UNIVERSIDAD DE LA REPUBLICA

FACULTAD DE CIENCIAS ECONOMICAS Y DE ADMINISTRACION

TRABAJO MONOGRÁFICO PARA OBTENER EL TITULO DE CONTADOR PÚBLICO

PROPUESTA DE IMPLEMENTACION DEL MARCO DE GESTION COBIT

por

GUSTAVO PEINADO

CIRO GARCIA

COORDINADOR: CR. LUIS SAULEDA

Montevideo

URUGUAY

2010

AGRADECIMIENTOS

Al A/P. Rafael Fabius[1] y al Cr. Carlos Serra[2] por sus aportes para desarrollar el Marco Conceptual y la Propuesta de Implementación, así como por el tiempo que nos brindaron.

A las demás personas que no fueron citadas, pero que de alguna manera directa o indirecta contribuyeron a la realización de este trabajo.

[1] Gerente de Calidad en Republica AFAP. Participó en la elaboración del Marco Cobit en sus versiones 4.0 y 4.1.
[2] Gerente de Proyectos en DATASEC IT Security & Control.

RESUMEN

El presente trabajo de investigación brinda una propuesta de implementación del marco de gestión Cobit (Objetivos de Control para la información y Tecnologías relacionadas), el cual plantea un conjunto de mejores prácticas para el manejo de información dentro de las organizaciones. Su finalidad es mostrar cómo el empleo del Marco permite identificar oportunidades de mejora en la gestión de la TI en la organización y desarrollar una alternativa metodológica para su aplicación. Para ello se describe en primer término su composición y luego se plantean las diferentes herramientas que lo integran, explicando su funcionamiento a través de planteos concretos. Una vez definidos los conceptos, abordamos el desarrollo práctico de la propuesta de implementación. A tales efectos, nos planteamos un caso hipotético y recorremos las diferentes etapas, a saber: Introducción, Capacitación y Planificación, Ejecución de actividades de evaluación, y por último la Gestión de las oportunidades de mejoras. De este modo exponemos un planteo que busca brindar una solución a la problemática referida a, cómo gestionar la tecnología en un mundo cada vez más informatizado y de continuos cambios.

DESCRIPTORES

Cobit. Marco de gestión. Gestión. TI. Implementación. Análisis de valor. Selección de procesos. Metas. Métricas. Matriz RACI. Modelo de madurez. Objetivo de control. Práctica de control.

TABLA DE CONTENIDO

TABLA DE CUADROS Y GRÁFICOS

1. INTRODUCCION, OBJETIVO Y ALCANCE

Introducción

El área informática dentro de las organizaciones ha tomado mayor importancia, dejando de conformar una actividad de apoyo, para pasar a ser un componente que contribuye a la generación de valor para el cliente. Asimismo, muchas organizaciones presentan en la actualidad una total dependencia de la tecnología de la información para lograr sus fines. Creemos que es relevante llevar a cabo el Trabajo de Investigación sobre un marco que enfatiza sobre el componente informático, dentro de la gestión empresarial.

El marco que trataremos en este trabajo, se denomina Cobit (Objetivos de Control para la información y Tecnologías relacionadas), el cual contiene un conjunto de mejores prácticas para el manejo de información creado por la ISACA (Information Systems Audit and Control Association) y el ITGI (IT Governance Institute)en 1992 en su versión Cobit 1.0, actualmente esta disponible la versión Cobit 4.1, asimismo existe un borrador en ingles sobre la versión 5.0. Juntos, ISACA e ITGI lideran la comunidad de Tecnología de la Información y dan soporte, proporcionando las herramientas necesarias de TI en un entorno en constante cambio.

El Objetivo de Cobit es brindar buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas de Cobit representan el consenso de los expertos, el objetivo en su proceso de desarrollo incluye la acumulación de las mejores prácticas de cada industria en la relación al control interno en TI. Están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones habilitadas por TI, asegurarán la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien. [3]

[3] Cobit 4.1, 2007, ITGI

La Misión de Cobit es "Investigar, desarrollar, hacer público y promover un marco de control de gerenciamiento de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento". [4]

Consideramos que es importante citar los siguientes motivos, por los cuales el Marco Cobit es útil para las empresas, ya que:

- Contribuye a alinear el componente tecnológico al giro comercial de las empresas.
- Abarca todas las funciones referidas al área de tecnología.
- Incluye prácticas de control, indicadores, riesgos y procedimientos de auditoria.
- En muchos países constituye un componente de los marcos regulatorios que fijan los gobiernos (ver Anexo 1).
- Es un marco compatible y que se complementa con otros marcos de gestión: COSO, ITIL, entre otros (ver Anexo 2).
- Hay una creciente preferencia por el uso del Marco para el gerenciamiento de TI dentro de las organizaciones a nivel mundial (ver Anexo 3).
- Está en continuo proceso de perfeccionamiento, en la actualidad existe un borrador de la versión 5.0.

Por otra parte, es preciso mencionar que este material puede resultar de utilidad para los siguientes actores dentro de la organización:

- Directivos y accionistas; a los efectos de definir la estrategia de TI y su aporte en la maximización de los beneficios.
- Gerencia general; en la toma de decisiones sobre la gestión de recursos de TI, respecto a costos, beneficios y riesgos.
- Gerencias de Departamento; en la definición de requerimientos de TI para el negocio.
- Gerencia del Departamento de TI; a los efectos de administrar y organizar los procesos de TI.
- Jefaturas de Sectores de TI; en la mejora de los procesos de TI a su cargo.
- Auditores de TI; en la planificación de las Auditorias de TI.

[4] Cobit 4.1, 2007, ITGI

Objetivo

El principal objetivo del presente trabajo es mostrar cómo con la aplicación del Marco de gestión Cobit pueden identificarse oportunidades de mejora para la gestión de TI dentro de la organización y plantear una propuesta metodológica para su implementación que, empleando sus diferentes componentes y herramientas, incluya también elementos adicionales que coadyuven al éxito del emprendimiento..

Son objetivos específicos:

a) Explicar de manera clara la composición del marco y sus herramientas;
b) Apoyar a las organizaciones interesadas en mejorar su gestión a partir de la aplicación de Cobit aportándoles una alternativa metodológica para su implementación.

Alcance

Comenzaremos por una aproximación teórica para luego aplicar dichos conceptos en un enfoque práctico, de manera de proveer una interpretación lo más clara posible del referido Marco y así generar un trabajo de referencia.

La aproximación teórica cumple la finalidad de introducir al lector en el contenido del Marco, a los efectos de que los desarrollos posteriores sean fácilmente comprendidos. En esta instancia se definen y explican las diferentes herramientas que contiene, con el objetivo de sentar las bases del conocimiento.

Luego se planteara el uso de las herramientas y se demostrara su aporte a través del análisis de dos de los Procesos contenidos en el Marco (AI 6 – Administrar cambios, DS 5 – Garantizar la seguridad de los sistemas). Esta dinámica nos permitirá generar planteos concretos de mejora a efectos de incorporarlos a la gestión de la organización.

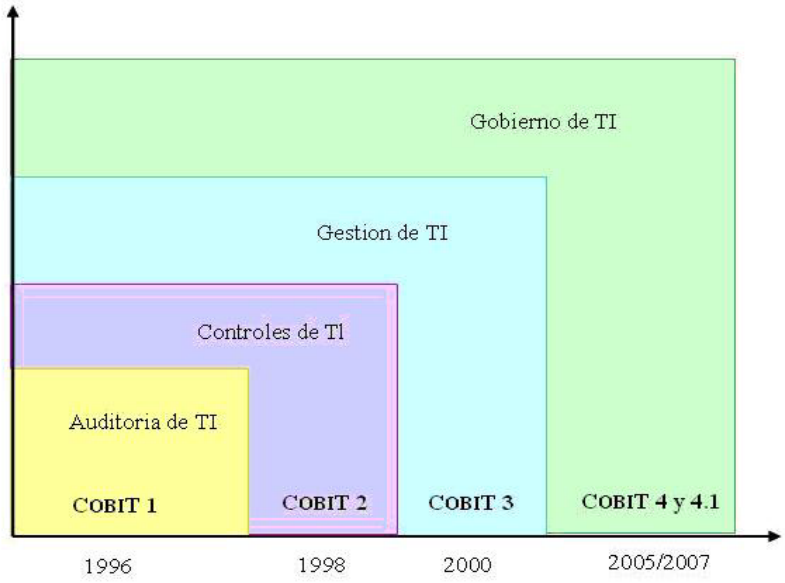
En definitiva es utilizar el Marco Cobit en toda su extensión, ello implica considerar aspectos relativos a su funcionamiento y estructura; herramientas como ser: madurez de procesos, objetivos de control de procesos, niveles de cumplimento de actividades; asimismo el mapeo de riesgos de TI; consideración de observaciones y recomendaciones de auditoria; importancia relativa de cada proceso para la organización; y planteo e implementación de mejoras y recomendaciones.

2. MARCO CONCEPTUAL

2.1 Antecedentes (Evolución de Cobit 1.0 a 4.1)

En su 1ra edición fue liberado por la ISACA en 1996 y trató aspectos preponderantemente de auditoria. La 2da edición reflejó un incremento en el número de documentos fuente, objetivos de control detallados, fue publicado en 1998, con énfasis en los procedimientos de control. La 3ra edición, emitida en el año 2000, marca el ingreso de un nuevo editor para Cobit, el ITGI; esta edición complemento a las anteriores aportando un enfoque de gestión.
En el año 2005 se publicó la 4ta edición y en al año 2007 se perfeccionó con el lanzamiento de la versión 4.1, aportando en ambos casos aspectos relacionado con el gerenciamiento de TI. A la fecha se encuentra en borrador una 5ta Edición, la cual es esperable que este finalizada en 2012.

Gráfico 2.1.1 – Evolución del Marco Cobit



Cobit se basó originalmente en los Objetivos de Control y pretendió ser un análogo a COSO para TI de la ISACA y ha sido mejorado con las actuales y emergentes estándares internacionales a nivel técnico, profesional, regulatorio y específicos de la industria. Los

Objetivos de Control resultantes han sido desarrollados para su aplicación en sistemas de información de toda la empresa. [5]

2.2 Funcionamiento general

El Marco de gestión Cobit fue creado basado en los siguientes cuatro pilares: “orientado al negocio”, “orientado a procesos”, “basado en controles” e “impulsado por mediciones”.

Cuando hablamos de que esta **orientado al negocio**, nos referimos a que fue diseñado de forma tal, que la Información que su aplicación proporciona verifique los siguientes aspectos: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad; es de destacar que dicha información está dirigida a la gerencia, a los responsables de los procesos de negocio, así como también a los auditores de TI.

Asimismo cuenta con herramientas para garantizar que los requisitos de información relacionada a TI y las metas del negocio vayan en el mismo curso de acción, ello se expone en el Apéndice 1 del Marco Cobit 4.1.

Para finalizar, es importante mencionar que muestra que necesidades de Recursos de TI (aplicaciones, información, infraestructura y personas) requiere cada proceso para poder ejecutarse y los aspectos de Gerenciamiento de TI en los que enfatiza el proceso (alineación estratégica, entrega de valor, administración de recursos, administración de riesgos, medición del desempeño).

El segundo pilar refiere a que esta **orientado a procesos,** ya que en el marco se definen las actividades de TI en un modelo genérico de Procesos organizado en cuatro Dominios. Estos dominios son Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y Monitorear y Evaluar. Los dominios se equiparan a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear.

[5] Cobit 3.0, 2000, ITGI

Los procesos se proporcionan en un modelo de referencia, con un lenguaje común para que todos en la empresa visualicen e identifiquen la importancia de las actividades de TI.

Cobit proporciona una lista de 34 procesos; sin embargo, no es necesario que apliquen todos, y, más aun, se pueden combinar como se necesite por cada empresa.

Para cada uno de los procesos, brinda información de cómo se pueden medir las metas, también se proporcionan cuales son sus actividades clave y quién es el responsable de ellas, tiene un enlace a las metas de negocio y TI a las que da soporte.

El tercer pilar en que se apoya el marco, es que esta **basado en controles.** Se definen Objetivos de control para cada uno de los 34 procesos enumerados en el marco. Estos representan un conjunto de requisitos de alto nivel, los cuales deben ser tenidos en cuenta por la gerencia para lograr un control efectivo de cada uno de los procesos. La gerencia de la empresa debe tomar decisiones relativas a estos objetivos de control, seleccionando aquellos que son aplicables para su caso particular, definiendo cuales implementar y como implementarlos.

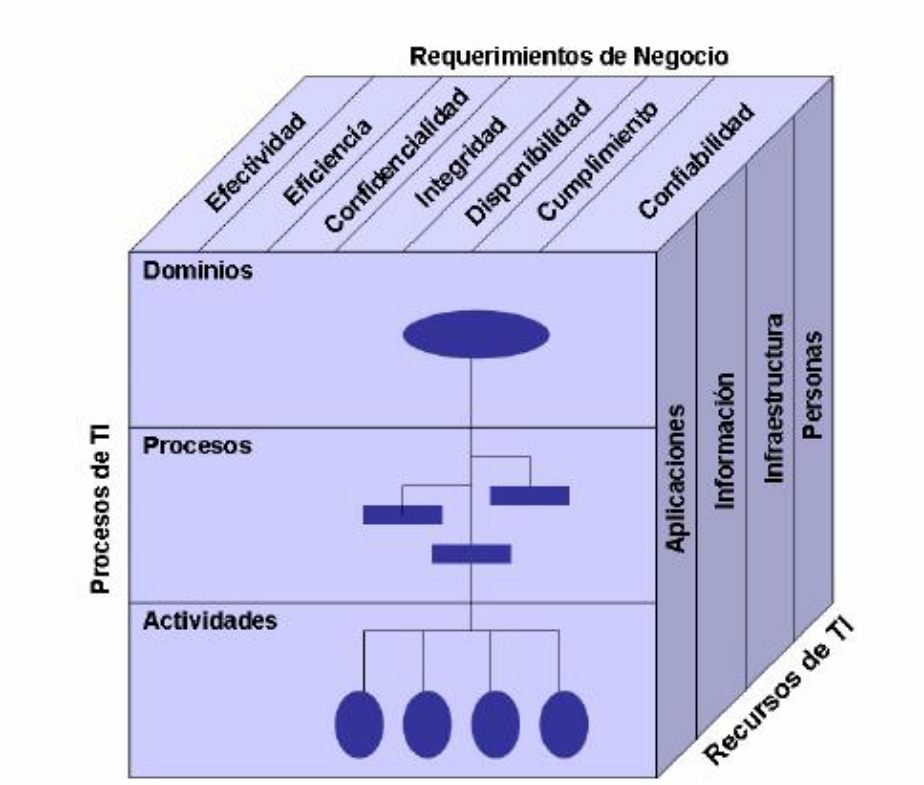
Por último, para que una empresa comprenda el estado de sus sistemas de TI debe estar **impulsado por mediciones**, de modo de poder definir los requisitos de administración y control que debe proporcionar. Las empresas deben medir donde se encuentran y donde precisan mejoras, por lo que deben ser capaces de realizar un análisis objetivo de la situación en que se encuentran, para ello se apoyan en el Modelo de madurez y en el uso de Métricas para monitorear el desempeño y el grado de alcance de las metas propuestas.

Luego de mencionar los pilares en los cuales se basa el marco y las herramientas que les dan sustento, es preciso mencionar el **principio fundamental** en que se basa el marco, asi como el relacionamiento que hay entre sus **diferentes componentes.**

El Marco Cobit se basa en el siguiente principio **“Para proporcionar la información que la empresa requiere para lograr sus objetivos (*requerimientos de negocio*), la empresa necesita invertir en, y administrar y controlar los *recursos de TI* usando un conjunto**

estructurado de *procesos* que provean los servicios que entregan la información empresarial requerida".[6]

Gráfico 2.2.1 – Funcionamiento general del Marco



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

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

• La eficiencia consiste en que la información sea generada con el más productivo y económico uso de los recursos.

• La confidencialidad se refiere a la protección de información sensible contra revelación no autorizada.

[6] Cobit 4.1, 2007, ITGI

• La integridad está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.
• La disponibilidad se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio. También concierne a la protección de los recursos y las capacidades necesarias asociadas.
• El cumplimiento tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.
• La confiabilidad se refiere a brindar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades.

Por otro lado tenemos los **procesos de TI**, con una agrupación que parte de los Dominios (los cuales se citaron anteriormente), desagregados en 34 Procesos y dentro de los cuales se deben ejecutar diferentes Actividades, ellas pueden visualizarse en la Matriz RACI en cada uno de los procesos, la cual sera explicada al referirnos a las herramientas.

Para poder llevar a cabo los procesos y en definitiva responder a los requerimientos que el negocio tiene hacia TI , debemos considerar los diferentes **recursos** que son necesarios, los cuales refieren a las habilidades de las personas y la infraestructura de tecnología para ejecutar aplicaciones automatizadas de negocio, mientras que al mismo tiempo se toma ventaja de la información del negocio.

Estos **recursos de TI**, se pueden definir como sigue:
• Las aplicaciones incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.
• La información son los datos en todas sus formas, de entrada, procesados y generados por los sistemas de información, en cualquier forma en que sean utilizados por el negocio.
• La infraestructura es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.

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

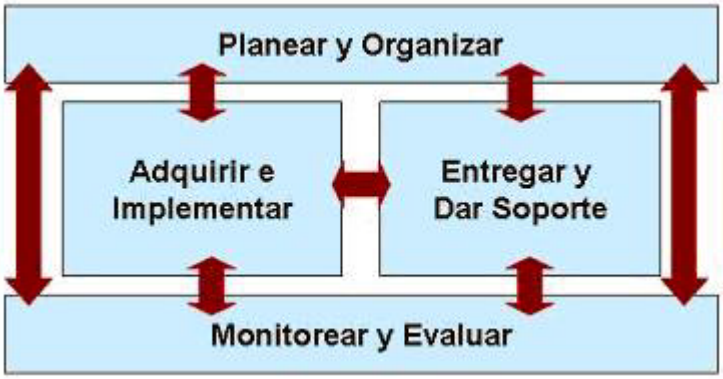
2.3 Descripción de Dominios y Procesos

El marco de gestión se organiza en base a Dominios (4) y Procesos (34). A efectos de lograr un mejor entendimiento planteamos una definición de estos términos y luego hacemos una breve revisión acerca de los mismos.

Dominio: Nos referimos a los **dominios** para agrupar los Objetivos de Control en cuatro etapas lógicas dentro del ciclo de vida de las inversiones referidas a TI (Planificar y Organizar, Adquirir e Implementar, Entregar y Dar soporte, Monitorear y Evaluar). [7]

Como puede observarse en el siguiente gráfico, los Dominios de Cobit están interrelacionados unos con otros.

Gráfico 2.3.1 – Interrelación entre los cuatro Dominios



Proceso: Un **proceso** es un conjunto de procedimientos influenciado por las políticas y procedimientos de la organización. En su ejecución se toman en cuenta un conjunto de recursos (aplicaciones, información, infraestructura y personas) así como también se nutre de

[7] Cobit 4.1 - Glosario, 2007, ITGI

determinados procesos (de entrada), con lo que genera información y apoyo útil para otros procesos (de salida).[8]

Dentro del marco Cobit, para cada proceso se definen:

- Dominio al que pertenece
- Criterios de información relacionados
- Recursos de TI requeridos
- Áreas de Gerenciamiento de TI relacionadas
- Requerimientos del negocio que satisface
- Foco del proceso
- Como se alcanza
- Como se mide

A continuación realizamos una breve descripción de los diferentes Dominios y Procesos:

PLANEAR Y ORGANIZAR (PO)

Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la forma en que TI puede contribuir mejor al logro de los objetivos del negocio.

Este dominio cubre aspectos tales como:

• Grado de convergencia entre las estrategias de TI y las del negocio.
• Optimización de recursos por parte de la empresa.
• Comprensión de todas las personas en la organización, de los objetivos de TI.
• Entendimiento y administración de los riesgos de TI.
• Calidad de los sistemas de TI para las necesidades del negocio.

PO 1. Definir un Plan Estratégico de TI

La planificación estratégica de TI es necesaria para alinear los recursos de Ti (aplicaciones, información, infraestructura y personas) con las prioridades del negocio. El plan de TI ayuda a la comprensión de las oportunidades y amenazas de TI, evalúa el desempeño, identifica la

[8] Cobit 4.1 - Glosario, 2007, ITGI

capacidad y los recursos humanos necesarios. La estrategia de negocios se reflejara en portafolios con objetivos concisos aceptados tanto por el negocio como por TI.

PO 2. Definir la Arquitectura de la Información

Los sistemas de información deben desarrollar y actualizar un modelo de información del negocio de modo de optimizar el uso de la información. Este proceso mejora la calidad en la toma de decisiones gerenciales, proporcionando información confiable y segura, y permite racionalizar los recursos de los sistemas de información para alinearlos con la estrategia del negocio. Este proceso también es fundamental para asignar responsabilidades sobre el control y la seguridad de la información.

