UNIVERSIDAD DE LAS CIENCIAS INFORMATICAS

ESTRATEGIA DE IMPLEMENTACION DEL MODELO COBIT EN LA FACULTAD 15 DE LA UNIVERSIDAD DE LAS CIENCIAS INFORMATICAS

Trabajo de diploma para optar por el título de Ingeniero en Ciencias Informáticas

Autores: Elide Consuegra Rabí

Armín Alexander González Quesada

Tutores: Ing. Liset González Polanco

Ing. Yadián Guillermo Pérez Betancourt

Ciudad de la Habana, 2010

FRASE

“Si no existe la organización, las ideas, después del primer momento de impulso, van perdiendo eficacia.”

DECLARACION DE AUTORIA

Declaramos que somos los únicos autores del trabajo titulado: Estrategia de implementación del modelo COBIT en la facultad 15 y autorizamos a la Universidad de las Ciencias Informáticas los derechos patrimoniales del mismo, con carácter exclusivo.

Para que así conste firmamos la presente a los___ días del mes de_____ del año_____.

_____ _____

Elide Consuegra Rabí Armín A. González Quesada

_____ _____

Ing. Liset González Polanco Ing. Yadián G. Pérez Betancourt

DATOS DE CONTACTO

Ing. Yadián Guillermo Pérez Betancourt

Graduado de Ingeniero en Ciencias Informáticas en el 2009. Título de Oro. Premio Mella. Cumplió misión en Venezuela. Integra el proyecto Modernización del Sistema Bancario Cubano y se desempeña como Gestor de la Configuración en el mismo.

Ing. Liset González Polanco

Graduado de Ingeniero en Ciencias Informáticas en el 2009. Título de Oro. Integra el proyecto Modernización del Sistema Bancario Cubano y se desempeña como Jefe de Calidad del mismo.

AGRADECIMIENTOS

De Elide:

A mis padres (Lázara Rabí Jiménez y Manuel Consuegra de la Torre) por todo el apoyo que me ha dado a lo largo de estos 5 años, por la fuerza que me han brindado en todos los momentos buenos y malos que he pasado, por ser mis fuentes de inspiración, por ser mis guías, un gran ejemplo a seguir y siempre haber creído en mí.

A mi hermanito querido (Manuel) te quiero mucho, gracias por cuidar a mamá cuando papá y yo estuvimos lejos de la casa.

A mi querida abuela mima (Zenaida Jiménez Abreu), por quererme tanto y estar siempre presente, por todo su cariño y apoyo incondicional.

A mi abuela biga (Abigail de la Torre) que a pesar de estar mas lejos de mi siempre esta atenta y preocupada por si necesito algo.

A toda mi familia en general, muchas gracias, por estar ahí siempre presente en todos estos años y por la ayuda y el apoyo que me han brindado.

A mi novio, por estar a mi lado siempre, tanto en los buenos como en los malos momentos, por ser mi compañero, mi amigo, mi confidente, por su ayuda y apoyo incondicional, y por quererme tanto.

A Joan por ser un amigo incondicional, por brindarme su apoyo en los buenos y malos momentos, por su amistad, confianza y cariño.

A mis amigos Pedro, Yohairo, Pepe (José Antonio), Yusbel, Angel Luis y Néstor, por su apoyo y amistad.

A la Revolución y a Fidel por darnos la oportunidad de superarnos y estudiar en esta Universidad.

A todas las personas que nos ayudaron en la realización de este trabajo.

A mis tutores por estar pendiente de la tesis en todo momento, por sus consejos y su ayuda en general.

Muchas gracias a todos.

De Armín:

A mi mamá por educarme todos estos años con la verdad como precepto e inculcar en mí todos los valores buenos que existen y por enseñarme a ver la vida positivamente.

A mi papá por ser mi otra guía y que al igual que mi mamá me enseñó lo positivo de las cosas y por ayudarme todo este tiempo a enfrentar cualquier tipo de situación. En fin a mis dos padres que siempre me mostraron el buen camino para formar a su hijo y que se convierta en lo que es hoy.

A mi hermano por cuidar a mi mamá todos estos años y por apoyarme cada vez que me hizo falta.

A mi novia por estar a mi lado siempre, tanto en los buenos como en los malos momentos, por ser mi compañera, mi amiga y sobre todo mi sustento y confidente.

A mi familia, a mi tía Ana y a todos mis tíos, a mis primos y a mis abuelos, en especial a mi abuela Ana.

A mi hermano Yoel Martín por mantener nuestra amistad durante tantos años y apoyarme en muchas decisiones importantes.

A mis amigos Joan, Pedro, Yohairo, Pepe (José Antonio), Yusbel, Angel Luis y Néstor, que en un momento u otro fuimos como hermanos, y a todos los demás que creyeron en mí.

A la Revolución por formarme como un profesional preparado de estos tiempos y dejarme ser parte de este maravilloso proyecto futuro que es la UCI.

A Fidel por ser mi ejemplo y guía, y por crear esta bella universidad.

A todos los profesores de la facultad que tuvieron que ver con mi formación y los que me ayudaron en algún momento a desarrollarme en mi vida estudiantil.

A mis tutores por estar pendiente de la tesis en todo momento, por sus consejos y su ayuda en general.

Muchas gracias a todos.

DEDICATORIA

De Elide:

A mi mamá, a mi papá, a mi hermanito, a mi abuela mima, a la memoria de mis abuelos (Silvio Rabí y Juan Consuegra) y a mi familia en general, que siempre me han apoyado incondicionalmente y creyeron en mí.

De Armín:

A mi mamá, a mi papá, a mi hermano, a la memoria de mi abuela Ana y a mi familia en general, que siempre creyeron en mí.

RESUMEN

Actualmente en el proceso productivo de la facultad 15 existe una notable ausencia de control interno dentro del mismo, además de que no hay una correcta organización de sus recursos humanos, así como de sus medios tecnológicos, por lo que se hace necesario proponer un modelo internacional que lleve a cabo el control de las Tecnologías de la Información (TI), debido a que estas constituyen un activo muy valioso para el proceso productivo en la facultad.

El presente trabajo aborda una estrategia de implementación o de implantación como tal del modelo COBIT (Objetivos de Control para la Información y las Tecnologías relacionadas) en los proyectos productivos de la facultad 15, donde se utiliza una metodología para la implantación de la estrategia. En la misma se describen los pasos o aspectos a seguir para obtener resultados satisfactorios, como los requerimientos del negocio, las metas del negocio para TI, las metas de TI alineadas, el modelo de madurez de controles, la arquitectura empresarial de TI y los procesos claves que soportan el negocio, todo esto a través de un marco de trabajo establecido por el modelo COBIT.

Mediante esta estrategia se obtendrá un modelo de madurez a la luz del proceso productivo aplicable en la facultad, llegando a un nivel optimizado cuando se aplique la misma y se obtengan los resultados positivos.

Palabras claves

Requerimientos del negocio de TI, metas de TI alineadas, modelo de madurez, arquitectura empresarial de TI, modelo COBIT.

INDICE DE CONTENIDO

INDICE DE TABLAS

INTRODUCCION

Desde que en los años 80 la compañía norteamericana IBM lanzara al mundo su modelo PC, el uso de las computadoras para la gestión de la información se ha generalizado a un nivel inimaginable. En el mundo de hoy, casi la totalidad de las empresas y organizaciones, dependen de las tecnologías de la información (TI) para realizar sus funciones, por lo que se debe realizar un manejo correcto de la información y las tecnologías, de forma que éstas no se conviertan en un obstáculo para los usuarios.

En la actualidad los datos y las tecnologías de la información son considerados por muchas empresas como sus activos más valiosos. La administración efectiva de la información y de las tecnologías relacionadas, así como de los riesgos que acarrea, son elementos críticos para el éxito y la supervivencia de las organizaciones.

En Cuba, las experiencias con el modelo COBIT (Objetivos de Control para la Información y las Tecnologías relacionadas) son pocas, comenzándose a utilizar en las Auditorías a las Tecnologías de la Información, por el Ministerio de Auditoría y Control (MAC), el Ministerio de la Informática y las Comunicaciones (MIC) y la Corporación CIMEX S.A. La implementación más profunda de COBIT se realizó en la Empresa de Telecomunicaciones de Cuba S.A. (ETECSA), en el ejercicio de las Auditorías Informáticas, desarrollándose soluciones para esta actividad; y más recientemente fue utilizado como marco de referencia en la revisión de las medidas de control para el uso de las redes de datos de dicha empresa.

En la facultad existe un volumen de producción bastante amplio. Los proyectos que se desarrollan son complejos y se encuentran muy ligados a la tecnología. Por la importancia que representan para el país y para los organismos que se beneficiarán con estos software que realizan dichos proyectos, en la facultad 15 los mismos deben estar regidos por un modelo de gobierno informático que mejore la eficiencia de estos. Por lo que se propone el uso del modelo internacional COBIT, como una estrategia de implementación en la facultad 15.

Por la experiencia que existe en el país se quiere implementar el modelo COBIT en la facultad 15 de la Universidad de las Ciencias Informáticas, pero existe la **situación problemática** de que no hay dominio de este modelo en la universidad y no se aplican las buenas prácticas que establece el mismo, por lo que no existe un concepto sólido de gobierno informático, lo que conlleva a que no se realice en la facultad 15.

Por lo que se traza como **problema a resolver**: ¿Cómo realizar gobierno informático en los procesos productivos de la facultad 15?

Por tanto el **objeto de estudio** de esta investigación lo constituyen los procesos productivos en proyectos de desarrollo de software.

De ello se deriva que el **campo de acción** sea: el gobierno informático de los procesos productivos de la Facultad 15.

Se plantea como **objetivo general** aplicar buenas prácticas de gobierno informático a partir del estándar internacional para las tecnologías de la información COBIT, en los procesos productivos de la facultad 15 de la Universidad de las Ciencias Informáticas.

Para darle solución al problema anteriormente planteado se definen los siguientes **objetivos específicos**:

- Definir la metodología para la implementación del marco de controles de TI.
- Evaluar el nivel de madurez del proceso productivo en cuanto a los controles de TI.
- Definir las políticas para el correcto uso de las TI en los procesos productivos de la facultad 15 de la Universidad de las Ciencias Informáticas.
- Obtener una guía para el correcto uso de las TI en los procesos productivos de la facultad 15.

Idea a defender:

La implementación del estándar internacional COBIT, en los procesos productivos de la facultad 15 asegurará buenas prácticas y gobierno de las TI, que permitirá alcanzar una mejor organización de los proyectos en la facultad, añadiendo competitividad y eficiencia.

Métodos empleados:

Se utiliza como estrategia de investigación la Investigación explicativa o experimental. Se hace uso de los métodos teóricos: analítico-sintético y el método de modelación, del cual se hará uso del modelo teórico, y dentro de los métodos empíricos, la entrevista.

Aportes prácticos esperados del trabajo:

Los posibles resultados que se esperan obtener con este trabajo son un correcto uso de los recursos informáticos en los proyectos productivos de la facultad, partiendo de un buen control interno, así como de una buena organización de los recursos humanos y medios tecnológicos, lo que en resumen se denominaría un buen gobierno informático.

1. Capítulo I. Los estándares internacionales para las TI. El proceso productivo en la facultad 15

1.1 Introducción

En este capítulo se hace una descripción de los proyectos productivos de la facultad 15, su organización y sus medios tecnológicos instalados. Además se detalla la situación problemática existente y se hace un recorrido por los principales estándares internacionales para las tecnologías de la información. También se brindan elementos conceptuales que son necesarios para entender el dominio del problema planteado, así como un estado del arte de las principales herramientas y metodologías de gobierno que se utilizan a nivel internacional realizando un análisis de cada una de ellas.

1.2 Conceptos fundamentales

1.2.1 Proceso productivo

Podemos decir que un proceso productivo, es aquel conjunto de elementos, personas, y acciones, que transforman materiales y/o brindan servicios de cualquier índole. Es decir, que se agrega algún tipo de valor. Por lo que resulta muy importante dominar el proceso a partir de sus componentes.

Pero, ¿qué es exactamente el proceso productivo del software desde un punto de vista técnico? Definimos un proceso productivo de software como un marco de trabajo de las tareas que se requieren para construir software de alta calidad. ¿Es proceso, sinónimo de ingeniería del software? La respuesta es sí y no. Un proceso de software define el enfoque que se toma cuando el software es tratado por la ingeniería. Pero la ingeniería del software también comprende la tecnología que tiene el proceso, métodos técnicos y herramientas automatizadas.

Aun más importante es que la ingeniería del software la realizan personas creativas, con conocimiento, que deberían trabajar dentro de un proceso del software definido y avanzado que es apropiado para los productos que construyen y para las demandas de su mercado. (Pressman, 2002).

1.2.2 Control interno

El control interno es un proceso llevado a cabo por las personas de una organización, diseñado con el fin de proporcionar un grado de seguridad "razonable" para la consecución de sus objetivos, dentro de las siguientes categorías:

- Eficiencia y eficacia de la operatoria.
- Fiabilidad de la información financiera.
- Cumplimiento de las leyes y normas aplicables.

El control interno, no consiste en un proceso secuencial, en donde algunos de los componentes afectan sólo al siguiente, sino en un proceso multidireccional repetitivo y permanente, en el cual más de un componente influye en los otros. Dado que el control interno es un proceso, su efectividad es un estado o condición del mismo en un punto en el tiempo. Determinar si un sistema de control interno en particular es "efectivo: es un juicio subjetivo resultante de una evaluación de si los cinco componentes mencionados están presentes y funcionando con efectividad.

1.2.3 Gobierno

En toda empresa es necesario tener un conjunto de directivas, funciones, responsabilidades y procesos para guiar, dirigir y controlar el uso de las tecnologías, manejar la toma de decisiones, formular estrategias y asegurar el logro de los objetivos que se hayan trazado (Microsoft Corporation, 2007). Las estructuras creadas para lograr esto, son las que en el marco de esta investigación están definidas como gobierno y para el caso específico de una empresa que decida adoptar el modelo COBIT, se define como gobierno informático.

1.2.3.1 Gobierno TI

Se entiende por Gobierno TI, el conjunto de acciones que realiza el área de TI en coordinación con la alta dirección para movilizar sus recursos de la forma más eficiente en respuesta a requisitos regulatorios, operativos o del negocio. Constituye una parte esencial del gobierno de la empresa en su conjunto y aglutina la estructura organizativa y directiva necesaria para asegurar que TI soporta y facilita el desarrollo de los objetivos estratégicos definidos.

1.3 Principales normas y estándares internacionales para el gobierno de las TI

1.3.1 Normas ISO

La Organización Internacional para la Normalización (ISO, International Organization for Standardization) es una federación mundial de entidades nacionales de normalización de 130 países, establecida en 1947. Su misión es promocionar el desarrollo de la normalización y actividades relacionadas en el mundo, con vista a facilitar el intercambio internacional de productos y servicios, y aumentar la cooperación en las esferas intelectuales, científicas, tecnológicas y la actividad económica. Existe un gran número de normas ISO, destinadas a casi todas las ramas de la industria, que son reconocidas y aplicadas por una gran cantidad de empresas y organizaciones de todo el mundo. (ISO/IEC 20000-1:2005).

1.3.1.1 ISO 20000

La norma ISO/IEC 20000 de diciembre de 2005 (Information technology – Service management) es la primera aceptada a nivel mundial que tiene como objetivo específico la gestión de los servicios de TI. Describe un conjunto integrado de procesos de gestión para la prestación en forma eficaz de servicios a los negocios y a sus clientes. Esta norma está alineada y se complementa con el enfoque por procesos definido dentro de la biblioteca de infraestructura de TI, ITIL de la Oficina Gubernamental de Comercio del Reino Unido (OGC, Office of Government Commerce). Este estándar es aplicable a pequeñas y grandes empresas, y establece procesos de administración de servicios que permiten entregar éstos con calidad y ajustándose a las necesidades del cliente, asegurándose de que se analizan y administran los riesgos.

