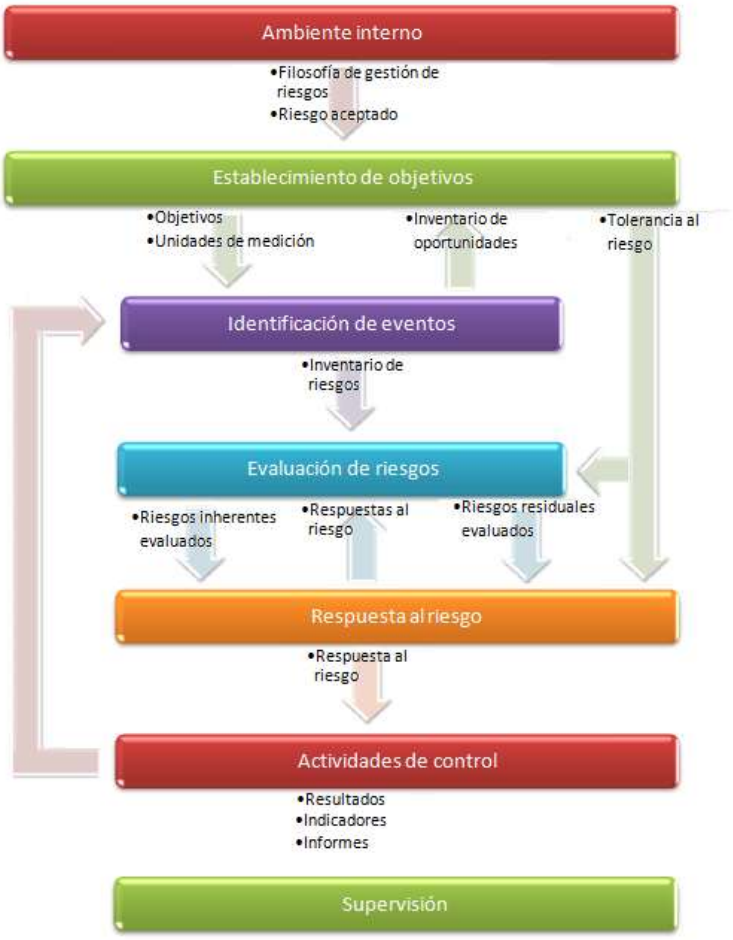

Figura 2.23*Flujos de Información ERM. (COSO, 2004, p. 87).*

2.6 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, MAGERIT

El método MAGERIT tiene un doble objetivo, primero estudiar los riesgos que soporta un determinado sistema de información y el entorno asociable con él, entendiendo por *riesgo* la posibilidad de que suceda un daño o perjuicio; y segundo recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados.MAGERIT, como método de análisis y gestión de riesgos, cubre sólo una fase de la gestión global de la seguridad de un sistema de información determinado. La gestión global de seguridad, representada en la Figura 2.24, es una acción permanente, cíclica y recurrente.(MARGERIT 1.0, n.d.)

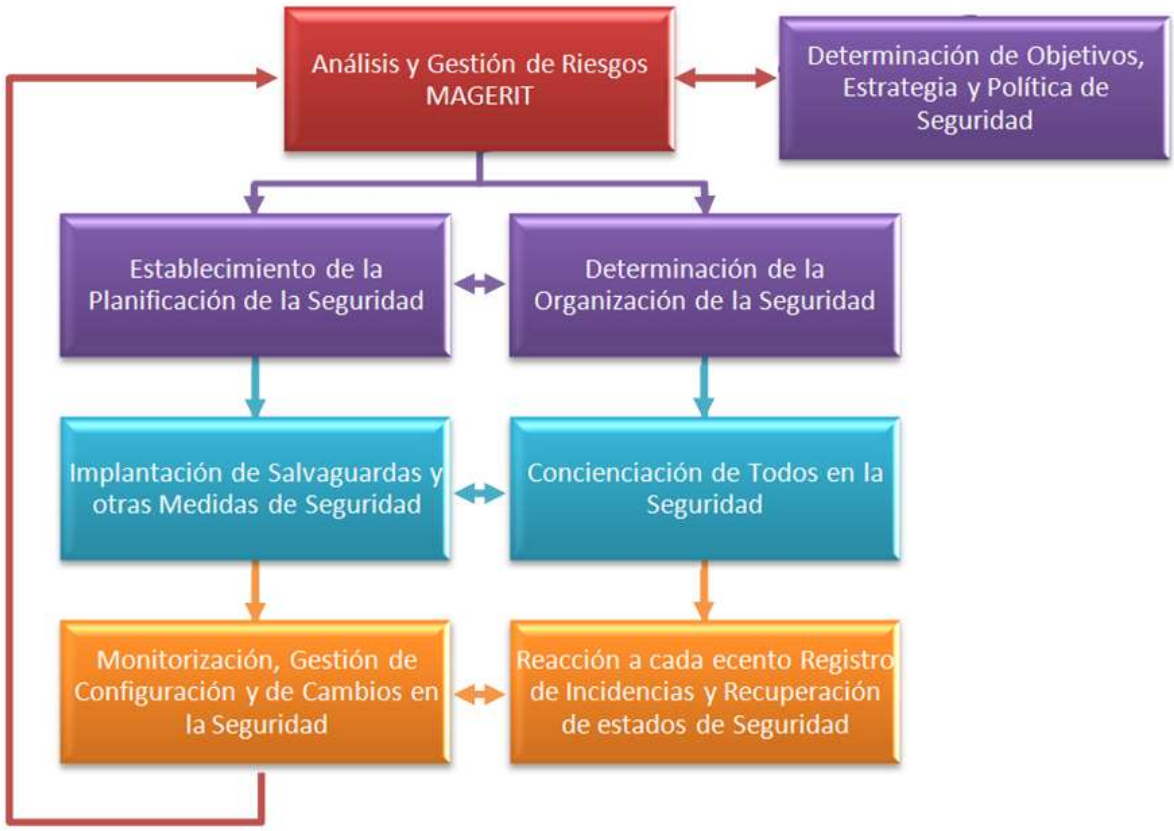

Figura 2.24*Análisis y Gestión de Riesgos MAGERIT.* (MARGERIT 1.0, n.d., p. 6)

MAGERIT maneja una visión estratégica global sobre la Seguridad de los Sistemas de Información de las Administraciones Públicas; visión que arranca de un Modelo de Análisis y Gestión de Riesgos que comprende 3 submodelos:Submodelo de elementos, eventos y de procesos. Ver Figura 2.25.

2.7 Normas ISO

ISO/IEC 27000. Las normas ISO/IEC 27000 constituyen una familia de estándares, desarrolladas por la International OrganizationforStandardization (ISO) y por la *International ElectrotechnicalCommission*(IEC). Esta familia de estándares se publicó ante la necesidad de contar con una base para la gestión de la seguridad de la información, especificando los requisitos para establecer, implementar,

controlar, mantener e innovar un Sistema de Gestión de Seguridad de la Información (SGSI). La serie ISO 27000 está formada por varias normas. Son consideradas como normas base: ISO 27001 e ISO 27002, mientras que las normas complementarias son principalmente: ISO 27003, ISO 27004, e ISO 27005.

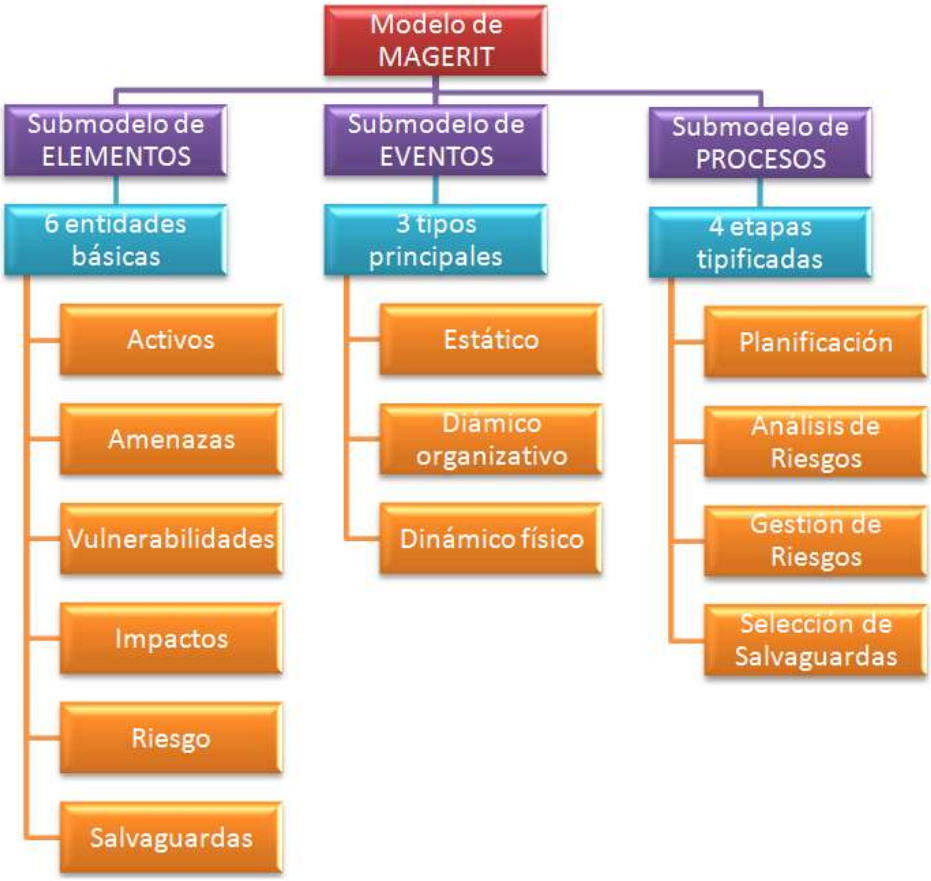

Figura 2.25 *Modelo MAGERIT.*(MARGERIT 1.0, n.d., p. 11)

ISO/IEC 20000. Proviene del estándar británico BS 15000. Es el primer estándar específico para la Gestión de Servicios de TI, y su objetivo es aportar los requisitos necesarios, dentro del marco de un sistema completo e integrado, que permita que una organización provea servicios TI gestionados, de calidad y que satisfagan los requisitos de la entidad. La norma ISO/IEC 20000 está estructurada en dos documentos:

ISO/IEC 20000-1: Este documento de la norma incluye el conjunto de los "requisitos obligatorios" que debe cumplir el proveedor de servicios TI, para realizar una gestión eficaz de los servicios que responda a las necesidades de las empresas y sus clientes.

ISO/IEC 20000-2: Esta parte contiene un código de prácticas para la gestión de servicios que trata cada uno de los elementos contemplados en la parte 1 analizando y aclarando su contenido. En síntesis este documento pretende ayudar a las organizaciones a establecer los procesos de forma que cumplan con los objetivos de la parte 1.

Figura 2.26 Ámbito de actuación de la norma ISO/IEC 20000. (Pérez, n.d., p. 1).

La norma ISO/IEC 20000 cubre las siguientes secciones:sistema de gestión de servicios TI, planificación e implementación de la gestión del servicio, planificación e implementación de servicios, nuevos o modificados, procesos de provisión de servicio, procesos de relaciones, procesos de resolución, procesos de control, y procesos de entrega. Eso se muestra en la Figura 2.27

Figura 2.27*Marco de referencia ISO/IEC 20000.* (Pérez, n.d.).

2.8Modelos de Madurez

Cada vez con más frecuencia, se requiere que las entidades corporativas y públicas empleen herramientas de evaluación hacia la administración de TI con el fin de obtener una medición relativa de donde se encuentra la organización; una manera de decidir hacia dónde ir de forma eficiente; y una herramienta para medir el avance contra la meta.

Modelo de Madurez de COBIT

El modelo de madurez genérico de COBIT consta de6 niveles:(COBIT 4.1, 2007)

- *0 No existente:* Carencia completa de cualquier proceso reconocible.
- *1 Inicial:* Existe evidencia que la entidad ha reconocido que los problemas existen y requieren ser resueltos.
- *2 Repetible:* Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea.
- *3 Definido:* Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento.
- *4 Administrado:* Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva.
- *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.

CapabilityMaturityModel, CMM

El Modelo de Madurez de Capacidades es un modelo de referencia para la aplicación de conceptos de gestión de procesos y de mejora de calidad en el desarrollo y mantenimiento de software. Según este modelo, la madurez de los procesos de desarrollo de software en una organización pasa por 5 niveles: primero o inicial, en que los procesos son inmaduros, no han sido medidos ni controlados nunca; segundo o repetible, centrado en la administración de proyectos, tercero o definido, que se fija en el proceso de ingeniería, cuarto o gestionado (o controlado) en el cual se mejora la calidad del producto y del proceso y quinto u optimizado, llegados a este punto la mejora de los procesos es continuo. Esto se muestra en la Figura 2.28 (SEI-CMM citado por Chacón, 2004)

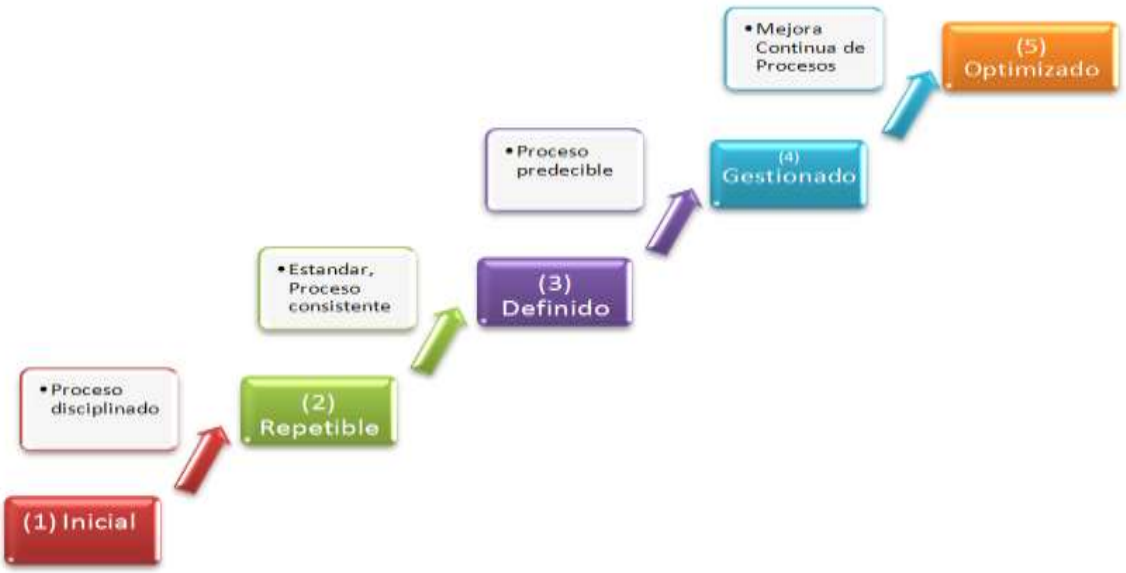

Figura 2.28*Niveles de Madurez de CMM.* (SEI-CMM citado por Chacón, 2004, p. 51)

CapabilityMaturityModelIntegration, CMMI

El Modelo Integrado de Capacidad de Madurez es un *modelo de procesos* que sirve como referencia a las organizaciones para implementar *mejoras* considerando el principio de aplicación de procesos, para mejorar la calidad y como base para la gestión de las empresas. (SEI-CMMI citadoporChacón, 2004)

Information Security Management Maturity Model, ISM3

El propósito de los sistemas de gestión de seguridad es prevenir o mitigar los ataques, errores y accidentes que puedan poner en riesgo la seguridad de los sistemas de información y los procesos organizativos soportados por ellos, optimizando el uso de la información, presupuesto, personal, tiempo e infraestructura. El Modelo de Madurez de la Gestión de la Seguridad de la Información (ISMMM o ISM3) ofrece un nuevo enfoque para especificar, implementar, operar y evaluar sistemas ISM.Los niveles de madurez ISM3 van del 0 al 4. (ISECOM, n.d.)

2.9 Computer Assisted Audit Techniques, CAAT

Las Técnicas de Auditoría Asistida por Computador, se refieren a la utilización de las herramientas informáticas en la realización de un trabajo de auditoría para evaluar la consistencia que presentan los sistemas de información, seleccionar muestras, analizar datos, conciliar los datos y/o buscar alguna información en particular.

Todas estas actividades, pueden ser realizadas a través de las siguientes herramientas informáticas:herramientas generales o utilitarias; herramientas administrativas; herramientas de análisis de datos;y herramientas especializadas. (Brito, Solis, 2004)

CAPITULO 3

ESTUDIO PRELIMINAR DEL ENTORNO A AUDITAR - SUPERTEL

3.1 Estudio de la Superintendencia de Telecomunicaciones

La estructura organizacional de la SUPERTEL se sustenta en un enfoque por procesos y en la filosofía de mejora continua y gestión de calidad.

Procesos de la SUPERTEL. (SUPERTEL-Ecuador - Reglamento Orgánico por Procesos, 2010, p. 6)

"Los productos y servicios que generan los procesos de la Superintendencia de Telecomunicaciones son responsabilizados como procesos concentrados a una Administración Central con sede en la ciudad de Quito y se delegan como procesos desconcentrados a través de oficinas en seis regiones administrativas en el territorio nacional. Según el grado de contribución y valor agregado al cumplimiento de la misión institucional, los procesos de la SUPERTEL se clasifican en:

a) *Procesos Gobernantes*, orientan la gestión institucional a través de la formulación de políticas y expedición de normas e instrumentos para el funcionamiento de la Superintendencia;
b) *Procesos Agregadores de Valor*, generan, administran y controlan los productos y servicios destinados a crear valor para los clientes y usuarios, dando cumplimiento a la misión institucional;
c) *Procesos Habilitantes*, encaminados a generar productos y servicios para los procesos gobernantes, agregadores de valor y para sí mismos, viabilizando la gestión institucional; se clasifican en procesos de asesoría y procesos de apoyo;
d) *Procesos Desconcentrados*, encaminados a generar productos y servicios institucionales en jurisdicciones específicas."

Misión Institucional

"Vigilar, auditar, intervenir y controlar técnicamente la prestación de los servicios de telecomunicaciones, radiodifusión, televisión y el uso del espectro radioeléctrico, para que se proporcione con eficiencia, responsabilidad, continuidad, calidad, transparencia y equidad; fomentando los derechos de los usuarios a través de la participación ciudadana, de conformidad al ordenamiento jurídico e interés general." (SUPERTEL-Ecuador - Reglamento Orgánico por Procesos, 2010, p. 9)

Objetivos Estratégicos(SUPERTEL-Ecuador - Reglamento Orgánico por Procesos,, 2010, p. 9)

- "Velar por el cumplimiento de los derechos de los usuarios de los servicios de telecomunicaciones, radiodifusión y televisión,
- Impulsar la migración a la televisión y radiodifusión digital,
- Alcanzar la calidad total en la gestión institucional,
- Coadyuvar al fortalecimiento del marco jurídico del sector de telecomunicaciones, de conformidad con la norma constitucional,
- Atender de manera solvente los requerimientos de los usuarios de los servicios de telecomunicaciones, radiodifusión y televisión,
- Fortalecer la infraestructura tecnológica institucional,
- Elevar la productividad laboral con talento humano altamente calificado y comprometido con la SUPERTEL y la sociedad."

Modelo de Gestión por Procesos

a) *Cadena de Valor: (Ver Figura 3.1)*

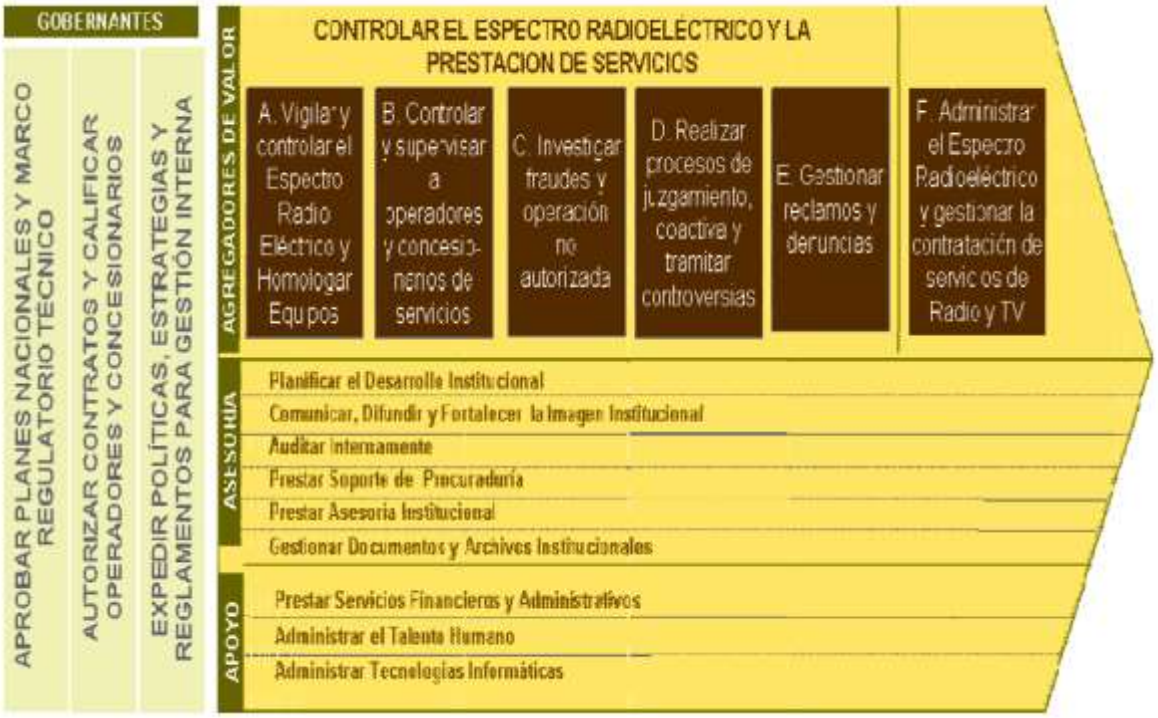

Figura 3.1*Cadena de Valor de la SUPERTEL.*
(SUPERTEL-Ecuador - Reglamento Orgánico por Procesos, 2010, p. 10)

b) Mapa de Procesos: (Ver Figura 3.2)

Figura 3.2*Mapa de Procesos de la SUPERTEL.*
(SUPERTEL-Ecuador - Reglamento Orgánico por Procesos, 2010, p. 11)

c) Organigrama Estructural: (Ver Figura 3.3)

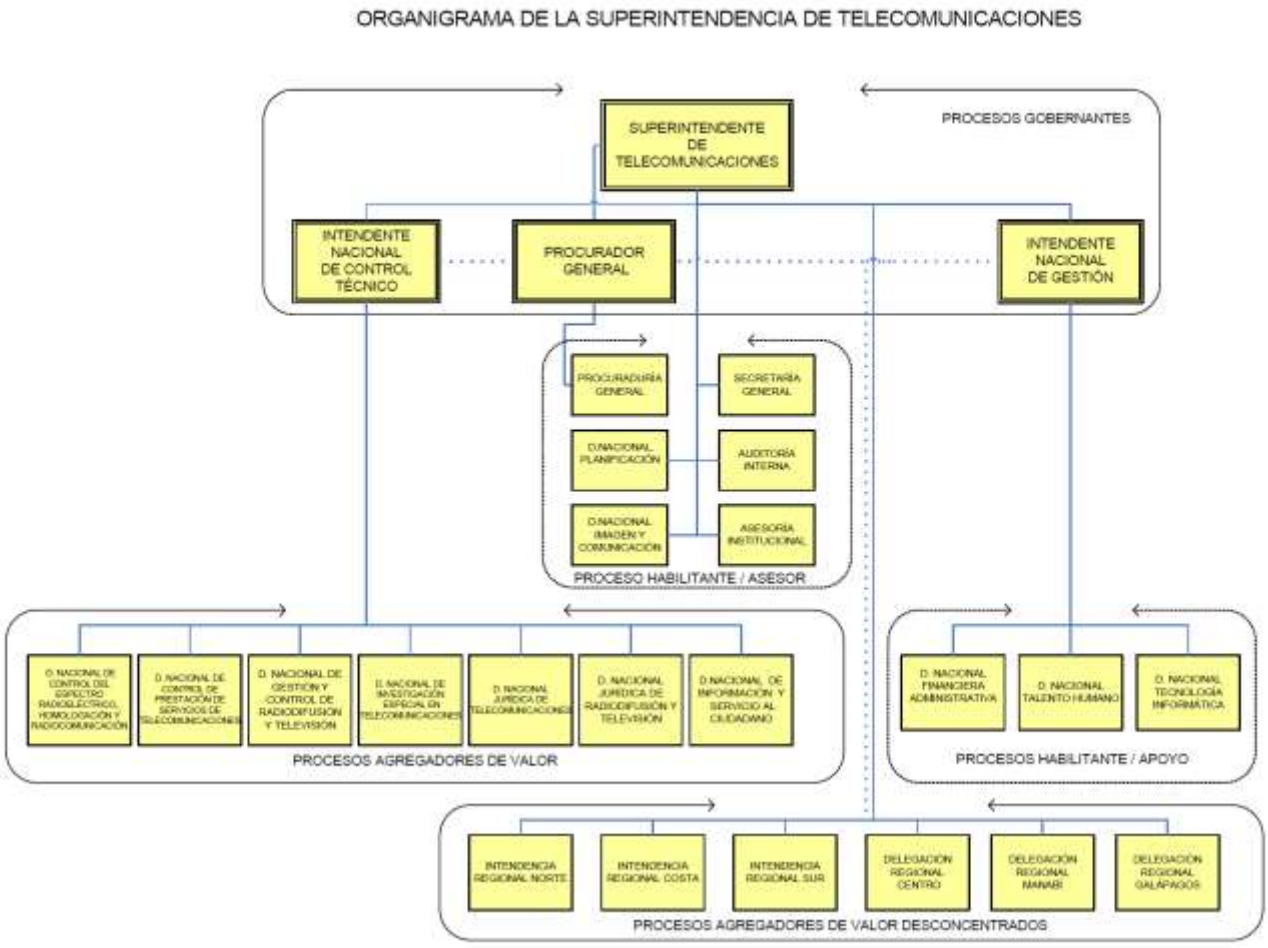

Figura 3.3 *Organigrama Estructural de la SUPERTEL.*
(SUPERTEL-Ecuador - Reglamento Orgánico por Procesos, 2010, p. 12)

Intendencias y Delegaciones Regionales: Tienen la misión de programar, coordinar, ejecutar e informar las acciones orientadas al control del espectro radioeléctrico, la prestación de servicios, el juzgamiento de infracciones, la atención de reclamos y controversias entre operaciones y/o concesionarios en el ámbito específico de su jurisdicción; en el marco de los procedimientos, mecanismos, programas y planes establecidos; y coadyuvar en la gestión del proceso coactivo. (SUPERTEL-Ecuador - Reglamento Orgánico por Procesos, 2010, p. 32). La estructura organizativa de las Intendencias Regionales se muestra en la Figura 3.4.

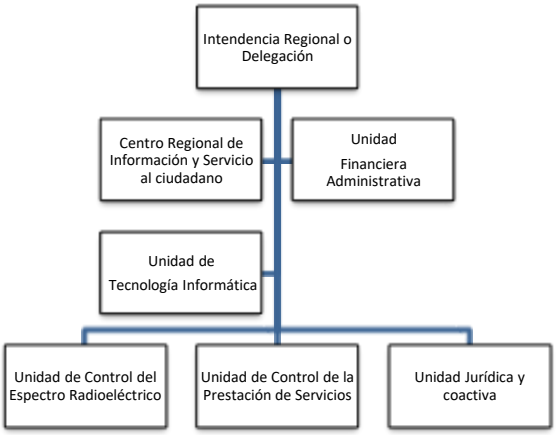

Figura 3.4 *Estructura Organizativa de las Intendencias Regionales. (SUPERTEL-Ecuador - Reglamento Orgánico por Procesos, 2010, p. 32)*

Puestos de Trabajo de la Superintendencia de Telecomunicaciones

El número de puestos de trabajo de acuerdo a las unidades que forman parte de los procesos desconcentrados se detallan en la Tabla 3.1

PUESTOS DE TRABAJO SUPERTEL	
Numero Total de Puestos de Trabajo	380
Numero Total de Puestos de Trabajo bajo la modalidad de Nombramiento	330
Número Total de Puestos de Trabajo bajo la modalidad de Contrato de Servicios Ocasionales	50
Número Total de Puestos de Trabajo en la Matriz	192
Número Total de Puestos de Trabajo en la Intendencia Regional Norte	75
Número Total de Puestos de Trabajo en la Intendencia Regional Costa	41
Número Total de Puestos de Trabajo en la Intendencia Regional Sur	28
Número Total de Puestos de Trabajo en la Delegación Manabí	16
Número Total de Puestos de Trabajo en la Delegación Centro	18
Número Total de Puestos de Trabajo en la Delegación Galápagos	10

Tabla 3.1*Puestos de Trabajo SUPERTEL. (SUPERTEL-POA, 2011)*

Proyectos de Inversión de la Superintendencia de Telecomunicaciones

La Superintendencia de Telecomunicaciones en concordancia con el plan estratégico y el plan operativo anual, mantiene siempre un presupuesto destinado a la innovación tecnológica, un detalle referencial de proyectos de inversión se muestra en la Tabla 3.2

PROYECTOS DE INVERSION SUPERTEL	
DESCRIPCIÓN	**VALOR INICIAL $**
1. Equipo para el control del espectro radioeléctrico	4.368.746,00
2. Obras Civiles (Construcción y mantenimiento)	1.635.400,00
2.1 Construcción de Obras Civiles	1.411.400,00
2.2 Mantenimiento y reparación en obras de líneas, redes e instalaciones en las estaciones de comprobación.	224.000,00
3. Equipo para control de los servicios de telecomunicaciones	4.310.580,00
4. Desarrollo informático	2.444.150,00
4.1 Hardware General	696.800,00
4.2 Software General	307.000,00
4.3 Hardware y Software Especializado	1.440.350,00
5. Red de Comunicaciones	20.150,00
6. Bienes inmuebles	300.000,00
Total	13.079.026,00

Tabla 3.2*Proyectos de Inversión SUPERTEL. (SUPERTEL-POA, 2011)*

3.2 Estudio de la Dirección de Tecnología de la Información

Atribuciones y responsabilidades de la Dirección de Tecnología de la Información

Entre las atribuciones y responsabilidades se encuentran las siguientes:(SUPERTEL-Ecuador - Reglamento Orgánico por Procesos, 2010, p. 39)

- Cumplir y hacer cumplir las leyes y normativa en materia de gestión informática,
- Participar en el diseño de servicios de tecnología de la información, en el marco de los planes aprobados y de las normas y reglamentos vigentes,
- Participar en la transferencia (implementación) de servicios de tecnología de la información, en el marco de los planes aprobados y de las normas y reglamentos vigentes,
- Operar localmente los servicios de tecnología de la información, en el marco de las normas y reglamentos vigentes,
- Participar en la mejora continua de los servicios, recoger localmente datos y analizar tendencias comparándolas con la línea base (acuerdos de nivel de servicio, rendimientos de entidades similares, objetivos),
- Brindar soporte técnico de primera línea a los usuarios locales,
- Apoyar la implementación de redes de datos y comunicaciones de la Intendencia o Delegación,
- Administrar y controlar el uso adecuado de la tecnología de la información,
- Apoyar en la operación de la central telefónica,
- Ejecutar los planes de tecnología de la información,
- Desarrollar aplicaciones de sistemas informáticos,

Productos Desarrollados por la Unidad de Tecnología de la Información

Los productos desarrollados por esta unidad son los siguientes:(SUPERTEL-Ecuador - Reglamento Orgánico por Procesos, 2010, p. 54)

Diseñar servicios: Catálogo de servicios, SLA's (Acuerdo de Nivel de Servicio), Plan de seguridad del servicio, Documento técnico del servicio / pliegos del servicio, Acta de entrega/recepción, Plan de difusión, Servicios diseñados.
Transferir (implementar) servicios: Versión de servicio desarrollada, Versión de servicio para pruebas, Versión de servicio probada, Servicio implementado, documentado y puesto en operación.

Operar Servicios: Indicadores de desempeño del servicio, Solicitud de acceso al servicio atendida, Incidente (incluye reporte de problema) resuelto, Estadísticas del servicio, Informes periódicos de gestión en el marco de los procedimientos vigentes.

Objetivos estratégicos de la Unidad de Tecnología de la Información

La Tecnología de la Información es una unidad de apoyo responsable de la administración y control de TI en el Organismo, los objetivos que plantea esta dirección se muestran en la Tabla 3.3

OBJETIVOS ESTRATEGICOS DTI	
Innovar tecnológicamente la institución	Desarrollar sistemas informáticos Dar mantenimiento a todos los sistemas de información que lo requieran Proporcionar líneas de comunicación efectivas hacia los usuarios. Dotar de herramientas tecnológicas a los Usuarios, que permitan incrementar su productividad. Proporcionar asesoría tecnológica para la ejecución de todos los proyectos, para que se realicen en el tiempo indicado.
Anticipar las necesidades tecnológicas de la institución	Investigar tendencias que cumplan con estándares internacionales y que pudieran proporcionar nuevas alternativas de servicios de valor agregado a la SUPERTEL
Mantener una estructura Dinámica	Hacer el seguimiento del marco regulatorio para el uso, administración y control del recurso tecnológico informático de la institución Optimizar los procesos de la Dirección.

Tabla 3.3*Objetivos de la Unidad de TI.*

Análisis FODA de la Unidad de Tecnología de la Información

Luego de un análisis mediante observación, indagación y entrevistas se identificaron las fortalezas, oportunidades, debilidades y amenazas de la Unidad de TI de la SUPERTEL. Eso se muestra en la Tabla 3.4

FORTALEZAS	OPORTUNIDADES
Buen nivel de conocimiento técnico Equipo humano homogéneo Predisposición al cambio Infraestructura física actualizada	Participación en proyectos institucionales. Nuevas áreas tecnológicas disponibles. Convergencia de servicios.
DEBILIDADES	**AMENAZAS**
La DTI no es una unidad asesora en la toma de decisiones, únicamente apoya en la ejecución. Carga laboral poco equilibrada debido a la falta de personal frente a la cantidad de servicios.	Falta de una normativa adecuada Altos costos de la tecnología

Tabla 3.4*Matriz FODA de la Unidad de TI – SUPERTEL.*

Recursos Humanos de la Dirección general de Tecnología

Para realizar las funciones de DTI que se definen en el Reglamento Orgánico Funcional por Procesos descrito anteriormente, ésta Dirección cuenta con el recurso humano especificado en la Tabla 3.5.

PUESTOS DE TRABAJO DTI		
PERFIL	CARGO ADMINISTRATIVO	#
Director	Director General	1
Coordinador	Coordinador General	1
Ingeniero de Desarrollo	Profesional Informático 2	1
	Profesional Informático 1	3
Ingeniero de Infraestructura	Profesional Informático 2	1
	Profesional Informático 1	4
Secretaria	Asistente Profesional 1	1
Ayudante de Oficina	Ayudante	1

Tabla 3.5*Recursos Humanos de DTI.*

Adicionalmente, para el cumplimiento de la desconcentración de funciones que se contemplan en la SUPERTEL, se han designado funcionarios en las unidades regionales como lo muestra la Tabla 3.6

PUESTOS DE TRABAJO DTI		
PERFIL	CARGO ADMINISTRATIVO	NO
Soporte Regional Norte	Asistente Profesional 3	1
Soporte Regional Sur	Profesional Informático 1	1
Soporte Regional Costa	Asistente Profesional 1	1
Soporte Regional Centro	Profesional Técnico 2	1

Tabla 3.6 Recursos Humanos de DTI - Regionales.

Estructura por Procesos de la Dirección de TI

La Dirección de TI, organiza su gestión por procesos, los mismos que se ajustan a ITIL V3. Una descripción detallada de ITIL se encuentra en el Capitulo 2.

Estándares establecidos en la Unidad de TI

La definición de estándares para el software, hardware, servicios de red y proveedores, busca asegurar en la SUPERTEL la correcta adquisición de los nuevos recursos tecnológicos en el área informática. La definición de marcas solo se aplica para compras puntuales que no deben alterar el parque informático existente, en concordancia con lo establecido en la Ley de Contratación Pública. Para compras mayores no se aplican marcas y se deja abierta la posibilidad de adoptar nuevos lineamientos conforme a Leyes y Reglamentos.

Estándares de Software.

El software que la Dirección General de Tecnología de la Información pone a disposición de la Superintendencia de Telecomunicaciones, permite que los funcionarios optimicen su trabajo y cumple con las características mostradas en la Figura A1.1, del Anexo 1 - CD.

Estándares de Hardware

Los computadores de la SUPERTEL deben estar en condiciones de ser conectados a la red LAN principal de datos de cada administración. Los dispositivos telefónicos deben ser compatibles con la central telefónica IP de CISCO. Los dispositivos y equipos que la institución adquiera deben cumplir requisitos mínimos de especificación de hardware. Las Figuras A1.2, a A1.6, del Anexo 1 - CD, presentan una muestra de especificaciones mínimas de hardware institucional.

Servicios Tecnológicos

La metodología de desarrollo de sistemas que emplea la SUPERTEL es el PROCESO UNIFICADO DE DESARROLLO DE SOFTWARE de Ivar Jacobson, Grady Booch y James Rumbaugh, por ser reconocida y aceptada mundialmente como estándar.

Desarrollo

Los nuevos servicios tecnológicos que la Superintendencia de Telecomunicaciones requiera, son desarrollados por la Dirección General de Tecnología de la Información o por terceros bajo su coordinación y supervisión directa. Los servicios a desarrollarse, la priorización y todos sus detalles se encuentra especificados en el portafolio de servicios que forma parte integrande del proceso de Diseño de Servicios.

Mantenimiento

Los servicios tecnológicos que posee la Superintendencia de Telecomunicaiones requieren mantenimeinto preventivo así como la implementación de mejoras y/o control de correcto funcionamiento. Este mantenimiento lo proporciona la Dirección General de Tecnología de la Información o el desarrollador del servicio con supervisión directa de ésta Dirección.

Se da mantenimiento de los servicios tecnológicos desarrollados por la Dirección y se proporciona asistencia, en los límites de lo posible, a todos aquellos servicios que son de desarrollo externo y que no poseen soporte contratado con el desarrollador original.

En lo referente al software comercial, se solicita asistencia a los vendedores del producto o directamente a los fabricantes, de ser posible y si el caso lo requiere.

Catálogo de Servicios Operativos

Los servicios operativos se encuentran en el catálogo de servicios que forma parte integrante del Diseño de Servicios.Un detalle de este catalogo se encuentra en el Anexo 2 - CD.

Plan de Inversión

En el plan de inversiones se proyecta la adquisición de software y hardware tanto de propósito general como de componentes específicos de servicios. De igual forma se contemplan las contrataciones de desarrollo de nuevos servicios y el mantenimiento de los existentes.La adquisición de software y hardware de propósito general se lo realiza de ser posible, una vez por año. La contratación de desarrollo de servicios se lo realiza según el cronograma que se defina en el portafolio de servicios atendiendo la prioridad de cada servicio. Ver Tabla 3.7.

PRESUPUESTO REFERENCIAL	
ITEM	**VALOR ANUAL (USD)**
Recurso Humano	436.890,00
Remuneración	419.250,00
Viáticos	17.640,00
Plan de Inversiones 2010	2.659.420,00
Plan de Inversiones 2011	3’765.950,00
Plan de Inversiones 2012	4’945.650,00

Tabla 3.7*Presupuesto Referencial.*
(SUPERTEL – Plan de Inversiones, 2012).

Los valores de inversión en hardware y software no incluyen aquellos ítems definidos en los proyectos que tienen financiamiento propio así como tampoco los impuestos de ley.El rubro de viáticos corresponde a movilizaciones nacionales necesarias para la ejecución de las actividades de desarrollo y mantenimiento de servicios.No están considerados en este presupuesto, los valores para capacitación nacional o internacional, así como tampoco se han considerado los montos para viáticos internacionales necesarios.

CAPITULO 4

PLANEACIÓN DE LA AUDITORÍA INFORMÁTICA A LA SUPERTEL

El plan de auditoría debe estar basado en la comprensión de las actividades de las entidades, sus sistemas de administración y control, la naturaleza de las transacciones, procesos que realiza y las leyes y reglamentos que aplican. El plan debe ser documentado como parte integral de los papeles de trabajo y modificado, cuando sea necesario durante el transcurso de la auditoria.El proceso de planeación comprenderá las siguientes etapas:

1. Planeación previa
2. Estudio preliminar del área a auditar.
3. Desarrollo de la estrategia de la auditoria
4. Recursos
5. Programas de auditoría

4.1 Planeación Previa

Para hacer una adecuada planeación de la auditoría en informática, se han realizado una serie de pasos previos, que permitirán dimensionar el tamaño y características del área informática dentro del organismo a auditar, sus sistemas, organización y equipo; con ello podremos determinar la estrategia, las herramientas necesarias y el tiempo, así como definir los planes y programas de trabajo para la ejecución de la auditoria.

La planeación se realizará desde el punto de vista de los cuatro objetivos identificados en el alcance: sistemas de información en operación; metodología de desarrollo o adquisición de sistemas de información; administración de hardware; y administración de telecomunicaciones. En cada una de las áreas se evaluará el desempeño y los riesgos en base al cumplimiento de los principios de seguridad, confiabilidad y eficiencia; cumplimiento de políticas y procedimientos; y en base al grado de satisfacción de la alta dirección y del personal usuario.

4.2 Estudio Preliminar

El estudio inicial del entorno a auditar, realizado en el capítulo anterior, pertenece a la primera fase dentro del proceso de auditoría de acuerdo a la metodología establecida en el Capítulo I, ha permitido tener una idea global y las estructuras fundamentales de la SUPERTEL, así como también una visión general y completa de la Unidad de Tecnología de la Información.

4.3 Desarrollo de la estrategia de auditoría

4.3.1 Determinación del Plan Estratégico de la Auditoría Informática a la SUPERTEL

El plan estratégico de una auditoria informática representa el soporte sobre el cual estarán basadas todas las actividades requeridas para la ejecución del trabajo, de modo que pueda ser alcanzado de forma eficiente. Para la realización de esta auditoría se tomará como estrategia el marco de referencia COBIT 4.1, analizado en el Capitulo II.

4.3.2 Justificación del Uso del Modelo de Referencia COBIT 4.1

Para la ejecución de la auditoría se ha tomado como marco de referencia COBIT 4.1, el cual es un marco de gobernabilidad de TI y un conjunto de herramientas de ayuda que permite asociar los conceptos de requerimientos de control, consideraciones técnicas y riesgos institucionales. Este conjunto de las mejores prácticas permiten evaluar la seguridad, eficacia, calidad y eficiencia de las TI., mediante lo cual se determinan los riesgos, se obtiene una gestión efectiva de los recursos, se mide el desempeño y cumplimiento de metas, y de manera principal el nivel de madurez de los procesos de la organización. Se ha elegido COBIT debido a que satisface las necesidades que tiene la organización en lo referente a las TI, tomando en cuenta los requerimientos de la institución, organizando las actividades mediante el modelo de procesos, identificando los recursos de TI prioritarios a ser utilizados y definiendo los controles de TI.

4.3.3 Determinación del Marco de Trabajo de la Auditoría a la SUPERTEL bajo COBIT

El marco de trabajo de la auditoría a la SUPERTEL se enfoca y orienta hacia cuatro elementos determinantes:

1. La institución
2. Los procesos
3. Los controles
4. Las métricas, mediciones e indicadores

Orientado a la Institución: Como se vio en el Capitulo II, el marco de trabajo COBIT plantea que la institución debe invertir en controlar y administrar los recursos de TI, usando un conjunto de procesos que garanticen la alineación con los requerimientos institucionales.

Orientado a Procesos: El marco de trabajo de la auditoría informática a la SUPERTEL estará basado en 34 procesos definidos por COBIT, que garantizan la alineación con los requerimientos de la institución y de TI. Estos procesos se encuentran organizados en cuatro dominios que se equiparan a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear. Como se vio en el capitulo II estos dominios son: planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte, Monitorear y Evaluar. (Ver figura 2.6)

Basado en controles: La auditoría empleará 34 objetivos de control generales, uno para cada proceso de TI y 209 objetivos de control detallados, que son políticas, procedimientos, prácticas y estructuras organizacionales que proporcionan un conjunto completo de requerimientos de alto nivel para un control efectivo de cada proceso de TI.

Impulsado por la medición: La necesidad básica de toda institución es entender el estado de sus propios procesos, sistemas y equipos de TI, donde se requieren mejoras, así como determinar qué nivel de administración y control debe proporcionar. La auditoría atenderá estos temas a través de los siguientes elementos: (COBIT 4.1, 2007)

1. Modelos de madurez, que facilitarán la evaluación por medio de benchmarking y permitirán identificar las mejoras necesarias.
2. Metas y mediciones de desempeño para los procesos de TI, que permitirán evaluar cómo los procesos satisfacen las necesidades de la SUPERTEL y de TI.
3. Metas de actividades para facilitar el desempeño efectivo de los procesos.