PO 3. Determinar la dirección tecnológica

Se debe determinar la dirección tecnológica para dar soporte al negocio. Se requiere la creación de un plan de infraestructura tecnológica que establezca lo que la tecnología puede ofrecer en términos de productos y servicios. Debe cubrir aspectos tales como arquitectura de sistemas, planes de adquisición, estándares, entre otros. El objetivo es estar a la vanguardia de los cambios en el ambiente competitivo.

PO 4. Definir los Procesos, Organización y Relaciones de TI

La organización de TI debe tomaren cuenta los requerimientos personal, funciones, autoridad, roles, responsabilidades entre otros. El marco de trabajo de procesos de TI debe asegurar la transparencia, el control y el involucramiento de los altos ejecutivos y la gerencia. Un comité estratégico y un comité de dirección deben determinar las prioridades de los recursos de TI alineados con las necesidades del negocio. Deben existir procesos, políticas y procedimientos para todas las funciones, para garantizar el control adecuado, la calidad de la información y eficaz administración de los riesgos.

PO 5. Administrar la Inversión en TI

Establecer un marco de trabajo para administrar la inversión en TI considerando costos, beneficios, prioridades y presupuesto. Los interesados (stakeholders) son consultados para identificar costos y beneficios en el contexto de TI y tomar medidas correctivas según sea

necesario. Este proceso brinda transparencia y permite identificar el retorno sobre las inversiones en TI.

PO 6. Comunicar las Aspiraciones y la Dirección de la Gerencia

La dirección debe elaborar un marco de trabajo de control empresarial para TI. Un programa de comunicación continua se debe implementar para que las políticas, procedimientos y objetivos se aliñen con la misión, el cual debe tener la aprobación y el soporte de la dirección.

PO 7. Administrar los Recursos Humanos de TI

La empresa debe adquirir una fuerza de trabajo que le permita crear y entregar servicios de TI. El seguimiento con prácticas definidas permite reclutar mantener y motivar al personal adquirido. El personal es uno de los activos más importantes, por lo que la motivación y la competencia juegan un rol clave.

PO 8. Administrar la Calidad

Se debe elaborar y mantener un sistema de administración de calidad, el cual debe incluir está ndares de desarrollo y adquisición. Planificación, implantación y mantenimiento son fundamentales para establecer políticas y procedimientos claros de calidad. La administración de la calidad es fundamental para asegurar que TI esta dando valor al negocio.

PO 9. Evaluar y Administrar los Riesgos de TI

Crear y mantener un marco de trabajo de administración de riesgos. En este marco se acuerda un nivel de riesgos de TI, así como las estrategias de mitigación de estos. Se deben analizar impactos potenciales y disminuir su probabilidad de ocurrencia.

PO 10. Administrar Proyectos

Establecer un marco de trabajo para la administración de proyectos de TI de modo de asignar prioridades adecuadamente, así como la coordinación de los mismos. Este marco debe: asignar recursos, asegurar la calidad, realizar y revisar pruebas después de la implantación para garantizar la administración de los riesgos del proyecto y la entrega de valor para el negocio.

ADQUIRIR E IMPLEMENTAR (AI)

Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos del negocio. Asimismo cubre los cambios y el mantenimiento de los sistemas existentes, en aras de garantizar que las soluciones sigan satisfaciendo los objetivos del negocio.

Este dominio cubre aspectos tales como:

• Probabilidad de que los nuevos proyectos generan soluciones que satisfagan las necesidades del negocio.

• Probabilidad de que los nuevos proyectos sean entregados a tiempo y dentro del presupuesto.

• Adecuado funcionamiento de los sistemas una vez sean implementados.

• Incidencia de los cambios en las operaciones actuales del negocio.

AI 1. Identificar soluciones automatizadas

Cada vez que es necesaria una nueva aplicación o función dentro de la empresa, se debe realizar un análisis para determinar si es más conveniente “comprar” o “desarrollar”. A la hora de tomar esta decisión se deberá realizar un análisis de cuales son los requisitos del negocio, los riesgos, la relación costo-beneficio, entre otros factores, de modo de tomar la decisión mas efectiva y eficiente para la necesidad a satisfacer.

AI 2. Adquirir y mantener software aplicativo

Las aplicaciones deben tener una relación directa con los requerimientos del negocio, es decir deben estar cubiertos: el diseño de las aplicaciones, controles aplicativos y requerimientos de seguridad. Las aplicaciones automatizadas correctamente brindan apoyo a la operativa de la organización.

AI 3 Adquirir y mantener infraestructura tecnológica

Las organizaciones deben contar con una planificación para adquirir, mantener y proteger la infraestructura tecnológica de acuerdo con la estrategia convenida. De esta manera se garantiza un soporte tecnológico continuo para las aplicaciones del negocio.

AI 4. Facilitar la operación y el uso

El conocimiento sobre los nuevos sistemas debe estar disponible. Este proceso requiere la generación de documentación y manuales para usuarios y para TI, y proporciona entrenamiento para garantizar el uso y la operación correcta de las aplicaciones y la infraestructura.

AI 5. Adquirir recursos de TI

Es necesario asegurar la adquisición de recursos de TI de una manera oportuna y rentable. Estos recursos incluyen personas, hardware, software y servicios. Para ello se deben definir los procedimientos de adquisición (selección de proveedores, regímenes contractuales y gestión de compras).

AI 6. Administrar cambios

Los cambios relacionados con la infraestructura y las aplicaciones deben administrarse formal y adecuadamente. Estos se deben registrar, evaluar y autorizar previo a la implantación y luego revisarse comparando con los resultados planeados. De este modo, se busca garantizar la reducción de riesgos.

AI 7. Instalar y acreditar soluciones y cambios

La funcionalidad de los nuevos sistemas es fundamental. Esto requiere pruebas adecuadas con datos relevantes y revisar la post-implementación. Esto garantiza que los sistemas operativos estén en línea con las expectativas convenidas y con los resultados.

ENTREGAR Y DAR SOPORTE (DS)

Este dominio abarca la entrega de los servicios requeridos. Incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativas.

Generalmente cubre los siguientes aspectos:

• Entrega de los servicios de TI de acuerdo con las prioridades del negocio.
• Optimización de los costos de TI.
• Capacidad del personal de utilizar los sistemas de TI de manera productiva y segura.

• Adecuada implementación de la confidencialidad, la integridad y la disponibilidad en la organización.

DS 1. Definir y Administrar los Niveles de Servicio

Contar con definición documentada de servicios de TI hace posible que exista un canal efectivo de comunicación entre la gerencia de TI y los clientes respecto de los servicios requeridos.

DS 2. Administrar los Servicios de Terceros

Es necesario un proceso efectivo de administración de terceros para asegurar que estos cumplan con los requerimientos del negocio. Se deben definir claramente los roles, responsabilidades y expectativas en los acuerdos con terceros. La efectiva administración minimiza el riesgo en caso de incumplimiento del proveedor.

DS 3. Administrar el Desempeño y la Capacidad

Para administrar correctamente este proceso, se requiere una revisión periódica del desempeño actual y la capacidad de los recursos de TI. Incluye el pronóstico de las necesidades futuras. Este proceso asegura que los recursos de información de los requerimientos del negocio están disponibles de manera continua.

DS 4. Garantizar la Continuidad del Servicio

Para garantizar esta continuidad es necesario desarrollar planes de continuidad de TI y tomar medidas como ser contar con respaldos fuera de las instalaciones. De esta forma se minimiza la probabilidad de grandes interrupciones de los servicios de TI.

DS 5. Garantizar la Seguridad de los Sistemas

Garantizar la seguridad de los activos de TI requiere de un proceso de administración de esta, que incluya asignación de roles y responsabilidades, políticas estándares y procedimientos. También incluye la realización de monitoreos, pruebas periódicas y acciones correctivas sobre las debilidades en la seguridad.

DS 6. Identificar y Asignar Costos

Se requiere de una medición precisa y un acuerdo con los usuarios del negocio de modo que el sistema de asignación de Costos sea justo y equitativo. Este proceso incluye la construcción de un sistema para distribuir y reportar costos de TI a los usuarios de los servicios.

DS 7. Educar y Entrenar a los Usuarios

Se debe lograr una educación efectiva de los usuarios de sistemas de TI, para lo cual se deben identificar las necesidades de entrenamiento. Un programa efectivo de entrenamiento incrementa el uso efectivo de la tecnología, la productividad y el cumplimiento de los controles clave tales como las medidas de seguridad.

DS 8. Administrar la Mesa de Servicio y los Incidentes

Una mesa de servicios adecuada permite responder a las consultas y problemas de los usuarios de TI, así como también contar con un proceso de administración de incidentes. Los beneficios del negocio se reflejan en el incremento de la productividad gracias a la resolución rápida de consultas. Además puede identificar la causa de los problemas.

DS 9. Administrar la Configuración

Para mantener adecuadamente las configuraciones de hardware y software, se debe contar con un repositorio completo y preciso. Esto facilita una mayor disponibilidad y minimiza los problemas de producción.

DS 10. Administración de Problemas

Para que esto sea posible se requiere la identificación y clasificación de problemas, así como su resolución. Este proceso también incluye generar recomendaciones de mejora. Si la administración es adecuada garantiza un mejor nivel de servicios.

DS 11. Administración de Datos

Para que este proceso sea efectivo se deben identificar los requerimientos de datos. También incluye el establecimiento de procedimientos efectivos para administrar medios, respaldar y recuperar datos. El objetivo es garantizar la calidad, oportunidad y disponibilidad de la información del negocio.

DS 12. Administración del Ambiente Físico

La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. Es fundamental la selección de instalaciones apropiadas y el diseño de procesos para detectar factores ambientales y administrar el acceso físico.
La administración adecuada del ambiente físico reduce las interrupciones del negocio.

DS 13. Administración de Operaciones

Se requiere una efectiva administración del procesamiento de datos y del mantenimiento del hardware. También incluye la definición de políticas y procedimientos de operación, protección de datos y monitoreo de infraestructura.

MONITOREAR Y EVALUAR (ME)

Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación de políticas de gerenciamiento.

Generalmente cubre los siguientes aspectos:
• Medición del desempeño de TI para detectar los problemas.
• Nivel de efectividad y eficiencia de los controles internos.
• Relación entre el desempeño de TI y las metas del negocio.
• Reportes de riesgos, controles, cumplimiento y desempeño.

ME 1. Monitorear y Evaluar el Desempeño de TI

En este proceso se deben definir indicadores de desempeño relevantes, además es preciso contar con reportes y medidas correctivas para las desviaciones. El monitoreo se requiere para que garantizar que las medidas están de acuerdo con las direcciones y política de la empresa.

ME 2. Monitorear y Evaluar el Control Interno

Este proceso incluye el monitoreo y reporte de las excepciones de control, resultados de las auto-evaluaciones y revisiones por parte de terceros. El monitoreo del control interno proporciona seguridad de las operaciones y cumplimiento de normativas.

ME 3. Garantizar el Cumplimiento con Requerimientos Externos

Se requiere de un proceso de revisión para garantizar el cumplimiento de las leyes, regulaciones y requerimientos contractuales. Se deben identificar requerimientos de cumplimiento, asegurar que estos se cumplen e integrar los reportes de cumplimiento de TI con el resto del negocio.

ME 4. Proporcionar Gerenciamiento de TI

Un marco de gerenciamiento efectivo se define a través de estructuras, procesos, liderazgo, roles y responsabilidades organizacionales, para garantizar que las inversiones en TI estén de acuerdo con las estrategias y objetivos empresariales.

Mientras la mayoría de las empresas ha definido las responsabilidades de planear, construir, ejecutar y monitorear para TI, y la mayoría tienen los mismos procesos clave, pocas tienen la misma estructura de procesos o le aplicaran todos los 34 procesos de Cobit.

2.4 Herramientas a Utilizar para Analizar los Procesos

Luego de haber realizado una definición de los Procesos, corresponde analizar las distintas herramientas que incluye el Marco para estudiar su funcionamiento. Dentro de cada Proceso se utilizan cada una de las diferentes herramientas que se describirán en este numeral.
Para realizar esta tarea tomaremos como ejemplo los procesos *AI 6 Administrar Cambios y DS 5 Garantizar la Seguridad de los Sistemas*, el funcionamiento es similar para todos los demás procesos.

2.4.1 **Objetivos de Control**

Para cada proceso se definen Objetivos de Control.

En el Marco encontramos que el *"Control se define como las políticas, procedimientos, practicas y estructuras organizacionales diseñadas para brindar una seguridad razonable*

que los objetivos de negocios se alcanzarán, y los eventos no deseados serán prevenidos y corregidos."[9]

Los Objetivos de Control de TI presentan un conjunto de requisitos de alto nivel, los cuales incluyen descripciones sobre las acciones que debe llevar a cabo la gerencia para aumentar el valor y reducir el riesgo, aumentar al máximo la probabilidad de concreción de los objetivos de negocio, disminuir al mínimo la probabilidad de concreción de eventos no deseados, facilitar la detección de posibles errores para su prevención y corrección, así como también incluyen la definición de las políticas y procedimientos a considerar por la gerencia.

La gerencia de la empresa necesita tomar decisiones relativas a estos Objetivos de Control, seleccionando aquellos aplicables, decidiendo cuales deben implementarse, elegir como implementarlos y aceptar el riesgo de no implementar aquellos que podrían aplicar.

Cada uno de los procesos de TI tiene definido un **Objetivo de Control de alto nivel**, y varios **Objetivos de Control detallados**, los cuales combinados hacen un todo sobre cómo se debe administrar un proceso correctamente.

Los Objetivos de Control de alto nivel coinciden con la descripción que fue realizada en el numeral 2.3, mientras que los Objetivos de Control detallados se identifican primero con las dos letras que hace referencia al dominio al cual pertenecen, más un número de proceso y un número de Objetivo de Control dentro del proceso.

Ejemplificamos con los procesos AI 6 y DS 5, los cuales además de los Objetivos de Control de alto nivel contienen los siguientes Objetivos de Control detallados:

AI 6 Administrar Cambios.

AI 6.1 Estándares y Procedimientos para Cambios: Toda solicitud de cambio requieren de un procedimiento estándar que lo respalde, ya sean cambios en las políticas, procedimientos, aplicaciones, parámetros de sistemas, etc.

[9] Cobit 4.1, 2007, ITGI

AI 6.2 Evaluación de Impacto, Priorización y Autorización: Cada solicitud de cambio se debe evaluar de una manera estructurada, de forma de divisar cuales puede ser su impacto en el sistema operativo para que el funcionamiento de este no se vea perjudicado. Estos cambios deben estar priorizados y autorizados por las personas correspondientes, sin dejar de lado a las partes que se verán afectadas por estos cambios.

AI 6.3 Cambios de Emergencia: Algunos cambios por su naturaleza de urgentes, requieren de hacerse sin el procedimiento estándar establecido por la empresa, por lo que esta deberá definir procedimientos para cambios de emergencia a modo de garantizar la correcta implementación de estos.

AI 6.4 Seguimiento y Reporte del Estatus de Cambio: Es fundamental contar con un sistema de seguimiento de los cambios establecidos, de modo de mantener informados a los principales actores, así como contar con reportes periódicos acerca del estatus del cambio.

AI 6.5 Cierre y Documentación del Cambio: Se debe establecer un procedimiento de revisión para finalizar de forma integral la implantación del cambio, así como actualizar la documentación para los usuarios.

DS 5 Garantizar la Seguridad de los Sistemas.

DS 5.1 Administración de la Seguridad de TI: La seguridad de TI se debe administrar en los altos mandos, de forma que esté adecuadamente alineada con los requerimientos del negocio.

DS 5.2 Plan de Seguridad de TI: El plan de seguridad de TI debe contener los requerimientos riesgos y cumplimiento del negocio. Asegurarse de que el plan esta implementado en las políticas y procedimientos de seguridad, junto con las inversiones necesarias en recursos.

DS 5.3 Administración de Identidad: Todos los usuarios de TI deben estar perfectamente identificables. Se deben establecer mecanismos de autenticación, permisos de acceso de los usuarios al sistema. Asegurar que el establecimiento de acceso de los usuarios sea solicitado

por la gerencia del usuario, aprobado e implementado por los responsables del sistema y la seguridad.

DS 5.4 Administración de Cuentas del Usuario: Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuarios, sean considerados por la gerencia que administra las cuentas de los usuarios. Es fundamental un procedimiento en el cual se identifique a los responsables de otorgar los privilegios de acceso. Estos procedimientos se deben aplicar para todos los usuarios. Por ultimo es necesario realizar revisiones regulares de la gestión de las cuentas.

DS 5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad: La seguridad de TI requiere de un constante cuidado de modo que el nivel de esta se mantenga, y así detectar actividades inusuales.

DS 5.6 Definición de los Incidentes de Seguridad: Definir las características de Incidentes de seguridad, para que puedan ser tratados y clasificados adecuadamente.

DS 5.7 Protección de la Tecnología de Seguridad: Tecnología resistente al sabotaje y confidente de información importante.

DS 5.8 Administración de Llaves Criptográficas: Es necesario que todo el ciclo de definición e implementación de las llaves criptográficas garanticen la protección contra modificaciones y divulgaciones.

DS 5.9 Prevención, Detección y Corrección de Software Malicioso: implantar medidas preventivas, de detección y correctivas, para proteger a la organización contra virus, Spyware, etc.

DS 5.10 Seguridad de la Red: utilización de técnicas de seguridad, para controlar la información que se mueve dentro de las redes.

DS 5.11 Intercambio de Datos Sensibles: Los datos muy importantes se deben intercambiar implementando controles de autenticidad de contenido, envío, recepción y origen.

Además, el Marco incluye una serie de requerimientos de control genéricos, los cuales son iguales para todos los procesos, y los cuales se consideran en forma conjunta de modo de tener una visión global acerca de los requisitos de control de los procesos, estos son:

- Metas y Objetivos del Proceso: Definir procesos, metas y objetivos específicos, con las métricas adecuadas para segurar que vayan en el mismo curso que las metas de negocio.

- Propiedad del Proceso: Definir quien va a ser el "propietario" del proceso de TI, lo cual requiere definir los roles y responsabilidades, interacción con otros procesos, medición del desempeño e identificación de oportunidades de mejora.

- Proceso Repetible: Diseñar los procesos de TI de manera que produzca los resultados esperados. Desarrollar una secuencia de actividades flexible de modo que lleve a los resultados esperados y permita manejar de forma rápida las emergencias.

- Roles y Responsabilidades: Definir las actividades clave de los procesos, y asignar los roles y responsabilidades de forma exacta, así se asegura el efectivo cumplimiento de estas.

- Políticas, Planes y Procedimientos: Definir, comunicar y documentar las políticas planes y procedimientos, así como también considerar su revisión posterior. Asegurar que sean accesibles, correctos y actualizados.

- Desempeño del Proceso: Identificar métricas para medir el desempeño del proceso, definir como los datos son obtenidos, tomar acciones sobre las desviaciones. Alinear las métricas con los objetivos del proceso.

Los objetivos de control bien definidos y correctamente aplicados reducen el riesgo, incrementan la entrega de valor y la eficiencia, como consecuencia generan menores errores y un funcionamiento integral de las políticas administrativas de la organización.

Ahora bien, hasta aquí hemos presentado los diferentes Objetivos de Control que brinda el Marco, aquellos en los que se basa y los que directamente se relacionan con cada proceso. Por lo tanto es bueno a esta instancia presentar como el Control Interno de la empresa impacta en el área de TI a tres diferentes niveles:

- A nivel de dirección ejecutiva: el enfoque de control y gestión a ser llevado a cabo en la organización se establece a nivel directivo y es orientado a toda la empresa. El ambiente de control de TI es guiado por este conjunto de políticas de alto nivel.

- A nivel de proceso de negocios: Se aplican controles para actividades específicas del negocio, los cuales son conocidos como controles de aplicaciones. A este nivel son una combinación de controles manuales, controles de negocio y controles automatizados. En cuanto a los de negocio y automatizados requieren del diseño y soporte de TI.
  Asimismo cuando hablamos de controles de aplicaciones nos referimos a los que tienen que ver directamente con los procesos de negocios como ser controles de autorización, validez, integridad entre otros. Los Controles de Aplicaciones automatizados son responsabilidad de TI, y están incluidos en Cobit en el Dominio de Adquirir e Implementar.

- A nivel de los controles generales de TI: Son los controles aplicados a todas las actividades de servicio de TI, estos deben sustentar a los controles de aplicaciones. Por ejemplo, una deficiente administración de cambios podría poner en riesgo la confiabilidad de los chequeos automáticos de integridad.

Es preciso mencionar que cuando hablamos de controles generales nos referimos a aquellos que están incluidos en los procesos de TI como ser la seguridad, el desarrollo de los sistemas entre otros.