Esta norma consiste de tres partes. La primera, ISO/IEC 20000-1:2005, está basada en la norma británica BS 15000-2, es la especificación formal y define los requisitos para que una organización preste servicios de una calidad aceptable a sus clientes. El costo actual de esta parte del estándar es de CHF 84.00 (aproximadamente 68 USD), y puede ser usado por negocios que pretenden ofertar servicios, para proporcionar una aproximación consistente de todos los proveedores de servicios de una cadena de suministros, para referenciar la administración de servicios de TI, como base para la auditoría externa, para demostrar la habilidad de cumplir los requisitos del cliente y/o para mejorar los servicios. Esta primera parte representa el estándar certificable. (ISO/IEC 20000-1:2005).

La segunda parte, ISO/IEC 20000-2:2005, es el código de prácticas y representa el conjunto de mejores prácticas adoptadas y aceptadas por la industria en materia de gestión de servicios de TI. Se basa en la norma británica BS 15000-2, está alineada con la biblioteca ITIL y sirve como guía y soporte en el establecimiento de acciones de mejora en el servicio o en la preparación de auditorías contra el ISO/IEC 20000-1. (ISO/IEC 20000-2:2005).

La tercera parte, establece una **guía sobre la definición del alcance y la aplicabilidad de la norma ISO / IEC 20000-1**

ISO/IEC TR 20000-3:2009 proporciona orientación sobre la definición del alcance, la aplicabilidad y la demostración de la conformidad de los proveedores de servicios orientados a satisfacer los requisitos de la norma ISO / IEC 20000-1, así como los proveedores de servicios que están planeando mejoras en el servicio con la intención de utilizar la norma ISO/IEC 20000 como un objetivo de negocio.

La norma ISO/IEC 20000 se encuentra actualmente bajo un proceso de revisión para alinearse mejor con ITIL V3 y con otros estándares ISO. Es por esto, por lo que tras la reciente publicación de la norma ISO/IEC 20000-3, se están desarrollando dos nuevas partes:

Parte 4: Modelo de Procesos de Referencia (PRM) de gestión de servicios

Este modelo establece las bases del modelo de madurez y el marco de evaluación.

Parte 5: Ejemplar del Plan de Implementación para la norma ISO/IEC 20000-1

1.3.2 ITIL

La Biblioteca de Infraestructura de Tecnologías de Información (ITIL, IT Infrastructure Library) es el marco de referencia más aceptado y utilizado en el mundo, enfocado a la entrega, soporte y administración de servicios de TI. Este estándar fue desarrollado por la Oficina Gubernamental de Comercio del Reino Unido (OGC) y propone una terminología estándar e independiente de la industria y la tecnología, para definir "qué hacer" y "qué no hacer" al aplicar en una organización la administración de servicios de TI.

El marco de ITIL apoya, pero no dicta los procesos de negocios en una organización, por lo que sus mejores prácticas adquieren distintas formas y matices, adaptándose a las necesidades individuales de cada entidad (ORTIZ, 2005). Los procesos de entrega de servicios descritos en ITIL son los siguientes:

- Administración de capacidad
- Administración de disponibilidad
- Administración financiera para los servicios de TI
- Administración de nivel de servicios
- Administración de continuidad de servicios de TI

Entre las ventajas que brinda la aplicación de este estándar se encuentran las siguientes:

- Aumentar la satisfacción de los clientes.
- Reducir el costo de desarrollo de prácticas y procedimientos.
- Mejorar los flujos de comunicación entre el personal de informática y los clientes o usuarios.
- Aumentar la productividad, las capacidades y la experiencia de los colaboradores.
- Incrementar la calidad del servicio y apoyar la operación de la organización.
- Obtener una visión clara de la capacidad de las TI y sus ventajas para la organización.
- Obtener información acerca de los cambios que proporcionarán un mayor beneficio para la organización.
- Permitir la implantación efectiva de las TI.

Favorecer una acertada toma de decisiones con base en indicadores de TI y organizacionales.

- Conocer los procesos de las TI y la forma en que apoyan a los procesos estratégicos.

Las buenas prácticas descritas en ITIL se pueden aplicar a la administración de los servicios de TI de forma interna al proceso productivo de la facultad 15, sin embargo este estándar no abarca todos los problemas que es preciso resolver, pues por ejemplo, no define un marco de control, no trata el tema de la gestión de riesgos, hace muy poca alusión a la estrategia y no presenta un modelo de madurez que permita evaluar la implementación.

En adición, es posible extrapolar los conceptos que brinda ITIL al modelo COBIT, el cómo hacerlo está fuera del alcance de este trabajo y está bien expresado en el documento publicado por la ISACA (Aligning COBIT, 2007).

1.3.3 COBIT

Objetivos de Control para la Información y las Tecnologías relacionadas (Control Objectives for Information and related Technology, COBIT) es una herramienta de gobierno de TI lanzada en 1996 por el IT Governance Institute (ITGI) de la Information Systems Audit and Control Association (ISACA), ambos con sede en Illinois, Estados Unidos. El ITGI "se estableció en 1998 para evolucionar el pensamiento y los estándares internacionales respecto a la dirección y control de la tecnología de información de una empresa. (...) El ITGI ofrece investigación original, recursos electrónicos y casos de estudio para ayudar a los líderes de las empresas y a sus consejos directivos en sus responsabilidades de Gobierno de TI." (COBIT, 2005)

La ISACA es "...una organización global líder de profesionales que representa a individuos en más de 100 países y comprende todos los niveles de la TI –Dirección ejecutiva, gerencia media y practicantes, (...) únicamente posesionada para cubrir el papel de generador central que armoniza los estándares de las prácticas de control de TI a nivel mundial." (COBIT, 2000).

La ISACA es una asociación sin ánimo de lucro, de más de 35,000 profesionales en Sistemas Informáticos dedicados a la auditoría, el control y la seguridad de sistemas informáticos, a través de un compromiso de educación, certificación y estandarización.

La misión de COBIT es: "Investigar, desarrollar, publicar y promover un conjunto de objetivos de control en tecnología de información con autoridad, actualizados, de carácter internacional y aceptados generalmente para el uso cotidiano de gerentes de empresas y auditores."(COBIT, 2000). Esta norma se aplica a los sistemas de información de toda la empresa, y está basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

"El objetivo principal del proyecto COBIT es el desarrollo de políticas claras y buenas prácticas para la seguridad y el control de Tecnología de Información, con el fin de obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales en todo el mundo. La meta del proyecto es desarrollar estos objetivos de control principalmente a partir de la perspectiva de los objetivos y necesidades de la empresa. Esto concuerda con la perspectiva COSO, que constituye el primer y mejor marco referencial para la administración en cuanto a controles internos.

Desde su primera publicación en 1996, este producto ha evolucionado hasta la versión 4.1 de marzo de 2007, que estará disponible en mayo. La cuarta edición, disponible en formato electrónico en el sitio Web de la ISACA y traducida al español, representa el mayor cambio realizado al estándar en el proceso de actualización. Las características a resaltar de este modelo son su enfoque al negocio, que está orientado a los procesos, basado en controles y conducido por mediciones, de forma que establece un puente entre los riesgos del negocio, los controles necesarios y los aspectos técnicos. COBIT está dirigido a tres tipos de audiencias: la administración, los auditores, y los usuarios de TI.

Los beneficios que brinda COBIT son: (COBIT, 2000).

- Mejor alineación de los objetivos de TI con los objetivos de la organización, basados en un enfoque de negocio.
- Una vista, comprensible por la administración, de lo que la tecnología de información hace.
- Posesión y responsabilidades claros, basados en la orientación a procesos.
- Aceptación general por terceros y reguladores.
- Entendimiento compartido entre todos los stakeholders, basado en un lenguaje común.
- Cumplimiento de los requerimientos de COSO para el entorno de control de TI.

1.3.4 Otros estándares y modelos

La tendencia actual que están tomando las empresas que se aventuran en la implementación de estándares, va siendo tomar de cada uno la parte que necesitan, en lugar de decidirse sólo por uno de ellos.

ISM3, SOX, PRINCE2, AS 8015-2005: Corporate Governance of ICT

1.4 Utilización de herramientas para el gobierno informático de las TI

1.4.1 COBIT Advisor 3rd Edition le brinda:

- Un proceso consistente para evaluar la administración y el control de TI.
- Un patrón de comparación (benchmark) reconocido para la administración y el control de TI.
- Revisiones enfocadas mediante selección de los procesos más relevantes, los criterios de información y los recursos de TI.
- Informes de alta calidad a medida de los requerimientos particulares del negocio.
- Una representación visual de la evaluación mediante graficación en línea.
- Comparación gráfica y elaboración de informes sobre las evaluaciones realizadas del negocio y en el tiempo.

COBIT Advisor 3rd Edition:

- Cuenta con una base de datos de 34 procesos, 302 objetivos de control y 374 guías de auditoría.
- Brinda pistas en los procesos.
- Asegura cobertura.
- Brinda revisiones más enfocadas mediante diferentes vistas.
- Brinda la generación de un programa de auditoría a medida.
- Facilita la administración de auditoría mediante registro de observaciones, su clasificación y filtrado.

1.5 Herramientas de monitoreo

1.5.1 Everest

Everest Ultimate Edition es una completa herramienta diseñada para el propósito de Administración y Seguridad, así como para el diagnóstico y solución de problemas en ordenadores, es una solución de auditoría de red automática, rastreo de cambio de sistema y monitoreo de red para todo tipo de iniciativa corporativa, ya sea pequeña, mediana o grande, realiza un extenso y detallado análisis del sistema, mostrando prácticamente todos los aspectos referentes a hardware, software, configuración de red y más. Su función es el monitoreo de los componentes de la PC.

Esta edición Ultimate no se centra tanto en aspectos de redes y conectividad como la Corporate, sino que incluye diversos bancos de pruebas especializados para someter a examen la capacidad de procesador, memoria, disco y otros elementos claves del sistema. Durante la optimización y ajuste del sistema, ofrece información esencial sobre el sistema y las posibilidades de mejora en el desempeño; monitoreo avanzado de los componentes del ordenador y capacidades de diagnóstico para revisar los efectos de los ajustes aplicados. Incluye indicadores de desempeño del CPU, FPU y memoria.

Sus principales características son:

- Herramienta de diagnóstico y ajuste del sistema.
  Información de componentes: placa base, CPU, adaptadores de vídeo, monitor, dispositivos de almacenamiento, adaptadores de red, etc.
- Información de programas: sistema operativo, servidores, visualización, redes, programas instalados en general, etc.
- Información de seguridad de Windows y aplicaciones.
- Información de aplicaciones de seguridad (firewall, antivirus, anti-spyware, etc.).
- Diagnóstico del sistema en general.
- Monitoreo de componentes.
- Monitoreo de memoria.
- Reportes detallados.

1.5.2 Herramientas de monitoreo y control basado en software libre

1.5.2.1 ProtoMon Lite

ProtoMon Lite es una herramienta para monitorear servidores en red, verificará automáticamente el funcionamiento de su servidor usando el protocolo HTTP o ICMP (Ping) y le notificará si no se encuentra en línea.

Si un servidor no está respondiendo, ProtoMon llevará a cabo algunas de las siguientes acciones:

- Desplegará una ventana emergente como notificación.
- Envía un mensaje de aviso por correo electrónico.

El programa puede realizar algunas acciones adicionales, tales como comprobar la conexión a Internet o filtrar el contenido descargado. ProtoMon almacena estadísticas completas del resultado del monitoreo, y puede representarlas en cualquier momento en formato de texto o gráficamente.

1.5.2.2 OpenVas

OpenVas realiza una evaluación de las vulnerabilidades del sistema y constituye un escáner de seguridad de red con herramientas asociadas. El componente básico es un servidor con un conjunto de pruebas de vulnerabilidades de red (NVTs) para detectar problemas de seguridad en sistemas remotos y las aplicaciones. Este es un producto basado en software libre con licencia GPL.

La nueva versión introduce nuevas características y una nueva arquitectura, que constituyen la base para convertir el escáner de vulnerabilidades en una solución de gestión de vulnerabilidades.

1.5.2.3 Zenoss

Zenoss es una herramienta de monitoreo de redes y servidores basada en otras herramientas como cacti y nagios (ambas código abierto) que permite a los administradores tener un control completo sobre la infraestructura de red. Desde la instalación, la configuración y la administración fueron simplificadas al máximo para permitirnos disponer de una poderosa herramienta de monitoreo con un esfuerzo mínimo.

La administración de Zenoss se realiza desde una interface web lo que simplifica la tarea a personas novatas en la aplicación y posibilita la configuración de la herramienta prácticamente sin la necesidad de modificar archivos de configuración.

Zenoss nos permite realizar monitoreo de sistemas operativos Windows y Linux prácticamente sin la necesidad de instalar agentes en los sistemas operativos.

Sus principales características son:

- Monitoreo de servicios
- Monitoreo de procesos
- Monitoreo de performance
- Colección de log

Todas estas funciones se realizan por medio de SNMP o WMI para los sistemas Windows.

1.5.2.4 Nessus

Nessus es la herramienta de evaluación de seguridad "Open Source" de mayor renombre. Es un escáner de seguridad remoto para Linux, BSD, Solaris y Otros Unix. Está basado en plug-in(s), tiene una interfaz basada en GTK, y realiza más de 1200 pruebas de seguridad remotas. Permite generar reportes en HTML, XML, LaTeX, y texto ASCII; también sugiere soluciones para los problemas de seguridad.

Hace posible evaluar módulos de seguridad intentando encontrar puntos vulnerables que deberían ser reparados. Está compuesto por dos partes: un servidor, y un cliente. El servidor/daemon, "nessusd" se encarga de los ataques, mientras que el cliente, "nessus", se ocupa del usuario por medio de una linda interfaz para X11/GTK+. Este paquete contiene el cliente para GTK+1.2, que además existe en otras formas y para otras plataformas.

El programa es 100% configurable por lo que se puede elegir el modo de trabajo del programa y el nivel de protección que deseas para tu red o simplemente tu PC.

Con Nessus se pueden grabar informes donde hay enlaces que explican el tipo de vulnerabilidad encontrada, cómo "explotarla" y cómo "evitarla". Los resultados también pueden ser guardados en una base de conocimiento para referencia en futuros escaneos de vulnerabilidades.

Entre sus características principales se encuentran:

Gratis: Nessus es gratuito para uso personal. Para obtenerlo no tiene que hacer más que descargarlo desde su página oficial.

Facilidad de uso: La seguridad es uno de los aspectos más importantes de un sistema, de manera que Nessus pretende proveer una interfaz sencilla, cómoda y fácil de usar.

Escaneo de puertos: Es una técnica empleada para monitorizar las posibles entradas a un ordenador. Un escaneado verifica que el host cliente esté activo para comenzar a buscar todos los puertos que la máquina tenga abiertos. Esta información será utilizada más tarde por Nessus para comprobar si alguno de los puertos abiertos presenta vulnerabilidades que puedan ser utilizadas para lograr acceso a dicha máquina.

Logs o Resultados obtenidos: Todos los datos obtenidos, junto con algunas estadísticas que quedan almacenadas en un completo informe.