La Tabla 4.1 resume cómo los distintos elementos del marco de trabajo de COBIT se relacionan con las áreas de enfoque del gobierno de TI.

MARCO DE TRABAJO COBIT Y ÁREAS DE ENFOQUE DE GOBIERNO DE TI				
	Metas	Métricas	Prácticas	Modelos de Madurez
Alineamiento Estratégico	P	P		
Entrega de Valor		P	S	P
Gestión de Riesgos		S	P	S
Gestión de Recursos		S	P	P
Medición del Desempeño	P	P		S

P= Facilitador Primario S=Facilitador Secundario

Tabla 4.1*Marco de Trabajo COBIT y Áreas de Enfoque de Gobierno de TI.*(COBIT 4.1, 2007)

4.3.4 Estrategia de la Auditoría Informática a la SUPERTEL

De acuerdo al marco de trabajo planteado en el punto anterior, la auditoría estará orientada a la institución y a los procesos de TI, empleando para su análisis objetivos de control, metas, métricas y mediciones. Las Tablas 4.2, 4.3, 4.4 y 4.5 indican los procesos y objetivos de control; las metas de TI de la SUPERTEL; las metas de TI de acuerdo a COBIT y las métricas y mediciones a ser empleadas en la auditoría informática a la SUPERTEL respectivamente. Además se brindará una visión global de cómo se relacionan las metas genéricas de la institución, con las metas de TI de acuerdo a COBIT, considerando también, los procesos de TI y los criterios de in-

formación. Para establecer esta relación entre procesos COBIT y SUPERTEL, se emplearán una serie de planos que se listan en la Tabla 4.6, y se describen más adelante.

Procesos y Objetivos de Control COBIT	
PLANEAR Y ORGANIZAR	
PO1	Definición del plan estratégico de TI
PO2	Definición de la arquitectura de la información
PO3	Determinación de la dirección tecnológica.
PO4	Definición de los procesos, organización y relaciones de TI.
PO5	Administración de la inversión en TI.
PO6	Comunicación con la Alta Dirección
PO7	Administración de los recursos humanos de TI.
PO8	Administración de la calidad de TI
PO9	Evaluación y administración de los riesgos de TI.
PO10	Administración de los proyectos de TI
ADQUIRIR E IMPLEMENTAR	
AI1	Identificación de las soluciones automatizadas.
AI2	Adquisición y mantenimiento del software aplicativo.
AI3	Adquisición y mantenimiento de la infraestructura tecnológica.
AI4	Facilitad de operación y uso de TI
AI5	Adquisición de recursos de TI.
AI6	Administración de cambios en TI
AI7	Instalación y acreditación de soluciones y cambios en TI
ENTREGAR Y DAR SOPORTE	
DS1	Definición y administración de los niveles de servicio.
DS2	Administración de los servicios de terceros.
DS3	Administración del desempeño y capacidad de TI
DS4	Garantías en la continuidad del servicio
DS5	Garantías en la seguridad de los sistemas.
DS6	Identificación y asignación de costos de TI.
DS7	Educación y entrenamiento a los usuarios.
DS8	Administración de la mesa de servicios de TI y los incidentes.
DS9	Administración de la configuración de TI.
DS10	Administración de los problemas con TI.
DS11	Administración de los datos.
DS12	Administración del ambiente físico.
DS13	Administración de las operaciones de TI.
MONITOREAR Y EVALUAR	
ME1	Monitoreo y evaluación del desempeño de TI.
ME2	Monitoreo y evaluación el control interno.
ME3	Garantías en el cumplimiento regulatorio.
ME4	Proporciona gobierno de TI.

Tabla 4.2*Procesos y Objetivos de Control COBIT.*(COBIT 4.1, 2007)

Metas Generales de TI - SUPERTEL		
Perspectiva Financiera	1	Proporcionar un buen retorno de inversión de TI
	2	Gestionar los riesgos de TI que afectan a la institución
	3	Fomentar la transparencia
Perspectiva del Cliente	4	Mejorar la orientación y servicio al usuario
	5	Ofrecer productos y servicios competitivos
	6	Establecer continuidad y disponibilidad de servicios
	7	Crear agilidad en la respuesta a los cambios de los requerimientos institucionales
	8	Lograr optimización de costos en la entrega de servicios
	9	Obtener información fiable y útil para tomar decisiones estratégicas
Perspectiva Interna	10	Mejorar y mantener funcionalidad de los procesos institucionales
	11	Reducir el costo de los procesos
	12	Proporcionar cumplimiento con leyes, reglamentos y regulaciones
	13	Proporcionar cumplimiento con políticas internas
	14	Gestionar cambios institucionales
	15	Mejorar y mantener operatividad en el control de las telecomunicaciones
Perspectiva de Aprendizaje y Crecimiento	16	Gestionar productos e innovación de la institución
	17	Adquirir y mantener personal cualificado y motivado

Tabla 4.3*Metas Generales de TI de la SUPERTEL.*

Metas de TI - COBIT	
1	Responder a los requerimientos de la institución alineados con el plan estratégico
2	Responder a los requerimientos de TI en línea con los procesos gobernantes de la SUPERTEL
3	Asegurar la satisfacción del usuario con la oferta de servicios y niveles de servicio
4	Optimizar el uso de la información
5	Crear agilidad de TI
6	Definir cómo la funcionalidad de las tareas de la institución y requerimientos de control, se trasladan en soluciones efectivas.
7	Adquirir y mantener sistemas de aplicación integrados y estandarizados
8	Adquirir y mantener una infraestructura de TI integrada y estandarizada
9	Adquirir y mantener habilidades de TI que responden a la estrategia de TI
10	Asegurar la satisfacción mutua de relaciones con terceras partes
11	Asegurar la integración sin fisuras de las aplicaciones dentro de los procesos de la institución
12	Asegurar la transparencia y la comprensión de costes de TI, beneficios, estrategia, políticas y niveles de servicio.
13	Asegurar el uso apropiado y desempeño de las soluciones de aplicación y tecnología
14	Tener en cuenta y proteger todos los activos de TI
15	Optimizar la infraestructura, recursos y capacidades de TI
16	Reducir los defectos de la solución y entrega de servicio.
17	Proteger el logro de los objetivos de TI
18	Establecer la claridad del impacto de los riesgos a los objetivos y recursos de TI
19	Asegurar que la información crítica y confidencial se retiene a aquellos que no deben tener acceso
20	Asegurar que las tareas de la institución sean automatizadas y los cambios a la información sean confiables
21	Asegurar que los servicios de TI y la infraestructura pueden resistir apropiadamente y recuperarse de fallos debidos a errores, ataques deliberados o desastres.
22	Asegurar el mínimo impacto a las tareas de la institución, en caso de una interrupción de servicios de TI o cambios
23	Asegurar que los servicios de TI estén disponibles según se requiere
24	Mejorar la eficiencia de costes de TI y sus contribuciones a las labores de la institución
25	Entregar proyectos a tiempo y sobre presupuesto, reuniendo los estándares de calidad
26	Mantener la integridad de la información e infraestructura de procesamiento
27	Asegurar que TI cumple con la legislación y regulación nacional.
28	Asegurar que TI demuestra le eficiencia de costes de calidad de servicios, mejora continua y disposición para cambios futuros.

Tabla 4.4*Metas de TI – COBIT (COBIT 4.1)*

Métricas y Mediciones de la AI a la SUPERTEL		
CALIFICADORES	**MODELOS**	**MATRICES**
Calificador Real del Estado del Proceso	MODELO DE MADUREZ	Matriz de Grados de Madurez de Procesos – SUPERTEL
	MODELO DE MEDICION DEL DESEMPEÑO	Matriz de Nivel de Servicio – SUPERTEL. Matriz de Evaluación de Procesos bajo Métricas COBIT
	MODELO DE MEDICION DE LOS OBJETIVOS DE CONTROL	Matriz de Cumplimiento de Objetivos de Control – COBIT
Impacto del Proceso	MODELO DE IMPACTOS	Matriz de Impactos de Procesos frente a los criterios de información de COBIT. Matriz de Diagnóstico de Procesos COBIT

Tabla 4.5*Métricas y Mediciones de la AI a la SUPERTEL*

Mapa de Relación COBIT-SUPERTEL	
Planos de Mapeo	Plano de Enlace de las Metas de la Institución, Metas TI y Criterios de Información
	Plano de Enlace de las Metas TI, Procesos COBIT y Criterios de Información
	Plano de Enlace Procesos de COBIT a Metas de TI
	Plano de Enlace de Procesos COBIT a Gobierno de TI y Criterios de Información
	Plano de Responsabilidades de Procesos COBIT

Tabla 4.6*Componentes del Mapa de Relación COBIT-SUPERTEL*

Calificador Real del Estado del Proceso

La auditoría obtendrá un calificador real del estado de cada uno de los 34 procesos de acuerdo a tres dimensiones: madurez, desempeño y cumplimiento de objetivos.

A su vez, cada dimensión tendrá un indicador cuantitativo, que se obtendrá de acuerdo a los modelos planteados en la sección siguiente. Ya que se trata de un espacio tridimensional, el calificador real del estado del proceso se obtendrá mediante la magnitud del vector resultante equivalente para indicadores con valores del 100% en las tres dimensiones. Las componentes vectoriales en i, j, y k corresponden a los indicadores resultantes de las dimensiones: madurez (i), desempeño (j), y cumplimiento de objetivos (k), respectivamente. Esto se muestra en la Figura 4.1

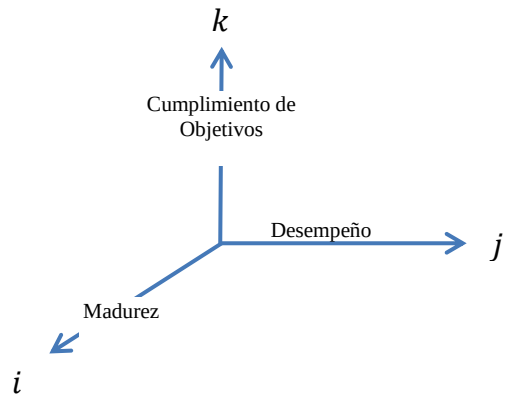

Figura 4.1*Dimensiones del Estado del Proceso.*

La magnitud del vector resultante con valor del 100% en los indicadores de cada dimensión sería:

$$C_{ideal} = \sqrt{i^2 + j^2 + k^2}$$

$$C_{ideal} = \sqrt{100^2 + 100^2 + 100^2}$$
$$C_{ideal} = \sqrt{3}(100) = 173.21$$

Se obtiene C_{ideal} igual a $\sqrt{3}(100)$por lo tanto para mantener 100% como valor referencial se deberá dividir por $\sqrt{3}$ el valor obtenido.

Es así que la magnitud del calificador real del estado del proceso se obtendrá mediante la siguiente expresión:

$$\mathrm{C} = \frac{\sqrt{m^2+d^2+o^2}}{\sqrt{3}} \qquad \text{Calificador Real}$$

donde$m$ = % Madurez (Grado de Madurez), d = % Desempeño y o = % Cumplimiento de Objetivos

El análisis vectorial tridimensional, además de un indicador global obtenido mediante el modulo del vector (C), nos brindará información adicional respecto al sentido y dirección del mismo.

Los valores de los indicadores de Madurez, Desempeño y Cumplimiento de Objetivos son siempre positivos por lo cual el sentido corresponderá siempre a un valor resultante positivo.

La dirección del vector vendrá dada por los ángulos alfa, beta y gama con respecto a los ejes cartesianos como sigue:

$$\alpha = cos^{-1}\left({}^{m}/_{C}\right)$$
$$\beta = cos^{-1}\left({}^{d}/_{C}\right)$$
$$\gamma = cos^{-1}\left({}^{o}/_{C}\right)$$

Si consideramos el caso ideal

$$\alpha = cos^{-1}\left({}^{100}/_{100\sqrt{3}}\right)$$
$$\alpha = cos^{-1}\left({}^{1}/_{\sqrt{3}}\right) = 54.74°$$

$$\beta = cos^{-1}\left({}^{100}/_{100\sqrt{3}}\right)$$

$$\beta = cos^{-1}\left({}^{1}/_{\sqrt{3}}\right) = 54.74°$$
$$\gamma = cos^{-1}\left({}^{100}/_{100\sqrt{3}}\right)$$
$$\gamma = cos^{-1}\left({}^{1}/_{\sqrt{3}}\right) = 54.74°$$

La información obtenida del análisis de los ángulos es también relevante ya que el ángulo con mayor valor corresponderá a la dimensión más débil del proceso.

Impacto Real del Proceso

Este indicador corresponde a un valor porcentual que determina el impacto real del proceso dentro del Unidad de TI de la SUPERTEL, determinado por el indicador obtenido mediante el modelo de impactos.

Se dará un valor cualitativo al valor porcentual del indicador de impacto en base a las equivalencias mostradas en la Tabla 4.6.

IMPACTO	
Alto	68-100
Medio	34-67
Bajo	0-33

Tabla 4.6*Equivalencias del Impacto*

4.3.5 Descripción de los Modelos de Medición

MODELO DE MADUREZ

La aplicación del modelo de madurez permitirá identificar:

- El desempeño real de la institución
- El objetivo de mejora de la institución

El incremento en la madurez reduce el riesgo y mejora la eficiencia, generando menos errores, más procesos predecibles y un uso rentable de los recursos.

Indicador de Madurez $(\boldsymbol{m})$

Para obtener el indicador de madurez de un proceso COBIT, se empleara la matriz especificada en la Tabla 4.7.

INDICADOR DE MADUREZ		
PARAMETRO		MATRIZ
1	Grado de madurez real para un nivel i $(\boldsymbol{m_{rl}})$	Matriz de Grados de Madurez de Procesos SUPERTEL.

Tabla 4.7*Parámetros del Indicador de Madurez*

El indicador de madurez, es el que se empleará para el cálculo del calificador global y se obtiene de la siguiente manera:

$$m = (i - 1) * 20\% + (20\% * m_{rl})$$

Donde m = Grado de Madurez, m_{rl}= Grado de Madurez Real correspondiente a un Nivel i.

Se emplea la constante 20%, dado que son 5 niveles, excluyendo el no existente (0). Por tanto $\frac{100\%}{5} = 20\%$. Esto es para el $Nivel\ 0 = 0\%$, $Nivel\ 1 = 20\%$, $Nivel\ 2 = 40\%$, $Nivel\ 3 = 60\%$, $Nivel\ 4 = 80\%$,$Nivel\ 5 = 100\%$.

Para determinar los parámetros que definan un nivel de madurez específico, se utilizará las recomendaciones descritas en el marco de trabajo de COBIT.

MODELO DE MEDICIÓN DEL DESEMPEÑO

La medición del desempeño es esencial para el gobierno de TI. COBIT le da soporte e incluye el establecimiento y el monitoreo de objetivos que se puedan medir, referentes a lo que los procesos de TI requieren generar (resultado del proceso) y cómo lo generan (capacidad y desempeño del proceso).

Indicador de Desempeño $(\boldsymbol{d})$

El indicador de desempeño se obtendrá en base a los parámetros y matrices especificados en la Tabla 4.8.

INDICADOR DE DESEMPEÑO		
PARAMETRO		MATRIZ
1	Grado de Desempeño Real $(\boldsymbol{d_r})$	Matriz de Nivel de Servicio – SUPERTEL.
2	Grado de Desempeño COBIT $(\boldsymbol{d_c})$	Matriz de Evaluación de Procesos bajo métricas COBIT.

Tabla 4.8*Parámetros del Indicador de Desempeño.*

El indicador de desempeño se obtendrá del promedio de los dos parámetros: desempeño real y desempeño COBIT, quedando la expresión como sigue:

$$d = \frac{d_r + d_c}{2}$$

donde: d_r= desempeño real, d_c=desempeño COBIT.

MODELO DE MEDICIÓN DE LOS OBJETIVOS DE CONTROL

Como se vio anteriormente COBIT plantea 34 objetivos de control generales, uno para cada proceso, y varios objetivos detallados para cada uno de ellos. El modelo de medición de los objetivos de control evalúa el grado de efectividad y madurez de los objetivos de control detallados pertenecientes a cada proceso.

Indicador de Cumplimiento de los Objetivos $(\boldsymbol{o})$

El indicador de cumplimiento de los objetivos por proceso, se obtendrá evaluando cada uno de los objetivos detallados, obteniendo un parámetro único correspondiente al porcentaje de cumplimiento del objetivo de control. Ver Tabla 4.9.

INDICADOR DE CUMPLIMIENTO DE LOS OBJETIVOS		
PARAMETRO		MATRIZ
1	Grado de Cumplimiento de los Objetivos de Control Detallados (p)	Matriz Cumplimiento de Objetivos de Control – COBIT

Tabla 4.9*Parámetros del Indicador de Cumplimiento de Objetivos.*

Al emplear un solo parámetro para el cálculo de este indicador, la correspondencia es directa

$$o = p$$

MODELO DE IMPACTO

Este modelo involucra tanto la importancia de un proceso dentro de la SUPERTEL como el impacto determinado por el marco de referencia COBIT para cada uno de ellos. Una combinación de estos dos parámetros proporcionará un impacto real de un determinado proceso dentro de TI.

Indicador de Impacto $(\boldsymbol{I})$

Se calculará efectuando un promedio del Impacto de los procesos frente a los criterios de información de COBIT, con el valor de la importancia del proceso dentro de la institución, como lo muestra la Tabla 4.10.

INDICADOR DE IMPACTO		
PARAMETRO		MATRIZ
1	Grado de Impacto (I_c)	Matriz de Impactos de Procesos frente a los criterios de información de COBIT
2	Grado de Importancia (I_s)	Matriz de Diagnostico de Procesos – SUPERTEL

Tabla 4.10 *Parámetros del Indicador de Impacto.*

$$\boldsymbol{I} = \frac{\boldsymbol{I_c} + \boldsymbol{I_s}}{2}$$

donde$\boldsymbol{I}$ = Impacto real, $\boldsymbol{I_c}$= Impacto - COBIT, $\boldsymbol{I_s}$= Importancia-SUPERTEL

4.4 Descripción del Mapa de Relación COBIT - SUPERTEL

El Mapa de Relación COBIT – SUPERTEL permitirá relacionar las metas de la institución y metas TI, con los procesos y criterios de información de COBIT. Se proporcionan cinco planos basados en las directrices de COBIT 4.1, que proporcionarán las equivalencias entre los procesos de TI de COBIT y las cinco áreas focales del gobierno de TI, los recursos de TI, las metas de TI y los criterios de información. Estos planos emplearán la P cuando exista una relación primaria y la S cuando solamente exista una relación secundaria. El hecho de que no exista una P ni una S no significa que no exista relación, sólo que es menos importante o marginal. COBIT 4.1 muestra un mapeo entre estos componentes, sin embargo, recomienda que se analicen nuevamente estos mapas dentro de cada institución, razón por la cual, los planos serán desarrollados en la etapa de ejecución de la auditoría.

Plano de Enlace de las Metas de la Institución, Metas TI y Criterios de Información

Esta matriz muestra las equivalencias de las metas de la institución (Ver Tabla 4.3), de acuerdo al BalancedScorecard, con las metas de TI– COBIT (Ver Tabla 4.4) y con los criterios de información de COBIT. Esto ayuda a mostrar, para una meta genérica de la institución, las metas de TI que por lo general dan soporte a esta meta, y los criterios de información de COBIT que se relacionan con la meta de la institución.Los criterios de información empleados fueron: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. La información adquirida durante la ejecución de la auditoría sobre éste plano se encuentra en el CD: Anexo 3 - Tabla A3.1.

Plano de Enlace de las Metas TI, Procesos COBIT y Criterios de Información

Muestra las equivalencias de las metas de TI - COBIT (Ver Tabla 4.4) con los procesos de TI de COBIT, así como los criterios de información sobre los cuales se basa la meta de TI. Esta información se encuentra en el CD: Anexo 3 - Tabla A3.2.

Plano de Enlace Procesos de COBIT a Metas de TI

Proporciona un mapeo inverso que muestra para cada proceso de COBIT, las metas de TI – COBIT (Ver Tabla 4.4) que son soportadas. La información adquirida durante la ejecución de la auditoría sobre éste plano se encuentra en el CD: Anexo 3 - Tabla A3.3.

Plano de Enlace de Procesos COBIT a Gobierno de TI y Criterios de Información

Este plano toma los procesos de TI listados en la Tabla 4.2, los relaciona con los criterios de información de COBIT (efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad) y con los áreas de enfoque de gobierno de TI (alineación estratégica, entrega de valor, gestión de riesgos, gestión de recursos y medición del desempeño). La información adquirida durante la ejecución de la auditoría sobre éste plano se encuentra en el CD: Anexo 3 - Tabla A3.4.

Plano de Responsabilidades de Procesos COBIT

Establece los responsables directos de cada proceso COBIT (Ver Tabla 4.2), de acuerdo al área encargada del proceso, en donde se incluyen los siguientes criterios:

Área Encargada del proceso	Unidad de TI, Dentro de la Institución, Externo, No se sabe con certeza

La información adquirida durante la ejecución de la auditoría sobre éste plano se encuentra en el CD: Anexo 3 - Tabla A3.5.

4.5 Descripción de las Matrices

Matriz de Grados de Madurez de Procesos - SUPERTEL

El modelo de madurez para la administración y el control de los procesos de TI de acuerdo a COBIT se basa en un método de evaluación de la institución, en una escala simple que muestra como un proceso evoluciona desde una capacidad no existente (0), hasta una capacidad optimizada (5).El modelo genérico de madurez propuesto por COBIT se muestra en la Tabla 4.7

El modelo de madurez a emplearse para la auditoría informática a la SUPERTEL, tomará los principios de COBIT, que a diferencia de la aproximación del CMM, CapabilityMaturityModel visto en el Capitulo II, no mide los niveles de forma precisa, ni certifica que un nivel se ha conseguido con exactitud. Una evaluación de la madurez bajo COBIT resultará en un perfil donde condiciones relevantes a diferentes niveles de madurez se han conseguido, es decir algunos procesos estarán en diferentes grados de madurez de acuerdo a como se hayan completado los objetivos, metas y actividades correspondientes a dicho proceso.

MODELO GENERICO DE MADUREZ COBIT		
0	No Existente	Carencia completa de cualquier proceso reconocible. La institución no ha reconocido siquiera que existe un problema a resolver.
1	Inicial	Existe evidencia que la institución 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 instituciones. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la institución se adapte de manera rápida.

Tabla 4.7*Modelo Genérico de Madurez – COBIT.* (COBIT 4.1, 2007)

Las equivalencias porcentuales para cada nivel se obtendrán de la siguiente manera:

$$v_i = \frac{100}{N_i} n_i$$

Donde:

v_i=valor porcentual del nivel i
N_i=numero total de características consideradas en el nivel i
n_i=numero de características que se cumplen en el nivel i

Los datos serán colocados en una tabla que mantenga un control de niveles por cada proceso.

El nivel de madurez alcanzado corresponderá a aquel nivel que tenga el mayor grado de madurez calculado. Esto es debido a que cada una de las características de los niveles describen el cumplimiento de hechos que sitúan a un proceso en determinado nivel.

$$m_r = Mayor(v_0, v_1, v_2, v_3, v_4, v_5)$$
$$n_r \Leftrightarrow m_r$$

dondem_r=Grado de Madurez Real, $v_0, v_1, v_2, v_3, v_4, v_5$=Valores porcentuales de los niveles del 0-5 respectivamente, n_r=Nivel de Madurez Real.

Los resultados obtenidos de cada proceso se resumirán en una Matriz de Grados de Madurez de Procesos – SUPERTEL que tendrá el grado y nivel de madurez para cada proceso COBIT. La información adquirida durante la ejecución de la auditoría para esta matriz se encuentra en el CD: Anexo 3 - Tabla A3.6.

Matriz de Nivel de Servicio – SUPERTEL

Evalúa el desempeño de cada uno de los procesos COBIT, de acuerdo al siguiente criterio:

Desempeño	Nivel de resultados que se está obteniendo de las actividades realizadas.

El parámetro desempeño es utilizado para el cálculo del indicador del mismo nombre, para lo cual se emplearán las equivalencias cuantitativas mostradas en la Tabla 4.8

EQUIVALENCIAS DEL DESEMPEÑO		
DESEMPEÑO		**CUMPLIMIENTO DE OBJETIVOS COBIT GENERALES**
No existe	0	No Cumple
Deficiente	1-20	Cumple Levemente
Regular	21-40	Cumple Parcialmente
Satisfactorio	41-60	Cumple Mayoritariamente
Muy Bueno	61-80	Cumple casi totalmente
Excelente	81-100	Cumple Totalmente

Tabla 4.8*Equivalencias del Desempeño*

La información adquirida durante la ejecución de la auditoría para ésta matriz se encuentra en el CD: Anexo 3 - Tabla A3.7.

Para las encuestas a los usuarios se empleará una descripción del proceso y se evaluará su nivel de cumplimiento, para que exista un mejor entendimiento de los encuestados. Los resultados serán tabulados empleando las equivalencias correspondientes.

Matriz de Evaluación de Procesos bajo Métricas COBIT

COBIT proporciona para cada proceso de TI un objetivo de control de alto nivel, junto con las metas y métricas que deben emplearse. En base a las mediciones propuestas por el marco de referencia se establecieron métricas aplicables a TI de la SUPERTEL que son empleadas en esta matriz. Ya que para la obtención de los resultados se emplean técnicas de indagación, observación, y recavación tanto de los procesos, como de la información disponible, la calificación de cada métrica se hace en base a parámetros cuantitativos. Para obtener la equivalencia en el valor porcentual se emplearán los valores mostrados en la Tabla 4.9.

EQUIVALENCIAS PARA METRICAS COBIT	
No Cumple	0
Cumple levemente	1-20
Cumple parcialmente	21-40
Cumple mayoritariamente	41-60
Cumple casi totalmente	61-80
Cumple totalmente	81-100

Tabla 4.9*Equivalencias empleadas en las métricas COBIT.*

El valor real de la evaluación del proceso de acuerdo a las métricas COBIT se obtiene del promedio de los valores porcentuales de las metas individuales, y recibirá el nombre de Desempeño COBIT.

$$d_c = \frac{v_1 + v_2 + \cdots + v_n}{n}$$

Donde: d_c=Desempeño COBIT, $v_1, v_2, \dots, v_n$ valores de las métricas $1,2, \dots, n$ respectivamente.

Esta matriz proporcionará un indicador numérico obtenido en base a las métricas de COBIT. La información obtenida durante la ejecución de la auditoría para cada proceso y métrica de COBIT se encuentra en el CD: Anexo 3 - Tabla A3.8.

Matriz de Cumplimiento de Objetivos de Control – COBIT

COBIT plantea una serie de objetivos de control para cada uno de los 34 procesos listados en la Tabla 4.2. Durante la ejecución de la auditoría se determinó el cumplimiento de cada objetivo de control, esto se muestra en la Tabla A3.9 del Anexo 3 – CD.

Matriz de Impacto de Procesos frente a los criterios de información de COBIT

Esta matriz corresponde al impacto de los procesos frente a los siete criterios de información y recursos de TI bajo COBIT.

La nomenclatura cualitativa utilizada en los criterios de información para esta tabla será la que se expuso anteriormente en la Tabla 4.9. Sin embargo se hará una correspondencia cuantitativa para obtener los porcentajes de los criterios de información o el porcentaje de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. Se asignará un valor al grado de impacto Primario cuyo efecto es alto o fuerte, Secundario cuyo efecto es leve o medio, Terciario cuyo efecto es bajo y Blanco (vació), el cual no tiene ningún impacto, es decir, es nulo. Este porcentaje se establece en base a una propuesta metodológica establecida por una metodología de manejo de riesgos como es COSO.

COSO (SponsoringOrganizations of theTreadway) establece una ponderación para el grado de impacto que tienen los criterios de información dentro de un proceso, además de permitir determinar el nivel de riesgo que tendría dicho proceso, para lo cual establece rangos de calificación para los niveles bajo, medio alto; como se puede apreciar en la Tabla 4.10.

INTERPRETACION DE IMPACTOS - COSO	
IMPACTO	**RANGO DE CALIFICACION**
Bajo	15%-50%
Medio	51%-75%
Alto	76%-95%
Vacío	-

Tabla 4.10*Interpretación de los Impactos de acuerdo a COSO.*

Tomando en cuenta la propuesta de COSO se ha generado una tabla de ponderaciones mediante la cual se propone asignar un valor numérico al impacto de los criterios de información de cada proceso, para esto se ha determinado tomar el valor promedio de cada uno de los rangos, eliminando así la subjetividad el momento en que se asigna un valor numérico al impacto, dando como resultado la Tabla 4.11.

EQUIVALENCIAS DEL IMPACTO

IMPACTO	PROMEDIO
Bajo	32%
Medio	63%
Alto	86%

Tabla 4.11*Equivalencias del Impacto.*

A continuación se colocarán los valores obtenidos en los criterios de Información que establece COBIT, dentro de cada uno de los procesos, para el grado de impacto Primario se asigna el 86%, cuyo impacto es alto, para el grado secundario se asigna el 63% cuyo impacto es medio, para el grado terciario se asigna 32% cuyo impacto es bajo y para el caso en que la casilla se encuentre en blanco (vació), no se asignara ningún valor, ya que no impacta en nada a los criterios de información, según lo que especifica COBIT. Finalmente una vez que se han especificados los valores a cada uno de los Criterios de información se procederá a utilizarlos en el cálculo del porcentaje de impacto, en donde intervendrán los criterios de efectividad y eficiencia. El porcentaje del impacto estará dado por el promedio del impacto de estos dos criterios de información

$$I = i_e + i_i$$

Donde I =Impacto, i_e=Impacto de la efEctividad, i_i=impacto de la eficiencia

La matriz de impacto de procesos, además de determinar un indicador numérico para cada criterio de información de COBIT y un porcentaje de impacto global, establecerá una relación con los recursos de TI empleados, considerando: personas, información, aplicaciones e infraestructura. Esta matriz se encuentra en el CD: Anexo 3 - Tabla A3.10.

Matriz de Diagnóstico de Procesos COBIT

Ayudará a determinar la importancia, el fundamento y los controles que se están realizando en cada uno de los procesos, de acuerdo a los siguientes criterios:

Importancia	Nivel de trascendencia de los procesos. (Poco importante, importante, Muy importante)
Formalizado	Se refiere a si existe algún documento que norme la forma de realizar la actividad consultada(No Formalizado, Formalizado, No, No aplica, No se sabe con certeza)
Control Interno	Se refiere a la documentación formal aprobada y difundida en la institución sobre las actividades realizadas y consultadas. (No Documentado, Documentado, No se sabe con certeza)
Auditado	(No Auditado, Auditado, No se sabe con certeza)

El parámetro de importancia se emplea en el cálculo del indicador de impacto para lo cual se emplean las equivalenciasmostradas en la Tabla 4.12

EQUIVALENCIAS DE IMPORTANCIA

Poco Importante	33%
Importante	67%
Muy Importante	100%

Tabla 4.12*Equivalencias Cuantitativas de la Importancia.*

La información de esta matriz desarrollada durante el proceso de auditoría se encuentra en el CD: Anexo 3, Tabla A3.11.

4.6 Determinación de Resultados y Productos de la Auditoría

Los resultados de la auditoría informática a la SUPERTEL se verán reflejados en el informe final y la carta de presentación, los mismos que presentarán el análisis de cada uno de los procesos basados en los productos obtenidos durante la ejecución de la auditoría.

PRODUCTOS DE LA AUDITORIA

Los productos de la auditoría informática, se agrupan en dos ámbitos conceptuales, planos y matrices, los primeros permitirán establecer las relaciones entre los procesos pertenecientes a la metodología aplicada COBIT y los procesos de la Superintendencia de Telecomunicaciones. Las matrices en cambio muestran indicadores cualitativos y/o cuantitativos que reflejan una situación sobre cada proceso u objetivo de control de COBIT. Un resumen se muestra en la Figura 4.2.

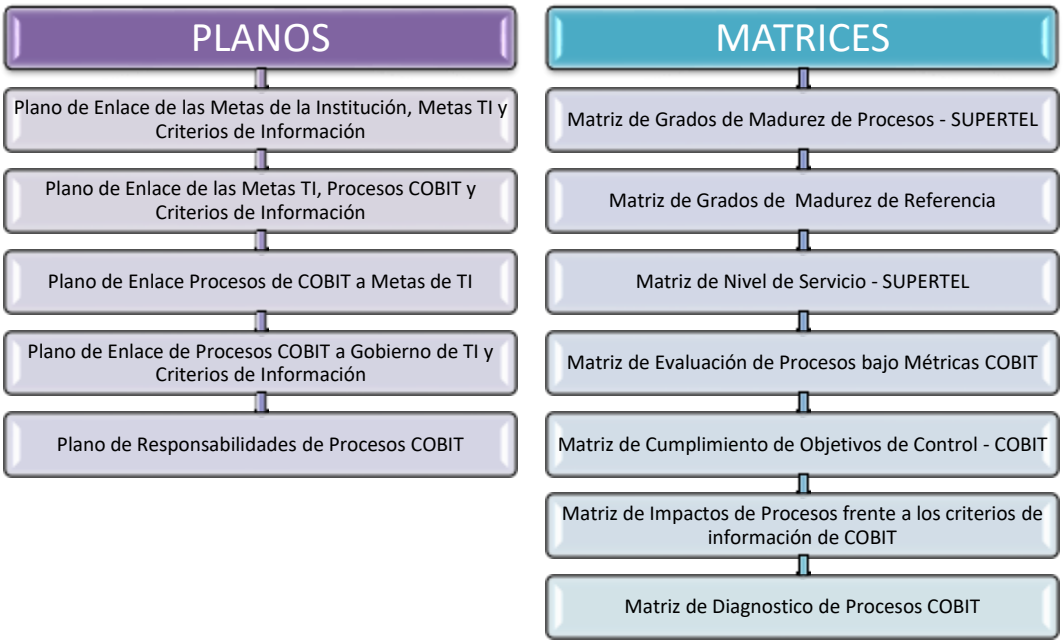

Figura 4.2*Productos de Auditoría Informática para la SUPERTEL*.

RESULTADOS

Los resultados de la auditoría se verán reflejados en los dos únicos documentos entregables, el informe final y la carta de presentación, los cuales serán los únicos elementos constatables de la realización de la auditoría. Ver Figura 4.3. El informe final describirá de manera detallada el análisis, resultados, recomendaciones e indicadores obtenidos para cada uno de los procesos COBIT. La carta de presentación llevará un resumen del informe de auditoría.

Figura 4.3*Resultados de Auditoría Informática para la SUPERTEL.*

4.7 Recursos para la auditoría

Una de las partes más importantes dentro de la planeación de la auditoria en informática es el personal que deberá participar. Uno de los esquemas generalmente aceptados para tener un grupo adecuado que intervenga en el proceso, es que esté debidamente capacitado, tenga disponibilidad y un alto sentido de moralidad, que pueda proporcionar toda la información que se solicite, coordinar las reuniones y entrevistas requeridas.

Éste es un punto muy importante ya que, de no tener el apoyo de la alta dirección ni contar con un grupo multidisciplinario en el cual estén presentes una o varias personas del área a auditar, sería casi imposible obtener información en el momento y con las características deseadas.

También se debe contar con personas asignadas a nivel de usuarios para que en el momento que se solicite información o bien se efectúe alguna entrevista de comprobación de hipótesis, nos proporcionen aquello que se está solicitando, y complementen el grupo multidisciplinario; ya no sólo se analizará el punto de vista de la dirección de informática, sino también el de los usuarios. Se establecen tres categorías para la realización de la auditoría:

- *Responsable de la auditoría:* Cumplirá con las tareas de coordinación de actividades con la institución, de obtención de las facilidades para el acceso a la información y la documentación de soporte para toda la auditoría. Ing. Verónica Quintuña

- *Auditor:* Cumplirá con las tareas de recopilación, sistematización, y análisis de la información. Deberá tener conocimiento de la metodología COBIT y su aplicación. Ing. Verónica Quintuña Rodríguez

- *Auditados:* Brindarán la información requerida y coordinarán actividades que se requieran para el cumplimiento del plan y programa de auditoría. La selección de la muestra de auditados se realizará a continuación.

Selección de la Muestra de Auditados

Para la realización de la auditoría a la Unidad de TI de la SUPERTEL, se realizará la selección de un grupo de personas que proporcionen los datos que reflejen las vivencias del encuestado en sus áreas de trabajo. Ver Figura 4.4.

De acuerdo al número de funcionarios de la SUPERTEL que son 349, es necesario aplicar una teoría de muestreo con enfoque matemático para la tabulación, se usará una selección de la muestra estratificada a partir de la población seleccionada.

$$n_0 = \left(\frac{Z}{\epsilon}\right)^2 * p * q$$

$$\mathrm{n} = \frac{n_0}{1 + \frac{n_0}{N}}$$

donde:
n_0: Cantidad teórica de elementos de la muestra.
n: Cantidad real de elementos de la muestra a partir de la población asumida
N: Número total de elementos que conforman la población. $N = 234$
z: Valor estandarizado en función del grado de confiabilidad de la muestra calculada. Para una confiabilidad de 95%, $z = 1.96$
ϵ: Error asumido en el cálculo. Para $N > 10$. Se asume $\epsilon = 0.05$ (un error del 5 %).
q: Probabilidad de la población que no presenta las características universales. Para $N \geq 160$. Se asume $q = 0.05 - 0.20$. (5 al 20%). Se asumirá un valor del 5% debido a que ya se ha excluido de la población a funcionarios auxiliares que no aportarían en la determinación de resultados. (ayudantes de oficina, conductores, entre otros). La probabilidad de que la población considerada no represente las características comunes será la mínima recomendada.
p: Probabilidad de la población que presenta las características universales.

$$p = 1 - q = 1 - 0.05 = 0.95$$

De acuerdo a los parámetros especificados, se calculará el tamaño de la muestra, quedando como sigue:

Figura 4.4*Selección de la Muestra de Auditados.*

$$n_0 = \left(\frac{Z}{\epsilon}\right)^2 * p * q = \left(\frac{1.96}{0.05}\right)^2 * 0.95 * 0.05 = 72.99$$

$$n = \frac{n_0}{1 + \frac{n_0}{N}} = \frac{72.99}{1 + \frac{72.99}{2\,65}} = 57.23 \sim 58$$

El tamaño de la muestra calculado corresponde a 58 personas que intervendrán en la encuesta, teniendo una población de 265 usuarios de tecnología de información, que forman parte de un total de 349 funcionarios de la Superintendencia de Telecomunicaciones. La muestra corresponde al 21.89% de la población. La Tabla 4.13 detalla el tamaño de las muestras por cada grupo definido por COBIT y de acuerdo a las unidades de la SUPERTEL. Los grupos considerados y sugeridos por COBIT, son:

DIRECTORIO: Para conocer la opinión de cuáles son los temas de mayor interés a nivel de autoridades y directivos.

UNIDAD DE TI: Constituye el ente que está siendo evaluado, por lo tanto es importante la opinión de ellos en las prioridades de la información recopilada.

USUARIOS: Proporcionan las pautas para evaluar el funcionamiento de sistemas, procesos, servicios y equipos de TI.

SELECCIÓN DE LA MUESTRA			
GRUPOS	**PARTICIPANTES**	**POBLACIÓN**	**MUESTRA**
DIRECTORIO	Directivos	27	6
TECNOLOGÍA DE LA INFORMACIÓN	Informáticos	22	5
USUARIOS	Administrativos	59	13
	Técnicos	119	26
	Jurídicos	23	5
	Financiero	15	3
TOTAL MUESTRA		**265**	**58**
OTROS		84	0
TOTAL FUNCIONARIOS		**349**	

Tabla 4.13*Selección de la muestra.*

Con esto estamos indicando que se 58 usuarios serán encuestados bajo diferentes cuestionarios, lo que permitirá definir las prioridades y la profundidad con la que se tratarán los procesos del marco de referencia COBIT sujetos a la auditoría.

Antes de empezar a recopilar los datos se ha preparado a los funcionarios y a los directivos para explicar lo que significa aplicar la metodología COBIT en la institución, qué beneficios se pueden obtener, cuáles son las áreas en las cuales se enfocará el estudio y cuál es el proceso que se seguirá.

De acuerdo a la planificación, la auditoría empleará cuestionarios, entrevistas, recopilación de información, y análisis de la misma. Por lo tanto se requerirá lo siguiente:

- Hardware: Computador de Características Generales, para la documentación y almacenamiento de resultados y actividades desarrolladas en el proceso de auditoría.

- Software: Los programas que servirán de apoyo para este trabajo de auditoría son los siguientes: procesadores de texto, hojas de cálculo, herramientas para generación y edición de gráficos, browsers.

4.8 Programa de auditoría

El programa de auditoria constituye un instrumento metodológico que guiara el proceso de análisis y determinación de cada uno de los parámetros que se evalúan dentro de los modelos contemplados en la estrategia. La aplicación de los Modelos basados en los procesos y objetivos de control propuestos por COBIT, permitirán cubrir políticas, planes y procesos en el área de tecnologías de la información, así como también el desempeño de equipos y sistemas, la satisfacción de los usuarios y el alineamiento con los objetivos estratégicos de la institución. El Programa planteado se detalla en la Tabla 4.14

PROGRAMA DE AUDITORIA		
MODELO	**PRODUCTO**	**TECNICA**
Mapa de Relación COBIT-SUPERTEL	Plano de Enlace de las Metas de la Institución, Metas TI y Criterios de Información	Se obtiene del análisis de la información de la Superintendencia de telecomunicaciones, observaciones, indagación, entrevistas y encuestas para recabar información.
	Plano de Enlace de las Metas TI, Procesos COBIT y Criterios de Información	
	Plano de Enlace Procesos de COBIT a Metas de TI	
	Plano de Enlace de Procesos COBIT a Gobierno de TI y Criterios de Información	
	Plano de Responsabilidades de Procesos COBIT	
Modelo de Madurez	Matriz de Grados de Madurez de Procesos – SUPERTEL	Se obtiene del análisis la información, observaciones, entrevistas y encuestas realizadas para recabar información
	Matriz de Grados de Madurez de Referencia	Obtenida del nivel de exigencia de los usuarios de TI de la SUPERTEL
Modelo de Desempeño	Matriz de Nivel de Servicio – SUPERTEL	Obtenida mediante encuestas
	Matriz de Evaluación de Procesos bajo Métricas COBIT	Obtenida mediante mediciones, evaluaciones, observaciones y análisis
Modelo de Cumplimiento de Objetivos	Matriz de Cumplimiento de Objetivos de Control – COBIT	Obtenida del análisis y observación del cumplimiento y desempeño de cada objetivo de control detallado.
Modelo de Impactos	Matriz de Impactos de Procesos frente a los criterios de información de COBIT	Marco de Referencia COBIT aplicado a la Superintendencia de Telecomunicaciones
	Matriz de Diagnostico de Procesos COBIT	Se obtiene mediante encuestas y análisis de información.

Tabla 4.14*Programa de Auditoría*

4.9 Cronograma de actividades para la Auditoría

El control del avance de la auditoria es fundamental para el logro eficiente de la misma por lo que se ha elaborado un cronograma de ejecución que define las tareas y tiempos asignados para su cumplimiento, lo cual permitirá el seguimiento a los procedimientos de control así como también permitirá asegurarse de que el trabajo se esta llevando a cabo de acuerdo con el programa de auditoria, con los recursos estimados y en el tiempo señalado en la planeación. En la Tabla 4.15 se detalla toda la planificación de la auditoría.

CRONOGRAMA DE ACTIVIDADES	
TAREA	**TIEMPO**
AUDITORÍA SUPERTEL	Días
ESTUDIO PRELIMINAR	75
Solicitud de la Información	10

Recopilación de información	20
Ordenamiento de la Información	15
Elaboración de cuestionarios	15
Realización de Encuestas y Entrevistas	15
PLANEACIÓN DE LA AUDITORIA	87
Comprensión del Control Interno	10
Desarrollo de la estrategia de auditoría	30
Determinación de los Resultados y productos de la auditoría	20
Determinación de los recursos necesarios para realizar la auditoría de sistemas.	10
Elaboración los Programas de Trabajo	15
Cronograma	2
EJECUCIÓN DE LA AUDITORIA	120
Entrevistas a líderes y usuarios mas relevantes de la dirección de TI	15
Entrevistas y encuestas a usuarios.	15
Determinación del Mapa de Relación COBIT-SUPERTEL	15
Ejecución de los Modelos de Madurez, Desempeño, Impacto y Riesgo	15
Evaluación y análisis del dominio planeación y organización	15
Evaluación y análisis del dominio adquisición e implementación	15
Evaluación y análisis del dominio entrega y soporte	15
Evaluación y análisis del dominio monitoreo y evaluación	15
INFORME FINAL	50
Revisión de los papeles de trabajo.	10
Elaboración del Informe.	30
Elaboración de la carta de presentación	10
TOTAL	**332**

Tabla 4.15*Programa de Auditoría*

CAPITULO 5

INFORME DE AUDITORÍA

En el desarrollo del presente capítulo se encuentra detallada la carta de presentación, que forma parte del “Informe Final” y corresponde a la última fase de la auditoría. La carta de presentación muestra resultados globales de los 34 procesos COBIT que intervinieron durante la ejecución de la AI, sin embargo un detalle de los resultados e indicadores para cada uno de los procesos se encuentra en el Anexo 4.