2.4.2 **Modelo de Madurez**

El Modelo de Madurez representa una de las dos herramientas fundamentales con que cuenta Cobit para desarrollar uno de los cuatro pilares; *Impulsado por Mediciones*, la cual es sumamente practica.

El desarrollo de este modelo surge en respuesta a la interrogante acerca de, qué tan bueno es el nivel de desarrollo y administración de TI que tiene la empresa, por lo que hay que prestar especial atención a aspectos tales como: qué esta haciendo la competencia en la industria y compararla con lo que esta haciendo nuestra empresa, cuáles son las mejores prácticas en la industria y cuál es nuestra posición con respecto a ello, y el último aspecto fundamental es poder identificar si lo que se está haciendo es suficiente para alcanzar un nivel adecuado de administración y control de TI.

El Modelo de Madurez aparece en cada uno de los procesos que se desarrollan en el Marco, por lo tanto el Modelo de Madurez de un determinado proceso nos esta dando una perspectiva respecto a ese proceso en particular, con lo cubre las siguientes necesidades:

- Da una visión relativa de donde se encuentra la empresa en el desarrollo de ese proceso,
- Proporciona una forma de ver cuál es el mejor curso a tomar de forma eficiente,
- Sirve de herramienta comparativa entre el avance y la meta a ser alcanzada.

Esta herramienta brinda la posibilidad a la organización de autoevaluarse, de forma tal que pueda ver por si misma su nivel actual en una escala de valores, clara y práctica la cual va desde el nivel 0 hasta el 5, para lo cual exponemos el modelo genérico desarrollado en el Marco:

Cuadro 2.4.2.1 – Modelo Genérico de Madurez

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

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

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

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

4 Administrado- Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

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

Estos niveles genéricos están desarrollados de forma tal que una empresa cualquiera reconocería como descripciones de estados posibles actuales y futuros de los procesos. No están diseñados como un modelo limitante, donde no se puede pasar al nivel superior sin haber cumplido todas las condiciones del nivel inferior, sino que apunta a tener una visión relativa de si las condiciones relevantes a un determinado nivel de madurez se han conseguido. Esto se debe a que cuando la empresa aplique a su realidad el Modelo de Madurez de Cobit, es muy probable que no todas las implantaciones se encuentren en el mismo nivel.

La gran utilidad y ventaja de esta herramienta esta en la relativa facilidad con que los usuarios de Cobit pueden ubicarse en esta escala, ya que fue diseñada de modo tal que los altos mandos vean reflejadas sus situaciones particulares en ella, y de ese modo evaluar que se requiere hacer en caso que sea necesaria una mejora.

Para cada uno de los 34 procesos definidos en Cobit, existe un desarrollo de un Modelo de Madurez, de modo de poder visualizar en que estado de avance se encuentra ese proceso particular. Este Modelo le brindará nociones de: donde se encuentra la realidad de la propia empresa, donde se encuentra la realidad de la industria, el objetivo de mejora de la empresa o dicho de otro modo el lugar en que quiere posicionarse, y por último la distancia existente

entre la situación actual y la situación deseada. Veamos el desarrollo en los procesos *AI 6 Administrar Cambios y DS 5 Garantizar la Seguridad de los Sistemas:*

Cuadro 2.4.2.2 – Niveles de Madurez del Proceso AI6

AI6 Administrar Cambios

La administración del proceso de *Administrar cambios* que satisfaga el requerimiento de negocio de TI de *responder a los requerimientos de acuerdo con la estrategia del negocio, mientras que se reducen los defectos y repeticiones de trabajos en la entrega de soluciones y servicios* es:

0 No Existente cuando
No existe un proceso definido de administración de cambio y los cambios se pueden realizar virtualmente sin control. No hay conciencia de que el cambio puede causar una interrupción para TI y las operaciones del negocio y no hay conciencia de los beneficios de la buena administración de cambio.

1 Inicial / Ad Hoc cuando
Se reconoce que los cambios se deben administrar y controlar. Las prácticas varían y es muy probable que se puedan dar cambios sin autorización. Hay documentación de cambio pobre o no existente y la documentación de configuración es incompleta y no confiable. Es posible que ocurran errores junto con interrupciones al ambiente de producción, provocados por una pobre administración de cambios.

2 Repetible pero Intuitivo cuando
Existe un proceso de administración de cambio informal y la mayoría de los cambios siguen este enfoque; sin embargo, el proceso no está estructurado, es rudimentario y propenso a errores. La exactitud de la documentación de la configuración es inconsistente y de planeación limitada y la evaluación de impacto se da previa al cambio.

3 Definido cuando
Existe un proceso formal definido para la administración del cambio, que incluye la categorización, asignación de prioridades, procedimientos de emergencia, autorización del cambio y administración de liberación, y va surgiendo el cumplimiento. Se dan soluciones temporales a los problemas y los procesos a menudo se omiten o se hacen a un lado. Aún pueden ocurrir errores y los cambios no autorizados ocurren ocasionalmente. El análisis de impacto de los cambios de TI en operaciones de negocio se está volviendo formal, para apoyar la implantación planeada de nuevas aplicaciones y tecnologías.

4 Administrado y Medible cuando
El proceso de administración de cambio se desarrolla bien y es consistente para todos los cambios, y la gerencia confía que hay excepciones mínimas. El proceso es eficiente y efectivo, pero se basa en manuales de procedimientos y controles considerables para garantizar el logro de la calidad. Todos los cambios están sujetos a una planeación minuciosa y a la evaluación del impacto para minimizar la probabilidad de tener problemas de post-producción. Se da un proceso de aprobación para cambios. La documentación de administración de cambios es vigente y correcta, con seguimiento formal a los cambios. La documentación de configuración es generalmente exacta. La planeación e implantación de la administración de cambios en TI se van integrando con los cambios en los procesos de negocio, para asegurar que se resuelven los asuntos referentes al entrenamiento, cambio organizacional y continuidad del negocio. Existe una coordinación creciente entre la administración de cambio de TI y el rediseño del proceso de negocio. Hay un proceso consistente para monitorear la calidad y el desempeño del proceso de administración de cambios.

5 Optimizado cuando
El proceso de administración de cambios se revisa con regularidad y se actualiza para permanecer en línea con las buenas prácticas. El proceso de revisión refleja los resultados del monitoreo. La información de la configuración es computarizada y proporciona un control de versión. El rastreo del cambio es sofisticado e incluye herramientas para detectar software no autorizado y sin licencia. La administración de cambio de TI se integra con la administración de cambio del negocio para garantizar que TI sea un factor que hace posible el incremento de productividad y la creación de nuevas oportunidades de negocio para la organización.

Cuadro 2.4.2.3 – Niveles de Madurez del Proceso DS 5

DS5 Garantizar la Seguridad de los Sistemas

La administración del proceso de *Garantizar la seguridad de los sistemas* que satisfaga el requerimiento de negocio de TI de *mantener la integridad de la información y de la infraestructura de procesamiento y minimizar el impacto de vulnerabilidades e incidentes de seguridad* es:

0 No Existente cuando
La organización no reconoce la necesidad de la seguridad para TI. Las responsabilidades y la rendición de cuentas no están asignadas para garantizar la seguridad. Las medidas para soportar la administrar la seguridad de TI no están implementadas. No hay reportes de seguridad de TI ni un proceso de respuesta para resolver brechas de seguridad de TI. Hay una total falta de procesos reconocibles de administración de seguridad de sistemas.

1 Inicial / Ad Hoc cuando
La organización reconoce la necesidad de seguridad para TI. La conciencia de la necesidad de seguridad depende principalmente del individuo. La seguridad de TI se lleva a cabo de forma reactiva. No se mide la seguridad de TI. Las brechas de seguridad de TI ocasionan respuestas con acusaciones personales, debido a que las responsabilidades no son claras. Las respuestas a las brechas de seguridad de TI son impredecibles.

2 Repetible pero Intuitivo cuando
Las responsabilidades y la rendición de cuentas sobre la seguridad, están asignadas a un coordinador de seguridad de TI, pero la autoridad gerencial del coordinador es limitada. La conciencia sobre la necesidad de la seguridad esta fraccionada y limitada. Aunque los sistemas producen información relevante respecto a la seguridad, ésta no se analiza. Los servicios de terceros pueden no cumplir con los requerimientos específicos de seguridad de la empresa. Las políticas de seguridad se han estado desarrollando, pero las herramientas y las habilidades son inadecuadas. Los reportes de la seguridad de TI son incompletos, engañosos o no aplicables. La habilitación sobre seguridad está disponible pero depende principalmente de la iniciativa del individuo. La seguridad de TI es vista primordialmente como responsabilidad y disciplina de TI, y el negocio no ve la seguridad de TI como parte de su propia disciplina.

3 Definido cuando
Existe conciencia sobre la seguridad y ésta es promovida por la gerencia. Los procedimientos de seguridad de TI están definidos y alineados con la política de seguridad de TI. Las responsabilidades de la seguridad de TI están asignadas y entendidas, pero no continuamente implementadas. Existe un plan de seguridad de TI y existen soluciones de seguridad motivadas por un análisis de riesgo. Los reportes no contienen un enfoque claro de negocio. Se realizan pruebas de seguridad adecuadas (por ejemplo, pruebas contra intrusos). Existe habilitación en seguridad para TI y para el negocio, pero se programa y se comunica de manera informal.

4 Administrado y Medible cuando
Las responsabilidades sobre la seguridad de TI son asignadas, administradas e implementadas de forma clara. Regularmente se lleva a cabo un análisis de impacto y de riesgos de seguridad. Las políticas y prácticas de seguridad se complementan con referencias de seguridad específicas. El contacto con métodos para promover la conciencia de la seguridad es obligatorio. La identificación, autenticación y autorización de los usuarios está estandarizada. La certificación en seguridad es buscada por parte del personal que es responsable de la auditoría y la administración de la seguridad. Las pruebas de seguridad se hacen utilizando procesos estándares y formales que llevan a mejorar los niveles de seguridad. Los procesos de seguridad de TI están coordinados con la función de seguridad de toda la organización. Los reportes de seguridad están ligados con los objetivos del negocio. La habilitación sobre seguridad se imparte tanto para TI como para el negocio. La habilitación sobre seguridad de TI se planea y se administra de manera que responda a las necesidades del negocio y a los perfiles de riesgo de seguridad. Los KGIs y KPIs ya están definidos pero no se miden aún.

5 Optimizado cuando
La seguridad en TI es una responsabilidad conjunta del negocio y de la gerencia de TI y está integrada con los objetivos de seguridad del negocio en la corporación. Los requerimientos de seguridad de TI están definidos de forma clara, optimizados e incluidos en un plan de seguridad aprobado. Los usuarios y los clientes se responsabilizan cada vez más de definir requerimientos de seguridad, y las funciones de seguridad están integradas con las aplicaciones en la fase de diseño. Los incidentes de seguridad son atendidos de forma inmediata con procedimientos formales de respuesta soportados por herramientas automatizadas. Se llevan a cabo valoraciones de seguridad de forma periódica para evaluar la efectividad de la implementación del plan de seguridad. La información sobre amenazas y vulnerabilidades se recolecta y analiza de manera sistemática. Se recolectan e implementan de forma oportuna controles adecuados para mitigar riesgos. Se llevan acabo pruebas de seguridad, análisis de causa-efecto e identificación pro-activa de riesgos para la mejora continua de procesos. Los procesos de seguridad y la tecnología están integrados a lo largo de toda la organización. Los KGIs y KPIs para administración de seguridad son recopilados y comunicados. La gerencia utiliza los KGIs y KPIs para ajustar el plan de seguridad en un proceso de mejora continua

Como se puede apreciar en los cuadros expuestos, están definidos en el Marco los posibles niveles de Madurez para cada uno de los procesos. De este modo veamos por ejemplo que en el Proceso *AI 6- Administrar Cambios*, cuando en una empresa la administración de los

cambios es informal, existe conciencia del proceso, pero este no esta estructurado y es rudimentario, podemos afirmar que el Proceso AI6 se encuentra en el nivel de madurez 2 - Repetible pero Intuitivo.

De este mismo modo considerando el Proceso *DS5 - Garantizar la Seguridad de los Sistemas*, si la empresa tiene conciencia de la existencia de este proceso, y además la gerencia promueve la seguridad de TI y los procedimientos de seguridad están alineados con la política de seguridad de TI, pero los reportes no tienen un enfoque claro de negocio y la comunicación se hace de manera informal, podemos afirmar que el Proceso DS5 se encuentra en el nivel de Madurez 3-Definido.

De este modo vemos el funcionamiento del Modelo de Madurez, el cual permite a la empresa visualizar en que nivel se encuentra respecto a determinado proceso, y a partir de ello comenzar a tomar medidas para alcanzar el nivel de Madurez que la empresa considere necesario para alinearse a las metas del negocio.

El tema de procesos de TI es muy complejo, por lo que resulta mucho mas fácil abordarlo con evaluaciones fáciles como las que propone este modelo, ya que aumentan la conciencia, logran un consenso amplio y motivan la mejora continua.

2.4.3 Matriz RACI

La Matriz RACI es una herramienta que identifica quien es Responsable (R), quien debe Rendir Cuentas (A), quien debe ser Consultado (C) y/o Informado (I) en cada una de las actividades de los procesos. Esta Matriz refleja para cada proceso, Involucrados y Roles estándar, los cuales sirven de guía pero pueden diferir con la realidad de la organización bajo análisis.

Es bueno precisar la diferencia entre Responsable (R) y quien debe Rendir Cuentas (A). El primero es quien debe llevar a cabo la actividad y el segundo debe monitorear el desempeño del responsable, es la persona que provee autorización y direccionamiento a una actividad.

Una correcta asignación de las responsabilidades entre los actores de la organización, es una de las claves del éxito para el buen gerenciamiento. Por un lado tenemos que identificar con exactitud quien es la persona responsable del proceso y quien debe rendir cuentas. Por otro lado la correcta identificación de quien debe ser consultado y quien debe ser informado es lo que garantiza que todas las personas involucradas den soporte al proceso.

Veamos la matriz RACI de los procesos en estudio:

Cuadro 2.4.3.1 – Matriz RACI del Proceso AI 6- Administrar Cambios

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Desarrollar e implementar un proceso para registrar, evaluar y dar prioridad en forma consistente a las solicitudes de cambio				A	I	R	C	R	C	C	C
Evaluar impacto y dar prioridad a cambios en base a las necesidades del negocio				I	R	A/R	C	R	C	R	C
Garantizar que cualquier cambio crítico y de emergencia sigue el proceso aprobado				I	I	A/R	I	R			C
Autorizar cambios				I	C	A/R		R			
Administrar y diseminar la información relevante referente a cambios				A	I	R	C	R	I	R	C

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Cuadro 2.4.3.2 – Matriz RACI del Proceso DS 5 - Garantizar la Seguridad de los Sistemas

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
Definir y mantener un plan de seguridad de TI	I	C	C	A	C	C	C	C	I	I	R
Definir, establecer y operar un proceso de administración de identidad (cuentas)			I	A	C	R	R	I			C
Monitorear incidentes de seguridad, reales y potenciales				A	I	R	C	C			R
Revisar y validar periódicamente los privilegios y derechos de acceso de los usuarios				I	A	C					R
Establecer y mantener procedimientos para mantener y salvaguardar las llaves criptográficas				A		R			I		C
Implementar y mantener controles técnicos y de procedimientos para proteger el flujo de información a través de la red				A	C	C	R	R			C
Realizar evaluaciones de vulnerabilidad de manera regular		I		A	I	C	C	C			R

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

Vemos entonces que en la Matriz RACI se identifican los siguientes Involucrados:

- CEO - Director Ejecutivo
- CFO - Director Financiero
- Ejecutivo del Negocio
- CIO - Director de la gestión de la Información
- Dueño del Proceso de Negocio
- Jefe de Operaciones
- Arquitecto en Jefe
- Jefe de Desarrollo
- Jefe de Administración de TI
- PMO - Director de Administración de Proyectos
- Oficial de Cumplimiento, Auditoría, Riesgo y Seguridad

Si analizamos el proceso DS 5 vemos que en la Matriz RACI se definen las actividades inherentes a este, y las mismas son referenciadas a los Involucrados previamente definidos, a través de los diferentes Roles; identificando quienes son los responsables y quienes dan soporte para que cada actividad quede garantida de cumplimiento, generando de este modo un funcionamiento integro del proceso.

Vemos por ejemplo que en la actividad de *Monitorear incidentes de seguridad reales y potenciales* se identifican como Responsables al Jefe de Operaciones, así como también a las personas involucradas en las tareas de Cumplimiento, Auditoria, Riesgo y Seguridad. Además se identifica al CIO - Director de la gestión de la Información como la persona que debe Rendir Cuentas, al Arquitecto en Jefe y al Jefe de Desarrollo como las personas que deben ser Consultadas, y por ultimo al Dueño del Proceso de Negocio como la persona a la cual se debe Informar acerca de la actividad en cuestión.

La gran utilidad de esta herramienta esta en que no da lugar a la existencia de “espacios vacios” en cuanto a la identificación de los principales actores a la hora monitorear el correcto funcionamiento del proceso.

2.4.4 Metas y Métricas

Además del Modelo de Madurez, Cobit cuenta con otra herramienta fundamental para desarrollar uno de sus cuatro pilares, *Impulsado por Mediciones*, la cual se denomina Metas y Métricas.

Esta herramienta esta definida en el Marco en tres niveles:

- Metas y Métricas de TI: buscan realizar mediciones de lo que el negocio espera de TI, a través de estas se obtienen conclusiones respecto a; qué tan alineada está TI con el negocio.
- Metas y Métricas de procesos: determinan lo que el proceso de TI debe generar para dar soporte a los objetivos de TI, en otras palabras se busca medir; qué tan bien se alinea el proceso en la contribución a los objetivos generales.
- Métricas de desempeño de los procesos: miden el desempeño de los procesos con el objetivo de obtener conclusiones acerca de; qué tan real es la consecución de las metas.

En definitiva, las Metas y Métricas pretenden monitorear qué tan bien los procesos satisfacen las necesidades del negocio y de TI.

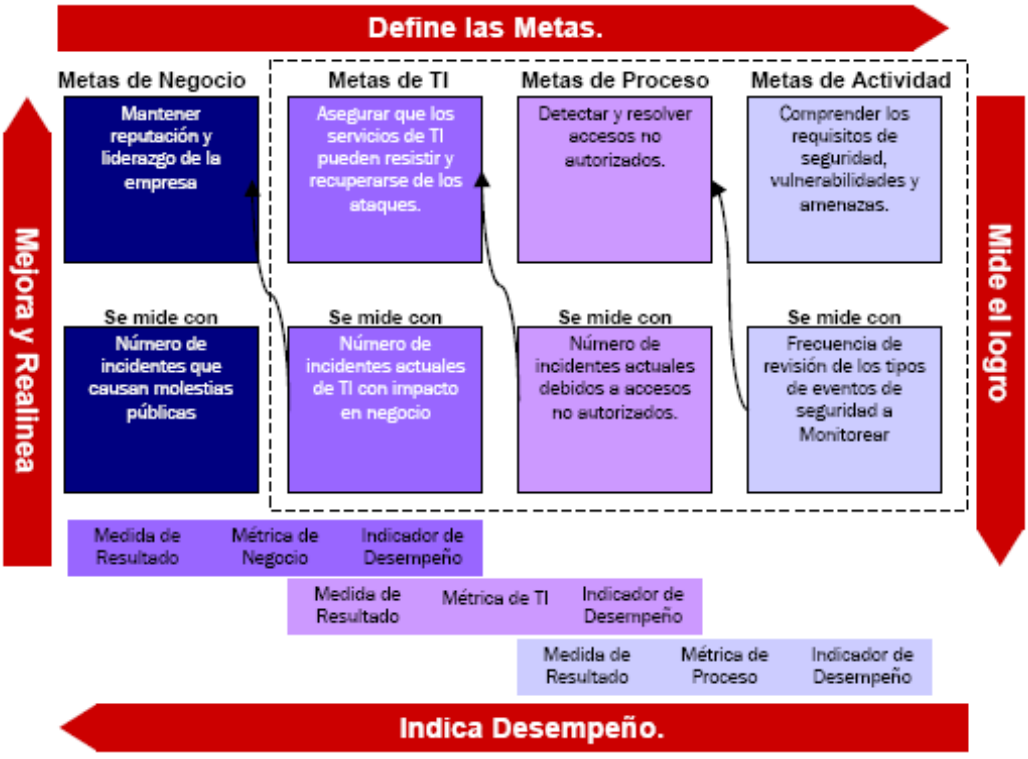
Para entender como son definidas las metas en el Marco, las debemos imaginar como una pirámide que tiene distintos niveles, en la cual cada nivel inferior sustenta a su superior directo. En la parte superior están las metas de negocio, son estas el objetivo principal a alcanzar, por lo que las restantes metas están definidas en función de éstas. Una meta de negocio tiene varias metas de TI, estas dan soporte ya que las metas de TI son un grado inferior a las metas de negocio.