Plataformas compatibles con Nessus: Podemos encontrar Nessus 3 para: Red HatEnterprise Server, Red Hat Fedora Core, SuSE Linux, Debian, FreeBSD, Solaris, Ubuntu, Windows y Mac OS X. La distribución de Nessus consta de cuatro ficheros básicos: las librerías del programa, las librerías NASL (Nessus Attack Scripting Language), el núcleo de la aplicación y sus plugins.

APLICACIÓN DE NESSUS EN LAS ETAPAS DE LA AUDITORÍA

Nessus actúa en las siguientes etapas de la Auditoria:

Analizar y evaluar el control Interno

En esta etapa, Nessus juega un rol importante. Analizar y evaluar el control interno permite realizar estimaciones sobre el grado de efectividad que dicho control interno suministra. Estas estimaciones son efectuadas por parte del Auditor a través de su experiencia profesional. Con Nessus, un Auditor puede lograr mayor o menor efectividad de acuerdo a los plugins utilizados.

Aplicar pruebas de auditoria

Nessus esta orientado a pruebas sustantivas, esto significa que se van a tener en cuenta los productos de los procesos en lugar de los procesos en si.

Informar sobre los resultados de la auditoria

Este software tiene la capacidad de realizar un informe detallado de los resultados de los ataques realizados utilizando datos estadísticos y gráficos, de manera relativa a la base de datos de plugins y fallas detectadas.

1.6 Herramientas de planificación y organización

1.6.1 Redmine

Redmine es una aplicación flexible para la gestión de los proyectos, además de que es multiplataforma. Es utilizada en la universidad para la planificación y organización de los mismos, la cual presenta varias funcionalidades como: gestión de tareas, incidencias, multi-proyecto, control de accesos por roles, diagramas de Gantt, gestión de avisos, gestión de documentos y ficheros, calendario de actividades, noticias, wiki y fórum por proyecto, registro de tiempos, campos personalizables, multi-lenguaje, integración con distintos repositorios de datos (Subversión, CVS, Mercurial, Bazaar y Dracs), autentificación por LDAP, generación de informes y soporte de múltiples bases de datos..

Presenta una interfaz muy limpia, intuitivo, sencillo de usar y rapidísimo. La configuración de la herramienta resulta, así mismo, muy sencilla, cada proyecto puede configurarse con los módulos que desees que tenga, además de poder definir campos personalizados por proyecto y tarea para permitir una mayor adaptación. Además brinda la posibilidad de definir un perfil distinto por usuario según el proyecto en el que participa.

FUNCIONALIDAD

Gestión de múltiples proyectos: Redmine permite gestionar múltiples proyectos desde una sola interfaz con una ventana de navegador. La navegación es muy sencilla y se puede saltar y cambiar de proyecto en cualquier momento. Además cada proyecto puede tener una configuración totalmente diferente y el usuario tener un rol distinto en cada uno.

Personalización de proyectos: En Redmine cada proyecto es totalmente personalizable, pudiendo encontrar proyectos muy distintos entre sí según sus objetivos. Lo más importante son los módulos que se pueden desactivar o activar para cada proyecto: wiki, foro, noticias, peticiones, control del tiempo, documentos, ficheros o repositorio, aunque hay módulos comunes a todos los proyectos como el de actividad y vistazo.

Sistema flexible de seguimiento de tareas: Una de las mecánicas más útiles para el desarrollo de un proyecto en Redmine son las peticiones y su visualización. Estas peticiones se dividen en 3 tipos (errores, tareas y soporte) y pueden asignarse a un miembro del proyecto.

Integración en repositorios de código: Redmine puede integrarse con un repositorio de código (Subversion, Git, CVS, entre otros) que esté montado en la misma máquina, tan solo hay que indicarle el directorio local.

Uso de calendario y diagrama de Gantt: Redmine incluye un calendario para visualizar todas las peticiones a lo largo de un mes elegido, marcando claramente el día de inicio y de fin de cada petición. Igualmente ocurre con la vista en diagrama de Gantt, que va marcando el porcentaje completado conforme avanzan los días. Las peticiones que se visualizan en ambos casos están sujetas a los filtros definidos por el usuario.

Notificaciones: Configurando previamente el servidor de correo SMTP, Redmine permite enviar notificaciones por correo electrónico en todos los proyectos, definiendo antes los eventos que activan estos avisos. Toda la actividad de cada proyecto también puede exportarse en Atom, para ser seguida desde un lector RSS.

Exportación a distintos formatos: Los informes de peticiones que pueden generarse añadiendo filtros, y que permiten visualizar las diferentes tareas de un proyecto, pueden exportarse en PDF o formato CSV, pudiendo así imprimirlos posteriormente en un formato organizado. Las páginas de la wiki en cambio, pueden exportarse en HTML o TXT.

1.7 Situación actual de los proyectos productivos de la facultad

Como parte de la investigación realizada y principalmente enmarcada en dos de los cuatro dominios principales que presenta el modelo de gobierno COBIT, se lleva a cabo un estudio en los proyectos productivos de la facultad 15, detectándose problemas dentro de los mismos, en cuanto a: su planificación y organización y al monitoreo y control permanente de los medios tecnológicos.

En estos momentos y tomándose dos de sus principales proyectos productivos como ejemplo: SUA (Sistema Único de Aduanas) y SAGEB (Sistema Automatizado para la Gestión Bancaria), se puede decir que en estos no existe ninguna de las herramientas conocidas para el monitoreo y control de hardware y software de las computadoras. La distribución de los recursos humanos se realiza de la siguiente manera: 2 o 3 estudiantes por computadora de acuerdo al horario docente, con una matrícula de 86, contando con 2 laboratorios de 31 computadoras para la producción en el proyecto Aduana, también se vinculan al mismo 20 profesores y 10 que no están en plantilla. En el caso de SAGEB hay como matricula 60 estudiantes, 20 profesores aproximadamente y se cuenta con dos laboratorios de 30 y 20 computadoras en ese orden respectivamente.

A esto se le añade el problema que existe con los roles de cada persona en los proyectos que no existe el rol que efectué el monitoreo y control de los medios tecnológicos y el rol que realiza la planificación y organización no trabaja eficientemente dentro de su ámbito.

Partiendo de esta situación se decide utilizar como herramienta de monitoreo y control para los proyectos, el software Everest, en el caso de los que utilicen como sistema operativo Windows y para los que utilicen GNU/Linux, se empleará Nessus.

1.8 Conclusiones parciales

A pesar de no ser el único estándar en el mundo, COBIT según reflejan las estadísticas a nivel internacional, es usado en muchas empresas y organizaciones, siendo así en más de 100 países. Desde hace algunos años en nuestro país se vienen dando los primeros pasos asegurando muchos especialistas que su uso se hará inevitable por los beneficios que brinda este modelo de gobierno informático. Ello se debe en parte a que no excluye el uso de otras herramientas, estándares, información, procedimientos y pruebas que estén dirigidas a la obtención de los mismos resultados (COBIT, 2000), y además, se basa en otros 41 estándares de seguridad, auditoría y control.

Una de las fortalezas de este modelo es su novedoso enfoque al negocio y sus objetivos, contemplando los procesos que están informatizados y los que no, de forma global. La documentación existente en el sitio Web de ISACA, tanto casos de estudio como guías de alineación con otros estándares, así como el propio estándar traducido al español, facilitan su uso.

A partir del nivel que se pretenda alcanzar se torna un poco complicado la aplicación de este modelo por la complejidad que el mismo posee, en nuestro caso en la facultad su éxito depende del entendimiento que se logre y de su aceptación.

2. Capítulo II. Estrategia de implementación del modelo COBIT.

2.1 Introducción

En este capítulo se hace referencia a los conceptos relacionados con COBIT que son necesarios para el entendimiento del lector, se describe la metodología diseñada para la implementación del marco de controles, se da una idea de la madurez del proceso productivo en cuanto a los controles de TI y se mencionan los requerimientos del negocio y metas de TI del proceso productivo de la facultad 15, se destacan además, los procesos clave de TI y se mencionan los controles a implementar por cada actividad de TI.

2.2 Marco conceptual

A continuación se relacionan algunos conceptos fundamentales que son necesarios conocer para el entendimiento del marco de trabajo de TI.

Control: Se define como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable que los objetivos de negocio se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos.

Objetivo de Control: Un objetivo de control de TI es una declaración del resultado o fin que se desea lograr al implantar procedimientos de control en una actividad de TI en particular. Los objetivos de control de COBIT son los requerimientos mínimos para un control efectivo de cada proceso de TI.

Nivel de Madurez: Los niveles de madurez están diseñados como perfiles de procesos de TI, que una empresa reconocería como descripciones de estados posibles actuales y futuros. No están diseñados para ser usados como un modelo limitante, donde no se puede pasar al siguiente nivel superior sin haber cumplido todas las condiciones del nivel inferior.

2.3 Marco de trabajo de COBIT

Cada vez más, la alta dirección de los proyectos productivos en la universidad se está dando cuenta del impacto significativo que la información puede tener en el éxito de una empresa. La dirección espera de las TI que contribuyan al éxito del negocio y se pueda obtener una ventaja competitiva de su buen uso. El éxito de la Organización depende en gran medida de que se entiendan los riesgos y se aprovechen los beneficios de las TI, para ello, se necesita:

- Alinear la estrategia de las TI con la estrategia del negocio.
- Lograr que toda la estrategia de las TI, así como las metas fluyan de forma gradual a toda la empresa.
- Proporcionar estructuras organizativas que faciliten la implementación de las metas del negocio.
- Crear las comunicaciones efectivas entre el negocio y las TI, y con los socios externos.
- Medir el desempeño de las TI.

El gobierno y los marcos de trabajo de control son parte de las mejores prácticas de la administración de las TI y facilitan su Gobierno, además de la necesidad de cumplir con el constante incremento de requerimientos regulatorios. Las mejores prácticas de las TI se han vuelto significativas debido a un número de factores:

- Directores de negocio y consejos directivos que demandan un mayor retorno de la inversión en las TI.
- Preocupación por el creciente nivel de gasto en las TI.
- Iniciativas de gobierno de TI que incluyen la adopción de marcos de referencia de control y de mejores prácticas para ayudar a monitorear y mejorar las actividades críticas de las TI, aumentar el valor del negocio y reducir sus riesgos.
- La madurez y concienciación creciente y la aceptación de marcos de trabajo respetados tales como: COBIT, ITIL, ISO, ISO 20 000, CMM y PRINCE2, etc.
- La necesidad de las empresas de valorar su desempeño en comparación con estándares generalmente aceptados y con respecto a su competencia.

COBIT define las actividades de TI en un modelo genérico de procesos en cuatro dominios. Estos dominios son: Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y Monitorear y Evaluar. Los dominios se equiparán a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear. La incorporación de un modelo y un lenguaje común para todas las partes de un negocio involucradas en TI es uno de los pasos iniciales más importantes hacia un buen gobierno. En el caso de la facultad 15 se enmarcarán solamente en dos de los cuatro dominios que propone COBIT: Planear y organizar (PO) y Monitorear y evaluar (ME).

Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados. Éstos se pueden resumir como sigue:

PLANEAR Y ORGANIZAR (PO)

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada.

Este dominio cubre los siguientes cuestionamientos típicos de la gerencia:

- ¿Están alineadas las estrategias de TI y del negocio?
- ¿La empresa está alcanzando un uso óptimo de sus recursos?
- ¿Entienden todas las personas dentro de la organización los objetivos de TI?
- ¿Se entienden y administran los riesgos de TI?
- ¿Es apropiada la calidad de los sistemas de TI para las necesidades del negocio?

MONITOREAR Y EVALUAR (ME)

Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.

Por lo general abarca las siguientes preguntas de la gerencia:

- ¿Se mide el desempeño de TI para detectar los problemas antes de que sea demasiado tarde?
- ¿La Gerencia garantiza que los controles internos son efectivos y eficientes?
- ¿Puede vincularse el desempeño de lo que TI ha realizado con las metas del negocio?
- ¿Se miden y reportan los riesgos, el control, el cumplimiento y el desempeño?

2.3.1 Estrategia de implementación

COBIT debido al costo de implementación se justifica cuando la empresa tiene necesidad de medir el riesgo Informático del negocio, esto se visualiza por las exigencias de auditoría tanto de los procesos informáticos (creación de usuarios, órdenes de cambio, metodologías de implementación, etc.) como de las aplicaciones (documentación, puntos de control, etc.). Por parte de la facultad 15 se tiene dicha necesidad, por lo cual se verifican todos los procesos que recogen los dos dominios a implantar dentro de la estrategia.

Los procesos actuales del área informática se mapean con los procesos COBIT, con esto se puede generar un análisis de gap. A partir del análisis de gap se establece cual es el grado de desarrollo de cada proceso de acuerdo al Modelo de Madurez de COBIT. El **análisis gap** examina las diferencias entre la gestión actual y la información presupuestada. Los resultados obtenidos representan el grado en el que una empresa ha cumplido sus objetivos. El **proceso de análisis gap** implica determinar, documentar y aprobar la discrepancia entre la diferencia existente entre los requerimientos de negocio y las capacidades actuales. El mismo consiste en realizar comparativas y otras valoraciones.

El objetivo principal de este análisis es conocer el diferencial en el desempeño de una organización respecto a las mejores prácticas, estándares y regulaciones legales; evaluar la desviación y establecer los planes para dirigir la organización hacia el cumplimiento de las mismas. El análisis responde dos interrogantes:

- ¿Dónde estamos?
- ¿Dónde deberíamos estar?

En otras palabras un **análisis gap** compara lo que existe actualmente en una organización contra lo que es requerido en seguridad de la información. Los requerimientos se derivan de los estándares, leyes y regulaciones que gobiernan una empresa o industria en particular.

Objetivos del análisis gap:

- Fundamentos para establecer la estrategia y cerrar la brecha de seguridad existente.
- Cumplir con los estándares, leyes y regulaciones exigidos.
- Proteger los activos de información.
- Mejorar los procesos de gestión de tecnología de información.

A partir de lo que expone este análisis y de la estrategia de implementación del modelo COBIT se traza una metodología que se describe mediante una serie de pasos a seguir para una correcta implantación de dicha estrategia, identificando requerimientos del negocio, las metas de TI y los objetivos de control detallados, así como un modelo de madurez de controles, lo cual se aplicará en el proceso productivo de la facultad 15.

2.4 Metodología a utilizar

COBIT no es un marco de referencia estricto con una serie de pasos a seguir, sino que se debe ajustar a las necesidades de control de cada empresa donde se desee utilizar. Por esta razón se diseñó una metodología basada en el marco de trabajo de COBIT que permite implementar controles objetivos y enfocarlos hacia el cumplimiento de los requerimientos del negocio, así como medir hasta qué punto se llegó con la implantación de estos. La metodología diseñada es la siguiente:

2.4.1 Definir los requerimientos del negocio

Una de las mayores ventajas de COBIT es que está enfocado al cumplimiento de los requerimientos del negocio, por tanto el primer paso para la implementación del marco de controles tiene que ser la determinación clara de los objetivos y metas del negocio. Esto le corresponde a la dirección del negocio dentro de los proyectos, en combinación con la alta gerencia.

2.4.2 Definir las metas del negocio para TI

Una vez determinados los requerimientos del negocio dentro del proyecto productivo, corresponde a la alta dirección definir qué es lo que el negocio espera que TI le proporcione, en correspondencia con los requerimientos del negocio. Este paso es clave para asegurar la alineación de TI con los requerimientos del negocio.

2.4.3 Definir las metas de TI alineadas

Las metas de TI constituyen la forma que se tiene de medir el desempeño de los procesos de TI de la organización, y se deben definir en concordancia con las metas del negocio para TI. Las metas de TI se deben definir por la alta dirección del proyecto por el método de expertos.