5.1 Carta de Presentación de la Auditoría Informática

La Superintendencia de Telecomunicaciones, como ente gubernamental encargado de vigilar, auditar, intervenir y controlar técnicamente la prestación de los servicios de telecomunicaciones, radiodifusión, televisión y el uso del espectro radioeléctrico; cuenta con una infraestructura tecnológica muy amplia para solventar dichas tareas, y se soporta en el manejo de información que atiende cada uno de los procesos que forman parte del Modelo de Gestión por Procesos Institucional, a través de la Unidad de Tecnología de Información.

La auditoría informática ha permitido evaluar el uso de la tecnología de la información en los procesos institucionales, y determinar indicadores de la situación actual, analizar tendencias, puntos débiles y amenazas, para emitir recomendaciones que permitan mantener una optimización constante de las tecnologías de la información en la institución.

El proceso de auditoría se desarrolló bajo el marco de referencia COBIT (Control ObjectivesforInformation and relatedTecnology) por ser un estándar que asocia las mejores prácticas para el control de TI y para la implementación de Gobierno de TI; ya que permite asociar los conceptos de requerimientos de control, consideraciones técnicas y riesgos institucionales. Estas características lo han posicionado como uno de los modelos más utilizados en el mundo, por usuarios, directivos y auditores.
Los temas que han sido objeto de la auditoría corresponden a treinta y cuatro procesos COBIT, que cubren todos los aspectos involucrados en Tecnología de la información y se agrupan en cuatro categorías: PLANEACIÓN Y ORGANIZACIÓN

(PO), ADQUISICIÓN E IMPLEMENTACIÓN (AI), ENTREGA Y SOPORTE (DS), MONITOREO Y EVALUACIÓN (ME).

La auditoría ha atendido estos temas a través de un conjunto de matrices que registran indicadores cualitativos y cuantitativos resultantes de la aplicación de modelos, y mediciones, que a su vez emplean para su construcción, diversas técnicas de auditoría como observaciones, entrevistas, indagaciones, entre otros. Los modelos, planos y matrices empleados durante la ejecución de la auditoría han sido los siguientes:

Modelos de madurez, que han permitido determinar la situación actual de los procesos de TI e identificar las mejoras necesarias. Interviene:

- Matriz de Grados de Madurez de Procesos - SUPERTEL

Metas y mediciones de desempeño para los procesos de TI, que han permitido evaluar cómo los procesos satisfacen las necesidades de la SUPERTEL y de TI. Intervienen las siguientes matrices:

- Matriz de Nivel de Servicio – SUPERTEL. Parámetro Desempeño
- Matriz de Evaluación de Procesos bajo Métricas COBIT

Mediciones de objetivos de control de manera que determinen el estado real de la ejecución de los procesos para facilitar su desempeño. Interviene la siguiente matriz:

- Matriz de Cumplimiento de Objetivos de Control – COBIT

Determinación del nivel de impacto de cada uno de los procesos en la institución. Intervienen las siguientes matrices:

- Matriz de Impactos de Procesos frente a los criterios de información de COBIT.
- Matriz de Diagnóstico de Procesos COBIT

Con el fin de enlazar los procesos de tecnologías de información estándares planteados por COBIT con los procesos de TI institucionales, se desarrolló un MAPA DE RELACIÓN COBIT-SUPERTEL, el cual está conformado por cinco planos:

- Plano de Enlace de las Metas de la Institución, Metas TI y Criterios de Información
- Plano de Enlace de las Metas TI, Procesos COBIT y Criterios de Información
- Plano de Enlace Procesos de COBIT a Metas de TI
- Plano de Enlace de Procesos COBIT a Gobierno de TI y Criterios de Información
- Plano de Responsabilidades de Procesos COBIT

Análisis de Resultados

El análisis general y los resultados de los 34 procesos COBIT agrupados en las

categorías: Planeación y Organización (PO), Adquisición e Implementación (AI), Entrega y Soporte (S) y Monitoreo y Evaluación (ME), se presentan en las Tablas 6.1, 6.2, 6.3, y 6.4 respectivamente. Cada tabla sintetiza el objetivo del proceso, las tendencias, fortalezas, debilidades y recomendaciones, así como también determina el estado del proceso en base a indicadores. El indicador global C, junto con el grado de impacto representan de manera general el estado real del proceso, estos valores serán ilustrados más adelante mediante gráficas, en donde el tamaño de la esfera que ubica al indicador global en la escala porcentual, representa el impacto; a menor tamaño, menor impacto.

PO	**PLANEAR Y ORGANIZAR**	**ESTADO DEL PROCESO**		**IMPACTO**
		$C = 68{,}72\%$	$\alpha = 59{,}73\%$ $\beta = 55{,}73\%$ $\gamma = 49{,}09\%$	Alto
OBJETIVO	Identificar la manera en que TI puede contribuir de la mejor manera al logro de los objetivos institucionales. Se debe implementar una estructura organizacional y una estructura tecnológica apropiada.			
SITUACION ACTUAL				
Indicador de Madurez	NIVEL 3	DEFINIDO		
Indicador de Desempeño	$d = 67{,}03\%$	Grado de Desempeño Real	$d_r = 58{,}59\%$	
	MUYBUENO	Grado de Desempeño COBIT	$d_c = 75{,}46\%$	
Indicador de Cumplimiento de Objetivos de Control	$o = 77{,}09\%$			
	CUMPLE CASI TOTALMENTE			
Impacto	$I = 70{,}77\%$	Grado de Impacto	$I_c = 71{,}44\%$	
	ALTO	Grado de Importancia	$I_s = 70{,}10\%$	
Formalizado / Normado		**Control Interno**	Documentado	**Responsable** Unidad de TI
TENDENCIAS	Proporcionar dirección para la entrega de soluciones y la entrega de servicios.			
FORTALEZAS	TI posee un marco de trabajo que define las metodologías adoptadas y aplicadas a cada proyecto, incluyendo puntos de control, evaluación de riesgos, y gestión de cambios.			
PUNTOS DEBILES Y AMENAZAS	TI identifica amenazas y vulnerabilidades sin embargo no cubre totalmente el abanico de riesgos para garantizar la operatividad y que además se tome en cuenta el costo beneficio de la seguridad.			
RECOMENDACIONES	Mantener siempre alineadas las estrategias de TI y de la institución. Optimizar el uso de los recursos. Fomentar una cultura institucional de apertura hacia TI. Administrar los riesgos de TI. Administrar la calidad de los sistemas de TI, para solventar las necesidades institucionales.			

Tabla 6.1*Indicadores del Proceso Planear y Organizar.(Basado en COBIT 4.1, 2007)*

AI	**ADQUIRIR E IMPLEMENTAR**	**ESTADO DEL PROCESO**		**IMPACTO**
		$C = 67{,}95\%$	$\alpha = 59{,}35$ $\beta = 56{,}70$	Alto

			$\gamma = 48{,}53$	
OBJETIVO	Garantizar que la estrategia de TI y los objetivos institucionales se lleven a cabo dentro de un marco de soluciones de TI efectivo, las mismas que necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos institucionales.			
SITUACION ACTUAL				
Indicador de Madurez	NIVEL 3	DEFINIDO		
Indicador de Desempeño	$d = 64{,}62\%$	Grado de Desempeño Real		$d_r = 58{,}03\%$
	MUY BUENO	Grado de Desempeño COBIT		$d_c = 71{,}20\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 77{,}94\%$			
	CUMPLE CASI TOTALMENTE			
Impacto	$I = 78{,}00\%$	Grado de Impacto		$I_c = 79{,}71\%$
	ALTO	Grado de Importancia		$I_s = 76{,}29\%$
Formalizado / Normado		**Control Interno**	Documentado	**Responsable** Unidad de TI
TENDENCIAS	Proporcionar soluciones y convertirlas en servicios.			
FORTALEZAS	TI posee un plan para adquirir, implementar y mantener la infraestructura tecnológica considerando los riesgos tecnológicos, y la vida útil de la inversión.			
PUNTOS DEBILES Y AMENAZAS	Los procesos para definir, y autorizar los cambios de manera oportuna no son estándares y si se los realiza de manera formal pueden tardar mas delo debido.			
RECOMENDACIONES	Orientarlas soluciones a satisfacer de manera óptima los procesos institucionales. Administrar el portafolio de proyecto bajo cronogramas bien definidos, de manera que los proyectos sean entregados a tiempo. Asegurar, la integración de nuevos sistemas de manera que interactúen con los ya existentes y no afecten las operaciones actuales.			

Tabla 6.2*Indicadores del Proceso Adquisición e Implementación.(Basado en COBIT 4.1, 2007)*

En la obtención del indicador global intervienen tres indicadores parciales correspondientes a madurez, desempeño y cumplimiento de objetivos de control COBIT. El indicador de madurez representa el grado de desarrollo de un determinado proceso, es decir que tan avanzada se encuentra su ejecución. El indicador de desempeño se refiere al grado de efectividad del proceso. Finalmente el indicador de cumplimiento de objetivos de control, es el resultante de la evaluación del proceso en base a métricas planteadas por COBIT. Cada uno de estos indicadores es el resultado de la integración de varios valores registrados en un conjunto de matrices COBIT y calculados en base a metodologías como se indicó en párrafos anteriores.[2]

		ESTADO DEL PROCESO		IMPACTO
DS	**ENTREGAR Y DAR SOPORTE**		$\alpha = 52{,}08$	
		$C = 75{,}15\%$	$\beta = 60{,}71$	Medio
			$\gamma = 51{,}77$	

[2]Un detalle de las metodologías y matrices COBIT que intervinieron en el proceso de auditoría se encuentra en el Capitulo 4, en donde se describe la Estrategia de la Auditoría Informática.

OBJETIVO	Entregar servicios y dar soporte a usuarios bajo un ambiente de seguridad, continuidad, y calidad.			
SITUACION ACTUAL				
Indicador de Madurez	NIVEL 4	ADMINISTRADO Y MEDIBLE		
Indicador de Desempeño	$d = 63{,}68\%$	Grado de Desempeño Real	$d_r = 63{,}32\%$	
	MUY BUENO	Grado de Desempeño COBIT	$d_c = 64{,}03\%$	
Indicador de Cumplimiento de Objetivos de Control	$o = 80{,}56\%$			
	CUMPLE CASI TOTALMENTE			
Impacto	$I = 60{,}16\%$	Grado de Impacto	$I_c = 66{,}46\%$	
	MEDIO	Grado de Importancia	$I_s = 53{,}85\%$	
Formalizado / Normado		**Control Interno**	Documentado	**Responsable** Unidad de TI
TENDENCIAS	Otorgar soluciones utilizables por usuarios finales			
FORTALEZAS	TI selecciona los centros de datos físicos considerando los riesgos asociados con desastres, ubicación del equipo crítico, áreas restringidas, las leyes y regulaciones de seguridad y salud ocupacional.			
PUNTOS DEBILES Y AMENAZAS	No se han creado procesos estándares para reportar y clasificar problemas que han sido identificados, incluyendo categorías, impacto, y prioridad.			
RECOMENDACIONES Y PLANES DE ACCIÓN	Definir un marco de trabajo que brinde un proceso formal de administración de niveles de servicio entre los funcionarios y TI, tomando en cuenta los criterios de desempeño para identificar tendencias positivas y negativas que permitan realizar mejoras Entregar los servicios de acuerdo con las prioridades institucionales. Optimizar los costos de TI Capacitar a los usuarios para que los sistemas se utilicen de forma productiva y segura. Vigilar de manera permanente que la confidencialidad, la integridad y la disponibilidad converjan.			

Tabla 6.3*Indicadores del Proceso Entregar y Dar Soporte.(Basado en COBIT 4.1, 2007)*

Los procesos involucrados en Planeación y Organización, tienen un alto impacto dentro del desenvolvimiento de tecnología de la información en la institución. Como se observa en la Figura 6.1 los temas de planificación presentan un cumplimiento del 77,94% en base a los objetivos de control COBIT, ya que la institución maneja de manera organizada, los planes estratégicos, tecnológicos y de trabajo, sin embargo se requiere fortalecer la administración de riesgos dentro de la planificación y administración de proyectos de TI. El grado de desempeño se encuentra un poco por debajo del indicador de cumplimiento, esto es 67,03%, ya que si bien se encuentran bien definidos los procesos, organización y relaciones de TI, así como los modelos de arquitectura de la información, dirección tecnológica y planes de inversión; los resultados de desempeño desde el punto de vista de los usuarios no cubren las expectativas de la planificación. El grado de madurez del 60% corresponde al tercer nivel planteado por COBIT, ya que los procesos de planificación y organización se encuentran completamente definidos, pero no completamente administrados y optimizados.

ME	**MONITOREAR Y EVALUAR**	**ESTADO DEL PROCESO**		**IMPACTO**
		$C = 70{,}43\%$	$\alpha = 60{,}54$	Alto
			$\beta = 59{,}05$	

			$\gamma = 45{,}37$		
OBJETIVO	Evaluar de forma regular los procesos de TI en cuanto a su calidad y cumplimiento de los requerimientos de control.				
SITUACION ACTUAL					
Indicador de Madurez	NIVEL 3	DEFINIDO			
Indicador de Desempeño	$d = 62{,}75\%$	Grado de Desempeño Real	$d_r = 65{,}49\%$		
	MUY BUENO	Grado de Desempeño COBIT	$d_c = 60{,}00\%$		
Indicador de Cumplimiento de Objetivos de Control	$o = 76{,}69\%$				
	CUMPLE CASI TOTALMENTE				
Impacto	$I = 76{,}38\%$	Grado de Impacto	$I_c = 86{,}00\%$		
	ALTO	Grado de Importancia	$I_s = 66{,}75\%$		
Formalizado / Normado		**Control Interno**	Documentado	**Responsable**	Unidad de TI
TENDENCIAS	Monitorear todos los procesos para asegurar que se sigue la dirección provista.				
FORTALEZAS	TI trabaja con el consejo directivo para garantizar que los programas de inversión habilitados por TI estén alineados con los objetivos institucionales.				
PUNTOS DEBILES Y AMENAZAS	Se monitorea esporádicamente la efectividad de los controles internos sobre TI por medio de revisiones de auditoría externa, y prácticas de benchmarking. (Comparar con modelos institucionales líderes a nivel mundial)				
RECOMENDACIONES	Medir el desempeño de TI para mantener un control preventivo.				

Tabla 6.4*Indicadores del proceso Medir y Evaluar. (Basado en COBIT 4.1, 2007)*

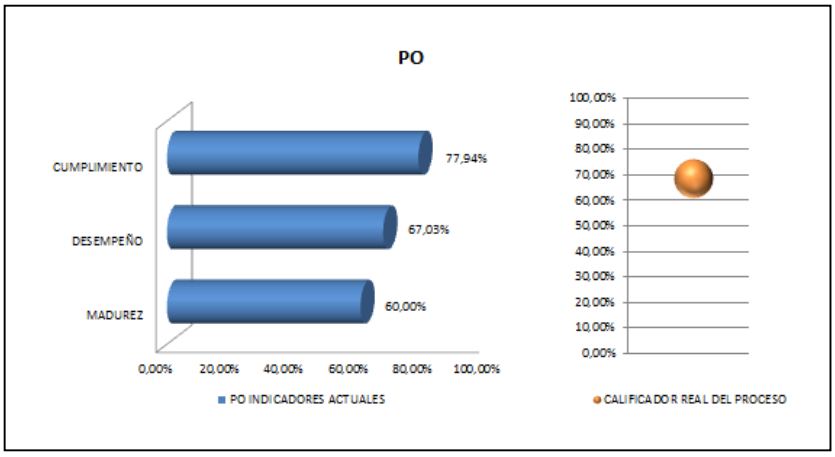

Figura 6.1*Indicadores del Proceso Planear y Organizar (PO).*

El objetivo de los procesos de Planeación y Organización es identificar la manera en que TI puede contribuir de la mejor manera al logro de los objetivos institucionales. Como se observa en las Figuras 6.2 y 6.3 el punto más débil corresponde al proceso PO9 que tiene como meta evaluar y administrar los riesgos, si bien, TI identifica amenazas y vulnerabilidades, sin embargo no cubre totalmente el abanico de riesgos para garantizar la operatividad y seguridad. Uno de los puntos más fuertes es PO10 que refleja una buena administración de proyectos de TI que mantiene la unidad de TI de la SUPERTEL ya que se cuenta con un marco de trabajo que define metodologías y estándares aplicables en cada proyecto.

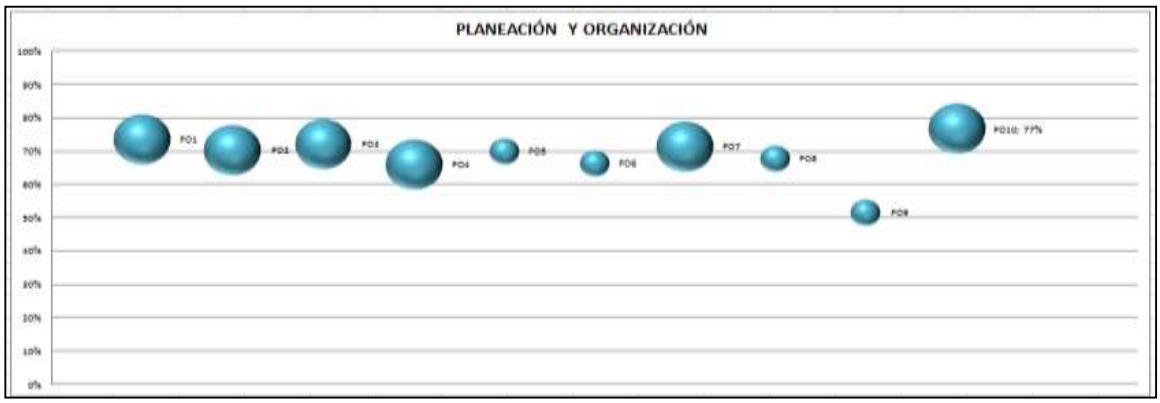

Figura 6.2*Calificador Real por Proceso Planear y Organizar.*

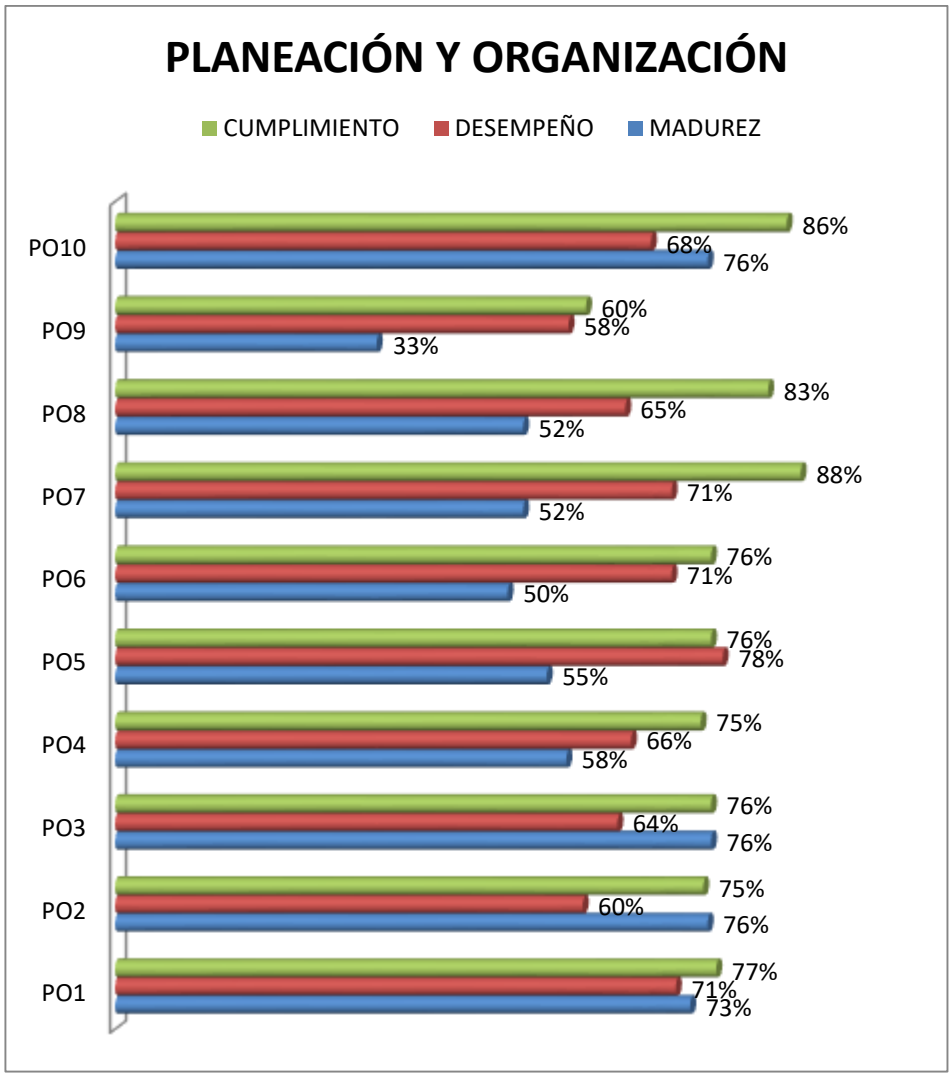

Figura 6.3*Indicadores por Proceso Planear y Organizar.*[3]

Los procesos de adquisición e implementación son también de alto impacto a nivel institucional; como se muestra en la Figura 6.4, el indicador global describe un estado de cumplimiento, madurez y desempeño correspondiente al 68% aproximadamente, lo cual permite garantizar mayoritariamente que la estrategia de TI y los objetivos institucionales se lleven a cabo dentro de un marco de soluciones de TI

[3]Para la descripción de cada proceso refiérase a la Tabla 4.2 Procesos y Objetivos de Control COBIT.

efectivo. El grado de madurez del proceso corresponde al nivel 3 de acuerdo a COBIT, esto es el proceso se encuentra claramente definido, sin embargo hacen falta procesos de control y optimización.

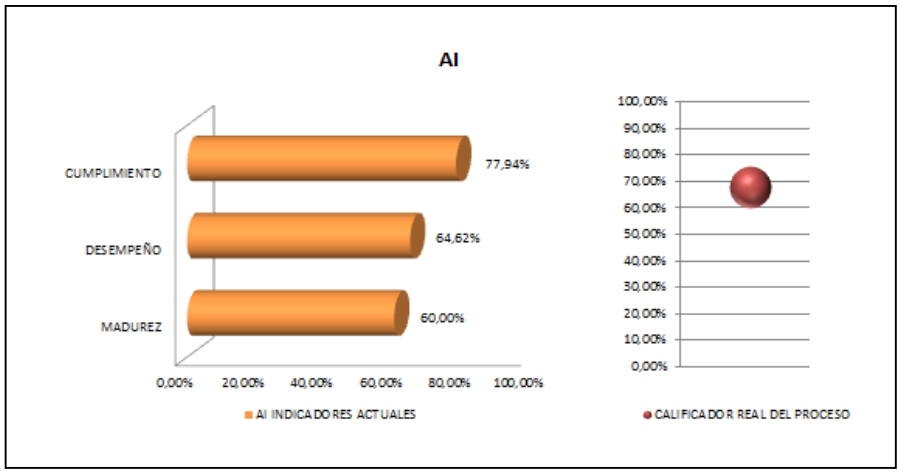

Figura 6.4*Indicadores del ProcesoAdquisición e Implementación (AI).*

Las Figuras 6.5 y 6.6 muestran como punto más débil al proceso AI2 y como punto más fuerte al proceso AI3, ambos de un impacto alto, a diferencia del proceso AI4 que tiene un impacto medio. AI2 corresponde a la adquisición y mantenimiento de software aplicativo, mientras que AI3 a la adquisición y mantenimiento de infraestructura tecnológica. En general, en este ámbito, la unidad de tecnología de la SUPERTEL mantiene planes de adquisición, implementación y mantenimiento de software e infraestructura tecnológica, sin embargo, al momento de autorizar y ejecutar cambios en base a procesos definidos, pueden demorar más de lo debido.

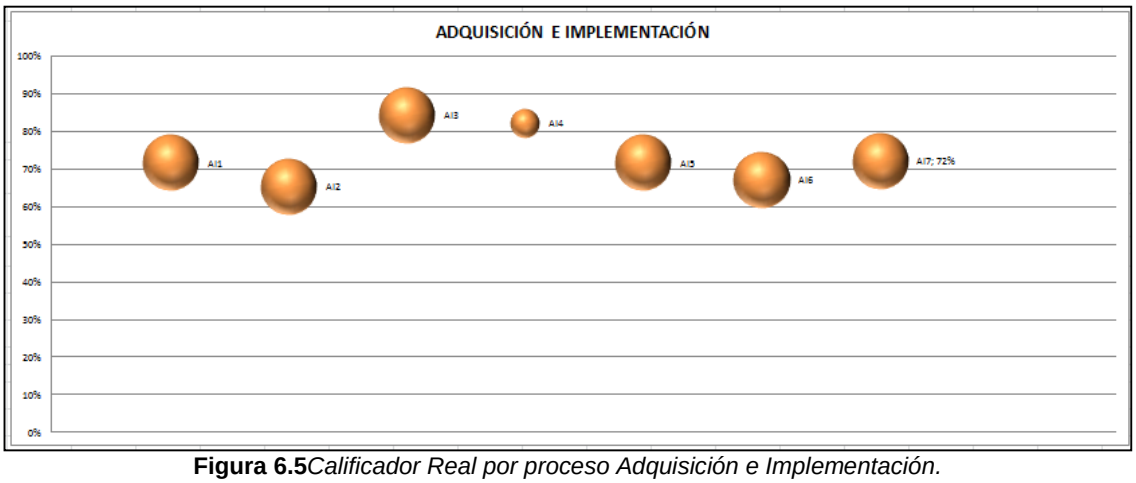

Figura 6.5*Calificador Real por proceso Adquisición e Implementación.*

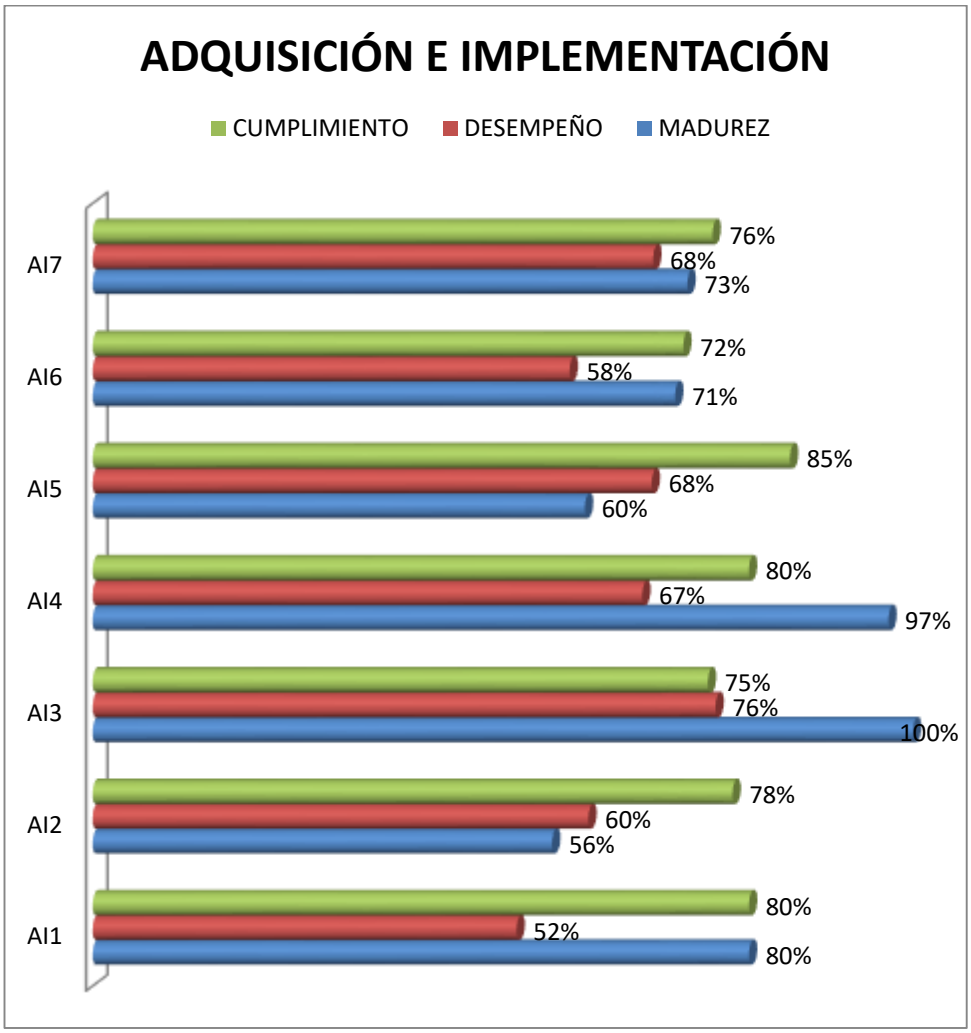

Figura 6.6*Indicadores por Proceso Adquirir e Implementar.*[4]

Los procesos de Entrega y Soporte (DS) tienen como objetivo principal atender a los usuarios bajo un ambiente de seguridad, continuidad, y calidad. Este proceso tiene un impacto medio de acuerdo a los niveles de importancia dentro de los procesos institucionales de la SUPERTEL y de acuerdo a las métricas COBIT, sin embargo, la unidad de tecnología de la información invierte eficientemente sus recursos en la administración de niveles de servicio, lo cual está permitiendo mejorar la atención al usuario e incrementar los niveles de satisfacción en la mesa de servicios. Este proceso se encuentra en un nivel de madurez 4, esto es, administrado y medible ya que como se mencionó TI maneja un esquema de niveles de servicio y además de esto, recepta las calificaciones otorgadas por los usuarios, luego de que ellos reciben un servicio o soporte. La Figura 6.7 ilustra los tres indicadores principales del proceso DS, y su calificador global.

[4]Para la descripción de cada proceso refiérase a la Tabla 4.2 Procesos y Objetivos de Control COBIT.

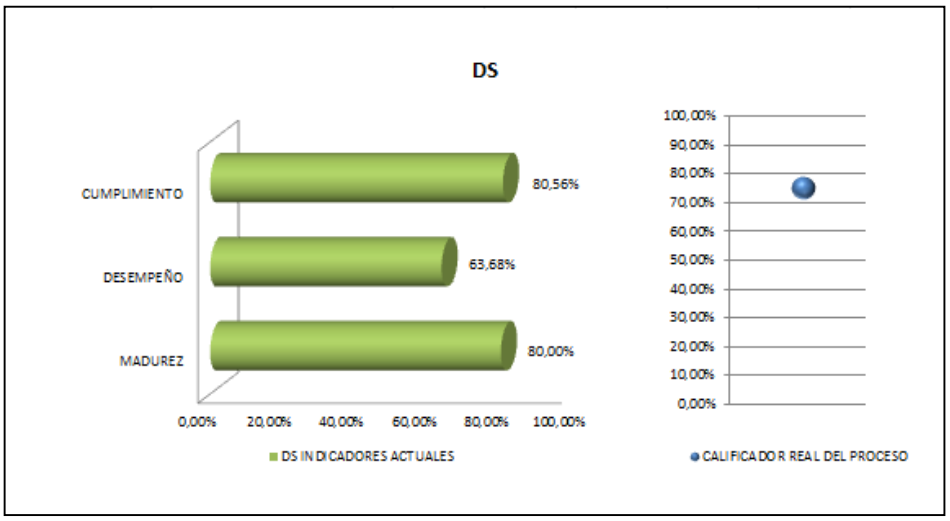

Figura 6.7*Indicadores de Entregar y Dar Soporte (DS).*

De acuerdo a las Figuras 6.8 y 6.9 uno de los procesos más débiles es DS10, mientras que los más fuertes son DS11 y DS12, estos corresponden respectivamente a: administración de los problemas con TI, administración de los datos y administración del ambiente físico. Una vez más los indicadores reflejan una realidad institucional observable a simple vista, ya que la Unidad de TI no escatima esfuerzos a la hora de proteger los activos de cómputo y la información institucional minimizando el riesgo de una interrupción del servicio; sin embargo, no existe un manejo adecuado de las prioridades institucionales cuando se presentan problemas.

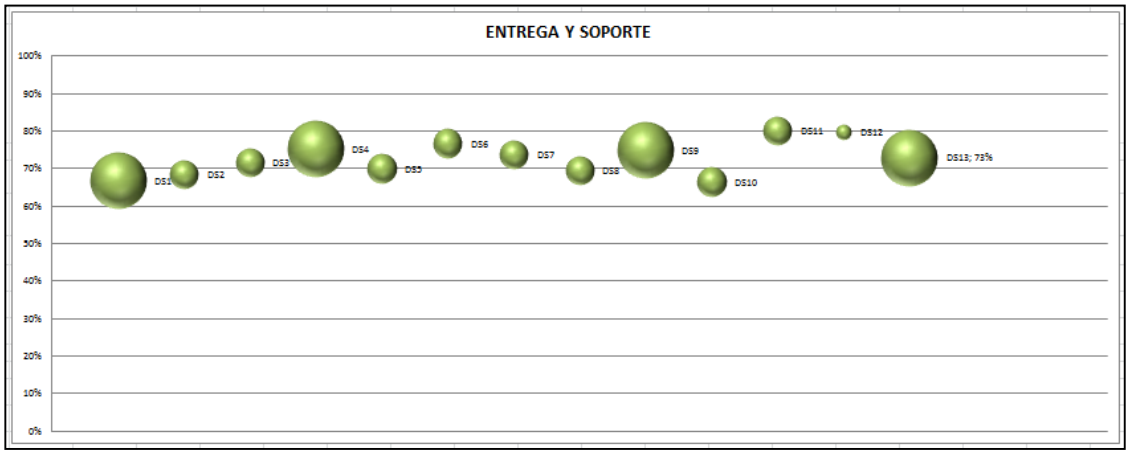

Figura 6.8*Calificador Real por Proceso para Entregar y Dar Soporte.*

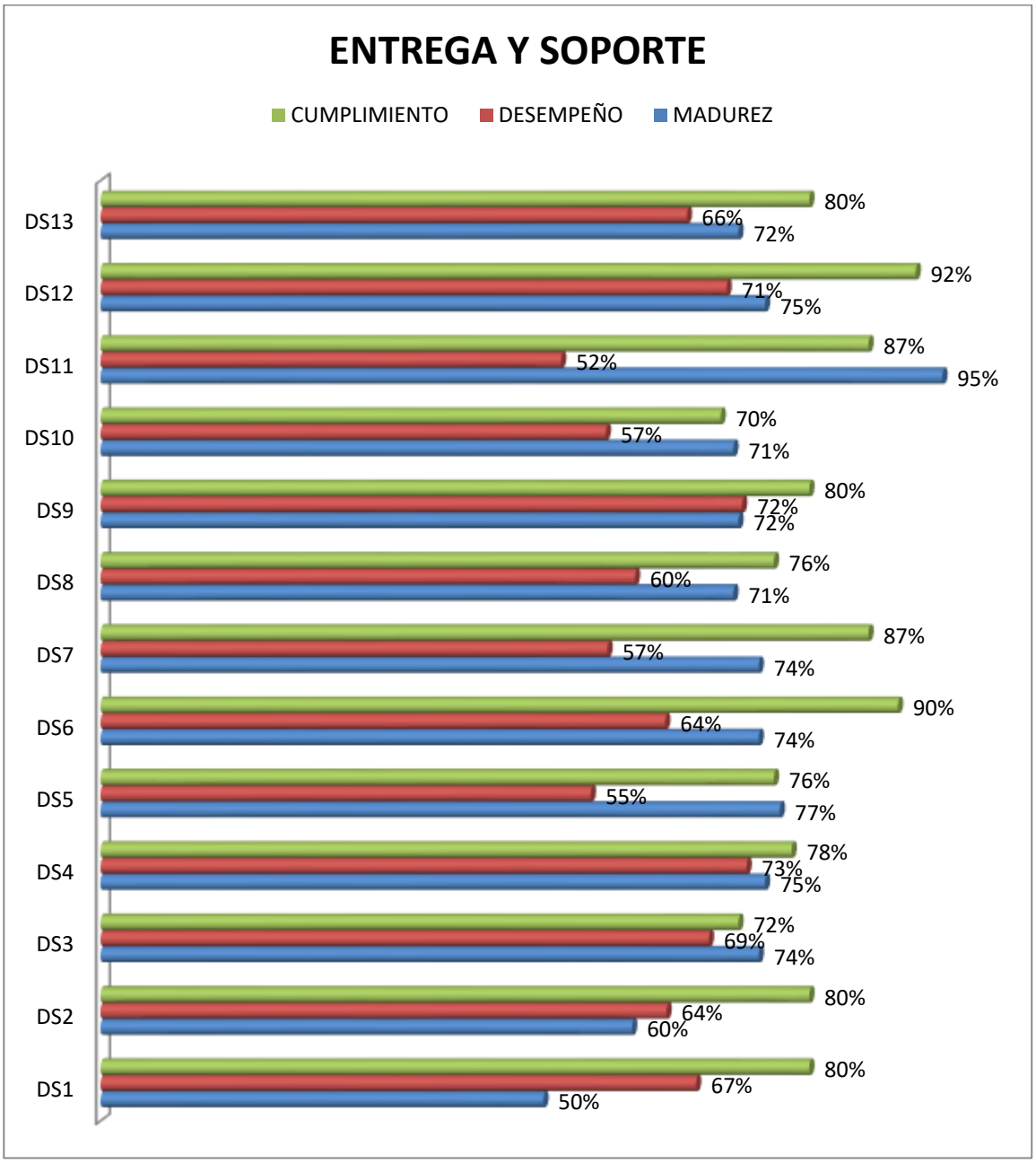

Figura 6.9*Indicadores de Entregar y Dar Soporte.*[5]

La Figura 6.10 ilustra los indicadores de desempeño, cumplimiento y madurez que describen el estado del proceso de Monitoreo y Evaluación, cuyo indicador global asciende al 70%. El objetivo principal en este ámbito es evaluar de forma regular los procesos de TI en cuanto a la calidad y cumplimiento de los requerimientos de control. El impacto de este proceso es alto, ya que constituye una forma eficiente de mantener una mejora continua de los procesos de tecnología de la información.

[5]Para la descripción de cada proceso refiérase a la Tabla 4.2 Procesos y Objetivos de Control COBIT.

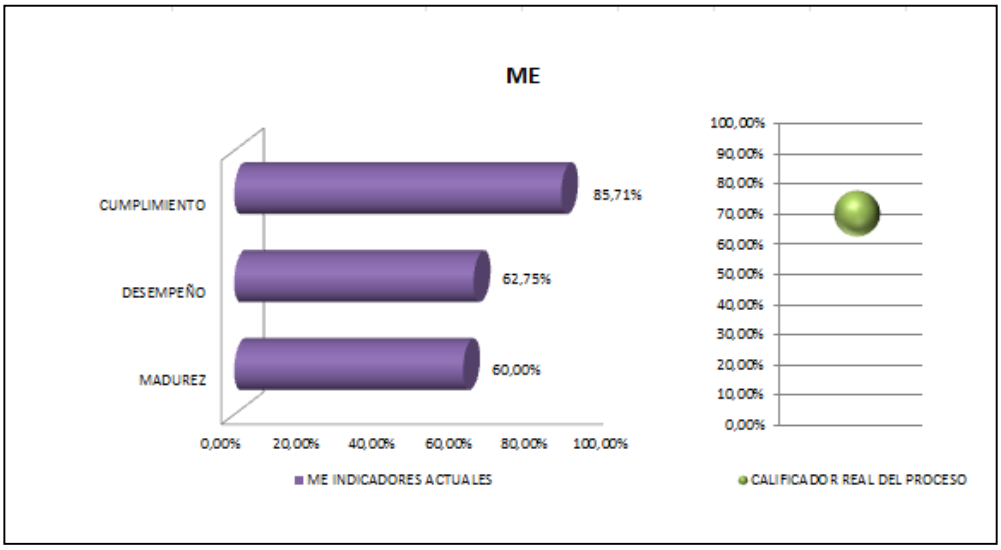

Figura 6.10*Indicadores del proceso Medir y Evaluar (ME).*

Como se muestra en las Figuras 6.11 y 6.12, el proceso más débil dentro de Monitoreo y Evaluación corresponde al ME2 cuya meta es monitorear y evaluar el control interno, pues hacen falta revisiones de auditoría externas y prácticas que le permitan a la unidad de TI compararse con modelos institucionales lideres a nivel mundial. Uno de los procesos más fuertes es ME4, cuyo fin es la integración del gobierno de TI con objetivos de la dirección y el cumplimiento de leyes y regulaciones, pues la unidad de Tecnología de la Información y más aún la Institución, al ser un ente de control público, pone especial atención al cumplimiento de resoluciones y normas en todos los ámbitos, un ejemplo de ello es la tendencia de migración al software libre, en cumplimiento de recomendaciones gubernamentales.

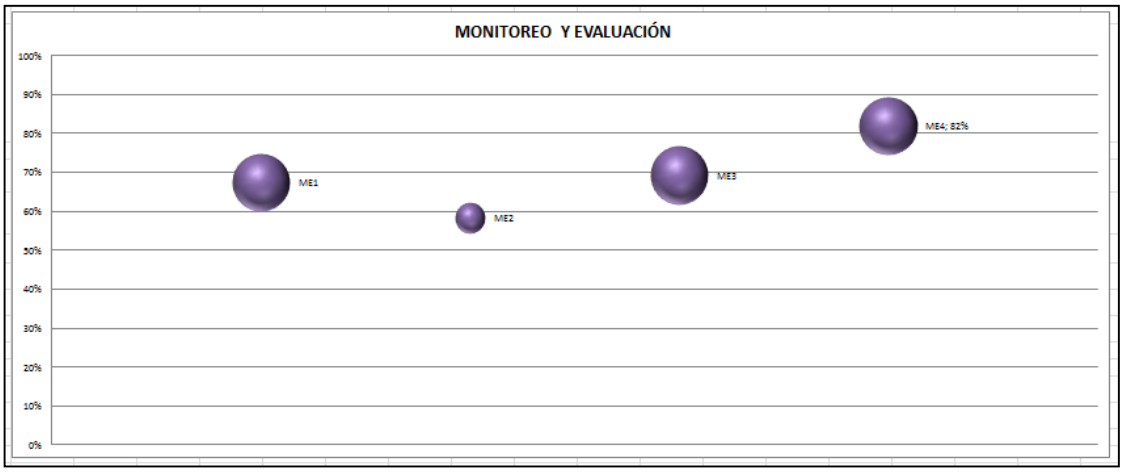

Figura 6.11*Calificador Real por Proceso Medir y Evaluar.*

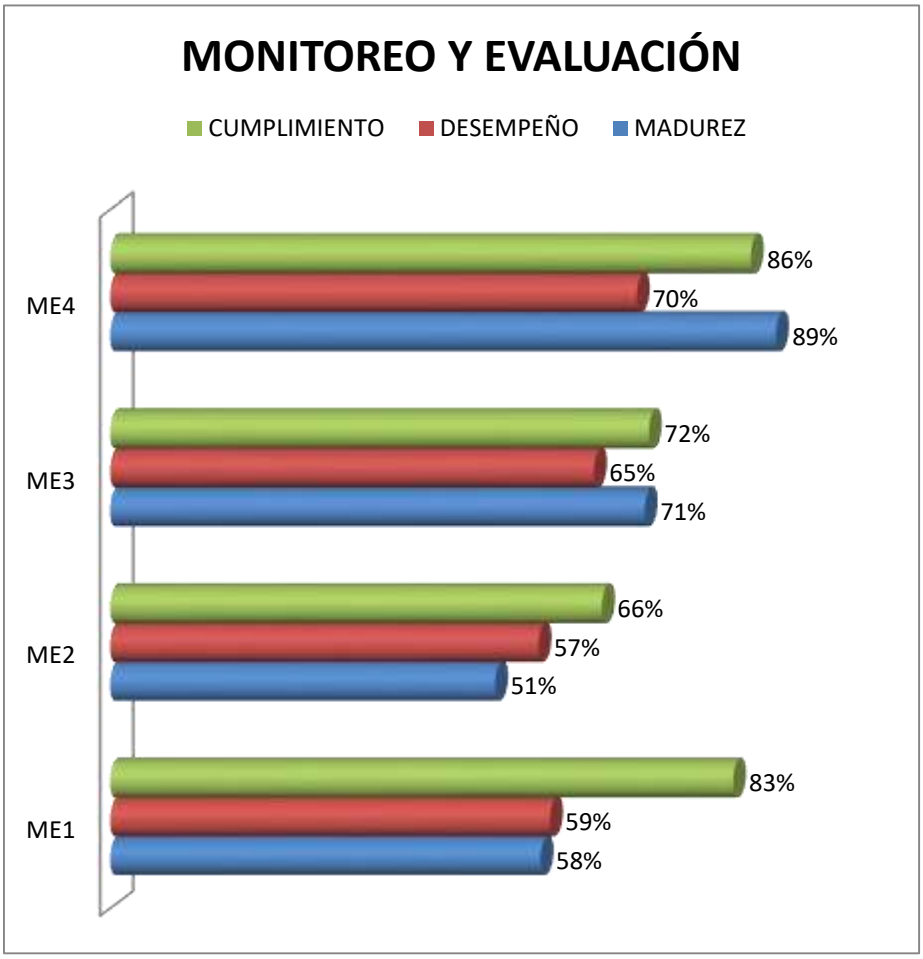

Figura 6.12*Indicadores por Proceso para Medir y Evaluar.*[6]

[6]Para la descripción de cada proceso refiérase a la Tabla 4.2 Procesos y Objetivos de Control COBIT.