Gráfico 2.4.4.1 - Niveles de las diferentes Metas

Las metas de TI están respaldadas por los procesos definidos en el Marco, por lo tanto a la hora de definir las metas de los procesos se presta especial atención, en que éstos contribuyan a las metas de TI. A su vez las metas de los procesos se sustentan en las metas de actividad, por lo que una meta de procesos esta determinada por varias metas de actividad.

Asimismo nos parece de utilidad, exponer un cuadro que demuestra la relación entre Procesos, Metas y Métricas, para lo cual nos ubicaremos dentro de *DS 5 Garantizar la Seguridad de los Sistemas*, ya que ayuda a una comprensión más cabal de esta herramienta.

Gráfico 2.4.4.2 - Relación entre Procesos Metas y Métricas (DS 5)



En este cuadro se puede apreciar claramente cuáles son los principales cursos de información que proporciona esta herramienta, indicados con flechas rojas.

Como veremos más adelante, Cobit solo proporciona Métricas para la parte que se ubica dentro de la línea punteada.

A continuación enumeramos los elementos que caracterizan a las métricas:

- Tienen una visión apuntada al esfuerzo.
- Son comparables con información interna con información pasada.
- Comparables con información externa sin importar las dimensiones de la empresa.
- Centrarse en unas pocas métricas pero de muy buena calidad.
- Fácil de medir, no confundir con los objetivos.

Para poder lograr este objetivo, Cobit brinda dentro de cada Proceso un cuadro en el cual se exponen las relaciones entre las Metas y Métricas de TI, de los Procesos y las Actividades. Dentro de este cuadro el Marco no desarrolla las Metas de negocio ni sus correspondientes Métricas.

Veamos como son desarrolladas las Metas y Métricas dentro de los procesos AI 6 y DS 5:

Gráfico 2.4.4.3 – Metas y Métricas del Proceso AI 6 - Administrar Cambios

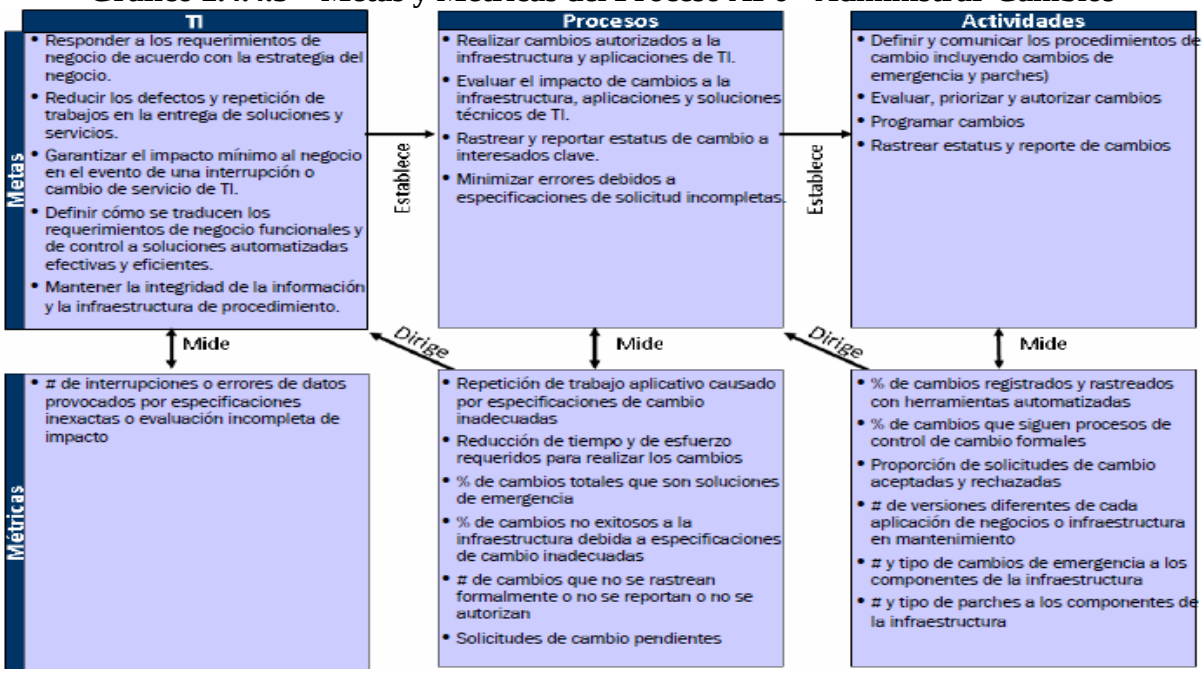
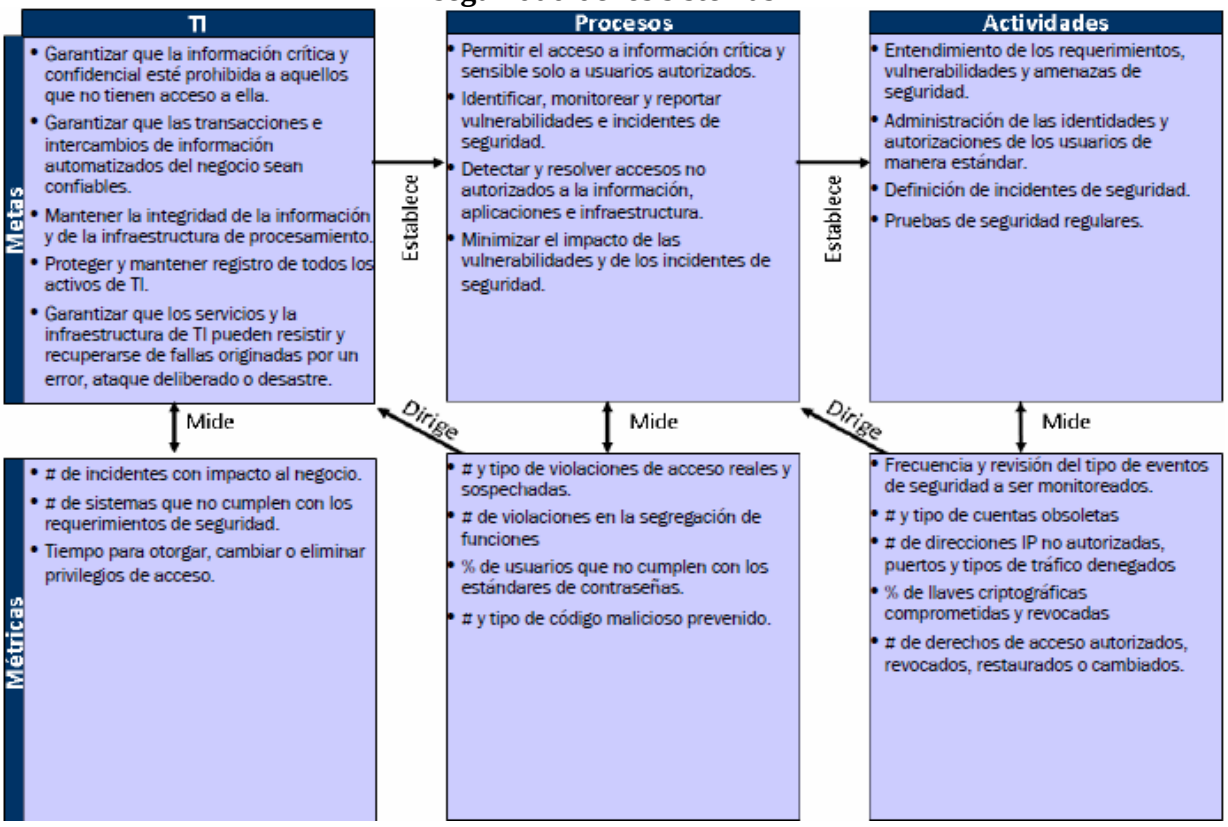


Gráfico 2.4.4.4 – Metas y Métricas del Proceso DS 5 - Garantizar la seguridad de los sistemas



Como se puede apreciar, en estos cuadros se establecen tres tipos de relaciones entre las metas y las métricas dentro de un proceso, las cuales están indicadas con flechas. En primer lugar, vemos que hay una relación entre metas, en la cual las metas de nivel superior "establecen" las metas de nivel inferior, es así que citando el ejemplo de *AI 6 Administrar Cambios*, la meta de actividad "evaluar, priorizar y autorizar cambios", va a estar establecida en función de todas las metas que integren este proceso las cuales aparecen definidas en el cuadro, y funciona de forma análoga con las restantes metas de actividad.

En segundo lugar, vemos que determinadas métricas establecen una relación a través de la cual se "miden" las metas de TI, procesos y actividades, estas son conocidas como medidas de resultados, por lo tanto para cada nivel de metas existen sus correspondientes medidas de resultados. Para el caso de los procesos en cuestión, para el proceso *DS 5 Garantizar Seguridad de los Sistemas*, las metas a nivel de proceso, están medidas por métricas tales como:

- Nº y tipo de violaciones reales y sospechadas,
- Nº de violaciones en la segregación de funciones,
- Porcentaje de usuarios que no cumplen con los estándares de contraseñas,
- Nº y tipo de código malicioso prevenido.

Las medidas de resultados de nivel más bajo se convierten en métricas de desempeño para las metas de mayor nivel. Tenemos que diferenciar ahora dos conceptos que se suelen confundir:

Por un lado tenemos los indicadores de resultados, los cuales brindan mediciones que informan a la gerencia, cuando una función, proceso o actividad de TI ha alcanzado sus metas, estas pueden medirse sólo después de ocurrido el hecho. Por otro lado tenemos los indicadores de desempeño, los cuales definen las medidas que determinan lo bien que el negocio, la función de TI o los procesos de TI se están realizando para que se consigan las metas, son indicadores enfocados en la eficiencia. Estos indicadores eran conocidos anteriormente como KGI´s (Key Goal Indicators) y KPI`s (Key Performance Indicators) respectivamente.

Para ver esto más claramente, en el proceso *AI 6 Administrar Cambios*, "reducir los defectos y repetición de trabajos en la entrega de soluciones y servicios" es una meta para TI, pero se convierte en un indicador de desempeño para las metas del negocio.

Es de aquí que nace la tercera relación marcada en los cuadros cómo "dirige", la cual establece por ejemplo que las métricas de TI son, además de lo expuesto anteriormente, un impulsor del desempeño de las metas de negocio, y lo mismo sucede en los escalones inferiores. Si tomamos como ejemplo *DS 5 Garantizar la Seguridad de los Sistemas*, vemos que las métricas para procesos expuestas anteriormente así como son medidas de resultados para las metas de procesos, son también impulsores de desempeño para las metas de TI.

Podemos entonces concluir que las métricas no solo sirven como una medida de resultado de las metas correspondientes a su nivel directo, sino que también proporcionan un indicador de desempeño para las metas de un nivel superior.

Esta herramienta es sumamente útil, una vez que Cobit ha sido implementado en la organización, ya que es un instrumento de monitoreo.

2.4.5 Entradas y salidas del proceso

Otra de las herramientas con las que cuenta el Marco son las entradas y salidas de procesos, la cual consiste en identificar cuales son las "entradas" que requiere el proceso en análisis de otros procesos, y cuales son las "salidas" que requieren otros procesos del proceso en análisis. En la descripción que se realiza de cada proceso existe un cuadro que muestra el aporte que le brindan otros procesos al proceso en cuestión y el aporte del proceso que estamos analizando sobre los demás procesos.

Como podemos ver la función que cumple esta herramienta es identificar de donde se nutre de información el proceso en cuestión, y a su vez nos permite ver hacia donde brinda información clave.

Ejemplificamos con los cuadros que brinda Cobit de los procesos AI 6 y DS 5:

Cuadro 2.4.5.1 – Entradas y salidas del Proceso AI 6 - Administrar Cambios

Desde	Entradas
PO1	Portafolio de proyectos TI
PO8	Acciones de mejora de la calidad
PO9	Planes de acción para solución de riesgos relacionados con TI
PO10	Directrices de administración de proyecto y plan de proyecto detallado
DS3	Cambios requeridos
DS5	Cambios de seguridad requeridos
DS8	Solicitudes de servicio / solicitudes de cambio
DS9-10	Solicitudes de cambio (dónde y cómo aplicar la solución)
DS10	Registros de problemas

Salidas	Hacia						
Descripción de proceso de cambio	AI1..AI3						
Reportes de estatus de cambio	ME1						
Autorización de cambio	AI7	DS8	DS10				

Cuadro 2.4.5.2 – Entradas y salidas del Proceso DS 5 - Garantizar la Seguridad de los Sistemas

Desde	Entradas
PO2	Arquitectura de Información; clasificación de datos asignados
PO3	Estándares de tecnología
PO9	Evaluación de riesgo
AI2	Especificaciones de controles de seguridad en las aplicaciones
DS1	OLAs

Salidas	Hacia
Definición de incidentes de seguridad	DS8
Requerimientos específicos de entrenamiento sobre conciencia de seguridad	DS7
Reportes de desempeño del proceso	ME1
Cambios de seguridad requeridos	AI6
Amenazas y vulnerabilidades de seguridad	PO9
Políticas y Planes de Seguridad de TI	DS11

Así vemos por ejemplo que un proceso clave de entrada para *Administrar cambios* es el PO9 *Evaluar y administrar los riesgos de TI*, ya que los niveles de riesgos predefinidos y la estrategia de mitigación del riesgo son entradas de información esenciales para una correcta administración de los cambios relacionados con TI. Por otro lado vemos que el Proceso de *Administración de cambios* es esencial como entrada para otros procesos como puede ser el proceso *DS 10 Administración de Problemas*, el cual repercute en acciones como ser la autorización de los cambios.

La gran utilidad de esta herramienta esta en que brinda información sobre el aporte que generan los procesos, entre sí. Al ser un instrumento de consulta, no ahondaremos en él al efectuar el desarrollo de la propuesta de implementación.

2.5 Herramientas Complementarias

Seguidamente expondremos dos herramientas complementarias a los efectos de lograr un mejor análisis, ya que ello redundará en mejores conclusiones.

2.5.1 Prácticas de control

Las prácticas de Control de Cobit se desprenden del documento emitido por el ITGI, Cobit Control Practices en su segunda edición. Este es un documento complementario al Marco Cobit 4.1.

Las Prácticas de Control de Cobit ofrecen una guía más detallada de lo que requiere la Gerencia, Proveedores de servicios, Usuarios finales y Profesionales del ámbito de control interno (Auditores, Controllers, entre otros). Asimismo los ayuda en el diseño de los controles específicos que resulten necesarios.

Proveen Cómo, Porqué y Qué debe ser implementado a los efectos de cada objetivo de control en particular, con la finalidad de mejorar el desempeño y/o proveer soluciones al área de TI, así como dar soporte a la gestión de riesgos.
En definitiva, las Prácticas de Control son una herramienta que provee, para cada uno de los Objetivos de Control detallados incluidos en cada uno de los 34 Procesos identificados por Cobit, una lista de tareas concretas a realizar para lograr ese Objetivo de Control, de modo que le da un enfoque sumamente práctico al sugerir acciones especificas.

De este modo nos ayudan a asegurarnos que las soluciones puestas en práctica sean más factibles y brinden una respuesta consonante con las necesidades de la organización. Asimismo nos orientan, respecto a los riesgos que deben ser tenidos en cuenta.

Los elementos que componen las Prácticas de Control son pautas para generar valor y controlar los riesgos. Las pautas que generan valor, proveen ejemplos sobre beneficios del negocio que pueden derivar del uso de Objetivos de Control en la gestión de la organización. Respecto a las pautas para controlar riesgos, proveen ejemplos de los riesgos que pueden existir.

En ambos casos ayudan a los profesionales del ámbito de control interno y a los responsables del área de TI, en la implementación de mejoras sobre los controles existentes y brindan sustento a los controles que no están mitigando correctamente los riesgos.

En síntesis, cada Práctica de control:

- Plantea un diseño de controles que mantienen vigencia a efectos de los Objetivos de Control.
- Describe una serie de pasos necesarios y suficientes a efectos de alcanzar los Objetivos de Control.

- Esta orientada a la acción.
- Es relevante a los efectos del propósito del Objetivo de Control.
- Considera las actividades, las entradas y salidas del proceso bajo análisis.
- Da sustento a la fijación de roles y responsabilidades asignadas.

Veamos ejemplos con los Procesos que venimos manejando. Comencemos por analizar el Objetivo de Control detallado *AI 6.3 Cambios de Emergencia,* las Prácticas de Control que le dan sustento son las siguientes:

- Asegurarse que dentro del proceso de gestión del cambio, exista un proceso documentado para evaluar, autorizar y registrar un cambio de emergencia.
- Asegurarse que los cambios de emergencia se procesan de acuerdo con las pautas del proceso formal de gestión de cambios.
- Asegurarse que todos los accesos de emergencia para realizar cambios estén debidamente autorizados, documentados y sean revocados una vez aplicado el cambio.
- Realizar una revisión post-implantación a todos los cambios de emergencia, involucrando a todos los interesados. Esta revisión debe considerar aspectos tales como la mejora en el mantenimiento de las aplicaciones del sistema, calidad en el desarrollo de software, documentación y manuales, e integridad de los datos.

Pasemos ahora a analizar el Objetivo de Control detallado *DS 5.11 Intercambio de datos sensibles,* las Prácticas de Control que lo sustentan son las siguientes:

- Determinar mediante el esquema establecido de clasificación de información, cómo deben ser protegidos los datos cuando se intercambian.
- Utilizar controles de aplicación, con la finalidad de proteger el intercambio de datos.
- Utilizar controles de infraestructura, basados en la clasificación de información y la tecnología en uso, para proteger el intercambio de datos.

De este modo vemos la gran utilidad de las Prácticas de Control, ya que mediante esta herramienta tenemos un enfoque práctico sobre los aspectos que debemos incorporar en la gestión a efectos de lograr los Objetivos de Control y por lo tanto mejorar el desempeño de los Procesos del Marco Cobit dentro de la organización.

2.5.2 Análisis de valor

Esta herramienta la confeccionamos a partir del Apéndice 1 de Cobit 4.1. Brinda una visión global de cómo se relacionan las Metas genéricas del negocio con las Metas de TI y con los Procesos de TI.

Resulta ser sumamente útil, ya que nos brinda la posibilidad de trabajar con la Dirección-Gerencia de la organización, utilizando conceptos que aluden a la gestión y gerenciamiento en una terminología clara y de fácil entendimiento; ya que a través de una ponderación y ordenamiento de las Metas del Negocio y las Metas de TI, logramos identificar los Procesos del Marco Cobit que más valor agregan a la gestión de TI dentro de la organización.

La misma se compone de un Cuadro de Mando Integral en el que se enumeran una serie de Metas genéricas del Negocio, asimismo se incluye un cuadro con Metas de TI, en otro cuadro se vinculan las Metas del Negocio y las de TI y por último encontramos un cuadro en que se detallan los Proceso de Cobit que dan soporte al logro de las Metas de TI. A los efectos de visualizar estos cuadros y de evitar ser reiterativos, los exponemos dentro del práctico en el numeral *3.2.4 Análisis de valor*.
Los cuadros ayudan a demostrar el alcance de Cobit y la relación general de negocio entre Cobit y los impulsores del negocio, permitiendo así establecer la equivalencia entre las metas típicas de negocio, por medio de las metas de TI, y los procesos de TI requeridos para dales soporte. Los cuadros se basan en metas genéricas y, por tanto, se deben usar como guía y adaptarse a la organización en cuestión.

3. DESARROLLO DE LA PROPUESTA DE IMPLEMENTACION

Partiendo de la base de que no hay una metodología de aplicación generalizada para la implementación de Cobit, entendemos importante avanzar hacia el desarrollo de una de ellas. A tales efectos, nos proponemos combinar buenas prácticas de gestión de proyectos, conjuntamente con las herramientas que plantea el Marco, así como con la experiencia personal en consultoria.

Buscamos con el presente trabajo exponer una PROPUESTA DE IMPLEMENTACION DEL MARCO DE GESTION COBIT, para lo cual ejemplificaremos con datos hipotéticos. Vamos a agrupar las tareas en 3 etapas, la primera de ellas de Introducción y Capacitación y Planificación, la siguiente de Ejecución de actividades y por último la Gestión de las oportunidades de mejora seleccionadas en la etapa anterior.

3.1 Primera Etapa – Introducción, Capacitación y Planificación

Al iniciar la propuesta, debemos tener presente que el éxito de la implantación depende enormemente del apoyo y entusiasmo que se despierte en los involucrados, por lo tanto es importante lograr la adhesión del personal, así como también un buen entendimiento de su parte respecto al alcance y los objetivos perseguidos.

Por consiguiente, en esta etapa es necesario realizar una presentación del proyecto y una introducción al Marco de gestión, con el propósito de involucrar al personal que formará parte del mismo. Luego nos planteamos llevar adelante una capacitación de los involucrados, así como crear un Comité para el seguimiento del proyecto y definir el alcance de las actividades a ser ejecutadas, en aras de elaborar una planificación de tareas y plazos. Por último, asignaremos los propietarios a los diferentes procesos del Marco, a los efectos de identificar responsables y poder comenzar a trabajar en la etapa siguiente.