2.4.4 Aplicar modelo de madurez de controles

El modelo de madurez de controles se aplica para conocer el estado inicial de la situación de los controles en el área de TI, y realizar una proyección del resultado que se desea obtener (al nivel que se desea llegar) con la implementación del marco de control. También permite obtener una idea de lo que se necesita hacer para llegar al nivel proyectado.

2.4.5 Definir la arquitectura empresarial de TI

La arquitectura empresarial de TI está formada por los procesos clave de TI, su responsable, así como el flujo de información (sus entradas y salidas de información).

También se encuentran dentro de la arquitectura las aplicaciones, ya sean manuales o automatizadas, que procesan la información de entrada y generan las salidas, así como el personal y la infraestructura necesarias para su ejecución. Esta arquitectura se desglosa como se describe a continuación.

2.4.5.1 Definir los procesos clave que soportan al negocio

Los procesos clave que soportan al negocio se determinan mediante técnicas de trabajo en grupo por la alta dirección de los proyectos productivos, a partir de los procesos genéricos que presenta COBIT, teniendo en cuenta los que ya se llevan a cabo en la universidad como empresa de software y desechando los que no se realizan o no son afines. A cada proceso se le debe asignar una importancia alta, media o baja.

2.4.5.2 Definir el responsable del proceso

El responsable del proceso se determina por parte de la alta dirección de los proyectos mediante el método de expertos. Debe existir una correcta segregación de funciones entre el responsable y las personas que ejecutan las aplicaciones para los dos dominios a utilizar.

2.4.5.3 Aplicar modelo de madurez de procesos

El modelo de madurez de procesos se realiza para cada proceso definido como clave para determinar el nivel inicial que presenta este proceso en la organización, para estimar al nivel que se pretende llegar con la implementación de los controles y para tener una idea de lo que se debe hacer para llegar a ese nivel.

2.4.5.4 Identificar actividades más importantes (Objetivos de control detallados)

Las actividades de TI más significativas que se deben desarrollar en la universidad para el cumplimiento de los objetivos y metas del negocio, se identifican mediante el método de expertos por parte de la alta dirección de los proyectos productivos.

2.4.5.5 Definir controles

En concordancia con el nivel que se desea obtener en el proceso, se deben definir controles (políticas, procedimientos, prácticas y estructuras organizacionales) que contribuyan al cumplimiento de los requisitos del negocio a los cuales responde el proceso de TI.

2.4.6 Aplicar modelo de madurez de controles

Cuando se hayan implementado todos los controles necesarios, se aplica nuevamente el modelo de madurez del control interno para verificar si se ha llegado al nivel que se esperaba, definido en el sub-epígrafe 2.4.4.

2.5 Requerimientos del negocio

Los requerimientos del negocio los constituyen tanto los objetivos del proceso productivo de la facultad 15 como las metas. A continuación se relacionan los objetivos y metas así como el nivel (**P**rimario, **S**ecundario o ninguno) en que tributan hacia las Metas de TI.

	Objetivos	Metas de TI*
O1	Lograr el funcionamiento óptimo de la tecnología instalada.	P
O2	Hacer los diseños de flujo productivo, que especifiquen las variantes posibles, acorde con la tecnología instalada.	P
O3	Capacitar al personal en el domino de la tecnología, en cada puesto de trabajo.	P
O4	Montar un sistema de vigilancia tecnológica, que nos permita mantener actualizada nuestra tecnología acorde con los estándares internacionales.	S
O5	Disminuir el consumo energético.	P
O6	Desarrollar productos propios.	S
O7	Contar con los datos necesarios para realizar una planeación estratégica efectiva.	P
O8	Establecer un sistema de control de la calidad, que garantice la excelencia en nuestros productos.	S
	Metas	Metas de TI
M1	Poseer una tecnología de punta y estandarizada.	P
M2	Contar con un personal altamente calificado y comprometido.	P
M3	Lograr la excelencia en la calidad y aceptación de nuestros productos*.	P
M4	Satisfacer a plenitud a nuestros clientes*.	P
M5	Gozar de un prestigio nacional e internacional*.	P
M6	Alcanzar altos niveles de organización empresarial en todas las operaciones y procesos que se generan en los proyectos productivos de la facultad.	P

Tabla 2.1 Objetivos y metas de TI

* Requerimientos facilitados por TI (Metas del Negocio para TI)

Niveles descritos:

Primario (P**):** Grado por el cual el objetivo de control definido satisface completamente el requerimiento de información concernido.

Secundario (S**):** Grado por el cual el objetivo de control definido sólo satisface en menor extensión o indirectamente el requerimiento del negocio concernido.

Ninguno (N**):** Podría ser aplicable, sin embargo, el requerimiento es más adecuadamente satisfecho por otro criterio en este proceso y/o por otro.

2.6 Metas de TI

A continuación se relacionan las Metas específicas de TI, así como la prioridad que representa cada una para el proceso productivo de la facultad 15. Se tomaron como referencia las metas genéricas de COBIT.

No.	Metas de TI	Prioridad
1	Responder a los requisitos del negocio de acuerdo a la estrategia del negocio.	P
2	Responder a los requisitos de gobierno.	P
3	Optimizar el uso de la información.	P
4	Crear agilidad de TI.	P
5	Definir cómo los requisitos funcionales y de control se traducen a soluciones automatizadas efectivas y eficientes.	S
6	Adquirir y mantener sistemas aplicativos integrados y estandarizados.	P
7	Adquirir y mantener infraestructura de TI integradas y estandarizada.	P
8	Adquirir y mantener habilidades de TI que respondan a la estrategia de TI.	P
9	Garantizar la transparencia y el entendimiento de los costos, beneficios, estrategias, políticas y niveles de servicio de TI.	S
10	Garantizar el uso y el desempeño apropiado de las soluciones aplicativas y tecnológicas.	P
11	Responder por todos los activos de TI y protegerlos.	P
12	Optimizar la infraestructura, recursos y capacidades de TI.	P
13	Reducir los defectos y trabajar en las soluciones y en la prestación del servicio.	S
14	Proteger el logro de los objetivos de TI.	P
15	Establecer claridad del impacto al negocio de los riesgos de los objetivos y recursos de TI.	P
16	Asegurar que la información crítica y confidencial se mantenga resguardada de aquellos que no deben tener acceso a ella.	P
17	Asegurarse de que se puede confiar en los intercambios de información.	S
18	Asegurarse de que los servicios y la infraestructura de TI pueden resistir y recuperarse adecuadamente de las fallas debidas a errores, ataques deliberados o desastres.	P
19	Garantizar un impacto mínimo al negocio en caso de una interrupción o cambio en el servicio de TI.	P
20	Garantizar que los servicios de TI estén disponibles según se requieran.	P
21	Mantener la integridad de la infraestructura de la información y del procesamiento.	P
22	Asegurar que TI cumple las leyes y reglamentos.	P
23	Asegurar que TI demuestra una calidad de servicio, mejora continua, presteza para cambios futuros.	P

Tabla 2.2 Metas específicas de TI

2.7 Análisis actual del flujo productivo a la luz del modelo de madurez de COBIT

Atendiendo al modelo de madurez genérico para el control interno que presenta COBIT, se determinó que el **proceso productivo de la facultad 15** se encuentra en nivel 1(Inicial/Ad hoc) ya que: se reconoce algo de la necesidad del control interno, el enfoque hacia los requerimientos de riesgo y control es ad hoc y desorganizado, sin comunicación o supervisión, no se identifican las deficiencias. En cuanto al establecimiento de controles internos no existe la conciencia de la necesidad de evaluar lo que se necesita en términos de controles de TI, cuando se llevan a cabo, son solamente de ad hoc, a alto nivel y como reacción de incidentes significativos, la evaluación solo se enfoca al incidente presente.

Figura 1.1 Nivel de madurez de los controles internos.

De modo que es este modelo, el que ha llevado que COBIT sea marco de referencia preferido de las grandes compañías mundiales de auditoría.

La siguiente es la descripción genérica de los estados del *Modelo de Madurez*:

- **Inexistente,** se carece totalmente de un proceso. La empresa no ha reconocido la necesidad.
- **Inicial,** existe evidencia que la empresa ha reconocido la necesidad del proceso. No existe un proceso formal – estandarizado – si no que existe enfoques *ad-hoc* que se aplican de manera individual o caso a caso. La gestión del mismo es desorganizada.

- **Repetible,** el proceso se encuentra en un nivel de desarrollo tal que distintas personas ejecutan más o menos los mismos procedimientos. No existe una comunicación ni entrenamiento formal de los procedimientos, y la responsabilidad se mantiene individual. Existe una gran dependencia del conocimiento que tiene los individuos y, por tanto existe una probabilidad de error importante.
- **Definido,** el proceso esta estandarizado, documentado y difundido mediante entrenamiento. Sin embargo, se deja a voluntad de los individuos la aplicación de los procedimientos del proceso y es poco probable que se detecten las desviaciones en su uso. Los procedimientos en sí no son sofisticados y corresponden a la formalización de las prácticas existentes.
- **Gestionado,** es posible monitorear y medir la conformidad en la aplicación de los procedimientos del proceso y es posible tomar acciones cuando el proceso no está operando adecuadamente. Los procesos están mejorándose continuamente. Se dispone de automatizaciones y de herramientas que son usadas de una manera limitada o fragmentada.
- **Optimizado,** el proceso ha sido refinado al nivel de las mejores prácticas, basado en los resultados del mejoramiento continuo y de los modelos ya maduros de otras compañías. Las TI son usadas integralmente para automatizar *workflow*, entregando herramientas que mejoran la calidad y efectividad, aumentando la capacidad de adaptación de le empresa.

El modelo es el que en definitiva posibilita que los procesos que establece COBIT sean auditables, estos son procesos que se pueden verificar primero si se cumplen y ejecutan de acuerdo a lo que la empresa declaró y, por otra parte, este modelo permite establecer cual es el nivel de desarrollo que tiene el proceso en la empresa. Para esto define 6 estados o niveles, cuya definición genérica es la que se incluye en la lista siguiente, no obstante para cada uno de los 34 procesos que conforman el modelo COBIT existe su propio y único *Modelo de Madurez*.

2.8 Procesos de TI identificados

Tomando como base los procesos genéricos de COBIT se identificaron 13 procesos y se definió la importancia (**A**lta, **M**edia o **B**aja) de cada uno de ellos para el proceso productivo de la facultad 15.

Planeación y organización		**Importancia**
PO1	Definir un plan estratégico de TI	A
PO2	Definir la arquitectura de la información	B
PO3	Definir la dirección tecnológica	M
PO4	Definir los procesos, organización y relaciones de TI	B
PO5	Comunicar las metas y la dirección de la gerencia	M
PO6	Administrar los recursos humanos de TI	M
PO7	Administrar la calidad	M
PO8	Evaluar y administrar los riesgos de TI	A
PO9	Administrar los proyectos	A

Tabla 2.4 Nivel de importancia de los Procesos del Dominio Planear y Organizar.

Monitorear y evaluar		**Importancia**
ME1	Monitorear y evaluar el desempeño de TI	A
ME2	Monitorear y evaluar el control interno	M
ME3	Garantizar el cumplimiento regulatorio	B
ME4	Proporcionar gobierno de TI	B

Tabla 2.5 Nivel de importancia de los Procesos del Dominio Monitorear y Evaluar.

3. Capítulo III. Arquitectura empresarial de TI y marco de controles obtenidos.

3.1 Introducción

En este capítulo se muestran en forma de tablas la arquitectura empresarial obtenida por cada proceso definido, estructurados en los dos dominios de COBIT que se trabajarán durante la investigación y la estrategia a definir, así como los controles propuestos a implementar. También se relacionan los niveles de madurez obtenidos para cada proceso de TI, además de una breve descripción y se realiza un resumen de los temas principales relacionados con COBIT basado en controles.

3.2 Basado en controles

COBIT define objetivos de control para los 34 procesos, así como para el proceso general y los controles de aplicación. Los objetivos de control de TI proporcionan un conjunto completo de requerimientos de alto nivel a considerar por la gerencia para un control efectivo de cada proceso de TI.

Ellos:

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

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

• Entradas y salidas genéricas
• Metas de actividades clave (las cosas más importantes a realizar)
• Métricas

3.3 Planeación y organización

PO1 Definir un Plan Estratégico de TI. Descripción del proceso.

La planeación estratégica de TI es necesaria para gestionar y dirigir todos los recursos de TI en línea con la estrategia y prioridades del negocio. La función de TI y los interesados del negocio son responsables de asegurar que el valor óptimo se consigue desde los proyectos y el portafolio de servicios. El plan estratégico mejora la comprensión de los interesados clave de las oportunidades y limitaciones de TI, evalúa el desempeño actual, identifica la capacidad y los requerimientos de recursos humanos, y clarifica el nivel de investigación requerido. (Institute, IT Governance. 2007)

Elementos de la arquitectura:

Proceso:	**Definir un plan estratégico de TI**		**PO1**
Responsable(s):	Gerente		
Importancia:	Alta	Nivel de madurez:	Inicial/Ad hoc (1)*
Entrada:			
• Reportes de costo / beneficio • Evaluación de riesgo • Portafolio de proyectos actualizado • Requerimientos de servicio nuevos / actualizados; portafolio de servicios actualizado • Estrategia y prioridades del negocio • Portafolio de programas • Entradas a desempeño de planeación de TI • Reporte del estado del gobierno de TI; dirección estratégica de la empresa para TI			
Salida:			
• Plan estratégico de TI • Plan táctico de TI • Portafolios de proyectos de TI • Portafolio de servicios de TI • Estrategia de contratación externa de TI • Estrategia de adquisición de TI			

Aplicaciones:	Personal e infraestructura:
Determinación de un plan estratégico para TI.	Jefes de grupos
Objetivos de control:	
PO1.1 Administración del Valor de TI PO1.2 Alineación de TI con el Negocio PO1.3 Evaluación del Desempeño y la Capacidad Actual PO1.4 Plan Estratégico de TI PO1.5 Planes Tácticos de TI PO1.6 Administración del Portafolio de TI	

Tabla 3.1: Elementos de la arquitectura. Definir un plan estratégico de TI (PO1).

Modelo de madurez:

** La gerencia de TI conoce la necesidad de una planeación estratégica de TI. La planeación de TI se realiza según se necesite como respuesta a un requisito de negocio específico. La planeación estratégica de TI se discute de forma ocasional en las reuniones de la gerencia de TI. La alineación de los requerimientos de las aplicaciones y tecnología del negocio se lleva a cabo de modo reactivo en lugar de hacerlo por medio de una estrategia organizacional. La posición de riesgo estratégico se identifica de manera informal proyecto por proyecto.*

Controles propuestos:

Controles:
• **Política para la definición del plan estratégico de TI**: Debe contemplar la participación de la alta gerencia y la gerencia del negocio, para alinear la planeación estratégica de TI con las necesidades del negocio actuales. El plan debe referir cómo la TI contribuirá al logro de las metas de la empresa y se deben describir claramente los riesgos relacionados. • **Procedimiento para la determinación de las capacidades actuales de TI:** Debe contribuir al entendimiento de las capacidades actuales de TI. • **Procedimiento para la priorización de los objetivos del negocio:** Debe permitir la aplicación de un esquema de prioridades que cuantifique los requerimientos del negocio.

Tabla 3.2: Controles propuestos. Definir un plan estratégico de TI (PO1).

PO2 Definir la arquitectura de la información. Descripción del proceso.