CAPITULO 6

CONCLUSIONES Y RECOMENDACIONES

En cuanto al modelo empleado para la planeación y ejecución de la auditoría informática a la Superintendencia de Telecomunicaciones, COBIT[7]; se puede afirmar que además de ser una herramienta de auditoría es un marco de gobierno de TI, ya que permite asegurar que los procesosy recursos tecnológicos, contribuyen al logro de los objetivos institucionales.

A diferencia de otros esquemas de control en materia de tecnología de la información como son SAC[8], y COSO[9]vistos en el Capítulo 2, COBIT provee una estructura amplia y ve el control como un proceso que incluye políticas, procedimientos, prácticas y estructuras organizacionales, que soportan más adecuadamente los procesos de la Superintendencia de Telecomunicaciones, y además permite hacer un control exhaustivoen base a métricas,de todos los procesos de TI. Otro aspecto que diferencia a COBIT de los demás, es su versatilidad, ya que está dirigido a tres audiencias distintas: la dirección, los usuarios y los auditores. SAC está primariamente dirigido a los auditores y COSO a los directorios.

Se dijo que COBIT ve al control como un proceso, SACen cambio, ve al control como un sistema, compuesto por subsistemas, funciones y gente interrelacionada. El enfoque de SAC es el más ajeno al esquema institucional de la Superintendencia, ya queno se encuentra basado en procesos.

COSO al igual que COBIT también acentúa el control como un proceso, sin embargo, lo toma como parte integrante de las actividades de una organización en un momento dado,por cuanto otorgaría una visión amplia a nivel de entidad, mas no fijaría su foco en las tecnologías de la información, distanciándose dela esencia de esta auditoría.

[7]COBIT: Control Objetives for Information and Related Technology.
[8]SAC: Systems Auditability and Control
[9]COSO: Committee of Sponsoring Organizations.

COBIT provee objetivos de control y métricas validadas globalmente para cada proceso de tecnología informática, esto ha brindado una guía pragmática de control para la auditoría realizada a la Superintendencia de Telecomunicaciones.

De la ejecución de la estrategia de auditoria elaborada bajo los principios de COBIT, se construyó el informe final que analiza cada uno de los treinta y cuatro procesos que define éste marco de trabajo. El informe enfatiza los resultados en base a indicadores que determinan para cada proceso el nivel de madurez, el calificador de desempeño y el grado de cumplimiento de los objetivos de control de COBIT, los cuales convergen en un calificador global del proceso. El análisis de éstos resultados ha permitido obtener las siguientes conclusiones:

La Unidad de Tecnología de información mantiene un marco de trabajo alineado a las estrategias y objetivos institucionales. Este aspecto se ve reflejado en el calificador global del proceso de Planeación y Organización que se encuentra alrededor del 69%. En este tema el proceso mejor calificado es el que corresponde a la administración de proyectos de TI, ya que la Superintendencia de Telecomunicaciones establece formalmente un plan de proyecto integrado y aprobado para orientar la ejecución y el control delos proyecto durante todo su ciclo de vida. El proceso más débil es el encargado de la evaluación y administración de los riesgos, el cual podría no estar completamente alineado con el nivel de tolerancia institucional.

El calificador global del proceso de Adquisición e Implementación, asciende al 68% con lo cual se muestra que la Unidad de TI posee planes y metodologías bastante adecuados para adquirir, implementar y mantener la infraestructura tecnológica, esto es hardware y software. Dichos planes y metodologías permiten dar seguimiento al estado de los procesos, administrar los riesgos, y garantizar su calidad.

El calificador global del proceso de Entrega y Soporte es el más alto, sobrepasa el 75%, sin embargo, en este tema se presentan ciertos contrastes ya que si bien existe una mesa de servicios claramente definidacomo conexión entre usuarios y TI; que registra, y atiende los requerimientos de servicio y las solicitudes de información, sin embargo no existe una apertura adecuada por parte de TI hacia los usuarios y viceversa. Mejorar este aspecto coadyuvaría a la consecución de objetivos institucionales de una manera más efectiva. Dentro de los temas contemplados en el proceso de Entrega y Soporte, sobresale como punto positivo la administración de la seguridad que mantiene la Unidad de TI de la Superintendencia de Telecomunicaciones, ya que garantiza la identificación única de los usuarios, administrando el acceso y controlandoel flujo de la información desde y hacia las redes.

Finalmente y de acuerdo al cuarto grupo de procesos COBIT, Monitorear y Evaluar, cuyo calificador global se encuentra alrededor del 70%, se recomienda mantener un monitoreo global de TI, tomando como punto de partida el marco de trabajo descrito en este proyecto, para iniciar acciones correctivas en base a la evaluación periódica del desempeño de los procesos contra las metas, ypara mantener niveles óptimos de seguridad, calidad y eficiencia.

BIBLIOGRAFÍA Y REFERENCIAS

Hernández, E. (1997). Auditoria Informática: Un Enfoque Metodológico y Práctico. México: Continental.

Zamarripa, E. (2002). Sistemas Tutoriales de Auditoría. Prentice Hall.

Kell, W., Ziegler, R. (n.d.).Auditoria Moderna. Continental.

Piattini, M. G., Del Peso, E. (2003). Auditoria Informática: Un Enfoque Práctico. España: computec RAMA.

Weber, R. (1982). EDP Auditing: Conceptual Foundations and Practice.
D'Amore, M. (1987). La Auditoría Informática y su Metodología de Realización. Actas Congreso Iberoamericano de Informática y Auditoría. CREI.
Echenique, J. A. (2003). Auditoría en Informática. México: Mcgraw-Hill.

Lorenzo Gil, E. (n.d.). Auditoría Informática. Obtenida el 15 de Noviembre del 2010, de http://inspeccion-uvmi3.iespana.es/inde7130.htm

Nava Garcia, J. (n.d.). Apuntes de Auditoría Informática. España. Obtenida el 18 de Noviembre del 2010, de http://www.gavab.es/wiki/download/ai/Temario/AudInf-Apuntes-1.pdf

Garrido Diaz, S. (2008). Auditoría de Informática. Ecuador. http://ainsonmer.blogspot.com/2008/06/tipos-de-auditora-informtica.html

Haro, M., Sanchez, D. (2006). Sistema para Realizar Auditoría de la Información del SAE. Ecuador. Obtenida el 20 de Noviembre del 2010, de http://bibdigital.epn.edu.ec/bitstream/15000/268/1/CD-0689.pdf

Caridad Simón. S. (2006). Auditoría Informática. España. Obtenida el 18 de Noviembre del 2010, de http://www.scaridad.com/files/Apuntes%20de%20AI.pdf

Republica de Nicaragua. Contraloría General de la República. (2009). Manual de Auditoría Gubernamental. Parte VIII. Auditoría Informática. Managua. [Versión Electrónica] http://www.google.com/url?sa=t&source=web&cd=1&ved=0CBUQFjAA&url=http%3A%2F%2Fwww.cgr.gob.ni%2Fcgr%2Findex.php%3Foption%3Dcom_docman%26task%3Ddoc_download%26gid%3D1631%26Itemid%3D101&rct=j&q=Manual%20de%20Auditor%C3%ADa%20Gubernamental.%20Parte%20N%20VIII.%20Auditor%C3%ADa%20Inform%C3%A1tica.%20Nicaragua.&ei=fycvTcObIoGs8Ab0psCJCQ&usg=AFQjCNHxSZnTTI_kbDLA7GtPXG8blqyBSQ&cad=rja

Apuntes de Auditoría Informática. (2009). México. Obtenida el 30 de Noviembre del 2010, de http://mx.oocities.com/acadentorno/aui3.pdf

Perú. Instituto Nacional de Estadística e Informática - INEI. (n.d.). ¿Qué es la Auditoría Informática?. Colección Cultura Informática. (vol 26). [Versión Electrónica] http://www1.inei.gob.pe/biblioineipub/bancopub/Inf/Lib5105/Libro.pdf

Auditoría Informática. (2002). Obtenida el 28 de Noviembre del 2010, de http://www.gestiopolis.com/recursos/documentos/fulldocs/fin/auditoriainformatica.htm

Kuna, H. (2006). Tesis de Magister en Ingeniería del Software: Asistente para la Realización de Auditorías de Sistemas en Organismos Públicos o Privados. España. Obtenida el 21 de Noviembre del 2010, de http://laboratorios.fi.uba.ar/lsi/rgm/tesistas/kuna-tesisdemagister.pdf

Quinn E. (2000). La Auditoria informática dentro de las etapas de Análisis de Sistemas Administrativos. Obtenida el 21 de Octubre del 2010. Página web de Monografías.com: http://www.monografias.com/trabajos5/audi/audi.shtml#inter

Marin, H. (2003). Auditoría Financiera. Obtenida el 22 de Octubre del 2010. Pagina web de Monografías.com: http://www.monografias.com/trabajos12/aufi/aufi.shtml

Jiménez, Y. (2003). Auditoria. Obtenida el 22 de Octubre del 2010. Página web de Monografías.com: http://www.monografias.com/trabajos14/auditoria/auditoria.shtml#AUADMI

Aguirre, Y. (n.d.a). Propuesta de implantación del área de auditoría en informática en un órgano legislativo. Seminario de Auditoría Informática. México Obtenida el 5 de Diciembre del 2010, de http://olea.org/~yuri/propuesta-implantacion-auditoria-informatica-organo-legislativo/index.html

Aguirre, Y. (n.d.b). Propuesta de Implantación del Área de Auditoría en Informática en un Órgano Legislativo. (Capitulo 3). Legislación informática, mejores prácticas y técnicas de auditoría informática - ComputerAssistedAuditTechniques CAAT. Obtenida el 27 de Febrero del 2011 de http://olea.org/~yuri/propuesta-implantacion-auditoria-informatica-organo-legislativo/ch03s04.html

México. Secretaria de la Función Pública – Proyecto ATLATL. (2003). Seminario Introducción a las Normas y Prácticas Profesionales de la Auditoría Gubernamental. Obtenida el 9 de Enero del 2011 de http://www.slideshare.net/JOVIMECARCH/tecnicas-de-practicas-auditoria-presentation

Ecuador. Contraloría General del Estado (2008). Fundamento Legal. Obtenida el 10 de Enero del 2011 de http://www.contraloria.gov.ec/la_institucion.asp?id_SubSeccion=3

Ecuador. Instituto Ecuatoriano de Propiedad Intelectual. (n.d.). Obtenida el 11 de Enero del 2011 de http://www.iepi.gob.ec/

Ecuador. Subsecretaría de Informática. (2007). Normativa Legal. Obtenida el 10 de Enero del 2011 de http://www.informatica.gob.ec/index.php/documentacion/legal

Brito, J., Solis, G. (2004). Análisis y Aprovechamiento de los Sistemas de Información para una Eficiente Auditoría y Control de Gestión. Obtenida el 7 de Diciembre del 2010, de http://www.dspace.espol.edu.ec/bitstream/123456789/1901/1/3786.pdf

Ecuador. **Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. (2002). Obtenida el 11 de Enero del 2011 de**http://www.informatica.gob.ec/files/Ley_CEFEMD_2002%281%29.pdf

Ecuador. Ley Orgánica de Transparencia y Acceso a la Información Pública. (2004). Obtenida el 5 de Enero del 2011 de http://www.informatica.gob.ec/files/LOTAIP.pdf

Ecuador. Reglamento a Ley de Transparencia y Acceso A Información Pública. (2005). Obtenida el 20 de Enero del 2011 de http://www.informatica.gob.ec/files/LOTAIP_Reglamento.pdf

Ecuador. Norma Técnica para la Aplicación de la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP) Guía para la Creación de Sitios Web. Obtenida el 12 de Enero del 2011 de http://www.informatica.gob.ec/files/LOTAIP_normatec.pdf

Miño Quintero, P., (2008). Se Decreta el Uso de Software Libre en la Administración Pública Central, Subsecretaría de Informática - Presidencia de la República de Ecuador. Obtenida el 5 de Enero del 2011 de http://www.informatica.gov.ec/index.php/titulares-historico/subsecretaria-historico-titulares/185-se-decreta-uso-de-sl-en-la-apc-ecuador

Ecuador. P**olítica Gubernamental de uso de Software Libre en la Administración Pública Central. (2008).** Obtenida el 18 de Enero de http://www.informatica.gob.ec/files/sidsl1014.pdf

Ecuador, Contraloría General del Estado (2009). Normas de Control Interno para las Entidades, Organismos del Sector Público y Personas Jurídicas de Derecho Privado que Dispongan de Recursos Públicos. Obtenida el 21 de Enero del 2011 dehttp://ecuadorimpuestos.com/index2.php?option=com_content&do_pdf=1&id=115

Ecuador. Contraloría General del Estado. (2003). **Manual General de Auditoria Gubernamental. Obtenida el 17 de Enero del 2011 de**
http://www.contraloria.gov.ec/documentos/normatividad/MGAG-ACUERDO.pdf
http://www.contraloria.gov.ec/documentos/normatividad/MGAG-Cap-I.pdf
http://www.contraloria.gov.ec/documentos/normatividad/MGAG-Cap-II.pdf
http://www.contraloria.gov.ec/documentos/normatividad/MGAG-Cap-III.pdf
http://www.contraloria.gov.ec/documentos/normatividad/MGAG-Cap-IV.pdf
http://www.contraloria.gov.ec/documentos/normatividad/MGAG-Cap-V.pdf
http://www.contraloria.gov.ec/documentos/normatividad/MGAG-Cap-VI.pdf
http://www.contraloria.gov.ec/documentos/normatividad/MGAG-Cap-VII.pdf
http://www.contraloria.gov.ec/documentos/normatividad/MGAG-Cap-VIII.pdf

Ecuador. IEPI. (2006). Ley de Propiedad Intelectual Codificada. Obtenida el 29 de Enero del 2011 de http://www.iepi.gob.ec/files/LeyTransparencia/EstructuraOrganica/BaseLegal/Normas/LeyPropiedadIntelectual.pdf

Ecuador. IEPI. (1998). Ley de Propiedad Intelectual Registro Oficial N°320. Obtenida el 29 de Enero del 2011 de http://www.iepi.gob.ec/files/LeyTransparencia/EstructuraOrganica/BaseLegal/Normas/RegistroOficial320LeyPropiedadIntelectual.pdf

Ecuador. Subsecretaría de Informática. (2009). Estrategia de Implantación de Software Libre en la Administración Pública Central. Obtenida el 19 de Enero del 2011 de http://www.informatica.gov.ec/descargas/emslapcv1.pdf

Ecuador. Subsecretaría de Informática. (2010). Lineamientos para Seguridad de Información en Entidades Públicas. Obtenida el 20 de Enero del 2011 de http://www.informatica.gob.ec/files/SIRecSegInfGub.pdf

Ecuador. Subsecretaría de Informática. (2010). Lineamientos Generales para Digitalización de Archivos Físicos. Obtenida el 21 de Enero del 2011 de http://www.informatica.gob.ec/files/Lingendigitarchfis.pdf

Ecuador. Subsecretaría de Informática. (2007). Base Legal. Obtenida el 10 de Enero del 2011 de http://www.informatica.gov.ec/index.php/inicio/subsecretaria/base-legal

Ecuador. Subsecretaría de Informática. (2007). Procedimientos Subsecretaria informática. Obtenida el 10 de Enero del 2011 de http://www.informatica.gob.ec/index.php/documentacion/procedimental-principal

Ecuador. Subsecretaría de Informática. (2007). Documentación Varios. Obtenida el 10 de Enero del 2011 de http://www.informatica.gob.ec/index.php/documentacion/varios

Sistema de información MIPYMES. (2010). Legislación Complementaria. Ecuador. Obtenida el 5 de Enero del 2011 de http://www.pymes.ec/modjuridico/legislacion_complementaria/default.aspx

TheworldLaw Guide. (2009). Legislación del Ecuador. Obtenida el 8 de Enero del 2011 de http://www.lexadin.nl/wlg/legis/nofr/oeur/lxweecu.htm

Jaramillo, M. (n.d.). Revista Informática Jurídica - República del Ecuador. Ecuador. Obtenida el 8 de Enero del 2011 de http://www.informatica-juridica.com/legislacion/ecuador.asp

IT Governance Institute. (2007). COBIT.(Versión 4.1). ISACA. EEUU. Obtenida el 15 de Enero del 2011 de http://www.isaca.org/Knowledge-Center/cobit/Documents/cobiT4.1spanish.pdf

ItSMF - The IT Service Management Forum. (2007). The IT Infrastructure Library An Introductory Overview of ITIL® V3. (Version 1.0). EEUU. Obtenida el 18 de Enero del 2011 de http://www.best-management-practice.com/gempdf/itSMF_An_Introductory_Overview_of_ITIL_V3.pdf

Ramírez, P., Donoso, F. (2006). Metodología ITIL. Chile. Universidad de Chile. Obtenida el 22 de Enero del 2011 de http://www.cybertesis.cl/tesis/uchile/2006/donoso_f/sources/donoso_f.pdf

Cruz, C. (2009). Desarrollo de un Plan que Permita la Implantación de un Centro de Servicio al Usuario para la Empresa Pinto S.A., Basado en el Marco de Referencia ITIL V3.0. Ecuador. Escuela Politécnica Nacional. Obtenida el 10 de Enero del 2011 de http://bibdigital.epn.edu.ec/bitstream/15000/1169/1/CD-2010.pdf

Ecuador. Ministerio de Relaciones Exteriores Comercio e Integración. (n.d.). Normas de Control Interno para el Sector Público. Obtenida el 5 de Enero del 2001 http://www.mmrree.gob.ec/ministerio/legal/normas_control_int.pdf

México. Universidad Autónoma de Yucatán - UADY. (2008). Informe COSO - Los Nuevos Conceptos de Control Interno. Obtenida el 5 de Enero del 2011 de http://www.auditoria.uady.mx/arts/INFORME%20COSO%20%28RESUMEN%29.pdf

COSO-Committee of Sponsoring Organizations of the Treadway Commission. (2004). Gestión de Riesgos Corporativos - Marco Integrado-Técnicas de Aplicación. EEUU. Obtenida el 20 de Enero del 2011 de http://212.9.83.4/auditoria/home.nsf/Todos/03C8949A3EA3E654C12571AC00827A40/$FILE/COSO+ERM.pdf

NASAudit. (2009). COSO II: Enterprise Risk Management. Colombia. Obtenida el 25 de Enero del 2011 de: http://actualicese.com/Blogs/DeNuestrosUsuarios/Nasaudit-COSO_II_Enterprise_Risk_Management_Primera_Parte.pdf

ISO/IEC. (2005). Estándar Internacional ISO/IEC 27001 - Tecnología de la Información. Técnicas de seguridad – Sistemas de Gestión de Seguridad de la Información – Requerimientos. Primera Edición. Obtenida el 28 de Enero del 2011 de http://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf

López A., Ruiz J. (n.d.a). ISO 27000. El portal de ISO 27001 en Español. España. Obtenida el 25 de Enero del 2011 de http://www.iso27000.es/iso27000.html

López A., Ruiz J. (n.d.b). La Serie 27000. El portal de ISO 27001 en Español. España. Obtenida el 25 de Enero del 2011 de http://www.iso27000.es/iso27000.html#section3b

López A., Ruiz J. (n.d.c). ¿Para qué sirve un SGSI?. El portal de ISO 27001 en Español. España. Obtenida el 25 de Enero del 2011 de http://www.iso27000.es/sgsi.html#section2b

López A., Ruiz J. (n.d.d). ¿Cómo se implementa un SGSI?. El portal de ISO 27001 en Español. España. Obtenida el 25 de Enero del 2011 de http://www.iso27000.es/sgsi.html#section2d

López A., Ruiz J. (n.d.e). ¿Cómo adaptarse?. El portal de ISO 27001 en Español. España. Obtenida el 25 de Enero del 2011 de http://www.iso27000.es/iso27000.html#section3e

López A., Ruiz J. (n.d.f). Controles ISO 27002. El portal de ISO 27001 en Español. España. Obtenida el 25 de Enero del 2011 de http://www.iso27000.es/download/ControlesISO27002-2005.pdf

ISO/IEC. (2005). International Standard ISO/IEC 27002 – Information Technology – Security Techniques – Code of Practice for Information Security Management. FirstEdition. Obtenida el 28 de Enero del 2011 de http://www.scribd.com/doc/48883668/Norma-ISO-27002

Corletti, A. (2009). ISO 27001 e ISO 27004. Obtenida el 29 de Enero del 2011 de http://www.slideshare.net/dcordova923/iso-27001-e-iso-27004

ISO/IEC. (2009). International Standard ISO/IEC 27004 – Information Technology – Security Techniques – Information Security Management – Measurement. FirstEdition. Obtenida el 28 de Enero del 2011 de http://webstore.iec.ch/preview/info_isoiec27004%7Bed1.0%7Den.pdf

López, G., Flores, J. (2009). Estandarización de las Herramientas de Gestión en las Telecomunicaciones. Ecuador: Escuela Superior Politécnica del Litoral. Obtenida el 29 de Enero del 2011 de http://www.dspace.espol.edu.ec/bitstream/123456789/10342/1/D-42118.pdf

Maxitana, J. (2005). Administración de Riesgos de Tecnología de Información de una Empresa del Sector Informático. Ecuador: Escuela Superior Politécnica del Litoral. Obtenida el 10 de Febrero del 2011 de http://www.dspace.espol.edu.ec/bitstream/123456789/3958/1/6484.pdf

Consejo Superior de Informática. (n.d.). MARGERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (Versión 1.0). Guía de procedimientos. Obtenida el 15 de Febrero del 2011 http://www.innovavirtual.org/campus/file.php/7/ASX03_00/archivos_curso/MAGERIT/2.%20MAGERIT%20v%201%200%20-%20gUIA%20DE%20PROCEDIMIENTOS.pdf

Pérez, A. (n.d.). ISO/IEC 20000 El Estándar para la Gestión de Servicios TI. España. Obtenida el 21 de Febrero del 2011 de http://www.uc3m.es/portal/page/portal/congresos_jornadas/congreso_itsmf/ISO%2020000%20-%20El%20estandar%20para%20la%20gestion%20de%20servicios%20TI.pdf

Universidad Politécnica de Valencia - Laboratorio de Sistemas de Información.(n.d.). CapabilityMaturityModel (CMM). España. Obtenida el 29 de Enero del 2011 de www.dsic.upv.es/asignaturas/facultad/lsi/trabajos/082000.doc

Chacón, W. (2004). Modelo de Capacidad de Madurez del Software y su Influencia en las Mejoras de Calidad del Software. Universidad San Carlos de Guatemala. Guatemala. Obtenida el 25 de Febrero del 2011 dehttp://biblioteca.usac.edu.gt/tesis/08/08_5776.pdf

Perez, C. (2010a). El modelo CMMI para el cambio y mejora organizacional. Obtenida el 29 de Enero del 2011 de http://www.suite101.net/content/modelo-cmmi-a18334#ixzz1Gs4T2DJK

Perez, C. (2010b). Evaluación SCAMPI para el modelo CMMI del SEI. Obtenida el 29 de Enero del 2011 de http://www.suite101.net/content/scampi-a21533#ixzz1GsCyhyD1

ISECOM – Institute for Security and Open Methodologies. (n.d.).ISM3 1.0.Information Security Management MaturityModel.EEUU. Obtenida el 29 de Enero del 2011 de http://hades.udg.edu/~xavier/downloads/White_Papers/ISM3.es.1.0.pdf

Ecuador. SUPERTEL. (2010). **REGLAMENTO ORGÁNICO POR PROCESOS DE LA SUPERINTENDENCIA DE TELECOMUNICACIONES. RESOLUCIÓN No. ST-2010-0572.** Obtenida el 1 de Marzo del 2011 http://www.supertel.gob.ec/pdf/informacion_publica/resolucion-572.pdf

Ecuador. SUPERTEL (2011). Plan Operativo Anual – 2011. Obtenida el 5 de Mayo del 2011de http://www.supertel.gob.ec/pdf/informacion_publica/plan_operativo_2011.pdf

Ecuador. SUPERTEL (2011). Plan Tecnológico – 2011.

Ecuador. SUPERTEL (2012). Plan de Inversiones – 2012.

Ecuador. SUPERTEL (2011). Proceso de Diseño de Servicios – 2011.

ANEXO 1: ESTADARES DE SOFTWARE Y HARDWARE

Sistemas Operativos:		
	Estaciones de Trabajo	Windows 7 Windows XP Profesional
	Servidores	Windows Server 32bits Windows Server 64bits AIX VMWARE
Software de Desarrollo:		
	Definido en las políticas de diseño de servicios (proceso de Diseño de Servicio)	
Software de Escritorio:		
	Oficina	MS Office Estándar MS Office Profesional Lotus Notes
	Graficadores	Corel Draw Quark Xpress Visio MapInfo
	Antivirus	Kaspersky corporativo
	Navegadores Internet	Internet Explorer Mozilla Firefox
	Otros	Winzip MS Project Adobe Acrobat Estándar Adobe Acrobat Profesional Joomla
Software de Soporte:		
	Administración de Red	IP Route PRTG VNC WS_FTP Tivoli

Figura A1.1 *Estándares de Software.*

.

Servidor tipo BLADE
Instalable en chasis H o S de IBM
Procesadores RISK o CISK
2 Procesadores instalados, desde 2.3 Ghz y 4 core cada uno
Bus frontal de 1333 Mhz
2 discos duros ATA de 320 GB, 7200 rpm
Soporte para SAS RAID 1
Memoria caché 1 Mb L2 por Core
Memoria RAM 8 Gb DDR-2, exp. 64Gb
2 puertos Fiber Channel
2 puertos Gigabit Ethernet
Alimentación eléctrica 120/240 VAC, 60Hz

Figura A1.2*Estándares de Hardware – Servidor tipo Blade. (SUPERTEL - Plan Tecnológico, 2012).*

Computadores de Escritorio:
Tipo Desktop small form factor
Procesador Core 2 Duo desde 2.33 Ghz, cache 4MB L2
Bus frontal de 1066 Mhz
Disco SATA desde 250 Gb, 7200 rpm
Memoria RAM 4 Gb DDR2, exp. 8 Gb desde 667 Mhz
Unidad de DVD-RW desde 52x16x52
2 Ranuras PCI para expansión
4 Puertos USB 2.0
1 Puerto serial
1 Puerto paralelo
1 Tarjeta de red 10/100/1000 con puerto RJ-45
Fuente de poder desde 240 watt, con alimentación eléctrica 120VAC, 60Hz
Monitor TFT de 17" de la misma marca que el CPU
Teclado PS/2 latinoamericano o español de la misma marca que el CPU
Mouse PS/2 de 2 botones con scroll de la misma marca que el CPU
Licencia de sistema operativo Windows 7 Business, downgrade a Win XP

Figura A1.3*Estándares de Hardware – Computadores de Escritorio. (SUPERTEL - Plan Tecnológico, 2012).*

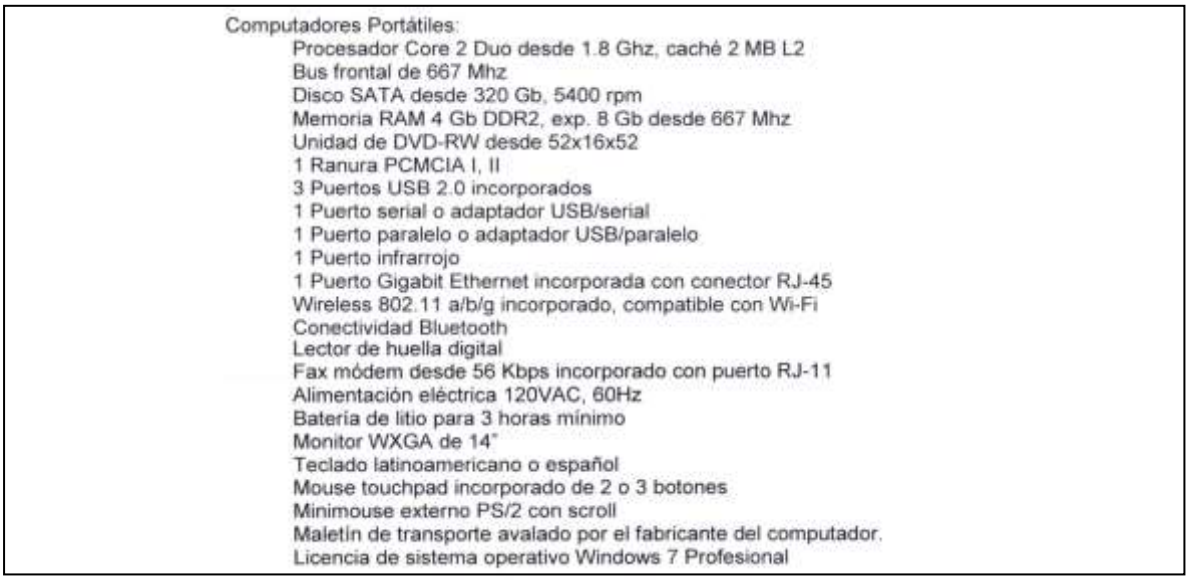

Figura A1.4*Estándares de Hardware – Computadores Portátiles. (SUPERTEL - Plan Tecnológico, 2012).*

Figura A1.5*Estándares de Hardware - Impresoras. (SUPERTEL - Plan Tecnológico, 2012).*

.

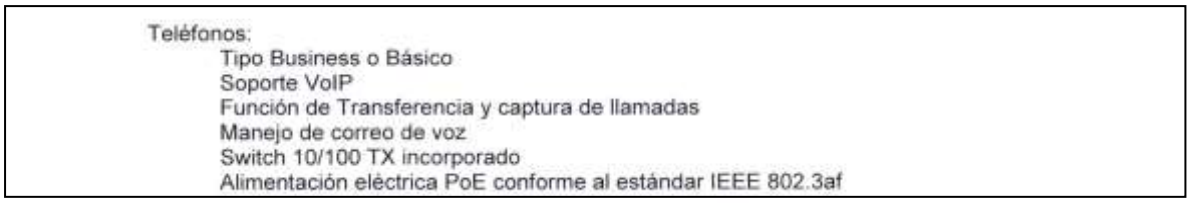

Figura A1.6*Estándares de Hardware - Teléfonos. (SUPERTEL - Plan Tecnológico, 2012).*

ANEXO 2: CATALOGO DE SERVICIOS INFORMATICOS

CATEGORÍA	NOMBRE	DESCRIPCION
TELEFONIA IP	TELEFONÍA BÁSICA	Sistema de telefonía para comunicación de voz
	TELEFONÍA UNIFICADA	Aplicaciones de convergencia de telefonía de voz con sistemas de mensajería
ADM. CONTENIDO EMPRESA-RIAL	RECURSOS COMPARTIDOS	Administración de recursos compartidos y almacenamiento de archivos en servidores institucionales
	ON BASE USUARIO FINAL	Software que permite el ingreso y búsqueda de los documentos electrónicos. Permite la digitalización y captura, es la base fundamentas del sistema de Manejo de Contenido Empresarial (ECM).
	ON BASE SERVIDOR	Servidor para el ingreso de documentos electrónicos o digitalizados. Este servidor contiene físicamente los archivos electrónicos, a nivel de directorios. Adicionalmente tiene un servidor de Base de Datos Ms SQL, donde están las claves de búsqueda de cada tipo de documento
	JOOMLA	Administrador de contenidos web
ADMINISTRACIÓN DE EQUIPOS	SERVIDORES INTEL	Administración de sistemas operativos y hardware de servidores con base Intel
	SERVIDORES RISC	Administración de sistemas operativos y hardware de servidores con base RISC
	CONSOLAS	Administración de consolas de Blade Center y Pi series tanto de centro de cómputo principal como alterno
	CABLEADO ESTRUCTURADO	Administración de infraestructura de cableado inteligente con ITRACS
	HARDWARE DE USUARIO	Administración de hardware que utiliza el usuario final para cumplir sus actividades
	VIRTUALIZACIÓN RISC	Administración de plataforma de virtualización de servidores Risc (AIX Virtual Machine).
	VIRTUALIZACIÓN INTEL	Administración de plataforma de virtualización de servidores Intel (VMWARE).
BASES DE DATOS	SQL SERVER	Administración de motor MS SQL Server
	ORACLE	Administración de motor ORACLE
	LOTUS DOMINO	Administración de DOMINO Server
	MYSQL	Administración de motor MYSQL
REDES Y COMUNICACIONES	OPTIMIZACIÓN DE TRÁFICO	Administración de sondas WAAS de optimización de tráfico sobra WAN
	INTERNET	Administración de acceso corporativo a Internet
	COMUNICACIÓN REGIONAL	Administrar la parte técnica de los contratos para transmisión de datos con las Unidades Regionales. Se incluyen las estaciones de comprobación técnica
	ROUTING	Administración de ruteo dinámico y estático para tráfico de voz y datos. Administración de tarjetería de voz contra PSTN
	SWITCHING	Administración de switches de core, acceso, SAN, blade y otros
	DNS	Administración de servidores de Nombres de dominio y sincronización
	DHCP	Servidores de Asignación Dinámica de direcciones IP en cada regional
	NTP	Administración de servidores de Tiempo y sincronización con medios externos
	RED INALÁMBRICA	Administración de red inalámbrica de todas las sedes de la institución así como la sonda de monitoreo y control
ADM. CONTINGENCIA	DOBLE TAKE	Administrador de software de sincronización de servidores Windows de centros de cómputo principal y alterno
	CLUSTER DOMINO	Administrar alta disponibilidad de servidores DOMINO
	CLUSTER ORACLE	Administrar alta disponibilidad de servidores de base de datos ORACLE
	CENTRO DE COMPUTO	Administrar la infraestructura instalada en los centros de cómputo tanto principal como alterno. Se incluye controles de acceso, climatización, sistema contra incendiso, y demás
	UNITY EXPRESS	Contingencia de Call Manager
	CENTROS DE UPS	Administración de energía regulada
MONITOREO	NAM	Sonda de administración de red
	CISCOWORKS	Servidor de consolidación de logs de equipos de comunicación
	MARS	Sonda de correlación de eventos
	LICENCIAMIENTO	Control de licenciamiento, inventario y trámites de renovación
ALMACENAMIENTO	STORAGE DS	Almacenamiento en línea
	STORAGE DR	Almacenamiento histórico
	BACKUPS	Administración de los sistemas de respaldo de la información contenida en servidores institucionales
SEGURIDAD	ANTIVIRUS	Administración de servicios de antivirus
	MAIL GATEWAY	Administración de sonda de filtrado de correos entrantes y salientes para análisis de virus en su contenido
	SEGURIDAD PERIMETRAL	Administración de seguridad perimetral. Incluyen los accesos corporativos a internet y el análisis de contenidos del tráfico desde y hacia Internet
	SEGURIDAD DE SERVIDORES	Administración de firewall, seguridad en segmento de servidores institucionales, políticas de active directory, políticas de acceso, cuantas usuario y demás relacionadas
	NAC	Control de acceso para usuarios de servicios VPN
HOSTING	INTRANET	Administración de recursos para el sitio web de la Intranet institucional
	WEB EXTERNA	Administración de recursos para el sitio web Institucional
	WEB TRANSPARENCIA	Administración de recursos para el sitio web de la Función de transparencia
ACCESIBILIDAD	CITRIX	Servicio de consolidación de aplicaciones informáticas
	BUS EMPRESARIAL	Es una orquestación de servicios que permiten interactuar de mejor forma y más rápidamente a las componentes técnicas y de información con aquellas relacionadas a los procesos de negocio de las capas superiores o mas altas como las de tipo presentación o BPM. En la supertel se utilizará para permitir comunicar diversas aplicaciones en diferentes plataformas.
SOPORTE	CONTROL REMOTO	Administración de software que permite el control remoto de equipos dentro de la intranet
	HELP DESK	Administración de servicio de soporte técnico a los usuarios de los servicios disponibles
ERP	BODEGA	Control de inventario de bodega institucional. Permite realizar ingresos, egresos, visualización de kardex
	CONTABILIDAD Y PRESU-PUESTO	Automatiza la gestión contable y presupuestaria, conjuntamente con la emisión de cheques y registro de depósitos, de una manera integrada. Así como los datos las Cuentas por Cobrar de la Cartera Activa de enero 1997 hasta la presente fecha. PLANES DE CUENTAS.- Permite mantener las cuentas de contabilidad y presupuesto, y crear nuevas de acuerdo al Plan de Cuentas aprobado por el Ministerio de Finanzas. COMPROBANTES.- Emitir comprobantes de ingreso, egreso, y diario. CONCILIACION BANCARIA.- Consolidar mensualmente las cuentas bancarias del Banco Central y Banca Privada. REPORTES.- Reportes varios para la gestión y verificación Contable Presupuestaria. Gestión de Cartera Activa 2001 hasta la presente fecha. COMPROMISOS.- Permite realizar el compromiso de los valores autorizados para la gestión financiera. CONTRATOS.- Controla la ejecución financiera de los contratos de la Institución. UTILITARIOS.- Permite el mantenimiento de varios parámetros, y permite la validación de posibles errores de ingresos en los datos. RETENCIONES EN LA FUENTE.- Controla las retenciones de impuestos al SRI.
	ACTIVOS FIJOS	El Sistema de Control de Activos Fijos realiza el control de todos los activos fijos de la Superintendencia de Telecomunicaciones. Mediante este Sistema se permite llevar un mejor y eficiente manejo de la información de los bienes adquiridos por la Institución y de los movimientos de los mismos, así como permite emitir actas y reportes útiles para la unidad de Inventarios. El Sistema tiene las siguientes opciones: INGRESO DE NUEVO BIEN.- Se ingresan los datos de un nuevo bien a ser inventariado. CONSULTA.- Permite la consulta de los bienes inventariados. VERIFICACION DE INVENTARIO.- Realiza la verificación del inventario por área o por encargado con el lector de código de barras. IMPRESIÓN DE COMPROBANTE.- Realiza la impresión del comprobante de registro del bien. REPORTES.- Proporciona varios reportes necesarios para la gestión de inventarios.