3.1.1 Presentación del Proyecto

El primer paso para dar comienzo al proyecto es realizar una breve presentación, dirigida a los involucrados, sobre los motivos por los cuales la organización pone en marcha dicho proyecto, con el objetivo de mostrar:

a) Las razones que han llevado a la organización a implementar el Marco Cobit.
b) Los objetivos que se pretenden alcanzar a través del proyecto.
c) El esquema de trabajo que se pretende seguir durante la ejecución del proyecto.
d) Delimitar las responsabilidades de los diferentes involucrados.

Posibles involucrados

Director del departamento de TI
Gerente de Sistemas
Gerente de Proyectos relacionados con TI
Gerente de Gestión de la información
Encargado de Soporte Técnico
Encargado de Redes
Encargado de Sistemas
Encargado de Ejecución de proyectos
Responsable de Seguridad de TI

3.1.2 Introducción al Marco de Gestión

En esta instancia buscamos dar una visión general sobre el Marco, exponiendo sus caracteres más importantes a efectos de mostrar su utilidad como herramienta de gestión. Para ello resulta útil plantear las siguientes interrogantes.

¿Cuáles son sus características?

- Provee buenas prácticas a través de un marco que se descompone en Dominios y Procesos
- Presenta las actividades en una estructura lógica y ordenada

• Esta fuertemente orientado a los controles más que a la ejecución de las actividades

• Se enfoca en lo que es necesario para lograr un adecuado Gerenciamiento y Control de TI

• Está alineado con otros Estándares y Buenas Practicas de TI, más detallados

¿En que contribuye la utilización del Marco?

Brinda soporte al Gerenciamiento de TI, a través de un marco. Ello contribuye a asegurarse que:

• TI esta alineada con el negocio

• TI da soporte al negocio y contribuye a maximizar los beneficios

• Los recursos de TI se utilizan de modo responsable

• Los riesgos de TI se gestionan apropiadamente

¿Qué ventajas y beneficios brinda incorporar el Marco?

El Marco Cobit brinda apoyo a los requisitos del negocio, debido a que:

- Los procesos del marco están directamente relacionados con los objetivos del negocio.
- Organiza las actividades de TI dentro de un esquema de procesos.
- Identifica los recursos críticos de TI a efectos de ser considerados en las oportunidades de mejora a implementar.
- Gerencia los objetivos de control que deben ser tenidos en cuenta.

Asimismo presenta beneficios, tales como:

- Debido a que en su constitución se buscó un enfoque en el negocio, presenta una mejor alineación que otros Marcos.
- Brinda una clara visión a la Gerencia respecto a lo que compete al área de TI.
- Una clara asignación de responsabilidades e identificación de propietarios de activos, debido a que se desarrolla en base a procesos.
- Un lenguaje común lo que permite un entendimiento por parte de todos los involucrados (desde Accionistas hasta Empleados de la organización).
- Esta alineado con otros Estándares y Marcos de Gestión (COSO, ITIL, ISO).

¿Con que Normas y Estándares de Gestión se relaciona?

Ver Anexo 2 - Relacionamiento con otros Marcos y Estándares.

Otras interrogantes, que es útil tener en cuenta son las siguientes:

- Como podemos asegurarnos que el Departamento de Tecnología satisface lo que la organización demanda?	COBIT facilita la alineación de: - Mapas de calor basados en análisis de valor y evaluaciones de riesgo. - Vincula los objetivos de la organización con los objetivos del departamento de tecnología y con los procesos de dicho departamento.
- Como podemos satisfacer la mejora en los servicios del Depto de Tecnología?	- A través de Marcos de Gestión que han sido ampliamente utilizados en todo el mundo.
- Que estamos haciendo? Lo estamos haciendo apropiadamente? Nos hemos focalizado en los aspectos correctos? Que deberíamos estar haciendo?	- COBIT presenta 34 procesos que cubren el ciclo complete del ciclo de vida del gerenciamiento de TI. - El Marco ITIL esta totalmente alineado.
- Quien es el propietario de los procesos en nuestra organización?	- A través de los dueños de los diferentes procesos.
- Quien esta involucrado y en qué?	- A través de la utilización de la Matriz RACI obtendremos una respuesta.
- Qué tan maduros están estos procesos en nuestra organización?	- Para ello se realizan las evaluaciones de madurez de los procesos y se realiza la definición de la situación inicial.
- Cual es la brecha actual? Que debemos hacer a efecto de mejorar el proceso bajo análisis?	- Comparación a nivel de madurez de procesos y objetivos de control entre nivel actual y metas. - Realización de evaluaciones sobre análisis de valor y observaciones de auditoria a

	efectos de identificar oportunidades de mejora.
- Como se están alcanzando las metas de nivelen cada proceso?	- Niveles de las métricas (metas-procesos-actividades)

3.1.3 Capacitación de los involucrados

Luego de la introducción al Marco, proponemos comenzar con la capacitación de los involucrados, quienes serán en su mayoría integrantes del Departamento de TI, además puede resultar recomendable brindar capacitación a otros individuos que por su rol dentro de la organización requieran tener conocimiento sobre el Marco y la propuesta.

Para ello es importante tener presente los conceptos descriptos anteriormente en el desarrollo del *2 - Marco Conceptual* del presente trabajo, precisamente en;

2.2 Funcionamiento General
2.3 Descripción de Dominios y Procesos
2.4 Herramientas a utilizar para Analizar los Procesos
2.5 Herramientas Complementarias

A los efectos de lograr un mejor entendimiento por parte de los participantes, la presentación debe ser clara y redactarse en un lenguaje de fácil entendimiento, evitando tecnicismos innecesarios. Es importante dar lugar a la aclaración de dudas, por lo cual es necesario al finalizar cada capítulo plantear dicha instancia.

3.1.4 Crear un Comité de Seguimiento del proyecto

A los efectos de realizar un seguimiento al proyecto y crear un ámbito de intercambio de ideas y propuestas de ajuste es conveniente definir un Comité de Seguimiento.
Respecto a los integrantes del Comité es recomendable involucrar al Director del departamento de TI, Gerente de Sistemas, Gerente de Proyectos relacionados con TI,

Gerente de Gestión de la información, y puede ser útil invitar a otros individuos que por los temas bajo análisis pueden realizar un aporte valioso.

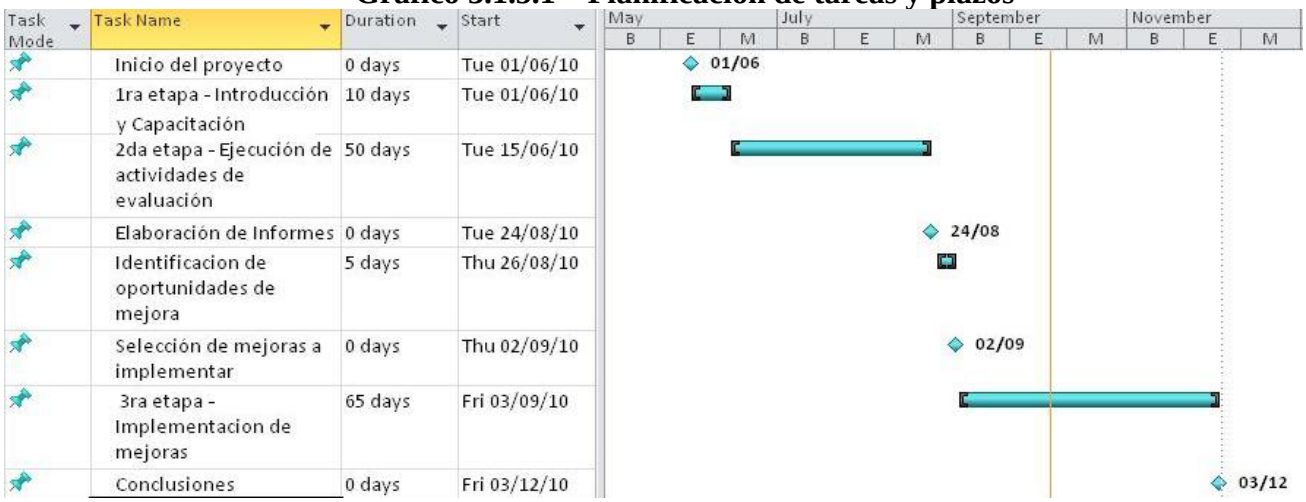
Dicho Comité debe reunirse con una periodicidad tal que sea de utilidad a los fines implícitos en su creación, por ejemplo quincenal o mensualmente.

Es conveniente que haya una comunicación fluida entre los diferentes participantes, por lo tanto es útil la utilización de cuentas de correo electrónico, ya que es un medio de comunicación formal de fácil utilización y de rápida entrega.

3.1.5 Definir el alcance de las actividades a llevar a cabo y elaborar una planificación de tareas y plazos

Una vez que se ha establecido el Comité de Seguimiento, es necesario elaborar una planificación para la propuesta de implementación, la cual es fundamental que contenga una estimación sobre la duración de las diferentes actividades que requerirá, así como una definición del alcance de las mismas y una consideración los recursos (personas, información, aplicaciones e infraestructura) necesarios para llevarlas adelante.
A efectos de obtener una visión integral de dichas actividades, utilizamos un gráfico, ya que nos ayuda a visualizar las actividades, su duración y el avance que se ha logrado sobre estas.
Exponemos a continuación un ejemplo.

Gráfico 3.1.5.1 – Planificación de tareas y plazos



3.1.6 Asignación de Propietarios a los Procesos del Marco

Antes de finalizar esta primera etapa, es importante identificar a los Propietarios (Accountable, quien debe rendir cuentas por el proceso) y a los Responsables de cada proceso dentro del Marco ya que serán estas, las personas con las cuales se realizará la Evaluación inicial de los procesos en la etapa siguiente. Ahora bien, para identificarlos resulta de utilidad elaborar una planilla como la que presentamos a continuación.

Cuadro 3.1.6.1 – Asignación de propietarios a los Procesos del Marco

Dominios	Procesos	A que Departamento compete el proceso?				El proceso está auditado?	Qué documentación de respaldo hay para el proceso?	Propietario del proceso (Accountable, quien debe rendir cuentas por el proceso)
		Depto de TI	Otro Depto	Está tercerizado	Se desconoce ó No aplica			
Planificar y Organizar								
	PO 1 Definir el plan estratégico de TI							
	PO 2 Definir la arquitectura de la información							
	PO 3 Determinar la dirección tecnológica							
	PO 4 Definir procesos, organización y relaciones de TI							
	PO 5 Administrar la inversión en TI							
	PO 6 Comunicar las aspiraciones y la dirección de la gerencia							
	PO 7 Administrar recursos humanos de TI							
	PO 8 Administrar calidad							
	PO 9 Evaluar y administrar riesgos de TI							
	PO 10 Administrar proyectos							

Adquirir e Implementar								
	AI 1 Identificar soluciones automatizadas							
	AI 2 Adquirir y mantener el software aplicativo							
	AI 3 Adquirir y mantener la infraestructura tecnológica							
	AI 4 Posibilitar la operación y el uso							
	AI5 Adquirir recursos de TI							
	AI6 Administrar cambios							
	AI7 Instalar y acreditar soluciones y cambios							
Entregar y Dar soporte								
	DS1 Definir y administrar niveles de servicio							
	DS2 Administrar servicios de terceros							
	DS3 Administrar desempeño y capacidad							
	DS4 Garantizar la continuidad del servicio							
	DS5 Garantizar la seguridad de los sistemas							
	DS6 Identificar y asignar costos							
	DS7 Educar y entrenar a los usuarios							
	DS8 Administrar la mesa de servicio y los incidentes							
	DS9 Administrar la configuración							
	DS10 Administrar los problemas							
	DS11 Administrar los datos							
	DS12 Administrar el ambiente físico							
	DS13 Administrar las operaciones							

Monitorear y Evaluar							
ME1 Monitorear y evaluar el desempeño de TI							
ME2 Monitorear y evaluar el control interno							
ME3 Garantizar el cumplimiento regulatorio							
ME4 Proporcionar gerenciamiento de TI							

A los efectos de ser completada es necesario reunirse con la Dirección y los Gerentes del Departamento de TI a modo de identificar: A qué departamento dentro de la organización compete administrar cada Proceso, y Quién es el propietario de dicho Proceso.

Luego de identificados los propietarios de los Procesos, debemos consultar si han sido objeto de auditorias y si hay documentación que evidencie los requerimientos que plantea el Marco, ya que podríamos recabar información útil para el desarrollo del numeral *3.2.2 Revisión de las observaciones y recomendaciones de auditoria.*

3.2 Segunda Etapa - Ejecución de actividades de evaluación

Luego de involucrado el personal dentro del contexto del Marco, estamos en condiciones de comenzar a ejecutar las actividades de evaluación; las cuales ejecutaremos básicamente a través de las herramientas citadas anteriormente en este trabajo, con el fin de identificar cuales serán los Procesos que resultarán seleccionados para la posterior búsqueda de oportunidades de mejora.
A tales efectos debemos realizar una evaluación inicial de los Procesos con quienes hayan sido identificados como Responsables al final de la etapa anterior, así como una revisión de las observaciones y recomendaciones de auditoria y una revisión de los riesgos existentes.
Luego nos planteamos llevar a cabo un análisis de valor de los Procesos a efectos de identificar aquellos que más aportan al logro de las Metas del Negocio y de TI dentro de la organización. Por último, para finalizar esta etapa nos planteamos seleccionar los Procesos para trabajar en la etapa siguiente.

3.2.1 Evaluación inicial de los Procesos

En esta instancia el objetivo es relevar la situación en que se encuentra la organización frente a los criterios que establece el Marco Cobit en sus herramientas.

La tarea consiste en trabajar conjuntamente con los Propietarios de los Procesos identificados en la etapa anterior y realizar una evaluación de cada Proceso.
De las diversas herramientas que citamos en *2.4 - Herramientas a Utilizar para Analizar los Procesos,* utilizaremos;

a) Modelo de madurez, ya que nos permite una rápida identificación del nivel de madurez en que se encuentra la organización, así como la posibilidad de fijar un nivel objetivo de madurez a alcanzar e identificar la brecha existente así como las potenciales mejoras a ser consideradas posteriormente en la Tercera Etapa.

Para llevar a cabo este análisis utilizamos la escala de madurez que se incluye dentro de cada Proceso. Vamos revisando los diferentes niveles comenzando por el nivel 0 y subiendo de nivel hasta llegar a aquel en cual los aspectos más relevantes, no se verifiquen. Por lo tanto la madurez de ese Proceso se encuentra en el nivel inmediato anterior a aquel en que no se verificaron los aspectos más relevantes. A los efectos de visualizar el resultado de este análisis suponemos los siguientes resultados.

Cuadro 3.2.1.1 - Resultado del análisis de los Niveles de madurez

Proceso	Nivel según evaluación inicial	Nivel objetivo	Brecha	Propietario del proceso
PO1	2	3	1	
,,,	1	3	2	
,,,	2	5	3	
,,,	2	5	3	
PO10	2	4	2	
AI1	2	3	1	
,,,	2	3	1	
AI 7	1	2	1	
DS1	2	4	2	
,,,	2	4	2	
DS7	2	4	2	
ME1	2	4	2	
…	2	4	2	
…	2	3	1	
ME4	2	5	3	

b) Objetivos de control, son un elemento fundamental para relevar el Ambiente de Control de TI existente en la organización, lo cual contribuya al Control Interno de la organización.

Con este ejercicio se busca evaluar el nivel de cumplimiento de cada uno de los Objetivos de control dentro de cada Proceso, para ello analizamos detenidamente cada Objetivo de control a modo de cuestionario.

En definitiva para cada Objetivo de control se plantea la evaluación de los aspectos que lo describen, a través de una serie de preguntas con las cuales se busca verificar la existencia y la

integridad de los controles. En caso de verificar que hay controles que la organización no los ha implementado o los ha implementado parcialmente, es útil tomar nota a efectos de su consideración posterior como oportunidad de mejora.

Para poder realizar una evaluación de las respuestas obtenidas, les asignaremos puntajes a cada una de ellas en función de una escala, de modo de poder cuantificarlas y poder hacer una comparación entre los resultados obtenidos en los diferentes Procesos. Cabe acotar que la cantidad de preguntas formuladas, así como la escala de puntajes utilizada, es a nuestro entender válida por su simplicidad pero no hay un criterio único y excluyente, sino que pueden fijarse como la organización lo estime conveniente o bien a sugerencia del Consultor. Sí es importante que una vez definida la escala, se utilice la misma para realizar la evaluación de cada uno de los Procesos de modo de no perder de vista la relación existente entre los resultados que se obtienen.

A modo de ejemplo nos hemos fijado la siguiente escala:

Respuesta	Puntaje asignado
Cumple plenamente	4
Cumple parcialmente	2,5
No se cumple	1
No aplica	-

A los efectos de plantear el desarrollo de este análisis, seleccionamos el proceso *AI 6 Administrar Cambios*, para desarrollar este análisis. Este proceso tiene cinco Objetivos de control detallados:

- AI 6.1 Estándares y Procedimientos para Cambios
- AI 6.2 Evaluación de Impacto, Priorización y Autorización
- AI 6.3 Cambios de Emergencia
- AI 6.4 Seguimiento y Reporte del Estatus de Cambio
- AI 6.5 Cierre y Documentación del Cambio

A su vez, para cada uno de estos Objetivos se incluye una descripción que le da contenido al Objetivo de control. Por ejemplo, para el AI 6.1 Estándares y Procedimientos para Cambios,

el Marco indica lo siguiente *"Establecer procedimientos de administración de cambio formales para manejar de manera estándar todas las solicitudes (incluyendo mantenimiento y parches) para cambios a aplicaciones, procedimientos, procesos, parámetros de sistema y servicio, y las plataformas fundamentales."*

Por lo tanto para evaluar este objetivo de control, se formulan preguntas como las que se citan a continuación:

1- ¿Se han incorporado procedimientos formales de control de cambios?
2- ¿Dichos procedimientos permiten un manejo estandarizado de todas las solicitudes de cambio?

Las respuestas posibles son las que mencionamos anteriormente. Una vez completado el cuestionario debemos obtener el puntaje de cada Objetivo de Control para luego obtener el promedio de todos los Objetivos de Control que corresponden a ese Proceso.

Si suponemos que las respuestas para el Objetivo de control detallado AI 6.1 fueran las siguientes:

Pregunta 1 – Cumple parcialmente	2.5
Pregunta 2 - No se cumple	1
Tendríamos, que en total suman	**3.5**

Luego, para obtener el puntaje individual de este Objetivo de control detallado, dividimos el resultado anterior entre el total de respuestas (en este caso 2)

"suma de respuestas/ total de respuestas": 3.5 / 2 = **1.75**

Por lo tanto el puntaje del objetivo de control AI6.1 es 1.75

Una vez evaluados todos los Objetivos de control detallados y obtenidos los puntajes individuales, debemos calcular el puntaje global para los Objetivos de control de ese Proceso. Suponiendo que los puntajes individuales fueran los siguientes:

AI 6.1	1.75
AI 6.2	1
AI 6.3	2.5
AI 6.4	2.5
AI 6.5	2.5
Obtendríamos un total de	**10.25**

El resultado anterior lo dividimos entre el total de Objetivos de control detallados del Proceso analizado, de modo de obtener un resultado promedio, comparable con los demás Procesos.

"suma de puntajes de objetivos de control/ total de controles": 10.25 / 5 = **2.05**

Aquí obtenemos el valor global de los Objetivos de control para ese proceso: 2.05 en una escala de 1 a 4.

Es importante aclarar que en caso de responder "No aplica" debe quedar constancia de los argumentos por los cuales ese control no es aplicable a la organización, y debemos tener presente a la hora de realizar los cálculos que ese control que no aplica no se incluye ni en la suma de puntajes (tiene valor cero) ni dentro del divisor.

Luego de efectuada la evaluación de los Objetivos de Control para cada proceso, se elabora un cuadro en el que se compilan los puntajes obtenidos, ello permite visualizar el nivel de cumplimiento de los Controles para cada Proceso y permite comparar los resultados entre Procesos. Suponemos los siguientes resultados.