La función de sistemas de información debe crear y actualizar de forma regular un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esta información. Esto incluye el desarrollo de un diccionario corporativo de datos que contiene las reglas de sintaxis de los datos de la organización, el esquema de clasificación de datos y los niveles de seguridad. (Institute, IT Governance. 2007)

Elementos de la arquitectura:

<table>
<tr><td>Proceso:</td><td colspan="3">Definir la arquitectura de la información</td><td>PO 2</td></tr>
<tr><td colspan="2">Responsable(s):</td><td colspan="3">Sub-gerente</td></tr>
<tr><td>Importancia:</td><td>Baja</td><td colspan="2">Nivel de madurez:</td><td>Inicial/Ad hoc (1)*</td></tr>
<tr><td colspan="5">Entrada:</td></tr>
<tr><td colspan="5">• Planes estratégicos y tácticos de TI
• Estudio de viabilidad de requerimientos de negocio
• Revisión post implementación
• Información de desempeño y capacidad
• Entrada de desempeño a planes de TI</td></tr>
<tr><td colspan="5">Salida:</td></tr>
<tr><td colspan="5">• Esquema de clasificación de datos
• Plan de sistemas de negocio optimizado
• Diccionario de datos
• Arquitectura de la información
• Clasificación de datos asignada
• Procedimientos y herramientas de clasificación</td></tr>
<tr><td colspan="2">Aplicaciones:</td><td colspan="3">Personal e infraestructura:</td></tr>
<tr><td colspan="2">El establecimiento de un modelo de datos empresarial que incluya un esquema de clasificación de información que garantice la integridad y consistencia de todos los datos.</td><td colspan="3">Alta dirección del proyecto</td></tr>
</table>

Objetivos de control:
PO2.1 Modelo de Arquitectura de Información Empresarial
PO2.2 Diccionario de Datos Empresarial y Reglas de Sintaxis de Datos
PO2.3 Esquema de clasificación de datos
PO2.4 Administración de integridad

Tabla 3.3: Elementos de la arquitectura. Definir la arquitectura de la información (PO2).

Modelo de madurez:

**La gerencia reconoce la necesidad de una arquitectura de información. El desarrollo de algunos componentes de una arquitectura de información ocurre de manera ad hoc o inicial. Las definiciones abarcan datos en lugar de información, y son impulsadas por ofertas de proveedores de software aplicativo. Existe una comunicación esporádica e inconsistente de la necesidad de una arquitectura de información.*

Controles propuestos:

Controles:
• **Procedimiento para el aseguramiento de la exactitud de la arquitectura de la información y del modelo de datos:** Debe contemplar el modelo de arquitectura de información empresarial que establecerá y mantendrá un modelo de información empresarial que facilite el desarrollo de aplicaciones y las actividades de soporte a la toma de decisiones, consistente con los planes de TI. El modelo facilita la creación, uso y compartición óptimas de la información por parte del negocio de una manera que conserva la integridad y es flexible, funcional, oportuna, segura y tolerante a fallas. • **Política de clasificación de la información:** Debe establecer un esquema de clasificación que aplique a toda la empresa, basado en que tan crítica y sensible es la información (esto es, pública, confidencial, secreta) de la empresa. Este esquema incluye detalles acerca de la propiedad de datos, la definición de niveles apropiados de seguridad y de controles de protección, y una breve descripción de los requerimientos de retención y destrucción de datos, además de qué tan críticos y sensibles son. Se usa como base para aplicar controles como el control de acceso, archivo o encriptación.

Tabla 3.4: Controles propuestos. Definir la arquitectura de la información (PO2).

PO3 Definir la dirección tecnológica. Descripción del proceso.

La función de servicios de información debe determinar la dirección tecnológica para dar soporte al negocio. Esto requiere de la creación de un plan de infraestructura tecnológica y de un comité de arquitectura que establezca y administre expectativas realistas y claras de lo que la tecnología puede ofrecer en términos de productos, servicios y mecanismos de aplicación. (Institute, IT Governance. 2007)

Elementos de la arquitectura:

<table>
<tr><td>Proceso:</td><td colspan="3">Definir la dirección tecnológica</td><td>PO3</td></tr>
<tr><td>Responsable(s):</td><td colspan="4">Sub-gerente</td></tr>
<tr><td>Importancia:</td><td>Media</td><td>Nivel de madurez:</td><td colspan="2">Inicial/Ad hoc (1)*</td></tr>
<tr><td colspan="5">Entrada:</td></tr>
<tr><td colspan="5">• Planes estratégicos y tácticos de TI
• Plan optimizado de sistemas del negocio y arquitectura de información
• Actualizaciones de los estándares tecnológicos
• Información de desempeño y capacidad</td></tr>
<tr><td colspan="5">Salida:</td></tr>
<tr><td colspan="5">• Oportunidades tecnológicas
• Estándares tecnológicos
• Actualizaciones rutinarias del “estado de la tecnología”
• Plan de infraestructura tecnológica
• Requerimientos de infraestructura</td></tr>
<tr><td colspan="3">Aplicaciones:</td><td colspan="2">Personal e infraestructura:</td></tr>
<tr><td colspan="3">Definición e implantación de un plan de infraestructura tecnológica, una arquitectura y estándares que tomen en cuenta y aprovechen las oportunidades tecnológicas.</td><td colspan="2">Jefes de grupos</td></tr>
<tr><td colspan="5">Objetivos de control:</td></tr>
<tr><td colspan="5">PO3.1 Planeación de la Dirección Tecnológica
PO3.2 Plan de Infraestructura Tecnológica
PO3.3 Monitoreo de tendencias y regulaciones futuras</td></tr>
</table>

Tabla 3.5: Elementos de la arquitectura. Definir la dirección tecnológica (PO3).

Modelo de madurez:

** La gerencia reconoce la necesidad de planear la infraestructura tecnológica. El desarrollo de componentes tecnológicos y la implantación de tecnologías emergentes son ad hoc y aisladas. Existe un enfoque reactivo y con foco operativo hacia la planeación de la infraestructura. La dirección tecnológica está impulsada por los planes evolutivos, con frecuencia contradictorios, del hardware, del software de sistemas y de los proveedores de software aplicativo. La comunicación del impacto potencial de los cambios en la tecnología es inconsistente.*

Controles propuestos:

Controles:
• **Política para dirigir la arquitectura y verificar el cumplimiento:** Debe establecer un foro tecnológico para brindar directrices tecnológicas, asesoría sobre los productos de la infraestructura y guías sobre la selección de la tecnología, y medir el cumplimiento de estos estándares y directrices. Este foro impulsa los estándares y las prácticas tecnológicas con base en su importancia y riesgo para el negocio y en el cumplimiento de requerimientos externos. • **Procedimiento para establecer un plan de infraestructura tecnológica equilibrado versus costos, riesgos y requerimientos:** Debe crear y mantener un plan de infraestructura tecnológica que esté de acuerdo con los planes estratégicos y tácticos de TI. El plan se basa en la dirección tecnológica e incluye acuerdos para contingencias y orientación para la adquisición de recursos tecnológicos. También toma en cuenta los cambios en el ambiente competitivo, las economías de escala en la obtención de equipo de sistemas de información, y la mejora en la interoperabilidad de las plataformas y las aplicaciones. • **Procediendo para la definición de estándares de infraestructura tecnológica:** Debe proporcionar soluciones tecnológicas consistentes, efectivas y seguras para toda la empresa, manteniendo las regulaciones establecidas en los estándares de infraestructura tecnológica basados en requerimientos de arquitectura de información.

Tabla 3.6: Controles propuestos. Definir la dirección tecnológica (PO3).

PO4 Definir los procesos, organización y relaciones de TI. Descripción del proceso.

Una organización de TI se debe definir tomando en cuenta los requerimientos de personal, funciones, rendición de cuentas, autoridad, roles, responsabilidades y supervisión. La organización está embebida en un marco de trabajo de procesos de TI que asegure la transparencia y el control, así como el involucramiento de los altos ejecutivos y la gerencia del negocio. Deben existir procesos, políticas de administración y procedimientos para todas las funciones, con atención específica en el control, el aseguramiento de la calidad, la administración de riesgos, la seguridad de la información, la propiedad de datos y de sistemas y la segregación de funciones. Para garantizar el soporte oportuno de los requerimientos del negocio, TI se debe involucrar en los procesos importantes de decisión. (Institute, IT Governance. 2007)

Elementos de la arquitectura:

Proceso:	**Definir los procesos, organización y relaciones de TI**		**PO4**
Responsable(s):	Sub-gerente		
Importancia:	Baja	Nivel de madurez:	Inicial/Ad hoc (1)*
Entrada:			
• Planes estratégicos y tácticos de TI • Políticas y procedimientos de TI y RH, matriz de habilidades de TI, descripciones de puestos • Actividades de mejoramiento de calidad • Planes de actividades para corregir riesgos relacionados con TI • Planes de acciones correctivas • Reportes de efectividad de los controles de TI • Catálogo de requerimientos legales y regulatorios relacionados con los servicios de TI • Mejoras al marco de procesos			
Salida:			
• Marco de trabajo para el proceso de TI • Dueños de sistemas documentados • Organización y relaciones de TI • Marco de procesos, roles documentados y responsabilidades de TI • Roles y responsabilidades documentados			

Aplicaciones:	Personal e infraestructura:
Establecimiento de estructuras organizacionales de TI transparentes, flexibles y responsables, y en la definición e implantación de procesos de TI con los propietarios y en la integración de roles y responsabilidades hacia los procesos de negocio y de decisión.	Alta dirección del proyecto
Objetivos de control:	
PO4.1 Marco de Trabajo de Procesos de TI PO4.2 Comité Estratégico de TI PO4.3 Comité directivo de TI PO4.4 Estructura organizacional PO4.5 Establecimiento de roles y responsabilidades PO4.6 Propiedad de datos y sistemas PO4.7 Personal Clave de TI	

Tabla 3.7: Elementos de la arquitectura. Definir los procesos, organización y relaciones de TI (PO4).

Modelo de madurez:

**Las actividades y funciones de TI son reactivas y se implantan de forma inconsistente. TI se involucra en los proyectos solo en las etapas finales. La función de TI se considera como una función de soporte, sin una perspectiva organizacional general. Existe un entendimiento explicito de la necesidad de una organización de TI; sin embargo los roles y responsabilidades no están formalizados y reforzados.*

Controles propuestos:

Controles:
• **Procedimiento para la definición del marco de trabajo de procesos de TI:** Debe contribuir a ejecutar el plan estratégico de TI. Incluyendo la estructura y relación de procesos de TI (administrando brechas y superposiciones de procesos), propiedad, medición del desempeño, mejoras, cumplimiento, metas de calidad y planes para alcanzarlas. Proporcionará integración entre los procesos que son específicos para TI, administración del portafolio de TI, procesos de negocio y procesos de cambio del negocio. El marco de trabajo de procesos de TI debe estar integrado en un sistema de administración de calidad y en un marco de trabajo de control interno. • **Procedimiento para el establecimiento de un cuerpo y una estructura organizacional apropiada:** Debe establecer una estructura organizacional de TI interna y externa que refleje las necesidades del negocio. Además implantar un proceso para revisar la estructura organizacional de TI de forma periódica para ajustar los requerimientos de personal y las estrategias internas para satisfacer los objetivos de negocio esperados y las circunstancias cambiantes. • **Política de definición de roles y responsabilidades:** Debe definir y comunicar los roles y las responsabilidades para todo el personal en la organización con respecto a los sistemas de información para permitir que ejerzan los roles y responsabilidades asignados con suficiente autoridad. Crear y actualizar periódicamente la descripción de roles. Estas descripciones deben estar alineadas con la responsabilidad y la autoridad incluyendo definiciones de habilidades y experiencia necesarias en cada posición y que serán aplicables en el uso y evaluación del desempeño.

Tabla 3.8: Controles propuestos. Definir los procesos, organización y relaciones de TI (PO4).

PO5 Comunicar las metas y la dirección de la gerencia. Descripción del proceso.

La dirección debe elaborar un marco de trabajo de control empresarial para TI, y definir y comunicar las políticas. Un programa de comunicación continua se debe implantar para articular la misión, los objetivos de servicio, las políticas y procedimientos, etc., aprobados y apoyados por la dirección. La comunicación apoya el logro de los objetivos de TI y asegura la concienciación y el entendimiento de los riesgos de negocio y de TI. El proceso debe garantizar el cumplimiento de las leyes y reglamentos relevantes. (Institute, IT Governance. 2007)

Elementos de la arquitectura:

<table>
<tr><td>Proceso:</td><td colspan="2">Comunicar las metas y la dirección de la gerencia</td><td>PO5</td></tr>
<tr><td>Responsable(s):</td><td colspan="3">Gerente</td></tr>
<tr><td>Importancia:</td><td>Media</td><td>Nivel de madurez:</td><td>Inicial/Ad hoc (1)*</td></tr>
<tr><td colspan="4">Entrada:
• Planes estratégicos y tácticos de TI, portafolios de proyectos y servicios
• Directrices de administración de riesgos relativos a TI
• Reportes sobre la efectividad de los controles de TI</td></tr>
<tr><td colspan="4">Salida:
• Marco de control empresarial para TI
• Políticas para TI</td></tr>
<tr><td colspan="2">Aplicaciones:</td><td colspan="2">Personal e infraestructura:</td></tr>
<tr><td colspan="2">Proporcionar políticas, procedimientos, directrices y otra documentación aprobada, de forma precisa y entendible y que se encuentre dentro del marco de control de TI a los interesados.</td><td colspan="2">Jefes de grupos</td></tr>
<tr><td colspan="4">Objetivos de control:
PO5.1 Ambiente de políticas y control
PO5.2 Riesgo Corporativo y Marco de Referencia de Control Interno de TI
PO5.3 Administración de Políticas para TI
PO5.4 Implantación de Políticas de TI
PO5.5 Comunicación de los Objetivos y la Dirección de TI</td></tr>
</table>

Tabla 3.9 Elementos de la arquitectura. Comunicar las metas y la dirección de la gerencia (PO5).

Modelo de madurez:

** La dirección del proyecto es reactiva al resolver los requerimientos del ambiente de control de información. Las políticas, procedimientos y estándares se elaboran y comunican de forma ad hoc de acuerdo a los temas. Los procesos de elaboración, comunicación y cumplimiento son informales e inconsistentes.*

Controles propuestos:

Controles:
• **Procedimiento de definición del marco de trabajo de control para TI**: Debe estar integrado por el marco de procesos de TI y el sistema de administración de calidad, y debe cumplir los objetivos generales de la empresa. Debe tener como meta maximizar el éxito de la entrega de valor mientras minimiza los riesgos para los activos de información por medio de medidas preventivas, la identificación oportuna de irregularidades, la limitación de pérdidas y la oportuna recuperación de activos del negocio. • **Procedimiento para la elaboración e implantación de políticas para TI:** Debe permitir la elaboración de un conjunto de políticas que apoyen la estrategia de TI. Estas políticas deben incluir la intención de las políticas, roles y responsabilidades, procesos de excepción, enfoque de cumplimiento y referencias a procedimientos, estándares y directrices. Las políticas deben incluir tópicos clave como calidad, seguridad, confidencialidad, controles internos y propiedad intelectual. Su relevancia se debe confirmar y aprobar de forma regular. La implantación debe contribuir a que las políticas de TI se implanten y se comuniquen a todo el personal relevante, y se refuercen, de tal forma que estén incluidas y sean parte integral de las operaciones empresariales. Los métodos de implantación deben resolver necesidades e implicaciones de recursos y concientización.

Tabla 3.10: Controles propuestos. Comunicar las metas y la dirección de la gerencia (PO5).