		ETIQUETAS.- Impresión de las etiquetas de código de barras. ACTAS ENTREGA-RECEPCION.- Genera las Actas Entrega-Recepción. TRASPASOS.- Gestiona el traspaso de bienes del custodio anterior al nuevo. HISTORIAL.- Registra el historial de los movimientos de los bienes inventariados. MANTENIMIENTO.- Permite el mantenimiento de áreas y empleados.
	REQUISICIONES	Implementación del flujo de trabajo de requisiciones de compra, lo que incluye la autorización del Departamento de Unidades de Bienes y Servicios con el fin de abastecer bienes o servicios. Ésta a su vez es originada y aprobada por el Departamento que requiere los bienes o servicios. Bondades: Integración con el directorio institucional, lo que permite un ágil movimiento de subrogaciones, direccionamiento por roles, entre otros. Flujo de trabajo para seguimiento de compras en bodega, servicios, bienes. Reportes generados por numero de requisición, responsable, atendidos.
	PLANILLAJE	El Sistema de Planillaje automatiza el control de las resoluciones que emiten la Superintendencia de Telecomunicaciones, con la finalidad de brindar agilidad y confiabilidad en los procesos involucrados en la facturación, y además que constituya la base de la emisión de facturas de cobro por multas. Además, permite emitir facturas de cobro por el servicio de homologación. Finalmente, este sistema permite generar convenios de pago con los concesionarios. INGRESO.- Permite el ingreso de la información necesaria de las Resoluciones, las Homologaciones y los Certificados de no Adeudar. CONSULTA.-Permite realizar la consulta de Multas, Homologaciones, Certificados de No Adeudar. ELIMINACION.- Elimina la resoluciones, órdenes de cobro y solicitudes de certificado de no adeudar, en el caso de que no hayan sido facturadas. IMPRESIÓN DE FACTURAS.- Realiza la emisión e impresión de las facturas, notas de venta y notas de débito, de acuerdo a los formularios establecidos, de las Multas, Convenios de Pagos de Multas, Homologaciones, Certificados de no Adeudar. LISTADO.- Proporciona varios listados requeridos para la gestión de recaudación. RESPALDO A ARCHIVO.- Realiza el respaldo de la información de las Regionales necesaria para ser consolidada a través de un programa en la Matriz. INGRESO DE INTERES.- Permite el ingreso y actualización del interés mensual, para los cálculos de intereses por mora. ANULACION DE NOTAS DE VENTA Y NOTAS DE DEBITO.- Registra las Notas de Ventas, Notas de Débito y las Facturas a ser anuladas. MODULO CONSOLIDAR INFORMACION.- Permite la consolidación de toda la información del planillaje mensual generada por las Administraciones Regionales. Para ser verificada por la Dirección Nacional Financiera Administrativa, a través de listados generados por el módulo.
	ROL DE PAGOS	El propósito de este Sistema es la automatización del proceso de pago de las remuneraciones a los funcionarios de la Superintendencia de Telecomunicaciones. Permite la realización del rol de pagos mensual, décimo cuarto, décimo tercero. Con las siguientes opciones: CAMBIO ROL.- Realiza el cambio de rol mensual, cada vez que se cierra el mes. ACTUALIZACION.- Permite la actualización de los datos de todos los empleados de la Supertel. EJECUCION.- Ejecuta el cálculo del rol de pagos mensual. UTILITARIOS.- Permite realizar varias acciones requeridas como parámetros del Sistema. REPORTES.- Reportes utilizados para verificar el rol de pagos. ARCHIVOS IESS.- Genera archivos requeridos por el IESS. ARCHIVOS AUXILIAR PARA CONTABILIDAD.- Genera archivos auxiliares para uso de Contabilidad.
	VIATICOS	Implementación de seguimiento y control en la solicitud de viáticos e informe de comisión de servicios según las normativas vigentes. Bondades: Integración con el directorio institucional, lo que permite un ágil movimiento de subrogaciones, automatico despliegue de cargos, entre otros. Calculo automatico de la prevision de valores economicos. Calculo automatico de zonas geograficassegun normativas INEN. Control automatico de fechas de viaje. Tanto para fecha inicial final y fechas de itinerario. Aprobación según reglamento en todo la organización. Consideración de días feriados. Impresión de documentos. Generación automática de informe de comisión. Registro de acciones
	CARTERA PASIVA	El Sistema de Cartera automatiza el proceso para cancelación de los concesionarios de la cartera pasiva de enero de 1993 a diciembre de 1996. \LISTADOS\CONTROL\CONING.- Ingreso de los concesionarios de cartera pasiva. \LISTADOS\DESCARGO\DESCARGO.- Descargo de los concesionarios de cartera pasiva. \LISTADOS\PORCOBRAR\LISTADOS.- Permite la generación de reportes consolidados para verificación de concesionarios de cartera pasiva.
COLABORACIÓN	VIDEO-CONFERENCIA	Administración del servicio de comunicación visual y colaboración utilizado para reuniones y capacitaciones institucionales minimizando el factor de ubicación física de los participantes
	SAMETIME	Aplicación Cliente/Servidor y aplicación middleware que provee en tiempo real comunicación unificada y colaboración para empresas. Estas capacidades incluyen información presente, mensajeriainstantanea, conferencia web, colaboración en la comunidad y capacidades de telefonía e integración. Precensia que incluye ubicación de la localidad Emoticons, e historias de chat Conversaciones en grupo y multiples Conferencia Web Tarjetas businesscard
	CORREO ELECTRÓNICO	Provee "enterprise-grade e-mail", capacidades de colaboración, y plataforma de aplicaciones customizadas. Bondades: Incremento de colaboración en la organización, Correo via web, en celular (IMAP), en escritorio. Manejo de agenda, calendario, tareas.
	CONTROL DOCUMENTAL	Administración de servicio de flujo documental institucional, considerando la existencia de ttrámites internos y externos
LEGALES	FIEL MAGISTER	Administración de solución externa que permite consultas de aspectos Legales en general
	LEGALTEL	Administración de sistema informático que permite consultas de aspectos legales de Telecomunicaciones.
	PATROCINIO JUDICIAL	El Sistema Informático de Control de Patrocinio permite al patrocinio judicial de la Superintendencia de Telecomunicaciones, llevar a cabo una gestión práctica de los documentos inherentes a los procesos judiciales para facilitar la presentación de escritos y el archivo de cada proceso judicial.
	INFRACCIONES Y SANCIONES	1. Mantenimiento de: Datos técnicos : Usuarios infractores, entre otros Datos Jurídicos: Boletas, Resoluciones, Impugciones Datos Financieros: Pagos de sanciones Integración con Onbase de todos los documentos realcionandos: Informe técnico, boleta, resolución, factura. Resoluciones Históricas Reportes Generales: varios Resportes Resoluciones Reportes Estadísticos 2. Certificados de no adeudar Ingreso de Solicitud, solicitante Emisión de Certificados Reportes 3. Diligencias de Clausuras Infractores Reportes 5. Administración de Usuarios

TALENTO HUMANO	COMPERS	1. Seguridades y Administración 2. Estructura Organizacional 3. Administración por Competencias 4. Inventario de RRHH 5. Reclutamiento y Selección 6. Evalación y Desempeño 7. Capacitación/Desarrollo 8. Bienestar Social 9. Valoración 10. Clima Laboral
	EVOLUTION	1.Módulo de Seguridad de usuarios 2.Módulo de Vacaciones Marcaciones Permisos Reportes 3.Consulta de Vacaciones
	REGISTRO DE ASPIRANTES	Aplicación web para registro de aspirantes a cargos dentro de la SUPERTEL
	ONLY CONTROL	Mantenimiento de: Huellas digitales Usuarios Configuración de equipos Reportes
TECNICOS DE CONTROL	HOMOLOGACIONES	1. Mantenimiento de: Personas solicitantes, Solicitudes, Equipos, Certificados, Orden de Pago,Reportes 2. Interface con la BDD ONBASE 3. Consultas de Homologaciones de equipos 4. Administración de Usuarios
	REGISTRO MEDICIONES SMA	1. Mantenimiento a los formularios (5 fases) de: • STM1: (LLAMADAS ESTABLECIDAS ON-NET). • STM7: (TASA DE MENSAJES CORTOS RECIBIDOS POR EL DESTINATARIO FINAL TIEMPO PROMEDIO DE RECEPCIÓN DE SMS). • STM9: (PORCENTAJE DE COBERTURA EN ZONAS URBANAS Y RURALES). • STM10: (SITIOS CON LLAMADAS CAÍDAS). • STM11: (PORCENTAJE DE COBERTURA EN CARRETERAS). • STM 12: (CALIDAD DE CONVERSACIÓN). 2. Reportes 3. Administración de sistema
	COMPLETACION DE LLAMADAS TEL. FIJA	1. Implementación de Plantillas de carga por regional: Alcatel EricsonHuawei Siemens Neax EE Neax Sigma 2. Subida de información Individual Por grupo 3. Comparativos Información CNT Información Supertel 4. Utilitarios: archivos 5. Reportes varios 6. Administración de Usuarios
	TELEFONOS ROBADOS	Sistema de consolidación de registros de teléfonos robados en las operadoras locales y operadoras de Colombia y Perú.
	INSPECCIONES	Aplicación que permite realizar el seguimiento de una inspección de forma automática mediante una orden de trabajo y la emisión de los respectivos informes de inspección de los servicios técnicos de la institución. Bondades: Integración con el directorio institucional, lo que permite un ágil movimiento de subrogaciones, automático despliegue de cargos, entre otros. Interacción con aplicación de viáticos. Registro de informes, inspecciones, guías de remisión, viáticos bajo un solo paquete de Plan de Comisión. Registro de aprobación de imprevistos y planificados. Reportes consolidados de inspecciones finalizadas.
	SIETEL 1	Establecer como único punto de recepción y cierre de requerimientos internos al CIR. Clasificación de todos los incidentes e inicial soporte Investigación y diagnosis oportuna. Resolución y recuperación de incidentes a tiempo, reducir el impacto en el negocio e incrementar efectividad Identificación proactiva de enmiendas/mejoras Negocio enfocado a la administración de información
	SIRA-TV	Solución que permite el registro y seguimiento de los concesionarios de servicios de Radiodifusión y TV
	GEOREFERENCIACIÓN	Solución para la ubicación geográfica de concesionarios de servicios de Radiodifusión y TV
	INDICADORES	Servicio que genera información de tipo gerencial basada en indicadores de gestión
	ICS	Solución comercial para la generación de estudios de ingenieria de propagación
	GLADIATOR	Solución comercial para postprocesamiento de mediciones de telefonía
	SAMM	Solución comercial para medición de calidad de servicios de telecomunicaciones
	SACER	Solución comercial para monitoreo del espectro radioeléctrico
	REGISTRO MEDICIONES SMA	
MEDIOS DE DIFUSION	ESCALAMIENTO	Aplicación que implementa el mecanismo que ayuda a la resolución dentro de los tiempos especificados de un escalamiento. Puede llevarse durante cualquier actividad en el proceso de resolución. ESCALAMIENTO FUNCIONAL (Competencia) (Contingencia al Call Center) De primer nivel a segundo y más allá. Asignación basado en la experiencia. ESCALAMIENTO JERARQUICO (Autoridad). Se escala el requerimiento a grupos o personas con mayor poder de decisión en la organización. Bondades: Detección y registro de requerimientos que ya han sido escalados internamente a la institución. Establecer como único punto de recepción y cierre de requerimientos internos al CIR. Clasificación de todos los incidentes e inicial soporte Investigación y diagnosis oportunaResolución y recuperación de incidentes a tiempo, reducir el impacto en el negocio e incrementar efectividad Identificación proactiva de enmiendas/mejoras. Negocio enfocado a la administración de información Cierre del requerimiento interno
	NOTICIERO DIGITAL	Informativo interno de las actividades que llevan a cabo cada uno de los órganos administrativos
	KIOSKOS	Servicio de recolección de reclamos y sugerencias que utiliza equipos portátiles ubicados en puntos estratégicos de algunas ciudades del país
MOTORES DE APLICACIÓN	INTERNET INFORMATION SERVER	Internet InformationServices o IIS es un servidor web y un conjunto de servicios para el sistema operativo Microsoft Windows, integrado en otros sistemas operativos de Microsoft destinados a ofrecer servicios. Sirve para correr aplicaciones desarrolladas con visual Studio.
	APACHE	Administración de servidores web utilizados sobre múltiples plataformas con soporte para java y PHP
	ORACLE AP. SERVER	Servidor de aplicaciones para Oracle
	DOMINO WEB ACCESS	Servidor HTTP para plataforma DOMINO
MOVILIDAD	LOTUS MOBILE	Servicio de correo electrónico sobre teléfonos celulares
	TELEFONÍA CELULAR	Convergencia de servicios de telefonía fija y celular. Incorporación de teléfonos celulares a la infraestructura de telefonía IP de la Supertel.
	ACCESO REMOTO	Acceso remoto a servicios institucionales desde Internet utilizando túnel encriptado con IPSEC. Requiere de un software cliente, servidor VPN o firewall configurado para el efecto y aplicación NAC para autenticación de los usuarios que cuentan con el permiso en el active directory
HERRAMIENTAS DE DESARROLLO DE SOFTWARE	RATIONALCOMPOSER	Herramienta para administración de requerimientos de software durante el ciclo de desarrollo de software
	JAZZ TEAM SERVER	Plataforma que permite la integración de herramientas de IBM Rational

Tabla A2.1*Catálogo de Servicios SUPERTEL. (SUPERTEL – Proceso de Diseño de Servicios, 2011).*

ANEXO 3: PLANOS Y MATRICES COBIT DESARROLLADOS DURANTE LA EJECUCION DE LA AUDITORIA A LA SUPERTEL

PLANO DE ENLACE DE LAS METAS DE LA INSTITUCIÓN, METAS TI Y CRITERIOS DE INFORMACIÓN																	
	METAS DE LA INSTITUCION		METAS DE TI								CRITERIOS DE INFORMACION DE COBIT						
											EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO	CONFIABILIDAD
Perspectiva Financiera	1	Proporcionar un buen retorno de inversión de TI	24	28								x					
	2	Gestionar los riesgos de TI que afectan a la institución	2	14	17	18	19	20	21	22			x	X	x		
	3	Fomentar la transparencia	2	18													x
Perspectiva del Cliente	4	Mejorar la orientación y servicio al usuario	3	23							x						
	5	Ofrecer productos y servicios competitivos	5	24							x	x					
	6	Establecer continuidad y disponibilidad de servicios	10	16	22	23					x				x		
	7	Crear agilidad en la respuesta a los cambios de los requerimientos institucionales	1	5	25						x	x					
	8	Lograr optimización de costos en la entrega de servicios	7	8	10	24						x					
	9	Obtener información fiable y útil para tomar decisiones estratégicas	2	4	12	20	26				x			X			x
Perspectiva Interna	10	Mejorar y mantener funcionalidad de los procesos institucionales	6	7	11						x	x					
	11	Reducir el costo de los procesos	7	8	13	15	24					x					
	12	Proporcionar cumplimiento con leyes, reglamentos y regulaciones	2	19	20	21	22	26	27				x			x	
	13	Proporcionar cumplimiento con políticas internas	2	13									x			x	
	14	Gestionar cambios institucionales	1	5	6	11	28				x	x					
	15	Mejorar y mantener operatividad en el control de las telecomunicaciones	7	8	11	13					x	x					
Perspectiva de Aprendizaje y Crecimiento	16	Gestionar productos e innovación de la institución	5	25	28						x	x					
	17	Adquirir y mantener personal cualificado y motivado	9								x	x					

Tabla A3.1*Plano de Enlace de las Metas de la Institución, Metas TI y Criterios de Información.*

PLANO DE ENLACE DE LAS METAS TI, PROCESOS COBIT Y CRITERIOS DE INFORMACIÓN																		
METAS DE TI		PROCESOS DE TI - COBIT										CRITERIOS DE INFORMACION DE COBIT						
												EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO	CONFIABILIDAD
1	Responder a los requerimientos de la institución alineados con el plan estratégico	PO1	PO2	PO4	PO10	AI1	AI6	AI7	DS1	DS3	ME1	P	P		S	S		
2	Responder a los requerimientos de TI en línea con los procesos gobernantes de la SUPERTEL	PO1	PO4	PO10	ME1	ME4						P	P					
3	Asegurar la satisfacción del usuario con la oferta de servicios y niveles de servicio	PO8	AI4	DS1	DS2	DS7	DS8	DS10	DS13			P	P		S	S		
4	Optimizar el uso de la información	PO2	DS11										S		P			S
5	Crear agilidad de TI	PO2	PO4	PO7	AI3							P	P		S			
6	Definir cómo la funcionalidad de las tareas de la institución y requerimientos de control, se trasladan en soluciones efectivas.	AI1	AI2	AI6								P	P				S	
7	Adquirir y mantener sistemas de aplicación integrados y estandarizados	PO3	AI2	AI5								P	P				S	
8	Adquirir y mantener una infraestructura de TI integrada y estandarizada	AI3	AI5									S	P					
9	Adquirir y mantener habilidades de TI que respondan a la estrategia de TI	PO7	AI5									P	P					
10	Asegurar la satisfacción mutua de relaciones con terceras partes	DS2										P	P	S	S	S	S	S
11	Asegurar la integración sin fisuras de las aplicaciones dentro de los procesos de la institución	PO2	AI4	AI7								P	P		S	S		
12	Asegurar la transparencia y la comprensión de costes de TI, beneficios, estrategia, políticas y niveles de servicio.	PO5	PO6	DS1	DS2	DS6	ME1	ME4				P	P				S	S
13	Asegurar el uso apropiado y desempeño de las soluciones de aplicación y tecnología	PO6	AI4	AI7	DS7	DS8						P	S					
14	Tener en cuenta y proteger todos los activos de TI	PO9	DS5	DS9	DS12	ME2						S	S	P	P	P	S	S
15	Optimizar la infraestructura, recursos y capacidades	P	A	D	D	D						S	P					

	de TI	O3	I3	S3	S7	S9												
16	Reducir los defectos de la solución y entrega de servicio.	PO8	AI4	AI6	AI7	DS10						P	P		S	S		
17	Proteger el logro de los objetivos de TI	PO9	DS10	ME2								P	P	S	S	S	S	S
18	Establecer la claridad del impacto de los riesgos a los objetivos y recursos de TI	PO9										S	S	P	P	P	S	S
19	Asegurar que la información crítica y confidencial se retiene a aquellos que no deben tener acceso	PO6	DS5	DS11	DS12									P	P	S	S	S
20	Asegurar que las tareas de la institución sean automatizadas y los cambios a la información sean confiables	PO6	AI7	DS5								P			P	S	S	
21	Asegurar que los servicios de TI y la infraestructura pueden resistir apropiadamente y recuperarse de fallos debidos a errores, ataques deliberados o desastres.	PO6	AI7	DS4	DS5	DS12	DS13	ME2				P	S		S	P		
22	Asegurar el mínimo impacto a las tareas de la institución, en caso de una interrupción de servicios de TI o cambios	PO6	AI6	DS4	DS12							P	S		S	P		
23	Asegurar que los servicios de TI estén disponibles según se requiere	DS3	DS4	DS8	DS13							P	P			P		
24	Mejorar la eficiencia de costes de TI y sus contribuciones a las labores de la institución	PO5	DS6									S	P					S
25	Entregar proyectos a tiempo y sobre presupuesto, reuniendo los estándares de calidad	PO8	PO10									P	P		S			S
26	Mantener la integridad de la información e infraestructura de procesamiento	AI6	DS5									P	P		P	P		S
27	Asegurar que TI cumple con la legislación y regulación nacional.	DS11	ME2	ME3	ME4									S	S		P	S
28	Asegurar que TI demuestra le eficiencia de costes de calidad de servicios, mejora continua y disposición para cambios futuros.	PO5	DS6	ME1	ME4							P	P					P

Tabla A3.2*Plano de Enlace de las Metas TI, Procesos COBIT y Criterios de Información.*

PLANO DE ENLACE PROCESOS DE COBIT A METAS DE TI

PROCESOS DE TI – COBIT		METAS DE TI																										
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
		Responder a los requerimientos de la institución alineados con el plan estratégico	Responder a los requerimientos de TI en línea con los procesos gobernantes de la SUPERTEL	Asegurar la satisfacción del usuario con la oferta de servicios y niveles de servicio	Optimizar el uso de la información	Crear agilidad de TI	Definir cómo la funcionalidad de las tareas de la institución y requerimientos de control, se trasladan en soluciones efectivas.	Adquirir y mantener sistemas de aplicación integrados y estandarizados	Adquirir y mantener una infraestructura de TI integrada y estandarizada	Adquirir y mantener habilidades de TI que responden a la estrategia de TI	Asegurar la satisfacción mutua de relaciones con terceras partes	Asegurar la integración sin fisuras de las aplicaciones dentro de los procesos de la institución	Asegurar la transparencia y la comprensión de costes de TI, beneficios, estrategia, políticas y niveles de servicio.	Asegurar la transparencia y la comprensión de costes de TI, beneficios, estrategia, políticas y niveles de servicio.	Tener en cuenta y proteger todos los activos de TI	Optimizar la infraestructura, recursos y capacidades de TI	Reducir los defectos de la solución y entrega de servicio y reelaborarlos	Proteger el logro de los objetivos de TI	Establecer la claridad del impacto de los riesgos a los objetivos y recursos de TI	Asegurar que la información crítica y confidencial se retiene a aquellos que no deben tener acceso	Asegurar que las tareas de la institución sean automatizadas y los cambios a la información sean confiables	Asegurar que los servicios de TI y la infraestructura pueden resistir apropiadamente y recuperarse de fallos debidos a errores, ataques deliberados o desastres.	Asegurar el mínimo impacto a las tareas de la institución, en caso de una interrupción de servicios de TI o cambios	Asegurar que los servicios de TI estén disponibles según se requiere	Mejorar la eficiencia de costes de TI y sus contribuciones a las labores de la institución	Entregar proyectos a tiempo y sobre presupuesto, reuniendo los estándares de calidad	Mantener la integridad de la información e infraestructura de procesamiento	Asegurar que TI cumple con la legislación y regulación nacional.	Asegurar que TI demuestra le eficiencia de costes de calidad de servicios, mejora continua y disposición para cambios futuros
PLANEAR Y ORGANIZAR																													
PO1	Definición del plan estratégico de TI	X	X																										
PO2	Definición de la arquitectura de la información	X			X	X						X																	
PO3	Determinación de la dirección tecnológica.							X								X													
PO4	Definición de los procesos, organización y relaciones de TI.	X	X			X																							
PO5	Administración de la inversión en TI.												X												X				X
PO6	Comunicación con la Alta Dirección												X	X						X	X	X	X						

PO7	Administración de los recursos humanos de TI.					X				X																		
PO8	Administración de la calidad de TI			X												X									X			
PO9	Evaluación y administración de los riesgos de TI.													X			X	X										
PO10	Administración de los proyectos de TI	X	X																						X			
ADQUIRIR E IMPLEMENTAR																												
AI1	Identificación de las soluciones automatizadas.						X																					
AI2	Adquisición y mantenimiento del software aplicativo.						X	X																				
AI3	Adquisición y mantenimiento de la infraestructura tecnológica.					X			X						X													
AI4	Facilitad de operación y uso de TI			X							X		X			X												
AI5	Adquisición de recursos de TI.							X	X	X																		
AI6	Administración de cambios en TI	X					X									X						X				X		
AI7	Instalación y acreditación de soluciones y cambios en TI	X									X		X			X				X	X							
ENTREGAR Y DAR SOPORTE																												
DS1	Definición y administración de los niveles de servicio.	X		X								X																
DS2	Administración de los servicios de terceros.			X							X		X															
DS3	Administración del desempeño y capacidad de TI	X													X								X					
DS4	Garantías en la continuidad del servicio																				X	X	X					
DS5	Garantías en la seguridad de los sistemas.													X					X	X	X					X		
DS6	Identificación y asignación de costos de TI.											X												X				X
DS7	Educación y entrenamiento a los usuarios.			X									X		X													
DS8	Administración de la mesa de servicios de TI y los incidentes.			X									X										X					

DS9	Administración de la configuración de TI.														X	X													
DS10	Administración de los problemas con TI.			X													X	X											
DS11	Administración de los datos.				X															X								X	
DS12	Administración del ambiente físico.														X					X		X	X						
DS13	Administración de las operaciones de TI.			X																		X		X					
MONITOREAR Y EVALUAR																													
ME1	Monitoreo y evaluación del desempeño de TI.	X	X										X																X
ME2	Monitoreo y evaluación el control interno.														X			X				X						X	
ME3	Garantías en el cumplimiento regulatorio.																											X	
ME4	Proporciona gobierno de TI.		X										X															X	X

Tabla A3.3*Plano de Enlace Procesos de COBIT a Metas de TI.* (COBIT 4.1, 2007)

PLANO DE ENLACE DE PROCESOS COBIT A GOBIERNO DE TI Y CRITERIOS DE INFORMACION

PROCESOS DE TI – COBIT		GOBIERNO DE TI						CRITERIOS DE INFORMACION DE COBIT						
		ALINEACIÓN ESTRATÉGICA	ENTREGA DE VALOR	GESTIÓN DE LOS RIESGOS	GESTIÓN DE RECURSOS	MEDICIÓN DEL DESEMPEÑO		EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO	CONFIABILIDAD
PLANEAR Y ORGANIZAR														
PO1	Definición del plan estratégico de TI	P		S	S			P	S				T	
PO2	Definición de la arquitectura de la información	P	S	P	S			S	P	S	P			
PO3	Determinación de la dirección tecnológica.	S	S	P	S			P	P					T
PO4	Definición de los procesos, organización y relaciones de TI.	S		P	P			P	P					S
PO5	Administración de la inversión en TI.	S	P	S		S		P	P		T			
PO6	Comunicación con la Alta Dirección	P			P			P					S	
PO7	Administración de los recursos humanos de TI.	P		P	S	S		P	P					
PO8	Administración de la calidad de TI	P	S		S			P	P		S			S
PO9	Evaluación y administración de los riesgos de TI.	P			P			S	S	P	P	P	S	S
PO10	Administración de los proyectos de TI	P	S	S	S	S		P	P					
ADQUIRIR E IMPLEMENTAR														
AI1	Identificación de las soluciones automatizadas.	P	P	S	S			P	S				T	
AI2	Adquisición y mantenimiento del software aplicativo.	P	P		S			P	P		S			S
AI3	Adquisición y mantenimiento de la infraestructura tecnológica.			P				S	P		S	S		
AI4	Facilitad de operación y uso de TI	S	P	S	S			P	P		S	S	S	S
AI5	Adquisición de recursos de TI.		S	P				S	P				S	
AI6	Administración de cambios en TI		P	S				P	P		P	P		S
AI7	Instalación y acreditación de soluciones y cambios en TI	S	P	S	S	S		P	S		S	´S		
ENTREGAR Y DAR SOPORTE														
DS1	Definición y administración de los niveles de servicio.	P	P	P		P		P	P	S	S	S	S	S
DS2	Administración de los servicios de terceros.		P	S	P	S		P	P	S	S	S	S	S

DS3	Administración del desempeño y capacidad de TI	S	S	P	S	S		P	P			S		
DS4	Garantías en la continuidad del servicio	S	P	S	P	S		P	S			P		
DS5	Garantías en la seguridad de los sistemas.				P				T	P	P	S	S	S
DS6	Identificación y asignación de costos de TI.		S	P		S			P					P
DS7	Educación y entrenamiento a los usuarios.	S	P	S	S			P	S			T		
DS8	Administración de la mesa de servicios de TI y los incidentes.		P			S		P	P			T		
DS9	Administración de la configuración de TI.		P	P	S			P	S			S		S
DS10	Administración de los problemas con TI.		P		S	S		P	P			S		
DS11	Administración de los datos.		P	P	P			T	T		P			P
DS12	Administración del ambiente físico.			S	P			T	T		P	P		
DS13	Administración de las operaciones de TI.			P				P	P		S	S		
MONITOREAR Y EVALUAR														
ME1	Monitoreo y evaluación del desempeño de TI.	S	S	S	S	P		P	P	S	S	S	S	S
ME2	Monitoreo y evaluación el control interno.		P		P			P	P	S	S	S	S	S
ME3	Garantías en el cumplimiento regulatorio.	P			P			P	P				P	S
ME4	Proporciona gobierno de TI.	P	P	P	P	P		P	P	S	S	S	S	S

P= Relación Primaria S=Relación Secundaria T=Relación Terciaria

Tabla A3.4*Plano de Enlace de Procesos COBIT a Gobierno de TI y Criterios de Información.*(COBIT 4.1, 2007)

PLANO DE RESPONSABILIDADES DE PROCESOS COBIT					
PROCESOS DE TI - COBIT		Responsable			
		Unidad de TI	Dentro de la Institución	Externo	No se sabe con certeza
PLANEAR Y ORGANIZAR					
PO1	Definición del plan estratégico de TI	x			
PO2	Definición de la arquitectura de la información	x			
PO3	Determinación de la dirección tecnológica.	x			
PO4	Definición de los procesos, organización y relaciones de TI.	x			
PO5	Administración de la inversión en TI.	x			
PO6	Comunicación con la Alta Dirección	x			
PO7	Administración de los recursos humanos de TI.	x			
PO8	Administración de la calidad de TI	x			
PO9	Evaluación y administración de los riesgos de TI.	x			
PO10	Administración de los proyectos de TI	x			
ADQUIRIR E IMPLEMENTAR					
AI1	Identificación de las soluciones automatizadas.	x			
AI2	Adquisición y mantenimiento del software aplicativo.	x			
AI3	Adquisición y mantenimiento de la infraestructura tecnológica.	x			
AI4	Facilitad de operación y uso de TI	x			
AI5	Adquisición de recursos de TI.	x			
AI6	Administración de cambios en TI	x			
AI7	Instalación y acreditación de soluciones y cambios en TI	x			

ENTREGAR Y DAR SOPORTE					
DS1	Definición y administración de los niveles de servicio.	x			
DS2	Administración de los servicios de terceros.	x			
DS3	Administración del desempeño y capacidad de TI	x			
DS4	Garantías en la continuidad del servicio	x			
DS5	Garantías en la seguridad de los sistemas.	x			
DS6	Identificación y asignación de costos de TI.	x			
DS7	Educación y entrenamiento a los usuarios.	x			
DS8	Administración de la mesa de servicios de TI y los incidentes.	x			
DS9	Administración de la configuración de TI.	x			
DS10	Administración de los problemas con TI.	x			
DS11	Administración de los datos.	x			
DS12	Administración del ambiente físico.	x			
DS13	Administración de las operaciones de TI.	x			
MONITOREAR Y EVALUAR					
ME1	Monitoreo y evaluación del desempeño de TI.	x			
ME2	Monitoreo y evaluación el control interno.	x			
ME3	Garantías en el cumplimiento regulatorio.	x			
ME4	Proporciona gobierno de TI.	x			

Tabla A3.5*Plano de Responsabilidades de Procesos COBIT.*(COBIT 4.1, 2007)

MATRIZ DE GRADOS DE MADUREZ DE PROCESOS – SUPERTEL			
PROCESOS DE TI - COBIT		**Grado de Madurez**	**Nivel de Madurez**
PLANEAR Y ORGANIZAR			**3***
PO1	Definición del plan estratégico de TI	66,67%	4
PO2	Definición de la arquitectura de la información	77,78%	4
PO3	Determinación de la dirección tecnológica.	80,00%	4
PO4	Definición de los procesos, organización y relaciones de TI.	87,50%	3
PO5	Administración de la inversión en TI.	83,33%	3
PO6	Comunicación con la Alta Dirección	50,00%	3
PO7	Administración de los recursos humanos de TI.	60,00%	3
PO8	Administración de la calidad de TI	60,00%	3
PO9	Evaluación y administración de los riesgos de TI.	66,67%	2
PO10	Administración de los proyectos de TI	77,78%	4
ADQUIRIR E IMPLEMENTAR			**3***
AI1	Identificación de las soluciones automatizadas.	100,00%	4
AI2	Adquisición y mantenimiento del software aplicativo.	80,00%	3
AI3	Adquisición y mantenimiento de la infraestructura tecnológica.	100,00%	5
AI4	Facilitad de operación y uso de TI	50,00%	3
AI5	Adquisición de recursos de TI.	100,00%	3
AI6	Administración de cambios en TI	55,56%	4
AI7	Instalación y acreditación de soluciones y cambios en TI	62,50%	4

ENTREGAR Y DAR SOPORTE			4*
DS1	Definición y administración de los niveles de servicio.	50,00%	3
DS2	Administración de los servicios de terceros.	100,00%	3
DS3	Administración del desempeño y capacidad de TI	71,43%	4
DS4	Garantías en la continuidad del servicio	75,00%	4
DS5	Garantías en la seguridad de los sistemas.	83,33%	4
DS6	Identificación y asignación de costos de TI.	71,43%	4
DS7	Educación y entrenamiento a los usuarios.	71.43%	4
DS8	Administración de la mesa de servicios de TI y los incidentes.	57,14%	4
DS9	Administración de la configuración de TI.	60,00%	4
DS10	Administración de los problemas con TI.	57,14%	4
DS11	Administración de los datos.	75,00%	5
DS12	Administración del ambiente físico.	75,00%	4
DS13	Administración de las operaciones de TI.	60,00%	4
MONITOREAR Y EVALUAR			**3***
ME1	Monitoreo y evaluación del desempeño de TI.	87,50%	3
ME2	Monitoreo y evaluación el control interno.	57,14%	3
ME3	Garantías en el cumplimiento regulatorio.	57,14%	4
ME4	Proporciona gobierno de TI.	45,45%	5

*Los valores son obtenidos de la moda de los procesos correspondientes

Tabla A3.6*Matriz de Grados de Madurez de Procesos – SUPERTEL.*(COBIT 4.1, 2007)

MATRIZ DE NIVEL DE SERVICIO – SUPERTEL									
PROCESOS DE TI - COBIT		DESEMPEÑO							
		NO CUMPLE	CUMPLE LEVEMENTE	CUMPLE PARCIALMENTE	CUMPLE MAYORITARIAMENTE	CUMPLE CASI TOTALMENTE	CUMLE TOTALMENTE	%
PLANEAR Y ORGANIZAR								58,59%
PO1	**Plan Estratégico de TI.** TI pose un plan estratégico que define la forma en que TI dará soporte a los programas de inversión, entrega de servicios, y cooperación con los objetivos estratégicos institucionales.					X		62,96%
PO2	**Arquitectura de la Información.** El modelo de arquitectura de la información facilita el desarrollo de aplicaciones, y actividades de			x				39,17%

	soporte a la toma de decisiones, así como también ayuda a conservar la integridad, disponibilidad y funcionalidad de la información. Se tiene un diccionario de datos que fomenta un entendimiento común entre los usuarios y previene la creación de datos incompatibles. El esquema de clasificación de datos permite aplicar controles de acceso y/o encriptación de la información.							
PO3	**Dirección Tecnológica.** TI proporciona soluciones tecnológicas consistentes, efectivas y seguras para toda la institución, basadas en tendencias del sector y aspectos legales y regulatorios.				x			48,00%
PO4	**Procesos, organización y relaciones de TI.** TI posee un marco de trabajo para ejecutar el plan estratégico de TI que incluye la medición del desempeño, y administración de la calidad, y además permite mantener una estructura de enlace, comunicación y coordinación óptima entre la función de TI y los funcionarios dentro y fuera de TI.				x			44,81%
PO5	**Inversión en TI**. TI prioriza la asignación de recursos de para las operaciones, proyectos y mantenimiento que maximicen la contribución de TI a optimizar el retorno del portafolio de programas de inversión en TI y otros servicios y activos de TI.					x		75,00%
PO6	**Aspiraciones de con la Alta Dirección.** Existen políticas de apoyo a la estrategia de TI que incluyan la intención de la alta dirección, los roles y responsabilidades, los estándares y directrices del enfoque de cumplimiento; que atiendan temas de calidad, seguridad, confidencialidad, y propiedad intelectual					x		75,19%
PO7	**Recursos humanos de TI.** Se proporciona a los funcionarios de TI la orientación necesaria y capacitación continua para desarrollar su conocimiento, aptitudes, y habilidades.					x		75,19%
PO8	**Calidad de TI.** TI posee sistemas de administración de la calidad cubriendo roles, tareas y responsabilidades, respecto a la resolución de conflictos entre el usuario y la unidad de TI.				x			60,00%
PO9	**Administración de riesgos de TI.** TI identifica amenazas y vulnerabilidades con un impacto potencial sobre los objetivos institucionales y de TI y mantiene respuestas a los riesgos que garanticen el costo beneficio de las medidas de seguridad.				x			48,89%
PO10	**Proyectos de TI.** TI posee un marco de trabajo que define las metodologías adoptadas y aplicadas a cada proyecto, incluyendo puntos de control, evaluación de riesgos, y gestión de cambios. Además existe el compromiso y la participación de los interesados afectados en la ejecución de los proyectos.				x			56,67%
ADQUIRIR E IMPLEMENTAR								58,03%
AI1	**Soluciones automatizadas.** TI identifica, y prioriza los requerimientos funcionales y técnicos que cubran el alcance completo de todas las iniciativas necesarias para lograr los resultados institucionales esperados.				x			48,33%
AI2	**Software aplicativo**. TI da seguimiento a los estados de los requerimientos particulares y a sus modificaciones durante el diseño, desarrollo, implementación, y puesta en marcha de aplicaciones. Mantiene una estrategia óptima para la corrección de fallas, mejoras, mantenimiento de la documentación, cambios de emergencia, interdependencia con otras aplicaciones, los riesgos y requerimientos de seguridad.				x			50,83%
AI3	**Infraestructura tecnológica.** TI posee un plan para adquirir, implementar y mantener la infraestructura tecnológica considerando los riesgos tecnológicos, y la vida útil de la inversión.					x		61,85%
AI4	**Facilidad de Operación y uso de TI.** TI transfiere el conocimiento y las habilidades a los usuarios finales incluyendo materiales de capacitación, manuales de usuario, manuales de procedimientos, ayuda en línea, asistencia a usuarios y evaluación.					x		69,26%
AI5	**Recursos de TI.** TI asegura la protección de los intereses de la institución en todos los acuerdos contractuales de adquisición de TI					x		69,63%

	incluyendo, licencias, mantenimiento, garantías, procedimientos de arbitraje, condiciones para la actualización, seguridad, custodia y derechos de acceso.							
AI6	**Administración de Cambios en TI.** TI posee procesos estándar para definir, sensibilizar, evaluar y autorizar los cambios formales y procesos diferenciados para asistir cambios de emergencia de manera oportuna.				x			42,96%
AI7	**Soluciones y cambios en TI.** TI posee un plan establecido para que todos los elementos necesarios tales como hardware, software, datos de transacciones, archivos maestros, interfaces, procedimientos y documentación sean convertidos de los viejos a los nuevos sistemas, manteniendo una auditoría de los resultados previos y posteriores a la conversión, siguiendo planes de implementación, pruebas y de aceptación.					x		63,33%
ENTREGAR Y DAR SOPORTE								63,32%
DS1	**Niveles de servicio.** TI tiene definido un marco de trabajo que brinde un proceso formal de administración de niveles de servicio entre los funcionarios y TI. Tomando en cuenta los criterios de desempeño para identificar tendencias positivas y negativas que permitan realizar mejoras.					x		67,78%
DS2	**Servicios de terceros.** TI posee procesos de monitoreo de los servicios proporcionados por terceros para asegurar que el proveedor se apegue a los acuerdos contractuales y de nivel de servicio, y que el desempeño sea competitivo con las condiciones del mercado.					x		61,11%
DS3	**Desempeño y la Capacidad de TI**. TI revisa la capacidad y el desempeño de los recursos de TI en intervalos regulares, para minimizar el riesgo de interrupciones del servicio originadas por la falta de capacidad o degradación del desempeño. La información recolectada se utiliza para realizar ajustes.					x		67,33%
DS4	**Continuidad del servicio.** TI posee planes de continuidad de TI, diseñados para reducir el impacto de una interrupción mayor de las funciones y los procesos clave de la institución. Los usuarios reciben sesiones de formación sobre los procedimientos en caso de incidentes o desastre y sus responsabilidades.					x		75,83%
DS5	**Seguridad de los sistemas.** TI administra la seguridad al nivel más apropiado y alineado con los requerimientos de la institución, identifica de manera única a todos los usuarios, garantiza que se cuenta con medidas de prevención, detección y corrección (parches de seguridad, y antivirus) para proteger los sistemas de información, y garantiza que se utilizan técnicas de seguridad y procedimientos de administración asociados (firewalls, dispositivos de seguridad, segmentación de redes y detección de intrusos) para autorizar el acceso y controlar los flujos de información desde y hacia las redes.				x			50,67%
DS6	**Asignación de Costos de TI.** TI identifica todos los costos y los equipara con los servicios brindados para soportar un modelo de costos transparente.				x			54,17%
DS7	**Entrenamiento a los usuarios de TI.** TI establece y actualiza de forma regular un programa de capacitación para cada grupo objetivo de funcionarios y al finalizar evalúa la calidad, percepción, retención del conocimiento y el costo.					x		67,78%
DS8	**Mesa de servicios de TI.** TI posee una mesa de servicios como conexión entre usuarios con TI que registra, comunica, atiende y analiza, todas las llamadas, los incidentes reportados, los requerimientos de servicio y las solicitudes de información. Se evalúa la actividad de la mesa de servicios, que permite medir el desempeño y los tiempos de respuesta, así como identificar tendencias de problemas recurrentes de forma que el servicio pueda mejorarse de forma continua.					x		67,33%
DS9	**Configuraciones de TI.** TI establece un repositorio central que contiene toda la información referente a los elementos de configuración					x		71,48%

	de hardware, software y las herramientas para operar, acceder y utilizar los sistemas y los servicios. TI revisa y verifica de manera regular el estado de los elementos de configuración y la existencia de cualquier software personal o no autorizado.							
DS10	**Administración de Problemas con TI.** Existen procesos para reportar y clasificar problemas que han sido identificados, incluyendo categorías, impacto, urgencia y prioridad. TI identifica la causa raíz de todos los problemas reportados, y genera soluciones sostenibles.				x			54,07%
DS11	**Administración de los Datos.** TI garantiza que se procesa toda la información recibida por parte de la institución, se preparan y entregan todos los reportes que requiere la institución y que las necesidades de los funcionarios están soportadas. Los datos permanecen accesibles y utilizables, considerando requerimientos de recuperación, rentabilidad, integridad, seguridad y cumplimientos legales.				x			45,19%
DS12	**Ambiente físico.** TI selecciona los centros de datos físicos considerando los riesgos asociados con desastres, ubicación del equipo crítico, áreas restringidas, las leyes y regulaciones de seguridad y salud ocupacional.					x		74,67%
DS13	**Operaciones de TI.** TI organiza la programación de los trabajos, procesos y tareas dentro de una secuencia eficiente, maximizando el rendimiento y utilización para alcanzar los requerimientos de la institución.					x		65,71%
MONITOREAR Y EVALUAR								65,49%
ME1	**Monitoreo del desempeño de TI.** Se realiza un monitoreo general de TI para medir los resultados de los servicios otorgados, y la satisfacción de los usuarios e inicia acciones correctivas en base a la evaluación periódica del desempeño contra las metas.				x			57,50%
ME2	**Evaluación del Control interno.** Se monitorea y reporta la efectividad de los controles internos sobre TI por medio de revisiones de auditoría externa, y prácticas de benchmarking. (Comparar con modelos institucionales líderes a nivel mundial)					x		64,44%
ME3	**Cumplimiento regulatorio.** TI garantiza el cumplimiento de los requisitos legales y regulatorios que cubren las políticas, estándares y procedimientos de TI.					x		69,26%
ME4	**Gobierno de TI.** TI trabaja con el consejo directivo para establecer un marco de trabajo para el gobierno de TI que incluye el liderazgo, los procesos, roles, responsabilidades, requerimientos de información, y estructuras organizacionales para garantizar que los programas de inversión habilitados por TI estén alineados con los objetivos institucionales.					x		70,74%

Tabla A3.7*Matriz de Nivel de Servicio USUARIOS – SUPERTEL.* (COBIT 4.1, 2007)

MATRIZ DE EVALUACIÓN DE PROCESOS BAJO MÉTRICAS COBIT							
	METRICAS COBIT						
PROCESOS DE TI -COBIT	NO CUMPLE	CUMPLE LEVEMENT	CUMPLE PARCIALME	CUMPLE MAYORITA	CUMPLE CASI TOTA	CUMPLE TOTALMEN	%

			E	NTE	RIAMENTE	LMENTE	TE	
PLANEAR Y ORGANIZAR								75,46%
PO1	Plan Estratégico de TI					X		80,00%
	Los objetivos de TI dan soporte al plan estratégico de la institución.					X		80,00%
	Los proyectos de TI en el portafolio de proyectos, se pueden rastrear hacia el plan táctico de TI.					X		80,00%
	Las actualizaciones del plan estratégico de TI se reflejan en actualizaciones de los planes tácticos de TI.					X		80,00%
PO2	Arquitectura de la Información					X		80,00%
	Se tiene un control efectivo de datos redundantes / duplicados.					X		80,00%
	Las aplicaciones existentes cumplen con la metodología de arquitectura de la información usada por la institución				X			60,00%
	Se efectúan actividades de validación de datos con frecuencia.						X	100,00 %
PO3	Dirección Tecnológica					X		80,00%
	El plan de infraestructura tecnológica se cumple sin desviaciones.					X		80,00%
	El plan de infraestructura tecnológica se revisa y actualiza con frecuencia.					X		80,00%
PO4	Procesos, Organización y Relaciones de TI						X	86,67%
	Los puestos de trabajo y sus roles se encuentran completamente documentados.						X	100,00 %
	Todas las unidades/procesos que conforman la SUPERTEL reciben soporte oportuno de TI de acuerdo con la estrategia institucional.					X		80,00%
	Todas las actividades clave de TI están sujetas a los estándares institucionales.					X		80,00%
PO5	Inversión en TI					X		80,00%
	Se tiene una adecuada relación costo-beneficio para todos los servicios de TI.					X		80,00%
PO6	Comunicación con la Alta Dirección					X		66,67%
	Las interrupciones en el servicio de TI son solucionadas de manera oportuna garantizando la continuidad de las operaciones de la institución.					X		80,00%
	Existe una comprensión mayoritaria del marco de trabajo de control de TI, por parte de los funcionarios.				X			60,00%
	Los funcionarios cumplen las políticas establecidas por TI.				X			60,00%
PO7	Recursos Humanos de TI					X		66,67%
	Se realiza una revisión periódica del desempeño del personal de TI.				X			60,00%
	Existe apoyo a los planes tácticos de TI mediante contratación y entrenamiento del personal de TI.					X		80,00%

	Existen planes de mitigación del riesgo de sobre-dependencia de recursos clave.				X			60,00%
PO8	Calidad de TI					X		70,00%
	Los funcionarios se encuentran satisfechos con la calidad de servicios de TI				X			60,00%
	Los procesos de TI son revisados de manera formal para asegurar su calidad.					X		80,00%
PO9	Administración de riesgos de TI					X		66,67%
	Todos los objetivos críticos de TI son cubiertos por la evaluación de riesgos.				X			60,00%
	Todos los riesgos críticos de TI son identificados con planes de acción elaborados.				X			60,00%
	Todos los planes de acción de administración de riesgos son aprobados para su implantación.					X		80,00%
PO10	Proyectos de TI					X		80,00%
	Los proyectos satisfacen las expectativas de los interesados (a tiempo, dentro del presupuesto, y con satisfacción de los requerimientos – ponderados por importancia)					X		80,00%
	Los proyectos son revisados post-implantación					X		80,00%
	Los proyectos siguen estándares y prácticas de administración de proyectos.					X		80,00%
ADQUIRIR E IMPLEMENTAR								71,20%
AI1	Soluciones automatizadas				X			60,00%
	Se realizan estudios de factibilidad de proyectos autorizados por la unidad dueña del proceso.				X			60,00%
	Los usuarios se encuentran satisfechos con la funcionalidad entregada por las soluciones automatizadas.				X			60,00%
AI2	Software aplicativo					X		70,00%
	Los problemas suscitados en la producción de aplicaciones no causan pérdidas de tiempo significativas.					X		80,00%
	Los usuarios se encuentran satisfechos con la funcionalidad entregada por el software aplicativo.				X			60,00%
AI3	Infraestructura tecnológica						X	90,00%
	Las plataformas se alinean con la arquitectura y estándares de TI definidos.						X	100,00 %
	Los procesos críticos se encuentran soportados por infraestructura tecnológica actualizada (no obsoleta o que pronto lo será).					X		80,00%
AI4	Facilidad de Operación y Uso de TI					X		66,67%
	Las aplicaciones integran los procedimientos de TI en forma transparente dentro de los procesos institucionales.					X		80,00%
	Los funcionarios se encuentran satisfechos con el entrenamiento y los materiales de apoyo.				X			60,00%
	Las aplicaciones cuentan con un plan adecuado de apoyo al usuario y a la operación.				X			60,00%
AI5	Recursos de TI					X		66,67%
	Los contratos de adquisición de recursos de TI se desempeñan sin controversias.				X			60,00%

	Se mantienen procesos de reducción del costo de compras				X			60,00%
	Los funcionarios se encuentran satisfechos con los proveedores de recursos y servicios de TI.					X		80,00%
AI6	Administración de cambios en TI					X		73,33%
	Existen especificaciones de cambio necesarias y una evaluación del impacto adecuados, para minimizar el numero de interrupciones o errores de datos frente a cambios.					X		80,00%
	Las especificaciones de cambio son adecuadas y garantizan la implementación de aplicaciones e infraestructura sin redundancias.					X		80,00%
	Los cambios siguen procesos de control de cambio formales.				X			60,00%
AI7	Soluciones y cambios en TI					X		73,33%
	Los planes de pruebas optimizan el tiempo invertido y reducen la aparición de problemas de datos.					X		80,00%
	Los sistemas implementados satisfacen los beneficios esperados.				X			60,00%
	Todos los proyectos poseen un plan de pruebas documentado y aprobado.					X		80,00%
ENTREGAR Y DAR SOPORTE								64,03%
DS1	Niveles de Servicio					X		66,67%
	Los funcionarios se encuentran satisfechos con los niveles de servicio entregados.				X			60,00%
	Todos los servicios entregados constan en un catálogo de servicios.				X			60,00%
	Se establecen reuniones formales periódicas para la revisión del Acuerdo de Niveles de Servicio (SLA) con los funcionarios.					X		80,00%
DS2	Servicios de Terceros					X		66,67%
	El número de quejas de los funcionarios debidas a los servicios contratados es mínimo o nulo.					X		80,00%
	Los proveedores cumplen claramente los requerimientos definidos y los niveles de servicio.				X			60,00%
	Los proveedores de servicios están sujetos a monitoreo.				X			60,00%
DS3	Desempeño y Capacidad de TI					X		70,00%
	El numero de horas perdidas por usuario al mes, debidas a la falta de planeación de la capacidad es mínimo o nulo					X		80,00%
	TI satisface los Acuerdos de Niveles de Servicio (SLA's) referentes al tiempo de respuesta de un requerimiento.				X			60,00%
DS4	Continuidad del Servicio					X		70,00%
	El número de horas perdidas por usuario al mes, debidas a interrupciones no planeadas es mínimo o nulo.					X		80,00%
	Los procesos críticos que dependen de TI, están cubiertos por un plan de continuidad.				X			60,00%
DS5	Seguridad de los Sistemas				X			60,00%
	El número de incidentes que dañan la reputación con los usuarios es bajo.					X		80,00%
	Todos los sistemas cumplen los requerimientos de seguridad.			X				40,00%
DS6	Asignación de Costos de TI					X		73,33%
	Las facturas de servicios de TI provistos por terceros son canceladas a tiempo.					X		80,00%