Cuadro 3.2.1.2 – Resultado del análisis de los Objetivos de control

Proceso	Puntaje
AI5 Adquirir recursos de TI	3,98
PO8 Administrar calidad	3,79
DS2 Administrar servicios de terceros	3,63
AI2 Adquirir y mantener el software aplicativo	3,55
DS4 Garantizar la continuidad del servicio	3,44
PO10 Administrar proyectos	3,17
DS7 Educar y entrenar a los usuarios	3,17
ME3 Garantizar el cumplimiento regulatorio	3,1
PO6 Comunicar las aspiraciones y la dirección de la gerencia	3,05
PO1 Definir el plan estratégico de TI	2,92
AI7 Instalar y acreditar soluciones y cambios	2,92
AI1 Identificar soluciones automatizadas	2,88
AI4 Posibilitar la operación y el uso	2,88
DS10 Administrar los problemas	2,81
PO7 Administrar recursos humanos de TI	2,78
DS11 Administrar los datos	2,75
ME2 Monitorear y evaluar el control interno	2,71
AI3 Adquirir y mantener la infraestructura tecnológica	2,69
DS8 Administrar la mesa de servicio y los incidentes	2,65
ME4 Proporcionar gerenciamiento de TI	2,64
PO9 Evaluar y administrar riesgos de TI	2,63
PO5 Administrar la inversión en TI	2,61
PO4 Definir procesos, organización y relaciones de TI	2,56
DS6 Identificar y asignar costos	2,5
DS12 Administrar el ambiente físico	2,5
PO2 Definir la arquitectura de la información	2,25
PO3 Determinar la dirección tecnológica	2,25
DS3 Administrar desempeño y capacidad	2,25
DS13 Administrar las operaciones	2,15

ME1 Monitorear y evaluar el desempeño de TI	2,10
DS1 Definir y administrar niveles de servicio	2,10
DS9 Administrar la configuración	2,08
AI6 Administrar cambios	**2,05**
DS5 Garantizar la seguridad de los sistemas	**1,5**

A partir de estos resultados, vemos que en los Procesos AI6 y DS5 seria recomendable realizar un análisis de los controles existentes y plantear las mejoras que fuera posible incorporar. Por otro lado, resultados tan cercanos a 4, como el caso de AI5, PO8, DS2 y AI2 es importante solicitar evidencia que le de sustento a lo que manifiestan. (Recordar que la escala de puntajes va de 1 a 4).

c) Matriz RACI, establece las Actividades que es necesario ejecutar para llevar a cabo el Proceso así como los diferentes Involucrados en dichas Actividades. Del cruzamiento de Actividades e Involucrados surgen los Roles esperados de los diversos integrantes de la organización, ya sea Consultado, Informado, etc.

A partir de la información incluida en esta herramienta buscamos evaluar el nivel de cumplimiento de las Actividades que integran el Proceso, para ello proponemos una escala y evaluamos el nivel de cumplimiento.

Los comentarios respecto a las escalas volcados anteriormente al tratar los Objetivos de control son válidos aquí también.

Escala sugerida a efectos de llevar a cabo la evaluación:

Respuesta	Puntaje asignado
Excelente	5
Muy bueno	4
Satisfactorio	3
Regular	2
Pobre	1

Para mostrar el uso de esta Matriz, utilizamos el Proceso AI 6 Administrar cambios, dentro del cual el Marco nos plantea las siguientes Actividades:

a) Desarrollar e implementar un proceso para registrar, evaluar y dar prioridad en forma consistente a las solicitudes de cambio.

b) Evaluar impacto y dar prioridad a cambios en base a las necesidades del negocio.
c) Garantizar que cualquier cambio crítico y de emergencia sigue el proceso aprobado.
d) Autorizar cambios.
e) Administrar y diseminar la información relevante referente a cambios.

En primer lugar, debemos evaluar el nivel de desempeño de cada una de ellas en base a la escala presentada anteriormente, suponiendo que las respuestas fueran las siguiente obtenemos los correspondientes puntajes.

Actividad	Respuesta	Puntaje asignado
a)	Regular	2
b)	Satisfactorio	3
c)	Regular	2
d)	Satisfactorio	3
e)	Satisfactorio	3
TOTAL		**13**

Una vez obtenido el total debemos calcular el puntaje de la Matriz RACI para el Proceso en cuestión, dividiendo el resultado anterior entre el total de actividades de la Matriz para ese proceso: 13 / 5 = **2.6** (en una escala de 1 a 5). De este modo obtenemos un resultado promedio, comparable con el resto de los Procesos.

Al igual que en el caso de los Objetivos de Control, luego de efectuada la evaluación de las Actividades para cada Proceso, se elabora una planilla en la que se compilan los puntajes obtenidos, ello permite visualizar el desempeño vigente de las diferentes actividades necesarias para cada Proceso y permite comparar los resultados entre Procesos. A tales efectos suponemos los siguientes resultados.

Cuadro 3.2.1.3 – Resultado del análisis de Matriz RACI

Proceso	Puntaje
PO7 Administrar recursos humanos de TI	4
AI5 Adquirir recursos de TI	4
DS2 Administrar servicios de terceros	3.83
AI3 Adquirir y mantener la infraestructura tecnológica	3.5
PO10 Administrar proyectos	3.43
ME4 Proporcionar gerenciamiento de TI	3.2
PO1 Definir el plan estratégico de TI	3
AI4 Posibilitar la operación y el uso	3
DS7 Educar y entrenar a los usuarios	3
DS4 Garantizar la continuidad del servicio	2.89

AI2 Adquirir y mantener el software aplicativo	2.88
DS10 Administrar los problemas	2.83
PO4 Definir procesos, organización y relaciones de TI	2.8
DS11 Administrar los datos	2.8
AI1 Identificar soluciones automatizadas	2.75
AI7 Instalar y acreditar soluciones y cambios	2.67
DS3 Administrar desempeño y capacidad	2.67
DS8 Administrar la mesa de servicio y los incidentes	2.67
PO3 Determinar la dirección tecnológica	2.6
DS9 Administrar la configuración	2.5
PO8 Administrar calidad	2.4
DS12 Administrar el ambiente físico	2.4
PO9 Evaluar y administrar riesgos de TI	2.3
DS13 Administrar las operaciones	2.29
PO5 Administrar la inversión en TI	2.2
DS1 Definir y administrar niveles de servicio	2
DS6 Identificar y asignar costos	2
ME3 Garantizar el cumplimiento regulatorio	2
ME2 Monitorear y evaluar el control interno	1.86
PO2 Definir la arquitectura de la información	1.8
PO6 Comunicar las aspiraciones y la dirección de la gerencia	1.67
ME1 Monitorear y evaluar el desempeño de TI	1.6
AI6 Administrar cambios	**1.2**
DS5 Garantizar la seguridad de los sistemas	**1.1**

A partir de estos resultados, vemos que en los Procesos AI6 y DS5 seria recomendable realizar un análisis de las actividades que se ejecutan y plantear las mejoras que fuera posible incorporar. Recordar que en este caso la escala de puntajes va de 1 a 5.

3.2.2 Revisión de las Observaciones y Recomendaciones de Auditoria

Para realizar esta tarea se solicitan a la organización:

- Informe de la Auditoria de Sistemas (Auditores Externos)
- Informes de los Auditores Internos de Sistemas, cuyo objeto de revisión refiera a:
    a) Cumplimiento de normativa y regulación legal
    b) Cumplimiento y desempeño de procedimientos de la organización

Una vez que tenemos esta información, debemos identificar con que Procesos del Marco más se relacionan las Observaciones y Recomendaciones existentes. Seguidamente planteamos un

ejemplo, en el cual pueden observarse en una columna las Observaciones y Recomendaciones de Auditoria y en otra los Procesos Cobit que identificamos como más relacionados con dichas Observaciones y Recomendaciones.

Cuadro 3.2.2.1 – Identificación de Procesos Cobit relacionados con las recomendaciones y observaciones de Auditoria

	Observación/ Recomendación de Auditoria	**Procesos COBIT relacionados**
a	Seguridad de los Documentos y Archivos - las claves de acceso deben ser cambiadas regularmente para mejorar la seguridad de los registros.	DS 5
b	Destrucción de Documentos y Archivos - asegurarse que los miembros del personal asistan a la capacitación en gestión de documentos, para asegurarse de que son conscientes de los riesgos que conlleva mantener la información durante un plazo de tiempo mayor al que se establece como necesario.	DS 5
c	La Política de Administración de Documentos debe tratar la temática que refiere al Ambiente físico necesario para el Almacenamiento - esta política debe incluir detalles en cuanto a como deben ser almacenados a fin de cumplir con la regulación existente en materia de prevención de incendios.	DS 5 - DS 11
d	Deben aplicarse controles de cambio a los cambios funcionales de las aplicaciones desarrolladas.	AI 6 - AI 2

Una vez finalizada la identificación de procesos relacionados, pasamos a elaborar un cuadro de resumen en el que exponemos la cantidad de veces que cada Proceso aparece asociado a observaciones y/o recomendaciones de auditoria. A tales efectos suponemos los resultados siguientes.

Cuadro 3.2.2.2 – Resultado del análisis de las observaciones y recomendaciones de Auditoria

Proceso	**Obs. y/o Rec.**	
	Cant.	**%**
DS5 Garantizar la seguridad de los sistemas	23	26%
PO10 Administrar proyectos	15	17%
AI2 Adquirir y mantener el software aplicativo	7	8%
DS8 Administrar la mesa de servicio y los incidentes	7	8%
AI1 Identificar soluciones automatizadas	6	7%
PO6 Comunicar las aspiraciones y la dirección de la gerencia	5	6%
AI7 Instalar y acreditar soluciones y cambios	5	6%
DS4 Garantizar la continuidad del servicio	3	3%
DS12 Administrar el ambiente físico	3	3%

PO9 Evaluar y administrar riesgos de TI	2	2%
DS1 Definir y administrar niveles de servicio	2	2%
DS11 Administrar los datos	2	2%
DS13 Administrar las operaciones	2	2%
PO1 Definir el plan estratégico de TI	1	1%
PO5 Administrar la inversión en TI	1	1%
AI6 Administrar cambios	1	1%
DS9 Administrar la configuración	1	1%
DS10 Administrar los problemas	1	1%
ME2 Monitorear y evaluar el control interno	1	1%
ME3 Garantizar el cumplimiento regulatorio	1	1%
PO2 Definir la arquitectura de la información	0	0%
PO3 Determinar la dirección tecnológica	0	0%
PO4 Definir procesos, organización y relaciones de TI	0	0%
PO7 Administrar recursos humanos de TI	0	0%
PO8 Administrar calidad	0	0%
AI3 Adquirir y mantener la infraestructura tecnológica	0	0%
AI4 Posibilitar la operación y el uso	0	0%
AI5 Adquirir recursos de TI	0	0%
DS2 Administrar servicios de terceros	0	0%
DS3 Administrar desempeño y capacidad	0	0%
DS6 Identificar y asignar costos	0	0%
DS7 Educar y entrenar a los usuarios	0	0%
ME1 Monitorear y evaluar el desempeño de TI	0	0%
ME4 Proporcionar gerenciamiento de TI	0	0%

Total	**89**	**100%**

A partir de este cuadro podemos concluir cuales son los procesos del Marco en los que nos debemos focalizar en aras de disminuir la cantidad de observaciones y recomendaciones de Auditoria. En definitiva, incorporar mejoras en la gestión asociadas a esos procesos repercutirá de modo ampliamente favorable sobre el desempeño del área de TI.

En esta instancia es posible realizar también un Análisis desagregado de importancia del Proceso, a efectos de las diferentes Obs./ Rec. - para ello consideramos por ejemplo hasta tres Procesos (en primer lugar corresponde el proceso que más contribuye a mejorar lo planteado en la observación/ recomendación, en segundo lugar aquél que aporta medianamente y en tercer lugar aquél que menos aporta) y lo que hacemos es considerar las veces que los Procesos aparecen en primer lugar, en segundo lugar o en tercer lugar asociados a las diferentes Obs./Rec. Suponiendo los resultados, planteamos, una tabla como la siguiente:

Cuadro 3.2.2.3 – Resultado del análisis de las observaciones y recomendaciones de Auditoria (desagregado)

Proceso	Cantidad de Observaciones y Recomendaciones 1er	2do	3er	TOTAL Cant.	%
DS5 Garantizar la seguridad de los sistemas	17	5	1	23	26%
PO10 Administrar proyectos	15	0	0	15	17%
AI2 Adquirir y mantener el software aplicativo	6	1	0	7	8%
DS8 Administrar la mesa de servicio y los incidentes	2	4	1	7	8%
AI1 Identificar soluciones automatizadas	2	4	0	6	7%
PO6 Comunicar las aspiraciones y la dirección de la gerencia	5	0	0	5	6%
AI7 Instalar y acreditar soluciones y cambios	1	4	0	5	6%
DS4 Garantizar la continuidad del servicio	3	0	0	3	3%
DS12 Administrar el ambiente físico	3	0	0	3	3%
PO9 Evaluar y administrar riesgos de TI	2	0	0	2	2%
DS1 Definir y administrar niveles de servicio	1	1	0	2	2%
DS11 Administrar los datos	0	2	0	2	2%
DS13 Administrar las operaciones	0	2	0	2	2%
PO1 Definir el plan estratégico de TI	1	0	0	1	1%
PO5 Administrar la inversión en TI	1	0	0	1	1%
AI6 Administrar cambios	1	0	0	1	1%
DS9 Administrar la configuración	1	0	0	1	1%
DS10 Administrar los problemas	1	0	0	1	1%
ME2 Monitorear y evaluar el control interno	0	1	0	1	1%
ME3 Garantizar el cumplimiento regulatorio	0	1	0	1	1%
PO2 Definir la arquitectura de la información	0	0	0	0	0%
PO3 Determinar la dirección tecnológica	0	0	0	0	0%
PO4 Definir procesos, organización y relaciones de TI	0	0	0	0	0%
PO7 Administrar recursos humanos de TI	0	0	0	0	0%
PO8 Administrar calidad	0	0	0	0	0%
AI3 Adquirir y mantener la infraestructura tecnológica	0	0	0	0	0%
AI4 Posibilitar la operación y el uso	0	0	0	0	0%
AI5 Adquirir recursos de TI	0	0	0	0	0%
DS2 Administrar servicios de terceros	0	0	0	0	0%
DS3 Administrar desempeño y capacidad	0	0	0	0	0%
DS6 Identificar y asignar costos	0	0	0	0	0%
DS7 Educar y entrenar a los usuarios	0	0	0	0	0%
ME1 Monitorear y evaluar el desempeño de TI	0	0	0	0	0%
ME4 Proporcionar gerenciamiento de TI	0	0	0	0	0%
Total	**62**	**25**	**2**	**89**	**100%**

De esta forma obtenemos una exposición de los resultados más desagregada, lo cual resulta de utilidad para dilucidar cuales son los procesos que aparecen en primer lugar ya que estos son los que más contribuyen a levantar las observaciones y cumplir las recomendaciones de auditoria que le formularon a la organización.

Cabe aclarar que a los efectos de este análisis, es importante identificar al menos un Proceso Cobit relacionado con cada Observación o Recomendación. Asimismo, en caso de utilizar Informes de Auditoria de temáticas específicas como ser Sistemas de TI, Gestión de Riesgos, es conveniente aclararlo a la hora de las conclusiones. De otro modo el análisis enfatizará en dichas temáticas, lo cual nos puede llevar a conclusiones erróneas.

3.2.3 Revisión de Riesgos dentro del Departamento u Organización

Para realizar este análisis es necesario solicitar a la organización la Planilla de Identificación y Análisis de Riesgos, ya que es consideramos que es una herramienta muy útil para esta instancia del trabajo por su clara exposición de los riesgos.
Consta básicamente de un documento en el cual se identifican las diferentes Amenazas, los Controles existentes, los Riesgos residuales y las Acciones correctivas a tomar respecto al riesgo. Asimismo incluye el Nivel de Impacto, el Grado de Exposición y el Nivel de Riesgo que surge como resultado del producto “Nivel de Impacto X Grado de Exposición”.

Para nuestro trabajo nos enfocaremos en aquellos riesgos que superen el umbral de Riesgo, o sea el Riesgo Máximo Aceptable (RMA.) definido por la empresa. Para estos casos lo que hacemos, es identificar que Procesos del marco están relacionados con tales riesgos.
A diferencia de las Observaciones y Recomendaciones de Auditoria, nos planteamos trabajar con hasta dos procesos relacionados. En primer término ubicamos al proceso que más contribuye a la mejora en la gestión del riesgo y en segundo término aquel que tiene una contribución moderada. Una vez realizada esta tarea obtendremos una planilla como la que exponemos a continuación.

Cabe acotar, que en este caso hacemos el supuesto de que la organización definió como RMA: 120 (la escala va de 0 a 200, ya que el nivel de Impacto va de 0 a 20 y el grado de Exposición de 0 a 10), por tanto consideramos todos aquellos riesgos cuyo nivel sea mayor o igual a 120.

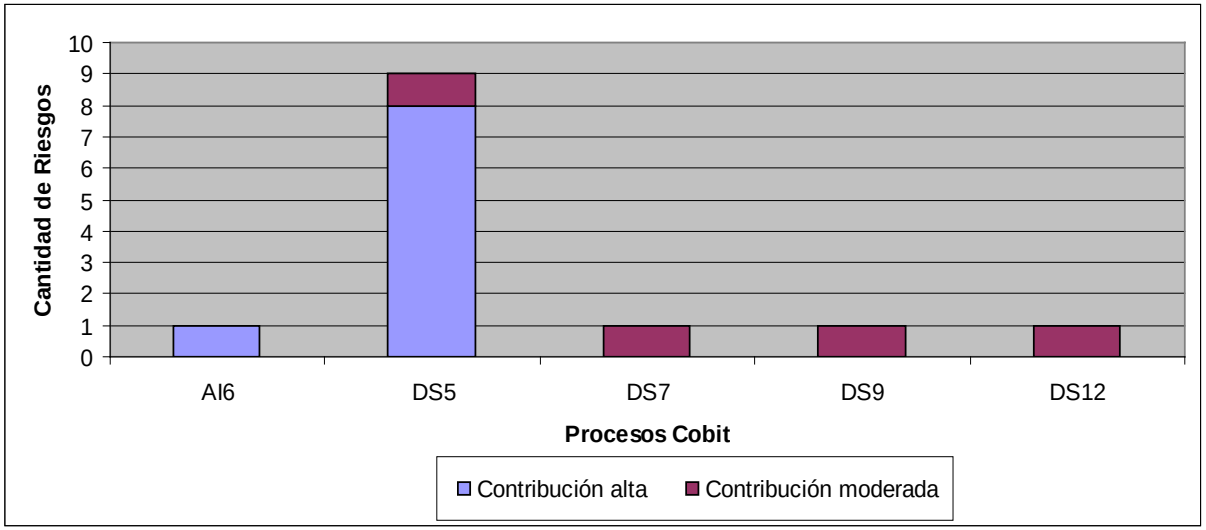
Cuadro 3.2.3.1 –Identificación de Procesos Cobit relacionados con los riesgos

Nivel de IMPACTO	Grado de EXPOSICION	Nivel de RIESGO	AMENAZA	CONTROLES EXISTENTES	RIESGO RESIDUAL	ACCIONES CORRECTIVAS	COBIT	
							Mayor Contribución	Contribución moderada
20	6	120	Mal uso de los sistemas informáticos por parte de los empleados y de terceras partes.	- Auditorias, herramientas de monitoreo, firewall, acceso restringido. - Control de acceso de usuarios/ Control de acceso remoto de usuarios. - Uso de políticas de Sistemas informáticos. - Acuerdos de Confidencialidad/ Términos y Condiciones de empleo.	- Incumplimiento de normativa vigente. - Incumplimiento de las políticas.	- Diseñar un Marco para la gestión de los Sistemas informáticos. - Llevar a cabo sesiones informativas y jornadas de entrenamiento para el personal.	DS5	
20	6	120	Hackeo / Ataque de virus.	- Controles de seguridad perimetral electrónica (por ejemplo, acceso remoto necesita símbolo + PIN + contraseña, bloqueo de contraseña después de 3 intentos fallidos, no puede ingresar). - Antivirus y herramientas de gestión de contenidos. - Imposibilidad de acceder a sitios de hackers.	- Pérdida temporal de la capacidad de procesamiento de información. - No se ejecutan actualizaciones a los antivirus.	- Considerar implementar herramientas de detección / prevención de accesos no autorizados (intrusos).	DS5	
20	6	120	Pérdida o corrupción (daño) de los activos de información.	- Los medios magnéticos de almacenamiento de datos, con información sensible deben ser resguardados en el Depto de Sistemas en armarios cerrados con llave.	- Riesgo de corrupción (daño).	- Asegurarse que los armarios estén bajo llave. - Establecer los procedimientos de eliminación de activos de información. - Establecer controles para la encriptación de información que se envíe a terceros.	DS5	DS12

20	6	120	Cambios no autorizados.	- Control de contraseñas. - Control de privilegios de acceso.	- Cambios arbitrarios, por ejemplo agregar columnas adicionales a bases de datos.	- Validación de bases de datos. - Revisión del proceso de control de cambios. - Revisión de los procedimientos de almacenamiento de datos.	AI6	DS5
20	10	200	Divulgación no autorizada.	- Política de control de contraseñas. - Política de control de privilegios de acceso.	- Acciones inadvertidas/ acciones deliberadas. - Fuga de datos en los dispositivos de memoria USB.	- Formación del personal respecto al uso del correo electrónico. - Implementar políticas de seguridad para restringir el uso de dispositivos de memoria USB.	DS5	DS7

Luego resumimos la frecuencia con que aparecen los Procesos en el análisis que estamos llevando a cabo, para lo cual elaboramos un gráfico como el siguiente:

Gráfico 3.2.3.2 - Contribución de los Procesos de Cobit a la gestión de riesgos (con puntaje superior o igual a 120, Total de Riesgos = 9)



Como podemos observar, el proceso DS 5 tiene una participación sobresaliente a efectos de mejorar la gestión de riesgos dentro de la organización. Sobre un total de 9 riesgos con nivel superior o igual al nivel de R.M.A., aporta en primer término a la gestión de 8 riesgos (88.88%).