PO6 Administrar los recursos humanos de TI. Descripción del proceso.

Adquirir, mantener y motivar una fuerza de trabajo para la creación y entrega de servicios de TI para el negocio. Esto se logra siguiendo practicas definidas y aprobadas que apoyan el reclutamiento, entrenamiento, la evaluación del desempeño, la promoción y la terminación. Este proceso es crítico, ya que las personas son activos importantes, y el ambiente de gobierno y de control interno depende fuertemente de la motivación y competencia del personal. (Institute, IT Governance. 2007)

Elementos de la arquitectura:

<table>
<tr><td>Proceso:</td><td colspan="3">Administrar los recursos humanos de TI</td><td>PO6</td></tr>
<tr><td>Responsable(s):</td><td colspan="4">Gerente</td></tr>
<tr><td>Importancia:</td><td>Media</td><td>Nivel de madurez:</td><td colspan="2">Repetible (2)*</td></tr>
<tr><td colspan="5">Entrada:</td></tr>
<tr><td colspan="5">• Organización y relaciones de TI; roles y responsabilidades documentados
• Estudio de factibilidad de los requerimientos del negocio</td></tr>
<tr><td colspan="5">Salida:</td></tr>
<tr><td colspan="5">• Políticas y procedimientos de recursos humanos de TI
• Matriz de habilidades de TI
• Descripciones de puestos
• Aptitudes y habilidades de los usuarios, incluyendo el entrenamiento individual
• Requerimientos específicos de entrenamiento
• Roles y responsabilidades</td></tr>
<tr><td colspan="3">Aplicaciones:</td><td colspan="2">Personal e infraestructura:</td></tr>
<tr><td colspan="3">Contratación y entrenamiento del personal, la motivación por medio de planes de carrera claros, la asignación de roles que correspondan a las habilidades, el establecimiento de procesos de revisión definidos, la creación de descripción de puestos y el aseguramiento de la conciencia de la dependencia sobre los individuos.</td><td colspan="2">Jefes de grupos</td></tr>
</table>

Objetivos de control:
PO6.1 Reclutamiento y Retención del Personal
PO6.2 Competencias del personal
PO6.3 Asignación de Roles
PO6.4 Entrenamiento del Personal de TI
PO6.5 Dependencia Sobre los Individuos
PO6.6 Procedimientos de Investigación del Personal
PO6.7 Evaluación del Desempeño del Empleado

Tabla 3.11: Elementos de la arquitectura. Administrar los recursos humanos de TI (PO6).

Modelo de madurez:

** Existe un enfoque táctico para contratar y administrar al personal de TI, dirigido por necesidades específicas de proyectos, en lugar de hacerlo con base en un equilibrio entendido de disponibilidad interna y externa de personal calificado. Se imparte entrenamiento informal al personal nuevo, quienes después reciben entrenamiento según sea necesario.*

Controles propuestos:

Controles:
• **Política de administración de recursos humanos:** Debe establecer un enfoque de administración de roles, donde se vean las responsabilidades de los mismos dentro de los proyectos, así como los mecanismos por medio de los cuales pueden satisfacer esas responsabilidades (tales como reportes y revisiones por etapa). • **Procedimiento para la administración de recursos humanos:** Debe establecer los roles adecuados dentro de los proyectos que se encarguen de la planeación y organización de los mismos y principalmente del monitoreo y control de los medios tecnológicos para asegurar un dominio de los recursos que poseen dichos proyectos. Saber además con cuanto personal se cuenta y tenerlo correctamente organizado.

Tabla 3.12: Controles propuestos.

PO7 Administrar la calidad. Descripción del proceso.

Se debe elaborar y mantener un sistema de administración de calidad, el cual incluya procesos y estándares probados de desarrollo y de adquisición. Esto se facilita por medio de la planeación, implantación y mantenimiento del sistema de administración de calidad, proporcionando requerimientos, procedimientos y políticas claras de calidad. (Institute, IT Governance. 2007)

Elementos de la arquitectura:

<table>
<tr><td>Proceso:</td><td colspan="3">Administrar la calidad</td><td>PO7</td></tr>
<tr><td>Responsable(s):</td><td colspan="4">Jefe del grupo de calidad (Administrador de la calidad)</td></tr>
<tr><td>Importancia:</td><td>Media</td><td>Nivel de madurez:</td><td colspan="2">Repetible (2)*</td></tr>
<tr><td colspan="5">Entrada:</td></tr>
<tr><td colspan="5">• Plan estratégico de TI
• Planes detallados de proyectos
• Planes de acciones correctivas</td></tr>
<tr><td colspan="5">Salida:</td></tr>
<tr><td colspan="5">• Estándares de adquisición
• Estándares de desarrollo
• Requerimientos de estándares y métricas de calidad
• Medidas para la mejora de la calidad</td></tr>
<tr><td colspan="3">Aplicaciones:</td><td colspan="2">Personal e infraestructura:</td></tr>
<tr><td colspan="3">La definición de un sistema de administración de calidad (QMS, por sus siglas en inglés), el monitoreo continuo del desempeño contra los objetivos predefinidos y la implantación de un programa de mejora continua de servicios de TI.</td><td colspan="2">Revisores de calidad</td></tr>
</table>

Objetivos de control:
PO7.1 Sistema de Administración de Calidad
PO7.2 Estándares y Prácticas de Calidad
PO7.3 Estándares de desarrollo y de Adquisición
PO7.4 Enfoque en el Cliente de TI
PO7.5 Mejora Continua
PO7.6 Medición, Monitoreo y Revisión de la Calidad

Tabla 3.13: Elementos de la arquitectura. Administrar la calidad (PO7).

Modelo de madurez:

** Se establece un programa para definir y monitorear las actividades de QMS dentro de TI. Las actividades de QMS que ocurren están enfocadas en iniciativas orientadas a procesos y proyectos, no a procesos de toda la organización.*

Controles propuestos:

Controles:
• **Procedimiento de definición de estándares y prácticas de calidad:** Debe contribuir a identificar y mantener estándares, procedimientos y prácticas para los procesos clave de TI para orientar a la organización hacia el cumplimiento del QMS. Usar las mejores prácticas de la industria como referencia al mejorar y adaptar las prácticas de calidad de la organización. • **Procedimiento para el monitoreo y revisión interna y externa del desempeño contra los estándares y prácticas de calidad definidas:** Debe definir, planear e implantar mediciones para monitorear el cumplimiento continuo del QMS, así como el valor que QMS proporciona. La medición, el monitoreo y el registro de la información deben ser usados por el dueño del proceso para tomar las medidas correctivas y preventivas apropiadas.

Tabla 3.14 Controles propuestos. Administrar la calidad (PO7).

PO8 Evaluar y administrar los riesgos de TI. Descripción del proceso.

Crear y dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar. Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable. (Institute, IT Governance. 2007)

Elementos de la arquitectura:

<table>
<tr><td>Proceso:</td><td colspan="2">Evaluar y administrar los riesgos de TI</td><td>PO8</td></tr>
<tr><td>Responsable(s):</td><td colspan="3">Sub-gerente</td></tr>
<tr><td>Importancia:</td><td>Alta</td><td>Nivel de madurez:</td><td>Inicial/Ad hoc (1)*</td></tr>
<tr><td colspan="4">Entrada:</td></tr>
<tr><td colspan="4">• Planes estratégicos y tácticos de TI, portafolio de servicios de TI
• Plan de administración de riesgos de proyectos
• Riesgos de proveedores
• Resultados de pruebas de contingencia
• Amenazas y vulnerabilidades de seguridad
• Tendencia y eventos de riesgos históricos
• Apetito empresarial de riesgos de TI</td></tr>
<tr><td colspan="4">Salida:</td></tr>
<tr><td colspan="4">• Evaluación de riesgos
• Reporte de riesgos
• Directrices de administración de riesgos relacionados con TI
• Planes de acciones correctivas para riesgos relacionados con TI</td></tr>
<tr><td colspan="2">Aplicaciones:</td><td colspan="2">Personal e infraestructura:</td></tr>
<tr><td colspan="2">Elaboración de un marco de trabajo de administración de riesgos el cual está integrado en los marcos gerenciales de riesgo operacional, evaluación de riesgos, mitigación del riesgo y comunicación de riesgos residuales.</td><td colspan="2">Jefes de grupos</td></tr>
</table>

Objetivos de control:
PO8.1 Marco de Trabajo de Administración de Riesgos
PO8.2 Establecimiento del Contexto del Riesgo
PO8.3 Identificación de Eventos
PO8.4 Evaluación de Riesgos de TI
PO8.5 Respuesta a los Riesgos
PO8.6 Mantenimiento y Monitoreo de un Plan de Acción de Riesgos

Tabla 3.15: Elementos de la arquitectura. Evaluar y administrar los riesgos de TI (PO8).

Modelo de madurez:

** Los riesgos de TI se toman en cuenta de manera ad hoc. Se realizan evaluaciones informales de riesgos según lo determine cada proyecto. En algunas ocasiones se identifican evaluaciones de riesgos en un plan de proyectos. Los riesgos específicos relacionados con TI tales como seguridad, disponibilidad e integridad se toman en cuenta ocasionalmente proyecto por proyecto. Los riesgos relativos a TI que afectan las operaciones del día con día, son rara vez discutidas en reuniones gerenciales. Cuando se toman en cuenta los riesgos, la mitigación es inconsistente. Existe un entendimiento emergente de que los riesgos de TI son importantes y necesitan ser considerados.*

Controles propuestos:

Controles:
• **Procedimiento para la alineación de la administración de riesgos de TI y del negocio:** Debe integrar el gobierno, la administración de riesgos y el marco de control de TI, al marco de trabajo de administración de riesgos de la organización. Esto incluye la alineación con el apetito de riesgo y con el nivel de tolerancia al riesgo de la organización. • **Política de evaluaciones de riesgo:** Debe evaluar de forma recurrente la posibilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La posibilidad e impacto asociados a los riesgos inherentes y residuales se debe determinar de forma individual, por categoría y con base en el portafolio. • **Procedimiento para el mantenimiento y monitoreo de un plan de acción de riesgos:** Debe permitir y asignar prioridades y planear las actividades de control a todos los niveles para implantar las respuestas a los riesgos, identificadas como necesarias, beneficios y la responsabilidad de la ejecución. Buscar la aprobación para las acciones recomendadas y la aceptación de cualquier riesgo residual, y asegurarse de que las acciones comprometidas son propiedad del dueño (s) de los procesos afectados. Monitorear la ejecución de los planes y reportar cualquier desviación a la alta dirección**.**

Tabla 3.16: Controles propuestos. Evaluar y administrar los riesgos de TI (PO8).

PO9 Administrar proyectos. Descripción del proceso.

Establecer un marco de trabajo de administración de programas y proyectos para la administración de todos los proyectos de TI establecidos. El marco de trabajo debe garantizar la correcta asignación de prioridades y la coordinación de todos los proyectos. Este enfoque reduce el riesgo de costos inesperados y de cancelación de proyectos, mejora la comunicación y el involucramiento del negocio y de los usuarios finales, asegura el valor y la calidad de los entregables de los proyectos, y maximiza la contribución a los programas de inversión facilitados por TI. (Institute, IT Governance. 2007)

Elementos de la arquitectura:

<table>
<tr><td>Proceso:</td><td colspan="2">Administrar proyectos</td><td>PO9</td></tr>
<tr><td>Responsable(s):</td><td colspan="3">Alta dirección del proyecto</td></tr>
<tr><td>Importancia:</td><td>Alta</td><td>Nivel de madurez:</td><td>Repetible (2)*</td></tr>
<tr><td colspan="4">Entrada:
• Portafolio de proyectos
• Portafolio de proyectos de TI actualizado
• Matriz de habilidades de TI
• Estándares de desarrollo
• Revisión post-implantación</td></tr>
<tr><td colspan="4">Salida:
• Reportes de desempeño del proyecto
• Plan de administración de riesgos de proyecto
• Directrices de administración del proyecto
• Planes detallados del proyecto
• Portafolio actualizado de proyectos de TI</td></tr>
<tr><td colspan="2">Aplicaciones:</td><td colspan="2">Personal e infraestructura:</td></tr>
<tr><td colspan="2">Programa y 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.</td><td colspan="2">Alta dirección del proyecto</td></tr>
</table>

Objetivos de control:
PO9.1 Marco de Trabajo para la Administración de Programas
PO9.2 Marco de Trabajo para la Administración de Proyectos
PO9.3 Enfoque de Administración de Proyectos
PO9.4 Compromiso de los interesados.
PO9.5 Declaración de Alcance del Proyecto
PO9.6 Inicio de las Fases del Proyecto
PO9.7 Plan Integrado del Proyecto
PO9.8 Recursos del Proyecto
PO9.9 Administración de Riesgos del Proyecto
PO9.10 Plan de Calidad del Proyecto
PO9.11 Control de Cambios del Proyecto
PO9.12 Planeación del Proyecto y Métodos de Aseguramiento

Tabla 3.17: Elementos de la arquitectura. Administrar proyectos (PO9).

Modelo de madurez:

**La alta dirección ha obtenido y comunicado la conciencia de la necesidad de la administración de los proyectos de TI. La organización está en proceso de desarrollar y utilizar algunas técnicas y métodos proyecto por proyecto. Los proyectos de TI han definido objetivos técnicos y de negocio de manera informal. Hay participación limitada de los interesados en la administración de los proyectos de TI. Las directrices iniciales se han elaborado para muchos aspectos de la administración de proyectos. La aplicación a proyectos de las directrices administrativas se deja a discreción de cada gerente de proyecto.*

Controles propuestos:

Controles:
• **Política de administración de proyectos:** Debe establecer un enfoque de administración de proyectos que corresponda al tamaño, complejidad y requerimientos regulatorios de cada proyecto. La estructura de gobierno de proyectos puede incluir los roles, las responsabilidades y la rendición de cuentas del patrocinador del programa, patrocinadores del proyecto, comité de dirección, oficina de proyectos, y gerente del proyecto, así como los mecanismos por medio de los cuales pueden satisfacer esas responsabilidades (tales como reportes y revisiones por etapa). Asegurarse que todos los proyectos de TI cuenten con patrocinadores con la suficiente autoridad para apropiarse de la ejecución del proyecto dentro del programa estratégico global. • **Procedimiento para la administración de riesgos del proyecto:** Debe eliminar o minimizar los riesgos específicos asociados con los proyectos individuales por medio de un proceso sistemático de planeación, identificación, análisis, respuestas, monitoreo y control de las áreas o eventos que tengan el potencial de ocasionar cambios no deseados. Los riesgos afrontados por el proceso de administración de proyectos y el producto entregable del proyecto se deben establecer y registrar de forma central. • **Política de planeación del proyecto y métodos de aseguramiento:** Debe identificar las tareas de aseguramiento requerido para apoyar la acreditación de sistemas nuevos o modificados durante la planeación del proyecto e incluirlos en el plan integrado. Las tareas deben proporcionar la seguridad de que los controles internos y las características de seguridad satisfagan los requerimientos definidos.

Tabla 3.18: Controles propuestos. Administrar proyectos (PO9).

3.4 Monitorear y evaluar

ME1 Monitorear y evaluar el desempeño de TI. Descripción del proceso.