	La variación entre los presupuestos, pronósticos y costos actuales es manejable.					X		80,00%
	Los costos totales de TI son distribuidos de acuerdo con los modelos acordados.				X			60,00%
DS7	Entrenamiento a los usuarios de TI				X			46,67%
	El número de llamadas de soporte debido a fallas de entrenamiento es mínimo o nulo.				X			60,00%
	Los usuarios se encuentran satisfechos con el entrenamiento recibido.				X			60,00%
	El lapso de tiempo entre la identificación de la necesidad de entrenamiento y la impartición del mismo, es corto y satisfactorio.		X					20,00%
DS8	Mesa de Servicios de TI				X			53,33%
	Lo usuarios están satisfechos con el soporte de primera línea.			X				40,00%
	Los incidentes son resueltos dentro de un lapso de tiempo aceptable / acordado.				X			60,00%
	El Índice de abandono de llamadas por larga espera es bajo.				X			60,00%
DS9	Configuraciones de TI					X		73,33%
	El número de problemas de cumplimiento debido a la inadecuada configuración de los sistemas es mínimo o nulo.					X		80,00%
	Las configuraciones actuales de los sistemas se rigen al repositorio de configuración establecido.				X			60,00%
	Todas las licencias compradas constan en el repositorio.					X		80,00%
DS10	Administración de Problemas con TI				X			60,00%
	El número de problemas recurrentes es mínimo o nulo.				X			60,00%
	Todos los problemas son resueltos dentro del período de tiempo solicitado.				X			60,00%
DS11	Administración de los Datos				X			60,00%
	Los funcionarios están satisfechos con la disponibilidad de la información.			X				40,00%
	Las restauraciones de datos son siempre exitosas.				X			60,00%
	La pérdida de datos sensitivos es mínima o nula.					X		80,00%
DS12	Ambiente Físico					X		66,67%
	El tiempo sin servicio ocasionado por incidentes relacionados con el ambiente físico es prácticamente nulo.					X		80,00%
	El número de incidentes ocasionados por fallas o brechas de seguridad física es mínimo o nulo.					X		80,00%
	La revisión y evaluación de riesgos físicos se realiza con frecuencia.			X				40,00%
DS13	Operaciones de TI					X		66,67%
	Los niveles de servicio no se ven afectados por incidentes en la operación.				X			60,00%
	El tiempo sin servicio a causa de incidentes en la operación es nulo.				X			60,00%
	Los activos de hardware se encuentran incluidos en los programas de mantenimiento.					X		80,00%
MONITOREAR Y EVALUAR								60,00%
ME1	Monitoreo del desempeño de TI				X			60,00%

	La alta dirección se encuentra plenamente satisfecha con los reportes de desempeño de TI				X			60,00%
	Las actividades de monitoreo impulsan acciones de mejoramiento que se concretan.				X			60,00%
	Los procesos críticos de la SUPERTEL son monitoreados.				X			60,00%
ME2	Evaluación del control Interno				X			50,00%
	Frecuentemente se toman en cuenta iniciativas para la mejora del control interno.				X			60,00%
	Se realizan auto evaluaciones de control.			X				40,00%
ME3	Cumplimiento regulatorio.				X			60,00%
	El costo del no cumplimiento de TI, incluyendo arreglos y multas es nulo.					X		80,00%
	La demora entre la identificación de los problemas externos de cumplimiento y su resolución es aceptable.				X			60,00%
	Se realizan revisiones frecuentes para asegurar el cumplimiento regulatorio.			X				40,00%
ME4	Gobierno de TI					X		70,00%
	Se emiten informes oportunos y satisfactorios de TI hacia el consejo directivo. (incluyendo el nivel de madurez)						X	100,00 %
	Se realizan revisiones independientes del cumplimiento de TI.			X				40,00%

Tabla A3.8*Matriz de Evaluación de Procesos bajo Métricas COBIT.* (COBIT 4.1, 2007)

MATRIZ DE CUMPLIMIENTO DE OBJETIVOS DE CONTROL – COBIT								
		OBJETIVOS DE CONTROL						
PROCESOS DE TI -COBIT		NO CUMPLE	CUMPLE LEVEMENTE	CUMPLE PARCIALMENTE	CUMPLE MAYORITARIAMENTE	CUMPLE CASI TOTALMENTE	CUMPLE TOTALMENTE	%
PLANEAR Y ORGANIZAR								77,09%
PO1	Plan estratégico de TI					X		76,67%
	Administración del Valor de TI. La rendición de cuentas del logro de los beneficios y del control de costos es claramente asignada y monitoreada.					X		80,00%

	Alineación de TI con la Institución. Las estrategias de la institución y de TI están integradas y son comunicadas de manera amplia.					X		80,00%
	Evaluación del Desempeño y la Capacidad Actual. Se evalúa el desempeño de los planes existentes y de los sistemas existentes en términos de su contribución con la institución.				X			60,00%
	Plan Estratégico de TI. El plan estratégico define la forma en que TI dará soporte a los programas de inversión, entrega de servicios, y cooperación con los objetivos estratégicos institucionales.					X		80,00%
	Planes Tácticos de TI. Los planes tácticos, se derivan del plan estratégico de TI, e incluyen las iniciativas y requerimientos de recursos.					X		80,00%
	Administración del Portafolio de TI. La administración del portafolio de TI incluye la definición de los proyectos, la asignación de recursos, garantías, responsables, y resultados deseados.					X		80,00%
PO2	Arquitectura de la información					X		75,00%
	Modelo de Arquitectura de Información. El modelo de arquitectura de la información facilita el desarrollo de aplicaciones, y actividades de soporte a la toma de decisiones, así como también ayuda a conservar la integridad, disponibilidad y funcionalidad de la información					X		80,00%
	Diccionario de Datos y Reglas de Sintaxis de Datos. Se mantiene un diccionario de datos institucional que incluye las reglas de sintaxis de los datos de la organización, y fomenta un entendimiento común entre los funcionarios previniendo la creación de datos incompatibles.					X		80,00%
	Esquema de Clasificación de Datos. El esquema de clasificación de datos incluye como mínimo los niveles de seguridad y criticidad, además permite aplicar controles de acceso y/o encriptación de la información.					X		80,00%
	Administración de Integridad. Se ha definido e implementado procedimientos para garantizar la integridad y consistencia de todos los datos almacenados en formato electrónico, tales como bases de datos, almacenes de datos y archivos.				X			60,00%
PO3	Dirección tecnológica					x		76,00%
	Planeación de la Dirección Tecnológica. Se planea cual dirección tecnológica es apropiada tomar para materializar la estrategia de TI y la arquitectura del sistema de la institución, considerando estrategias de migración y aspectos de contingencia.					X		80,00%
	Plan de Infraestructura Tecnológica. Existe un plan de infraestructura tecnológica y está de acuerdo con el plan estratégico y táctico de TI.						X	100,00%
	Monitoreo de Tendencias y Regulaciones Futuras. Existen procesos para monitorear las tendencias del sector, las tecnologías, la infraestructura y los aspectos legales y regulatorios.				X			60,00%
	Estándares Tecnológicos. Se proporcionan soluciones tecnológicas consistentes, efectivas y seguras para toda la institución.					X		80,00%
	Consejo de Arquitectura de TI. Existe un consejo de arquitectura de TI que proporciona directrices sobre la arquitectura y asesoría de su aplicación y verifica el cumplimiento.				X			60,00%
PO4	Procesos, organización y relaciones de TI					X		74,67%
	Marco de Trabajo de Procesos de TI. Existe un marco de trabajo del proceso de TI para ejecutar el plan estratégico e incluye la medición del desempeño, y administración de la calidad.					X		80,00%
	Comité Estratégico de TI. Existe un comité estratégico de TI a nivel del consejo directivo, que garantiza que el gobierno de TI se maneja de forma adecuada.					X		80,00%

	Comité Directivo de TI. Existe un comité directivo de TI compuesto por la administración ejecutiva de la institución y de TI, que determina las prioridades de los programas de inversión, da seguimiento al estado de los proyectos y monitorea los niveles del servicio.					X		80,00%
	Ubicación Organizacional de la Función de TI. Se ubica a la función de TI dentro de la estructura institucional, supeditada a la importancia dentro de la organización.						X	100,00%
	Estructura Organizacional. Se implementan procesos para revisar la estructura organizacional de TI de forma periódica para ajustar los requerimientos de personal y las estrategias internas para satisfacer los objetivos institucionales y las circunstancias cambiantes.					x		80,00%
	Establecimiento de Roles y Responsabilidades. Se establece y actualiza periódicamente la descripción de roles, de manera que estén alineados con las habilidades, experiencias y evaluación del desempeño.				X			60,00%
	Responsabilidad de Aseguramiento de Calidad de TI. Existen controles e aseguramiento de calidad que satisfacen los requerimientos de la institución.					X		80,00%
	Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento. Se define y asigna roles críticos para administrar los riesgos, la seguridad física y el cumplimiento.				X			60,00%
	Propiedad de Datos y de Sistemas. Existen herramientas que permiten enfrentar las responsabilidades sobre la propiedad de los datos y sistemas de información.					X		80,00%
	Supervisión. Se supervisa que se ejerzan de forma apropiada los roles, responsabilidades y desempeño.					x		80,00%
	Segregación de Funciones. Se implementa una división de roles y responsabilidades que reduzca la posibilidad de que un solo individuo afecte negativamente un proceso crítico y se asegura de que el personal realice sólo tareas relevantes a sus puestos.					X		80,00%
	Personal de TI. El proceso de dotación de personal toma en cuenta la capacitación funcional cruzada, la rotación de puestos y las oportunidades de personal externo.				X			60,00%
	Personal Clave de TI. Se identifica el personal clave y se tiene un plan para contactarlo en caso de emergencia.				X			60,00%
	Políticas y Procedimientos para Personal Contratado. Se definen e implementan procedimientos que garanticen la protección de los activos de la institución y el cumplimiento de los acuerdos contractuales.					x		80,00%
	Relaciones. Se establece y mantiene una estructura de enlace, comunicación y coordinación óptima entre la función de TI y los funcionarios dentro y fuera de TI.				X			60,00%
PO5	Inversión en TI					X		76,00%
	Marco de Trabajo para la Administración Financiera. Existe un marco de trabajo financiero para TI, que impulse el presupuesto y el análisis de rentabilidad basado en los portafolios de inversión, de servicios y de activos.					X		80,00%
	Prioridades Dentro del Presupuesto de TI. Se prioriza la asignación de recursos de TI para las operaciones, proyectos y mantenimiento, que maximice la contribución de TI a optimizar el retorno del portafolio institucional de programas de inversión en TI.					x		80,00%
	Proceso Presupuestal. Existe un proceso para elaborar y administrar el presupuesto, que incluya los costos recurrentes de operación y mantenimiento de la infraestructura actual.				x			60,00%
	Administración de Costos de TI. Existe un proceso de administración de costos, que compare los costos reales con los presupuestados.					X		80,00%

	Administración de Beneficios. Existe un proceso de monitoreo de beneficios, en base al cual se toman las medidas apropiadas.					x		80,00%
PO6	Comunicación con la Alta Dirección					x		76,00%
	Ambiente de Políticas y de Control. Existen elementos de control de inversiones, riesgos, integridad, responsabilidad, valores éticos, la competencia del personal y la rendición de cuentas.					X		80,00%
	Riesgo Corporativo y Marco de Referencia de Control Interno de TI. Existe un marco de trabajo que establezca el enfoque institucional hacia los riesgos y el control interno para entregar valor, mientras se protegen los recursos y sistemas de TI.				X			60,00%
	Administración de Políticas para TI. Existen políticas de apoyo a la estrategia de TI, que incluyan la intención de la alta dirección, los roles y responsabilidades, los estándares y directrices del enfoque de cumplimiento; que atiendan temas de calidad, seguridad, confidencialidad, y propiedad intelectual				x			60,00%
	Implantación de Políticas de TI. Las políticas de TI se implementan y se comunican a todo el personal relevante, resuelven necesidades e implicaciones de recursos y concientización.					X		80,00%
	Comunicación de los Objetivos y la Dirección de TI. Se comunica a toda la organización la conciencia sobre la seguridad de TI, la calidad, el código de ética, los objetivos de servicio, las políticas y procedimientos y una misión claramente definida.						X	100,00%
PO7	Recursos humanos de TI						x	87,50%
	Reclutamiento y Retención del Personal. Se asegura que el reclutamiento del personal de TI, esté de acuerdo con las políticas y procedimientos generales de la organización.						X	100,00%
	Competencias del Personal. Se verifica periódicamente que el personal tenga las competencias para cumplir sus funciones, y se definen los requisitos esenciales de certificación.					x		80,00%
	Asignación de Roles. Se definen, monitorean y supervisan las funciones, responsabilidades y los marcos de compensación para el personal, incluida la obligación de adherirse a las políticas y procedimientos de gestión, al código de ética y prácticas profesionales.					X		80,00%
	Entrenamiento del Personal de TI. Se proporciona a los funcionarios de TI la orientación necesaria y capacitación continua para desarrollar su conocimiento, aptitudes, y habilidades.					X		80,00%
	Dependencia Sobre los Individuos. Se minimiza la exposición a dependencias críticas sobre individuos clave por medio de documentación, planeación de la sucesión, y compartir el conocimiento.					X		80,00%
	Procedimientos de Investigación del Personal. Se incluye verificaciones de antecedentes en el proceso de reclutamiento de TI, cuyo grado y frecuencia de estas verificaciones dependen de la función.						X	100,00%
	Evaluación del Desempeño del Empleado. Se realizan evaluaciones periódicamente, comparando contra los objetivos individuales derivados de las metas institucionales y responsabilidades específicas de cada puesto, además los empleados reciben retroalimentación sobre su desempeño y conducta.						x	100,00%
	Cambios y Terminación del Contrato de Trabajo. Se toman medidas expeditas y se realiza la transferencia del conocimiento, reasignación de responsabilidades y eliminación de los privilegios de acceso.					x		80,00%
PO8	Calidad						X	83,33%
	Sistema de Administración de Calidad. Existe y se mantiene un sistema de administración de la calidad cubriendo roles, tareas y					x		80,00%

	responsabilidades.							
	Estándares y Prácticas de Calidad. Se utilizan las mejores prácticas existentes como una referencia para la mejora y adaptación de prácticas de calidad de la institución.					x		80,00%
	Estándares de desarrollo y de adquisición. Existen estándares para el desarrollo y adquisición, que consideran codificación de software, nomenclatura, formatos de archivos, estándares de interfaz, interoperabilidad, eficiencia de desempeño, escalabilidad, y estándares de pruebas.						X	100,00%
	Enfoque en el Usuario de TI. Se han definido los roles y responsabilidades respecto a la resolución de conflictos entre el usuario y la unidad de TI.					X		80,00%
	Mejora Continua. Se elabora y comunica un plan global de calidad que promueva la mejora continua de forma periódica.					x		80,00%
	Medición, Monitoreo y Revisión de la Calidad. La medición, el monitoreo y el registro de la información son utilizados por el dueño del proceso para tomar las medidas correctivas y preventivas apropiadas.					X		80,00%
PO9	Administración de riesgos de TI				X			60,00%
	Marco de Trabajo de Administración de Riesgos. La administración de riesgos está alineada con el nivel de tolerancia al riesgo de la institución.			X				40,00%
	Establecimiento del Contexto del Riesgo. Se determina el contexto interno y externo de cada evaluación de riesgos, la meta de evaluación y los criterios contra los cuales se evalúan.				x			60,00%
	Identificación de Eventos. Se identifican amenazas y vulnerabilidades con un impacto potencial sobre los objetivos institucionales y de TI.				X			60,00%
	Evaluación de Riesgos de TI. Se determina la posibilidad e impacto asociados a los riesgos inherentes y residuales, de forma individual, por categoría y con base al portafolio.				X			60,00%
	Respuesta a los Riesgos. Se elaboran y mantienen respuestas a los riesgos que garanticen el costo beneficio de los controles y las medidas de seguridad para mitigar el riesgo sobre una base continua.				X			60,00%
	Mantenimiento y Monitoreo de un Plan de Acción de Riesgos. Se asignan prioridades en base al costo beneficio, para implementar las respuestas a los riesgos identificadas como necesarias.					X		80,00%
PO10	Proyectos de TI						X	85,71%
	Marco de Trabajo para la Administración de Programas. Se mantiene el programa de proyectos relacionado con el portafolio de los programas de inversión de TI vigente.					X		80,00%
	Marco de Trabajo para la Administración de Proyectos. Existe un marco de trabajo que define las metodologías adoptadas y aplicadas a cada proyecto, incluyendo puntos de control y aprobaciones.						x	100,00%
	Enfoque de Administración de Proyectos. Se establece un enfoque de administración de proyectos acorde con el tamaño, la complejidad y los requisitos regulatorios de cada proyecto, asegurándose de que todos los proyectos cuenten con la suficiente autoridad para la ejecución propia dentro del programa estratégico global.					X		80,00%
	Compromiso de los Interesados. Existe el compromiso y la participación de los funcionarios implicados en la definición y ejecución de los proyectos dentro del contexto global de inversión en TI.					X		80,00%
	Declaración de Alcance del Proyecto. Se define y documenta el alcance de los proyectos para confirmar y desarrollar, un entendimiento común y la relación con otros proyectos.					X		80,00%

	Inicio de las Fases del Proyecto. Se asegura que el inicio de las etapas importantes de un proyecto se apruebe formalmente y se comunique a todos los funcionarios implicados.						x	100,00%
	Plan Integrado del Proyecto. Se establece formalmente un plan de proyecto integrado y aprobado para orientar la ejecución y el control del proyecto durante todo el ciclo de vida.						X	100,00%
	Recursos del Proyecto. Se define para los miembros del equipo del proyecto las responsabilidades, relaciones, autoridades y criterios de desempeño.					X		80,00%
	Administración de Riesgos del Proyecto. Se eliminan o minimizan los riesgos específicos asociados con proyectos individuales a través de un proceso sistemático de planificación.					X		80,00%
	Plan de Calidad del Proyecto. Se prepara un plan de gestión de calidad que describe el sistema de calidad del proyecto y cómo será implementado.					X		80,00%
	Control de Cambios del Proyecto. Se establece un sistema de control de cambios para cada proyecto, de modo que todos los cambios de la línea base del proyecto estén debidamente revisados, aprobados e incorporados en el plan integrado del proyecto.					X		80,00%
	Planeación del Proyecto y Métodos de Aseguramiento. Se identifican las tareas de aseguramiento requeridas para apoyar la acreditación de sistemas nuevos o modificados durante la planeación del proyecto.					X		80,00%
	Medición del Desempeño, Reporte y Monitoreo del Proyecto. Se mide el rendimiento del proyecto contra los requerimientos claves del proyecto (alcance, cronograma, costos, riesgos, calidad), se identifica cualquier desviación con respecto al plan.						X	100,00%
	Cierre del Proyecto. Al final de cada proyecto se determina si el proyecto dio los resultados y beneficios previstos.					X		80,00%
ADQUIRIR E IMPLEMENTAR								77,94%
AI1	Soluciones automatizadas					X		80,00%
	Definición y Mantenimiento de los Requerimientos Técnicos y Funcionales de la institución. Se identifican, priorizan, especifican y acuerdan los requerimientos funcionales y técnicos, que cubran el alcance completo de todas las iniciativas necesarias, para lograr los resultados esperados de los programas de inversión en TI.					X		80,00%
	Reporte de Análisis de Riesgos. Se identifica, documenta y analiza los riesgos incluyendo las amenazas a la integridad, seguridad, disponibilidad y privacidad de los datos y el cumplimiento de leyes y reglamentos.				X			60,00%
	Estudio de Factibilidad y Formulación de Cursos de Acción Alternativos. Se evalúa la factibilidad tecnológica y económica de cada uno de los cursos de acción identificados en el contexto de los programas de inversión en TI actuales.					X		80,00%
	Requerimientos, Decisión de Factibilidad y Aprobación. El directorio aprueba y autoriza los requerimientos institucionales y tiene la decisión final con respecto a la elección de la solución y al enfoque de adquisición.						X	100,00%
AI2	Software aplicativo					X		78,00%
	Diseño de Alto Nivel. Se traducen los requerimientos de la institución a una especificación de diseño de alto nivel para desarrollo de software, que tome en cuenta las directivas tecnológicas, la arquitectura de la información dentro de la organización y la aprobación de las especificaciones.						X	100,00%

	Diseño Detallado. Se prepara el diseño detallado y se aprueba los requerimientos para garantizar que corresponden al diseño de alto nivel.					X		80,00%
	Control y Posibilidad de Auditar las Aplicaciones. Se asegura que los controles incluyan mecanismos de integridad de la información, respaldo, mecanismos de acceso y diseño de pistas de auditorías.				X			60,00%
	Seguridad y Disponibilidad de las Aplicaciones. Se direcciona la seguridad de las aplicaciones y los requerimientos de disponibilidad en respuesta a los riesgos identificados, la clasificación de los datos y la arquitectura de la información.					X		80,00%
	Configuración e Implantación de Software Aplicativo Adquirido. Se personaliza e implementa la función automatizada, incluyendo la validación de los términos contractuales, la arquitectura de la información, la interoperabilidad con las aplicaciones existentes, las bases de datos, la eficiencia del desempeño, la documentación, os manuales de usuario, la integración y los planes de prueba.					x		80,00%
	Actualizaciones Importantes en Sistemas Existentes. Se sigue un proceso de desarrollo similar al de sistemas nuevos, considerando el análisis de impacto, la justificación costo beneficio, y la administración de requerimientos.					X		80,00%
	Desarrollo de Software Aplicativo. Se aprueba y autoriza cada etapa clave del proceso de desarrollo de software aplicativo, como son las especificaciones de diseño, las solicitudes de cambio, las garantías legales y contractuales; dando seguimiento a la terminación exitosa de revisiones de funcionalidad, desempeño y calidad.						X	100,00%
	Aseguramiento de la Calidad del Software. Se desarrolla y se ejecuta un plan de aseguramiento de la calidad que incluye los procesos de validación y verificación.					X		80,00%
	Administración de los Requerimientos de Aplicaciones. Durante el diseño, desarrollo e implementación se da seguimiento a los estados de los requerimientos particulares y a sus modificaciones.				X			60,00%
	Mantenimiento de Software Aplicativo. Se desarrolla una estrategia y un plan de mantenimiento que incluya la puesta en marcha, los recursos, la corrección de fallas, mejoras, mantenimiento de la documentación, cambios de emergencia, interdependencia con otras aplicaciones, estrategias de actualización, los riesgos y requerimientos de seguridad.				x			60,00%
AI3	Infraestructura tecnológica					X		75,00%
	Plan de Adquisición de Infraestructura Tecnológica. Existe un plan para adquirir, implementar y mantener la infraestructura tecnológica considerando los riesgos tecnológicos, y la vida útil de la inversión.					X		80,00%
	Protección y Disponibilidad del Recurso de Infraestructura. Se implementan medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura.				X			60,00%
	Mantenimiento de la Infraestructura. Existe una estrategia y un plan de mantenimiento de infraestructura, que incluye la revisión periódica de necesidades institucionales, actualizaciones (parches), riesgos, vulnerabilidades y seguridad.					X		80,00%
	Ambiente de Prueba de Factibilidad. Se establecen ambientes de desarrollo y prueba que consideran la funcionalidad, configuración de hardware y software, pruebas de integración, pruebas de desempeño, migración entre ambientes, control de versiones, y seguridad.					X		80,00%
AI4	Facilidad de operación y uso de TI					X		80,00%
	Plan para Soluciones de Operación. Se desarrolla un plan para identificar y documentar todos los aspectos técnicos, la capacidad de operación y los niveles de servicio de sistemas automatizados o de					X		80,00%

	infraestructura.							
	Transferencia de Conocimiento al Área Directiva. Se transfiere el conocimiento a la parte administrativa, de manera que les permita asumir la propiedad del sistema y los datos, así como la responsabilidad de ejercer la entrega y calidad del servicio, el control interno, y los procesos administrativos de la aplicación.					X		80,00%
	Transferencia de Conocimiento a Usuarios Finales. Se transfiere el conocimiento y las habilidades a los usuarios finales incluyendo materiales de capacitación, manuales de usuario, manuales de procedimientos, ayuda en línea, asistencia a usuarios y evaluación.					X		80,00%
	Transferencia de Conocimiento al Personal de Operaciones y Soporte. Se transfiere el conocimiento y las habilidades al personal de soporte técnico y de operaciones, de manera que les permita entregar, apoyar y mantener las aplicaciones, la infraestructura y los niveles de servicio requeridos.					X		80,00%
AI5	Recursos de TI						X	85,00%
	Control de Adquisición. Se desarrolla y sigue un conjunto de procedimientos y estándares consistentes con el proceso general de adquisiciones de la organización.						X	100,00%
	Administración de Contratos con Proveedores. Existe un procedimiento para establecer modificar y concluir contratos, que apliquen a todos los proveedores.					X		80,00%
	Selección de Proveedores. Se selecciona a los proveedores de acuerdo a una práctica justa y formal, para garantizar que se tome la opción más viable y favorable.					X		80,00%
	Adquisición de Recursos de TI. Se asegura la protección de los intereses de la institución, en todos los acuerdos contractuales de adquisición incluyendo, licencias, mantenimiento, garantías, procedimientos de arbitraje, condiciones para la actualización, seguridad, custodia y derechos de acceso.					X		80,00%
AI6	Administración de cambios en TI					X		72,00%
	Estándares y Procedimientos para Cambios. Existen procedimientos de administración de cambios formales, para manejar de manera estándar todas las solicitudes; incluyen cambios a aplicaciones, procedimientos, procesos, servicios, y plataformas.					X		80,00%
	Evaluación de Impacto, Priorización y Autorización. Se asegura que todas las solicitudes de cambio se evalúan de una manera estructurada, en cuanto a impactos en el sistema operacional y su funcionabilidad.				X			60,00%
	Cambios de Emergencia. Existe un proceso para definir, sensibilizar, evaluar y autorizar los cambios de emergencia que no sigan el proceso de cambio establecido.					X		80,00%
	Seguimiento y Reporte del Estatus de Cambio. Se establece un sistema de seguimiento y reporte para mantener actualizados a los solicitantes de cambio y a los interesados relevantes.					X		80,00%
	Cierre y Documentación del Cambio. Siempre que se implementan cambios al sistema, se actualiza la documentación, los sistemas asociados y los procedimientos correspondientes, además se establece un proceso de revisión para garantizar la implementación completa de los cambios.				x			60,00%
AI7	Soluciones y cambios en TI					X		75,56%
	Entrenamiento. Se capacita al personal de las unidades implicadas con el cambio y al grupo de operaciones de la función de TI.				x			60,00%
	Plan de Prueba. Se establece un plan de pruebas basado en los estándares de la institución, se define roles, responsabilidades y					X		80,00%

	criterios de éxito.							
	Plan de Implantación. Se establece un plan de implementación que define el diseño de versiones, construcción de paquetes, procedimientos de implementación / instalación, manejo de incidentes, controles de distribución, almacenamiento del software, documentación de cambios y medidas de respaldo y recuperación.				X			80,00%
	Ambiente de Prueba. Se tiene un ambiente separado para pruebas, que refleja el ambiente futuro de operaciones.						X	100,00%
	Conversión de Sistemas y Datos. Existe un plan establecido para que todos los elementos necesarios tales como hardware, software, datos de transacciones, archivos maestros, interfaces, procedimientos y documentación sean convertidos del viejo al nuevo sistema, manteniendo una auditoría de los resultados previos y posteriores a la conversión.				x			60,00%
	Pruebas de Cambios. Se garantiza que se prueban los cambios de acuerdo con el plan de aceptación definido y en base a una evaluación de impacto y recursos.				X			60,00%
	Prueba de Aceptación Final. Se garantiza que los procedimientos proporcionan formalmente una evaluación y aprobación de los resultados de prueba, por parte de las unidades implicadas y de TI.					X		80,00%
	Transferencia a Producción. Se tienen implementados los procedimientos formales para controlar la transferencia de los sistemas, desde el ambiente de desarrollo al de pruebas, de acuerdo con el plan de implementación.					X		80,00%
	Revisión Posterior a la Implantación. Se establecen procedimientos de revisión posterior a la implementación, para evaluar y reportar si el cambio satisface los requerimientos del usuario y entrega los beneficios esperados de la forma más rentable.					X		80,00%
ENTREGAR Y DAR SOPORTE								80,56%
DS1	Niveles de servicio					X		80,00%
	Marco de Trabajo de la Administración de los Niveles de Servicio. Se tiene definido un marco de trabajo que brinde un proceso formal de administración de niveles de servicio entre el usuario y el proveedor del servicio.						X	100,00%
	Definición de Servicios. Se tiene elaborado un catálogo o portafolio de servicios que, de manera organizada y centralizada, contiene las definiciones base de los servicios de TI, en cuanto a características del servicio y requerimientos de la institución.					X		80,00%
	Acuerdos de Niveles de Servicio.(SLA's) Se ha definido y acordado convenios de niveles de servicio para todos los procesos críticos de TI, con base en los requerimientos del usuario y las capacidades en TI. Los acuerdos incluyen compromisos, requerimientos, métricas, arreglos comerciales, roles y responsabilidades.					X		80,00%
	Acuerdos de Niveles de Operación (OLA's). Se asegura que los acuerdos de niveles de operación, expliquen cómo serán entregados técnicamente los servicios, para soportar el o los SLA's de matera óptima.					X		80,00%
	Monitoreo y Reporte del Cumplimento de los Niveles de Servicio. Se monitorean continuamente los criterios de desempeño especificados para cada nivel de servicio. Las estadísticas del monitoreo son analizadas para identificar tendencias positivas y negativas, tanto de servicios individuales como de los servicios en conjunto.					X		80,00%
	Revisión de los Acuerdos de Niveles de Servicio y de los Contratos. Se revisa regularmente con los proveedores internos y externos los acuerdos de niveles de servicio para asegurar que son efectivos, y están actualizados.				X			60,00%

DS2	Servicios de terceros					X		80,00%
	Identificación de Todas las Relaciones con Proveedores. Se identifican todos los servicios de los proveedores, y se categorizan de acuerdo con el tipo de proveedor, la importancia y la criticidad.					X		80,00%
	Gestión de Relaciones con Proveedores. Se formaliza el proceso de administración de relaciones con proveedores por cada proveedor, con base en la confianza y la transparencia.					X		80,00%
	Administración de Riesgos del Proveedor. Se identifica y mitiga los riesgos relacionados con la capacidad de los proveedores, y se asegura que los contratos estén de acuerdo con los estándares de la institución, para garantizar una efectiva entrega de servicios.						X	100,00%
	Monitoreo del Desempeño del Proveedor. Se establece el proceso de monitoreo de entrega de servicio para asegurar que el proveedor se apegue a los acuerdos contractuales y de nivel de servicio, y que el desempeño sea competitivo con las condiciones del mercado.				X			60,00%
DS3	Desempeño y la Capacidad de TI					X		72,00%
	Planeación del Desempeño y la Capacidad. Se establece un proceso de planeación para la revisión del desempeño y la capacidad de los recursos de TI.					X		80,00%
	Capacidad y Desempeño Actual. Se revisa la capacidad y desempeño actual de los recursos de TI en intervalo regulares, para determinar si se dispone de suficiente capacidad y desempeño, para prestar los servicios con base en los niveles de servicio acordados.					X		80,00%
	Capacidad y Desempeño Futuros. Se lleva a cabo un pronóstico de desempeño y capacidad de los recursos de TI en intervalos regulares, para minimizar el riesgo de interrupciones del servicio originadas por la falta de capacidad o degradación del desempeño.				X			60,00%
	Disponibilidad de Recursos de TI. Se proporciona la capacidad y desempeño requeridos, considerando las cargas de trabajo normales, las contingencias, requerimientos de almacenamiento y los ciclos de vida de los recursos de TI. Cuando el desempeño y la capacidad no están en el nivel requerido, se establecen prioridades, y mecanismos de tolerancia de fallas.					X		80,00%
	Monitoreo y Reporte. Se monitorea continuamente el desempeño y la capacidad de los recursos de TI; y la información recolectada se utiliza para realizar ajustes.				x			60,00%
DS4	Continuidad del servicio					x		78,00%
	Marco de Trabajo de Continuidad de TI. Existe un marco de continuidad de TI que apoye la continuidad de la institución, que incluye planes de contingencia, planes de recuperación de desastres y la estructura organizativa para la administración de la continuidad.					X		80,00%
	Planes de Continuidad de TI. Se desarrolla planes de continuidad de TI con base en el marco de continuidad, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave de la institución.					X		80,00%
	Recursos Críticos de TI. Se centra la atención en los puntos críticos de acuerdo al plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación.					X		80,00%
	Mantenimiento del Plan de Continuidad de TI. Se exhorta a la administración de TI a definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua las necesidades reales de la institución.				X			60,00%
	Pruebas del Plan de Continuidad de TI. Se prueba el plan de continuidad de TI de forma regular, garantizando que los sistemas pueden ser recuperados de forma efectiva, que las deficiencias son					x		80,00%

	atendidas y que el plan sigue siendo aplicable.							
	Entrenamiento del Plan de Continuidad de TI. Se asegura que todas las partes implicadas reciben periódicamente sesiones de formación sobre los procedimientos en caso de incidentes o desastre y sus responsabilidades.					x		80,00%
	Distribución del Plan de Continuidad de TI. Se dispone de una estrategia de distribución definida y administrada que asegure que los planes se distribuyen de manera apropiada y estén disponibles cuando se requiera.					x		80,00%
	Recuperación y Reanudación de los Servicios de TI. Se tiene un plan de acción, que TI debe tomar para reanudar y recuperar los servicios.					x		80,00%
	Almacenamiento de Respaldos Fuera de las Instalaciones. Los recursos críticos de TI, necesarios para la recuperación, se almacenan fuera de las instalaciones.						X	100,00%
	Revisión Post Reanudación. Existen procedimientos para valorar los resultados del plan de reanudación de las funciones de TI después de un desastre, y en consecuencia actualizarlo.					X		60,00%
DS5	Seguridad de los sistemas					X		76,00%
	Administración de la Seguridad de TI. Se administra la seguridad de TI al nivel más apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos de la institución.						X	80,00%
	Plan de Seguridad de TI. El plan de seguridad de TI contiene los requerimientos de información de la institución, la configuración de TI, planes de acción del riesgo de la información y la cultura sobre la seguridad de la información.					X		80,00%
	Administración de Cuentas del Usuario. Se identifican de manera única todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicaciones, sistemas operacionales, desarrollo y mantenimiento). Se garantiza que la solicitud, emisión, suspensión, modificación y cierre de cuentas y privilegios de acceso, sean dirigidas por un administrador.						X	100,00%
	Pruebas, Vigilancia y Monitoreo de la Seguridad. Se garantiza que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa.					X		80,00%
	Definición de Incidente de Seguridad. Se garantiza que las características de los posibles incidentes de seguridad, sean definidas y comunicadas de forma clara, de manera que los problemas de seguridad sean atendidos de forma apropiada, por medio del proceso de administración de problemas o incidentes.				X			60,00%
	Protección de la Tecnología de Seguridad. La protección de la tecnología garantiza, que la tecnología importante relacionada con la seguridad no sea susceptible de sabotaje.				X			60,00%
	Administración de Llaves Criptográficas. Se implementan políticas y procedimientos, que garantizan la protección de llaves criptográficas contra modificaciones y divulgación no autorizada.					X		80,00%
	Prevención, Detección y Corrección de Software Malicioso. Se garantiza que se cuente con medidas de prevención, detección y corrección (parches de seguridad, y antivirus) a lo largo de la institución, para proteger la tecnología y sistemas de información.					X		80,00%
	Seguridad de la Red. Se garantiza que se utilizan técnicas de seguridad y procedimientos de administración asociados (firewalls, dispositivos de seguridad, segmentación de redes y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.				X			60,00%

	Intercambio de Datos Sensitivos. Se garantiza que las transacciones de datos sensibles son intercambiadas solamente a través de un medio confiable, mediante pruebas de envío, pruebas de recepción, y autenticidad del contenido.					X		80,00%
DS6	Asignación de costos de TI						X	90,00%
	Definición de Servicios. Se identifican todos los costos de TI y se equiparan a los servicios de TI, para soportar un modelo de costos transparente.						X	100,00%
	Contabilización de TI. Se registran y se asignan los costos actuales de acuerdo con el modelo de costos definido, y se reportan las variaciones de los presupuestos.						X	100,00%
	Modelación de Costos y Cargos. Existe un modelo de costos de los servicios, que incluye costos directos, indirectos, y fijos; y garantiza que los cargos por servicios son identificables, medibles y predecibles para propiciar un adecuado uso de los recursos.					x		80,00%
	Mantenimiento del Modelo de Costos. Se revisa y compara de forma regular lo apropiado del modelo de costos/recargos para mantener su relevancia para la institución y las actividades de TI.					x		80,00%
DS7	Entrenamiento a los usuarios de TI						X	86,67%
	Identificación de Necesidades de Entrenamiento y Educación. Se establece y actualiza de forma regular un programa de capacitación para cada grupo objetivo de funcionarios.						X	100,00%
	Impartición de Entrenamiento y Educación. Se identifican los grupos objetivo de funcionarios, los mecanismos de entrega eficientes, y los instructores con base en las necesidades de capacitación.					X		80,00%
	Evaluación del Entrenamiento Recibido. Al finalizar la capacitación, se evalúa respecto a la relevancia, calidad, efectividad, percepción, retención del conocimiento y el costo.					x		80,00%
DS8	Mesa de servicios de TI					X		76,00%
	Mesa de Servicios. Existe una mesa de servicios como conexión de los funcionarios con TI que registra, comunica, atiende y analiza, todas las llamadas, los incidentes reportados, los requerimientos de servicio y las solicitudes de información. Además se mide la satisfacción del usuario en cuanto a la calidad de la mesa de servicios.						X	100,00%
	Registro de Consultas. Se dispone de un sistema que permite el registro de llamadas, incidentes, solicitudes de servicio y necesidades de información.				X			60,00%
	Escalamiento de Incidentes. Se disponen de procedimientos de mesa de servicios, de manera que los incidentes que no puedan resolverse de forma inmediata sean escalados apropiadamente, de acuerdo con los límites acordados en el SLA.				X			60,00%
	Cierre de Incidentes. Cuando se resuelve el incidente en la mesa de servicios, se registra la causa raíz y se confirma que la acción tomada fue acordada con el funcionario implicado.					X		80,00%
	Análisis de Tendencias. Se emiten reportes de la actividad de la mesa de servicios, que permite medir el desempeño y los tiempos de respuesta, así como identificar tendencias de problemas recurrentes de forma que el servicio pueda mejorarse de forma continua.					x		80,00%
DS9	Configuraciones de TI					X		80,00%
	Repositorio y Línea Base de Configuración. Se establece un repositorio central que contenga toda la información referente a los elementos de configuración de hardware, software, middleware, y las herramientas para operar, acceder y utilizar los sistemas y los servicios.					X		80,00%

	Identificación y Mantenimiento de Elementos de Configuración. Se cuenta con procedimientos para identificar elementos de configuración y sus atributos; registrar elementos de configuración nuevos, modificados y eliminados; y prevenir la inclusión de software no autorizado.					X		80,00%
	Revisión de Integridad de la Configuración. Se revisa y verifica de manera regular el estado de los elementos de configuración y la existencia de cualquier software personal o no autorizado.					X		80,00%
DS10	Administración de Problemas con TI					x		70,00%
	Identificación y Clasificación de Problemas. Existen procesos para reportar y clasificar problemas que han sido identificados como parte de la administración de incidentes, incluyendo categoría, impacto, urgencia y prioridad.					X		80,00%
	Rastreo y Resolución de Problemas. El sistema de administración de problemas mantiene pistas de auditoría adecuadas, que permitan rastrear, analizar y determinar la causa raíz de todos los problemas reportados, e identificar soluciones sostenibles por medio del proceso de administración de cambios establecido. El avance de la resolución de un problema es monitoreado contra los niveles de servicio (SLA's).					X		80,00%
	Cierre de Problemas. Se dispone de un procedimiento para cerrar registros de problemas, ya sea después de confirmar la eliminación exitosa del error conocido o después de acordar con la institución cómo manejar el problema de manera alternativa.				X			60,00%
	Integración de las Administraciones de Cambios, Configuración y Problemas. Se garantiza una adecuada administración de problemas e incidentes, así como la integración de los procesos relacionados de administración de cambios, configuración y problemas.				x			60,00%
DS11	Administración de los datos						X	86,67%
	Requerimientos de la institución para Administración de Datos. Se tienen mecanismos para garantizar que se reciben documentos originales, que se procesa toda la información recibida por parte de la institución, que se preparan y entregan todos los reportes que requiere la institución y que las necesidades están soportadas.						X	100,00%
	Acuerdos de Almacenamiento y Conservación. Se dispone de procedimientos para el archivo y almacenamiento de los datos, de manera que los datos permanezcan accesibles y utilizables, considerando requerimientos de recuperación, rentabilidad, integridad, seguridad y cumplimientos legales.					x		80,00%
	Sistema de Administración de Librerías de Medios. Se definen e implementan procedimientos para mantener un inventario de medios y garantizar su integridad y uso.					X		80,00%
	Eliminación. Se definen e implementan procedimientos para prevenir el acceso a datos sensitivos y al software, desde equipos o medios, una vez que son eliminados o transferidos para otro uso.						X	100,00%
	Respaldo y Restauración. Se definen e implementa procedimientos de respaldo y restauración de sistemas, datos y configuraciones alineados con el plan de continuidad.					X		80,00%
	Requerimientos de Seguridad para la Administración de Datos. Se establecen mecanismos para identificar y aplicar requerimientos de seguridad a la recepción, procesamiento, almacenamiento y entrega de la información.					x		80,00%
DS12	Ambiente físico						X	92,00%
	Selección y Diseño del Centro de Datos. Se define y selecciona los centros de datos físicos para el equipo de TI, considerando los riesgos asociados con desastres, las leyes y regulaciones de seguridad y salud ocupacional.					x		80,00%