3.2.4 Análisis de valor

A los efectos de llevar a cabo este análisis dentro de la organización, comenzaremos por considerar las Metas genéricas de Negocio propuestas por Cobit. En primer lugar la Dirección de la organización debe priorizar las cuatro perspectivas de negocio del Cuadro de Mando Integral, asignando un valor de 1 o 2, donde 1 corresponde a las de mayor prioridad y 2 a las de menor prioridad. Luego, dentro de cada perspectiva de negocio deben priorizar las Metas de Negocio asignándole un valor de acuerdo a su importancia para la organización, correspondiendo valor 1 a la meta de mayor importancia.

Para llevar adelante este análisis trabajaremos con datos supuestos, al igual que lo venimos realizando hasta ahora.

Cabe acotar que todas las escalas utilizadas en la herramienta son fijadas de modo arbitrario, por tanto puede ajustarse al criterio que establezca la organización o el Consultor. Las escalas que nos planteamos son de fácil comprensión y utilización a efectos ilustrativos. Sí es importante que una vez definidas las escalas estas se respeten para la realización de todo el análisis.

Cuadro 3.2.4.1 – Priorización de las Metas genéricas del Negocio

		Metas de Negocio	Importancia	
Perspectiva Financiera	1	Proporcionar un buen retorno de inversión de TI - permitiendo inversión en negocio	2	2
	2	Gestionar los riesgo de TI que afectan al negocio		1
	3	Mejorar gobierno corporativo y transparencia		3
Perspectiva del Cliente	4	Mejorar la orientación y servicio al cliente	1	2
	5	Ofrecer productos y servicios competitivos		6
	6	Establecer continuidad y disponibilidad de servicios		1
	7	Crear agilidad en la respuesta a los cambios de los requerimientos de negocio		3
	8	Lograr optimización de costos de la entrega de servicios		4
	9	Obtener información fiable y útil para tomar decisiones estratégicas		5
Perspectiva Interna	10	Mejorar y mantener funcionalidad de procesos de negocio	1	4
	11	Reducir el costo de los procesos		3
	12	Proporcionar cumplimiento con leyes externas, regulaciones y contratos		1
	13	Proporcionar cumplimiento con políticas internas		5
	14	Gestionar cambios de negocio		6
	15	Mejorar y mantener productividad operacional y de personal		2
Perspectiva de Aprendizaje y Desarrollo	16	Gestionar productos e innovación de negocio	2	2
	17	Adquirir y mantener personal calificado y motivado		1

En segundo lugar, consideramos las Metas genéricas de TI propuestas por Cobit y la tarea consiste en asignar un valor de 0 a 4 según la importancia que le asigne la Dirección a cada una de ellas, para lo cual proponemos la siguiente escala:

0 - Importancia critica para el Depto de TI
1 - Muy importante para el Depto de TI
2 - Importante para el Depto de TI
3 - Importancia moderada para el Depto de TI
4 - No aplicable para el Depto de TI

Cuadro 3.2.4.2 – Importancia de las Metas genéricas de TI

	Metas de TI	Importancia
1	Responder a requerimientos de negocio alineado con la estrategia de negocio.	3
2	Responder a los requerimientos de gobierno en línea con la dirección ejecutiva.	2
3	Asegurar la satisfacción del usuario final con la oferta de servicios y niveles de servicio.	2
4	Optimizar el uso de la información	2
5	Crear agilidad de TI.	3
6	Definir como la funcionalidad de negocio y requerimientos de control se trasladan en soluciones efectivas.	3
7	Adquirir y mantener sistemas de aplicación integrados y estandarizados	0
8	Adquirir y mantener una infraestructura de TI integrada y estandarizada.	0
9	Adquirir y mantener habilidades de TI que responden a la estrategia de TI.	1
10	Asegurar la satisfacción mutual de relaciones con terceras partes.	3
11	Asegurar la integración sin fisuras de las aplicaciones dentro de los procesos del negocio.	3
12	Asegurar la transparencia y comprensión de costos de TI, beneficios, estrategia, políticas y niveles de servicio.	3
13	Asegurar el uso apropiado y desempeño de las soluciones de aplicación y tecnología.	2
14	Tener en cuenta y proteger todos los activos de TI.	3
15	Optimizar la infraestructura, recursos y capacidades de TI.	0
16	Reducir los defectos de la solución y entrega de servicio, y reelaborar.	3
17	Proteger el logro de los objetivos de TI.	3
18	Establecer la claridad del impacto de negocio de los riesgos a los objetivos y recursos de TI.	3
19	Asegurar que la información crítica y confidencial se retiene a aquellos que no deben tener acceso.	0
20	Asegurar que las transacciones del negocio automatizadas y los cambios a la información son confiables.	1
21	Asegurar que los servicios de TI y la infraestructura pueden resistir apropiadamente y recuperar de fallos debidos a errores, ataques deliberados o desastres.	0
22	Asegurar el mínimo impacto de negocio en caso de una interrupción de servicios de TI o cambios.	1
23	Estar seguro que los servicios de TI están disponibles según se requiere.	3
24	Mejorar la eficiencia de costos de TI y sus contribuciones a la rentabilidad del negocio.	3
25	Entregar proyectos a tiempo y sobre presupuesto, reuniendo los estándares de calidad.	2
26	Mantener la integridad de la información e infraestructura de procesamiento.	3
27	Asegurar que TI cumple con la legislación, regulación y contratos.	2
28	Asegurar que TI demuestra la eficiencia de costos de la calidad de servicios, mejora continua y disposición para cambios futuros.	2

Es muy útil tener presente el siguiente cuadro, ya que en el se puede observar como el Marco vincula las Metas de Negocio y las Metas de TI, lo cual se logra combinando los dos cuadros anteriores.

Cuadro 3.2.4.3 – Relacionamiento entre las Metas de Negocio y las Metas de TI

		Metas de Negocio	Metas de TI							
Perspectiva Financiera	1	Proporcionar un buen retorno de inversión de TI - permitiendo inversión en negocio	24	28						
	2	Gestionar los riesgo de TI que afectan al negocio	2	14	17	18	19	20	21	22
	3	Mejorar gobierno corporativo y transparencia	2	18						
Perspectiva del Cliente	4	Mejorar la orientación y servicio al cliente	3	23						
	5	Ofrecer productos y servicios competitivos	5	24						
	6	Establecer continuidad y disponibilidad de servicios	10	16	22	23				
	7	Crear agilidad en la respuesta a los cambios de los requerimientos de negocio	1	5	25					
	8	Lograr optimización de costos de la entrega de servicios	7	8	10	24				
	9	Obtener información fiable y útil para tomar decisiones estratégicas	2	4	12	20	26			
Perspectiva Interna	10	Mejorar y mantener funcionalidad de procesos de negocio	6	7	11					
	11	Reducir el costo de los procesos	7	8	13	15	24			
	12	Proporcionar cumplimiento con leyes externas, regulaciones y contratos	2	19	20	21	22	26	27	
	13	Proporcionar cumplimiento con políticas internas	2	13						
	14	Gestionar cambios de negocio	1	5	6	11	28			
	15	Mejorar y mantener productividad operacional y de personal	7	8	11	13				
Perspectiva de Aprendizaje y Desarrollo	16	Gestionar productos e innovación de negocio	5	25	28					
	17	Adquirir y mantener personal calificado y motivado	9							

Asimismo, debemos considerar el vínculo entre las Metas de TI y los Procesos de Cobit. Estos enlaces se utilizan para tener una idea clara del aporte que los Procesos brindan al logro de las Metas de TI.

Cuadro 3.2.4.4 – Relacionamiento entre las Metas de TI y los Procesos Cobit

	Metas de TI	Procesos Cobit									
1	Responder a requerimientos de negocio alineado con la estrategia de negocio.	PO1	PO2	PO4	PO10	AI1	AI6	AI7	DS1	DS3	ME1
2	Responder a los requerimientos de gobierno en línea con la dirección ejecutiva.	PO1	PO4	PO10	ME1	ME4					
3	Asegurar la satisfacción del usuario final con la oferta de servicios y niveles de servicio.	PO8	AI4	DS1	DS2	DS7	DS8	DS10	DS13		
4	Optimizar el uso de la información	PO2	DS11								
5	Crear agilidad de TI.	PO2	PO4	PO7	AI3						
6	Definir como la funcionalidad de negocio y requerimientos de control se trasladan en soluciones efectivas.	AI1	AI2	AI6							
7	Adquirir y mantener sistemas de aplicación integrados y estandarizados	PO3	AI2	AI5							
8	Adquirir y mantener una infraestructura de TI integrada y estandarizada.	AI3	AI5								
9	Adquirir y mantener habilidades de TI que responden a la estrategia de TI.	PO7	AI5								
10	Asegurar la satisfacción mutual de relaciones con terceras partes.	DS2									
11	Asegurar la integración sin fisuras de las aplicaciones dentro de los procesos del negocio.	PO2	AI4	AI7							

12	Asegurar la transparencia y comprensión de costos de TI, beneficios, estrategia, políticas y niveles de servicio.	PO5	PO6	DS1	DS2	DS6	ME1	ME4			
13	Asegurar el uso apropiado y desempeño de las soluciones de aplicación y tecnología.	PO6	AI4	AI7	DS7	DS8					
14	Tener en cuenta y proteger todos los activos de TI.	PO9	DS5	DS9	DS12	ME2					
15	Optimizar la infraestructura, recursos y capacidades de TI.	PO3	AI3	DS3	DS7	DS9					
16	Reducir los defectos de la solución y entrega de servicio, y reelaborar.	PO8	AI4	AI6	AI7	DS10					
17	Proteger el logro de los objetivos de TI.	PO9	DS10	ME2							
18	Establecer la claridad del impacto de negocio de los riesgos a los objetivos y recursos de TI.	PO9									
19	Asegurar que la información crítica y confidencial se retiene a aquellos que no deben tener acceso.	PO6	DS5	DS11	DS12						
20	Asegurar que las transacciones del negocio automatizadas y los cambios a la información son confiables.	PO6	AI7	DS5							
21	Asegurar que los servicios de TI y la infraestructura pueden resistir apropiadamente y recuperar de fallos debidos a errores, ataques deliberados o desastres.	PO6	AI7	DS4	DS5	DS12	DS13	ME2			
22	Asegurar el mínimo impacto de negocio en caso de una interrupción de servicios de TI o cambios.	PO6	AI6	DS4	DS12						
23	Estar seguro que los servicios de TI están disponibles según se requiere.	DS3	DS4	DS8	DS13						
24	Mejorar la eficiencia de costos de TI y sus contribuciones a la rentabilidad del negocio.	PO5	DS6								
25	Entregar proyectos a tiempo y sobre presupuesto, reuniendo los estándares de calidad.	PO8	PO10								
26	Mantener la integridad de la información e infraestructura de procesamiento.	AI6	DS5								
27	Asegurar que TI cumple con la legislación, regulación y contratos.	DS11	ME2	ME3	ME4						
28	Asegurar que TI demuestra la eficiencia de costos de la calidad de servicios, mejora continua y disposición para cambios futuros.	PO5	DS6	ME1	ME4						

Hasta aquí, la Dirección de la organización ha clasificado las Metas de Negocio y las Metas de TI de acuerdo a su criterio. Luego se expusieron los vínculos entre las Metas de Negocio y las Metas de TI, y de las Metas de TI y los Procesos de Cobit. A través del procesamiento de la información obtenida, llegaremos a concluir cuales son los Procesos que más valor agregan a la gestión de TI dentro de la organización.

A continuación trabajaremos con las Metas de TI, para ello consideramos la evaluación sobre las Metas genéricas de TI realizada por la Dirección (ver Cuadro 3.2.4.2) y el cuadro que relaciona las Metas de TI y los Procesos de Cobit (ver Cuadro 3.2.4.4), en caso de que una Meta sea considerada de importancia crítica, los Procesos necesarios para llevarla adelante serán considerados igualmente críticos.

Por lo tanto, si tenemos una Meta de TI como la número 7 que fue evaluada con puntaje 0 por considerarla de importancia critica, a los Procesos de Cobit necesarios para lograr alcanzarla (PO3, AI2 y AI5) se los tilda en la columna de valor 0. Igual criterio deberá aplicarse en los demás casos.

Cabe precisar, que si un Proceso resulta de importancia para la consecución de más de una Meta, se le asignará el puntaje de la Meta de mayor importancia. Partiendo de un Proceso como el DS5, tenemos que contribuye a:

- 2 Metas de TI (19 y 21) de importancia critica, 0
- 1 Meta de TI (20) muy importante, 1
- 2 Metas de TI (14 y 26) de importancia moderada, 2

Por lo tanto a este Proceso le asignamos un valor de 0

Luego de realizar este ejercicio con todas las Metas de TI y los Procesos del Marco, planteamos un cuadro como el siguiente en el cual se resumen los resultados obtenidos:

Cuadro 3.2.4.5 – Aporte de los Procesos del Marco al logro de las Metas de TI

	Importancia					
Procesos	**0**	**1**	**2**	**3**	**4**	**Mayor**
PO1 Definir el plan estratégico de TI			√	√		2
PO2 Definir la arquitectura de la información			√	√		2
PO3 Determinar la dirección tecnológica	√					0
PO4 Definir procesos, organización y relaciones de TI			√	√		2
PO5 Administrar la inversión en TI			√	√		2
PO6 Comunicar las aspiraciones y la dirección de la gerencia	√	√	√	√		0
PO7 Administrar recursos humanos de TI		√		√		1
PO8 Administrar calidad			√	√		2
PO9 Evaluar y administrar riesgos de TI				√		3
PO10 Administrar proyectos			√	√		2
AI1 Identificar soluciones automatizadas				√		3
AI2 Adquirir y mantener el software aplicativo	√			√		0
AI3 Adquirir y mantener la infraestructura tecnológica	√			√		0
AI4 Posibilitar la operación y el uso			√	√		2
AI5 Adquirir recursos de TI	√	√				0
AI6 Administrar cambios		√		√		1
AI7 Instalar y acreditar soluciones y cambios	√	√	√	√		0
DS1 Definir y administrar niveles de servicio			√	√		2
DS2 Administrar servicios de terceros			√	√		2
DS3 Administrar desempeño y capacidad	√			√		0
DS4 Garantizar la continuidad del servicio	√	√		√		0
DS5 Garantizar la seguridad de los sistemas	√	√		√		0
DS6 Identificar y asignar costos			√	√		2
DS7 Educar y entrenar a los usuarios	√		√			0
DS8 Administrar la mesa de servicio y los incidentes			√	√		2
DS9 Administrar la configuración	√			√		0

DS10 Administrar los problemas			√	√		2
DS11 Administrar los datos	√		√			0
DS12 Administrar el ambiente físico	√	√		√		0
DS13 Administrar las operaciones	√		√	√		0
ME1 Monitorear y evaluar el desempeño de TI			√	√		2
ME2 Monitorear y evaluar el control interno	√		√	√		0
ME3 Garantizar el cumplimiento regulatorio			√			2
ME4 Proporcionar gerenciamiento de TI			√	√		2

Por último trabajaremos con las Metas del Negocio, para lo cual consideramos la evaluación que la Dirección realizó sobre las Perspectivas de Negocio y sus respectivas Metas (ver Cuadro 3.2.4.1), las cuales ponderamos de acuerdo a las escalas que proponemos a continuación:

Nivel de importancia de la Perspectiva	Ponderador asignado a la importancia
1	10
2	5

Nivel de importancia de la Meta de Negocio			Ponderador asignado al ordinal		
1	1	1	1	1	1
2	2	2	1/2	1/3	1/6
3	3		1/3	1/6	
4			1/4		
5			1/5		
6			1/6		

Con estos ponderadores le asignaremos un puntaje a cada una de las Metas de Negocio que resulta del producto entre el nivel de importancia de la Perspectiva de Negocio y el nivel de importancia de la Meta de Negocio, es así que si miramos la *Meta 4 – Mejorar la orientación y servicio al cliente*, por ejemplo la ponderación total será igual a 10 x ½ = 5.

Cuadro 3.2.4.6 – Ponderación de las Perspectivas y Metas de Negocio

					Ponderacion		
		Metas de Negocio	Importancia		Perspectiva	Meta	Total
Perspectiva Financiera	1	Proporcionar un buen retorno de inversión de TI - permitiendo inversión en negocio	2	2	5	1/3	1.67
	2	Gestionar los riesgo de TI que afectan al negocio		1	5	1	5.00
	3	Mejorar gobierno corporativo y transparencia		3	5	1/6	0.83
Perspectiva del Cliente	4	Mejorar la orientación y servicio al cliente	1	2	10	1/2	5.00
	5	Ofrecer productos y servicios competitivos		6	10	1/6	1.67
	6	Establecer continuidad y disponibilidad de servicios		1	10	1	10.00
	7	Crear agilidad en la respuesta a los cambios de los requerimientos de negocio		3	10	1/3	3.33
	8	Lograr optimización de costos de la entrega de servicios		4	10	1/4	2.50
	9	Obtener información fiable y útil para tomar decisiones estratégicas		5	10	1/5	2.00
Perspectiva Interna	10	Mejorar y mantener funcionalidad de procesos de negocio	1	4	10	1/4	2.50
	11	Reducir el costo de los procesos		3	10	1/3	3.33
	12	Proporcionar cumplimiento con leyes externas, regulaciones y contratos		1	10	1	10.00
	13	Proporcionar cumplimiento con políticas internas		5	10	1/5	2.00
	14	Gestionar cambios de negocio		6	10	1/6	1.67
	15	Mejorar y mantener productividad operacional y de personal		2	10	1/2	5.00
Perspectiva de Aprendizaje y Desarrollo	16	Gestionar productos e innovación de negocio	2	2	5	1/6	0.83
	17	Adquirir y mantener personal calificado y motivado		1	5	1	5.00

Una vez obtenidos los puntajes de cada una de las Metas del Negocio, debemos asignar a cada Meta de TI relacionada a dichas Metas el respectivo puntaje. Para ello es útil visualizar la relación entre las Metas del Negocio y las de TI (ver Cuadro 3.2.4.3) asignándole a cada Meta de TI los puntajes en función de los cálculos resumidos anteriormente en el Cuadro 3.2.4.6.

A modo de explicar los cálculos realizados, consideramos la Meta de TI numero 1 - *Responder a requerimientos de negocio alineado con la estrategia de negocio*, la cual vemos que aporta al logro de las metas del Negocio 7 y 14 (ver Cuadro 3.2.4.3), y en el cuadro 3.2.4.6 vemos que el puntaje de tales metas es:

Meta de Negocio 7	puntaje	3.33
Meta de Negocio 14	puntaje	1.67
		5.00

Por lo tanto a esta Meta de TI le corresponde dicho puntaje, igual razonamiento debemos realizar para las demás Metas de TI.

Luego de obtenidos los puntajes de cada una de las Metas de TI, debemos asignar tales valores a los Procesos del Marco Cobit, para ello consideramos el relacionamiento entre las Metas de TI y los Proceso de Cobit (ver Cuadro 3.2.4.4). De este modo asignamos a cada Proceso, el valor que resulta de la sumatoria de cada una de las contribuciones que dicho Proceso realiza a las Metas de TI.