Una efectiva administración del desempeño de TI requiere un proceso de monitoreo. El proceso incluye la definición de indicadores de desempeño relevante, reportes sistemáticos y oportunos de desempeño y tomar medidas expeditas cuando existan desviaciones. El monitoreo se requiere para garantizar que las cosas correctas se hagan y que estén de acuerdo con el conjunto de direcciones y políticas. (Institute, IT Governance. 2007)

Elementos de la arquitectura:

<table>
<tr><td>Proceso:</td><td colspan="2">Monitorear y evaluar el desempeño de TI</td><td>ME1</td></tr>
<tr><td>Responsable(s):</td><td colspan="3">Sub-gerente</td></tr>
<tr><td>Importancia:</td><td>Alta</td><td>Nivel de madurez:</td><td>Inicial/Ad hoc (1)*</td></tr>
<tr><td colspan="4">Entrada:</td></tr>
<tr><td colspan="4">• Reportes de costo-beneficio
• Reportes de desempeño del proyecto
• Reportes del estatus de los cambios
• Reportes de desempeño del proceso
• Reportes de satisfacción del usuario
• Reportes de la efectividad de los controles de TI
• Reportes sobre el cumplimiento de las actividades de TI respecto a requerimientos legales y regulatorios externos
• Reportes sobre el estatus del gobierno de TI</td></tr>
<tr><td colspan="4">Salida:</td></tr>
<tr><td colspan="4">• Indicadores de desempeño a planeación de TI
• Planes de acciones correctivas
• Tendencias y eventos de riesgos históricos
• Reporte de desempeño del proceso</td></tr>
<tr><td colspan="2">Aplicaciones:</td><td colspan="2">Personal e infraestructura:</td></tr>
<tr><td colspan="2">Monitorear y reportar las métricas del proceso e identificar e implantar acciones de mejoramiento del desempeño.</td><td colspan="2">Jefes de grupos</td></tr>
</table>

Objetivos de control:
ME1.1 Enfoque del Monitoreo
ME1.2 Definición y Recolección de Datos de Monitoreo
ME1.3 Método de Monitoreo
ME1.4 Evaluación del Desempeño
ME1.5 Reportes al Consejo Directivo y a Ejecutivos
ME1.6 Acciones Correctivas

Tabla 3.19: Elementos de la arquitectura. Monitorear y evaluar el desempeño de TI (ME1).

Modelo de madurez:

** La gerencia reconoce una necesidad de recolectar y evaluar información sobre los procesos de monitoreo. No se han identificado procesos estándar de recolección y evaluación. El monitoreo se implanta y las métricas se seleccionan de acuerdo a cada caso, de acuerdo a las necesidades de proyectos y procesos de TI específicos.*

Controles propuestos:

Controles:
• **Procedimiento para la definición y recolección de datos de monitoreo:** Debe garantizar que la gerencia de TI, trabajando en conjunto con el negocio, defina un conjunto balanceado de objetivos, mediciones, metas y comparaciones de desempeño y que estas se encuentren acordadas formalmente con el negocio y otros interesados relevantes. Los indicadores de desempeño deberán incluir: 1. Desempeño contra el plan estratégico del negocio y de TI. 2. Riesgo y cumplimiento de las regulaciones. 3. Satisfacción del usuario interno y externo. 4. Procesos clave de TI que incluyan desarrollo y entrega del servicio. • **Política de realización de medidas correctivas:** Debe permitir identificar e iniciar medidas correctivas basadas en el monitoreo del desempeño, evaluación y reportes. Esto incluye el seguimiento de todo el monitoreo, de los reportes y de las evaluaciones con: 1. Revisión, negociación y establecimiento de respuestas administrativas. 2. Asignación de responsabilidades por la corrección.

Tabla 3.20: Controles propuestos. Monitorear y evaluar el desempeño de TI (ME1).

ME2 Monitorear y evaluar el control interno. Descripción del proceso.

Establecer un programa de control interno efectivo para TI requiere un proceso bien definido de monitoreo. Este proceso incluye el monitoreo y el reporte de las excepciones de control, resultados de las auto-evaluaciones y revisiones por parte de terceros. Un beneficio clave del monitoreo del control interno es proporcionar seguridad respecto a las operaciones eficientes y efectivas y el cumplimientos de las leyes y regulaciones aplicables. (Institute, IT Governance. 2007)

Elementos de la arquitectura:

<table>
<tr><td>Proceso:</td><td colspan="2">Monitorear y evaluar el control interno</td><td>ME2</td></tr>
<tr><td>Responsable(s):</td><td colspan="3">Sub-gerente</td></tr>
<tr><td>Importancia:</td><td>Media</td><td>Nivel de madurez:</td><td>Inicial/Ad hoc (1)*</td></tr>
<tr><td colspan="4">Entrada:</td></tr>
<tr><td colspan="4">• Monitoreo de Controles Internos
• Reporte de desempeño de procesos</td></tr>
<tr><td colspan="4">Salida:</td></tr>
<tr><td colspan="4">• Reporte sobre la efectividad de los controles de TI</td></tr>
<tr><td colspan="2">Aplicaciones:</td><td colspan="2">Personal e infraestructura:</td></tr>
<tr><td colspan="2">El monitoreo de los procesos de control interno para las actividades relacionadas con TI e identificar las acciones de mejoramiento.</td><td colspan="2">Jefes de grupos</td></tr>
<tr><td colspan="4">Objetivos de control:</td></tr>
<tr><td colspan="4">ME2.1 Monitoreo del Marco de Trabajo de Control Interno
ME2.2 Revisiones de Auditoría
ME2.3 Excepciones de Control
ME2.4 Control de Auto Evaluación
ME2.5 Aseguramiento del Control Interno
ME2.6 Control Interno para Terceros
ME2.7 Acciones Correctivas</td></tr>
</table>

Tabla 3.21: Elementos de la arquitectura. Monitorear y evaluar el control interno (ME2).

Modelo de madurez:

** La gerencia reconoce la necesidad de administrar y asegurar el control de TI de forma regular. La experiencia individual para evaluar la suficiencia del control interno se aplica de forma ad hoc. La gerencia de TI no ha asignado de manera formal las responsabilidades para monitorear la efectividad de los controles internos. Las evaluaciones de control interno de TI se realizan como parte de las auditorías financieras tradicionales, con metodologías y habilidades que no reflejan las necesidades de la función de los servicios de información.*

Controles propuestos:

Controles:
• **Procedimiento para el monitoreo del marco de trabajo de control interno:** Debe monitorear de forma continua el ambiente de control y el marco de control de TI. Se debe realizar la evaluación usando mejores prácticas de la industria y se deberá utilizar benchmarking para mejorar el ambiente y el marco de trabajo de control de TI. • **Procedimiento para reportar las excepciones de control a la gerencia:** Debe registrar la información referente a todas las excepciones de control y garantizar que esto conduzca al análisis de las causas subyacentes y a la toma de acciones correctivas. La gerencia debería decidir cuáles excepciones se deberían comunicar al individuo responsable de la función y cuáles excepciones deberían ser escaladas. La gerencia también es responsable de informar a las partes afectadas. • **Procedimiento para la realización de acciones correctivas:** Debe identificar e iniciar medidas correctivas basadas en las evaluaciones y en los reportes de control. Esto incluye el seguimiento de todas las evaluaciones y los reportes con: 1. La revisión, negociación y establecimiento de respuestas administrativas. 2. La asignación de responsabilidades para corrección (puede incluir la aceptación de los riesgos). 3. El rastreo de los resultados de las acciones comprometidas.

Tabla 3.22: Controles propuestos. Monitorear y evaluar el control interno (ME2).

ME3 Garantizar el cumplimiento regulatorio. Descripción del proceso.

Una supervisión efectiva del cumplimiento requiere del establecimiento de un proceso de revisión para garantizar el cumplimiento de las leyes, regulaciones y requerimientos contractuales. Este proceso incluye la identificación de requerimientos de cumplimiento, optimizando y evaluando la respuesta, obteniendo aseguramiento de que los requerimientos se han cumplido y, finalmente integrando los reportes de cumplimiento de TI con el resto del negocio. (Institute, IT Governance. 2007)

Elementos de la arquitectura:

<table>
<tr><td>Proceso:</td><td colspan="2">Garantizar el cumplimiento regulatorio</td><td>ME3</td></tr>
<tr><td>Responsable(s):</td><td colspan="3">Gerente</td></tr>
<tr><td>Importancia:</td><td>Baja</td><td>Nivel de madurez:</td><td>Inicial/Ad hoc (1)*</td></tr>
<tr><td colspan="4">Entrada:</td></tr>
<tr><td colspan="4">• Requerimientos de cumplimiento legal y regulatorio
• Políticas de TI</td></tr>
<tr><td colspan="4">Salida:</td></tr>
<tr><td colspan="4">• Catálogo de requerimientos legales y regulatorios relacionados con la prestación del servicio de TI
• Reporte sobre el cumplimiento de las actividades de TI con los requerimientos externos legales y regulatorios</td></tr>
<tr><td colspan="2">Aplicaciones:</td><td colspan="2">Personal e infraestructura:</td></tr>
<tr><td colspan="2">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.</td><td colspan="2">Alta dirección del proyecto</td></tr>
<tr><td colspan="4">Objetivos de control:</td></tr>
<tr><td colspan="4">ME3.1 Identificar los Requerimientos de las Leyes, Regulaciones y Cumplimientos Contractuales
ME3.2 Optimizar la Respuesta a Requerimientos Externos
ME3.3 Evaluación del Cumplimiento con Requerimientos Externos
ME3.4 Aseguramiento Positivo del Cumplimiento
ME3.5 Reportes Integrados</td></tr>
</table>

Tabla 3.23: Elementos de la arquitectura. Garantizar el cumplimiento regulatorio (ME3).

Modelo de madurez:

** Existe conciencia de los requisitos de cumplimiento regulatorio, contractual y legal que tienen impacto en la organización. Se siguen procesos informales para mantener el cumplimiento, pero solo si la necesidad surge en nuevos proyectos o como respuesta a auditorías o revisiones.*

Controles propuestos:

Controles:
• **Procedimiento para la identificación de los requisitos legales y regulatorios relacionados con la TI:** Debe definir e implantar un proceso para garantizar la identificación oportuna de requerimientos locales e internacionales legales, contractuales, de políticas y regulatorios, relacionados con la información, con la prestación de servicios de información – incluyendo servicios de terceros – y con la función, procesos e infraestructura de TI. Tomar en cuenta las leyes y reglamentos de comercio electrónico, flujo de datos, privacidad, controles internos, reportes financieros, reglamentos específicos de la industria, propiedad intelectual y derechos de autor, además de salud y seguridad. • **Procedimiento para la evaluación del impacto de los requisitos regulatorios:** Debe permitir la evaluación de forma eficiente el cumplimiento de las políticas, estándares y procedimientos de TI, incluyendo los requerimientos legales y regulatorios, con base en la supervisión del gobierno de la gerencia de TI y del negocio y la operación de los controles internos.

Tabla 3.24: Controles propuestos. Garantizar el cumplimiento regulatorio (ME3).

ME4 Proporcionar gobierno de TI. Descripción del proceso.

El establecimiento de un marco de trabajo de gobierno efectivo, incluye la definición de estructuras, procesos, liderazgo, roles y responsabilidades organizacionales para garantizar así que las inversiones empresariales en TI estén alineadas y de acuerdo con las estrategias y objetivos empresariales. (Institute, IT Governance. 2007)

Elementos de la arquitectura:

<table>
<tr><td>Proceso:</td><td colspan="2">Proporcionar gobierno de TI</td><td>ME4</td></tr>
<tr><td>Responsable(s):</td><td colspan="3">Gerente</td></tr>
<tr><td>Importancia:</td><td>Baja</td><td>Nivel de madurez:</td><td>Inicial/Ad hoc (1)*</td></tr>
<tr><td colspan="4">Entrada:</td></tr>
<tr><td colspan="4">• Marco de trabajo del proceso de TI
• Reportes de costo/beneficio
• Evaluación y reportes de riesgo
• Reportar la efectividad de los controles de TI
• Catálogo de requisitos legales y regulatorios relacionados con la prestación de servicios de TI</td></tr>
<tr><td colspan="4">Salida:</td></tr>
<tr><td colspan="4">• Mejoras al marco de trabajo de los procesos
• Reportar el estatus del gobierno de TI
• Resultados de negocio esperados de las inversiones de TI
• Dirección estratégica empresarial para TI
• Apetito empresarial de riesgos de TI</td></tr>
<tr><td colspan="2">Aplicaciones:</td><td colspan="2">Personal e infraestructura:</td></tr>
<tr><td colspan="2">Elaboración de informes para el consejo de dirección sobre la estrategia, el desempeño y los riesgos de TI y responder a los requerimientos de gobierno de acuerdo a las directrices del consejo de dirección.</td><td colspan="2">Sub-gerente</td></tr>
</table>

Objetivos de control:
ME4.1 Establecimiento de un Marco de Gobierno de TI
ME4.2 Alineamiento Estratégico
ME4.3 Entrega de Valor
ME4.4 Administración de Recursos
ME4.5 Administración de Riesgos
ME4.6 Medición del Desempeño
ME4.7 Aseguramiento Independiente

Tabla 3.25: Elementos de la arquitectura. Proporcionar gobierno de TI (ME4).

Modelo de madurez:

** Se reconoce que el tema del gobierno de TI existe y que debe ser resuelto. Existen enfoques ad hoc aplicados individualmente o caso por caso. El enfoque de la gerencia es reactivo y solamente existe una comunicación esporádica e inconsistente sobre los temas y los enfoques para resolverlos. La gerencia solo cuenta con una indicación aproximada de cómo TI contribuye al desempeño del negocio. La gerencia solo responde de forma reactiva a los incidentes que hayan causado pérdidas o vergüenza a la organización.*

Controles propuestos:

Controles:
• **Procedimiento para establecer un marco de trabajo de gobierno para TI:** Debe permitir el trabajo con el consejo de dirección para definir y establecer un marco de trabajo para el gobierno de TI, incluyendo liderazgo, procesos, roles y responsabilidades, requerimientos de información, y estructuras organizacionales para garantizar que los programas de inversión habilitados por TI de la empresa ofrezcan y estén alineados con las estrategias y objetivos empresariales. • **Política de aseguramiento independiente**: Debe garantizar que la organización establezca y mantenga una función competente y que cuente con el personal adecuado y/o busque servicios de aseguramiento externo para proporcionar al consejo directivo aseguramiento independiente y oportuno sobre el cumplimiento que tiene TI respecto a sus políticas, estándares y procedimientos, así como con las prácticas generalmente aceptadas.

Tabla 3.26: Controles propuestos. Proporcionar gobierno de TI (ME4).

CONCLUSIONES

Una vez concluido el estudio de los procesos productivos de la facultad 15, se realizó una estrategia de implementación del modelo COBIT en base a las necesidades que existen en los proyectos de la facultad, lo cual se llevará a cabo en dos de los proyectos de la misma para llegar a obtener un modelo de madurez optimizado.

Para la realización de dicha estrategia se tuvo en cuenta lo que plantea el modelo COBIT en cuanto a los requerimientos del negocio para TI, así como las metas de TI alineadas y los objetivos de control establecidos para los procesos de los dominios analizados, identificando dentro de los mismos los procesos que se manifestaban en el proceso productivo de la facultad 15.

De forma general los resultados se obtendrán en dependencia de lo que se aplique de la estrategia planteada, y de aplicarse detalladamente por lo que describe dicha estrategia, se llegará al nivel que se pretende.

RECOMENDACIONES

- Profundizar en el estudio del modelo COBIT en otras facultades para una futura implementación de esta estrategia a nivel de universidad.

- Desarrollar dentro de la estrategia los cuatro dominios que propone el modelo COBIT, llegando a identificar todos los procesos que se ponen de manifiesto en el proceso productivo de la universidad, con vistas a incrementar la eficiencia, calidad y aceptación de los proyectos tanto nacionales, como internacionales.