	Medidas de Seguridad Física. Se definen e implementan medidas de seguridad física, que incluyen las zonas de seguridad, la ubicación de equipo crítico, las áreas de envío y recepción y los procedimientos de monitoreo.						X	100,00%
	Acceso Físico. Se definen e implementan procedimientos para otorgar, limitar y revocar el acceso a edificios y áreas de acuerdo a las necesidades de la institución incluyendo las emergencias.						x	100,00%
	Protección Contra Factores Ambientales. Se ha diseñado e implementado medidas de protección contra factores ambientales, y se han instalado dispositivos especializados para monitorear y controlar el ambiente.					X		80,00%
	Administración de Instalaciones Físicas. La administración de las instalaciones, incluyendo los equipos de suministro de energía y comunicación están alineados con las leyes y regulaciones, requerimientos técnicos y de la institución, especificaciones del proveedor y los lineamientos de seguridad y salud.						X	100,00%
DS13	Operaciones de TI					X		80,00%
	Procedimientos e Instrucciones de Operación. Se han definido, e implementado procedimientos estándar para las operaciones de TI.					x		80,00%
	Programación de Tareas. Se organiza la programación de los trabajos, procesos y tareas dentro de una secuencia eficiente, maximizando el rendimiento y utilización, para alcanzar los requerimientos de la institución.					X		80,00%
	Monitoreo de la Infraestructura de TI. Se han definido e implementado procedimientos para monitorear la infraestructura de TI y eventos relacionados, se almacena información cronológica en los registros de operaciones, que permiten reconstruir, revisar y analizar la secuencia de las operaciones.					X		80,00%
	Documentos Sensitivos y Dispositivos de Salida. Se han establecido resguardos físicos, prácticas de registro y administración de inventarios adecuados sobre los activos de TI más sensitivos.					x		80,00%
	Mantenimiento Preventivo del Hardware. Existen procedimientos para asegurar el mantenimiento oportuno de la infraestructura, de manera que se reduce la frecuencia e impacto de las fallas y la degradación del desempeño.					X		80,00%
MONITOREAR Y EVALUAR								76,69%
ME1	Monitoreo del desempeño de TI						X	83,33%
	Enfoque del Monitoreo. Existe un marco de trabajo de monitoreo general de TI y un enfoque que define el alcance, la metodología y el proceso a seguir, para medir los resultados de los procesos para la entrega de servicios de TI.						X	100,00%
	Definición y Recolección de Datos de Monitoreo. Se garantiza que la dirección de TI, trabaja en conjunto con la institución y define un conjunto balanceado de objetivos, mediciones, metas, comparaciones de desempeño y satisfacción de los usuarios.					X		80,00%
	Método de Monitoreo. Se garantiza que el proceso de monitoreo implante un método (ej., BalancedScorecard) que brinde una visión sucinta y desde todos los ángulos del desempeño de TI y que se adapte al sistema de monitoreo institucional.					X		80,00%
	Evaluación del Desempeño. Se compara de forma periódica el desempeño contra las metas y se inician acciones correctivas para subsanar las causas subyacentes.				X			60,00%
	Reportes al Consejo Directivo. Se proporcionan reportes administrativos para ser revisados por la alta dirección, sobre el avance de la institución hacia metas identificadas, específicamente en términos del desempeño del portafolio de programas de inversión						X	100,00%

	habilitados por TI, niveles de servicio de programas individuales y la contribución de TI a ese desempeño.							
	Acciones Correctivas. Se identifican e inician acciones correctivas basadas en el monitoreo del desempeño,					X		80,00%
ME2	Evaluación del control interno					x		65,71%
	Monitoreo del Marco de Trabajo de Control Interno. Se monitorea de forma continua el ambiente de control y el marco de control de TI, haciendo uso de las mejores prácticas y benchmarking.(comparar con modelos institucionales líderes a nivel mundial)				X			60,00%
	Revisiones de Auditoría. Se monitorea y reporta la efectividad de los controles internos sobre TI, por medio de revisiones de auditoría, incluyendo el cumplimiento de políticas y estándares, seguridad de la información, controles de cambios y controles establecidos en acuerdos de niveles de servicio.					X		80,00%
	Excepciones de Control. Se registra la información referente a todas las excepciones de control, se asegura que se lleve a cabo tanto el análisis de la causa subyacente como la acción correctiva.				x			60,00%
	Auto Evaluación del Control. Se evalúa la completitud y efectividad de los controles internos administrativos sobre los procesos, las políticas y contratos de TI, por medio de un programa continuo de auto evaluación.			x				40,00%
	Aseguramiento del Control Interno. Se obtiene un mayor aseguramiento de la completitud y efectividad de los controles internos por medio de revisiones por terceros. (auditores, consultores externos u organismos de certificación)				x			60,00%
	Control Interno para Terceros. Se confirma que los proveedores externos de servicios cumplan con los requerimientos legales y regulatorios,y con las obligaciones contractuales.					X		80,00%
	Acciones Correctivas. Se identifican e inician medidas correctivas basadas en las evaluaciones y en los reportes de control.					X		80,00%
ME3	Cumplimiento regulatorio					X		72,00%
	Identificar los Requerimientos de las Leyes, Regulaciones y Cumplimientos Contractuales. Está definido o implementado un proceso para garantizar la identificación oportuna de requerimientos legales locales, internacionales, contractuales, de políticas y regulatorios, relacionados con la información, prestación de servicios, procesos e infraestructura.					X		80,00%
	Optimizar la Respuesta a Requerimientos Externos. Se garantiza que los requisitos legales y regulatorios cubran de forma eficiente las políticas, estándares y procedimientos de TI.					X		80,00%
	Evaluación del Cumplimiento con Requerimientos Externos. Se evalúa el cumplimiento de las políticas, estándares y procedimientos de TI, con base en la supervisión de la dirección de TI y la operación de los controles internos.				X			60,00%
	Aseguramiento Positivo del Cumplimiento. Se definen e implementan procedimientos, para obtener un reporte del aseguramiento del cumplimiento y, donde sea necesario, que el propietario del proceso tome las acciones correctivas oportunas para resolver cualquier brecha de cumplimiento.				X			60,00%
	Reportes Integrados. Se integran los reportes de TI sobre el cumplimiento regulatorio, con las salidas similares provenientes de otras funciones de la institución.					X		80,00%
ME4	Gobierno de TI					X		85,71%
	Establecimiento de un Marco de Gobierno de TI. Se trabaja con el consejo directivo para definir y establecer un marco de trabajo para el						X	100,00%

	gobierno de TI, que incluye el liderazgo, los procesos, roles, responsabilidades, requerimientos de información, y estructuras organizacionales para garantizar que los programas de inversión habilitados por TI, estén alineados con los objetivos institucionales.							
	Alineamiento Estratégico. El comité estratégico de TI, facilita la alineación de TI con la institución, en lo referente a estrategia y operaciones, fomentando la co-responsabilidad entre la institución y TI en forma de decisiones estratégicas y en la obtención de los beneficios provenientes de las inversiones habilitadas con TI.						X	100,00%
	Entrega de Valor. Se administra los programas de inversión habilitados con TI, así como otros activos y servicios de TI, para asegurar que ofrezcan el mayor valor posible, para apoyar la estrategia y los objetivos institucionales.						X	100,00%
	Administración de Recursos. Se optimiza la inversión, uso y asignación de los activos de TI por medio de evaluaciones periódicas, garantizando que TI cuente con recursos suficientes, competentes y capaces para ejecutar los objetivos estratégicos actuales y futuros, y seguir el ritmo de los requerimientos institucionales.					X		80,00%
	Administración de Riesgos. Se integra las responsabilidades de administración de riesgos en la organización, asegurando que tanto la institución como TI evalúen y reporten periódicamente los riesgos asociados con TI y su impacto institucional.				X			60,00%
	Medición del Desempeño. Se informa el desempeño relevante del portafolio de los programas de TI, al consejo directivo y a los ejecutivos de manera oportuna y precisa, hacia metas identificadas.					X		80,00%
	Aseguramiento Independiente. Se asegura que la institución mantiene una función competente y con el personal adecuado; y/o busque servicios de aseguramiento externos, para proveer oportunamente a la junta directiva un aseguramiento independiente acerca del cumplimiento de TI con sus políticas, estándares y procedimientos, así como con las prácticas generalmente aceptadas.					x		80,00%

Tabla A3.9*Matriz de Cumplimiento de Objetivos de Control – COBIT.*(COBIT 4.1, 2007)

MATRIZ DE IMPACTO DE PROCESOS FRENTE A LOS CRITERIOS DE INFORMACIÓN DE COBIT

PROCESOS DE TI - COBIT		CRITERIOS DE INFORMACIÓN DE COBIT							RECURSOS DE TI				IMPACTO
		EFECTIVIDAD	EFICIENCIA	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CUMPLIMIENTO	CONFIABILIDAD	PERSONAS	INFORMACION	APLICACION	INFRAESTRUCTURA	%
PLANEAR Y ORGANIZAR (PO)													**77,44%**
PO1	Definición del plan estratégico de TI	0,86	0,63				0,32		X	X	X	X	75,00%
PO2	Definición de la arquitectura de la información	0,63	0,86	0,63	0,86					X	X		75,00%
PO3	Determinación de la dirección tecnológica.	0,86	0,86					0,32			X	X	86,00%
PO4	Definición de los procesos, organización y relaciones de TI.	0,86	0,86						X				86,00%
PO5	Administración de la inversión en TI.	0,86	0,86		0,32			0,63	X		X	X	86,00%
PO6	Comunicación con la Alta Dirección	0,86					0,63		X	X			43,00%
PO7	Administración de los recursos humanos de TI.	0,86	0,86						X				86,00%
PO8	Administración de la calidad de TI	0,86	0,86		0,63			0,63	X	X	X	X	86,00%
PO9	Evaluación y administración de los riesgos de TI.	0,63	0,63	0,86	0,86	0,86	0,63	0,63	X	X	X	X	63,00%
PO10	Administración de los proyectos de TI	0,86	0,86						X		X	X	86,00%
ADQUIRIR E IMPLEMENTAR (AI)													**79,71%**
AI1	Identificación de las soluciones automatizadas.	0,86	0,63				0,32				X	X	75,00%
AI2	Adquisición y mantenimiento del software aplicativo.	0,86	0,86		0,63			0,63			X		86,00%
AI3	Adquisición y mantenimiento de la infraestructura tecnológica.	0,63	0,86		0,63	0,63						X	75,00%
AI4	Facilitad de operación y uso de TI	0,86	0,86		0,63	0,63	0,63	0,63	X		X	X	86,00%
AI5	Adquisición de recursos de TI.	0,63	0,86				0,63		X	X	X	X	75,00%
AI6	Administración de cambios en TI	0,86	0,86		0,86	0,86		0,63	X	X	X	X	86,00%
AI7	Instalación y acreditación de soluciones y cambios en TI	0,86	0,63		0,63	0,63			X	X	X	X	75,00%
ENTREGAR Y DAR SOPORTE (DS)													**66,46%**
DS1	Definición y administración de los niveles de servicio.	0,86	0,86	0,63	0,63	0,63	0,63	0,63	X	X	X	X	86,00%

DS2	Administración de los servicios de terceros.		0,86	0,86	0,63	0,63	0,63	0,63	0,63		X	X	X	X		86,00%
DS3	Administración del desempeño y capacidad de TI		0,86	0,86			0,63						X	X		86,00%
DS4	Garantías en la continuidad del servicio		0,86	0,63			0,86				X	X	X	X		75,00%
DS5	Garantías en la seguridad de los sistemas.			0,32	0,86	0,86	0,63	0,63	0,63		X	X	X	X		16,00%
DS6	Identificación y asignación de costos de TI.			0,86					0,86		X	X	X	X		43,00%
DS7	Educación y entrenamiento a los usuarios.		0,86	0,63			0,32				X					75,00%
DS8	Administración de la mesa de servicios de TI y los incidentes.		0,86	0,86			0,32				X		X			86,00%
DS9	Administración de la configuración de TI.		0,86	0,63			0,63		0,63			X	X	X		75,00%
DS10	Administración de los problemas con TI.		0,86	0,86			0,63				X	X	X	X		86,00%
DS11	Administración de los datos.		0,32	0,32		0,86			0,86			X				32,00%
DS12	Administración del ambiente físico.		0,32	0,32		0,86	0,86							X		32,00%
DS13	Administración de las operaciones de TI.		0,86	0,86		0,63	0,63				X	X	X	X		86,00%
MONITOREAR Y EVALUAR (ME)																**86,00%**
ME1	Monitoreo y evaluación del desempeño de TI.		0,86	0,86	0,63	0,63	0,63	0,63	0,63		X	X	X	X		86,00%
ME2	Monitoreo y evaluación el control interno.		0,86	0,86	0,63	0,63	0,63	0,63	0,63		X	X	X	X		86,00%
ME3	Garantías en el cumplimiento regulatorio.		0,86	0,86				0,86	0,63		X	X	X	X		86,00%
ME4	Proporciona gobierno de TI.		0,86	0,86	0,63	0,63	0,63	0,63	0,63		X	X	X	X		86,00%

Tabla A3.10*Matriz de Impacto de Procesos frente a los Criterios de Información de COBIT.*(COBIT 4.1, 2007)

MATRIZ DE DIAGNOSTICO DE PROCESOS COBIT

PROCESOS DE TI – COBIT		IMPORTANCIA				FORMALIZADO / NORMADO				CONTROL INTERNO			AUDITADO		
		POCO IMPORTANTE	IMPORTANTE	MUY IMPORTANTE	%	NO FORMALIZADO	FORMALIZADO	NO APLICA	NO SE SABE CON CERTEZA	NO DOCUMENTADO	DOCUMENTADO	NO SE SABE CON CERTEZA	NO AUDITADO	AUDITADO	NO SE SABE CON CERTEZA
PLANEAR Y ORGANIZAR					**70,10%**										
PO1	Definición del plan estratégico de TI			X	100,00 %	x				X			x		
PO2	Definición de la arquitectura de la información			X	100,00 %	x				X			x		
PO3	Determinación de la dirección tecnológica.			X	100,00 %		x				X		x		
PO4	Definición de los procesos, organización y relaciones de TI.		X		67,00%		x				X		x		
PO5	Administración de la inversión en TI.	X			33,00%	x				X			x		
PO6	Comunicación con la Alta Dirección		X		67,00%		x				X		x		
PO7	Administración de los recursos humanos de TI.		X		67,00%		x				x		x		
PO8	Administración de la calidad de TI	X			33,00%	x				x			X		
PO9	Evaluación y administración de los riesgos de TI.		X		67,00%		x				X		X		
PO10	Administración de los proyectos de TI		X		67,00%	x					X		X		
ADQUIRIR E IMPLEMENTAR					**76,29%**										
AI1	Identificación de las soluciones automatizadas.			X	100,00%	x				X			X		
AI2	Adquisición y mantenimiento del software aplicativo.			X	100,00%		x				X		X		
AI3	Adquisición y mantenimiento de la infraestructura tecnológica.		X		67,00%		x				X		X		
AI4	Facilitad de operación y uso de TI	X			33,00%		x				X		X		
AI5	Adquisición de recursos de TI.			X	100,00%		x				X			x	
AI6	Administración de cambios en TI		X		67,00%		x				X		X		
AI7	Instalación y acreditación de soluciones y cambios en TI		X		67,00%	x				X			x		
ENTREGAR Y DAR SOPORTE					**53,85%**										
DS1	Definición y administración de los niveles de servicio.		X		67,00%		x				x		X		
DS2	Administración de los servicios de terceros.	X			33,00%		x				x		X		
DS3	Administración del desempeño y capacidad de TI	X			33,00%	x				x			X		

DS4	Garantías en la continuidad del servicio			X	100,00 %		x				x		X		
DS5	Garantías en la seguridad de los sistemas.		X		67,00%	x					x		X		
DS6	Identificación y asignación de costos de TI.		X		67,00%		x				x		X		
DS7	Educación y entrenamiento a los usuarios.	X			33,00%	x				x			X		
DS8	Administración de la mesa de servicios de TI y los incidentes.	X			33,00%		x				x		X		
DS9	Administración de la configuración de TI.		X		67,00%		x			x			X		
DS10	Administración de los problemas con TI.	X			33,00%		x			x			X		
DS11	Administración de los datos.		X		67,00%	x					x		X		
DS12	Administración del ambiente físico.	x			33,00%		x				x		X		
DS13	Administración de las operaciones de TI.		X		67,00%	x				x			X		
MONITOREAR Y EVALUAR					**66,75%**										
ME1	Monitoreo y evaluación del desempeño de TI.		X		67,00%	x					x		X		
ME2	Monitoreo y evaluación el control interno.	X			33,00%	x				x			X		
ME3	Garantías en el cumplimiento regulatorio.		X		67,00%		x				x		X		
ME4	Proporciona gobierno de TI.			x	100,00 %	x				x			X		

Tabla A3.11*Matriz de Diagnóstico de Procesos COBIT.*

ANEXO 4: INDICADORES DE RESULTADOS DE LA AUDITORIA INFORMATICA A LA SUPERTEL

PO1 Definir un Plan Estratégico de TI			ESTADO DEL PROCESO		IMPACTO
			C = 73,86%	$\alpha = 55024$ $\beta = 56,03$ $\gamma = 53,18$	Alto
OBJETIVO	Sostener los requerimientos de la estrategia institucional, al mismo tiempo que se mantiene la transparencia sobre los beneficios, costos y riesgos				
SITUACION ACTUAL					
Objetivos de Control	Administración del Valor de TI				80,00%
	Alineación de TI con la Institución				80,00%
	Evaluación del Desempeño y la Capacidad Actual				60,00%
	Plan Estratégico de TI				80,00%
	Planes Tácticos de TI				80,00%
	Administración del Portafolio de TI				80,00%
Indicador de Madurez	$m = 73,33\%$	Grado de Madurez Real de la Institución			$m_{ri} = 66,67\%$
	NIVEL 4				
Indicador de Desempeño	$d = 71,48\%$	Grado de Desempeño Real			$d_r = 62,96\%$
	MUY BUENO	Grado de Desempeño COBIT			$d_c = 80,00\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 76,67\%$				
	CUMPLE CASI TOTALMENTE				
Impacto	$I = 87,50\%$	Grado de Impacto			$I_c = 75,00\%$
	ALTO	Grado de Importancia			$I_s = 100,00\%$
Formalizado / Normado	NO	**Control Interno**	No Documentado	**Responsable**	Unidad de TI
TENDENCIAS	La incorporación de TI y de la dirección, en la traducción de los requerimientos a ofertas de servicio, y el desarrollo de estrategias para entregar estos servicios de una forma transparente y eficiente.				
FORTALEZAS	Las estrategias de la institución y de TI están integradas y son comunicadas de manera amplia.				
PUNTOS DEBILES Y AMENAZAS	No se realiza una evaluación adecuada del desempeño de los planes existentes y de los sistemas existentes en términos de su contribución con la institución.				
RECOMENDACIONES Y PLANES DE ACCIÓN	Fomentar el compromiso con la dirección, para alinear la planeación estratégica de TI con las necesidades institucionales actuales y futuras. Aplicar un esquema de prioridades para los objetivos institucionales que cuantifique los requerimientos.				

PO2 Definir la arquitectura de información			ESTADO DEL PROCESO		IMPACTO
			C = 70,44%	$\alpha = 51,73$ $\beta = 60,76$ $\gamma = 52,07$	Alto
OBJETIVO	Agilizar la respuesta a los requerimientos, proporcionar información confiable y consistente, para integrar de forma transparente las aplicaciones dentro de los procesos institucionales.				
SITUACION ACTUAL					
Objetivos de Control	Modelo de Arquitectura de Información Empresarial				80,00%
	Diccionario de Datos Empresarial y Reglas de Sintaxis de Datos				80,00%
	Esquema de Clasificación de Datos				80,00%
	Administración de Integridad				60,00%
Indicador de Madurez	$m = 75,56\%$	Grado de Madurez Real de la Institución			$m_{ri} = 77.78\%$
	NIVEL 4				
Indicador de Desempeño	$d = 59,59\%$	Grado de Desempeño Real			$d_r = 39,17\%$
	SATISFACTORIO	Grado de Desempeño COBIT			$d_c = 80,00\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 75,00\%$				
	CUMPLE CASI TOTALMENTE				

Impacto	$I = 87{,}50\%$	Grado de Impacto			$I_c = 75{,}00\%$
	ALTO	Grado de Importancia			$I_s = 100{,}00\%$
Formalizado / Normado	NO	**Control Interno**	No Documentado	**Responsable**	Unidad de TI
TENDENCIAS	El establecimiento de un modelo de datos que incluya un esquema de clasificación de información que garantice la integridad y consistencia de todos los datos.				
FORTALEZAS	El modelo de arquitectura de la información facilita el desarrollo de aplicaciones, y actividades de soporte a la toma de decisiones.				
PUNTOS DEBILES Y CAPITULO 5 INFORME DE AUDITORÍA..... **AMENAZAS**	Los procedimientos para garantizar la integridad y consistencia de todos los datos presentan ciertas vulnerabilidades.				
RECOMENDACIONES Y PLANES DE ACCIÓN	Asegurar la exactitud de la arquitectura de la información y del modelo de datos. Clasificar la información usando un esquema de clasificación.				

PO3	**Determinar la dirección tecnológica**	**ESTADO DEL PROCESO**		**IMPACTO**
		C = 72,22%	$\alpha = 52{,}59$ $\beta = 59{,}23$ $\gamma = 59{,}59$	Alto
OBJETIVO	Contar con sistemas aplicativos estándares, bien integrados, rentables y estables, así como recursos y capacidades que satisfagan requerimientos institucionales, actuales y futuros.			

SITUACION ACTUAL			
Objetivos de Control	Planeación de la Dirección Tecnológica		80,00%
	Plan de Infraestructura Tecnológica		100,00%
	Monitoreo de Tendencias y Regulaciones Futuras		60,00%
	Estándares Tecnológicos		80,00%
	Consejo de Arquitectura de TI		60,00%
Indicador de Madurez	$m = 76.00\%$ NIVEL 4	Grado de Madurez Real de la Institución	$m_{ri} = 80.00\%$
Indicador de Desempeño	$d = 64{,}00\%$	Grado de Desempeño Real	$d_r = 48{,}00\%$
	MUY BUENO	Grado de Desempeño COBIT	$d_c = 80{,}00\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 76{,}00\%$ CUMPLE CASI TOTALMENTE		
Impacto	$I = 93{,}00\%$	Grado de Impacto	$I_c = 86{,}00\%$
	ALTO	Grado de Importancia	$I_s = 100{,}00\%$

Formalizado / Normado	Si	**Control Interno**	Documentado	**Responsable**	Unidad de TI
TENDENCIAS	La definición e implementación de un plan de infraestructura tecnológica, una arquitectura y estándares que tomen en cuenta y aprovechen las oportunidades tecnológicas.				
FORTALEZAS	Se planea cual dirección tecnológica es apropiada tomar para materializar la estrategia de TI, considerando la migración de datos y aspectos de contingencia.				
PUNTOS DEBILES Y AMENAZAS	No existen procesos bien definidos para monitorear las tendencias del sector, las tecnologías, la infraestructura y los aspectos legales y regulatorios.				
RECOMENDACIONES Y PLANES DE ACCIÓN	Establecer un foro para dirigir la arquitectura y verificar el cumplimiento. Definir estándares de infraestructura tecnológica basados en requerimientos de arquitectura de información.				

PO4	**Definir los procesos, organización y relaciones de TI**	**ESTADO DEL PROCESO**		**IMPACTO**
		C = 66,34%	$\alpha = 59{,}97$ $\beta = 55{,}10$ $\gamma = 49{,}47$	Alto
OBJETIVO	Agilizar la respuesta a las estrategias institucionales mientras se establecen puntos de contacto definidos y competentes.			

SITUACION ACTUAL		
Objetivos de Control	Marco de Trabajo de Procesos de TI	80,00%
	Comité Estratégico de TI	80,00%
	Comité Directivo de TI	80,00%
	Ubicación Organizacional de la Función de TI	100,00%
	Estructura Organizacional	80,00%
	Establecimiento de Roles y Responsabilidades	60,00%
	Responsabilidad de Aseguramiento de Calidad de TI	80,00%

	Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento		60,00%
	Propiedad de Datos y de Sistemas		80,00%
	Supervisión		80,00%
	Segregación de Funciones		80,00%
	Personal de TI		60,00%
	Personal Clave de TI		60,00%
	Políticas y Procedimientos para Personal Contratado		80,00%
	Relaciones		60,00%
Indicador de Madurez	$m = 57{,}50\%$	Grado de Madurez Real de la Institución	$m_{rl} = 87{,}50\%$
	NIVEL 3		
Indicador de Desempeño	$d = 65{,}74\%$	Grado de Desempeño Real	$d_r = 44{,}81\%$
	MUY BUENO	Grado de Desempeño COBIT	$d_c = 86{,}67\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 74{,}67\%$		
	CUMPLE CASI TOTALMENTE		
Impacto	$I = 76{,}50\%$	Grado de Impacto	$I_c = 86{,}00\%$
	ALTO	Grado de Importancia	$I_s = 67{,}00\%$

Formalizado / Normado	Si	**Control Interno**	Documentado	**Responsable**	Unidad de TI

TENDENCIAS	El establecimiento de estructuras organizacionales de TI transparentes, flexibles y responsables.
FORTALEZAS	Se ubica a la función de TI dentro de la estructura institucional, supeditada a la importancia dentro de la organización.
PUNTOS DEBILES Y AMENAZAS	La descripción de roles, puede resultar obsoleta y no estar alineada con las habilidades, experiencias y evaluación del desempeño. El proceso de dotación de personal no toma en cuenta la capacitación funcional cruzada, y la rotación de puestos.
RECOMENDACIONES Y PLANES DE ACCIÓN	Definir un marco de trabajo de procesos de TI, con roles y responsabilidades. Establecer una estructura organizacional apropiada.

PO5	**Administrar la inversión en TI**	**ESTADO DEL PROCESO**		**IMPACTO**
		$C = 70{,}25\%$	$\alpha = 63{,}13$ $\beta = 50{,}44$ $\gamma = 51{,}35$	Medio

OBJETIVO	Mejorar de forma continua y demostrable la rentabilidad de TI y su contribución a la institución con servicios integrados y estandarizados que satisfagan las expectativas del usuario.

SITUACION ACTUAL

Objetivos de Control	Marco de Trabajo para la Administración Financiera		80,00%
	Prioridades Dentro del Presupuesto de TI		80,00%
	Proceso Presupuestal		60,00%
	Administración de Costos de TI		80,00%
	Administración de Beneficios		80,00%
Indicador de Madurez	$m = 55{,}00\%$	Grado de Madurez Real de la Institución	$m_{rl} = 83{,}33\%$
	NIVEL 3		
Indicador de Desempeño	$d = 77{,}50\%$	Grado de Desempeño Real	$d_r = 75{,}00\%$
	MUY BUENO	Grado de Desempeño COBIT	$d_c = 80{,}00\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 76{,}00\%$		
	CUMPLE CASI TOTALMENTE		
Impacto	$I = 59{,}50\%$	Grado de Impacto	$I_c = 86{,}00\%$
	MEDIO	Grado de Importancia	$I_s = 33{,}00\%$

Formalizado / Normado	NO	**Control Interno**	No Documentado	**Responsable**	Unidad de TI

TENDENCIAS	Decisiones de portafolio e inversión en TI efectivas y eficientes, y el establecimiento y seguimiento de presupuestos de TI de acuerdo a la estrategia de TI y a las decisiones de inversión.
FORTALEZAS	Se prioriza la asignación de recursos de TI para las operaciones, proyectos y mantenimiento, que maximice la contribución de TI a optimizar el retorno del portafolio institucional de programas de inversión en TI.

PUNTOS DEBILES Y AMENAZAS	En los procesos de administración de presupuesto, pueden ser relegados costos recurrentes de operación y mantenimiento de la infraestructura actual.					
RECOMENDACIONES Y PLANES DE ACCIÓN	Definir criterios formales de inversión.					
PO6	**Comunicar las aspiraciones y la dirección de la gerencia**		**ESTADO DEL PROCESO**		**IMPACTO**	
			$C = 66{,}60$	$\alpha = 64{,}31$ $\beta = 52{,}06$ $\gamma = 48{,}79$	Medio	
OBJETIVO	Una información precisa y oportuna sobre los servicios de TI actuales y futuros, los riesgos asociados y las responsabilidades.					
SITUACION ACTUAL						
Objetivos de Control	Ambiente de Políticas y de Control				80,00%	
	Riesgo Corporativo y Marco de Referencia de Control Interno de TI				60,00%	
	Administración de Políticas para TI				60,00%	
	Implantación de Políticas de TI				80,00%	
	Comunicación de los Objetivos y la Dirección de TI				100,00%	
Indicador de Madurez	$m = 50{,}00\%$ NIVEL 3	Grado de Madurez Nivel 3			$m_{ri} = 50{,}00\%$	
Indicador de Desempeño	$d = 70{,}93\%$	Grado de Desempeño Real			$d_r = 75{,}19\%$	
	MUY BUENO	Grado de Desempeño COBIT			$d_c = 66{,}67\%$	
Indicador de Cumplimiento de Objetivos de Control	$o = 76{,}00\%$					
	CUMPLE CASI TOTALMENTE					
Impacto	$I = 55{,}00\%$	Grado de Impacto			$I_c = 43{,}00\%$	
	MEDIO	Grado de Importancia			$I_s = 67{,}00\%$	
Formalizado / Normado	Si	**Control Interno**	Documentado	**Responsable**	Unidad de TI	
TENDENCIAS	Proporcionar políticas, procedimientos, directrices y otra documentación aprobada, de forma precisa y entendible y que se encuentre dentro del marco de trabajo de control de TI a los interesados.					
FORTALEZAS	Se comunica a toda la institución la conciencia sobre la seguridad de TI, la calidad, las políticas y procedimientos.					
PUNTOS DEBILES Y AMENAZAS	No se ha determinado un enfoque institucional concreto hacia los riesgos y el control interno para entregar valor, mientras se protegen los recursos y sistemas de TI.					
RECOMENDACIONES Y PLANES DE ACCIÓN	Definir un marco de trabajo de control y políticas para TI.					
PO7	**Administrar los recursos humanos de TI**		**ESTADO DEL PROCESO**		**IMPACTO**	
			$C = 71{,}63\%$	$\alpha = 65{,}22$ $\beta = 55{,}13$ $\gamma = 45{,}15$	Alto	
OBJETIVO	Adquirir gente competente y motivada para crear y entregar servicios de TI.					
SITUACION ACTUAL						
Objetivos de Control	Reclutamiento y Retención del Personal				100,00%	
	Competencias del Personal				80,00%	
	Asignación de Roles				80,00%	
	Entrenamiento del Personal de TI				80,00%	
	Dependencia Sobre los Individuos				80,00%	
	Procedimientos de Investigación del Personal				100,00%	
	Evaluación del Desempeño del Empleado				100,00%	
	Cambios y Terminación de Trabajo				80,00%	
Indicador de Madurez	$m = 52{,}00\%$ NIVEL 3	Grado de Madurez Real de la Institución			$m_{ri} = 60{,}00\%$	
Indicador de Desempeño	$d = 70{,}93$	Grado de Desempeño Real			$d_r = 75{,}19\%$	
	MUY BUENO	Grado de Desempeño COBIT			$d_c = 66{,}67\%$	
Indicador de Cumplimiento de Objetivos de Control	$o = 87{,}50\%$					

	CUMPLE TOTALMENTE					
Impacto	$I = 76{,}50$	Grado de Impacto	$I_c = 86{,}00\%$			
	ALTO	Grado de Importancia	$I_s = 67{,}00\%$			
Formalizado / Normado	Si	**Control Interno**	Documentado	**Responsable**	Unidad de TI	
TENDENCIAS	La contratación y entrenamiento del personal, la motivación por medio de planes de carrera claros.					
FORTALEZAS	Se asegura que el reclutamiento del personal de TI, esté de acuerdo con las políticas y procedimientos generales de la institución.					
PUNTOS DEBILES Y AMENAZAS	Hay exposición a dependencias críticas sobre individuos clave.					
RECOMENDACIONES Y PLANES DE ACCIÓN	Entrenar al personal de TI para apoyar los planes tácticos de TI. Mitigar el riesgo de sobre-dependencia de recursos clave.					

		ESTADO DEL PROCESO		**IMPACTO**
PO8	**Administrar la calidad**	C = 68,00%	$\alpha = 63{,}80$ $\beta = 56{,}51$ $\gamma = 44{,}97$	Medio
OBJETIVO	La mejora continua y medible de la calidad de los servicios prestados por TI.			

SITUACION ACTUAL			
Objetivos de Control	Sistema de Administración de Calidad		80,00%
	Estándares y Prácticas de Calidad		100,00%
	Estándares de desarrollo y adquisición		80,00%
	Enfoque en el Cliente de TI		80,00%
	Mejora Continua		80,00%
	Medición, Monitoreo y Revisión de la Calidad		80,00%
Indicador de Madurez	$m = 52{,}00\%$ NIVEL 3	Grado de Madurez Real de la Institución	$m_{rl} = 60{,}00\%$
Indicador de Desempeño	$d = 65{,}00\%$	Grado de Desempeño Real	$d_r = 60{,}00\%$
	MUY BUENO	Grado de Desempeño COBIT	$d_c = 70{,}00\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 83{,}33\%$		
	CUMPLE TOTALMENTE		
Impacto	$I = 59{,}50$	Grado de Impacto	$I_c = 86{,}00\%$
	MEDIO	Grado de Importancia	$I_s = 33{,}00\%$

Formalizado / Normado	NO	**Control Interno**	No Documentado	**Responsable**	Unidad de TI
TENDENCIAS	La definición de un sistema de administración de calidad, el monitoreo continuo del desempeño contra los objetivos predefinidos, y la implantación de un programa de mejora continua de servicios de TI.				
FORTALEZAS	Se utilizan las mejores prácticas existentes como una referencia para la mejora y adaptación de prácticas de calidad de la institución.				
PUNTOS DEBILES Y AMENAZAS	La medición, el monitoreo y el registro de la información no son utilizados por el dueño del proceso para tomar las medidas correctivas y preventivas apropiadas.				
RECOMENDACIONES Y PLANES DE ACCIÓN	Definir estándares y prácticas de calidad y su mejora continua. Realizar monitoreo y revisión interna y externa del desempeño contra los estándares y prácticas de calidad definidas.				

		ESTADO DEL PROCESO		**IMPACTO**
PO9	**Evaluar y administrar los riesgos de TI**	C = 51,80%	$\alpha = 68{,}19$ $\beta = 49{,}91$ $\gamma = 48{,}03$	Medio
OBJETIVO	Analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y metas institucionales.			

SITUACION ACTUAL			
Objetivos de Control	Marco de Trabajo de Administración de Riesgos		40,00%
	Establecimiento del Contexto del Riesgo		60,00%
	Identificación de Eventos		60,00%
	Evaluación de Riesgos de TI		60,00%
	Respuesta a los Riesgos		60,00%
	Mantenimiento y Monitoreo de un Plan de Acción de Riesgos		80,00%
Indicador de Madurez	$m = 33{,}33\%$	Grado de Madurez Real de la Institución	$m_{rl} = 66{,}67\%$

	NIVEL 2		
Indicador de Desempeño	$d = 57{,}78\%$	Grado de Desempeño Real	$d_r = 48{,}89\%$
	SATISFACTORIO	Grado de Desempeño COBIT	$d_c = 66{,}67\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 60{,}00\%$		
	CUMPLE PARCIALMENTE		
Impacto	$I = 65{,}00\%$	Grado de Impacto	$I_c = 63{,}00\%$
	MEDIO	Grado de Importancia	$I_s = 67{,}00\%$

Formalizado / Normado	Si	**Control Interno**	Documentado	**Responsable**	Unidad de TI

TENDENCIAS	La elaboración de un marco de trabajo de administración de riesgos, evaluación de riesgos, mitigación del riesgo y comunicación de riesgos residuales.
FORTALEZAS	Se asignan prioridades en base al costo beneficio, para implementar las respuestas a los riesgos identificadas como necesarias.
PUNTOS DEBILES Y AMENAZAS	La administración de riesgos no está completamente alineada con el nivel de tolerancia al riesgo de la institución.
RECOMENDACIONES Y PLANES DE ACCIÓN	Garantizar que la administración de riesgos está incluida completamente en los procesos administrativos, tanto interna como externamente, y se aplica de forma consistente. Realizar evaluaciones de riesgo y comunicar planes de acción para remediar riesgos.

		ESTADO DEL PROCESO		**IMPACTO**
PO10	**Administrar los proyectos**	$C = 76{,}85\%$	$\alpha = 55{,}41$ $\beta = 59{,}14$ $\gamma = 49{,}92$	Alto

OBJETIVO	La entrega de resultados de proyectos dentro de marcos de tiempo, presupuesto y calidad acordados.

SITUACION ACTUAL

Objetivos de Control	Marco de Trabajo para la Administración de Programas		80,00%
	Marco de Trabajo para la Administración de Proyectos		100,00%
	Enfoque de Administración de Proyectos		80,00%
	Compromiso de los Interesados		80,00%
	Declaración de Alcance del Proyecto		80,00%
	Inicio de las Fases del Proyecto		100,00%
	Plan Integrado del Proyecto		100,00%
	Recursos del Proyecto		80,00%
	Administración de Riesgos del Proyecto		80,00%
	Plan de Calidad del Proyecto		80,00%
	Control de Cambios del Proyecto		80,00%
	Planeación del Proyecto y Métodos de Aseguramiento		80,00%
	Medición del Desempeño, Reporte y Monitoreo del Proyecto		100,00%
	Cierre del Proyecto		80,00%
Indicador de Madurez	$m = 75{,}56\%$	Grado de Madurez Real de la Institución	$m_{rl} = 77{,}78\%$
	NIVEL 4		
Indicador de Desempeño	$d = 68{,}29\%$	Grado de Desempeño Real	$d_r = 56{,}57\%$
	MUY BUENO	Grado de Desempeño COBIT	$d_c = 80{,}007\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 85{,}71\%$		
	CUMPLE TOTALMENTE		
Impacto	$I = 76{,}50\%$	Grado de Impacto	$I_c = 86{,}00\%$
	ALTO	Grado de Importancia	$I_s = 67{,}00\%$

Formalizado / Normado	NO	**Control Interno**	No Documentado	**Responsable**	Unidad de TI

TENDENCIAS	Un programa y un enfoque de administración de proyectos definidos, el cual se aplica a todos los proyectos de TI, lo cual facilita la participación de los interesados y el monitoreo de los riesgos y los avances de los proyectos.
FORTALEZAS	Se establece formalmente un plan de proyecto integrado y aprobado para orientar la ejecución y el control del proyecto durante todo el ciclo de vida.

PUNTOS DEBILES Y AMENAZAS	En varios proyectos no se detalla un plan de gestión de calidad que describa el sistema de calidad del proyecto y cómo será implementado.				
RECOMENDACIONES Y PLANES DE ACCIÓN	Emitir directrices de administración para proyectos. Definir la planeación de proyectos para todos los proyectos incluidos en el portafolio de proyectos.				
AI1	**Identificar las soluciones automatizadas**		**ESTADO DEL PROCESO**		**IMPACTO**
			$C = 71{,}81\%$	$\alpha = 49{,}97$ $\beta = 65{,}46$ $\gamma = 49{,}97$	Alto
OBJETIVO	Traducir los requerimientos funcionales y de control a un diseño efectivo y eficiente de soluciones automatizadas.				
SITUACION ACTUAL					
Objetivos de Control	Definición y Mantenimiento de los Requerimientos Técnicos y Funcionales del Negocio				80,00%
	Reporte de Análisis de Riesgos				60,00%
	Estudio de Factibilidad y Formulación de Cursos de Acción Alternativos				80,00%
	Requerimientos, Decisión de Factibilidad y Aprobación				100,00%
Indicador de Madurez	$m = 80{,}00\%$ NIVEL 4	Grado de Madurez Real de la Institución			$m_{rl} = 100{,}00\%$
Indicador de Desempeño	$d = 51{,}67\%$	Grado de Desempeño Real			$d_r = 48{,}33\%$
	SATISFACTORIO	Grado de Desempeño COBIT			$d_c = 60{,}00\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 80{,}00\%$				
	CUMPLE CASI TOTALMENTE				
Impacto	$I = 87{,}50\%$	Grado de Impacto			$I_c = 75{,}00\%$
	ALTO	Grado de Importancia			$I_s = 100{,}00\%$
Formalizado / Normado	NO	**Control Interno**	No Documentado	**Responsable**	Unidad de TI
TENDENCIAS	La identificación de soluciones técnicamente factibles y rentables.				
FORTALEZAS	El directorio aprueba y autoriza los requerimientos institucionales y tiene la decisión final con respecto a la elección de la solución y al enfoque de adquisición.				
PUNTOS DEBILES Y AMENAZAS	No se documenta adecuadamentelos riesgos incluyendo las amenazas a la integridad, seguridad, disponibilidad y privacidad de los datos.				
RECOMENDACIONES Y PLANES DE ACCIÓN	Realizar estudios de factibilidad autorizados por el dueño del proceso Monitorear la satisfacción de los usuarios con la funcionalidad entregada				
AI2	**Adquirir y mantener software aplicativo**		**ESTADO DEL PROCESO**		**IMPACTO**
			$C = 65{,}50\%$	$\alpha = 60{,}42\%$ $\beta = 57{,}82\%$ $\gamma = 46{,}56\%$	Alto
OBJETIVO	Construir las aplicaciones de acuerdo con los requerimientos institucionales y haciéndolas a tiempo y a un costo razonable.				
SITUACION ACTUAL					
Objetivos de Control	Diseño de Alto Nivel				100,00%
	Diseño Detallado				80,00%
	Control y Posibilidad de Auditar las Aplicaciones				60,00%
	Seguridad y Disponibilidad de las Aplicaciones				80,00%
	Configuración e Implantación de Software Aplicativo Adquirido				80,00%
	Actualizaciones Importantes en Sistemas Existentes				80,00%
	Desarrollo de Software Aplicativo				100,00%
	Aseguramiento de la Calidad del Software				80,00%
	Administración de los Requerimientos de Aplicaciones				60,00%
	Mantenimiento de Software Aplicativo				60,00%
Indicador de Madurez	$m = 56{,}00\%$ NIVEL 3	Grado de Madurez Real de la Institución			$m_{rl} = 80{,}00\%$
Indicador de Desempeño	$d = 60{,}42\%$	Grado de Desempeño Real			$d_r = 50{,}83\%$
	SATISFACTORIO	Grado de Desempeño COBIT			$d_c = 70{,}00\%$

Indicador de Cumplimiento de Objetivos de Control	$o = 78{,}00\%$				
	CUMPLE CASI TOTALMENTE				
Impacto	$I = 93{,}00\%$	Grado de Impacto		$I_c = 86{,}00\%$	
	ALTO	Grado de Importancia		$I_s = 100{,}00\%$	
Formalizado / Normado	Si	**Control Interno**	Documentado	**Responsable**	Unidad de TI
TENDENCIAS	Garantizar que exista un proceso de desarrollo oportuno y confiable.				
FORTALEZAS	Se aprueba y autoriza cada etapa clave del proceso de desarrollo de software aplicativo, como son las especificaciones de diseño, las solicitudes de cambio, las garantías legales y contractuales; dando seguimiento a la terminación exitosa de revisiones de funcionalidad, desempeño y calidad.				
PUNTOS DEBILES Y AMENAZAS	No se asegura que los controles incluyan mecanismos de integridad de la información, y respaldo.				
RECOMENDACIONES Y PLANES DE ACCIÓN	Emplear los estándares de desarrollo para todas las modificaciones. Separar las actividades de desarrollo, de pruebas y operativas.				
AI3	**Adquirir y mantener la infraestructura tecnológica**		**ESTADO DEL PROCESO**		**IMPACTO**
			C = 84,44%	$\alpha = 46{,}86$ $\beta = 58{,}73$ $\gamma = 59{,}15$	Alto
OBJETIVO	Adquirir y dar mantenimiento a una infraestructura integrada y estándar de TI.				
SITUACION ACTUAL					
Objetivos de Control	Plan de Adquisición de Infraestructura Tecnológica				80,00%
	Protección y Disponibilidad del Recurso de Infraestructura				60,00%
	Mantenimiento de la Infraestructura				80,00%
	Ambiente de Prueba de Factibilidad				80,00%
Indicador de Madurez	$m = 100\%$	Grado de Madurez Real de la Institución		$m_{rl} = 100\%$	
	NIVEL 5				
Indicador de Desempeño	$d = 75{,}93\%$	Grado de Desempeño Real		$d_r = 61{,}85\%$	
	MUY BUENO	Grado de Desempeño COBIT		$d_c = 90{,}00\%$	
Indicador de Cumplimiento de Objetivos de Control	$o = 75{,}00\%$				
	CUMPLE CASI TOTALMENTE				
Impacto	$I = 71{,}00\%$	Grado de Impacto		$I_c = 75{,}00\%$	
	ALTO	Grado de Importancia		$I_s = 67{,}00\%$	
Formalizado / Normado	Si	**Control Interno**	Documentado	**Responsable**	Unidad de TI
TENDENCIAS	Proporcionar plataformas adecuadas para las aplicaciones de acuerdo con la arquitectura definida de TI y los estándares de tecnología				
FORTALEZAS	Se establecen ambientes de desarrollo y prueba que consideran la funcionalidad, configuración de hardware y software, pruebas de integración, pruebas de desempeño, migración entre ambientes, control de versiones, y seguridad.				
PUNTOS DEBILES Y AMENAZAS	No se toman medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura.				
RECOMENDACIONES Y PLANES DE ACCIÓN	Establecer un plan de adquisición de tecnología que se alinea con el plan de infraestructura tecnológica. Implantar medidas de control interno, seguridad y auditabilidad.				
AI4	**Facilitar la operación y el uso**		**ESTADO DEL PROCESO**		**IMPACTO**
			C = 65,18%	$\alpha = 63{,}71$ $\beta = 52{,}98$ $\gamma = 48{,}37$	Medio
OBJETIVO	Garantizar la satisfacción de los usuarios finales mediante ofrecimientos de servicios y niveles de servicio, y de forma transparente integrar las soluciones de aplicación y tecnología dentro de los procesos institucionales.				
SITUACION ACTUAL					
Objetivos de Control	Plan para Soluciones de Operación				80,00%
	Transferencia de Conocimiento a la Gerencia del Negocio				80,00%
	Transferencia de Conocimiento a Usuarios Finales				80,00%
	Transferencia de Conocimiento al Personal de Operaciones y Soporte				80,00%
Indicador de Madurez	$m = 50{,}00\%$	Grado de Madurez Real de la Institución		$m_{rl} = 50{,}00\%$	
	NIVEL 3				
Indicador de Desempeño	$d = 67{,}97\%$	Grado de Desempeño Real		$d_r = 69{,}26\%$	

	MUY BUENO	Grado de Desempeño COBIT	$d_c = 66{,}67\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 80{,}00\%$		
	CUMPLE CASI TOTALMENTE		
Impacto	$I = 59{,}60\%$	Grado de Impacto	$I_c = 86{,}00\%$
	MEDIO	Grado de Importancia	$I_s = 33{,}00\%$

Formalizado / Normado	Si	**Control Interno**	Documentado	**Responsable**	Unidad de TI

TENDENCIAS	Proporcionar manuales efectivos de usuario y de operación y materiales de entrenamiento para transferir el conocimiento necesario para la operación y el uso exitosos del sistema.
FORTALEZAS	Se transfiere el conocimiento y las habilidades a los usuarios finales incluyendo materiales de capacitación, manuales de usuario, manuales de procedimientos, ayuda en línea, asistencia a usuarios y evaluación
PUNTOS DEBILES Y AMENAZAS	En algunas ocasiones no se transfiere el conocimiento y las habilidades al personal de soporte técnico y de operaciones, dificultando las labores de apoyo y mantenimiento.
RECOMENDACIONES Y PLANES DE ACCIÓN	Desarrollar documentación para transferir el conocimiento. Entrenar a usuarios, al personal de apoyo y al personal de operación.

AI5 Adquirir recursos de TI	**ESTADO DEL PROCESO**		**IMPACTO**
	C = 71,81%	$\alpha = 61{,}16$	Alto
		$\beta = 56{,}77$	
		$\gamma = 46{,}89$	

OBJETIVO	Mejorar la rentabilidad de TI.

SITUACION ACTUAL

Objetivos de Control	Control de Adquisición		100,00%
	Administración de Contratos con Proveedores		80,00%
	Selección de Proveedores		80,00%
	Adquisición de Recursos de TI		80,00%
Indicador de Madurez	$m = 60{,}00\%$	Grado de Madurez Real de la Institución	$m_{rl} = 100{,}00\%$
	NIVEL 3		
Indicador de Desempeño	$d = 68{,}15\%$	Grado de Desempeño Real	$d_r = 69{,}63\%$
	MUY BUENO	Grado de Desempeño COBIT	$d_c = 66{,}67\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 85{,}00\%$		
	CUMPLE TOTALMENTE		
Impacto	$I = 87{,}50\%$	Grado de Impacto	$I_c = 75{,}00\%$
	ALTO	Grado de Importancia	$I_s = 100{,}00\%$

Formalizado / Normado	Si	**Control Interno**	Documentado	**Responsable**	Unidad de TI

TENDENCIAS	Adquirir y mantener las habilidades de TI que respondan a la estrategia de entrega, en una infraestructura TI integrada y estandarizada, y reducir el riesgo de adquisición de TI.
FORTALEZAS	Se selecciona a los proveedores de acuerdo a una práctica justa y formal, para garantizar que se tome la opción más viable y favorable.
PUNTOS DEBILES Y AMENAZAS	Pueden surgir ocasiones en las cuales no se protejan adecuadamente los intereses de la institución, en todos los acuerdos contractuales de adquisición.
RECOMENDACIONES Y PLANES DE ACCIÓN	Obtener asesoría profesional legal y contractual. Definir procedimientos y estándares de adquisición.

AI6 Administrar cambios	**ESTADO DEL PROCESO**			**IMPACTO**
	C = 67,38%	$\alpha = 52{,}46$		Alto
		$\beta = 60{,}12$		
		$\gamma = 51{,}91$		

OBJETIVO	Responder a los requerimientos institucionales, mientras se reducen los defectos y la repetición de trabajos en la prestación del servicio y en la solución.

SITUACION ACTUAL

Objetivos de Control	Estándares y Procedimientos para Cambios	80,00%
	Evaluación de Impacto, Priorización y Autorización	60,00%
	Cambios de Emergencia	80,00%
	Seguimiento y Reporte del Estatus de Cambio	80,00%
	Cierre y Documentación del Cambio	60,00%

Indicador de Madurez	$m = 71{,}11\%$	Grado de Madurez Real de la Institución	$m_{rl} = 55{,}56\%$
	NIVEL 4		
Indicador de Desempeño	$d = 58{,}15\%$	Grado de Desempeño Real	$d_r = 42{,}96\%$
	SATISFACTORIO	Grado de Desempeño COBIT	$d_c = 73{,}33\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 72{,}00\%$		
	CUMPLE CASI TOTALMENTE		
Impacto	$I = 76{,}50\%$	Grado de Impacto	$I_c = 86{,}00\%$
	ALTO	Grado de Importancia	$I_s = 67{,}00\%$

Formalizado / Normado	Si	**Control Interno**	Documentado	**Responsable**	Unidad de TI

TENDENCIAS	Controlar la evaluación de impacto, autorización e implantación de todos los cambios a la infraestructura de TI, aplicaciones y soluciones técnicas, minimizando errores que se deben a especificaciones incompletas de la solicitud y detener la implantación de cambios no autorizados.
FORTALEZAS	Existen procedimientos de administración de cambios formales, para manejar de manera estándar todas las solicitudes.
PUNTOS DEBILES Y AMENAZAS	No se pone especial atención al impacto que puede ocasionar un cambio en el sistema operacional y su funcionabilidad.
RECOMENDACIONES Y PLANES DE ACCIÓN	Definir y comunicar procedimientos de cambio. Dar seguimiento del estatus y reporte de los cambios.

AI7	**Instalar y acreditar soluciones y cambios**	**ESTADO DEL PROCESO**		**IMPACTO**
		$C = 72{,}19\%$	$\alpha = 54{,}56$ $\beta = 56{,}87$ $\gamma = 52{,}82$	Alto

OBJETIVO	Contar con sistemas nuevos o modificados que trabajen sin problemas importantes después de la instalación.

SITUACION ACTUAL

Objetivos de Control	Entrenamiento	60,00%
	Plan de Prueba	80,00%
	Plan de Implantación	80,00%
	Ambiente de Prueba	100,00%
	Conversión de Sistemas y Datos	60,00%
	Pruebas de Cambios	60,00%
	Prueba de Aceptación Final.	80,00%
	Promoción a Producción	80,00%
	Revisión Posterior a la Implantación	80,00%

Indicador de Madurez	$m = 72{,}50\%$	Grado de Madurez Real de la Institución	$m_{rl} = 62{,}50\%$
	NIVEL 4		
Indicador de Desempeño	$d = 68{,}33\%$	Grado de Desempeño Real	$d_r = 63{,}33\%$
	MUY BUENO	Grado de Desempeño COBIT	$d_c = 73{,}33\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 75{,}56\%$		
	CUMPLE CASI TOTALMENTE		
Impacto	$I = 71{,}00\%$	Grado de Impacto	$I_c = 75{,}00\%$
	ALTO	Grado de Importancia	$I_s = 67{,}00\%$

Formalizado / Normado	NO	**Control Interno**	No Documentado	**Responsable**	Unidad de TI

TENDENCIAS	Probar que las soluciones de aplicaciones e infraestructura son apropiadas para el propósito deseado y estén libres de errores, y planear las liberaciones a producción.
FORTALEZAS	Se tiene un ambiente separado para pruebas, que refleja el ambiente futuro de operaciones.
PUNTOS DEBILES Y AMENAZAS	No estaestablecido un plan adecuado para que todos los elementos necesarios tales como hardware, software, datos de transacciones, archivos maestros, interfaces, procedimientos y documentación sean convertidos del viejo al nuevo sistema, manteniendo una auditoría de los resultados previos y posteriores a la conversión.
RECOMENDACIONES Y PLANES DE ACCIÓN	Establecer una metodología de prueba. Evaluar y aprobar los resultados de las pruebas por parte de la dirección. Ejecutar revisiones posteriores a la implantación.

DS1	**Definir y administrar los niveles de servicio**	**ESTADO DEL PROCESO**		**IMPACTO**
		$C = 66{,}88\%$	$\alpha = 64{,}43\%$	Alto

			$\beta = 54{,}53\%$ $\gamma = 46{,}32\%$	
OBJETIVO	Asegurar la alineación de los servicios claves de TI con la estrategia institucional.			
SITUACION ACTUAL				
Objetivos de Control	Marco de Trabajo de la Administración de los Niveles de Servicio			100,00%
	Definición de Servicios			80,00%
	Acuerdos de Niveles de Servicio			80,00%
	Acuerdos de Niveles de Operación			80,00%
	Monitoreo y Reporte del Cumplimento de los Niveles de Servicio			80,00%
	Revisión de los Acuerdos de Niveles de Servicio y de los Contratos			60,00%
Indicador de Madurez	$m = 50{,}00\%$ NIVEL 3	Grado de Madurez Real de la Institución		$m_{rl} = 50{,}00\%$
Indicador de Desempeño	$d = 67{,}23\%$	Grado de Desempeño Real		$d_r = 67{,}78\%$
	MUY BUENO	Grado de Desempeño COBIT		$d_c = 66{,}67\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 80{,}00\%$ CUMPLE CASI TOTALMENTE			
Impacto	$I = 76{,}50\%$	Grado de Impacto		$I_c = 86{,}00\%$
	ALTO	Grado de Importancia		$I_s = 67{,}00\%$
Formalizado / Normado	Si	**Control Interno**	Documentado	**Responsable** Unidad de TI
TENDENCIAS	La identificación de requerimientos de servicio, el acuerdo de niveles de servicio y el monitoreo del cumplimiento de los niveles de servicio.			
FORTALEZAS	Se tiene definido un marco de trabajo que brinde un proceso formal de administración de niveles de servicio entre el usuario y el proveedor del servicio.			
PUNTOS DEBILES Y AMENAZAS	Se revisa esporádicamente con los proveedores internos y externos los acuerdos de niveles de servicio por lo que no se asegura que son efectivos, y están actualizados.			
RECOMENDACIONES Y PLANES DE ACCIÓN	Formalizar acuerdos internos y externos en línea con los requerimientos y las capacidades de entrega. Notificar el cumplimiento de los niveles de servicio. Comunicar los requerimientos de servicios actualizados y nuevos para planeación estratégica.			
DS2	**Administrar los servicios de terceros**		**ESTADO DEL PROCESO**	**IMPACTO**
			C = 68,51%	$\alpha = 59{,}63$ $\beta = 57{,}43$ $\gamma = 47{,}61$ Medio
OBJETIVO	Brindar servicios satisfactorios de terceros con transparencia acerca de los beneficios, riesgos y costos.			
SITUACION ACTUAL				
Objetivos de Control	Identificación de Todas las Relaciones con Proveedores			80,00%
	Gestión de Relaciones con Proveedores			80,00%
	Administración de Riesgos del Proveedor			100,00%
	Monitoreo del Desempeño del Proveedor			60,00%
Indicador de Madurez	$m = 60{,}00\%$ NIVEL 3	Grado de Madurez Real de la Institución		$m_{rl} = 100{,}00\%$
Indicador de Desempeño	$d = 63{,}89\%$	Grado de Desempeño Real		$d_r = 61{,}11\%$
	MUY BUENO	Grado de Desempeño COBIT		$d_c = 66{,}67\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 80{,}00\%$ CUMPLE CASI TOTALMENTE			
Impacto	$I = 59{,}50\%$	Grado de Impacto		$I_c = 86{,}00\%$
	MEDIO	Grado de Importancia		$I_s = 33{,}00\%$
Formalizado / Normado	Si	**Control Interno**	Documentado	**Responsable** Unidad de TI
TENDENCIAS	El establecimiento de relaciones y responsabilidades bilaterales con proveedores calificados de servicios tercerizados y el monitoreo de la prestación del servicio para verificar y asegurar la adherencia a los convenios.			
FORTALEZAS	Se identifica y mitiga los riesgos relacionados con la capacidad de los proveedores, y se asegura que los contratos estén de acuerdo con los estándares de la institución, para garantizar una efectiva entrega de servicios.			

PUNTOS DEBILES Y AMENAZAS	Muchas veces no seestablece el proceso de monitoreo de entrega de servicio.				
RECOMENDACIONES Y PLANES DE ACCIÓN	Categorizar los servicios del proveedor. Mitigar los riesgos del proveedor. Monitorear y medir el desempeño del proveedor.				
DS3	**Continuidad del Servicio**		**ESTADO DEL PROCESO**		**IMPACTO**
			$\mathbb{C} = 71{,}69\%$	$\alpha = 53{,}25$ $\beta = 56{,}43$ $\gamma = 54{,}56$	Medio
OBJETIVO	Optimizar el desempeño de la infraestructura, los recursos y las capacidades de TI en respuesta a las necesidades institucionales.				
SITUACION ACTUAL					
Objetivos de Control	Planeación del Desempeño y la Capacidad				80,00%
	Capacidad y Desempeño Actual				80,00%
	Capacidad y Desempeño Futuros				60,00%
	Disponibilidad de Recursos de TI				80,00%
	Monitoreo y Reporte				60,00%
Indicador de Madurez	$m = 74{,}29\%$ NIVEL 4	Grado de Madurez Real de la Institución			$m_{rl} = 71{,}43\%$
Indicador de Desempeño	$d = 68{,}67\%$	Grado de Desempeño Real			$d_r = 67{,}33\%$
	MUY BUENO	Grado de Desempeño COBIT			$d_c = 70{,}00\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 72{,}00\%$ CUMPLE CASI TOTALMENTE				
Impacto	$I = 59{,}50\%$	Grado de Impacto			$I_c = 86{,}00\%$
	MEDIO	Grado de Importancia			$I_s = 33{,}00\%$
Formalizado / Normado	NO	**Control Interno**	No Documentado	**Responsable**	Unidad de TI
TENDENCIAS	Cumplir con los requerimientos de tiempo de respuesta de los acuerdos de niveles de servicio, minimizando el tiempo sin servicio y haciendo mejoras continuas de desempeño y capacidad de TI a través del monitoreo y la medición.				
FORTALEZAS	Se proporciona la capacidad y desempeño requeridos, considerando las cargas de trabajo normales, las contingencias, requerimientos de almacenamiento y los ciclos de vida de los recursos de TI.				
PUNTOS DEBILES Y AMENAZAS	No se lleva a cabo un pronóstico de desempeño y capacidad de los recursos de TI en intervalos regulares, para minimizar el riesgo de interrupciones del servicio originadas por la falta de capacidad o degradación del desempeño.				
RECOMENDACIONES Y PLANES DE ACCIÓN	Planear y entregar capacidad y disponibilidad del sistema. Monitorear y reportar el desempeño del sistema. Modelar el desempeño del sistema.				
DS4	**Garantizar la continuidad del servicio**		**ESTADO DEL PROCESO**		**IMPACTO**
			$\mathbb{C} = 75{,}33\%$	$\alpha = 54{,}91$ $\beta = 56{,}03$ $\gamma = 53{,}29$	Alto
OBJETIVO	Asegurar el mínimo impacto al negocio en caso de una interrupción de servicios de TI.				
SITUACION ACTUAL					
Objetivos de Control	Marco de Trabajo de Continuidad de TI				80,00%
	Planes de Continuidad de TI				80,00%
	Recursos Críticos de TI				80,00%
	Mantenimiento del Plan de Continuidad de TI				60,00%
	Pruebas del Plan de Continuidad de TI				80,00%
	Entrenamiento del Plan de Continuidad de TI				80,00%
	Distribución del Plan de Continuidad de TI				80,00%
	Recuperación y Reanudación de los Servicios de TI				80,00%
	Almacenamiento de Respaldos Fuera de las Instalaciones				100,00%
	Revisión Post Reanudación				60,00%
Indicador de Madurez	$m = 75{,}00\%$ NIVEL 4	Grado de Madurez Real de la Institución			$m_{rl} = 75{,}00\%$
Indicador de Desempeño	$d = 72{,}92\%$	Grado de Desempeño Real			$d_r = 75{,}83\%$

	MUY BUENO	Grado de Desempeño COBIT	$d_c = 70{,}00\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 78{,}00\%$		
	CUMPLE CASI TOTALMENTE		
Impacto	$I = 87{,}50\%$	Grado de Impacto	$I_c = 75{,}00\%$
	ALTO	Grado de Importancia	$I_s = 100{,}00\%$

Formalizado / Normado	Si	**Control Interno**	Documentado	**Responsable**	Unidad de TI

TENDENCIAS	El desarrollo de resistencia en las soluciones automatizadas y desarrollando, manteniendo y probando los planes de continuidad de TI.
FORTALEZAS	Los recursos críticos de TI, necesarios para la recuperación, se almacenan fuera de las instalaciones.
PUNTOS DEBILES Y AMENAZAS	No están bien definidos procedimientos para valorar los resultados del plan de reanudación de las funciones de TI después de un desastre.
RECOMENDACIONES Y PLANES DE ACCIÓN	Desarrollar y mantener los planes de contingencia de TI, con entrenamiento y pruebas guardando copias de los datos fuera de las instalaciones.

		ESTADO DEL PROCESO		**IMPACTO**
DS5	**Garantizar la seguridad de los sistemas**	C = 70,04	$\alpha = 50{,}80$ $\beta = 62{,}86$ $\gamma = 51{,}21$	Alto

OBJETIVO	Mantener la integridad de la información y de la infraestructura de procesamiento y minimizar el impacto de las vulnerabilidades e incidentes de seguridad.

SITUACION ACTUAL

Objetivos de Control	Administración de la Seguridad de TI		80,00%
	Plan de Seguridad de TI		80,00%
	Administración de Cuentas del Usuario		100,00%
	Pruebas, Vigilancia y Monitoreo de la Seguridad		80,00%
	Definición de Incidente de Seguridad		60,00%
	Protección de la Tecnología de Seguridad		60,00%
	Administración de Llaves Criptográficas		80,00%
	Prevención, Detección y Corrección de Software Malicioso		80,00%
	Seguridad de la Red		60,00%
	Intercambio de Datos Sensitivos		80,00%
Indicador de Madurez	$m = 76{,}67\%$	Grado de Madurez Real de la Institución	$m_{rl} = 83{,}33\%$
	NIVEL 4		
Indicador de Desempeño	$d = 55{,}34\%$	Grado de Desempeño Real	$d_r = 50{,}67\%$
	SATISFACTORIO	Grado de Desempeño COBIT	$d_c = 60{,}00\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 76{,}00\%$		
	CUMPLE CASI TOTALMENTE		
Impacto	$I = 41{,}50\%$	Grado de Impacto	$I_c = 16{,}00\%$
	MEDIO	Grado de Importancia	$I_s = 67{,}00\%$

Formalizado / Normado	NO	**Control Interno**	Documentado	**Responsable**	Unidad de TI

TENDENCIAS	La definición de políticas, procedimientos y estándares de seguridad de TI y el monitoreo, detección, reporte y resolución de las vulnerabilidades e incidentes de seguridad.
FORTALEZAS	Se identifican de manera única todos los usuarios y su actividad en sistemas de TI. Se garantiza que la solicitud, emisión, suspensión, modificación y cierre de cuentas y privilegios de acceso, sean dirigidas por un administrador.
PUNTOS DEBILES Y AMENAZAS	A pesar de que **s**e utilizan técnicas de seguridad y procedimientos de administración asociados para autorizar acceso y controlar los flujos de información desde y hacia las redes, pueden surgir vulnerabilidades.
RECOMENDACIONES Y PLANES DE ACCIÓN	Entender y priorizar los requerimientos, vulnerabilidades y amenazas de seguridad. Probar la seguridad de forma regular.

		ESTADO DEL PROCESO		**IMPACTO**
DS6	**Identificar y asignar costos**	C = 76,77%	$\alpha = 56{,}04$ $\beta = 61{,}35$ $\gamma = 47{,}40$	Medio

OBJETIVO	Transparentar y entender los costos de TI y mejorar la rentabilidad a través del uso bien informado de los servicios de TI.

SITUACION ACTUAL				
Objetivos de Control	Definición de Servicios			100,00%
	Contabilización de TI			100,00%
	Modelación de Costos y Cargos			80,00%
	Mantenimiento del Modelo de Costos			80,00%
Indicador de Madurez	$m = 74{,}29\%$	Grado de Madurez Real de la Institución		$m_{rl} = 71{,}43\%$
	NIVEL 4			
Indicador de Desempeño	$d = 63{,}75\%$	Grado de Desempeño Real		$d_r = 54{,}17\%$
	MUY BUENO	Grado de Desempeño COBIT		$d_c = 73{,}33\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 90{,}00\%$			
	CUMPLE TOTALMENTE			
Impacto	$I = 55{,}00\%$	Grado de Impacto		$I_c = 43{,}00\%$
	MEDIO	Grado de Importancia		$I_s = 67{,}00\%$
Formalizado / Normado	Si	**Control Interno**	Documentado	**Responsable** Unidad de TI
TENDENCIAS	El registro completo y preciso de los costos de TI, un sistema equitativo para asignación acordado con los usuarios, y un sistema para reportar oportunamente el uso de TI y los costos asignados.			
FORTALEZAS	Se identifican todos los costos de TI y se equiparan a los servicios de TI, para soportar un modelo de costos transparente.			
PUNTOS DEBILES Y AMENAZAS	En ocasioneslos cargos por servicios no son identificables, medibles y predecibles para propiciar un adecuado uso de los recursos.			
RECOMENDACIONES Y PLANES DE ACCIÓN	Alinear los cargos con la calidad y cantidad de los servicios brindados. Construir y aceptar un modelo de costos completo. Aplicar cargos en base a políticas acordadas.			

DS7	**Educar y entrenar a los usuarios**	**ESTADO DEL PROCESO**		**IMPACTO**
		$C = 73{,}72\%$	$\alpha = 54{,}43$	Medio
			$\beta = 63{,}37$	
			$\gamma = 47{,}25$	

OBJETIVO	El uso efectivo y eficiente de soluciones y aplicaciones tecnológicas y el cumplimiento del usuario con las políticas y procedimientos.

SITUACION ACTUAL				
Objetivos de Control	Identificación de Necesidades de Entrenamiento y Educación			100,00%
	Impartición de Entrenamiento y Educación			80,00%
	Evaluación del Entrenamiento Recibido			80,00%
Indicador de Madurez	$m = 74{,}29\%$	Grado de Madurez Real de la Institución		$m_{rl} = 71{,}43\%$
	NIVEL 4			
Indicador de Desempeño	$d = 57{,}23\%$	Grado de Desempeño Real		$d_r = 67{,}78\%$
	SATISFACTORIO	Grado de Desempeño COBIT		$d_c = 46{,}67\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 86{,}67\%$			
	CUMPLE TOTALMENTE			
Impacto	$I = 54{,}00\%$	Grado de Impacto		$I_c = 75{,}00\%$
	MEDIO	Grado de Importancia		$I_s = 33{,}00\%$
Formalizado / Normado	NNO	**Control Interno**	No Documentado	**Responsable** Unidad de TI
TENDENCIAS	Un claro entendimiento de las necesidades de entrenamiento de los usuarios de TI, la ejecución de una efectiva estrategia de entrenamiento y la medición de resultados.			
FORTALEZAS	Se establece y actualiza de forma regular un programa de capacitación para cada grupo objetivo de funcionarios.			
PUNTOS DEBILES Y AMENAZAS	Al finalizar la capacitación, generalmente no se evalúa respecto a la relevancia, calidad, efectividad, percepción, retención del conocimiento y el costo.			
RECOMENDACIONES Y PLANES DE ACCIÓN	Establecer un programa de entrenamiento. Organizar el entrenamiento. Impartir el entrenamiento. Monitorear y reportar la efectividad del entrenamiento.			

DS8	**Administrar la mesa de servicio y los incidentes**	**ESTADO DEL PROCESO**		**IMPACTO**
		$C = 69{,}56\%$	$\alpha = 53{,}64$	Medio
			$\beta = 59{,}95$	

			$\gamma = 50,89$	
OBJETIVO	Permitir el efectivo uso de los sistemas de TI garantizando la resolución y el análisis de las consultas de los usuarios finales, incidentes y preguntas.			
SITUACION ACTUAL				
Objetivos de Control	Mesa de Servicios			100,00%
	Registro de Consultas de Clientes			60,00%
	Escalamiento de Incidentes			60,00%
	Cierre de Incidentes			80,00%
	Análisis de Tendencias			80,00%
Indicador de Madurez	$m = 71,43\%$	Grado de Madurez Real de la Institución		$m_{rl} = 57,14\%$
	NIVEL 4			
Indicador de Desempeño	$d = 60,33\%$	Grado de Desempeño Real		$d_r = 67,33\%$
	SATISFACTORIO	Grado de Desempeño COBIT		$d_c = 53,33\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 76,00\%$			
	CUMPLE CASI TOTALMENTE			
Impacto	$I = 59,50\%$	Grado de Impacto		$I_c = 86,00\%$
	MEDIO	Grado de Importancia		$I_s = 33,00\%$
Formalizado / Normado	Si	**Control Interno**	Documentado	**Responsable** Unidad de TI
TENDENCIAS	Una función profesional de mesa de servicio, con tiempo de respuesta rápido, procedimientos de escalamiento claros y análisis de tendencias y de resolución.			
FORTALEZAS	Existe una mesa de servicios como conexión de los funcionarios con TI que registra, comunica, atiende y analiza, todas las llamadas, los incidentes reportados, los requerimientos de servicio y las solicitudes de información. Además se mide la satisfacción del usuario en cuanto a la calidad de la mesa de servicios.			
PUNTOS DEBILES Y AMENAZAS	No se disponen de procedimientos adecuados de mesa de servicios, de manera que los incidentes que no puedan resolverse de forma inmediata sean escalados apropiadamente, de acuerdo con los límites acordados en el SLA.			
RECOMENDACIONES Y PLANES DE ACCIÓN	Monitoreo y reporte de tendencias de las mesas de servicios. Definir procedimientos y criterios de escalamiento claros.			

DS9 Administrar la configuración	**ESTADO DEL PROCESO**		**IMPACTO**
	$C = 74,89\%$	$\alpha = 56,29$ $\beta = 56,07$ $\gamma = 51,92$	Alto

OBJETIVO	Optimizar la infraestructura, recursos y capacidades de TI, y llevar registro de los activos de TI.			
SITUACION ACTUAL				
Objetivos de Control	Repositorio y Línea Base de Configuración			80,00%
	Identificación y Mantenimiento de Elementos de Configuración			80,00%
	Revisión de Integridad de la Configuración			80,00%
Indicador de Madurez	$m = 72,00\%$	Grado de Madurez Real de la Institución		$m_{rl} = 60,00\%$
	NIVEL 4			
Indicador de Desempeño	$d = 72,41\%$	Grado de Desempeño Real		$d_r = 71,48\%$
	MUY BUENO	Grado de Desempeño COBIT		$d_c = 73,33\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 80,00\%$			
	CUMPLE CASI TOTALMENTE			
Impacto	$I = 71,00\%$	Grado de Impacto		$I_c = 75,00\%$
	ALTO	Grado de Importancia		$I_s = 67,00\%$
Formalizado / Normado	Si	**Control Interno**	No Documentado	**Responsable** Unidad de TI
TENDENCIAS	Establecer y mantener un repositorio completo y preciso de atributos de la configuración de los activos y de líneas base y compararlos contra la configuración actual.			
FORTALEZAS	Se revisa y verifica de manera regular el estado de los elementos de configuración y la existencia de cualquier software personal o no autorizado.			
PUNTOS DEBILES Y AMENAZAS	No está establecido un repositorio central que contenga toda la información referente a los elementos de configuración de hardware, software, middleware, y las herramientas para operar, acceder y utilizar los sistemas y los servicios.			
RECOMENDACIONES Y PLANES DE ACCIÓN	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.				
DS10 Administrar los problemas			**ESTADO DEL PROCESO**		**IMPACTO**
			$C = 66{,}47\%$	$\alpha = 51{,}65$ $\beta = 60{,}30$ $\gamma = 52{,}55$	Medio
OBJETIVO	Garantizar la satisfacción de los usuarios finales con ofrecimientos de servicios y niveles de servicio, reducir el trabajo y los defectos en la prestación de los servicios y de las soluciones.				
SITUACION ACTUAL					
Objetivos de Control	Identificación y Clasificación de Problemas				80,00%
	Rastreo y Resolución de Problemas				80,00%
	Cierre de Problemas				60,00%
	Integración de las Administraciones de Cambios, Configuración y Problemas				60,00%
Indicador de Madurez	$m = 71{,}43\%$ NIVEL 4	Grado de Madurez Real de la Institución			$m_{rl} = 57{,}14\%$
Indicador de Desempeño	$d = 57{,}04\%$	Grado de Desempeño Real			$d_r = 54{,}07\%$
	SATISFACTORIO	Grado de Desempeño COBIT			$d_c = 60{,}00\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 70{,}00\%$				
	CUMPLE CASI TOTALMENTE				
Impacto	$I = 59{,}50\%$	Grado de Impacto			$I_c = 86{,}00\%$
	MEDIO	Grado de Importancia			$I_s = 33{,}00\%$
Formalizado / Normado	Si	**Control Interno**	No Documentado	**Responsable**	Unidad de TI
TENDENCIAS	Registrar, rastrear y resolver problemas operativos; investigación de las causas raíz de todos los problemas relevantes y definir soluciones para los problemas operativos identificados.				
FORTALEZAS	Se analiza y determina la causa raíz de gran parte de los problemas.				
PUNTOS DEBILES Y AMENAZAS	No se cuenta con un sistema o plan de administración de problemas que establezca mecanismos de análisis óptimos.				
RECOMENDACIONES Y PLANES DE ACCIÓN	Realizar un análisis de causas raíz de los problemas reportados. Analizar las tendencias. Tomar propiedad de los problemas con una resolución de problemas progresiva.				
DS11 Administrar los datos			**ESTADO DEL PROCESO**		**IMPACTO**
			$C = 80{,}21\%$	$\alpha = 46{,}86$ $\beta = 67{,}76$ $\gamma = 51{,}40$	Medio
OBJETIVO	Optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera.				
SITUACION ACTUAL					
Objetivos de Control	Requerimientos de la Institución para Administración de Datos				100,00%
	Acuerdos de Almacenamiento y Conservación				80,00%
	Sistema de Administración de Librerías de Medios				80,00%
	Eliminación				100,00%
	Respaldo y Restauración				80,00%
	Requerimientos de Seguridad para la Administración de Datos				80,00%
Indicador de Madurez	$m = 95{,}00\%$ NIVEL 5	Grado de Madurez Real de la Institución			$m_{rl} = 75{,}00\%$
Indicador de Desempeño	$d = 52{,}60\%$	Grado de Desempeño Real			$d_r = 45{,}19\%$
	SATISFACTORIO	Grado de Desempeño COBIT			$d_c = 60{,}00\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 86{,}67\%$				
	CUMPLE TOTALMENTE				
Impacto	$I = 49{,}50\%$	Grado de Impacto			$I_c = 32{,}00\%$
	MEDIO	Grado de Importancia			$I_s = 67{,}00\%$
Formalizado / Normado	NO	**Control Interno**	Documentado	**Responsable**	Unidad de TI
TENDENCIAS	Mantener la integridad, exactitud, disponibilidad y protección de los datos.				

FORTALEZAS	Se tienen mecanismos para garantizar que se reciben documentos originales, que se procesa toda la información recibida por parte de la institución.				
PUNTOS DEBILES Y AMENAZAS	No se establecen mecanismos adecuados para identificar y aplicar requerimientos de seguridad a la recepción, procesamiento, almacenamiento y entrega de la información.				
RECOMENDACIONES Y PLANES DE ACCIÓN	Respaldar los datos y probar la restauración. Administrar almacenamiento de datos en sitio y fuera de sitio. Desechar de manera segura los datos y el equipo.				
DS12 Administrar el ambiente físico		**ESTADO DEL PROCESO**			**IMPACTO**
		C = 79,76%	$\alpha = 57{,}12$ $\beta = 59{,}23$ $\gamma = 48{,}24$		Bajo
OBJETIVO	Proteger los activos de cómputo y la información institucional minimizando el riesgo de una interrupción del servicio.				
SITUACION ACTUAL					
Objetivos de Control	Selección y Diseño del Centro de Datos				80,00%
	Medidas de Seguridad Física				100,00%
	Acceso Físico				100,00%
	Protección Contra Factores Ambientales				80,00%
	Administración de Instalaciones Físicas				100,00%
Indicador de Madurez	$m = 75{,}00\%$ NIVEL 4	Grado de Madurez Real de la Institución			$m_{rl} = 75{,}00\%$
Indicador de Desempeño	$d = 70{,}67\%$	Grado de Desempeño Real			$d_r = 74{,}67\%$
	MUY BUENO	Grado de Desempeño COBIT			$d_c = 66{,}67\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 92{,}00\%$				
	CUMPLE TOTALMENTE				
Impacto	$I = 32{,}50\%$	Grado de Impacto			$I_c = 32{,}00\%$
	BAJO	Grado de Importancia			$I_s = 33{,}00\%$
Formalizado / Normado	Si	**Control Interno**	Documentado	**Responsable**	Unidad de TI
TENDENCIAS	Proporcionar y mantener un ambiente físico adecuado para proteger los activos de TI contra acceso, daño o robo.				
FORTALEZAS	Se definen e implementan medidas de seguridad física, que incluyen las zonas de seguridad, la ubicación de equipo crítico, las áreas de envío y recepción y los procedimientos de monitoreo.				
PUNTOS DEBILES Y AMENAZAS	No se han instalado dispositivos especializados para monitorear y controlar el ambiente.				
RECOMENDACIONES Y PLANES DE ACCIÓN	Implementar medidas de seguridad físicas.				
DS13 Administrar las operaciones		**ESTADO DEL PROCESO**			**IMPACTO**
		C = 72,95%	$\alpha = 55{,}26$ $\beta = 58{,}41$ $\gamma = 50{,}72$		Alto
OBJETIVO	Mantener la integridad de los datos y garantizar que la infraestructura de TI puede resistir y recuperase de errores y fallas.				
SITUACION ACTUAL					
Objetivos de Control	Procedimientos e Instrucciones de Operación				80,00%
	Programación de Tareas				80,00%
	Monitoreo de la Infraestructura de TI				80,00%
	Documentos Sensitivos y Dispositivos de Salida				80,00%
	Mantenimiento Preventivo del Hardware				80,00%
Indicador de Madurez	$m = 72{,}00\%$ NIVEL 4	Grado de Madurez Real de la Institución			$m_{rl} = 60{,}00\%$
Indicador de Desempeño	$d = 66{,}19\%$	Grado de Desempeño Real			$d_r = 65{,}71\%$
	MUY BUENO	Grado de Desempeño COBIT			$d_c = 66{,}67\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 80{,}00\%$				
	CUMPLE CASI TOTALMENTE				
Impacto	$I = 76{,}50\%$	Grado de Impacto			$I_c = 86{,}00\%$

	ALTO	Grado de Importancia			$I_s = 67{,}00\%$
Formalizado / Normado	NO	**Control Interno**	No Documentado	**Responsable**	Unidad de TI
TENDENCIAS	Cumplir con los niveles operativos de servicio para procesamiento de datos programado, protección de datos de salida sensitivos y monitoreo y mantenimiento de la infraestructura.				
FORTALEZAS	Se han establecido resguardos físicos, prácticas de registro y administración de inventarios adecuados sobre los activos de TI más sensitivos				
PUNTOS DEBILES Y AMENAZAS	Existen deficiencias en los procedimientos de mantenimiento, de manera que no se reduce el impacto de las fallas y la degradación del desempeño.				
RECOMENDACIONES Y PLANES DE ACCIÓN	Operar el ambiente de TI en línea con los niveles de servicio acordados y con las instrucciones definidas. Mantener la infraestructura de TI.				
ME1	**Monitorear y evaluar el desempeño de TI**	**ESTADO DEL PROCESO**			**IMPACTO**
		$\mathbb{C} = 67{,}58\%$	$\alpha = 60{,}58$ $\beta = 59{,}87$ $\gamma = 44{,}61$		Alto
OBJETIVO	Transparencia y entendimiento de los costos, beneficios, estrategia, políticas y niveles de servicio de TI de acuerdo con los requisitos institucionales.				
SITUACION ACTUAL					
Objetivos de Control	Enfoque del Monitoreo				100,00%
	Definición y Recolección de Datos de Monitoreo				80,00%
	Método de Monitoreo				80,00%
	Evaluación del Desempeño				60,00%
	Reportes al Consejo Directivo y a Ejecutivos				100,00%
	Acciones Correctivas				80,00%
Indicador de Madurez	$m = 57{,}50\%$ NIVEL 3	Grado de Madurez Real de la Institución			$m_{rl} = 87{,}50\%$
Indicador de Desempeño	$d = 58{,}75\%$	Grado de Desempeño Real			$d_r = 57{,}50\%$
	SATISFACTORIO	Grado de Desempeño COBIT			$d_c = 60{,}00\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 83{,}33\%$ CUMPLE TOTALMENTE				
Impacto	$I = 76{,}50\%$	Grado de Impacto			$I_c = 86{,}00\%$
	ALTO	Grado de Importancia			$I_s = 67{,}00\%$
Formalizado / Normado	NO	**Control Interno**	Documentado	**Responsable**	Unidad de TI
TENDENCIAS	Monitorear y reportar las métricas del proceso e identificar e implementar acciones de mejoramiento del desempeño.				
FORTELEZAS	Se proporcionan reportes administrativos para ser revisados por la alta dirección, sobre el avance de la institución hacia metas identificadas, específicamente en términos del desempeño del portafolio de programas de inversión habilitados por TI, niveles de servicio de programas individuales y la contribución de TI a ese desempeño.				
PUNTOS DEBILES Y AMENAZAS	Se compara de forma aperiódica el desempeño contra las metas y se tarda en iniciar acciones correctivas para subsanar las causas subyacentes.				
RECOMENDACIONES Y PLANES DE ACCIÓN	Cotejar y traducir los reportes de desempeño de proceso a reportes gerenciales. Comparar el desempeño contra las metas acordadas e iniciar las medidas correctivas necesarias.				
ME2	**Monitorear y evaluar el control interno**	**ESTADO DEL PROCESO**			**IMPACTO**
		$\mathbb{C} = 58{,}41\%$	$\alpha = 59{,}45$ $\beta = 55{,}56$ $\gamma = 49{,}50$		Medio
OBJETIVO	Proteger el logro de los objetivos de TI y cumplir las leyes y reglamentos relacionados con TI.				
SITUACION ACTUAL					
Objetivos de Control	Monitoreo del Marco de Trabajo de Control Interno				60,00%
	Revisiones de Auditoría				80,00%
	Excepciones de Control				60,00%
	Auto Evaluación del Control				40,00%
	Aseguramiento del Control Interno				60,00%
	Control Interno para Terceros				80,00%
	Acciones Correctivas				80,00%
Indicador de Madurez	$m = 51{,}43\%$	Grado de Madurez Real de la Institución			$m_{rl} = 57{,}14\%$

	NIVEL 3		
Indicador de Desempeño	$d = 57{,}22\%$	Grado de Desempeño Real	$d_r = 64{,}44\%$
	SATISFACTORIO	Grado de Desempeño COBIT	$d_c = 50{,}00\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 65{,}71\%$		
	CUMPLE CASI TOTALMENTE		
Impacto	$I = 59{,}50\%$	Grado de Impacto	$I_c = 86{,}00\%$
	MEDIO	Grado de Importancia	$I_s = 33{,}00\%$

Formalizado / Normado	NO	**Control Interno**	No Documentado	**Responsable**	Unidad de TI

TENDENCIAS	El monitoreo de los procesos de control interno para las actividades relacionadas con TI e identificar las acciones de mejoramiento.
FORTALEZAS	Se confirma que los proveedores externos de servicios cumplan con los requerimientos legales y regulatorios, y con las obligaciones contractuales.
PUNTOS DEBILES Y AMENAZAS	No se tiene un programa continuo de autoevaluación.
RECOMENDACIONES Y PLANES DE ACCIÓN	Definir un sistema de controles internos integrados 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 dirección para tomar acciones.

ME3	**Garantizar el cumplimiento regulatorio**	**ESTADO DEL PROCESO**		**IMPACTO**
		$C = 69{,}43$	$\alpha = 53{,}56$ $\beta = 57{,}49$ $\gamma = 53{,}22$	Alto

OBJETIVO	Cumplir las leyes y regulaciones.

SITUACION ACTUAL

Objetivos de Control	Identificar los Requerimientos de las Leyes, Regulaciones y Cumplimientos Contractuales		80,00%
	Optimizar la Respuesta a Requerimientos Externos		80,00%
	Evaluación del Cumplimiento con Requerimientos Externos		60,00%
	Aseguramiento Positivo del Cumplimiento		60,00%
	Reportes Integrados		80,00%
Indicador de Madurez	$m = 71{,}43\%$	Grado de Madurez Real de la Institución	$m_{rl} = 57{,}14\%$
	NIVEL 4		
Indicador de Desempeño	$d = 64{,}63\%$	Grado de Desempeño Real	$d_r = 69{,}26\%$
	MUY BUENO	Grado de Desempeño COBIT	$d_c = 60{,}00\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 72{,}00\%$		
	CUMPLE CASI TOTALMENTE		
Impacto	$I = 76{,}50\%$	Grado de Impacto	$I_c = 86{,}00\%$
	ALTO	Grado de Importancia	$I_s = 67{,}00\%$

Formalizado / Normado	Si	**Control Interno**	Documentado	**Responsable**	Unidad de TI

TENDENCIAS	La identificación de todas las leyes y regulaciones aplicables y el nivel correspondiente de cumplimiento de TI y la optimización de los procesos de TI para reducir el riesgo de no cumplimiento.
FORTALEZAS	Está definido o implementado un proceso para garantizar la identificación oportuna de requerimientos legales locales, internacionales, contractuales, de políticas y regulatorios, relacionados con la información, prestación de servicios, procesos e infraestructura.
PUNTOS DEBILES Y AMENAZAS	Los propietarios de los procesos no siempre toman las acciones correctivas oportunas para resolver cualquier brecha de cumplimiento.
RECOMENDACIONES Y PLANES DE ACCIÓN	Identificar los requisitos legales y regulatorios relacionados con TI. Evaluar el impacto de los requisitos regulatorios. Monitorear el cumplimiento de los requisitos regulatorios.

ME4	**Proporcionar gobierno de TI**	**ESTADO DEL PROCESO**		**IMPACTO**
		$C = 82{,}13\%$	$\alpha = 51{,}22$ $\beta = 60{,}35$ $\gamma = 52{,}95$	Alto

OBJETIVO	La integración de un gobierno de TI con objetivos de la dirección y el cumplimiento con las leyes y regulaciones.

SITUACION ACTUAL

Objetivos de Control	Establecimiento de un Marco de Gobierno de TI	100,00%

	Alineamiento Estratégico		100,00%
	Entrega de Valor		100,00%
	Administración de Recursos		80,00%
	Administración de Riesgos		60,00%
	Medición del Desempeño		80,00%
	Aseguramiento Independiente		80,00%
Indicador de Madurez	$m = 89{,}09\%$	Grado de Madurez Real de la Institución	$m_{rl} = 45{,}45\%$
	NIVEL 5		
Indicador de Desempeño	$d = 70{,}37\%$	Grado de Desempeño Real	$d_r = 70{,}74\%$
	MUY BUENO	Grado de Desempeño COBIT	$d_c = 70{,}00\%$
Indicador de Cumplimiento de Objetivos de Control	$o = 85{,}71\%$		
	CUMPLE TOTALMENTE		
Impacto	$I = 93{,}00\%$	Grado de Impacto	$I_c = 86{,}00\%$
	ALTO	Grado de Importancia	$I_s = 100{,}00\%$

Formalizado / Normado	NO	**Control Interno**	No Documentado	**Responsable**	Unidad de TI

TENDENCIAS	La elaboración de informes para el consejo directivo sobre la estrategia, el desempeño y los riesgos de TI y responder a los requerimientos de gobierno de acuerdo a las directrices del consejo directivo.
FORTALEZAS	Se trabaja con el consejo directivo para definir y establecer un marco de trabajo para el gobierno de TI, que incluye el liderazgo, los procesos, roles, responsabilidades, requerimientos de información, y estructuras organizacionales para garantizar que los programas de inversión habilitados por TI, estén alineados con los objetivos institucionales
PUNTOS DEBILES Y AMENAZAS	No se asegura que tanto la institución como TI evalúen y reporten periódicamente los riesgos asociados con TI y su impacto institucional
RECOMENDACIONES Y PLANES DE ACCIÓN	Establecer un marco de trabajo para el gobierno de TI, integrado al gobierno institucional. Obtener aseguramiento independiente sobre el estatus del gobierno de TI.

Tabla A4.1*Indicadores de Resultados de la AI a la SUPERTEL.(Basado en COBIT 4.1, 2007)*