BIBLIOGRAFIA CITADA

[1] ISACA. *Aligning COBIT, ITIL and ISO 17799 for Business Benefit*. ISACA, 2007. Disponible en: http://www.isaca.org/Content/ContentGroups/Research1/Deliverables/AligningCOBIT,ITIL.pdf

[2] IT Governance Institute. *COBIT. 4ta edición*. ITGI, 2005. p. ISBN 1-933284-37-4

[3] ISACA. *COBIT Objetivos de Control. 3a edición*. ISACA, 2000. p. ISBN 1-893209-99-7

[4] ISACA. *COBIT Edición 4.0*. ISACA. [En línea] 2005. http://www.isaca.org/Template.cfm?Section=Downloads5&CONTENTID=31413. ISBN 1-933284-37-4.

[5] IRCA. *¿Qué es la norma ISO 20000:2005?: Inform, IRCA, Registro Internacional de Auditores Certificados*, 2006. 12.

[6] Vandama, Nancy y Lescay, Milagros. *Implementación del modelo COBIT en el desarrollo de las Auditorías Informáticas*. La Habana: s.n., 2002. Simposio Latinoamericano y del Caribe, La Educación, La Ciencia y la Cultura en la Sociedad de la Información, SimpLAC 2002.

[7] ISO/IEC 20000-1:2005. *ISO/IEC*, 2007. Disponible en: http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=41332

[8] ISO/IEC 20000-2:2005. *ISO/IEC*, 2007. Disponible en: http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=41333

[9] ORTÍZ, S. G. C. and D. F. J. P. MARTÍNEZ. *ITIL: servicios de tecnologías de información*, 2005. [2007]. Disponible en: http://www.enterate.unam.mx/Articulos/2005/noviem/itil.htm

[10] VANDAMA, N. and M. LESCAY. *Implementación del modelo COBIT en el desarrollo de las Auditorías Informáticas*. Simposio Latinoamericano y del Caribe, La Educación, La Ciencia y la Cultura en la Sociedad de la Información, SimpLAC 2002 La Habana, Cuba, UNESCO, 2002.

[11] Pressman, Roger S. / Madrid, McGraw-Hill, 2002, ed. 5ta. Ed. Disponible en: http://bibliodoc.uci.cu/pdf/reg02689.pdf.

[12] Microsoft Corporation. 2007. Microsoft Corporation. Disponible en: http://www.microsoft.com/soa/default.aspx.

[13] IT Governance Institute. 2007. *COBIT 4.1*, Rolling Meadows, EE.UU. Disponible en: http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders1/COBIT6/Obtain_COBIT/cobiT4.1spanish.pdf

[14] IT Governance Institute. **ITGI**. [En línea] noviembre de 2005. [Citado el: 6 de abril de 2010.] Disponible en: http://www.itgi.org.

BIBLIOGRAFIA CONSULTADA

[1] Chuo Audit Corporation. August 1994. *Japan Information Systems Auditing Standards: Information System Auditing Standard of Japan*. Tokyo: s.n., August 1994.

[2] CISA Job Analysis. 1994. *Certified Information Systems Auditor Job Analysis Study*. Rolling Meadows, IL: s.n., 1994.

[3] Committee of Sponsoring Organizations of the Treadway Commission. COSO. 1994. *Internal Control – Integrated Framework. 2 Vols, American Institute of Certified Accountants*. New Jersey: s.n., 1994.

[4] Coopers & Lybrand, SAP R/3. 1997. *C & L Audit Guide. Its Use, Control and Audit*. New York, NY: s.n., 1997.

[5] EDP Auditors Foundation (now the Information Systems Audit and Control. 1992. *Computerized Information Systems (CIS) Audit Manual Foundation)*. Rolling Meadows, IL: s.n., 1992.

[6] EDP Auditors Foundation (now the Information Systems Audit and Control Foundation). 1992. *Control Objectives Controls in an Information Systems Environment: Control Guidelines and Audit Procedures, Fourth Edition*. Rolling Meadows, IL: s.n., 1992.

[7] Institute of Internal Auditors Research Foundation. 1991, 1994. *IIA, SAC Systems Audibility and Control. Systems Audibility and Control. .* Alamonte Springs, FL: s.n., 1991, 1994.

[8] International Organization for Standardization (ISO) Technical Committee on Information Technology Security. 1998. *ISO IEC JTC1/SC27 Information Technology - Security*. Switzerland: s.n., 1998.

[9] International Organization for Standardization (ISO) Technical Committee on Software Process Assessment. 1992. *An Assessment Model and Guidance Indicator*. Switzerland: s.n., 1992.

[10] IT Governance Institute. 2005. *COBIT 4.0 Control Objectives, Management Guidelines and Maturity Models, Primera Edición*. Estados Unidos de América: s.n., 2005.

[11] IT Governance Institute. 2005. *COBIT Mapping, Segunda Edición*. Estados Unidos de América: s.n., 2005.

[12] National Institute of Standards and Technology, U.S. Department of Commerce. 1995. *An Introduction to Computer Security: The NIST Handbook*. Washington, DC: s.n., 1995.

[13] National Institute of Standards and Technology, U.S. Department of Commerce. 1988. *Guide for Auditing for Controls and Security, A System Development Life Cycle Approach*. Washington, DC: NBS Special Publication, 1988. 500-153.

[14] Organization for Economic Co-operation and Development. OECD Guidelines. 1992. *Guidelines for the Security of Information*. Paris: s.n., 1992.

[15] The Central Computer and Telecommunications Agency (CCTA). 1989. *ITIL IT Management Practices: Information Technology Infrastructure Library. Practices and guidelines*. London: s.n., 1989.

[16] U.S. General Accounting Office. 1994. *Government Auditing Standards*. Washington, DC: s.n., 1994.

[17] U.S. General Accounting Office. 1983. *Standards for Internal Control in the U.S. Federal Government*. Washington, DC: s.n., 1983.

[18] Instituto de Auditores Internos de España (IAIE). Nº. 78, 2006. *Auditoría interna: publicación periódica del Instituto de Auditores Internos de España*. España: s.n., Nº. 78, 2006. ISSN 1137-3911.

[19] COSO. 2004. *Administración de Riesgos Empresarial - Marco de Trabajo Integrado.* 2004.

[20] COSO. 1994. *Control Interno - Marco de Trabajo Integrado.* 1994.

[21] Foro de Seguridad de Información (ISF). 2004. *El estándar de buenas prácticas para la seguridad de la información.* 2004.

[22] Instituto de Gestión de Proyectos (PMI). 2004. *Guía para el Cuerpo de Conocimiento de Gestión de Proyectos (PMBOK).* 2004.

[23] Instituto de Ingeniería de Software (SEI). 2003. *SEI Modelo de madurez de la capacidad (CMM).* 2003.

[24] ISACA. 2006. *Manual de revisión, CISA.* USA : s.n., 2006.

[25] ITGI. 2006. *Objetivos de Control de TI para Sarbanes-Oxley: El rol de TI en el diseño e implementación de Controles Internos.* USA : s.n., 2006.

[26] Oficina de Comercio Gubernamental (OGC). 1999 - 2004. *Biblioteca de Infraestructura de TI (ITIL).* 1999 - 2004.

[27] Cepeda, Gustavo. 1997. *Auditoría y Control Interno, Segunda Edición.* Colombia : s.n., 1997. págs. Páginas 208-224, 227-232.

[28] R. Bernal Montañes y Simón O. Coltell. 1986. *Auditoría de los sistemas de información.* España : Servicios de Publicaciones, 1986.

[29] Comité Directivo de COBIT e ISACA. 1998. *Directrices de Auditoría, Segunda Edición.* EE.UU : s.n., 1998. págs. Páginas 8-18, 23-27, 70-73. Disponible en: www.isaca.org.

[30] Comité Directivo de COBIT y El IT Governance Institute. 2002. *Objetivos de Control, Tercera Edición.* EE.UU : s.n., 2002. págs. Páginas 5-20, 52-54. Disponible en: www.isaca.org, www.ltgovernance.org.

[31] Comité Internacional de Prácticas de Auditoría. 1995. *Normas Internacionales de Auditoría.* México : s.n., 1995. ISBN 968 – 6964-27-4.

[32] Connell, Steve Mc. 1996. *Desarrollo y Gestión de Proyectos Informáticos: Gestión de Riesgos, Primera Edición.* España : s.n., 1996.

[33] COOPERS & LYBRAND. 1997. *Los nuevos conceptos de Control Interno (Informe COSO).* Madrid, España : s.n., 1997.

[34] Pinilla Forero, José Dagoberto. 1997. *Auditoría Informática - Aplicaciones en Producción: Análisis de Riesgos, Primera Edición.* Colombia : ECOE Ediciones, 1997. págs. Páginas 129-141, 165-186.

[35] KPMG LLP, Sarbanes-Oxley. 2003. *Section 404: Management Assessment of Internal Control and the proposed Auditing Standards, Primera Edición.* EE.UU : s.n., 2003. págs. Páginas 9-12, 17-20. Disponible en: www.kpmg.com.

[36] Mario Piattini y Emilio Del Peso. *Auditoría Informática: Un Enfoque Práctico, Segunda Edición.* España : Editorial RA-MA. págs. Páginas 45-89, 310-317, 394-401, 570-581, 616.

ANEXOS

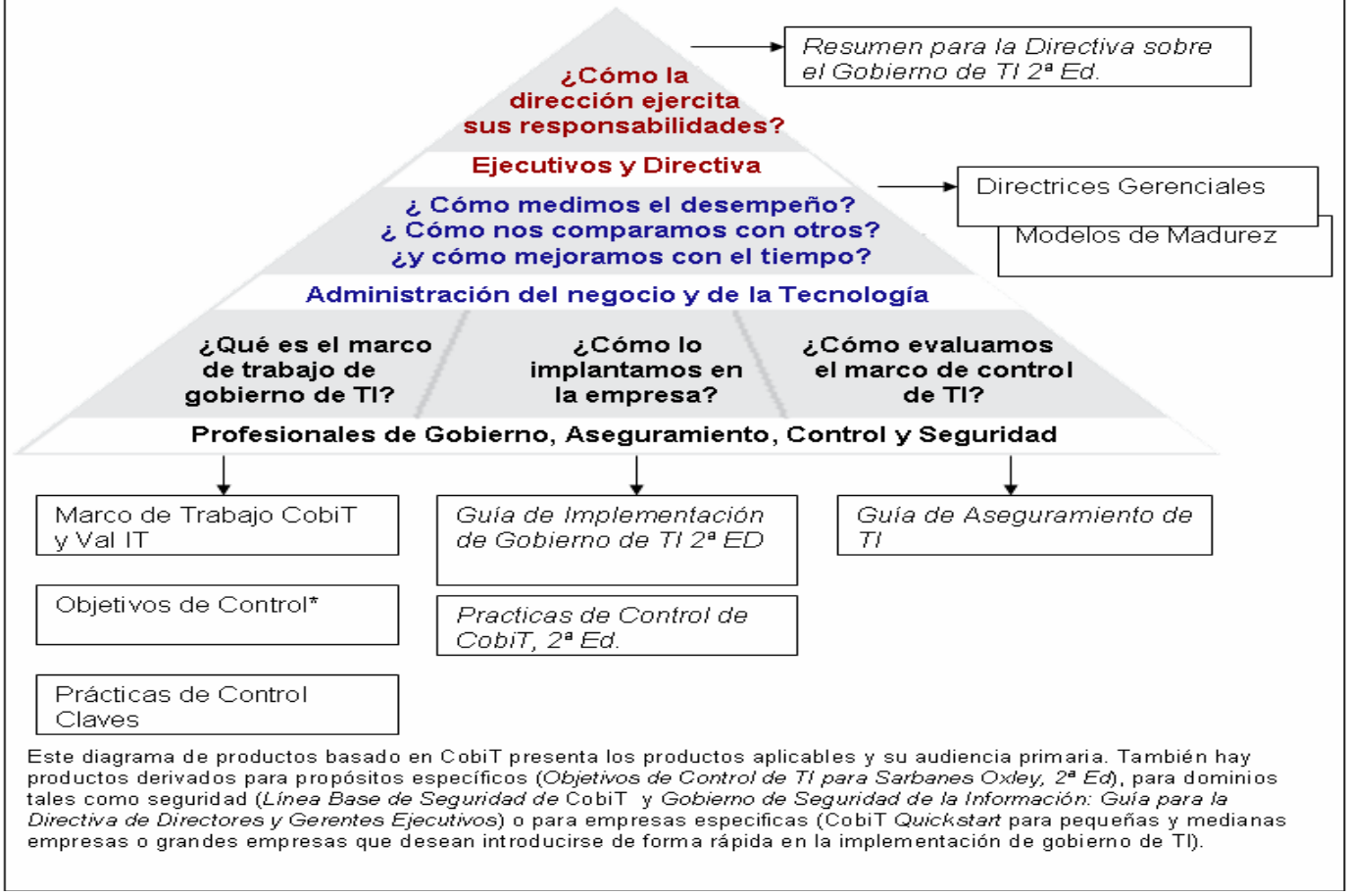
Figura 1 – Administración de la Información

¿Cómo hacen los gerentes responsables para mantener el barco en curso?	TABLEROS DE CONTROL	→ Indicadores?
¿Cómo puede la empresa lograr resultados que sean satisfactorios para la mayor parte de los interesados?	MARCADORES DE PUNTUACIÓN	→ Mediciones?
¿Cómo puede la empresa adaptarse de manera oportuna a las tendencias y avances del ambiente empresarial?	BENCHMARKING	→ Escalas?

Figura 2 – Áreas de Enfoque del Gobierno de TI

•**Alineación Estratégica** se enfoca en garantizar la alineación entre los planes de negocio y de TI; en definir, mantener y validar la propuesta de valor de TI; y en alinear las operaciones de TI con las operaciones de la empresa.
•**Entrega de Valor** se refiere a ejecutar la propuesta de valor a todo lo largo del ciclo de entrega, asegurando que TI genere los beneficios prometidos en la estrategia, concentrándose en optimizar los costos y en brindar el valor intrínseco de la TI.
•**Administración de Recursos** se trata de la inversión óptima, así como la administración adecuada de los recursos críticos de TI: , aplicaciones, información, infraestructura y personas. Los temas claves se refieren a la optimización de conocimiento y de infraestructura.
•**Administración de Riesgos** requiere conciencia de los riesgos por parte de los altos ejecutivos de la empresa, un claro entendimiento del apetito de riesgo que tiene la empresa, comprender los requerimientos de cumplimiento, transparencia de los riesgos significativos para la empresa, y la inclusión de las responsabilidades de administración de riesgos dentro de la organización.
•**Medición del Desempeño** rastrea y monitorea la estrategia de implementación, la terminación del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega del servicio, con el uso, por ejemplo, de balanced scorecards que traducen la estrategia en acción para lograr las metas medibles más allá del registro convencional.

Figura 3 – Productos COBIT



Este diagrama de productos basado en CobiT presenta los productos aplicables y su audiencia primaria. También hay productos derivados para propósitos específicos (*Objetivos de Control de TI para Sarbanes Oxley, 2ª Ed*), para dominios tales como seguridad (*Línea Base de Seguridad de* CobiT y *Gobierno de Seguridad de la Información: Guía para la Directiva de Directores y Gerentes Ejecutivos*) o para empresas especificas (CobiT *Quickstart* para pequeñas y medianas empresas o grandes empresas que desean introducirse de forma rápida en la implementación de gobierno de TI).

Figura 4 – Interrelaciones de los componentes de COBIT