Cuadro 3.2.4.7 - Aporte de los Procesos del Marco al logro de las Metas del Negocio

		PROCESOS																																	
Metas de TI	Valor total de las METAS de TI ponderadas	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	AI1	AI2	AI3	AI4	AI5	AI6	AI7	DS1	DS2	DS3	DS4	DS5	DS6	DS7	DS8	DS9	DS10	DS11	DS12	DS13	ME1	ME2	ME3	ME4
1	5.00	5.00	5.00		5.00						5.00	5.00					5.00	5.00	5.00		5.00											5.00			
2	19.83	19.83			19.83						19.83																					19.83			19.83
3	5.00								5.00						5.00				5.00	5.00					5.00	5.00		5.00			5.00				
4	2.00		2.00																										2.00						
5	7.50		7.50		7.50			7.50						7.50																						
6	4.17											4.17	4.17				4.17																			
7	13.33			13.33									13.33			13.33																			
8	10.83													10.83		10.83																			
9	5.00							5.00								5.00																			
10	12.50																			12.50															
11	9.17		9.17												9.17			9.17																	
12	2.00					2.00	2.00												2.00	2.00				2.00								2.00			2.00
13	10.33						10.33								10.33			10.33							10.33	10.33									
14	5.00									5.00													5.00				5.00			5.00			5.00		
15	3.33			3.33										3.33							3.33				3.33		3.33								
16	10.00								10.00						10.00		10.00	10.00										10.00							
17	5.00									5.00																		5.00					5.00		
18	5.83									5.83																									
19	15.00						15.00																15.00						15.00	15.00					
20	17.00						17.00											17.00					17.00												
21	15.00						15.00											15.00				15.00	15.00							15.00	15.00		15.00		
22	25.00						25.00										25.00					25.00								25.00					
23	15.00																				15.00	15.00				15.00					15.00				
24	9.17					9.17																		9.17											
25	4.17								4.17		4.17																									
26	12.00																12.00						12.00												
27	10.00																												10.00				10.00	10.00	10.00
28	2.50					2.50																		2.50								2.50			2.50
		24.83	23.67	16.67	32.33	13.67	84.33	12.50	19.17	15.83	29.00	9.17	17.50	21.67	34.50	29.17	56.17	66.50	12.00	19.50	23.33	55.00	64.00	13.67	18.67	30.33	8.33	20.00	27.00	60.00	35.00	29.33	35.00	10.00	34.33

El siguiente cuadro resume los puntajes asignados a cada uno de los Procesos, con respecto a las Metas de Negocio y las Metas de TI, lo cual se desprende de los Cuadros 3.2.4.5 y 3.2.4.7 respectivamente.

Cuadro 3.2.4.8 – Resumen del aporte de los Procesos del Marco al logro de las Metas del Negocio y las Metas de TI

Proceso	Valor según analisis de	
	Metas de TI	Metas del Negocio
PO1 Definir el plan estratégico de TI	2	24.83
PO2 Definir la arquitectura de la información	2	23.67
PO3 Determinar la dirección tecnológica	0	16.67
PO4 Definir procesos, organización y relaciones de TI	2	32.33
PO5 Administrar la inversión en TI	2	13.67
PO6 Comunicar las aspiraciones y la dirección de la gerencia	0	84.33
PO7 Administrar recursos humanos de TI	1	12.50
PO8 Administrar calidad	2	19.17
PO9 Evaluar y administrar riesgos de TI	3	15.83
PO10 Administrar proyectos	2	29.00
AI1 Identificar soluciones automatizadas	3	9.17
AI2 Adquirir y mantener el software aplicativo	0	17.50
AI3 Adquirir y mantener la infraestructura tecnológica	0	21.67
AI4 Posibilitar la operación y el uso	2	34.50
AI5 Adquirir recursos de TI	0	29.17
AI6 Administrar cambios	1	56.17
AI7 Instalar y acreditar soluciones y cambios	0	66.50
DS1 Definir y administrar niveles de servicio	2	12.00
DS2 Administrar servicios de terceros	2	19.50
DS3 Administrar desempeño y capacidad	0	23.33
DS4 Garantizar la continuidad del servicio	0	55.00
DS5 Garantizar la seguridad de los sistemas	0	64.00
DS6 Identificar y asignar costos	2	13.67
DS7 Educar y entrenar a los usuarios	0	18.67
DS8 Administrar la mesa de servicio y los incidentes	2	30.33
DS9 Administrar la configuración	0	8.33
DS10 Administrar los problemas	2	20.00
DS11 Administrar los datos	0	27.00
DS12 Administrar el ambiente físico	0	60.00
DS13 Administrar las operaciones	0	35.00
ME1 Monitorear y evaluar el desempeño de TI	2	29.33
ME2 Monitorear y evaluar el control interno	0	35.00
ME3 Garantizar el cumplimiento regulatorio	2	10.00
ME4 Proporcionar gerenciamiento de TI	2	34.33

A los efectos de concluir con el análisis de valor, exponemos los datos del Cuadro 3.2.4.8 en un mapa de calor el cual refleja en un eje el Aporte de los Procesos a las Metas de TI y en el otro eje el Aporte a las Metas del Negocio.

Cuadro 3.2.4.9 – Aporte de los Procesos a las Metas del Negocio y las Metas de TI (Mapa de calor)

Aporte del Proceso a las Metas del Negocio				
	Contribución alta (valor mayor o igual a 41)		AI6 (56)	PO6 (84) AI7 (66) DS5 (64) DS12 (60) DS4 (55)
	Contribución moderada (valor entre 21 y 40)	AI4 (34) ME4 (34) PO4 (32) DS8 (30) ME1 (29) PO10 (29) PO1 (25) PO2 (24)		DS13 (35) ME2 (35) AI5 (29) DS11 (27) DS3 (23) AI3 (22)
	Contribución baja (valor entre 0 y 20)	DS10 (20) DS2 (19) PO8 (19) PO9 (16) PO5 (14) DS6 (14) DS1 (12) ME3 (10) AI1 (9)	PO7 (12)	DS7 (19) AI2 (17) PO3 (17) DS9 (8)
		Metas importantes o de importancia moderada (2-3)	Meta muy importante (1)	Meta de importancia critica (0)
		Aporte del Proceso a las Metas de TI		

Para interpretar los resultados, podemos ver en este gráfico que en el cuadrante superior del extremo derecho se ubican aquellos procesos de importancia crítica para las Metas de TI que a su vez tienen la mayor contribución para el logro de las Metas del Negocio. Por lo tanto podemos concluir que a través de la gestión de tales procesos, generaremos él mayor valor para la organización.

3.2.5 Selección de procesos para comenzar a trabajar en profundidad

En esta instancia y luego de haber utilizado gran cantidad de las herramientas que nos brinda el Marco, estamos en condiciones de seleccionar los Procesos cuya implementación ó mejora tendrán un efecto más provechoso respecto a la gestión del área de TI.
A tales efectos consideramos los resultados y las conclusiones obtenidas del uso de las diferentes herramientas aplicadas a la realidad de la organización.

Cuadro 3.2.5.1 – Selección de procesos

Herramienta	Procesos que más aportan a la mejora	Comentarios
Evaluación inicial Madurez Objetivos de control Matriz RACI	 No corresponde DS5 – AI6 DS5 – AI6	Se identifican los niveles de los Procesos
Observaciones y Recomendaciones de Auditoria	DS5 – PO10	
Análisis de Riesgos	DS 5 – AI6	
Análisis de Valor	PO 6 – AI7 - DS5	

A partir de este cuadro seleccionaremos los procesos con los cuales daremos comienzo a la etapa de Gestión de las oportunidades de Mejora, teniendo las evidencias suficientes como para argumentar que los procesos seleccionados son los más adecuados para comenzar con la mejora en la gestión de TI.

A los efectos del presente análisis, seleccionamos los Procesos *DS5 Garantizar la seguridad de los Sistemas* y *AI6 Administrar Cambios*, ya que la mejora en su desempeño tendrá el impacto más favorable sobre la gestión de TI y en definitiva sobre la consecución de las metas que se propone la organización.

3.3 Tercera Etapa - Gestión de las oportunidades de mejora

Una vez identificados los Procesos para trabajar en profundidad, estamos en condiciones de abordar la etapa que refiere a la gestión las oportunidades de mejora que se desprenden de todo el análisis, ya que el objetivo de la propuesta es brindar una selección de mejoras para ser implementadas.

Para ello debemos comenzar por una reevaluación de los Procesos seleccionados, luego debemos proceder a identificar y seleccionar las oportunidades de mejora que surjan, para ser implementadas en la organización, buscando mejorar la gestión y en consecuencia alcanzar las Metas de TI y las Metas de Negocio que se ha propuesto la organización.

3.3.1 Reevaluación de procesos seleccionados

Una vez identificados los procesos con los cuales se trabajará en toda esta etapa (en este caso DS5 y AI6), debemos comenzar por reevaluarlos. A tales efectos, se volverá a trabajar con el Modelo de Madurez, los Objetivos de control y la Matriz RACI, pero con un mayor detenimiento ya que es necesario cubrir todos los planteos que incluye el Marco en tales Procesos. Asimismo se trabajará con las Prácticas de control a efectos de obtener un análisis más integral sobre los Procesos.

Esta tarea resulta sumamente útil a efectos de; a) asegurarnos que lo que nos manifestaron en la Evaluación Inicial de los Procesos es como lo indicaron, b) obtener información que no se nos había comunicado, o bien no había conocimiento a nivel interno que era de utilidad a efectos de la implementación del Marco.

3.3.2 Identificación de oportunidades de mejora

Del numeral *3.2 Segunda etapa – Ejecución de actividades de evaluación,* obtenemos gran parte de la materia prima para desarrollar el presente numeral. Ahora bien no todo lo que sea identificado como oportunidad de mejora o recomendación será considerado, si bien podría entregarse un Informe con todos los aspectos que pueden ser implementados ó mejorados a efectos de la gestión de TI, a los efectos de nuestra tarea se consideran las mejoras y recomendaciones relacionadas con los procesos seleccionados en *3.2.5 Selección de procesos para comenzar a trabajar en profundidad* y obviamente la información recabada al llevar adelante la *3.3.1 Reevaluación de procesos seleccionados.*

Respecto al Proceso *DS5 – Garantizar la seguridad de los sistemas*

Modelo de Madurez

Comenzaremos trabajando con el Modelo de Madurez, a tales efectos haremos el supuesto de que la organización se encuentra en el Nivel 2 – *Repetible pero intuitivo* y se planteo como objetivo alcanzar un Nivel 3 - *Definido*, por lo tanto enfocamos nuestro análisis en estos niveles, ya que entendemos que los niveles 0 y 1 se verifican y los niveles 4 y 5 requieren circunstancias que distan de la realidad de la organización.

De la aplicación de esta herramienta, surgen las siguientes:

1 - La empresa debe asegurarse al contratar servicios con terceros, que estos tengan conocimiento de los parámetros de seguridad de la organización necesarios para llevar a cabo su tarea.

2 - Los procedimientos de seguridad de TI deben ser definidos y alineados con las políticas de seguridad de TI.

3 - Las responsabilidades de la seguridad deben ser asignadas y entendidas claramente por los responsables.

4 - Debe diseñarse un plan de seguridad de TI.

Objetivos de Control

Luego evaluamos los Objetivos de Control detallados y detectamos que los siguientes aspectos deben ser tenidos en cuenta:

5 - Si bien la organización gestiona al más alto nivel la seguridad referente a TI, debe alinearse a los requerimientos del negocio.

6 - Las políticas y procedimientos de seguridad deben ser comunicadas por medios formales, a efectos de tener certeza sobre el conocimiento de las mismas por parte de los usuarios.

7 - Asegurarse que los permisos de acceso a los sistemas estén en línea con los roles de los usuarios dentro de la organización.

8 - Definir de forma adecuada quien aprueba los permisos de acceso para los usuarios.

9 - La Gerencia debe realizar revisiones periódicas de las cuentas y privilegios de los usuarios.

10 - Establecer políticas que garanticen la aplicación periódica de medidas preventivas, de detección y corrección (particularmente las actualizaciones de seguridad y el control de virus) a fin de proteger los sistemas y la tecnología de la información del software malicioso (virus, spyware, correo electrónico no solicitado, etc.).

Matriz RACI

Del análisis de las actividades incluidas en la Matriz RACI, concluimos que seria importante considerar:

11 - Implementar un monitoreo periódico de los potenciales incidentes de seguridad.

12 - Realizar periódicamente evaluaciones de las vulnerabilidades existentes en el Departamento.

Prácticas de Control

Considerando esta herramienta, nos parece importante:

13 - Definir pautas para la seguridad de TI, estableciendo para la gestión de la seguridad:

- El ámbito de aplicación y los objetivos de gestión
- Las responsabilidades
- Los aspectos a tener en cuenta (por ejemplo, riesgos, rendimiento)

14 - Definir y mantener un plan general de seguridad de TI, que incluya:

- Un conjunto de políticas y normas de seguridad alineadas entre sí.
- Procedimientos detallados para aplicar y hacer cumplir las políticas y normas
- Funciones y responsabilidades a cumplir por parte de los individuos
- Las inversiones en recursos de seguridad necesarios

15 - Establecer métodos de autentificación y autorización para los usuarios, de modo de delimitar la responsabilidad y hacer cumplir los derechos de acceso.

16- Asegurar que todo hardware, software y servicio relacionado con la función de seguridad y los controles, sea inviolable.

17 - Revisar periódicamente y evaluar potenciales amenazas.

18 - Establecer, mantener, comunicar y hacer cumplir una política de seguridad de redes que sea revisada y actualizada regularmente.

Observaciones y Recomendaciones de Auditoria

Del análisis efectuado en el numeral *3.2.2 – Revisión de las Observaciones y Recomendaciones de Auditoria*, resulta pertinente considerar en esta instancia, lo siguiente:

19 - Seguridad de los Documentos y Archivos - las claves de acceso deben ser cambiadas regularmente para mejorar la seguridad de los registros.

20 - Destrucción de Documentos y Archivos - asegurarse que los miembros del personal asistan a la capacitación en gestión de documentos, para asegurarse de que son conscientes de los riesgos que conlleva mantener la información durante un plazo de tiempo mayor al que se establece como necesario.

21 - La política de Administración de Documentos debe tratar la temática que refiere al Ambiente físico necesario para el Almacenamiento - esta política debe incluir detalles en cuanto a como deben ser almacenados a fin de cumplir con la regulación existente en materia de prevención de incendios.

Análisis de Riesgos

En el numeral *3.2.3 – Revisión de Riesgos dentro del Departamento u Organización* detectamos que deben ser consideradas las siguientes mejoras:

22 - Diseñar un Marco para la gestión de los Sistemas informáticos.

23 - Llevar a cabo sesiones informativas y jornadas de entrenamiento para el personal.

24 - Considerar implementar herramientas de detección / prevención de accesos no autorizados (intrusos).

25 - Asegurarse que los armarios estén bajo llave.

26 - Establecer los procedimientos de eliminación de activos de información.

27 - Establecer controles para la encriptación de información que se envíe a terceros.

28 - Formación del personal respecto al uso del correo electrónico.

29 - Implementar políticas de seguridad para restringir el uso de dispositivos de memoria USB.

Respecto al Proceso *AI6 – Administrar cambios*

Modelo de Madurez

Al igual que en proceso anterior, suponemos que la organización se encuentra actualmente en un Nivel 2 – *Repetible pero intuitivo* y se plantea alcanzar un nivel 3 – *Definido*. A tales efectos es necesario considerar:

30 – Debe existir un proceso formal para gestionar los cambios, que incluya al menos la categorización y priorización de los mismos.

31- La evaluación del impacto de los cambios de TI (nuevas aplicaciones y tecnologías) sobre el negocio debe realizarse oportunamente, con el objetivo de contribuir a la toma de decisiones respecto a que cambios considerar y evitar sorpresas a la hora de su implantación.

Objetivos de Control

Del análisis de los Objetivos de Control detallados, surgen las siguientes oportunidades:

32 - Deben definirse procedimientos formales de control de cambios para manejar de forma estándar todas las solicitudes de cambios a las aplicaciones, procedimientos y procesos.

33 - Asegurarse que los cambios a implementar estén debidamente aprobados por quien solicitó el cambio.

34 - Debe implementarse un sistema de seguimiento y comunicación para mantener informado a los solicitantes de los cambios y a las partes interesadas acerca del estado de los cambios a las aplicaciones, procedimientos y procesos.

Matriz RACI

A continuación, citamos los planteos que surgen del análisis de las actividades de la Matriz RACI:

35 – Cerciorarse que los cambios de emergencia siguen el proceso de aprobación de cambios establecido en la organización.

36 – Los usuarios deben ser informados sobre los cambios introducidos en las aplicaciones, los procedimientos y procesos que requieren su participación.

Prácticas de Control

Veamos ahora las consideraciones que surgen del análisis de las Prácticas de Control:

37 - Considerar el impacto de los proveedores de servicios contratados (por ejemplo, de infraestructura, desarrollo de aplicaciones) sobre el proceso de gestión de cambios.

38 - Categorizar los cambios solicitados (por ejemplo, infraestructura, sistemas operativos, redes, software de aplicación).

39 - Priorizar los cambios solicitados, asegurando que el proceso de gestión del cambio considera tanto las necesidades comerciales, como las técnicas.

40 - Implementar informes sobre la situación de los cambios que incluyan métricas de desempeño, para permitir a la Dirección realizar una revisión y monitorear el estado en que se encuentran los cambios.

41 - Mantener actualizados los procesos de negocio, en concordancia con los cambios en el hardware o software, de modo de asegurarse que las nuevas funcionalidades o aplicaciones se utilizan.

Observaciones y Recomendaciones de Auditoria

Al igual que en el proceso anterior, debemos considerar el análisis efectuado en el numeral *3.2.2 – Revisión de las Observaciones y Recomendaciones de Auditoria*, del cual surge que:

42 - Deben aplicarse controles de validez a los cambios en las funcionalidades de las aplicaciones desarrolladas internamente.

Análisis de Riesgos

Por último, enumeramos las recomendaciones que surgen del numeral *3.2.3 – Revisión de Riesgos dentro del Departamento u Organización*:

43 – Las bases de datos deben ser validadas.

44 – Debe realizarse una revisión periódica del Proceso de Control de Cambios.

45 – Debe realizarse una revisión periódica de los Procedimientos de Almacenamiento de Datos.

Marcos relacionados

A los efectos de obtener una propuesta más integral, es recomendable considerar los Marcos Relacionados citados en *5.2 Anexo 2 – Relacionamiento con otros Marcos y Estándares*. La tarea consiste en utilizar tales Marcos y Estándares buscando aspectos que, bien pueden ser

incorporados ó mejorados a efectos de lograr un mejor desempeño de TI dentro de la organización.

3.3.3 Selección de las mejoras a implementar

A partir de las Oportunidades de Mejora que fueron identificadas en el numeral anterior, debemos efectuar una priorización con la finalidad de seleccionar aquellas que a criterio de la Dirección sean de mayor contribución al logro de las Metas del Negocio. Es importante destacar, que en esta instancia es de gran utilidad la participación del Consultor.

A modo de ejemplificar, exponemos a continuación una propuesta:

Cuadro 3.3.3.1 – Selección de las mejoras a implementar

Op Mejora	Herramienta	Priorización	Descripción
Proceso DS5 - Garantizar la seguridad de los sistemas			
2	MM	1	2 - Los procedimientos de seguridad de TI deben ser definidos y alineados con las políticas de seguridad de TI.
3	MM	1	3 - Las responsabilidades de la seguridad deben ser asignadas y entendidas claramente por los responsables.
4	MM	1	4 - Debe diseñarse un plan de seguridad de TI.
5	OC	1	5 - Si bien la organización gestiona al más alto nivel la seguridad referente a TI, debe alinearse a los requerimientos del negocio.
6	OC	1	6 - Las políticas y procedimientos de seguridad deben ser comunicadas por medios formales, a efectos de tener certeza sobre el conocimiento de las mismas por parte de los usuarios.
10	OC	1	10 - Establecer políticas que garanticen la aplicación periódica de medidas preventivas, de detección y corrección (particularmente las actualizaciones de seguridad y el control de virus) a fin de proteger los sistemas y la tecnología de la información del software malicoso (virus, spyware, correo electrónico no solicitado, etc.).
11	RACI	1	11 - Implementar un monitoreo periódico de los potenciales incidentes de seguridad.
13	PC	1	13 - Definir pautas para la seguridad de TI, estableciendo para la gestión de la seguridad: • El ámbito de aplicación y los objetivos de gestión • Las responsabilidades • Los aspectos a tener en cuenta (por ejemplo, riesgos, rendimiento)
14	PC	1	14 - Definir y mantener un plan general de seguridad de TI, que incluya: • Un conjunto de políticas y normas de seguridad alineadas entre sí. • Procedimientos detallados para aplicar y hacer cumplir las políticas y normas • Funciones y responsabilidades a cumplir por parte de los individuos • Las inversiones en recursos de seguridad necesarios
18	PC	1	18 - Establecer, mantener, comunicar y hacer cumplir una política de seguridad de redes que sea revisada y actualizada regularmente.
7	OC	1	7 - Asegurarse que los permisos de acceso a los sistemas estén en línea con los roles de los usuarios dentro de la organización.
8	OC	1	8 - Definir de forma adecuada quien aprueba los permisos de acceso para los usuarios.
9	OC	1	9 - La Gerencia debe realizar revisiones periódicas de las cuentas y privilegios de los usuarios.
15	PC	1	15 - Establecer métodos de autentificación y autorización para los usuarios, de modo de delimitar la responsabilidad y hacer cumplir los derechos de acceso.
24	AR	1	24 - Considerar implementar herramientas de detección / prevención de accesos no autorizados (intrusos).
29	AR	1	29 - Implementar políticas de seguridad para restringir el uso de dispositivos de memoria USB.
22	AR	1	22 - Diseñar un Marco para la gestión de los Sistemas informáticos.
12	RACI	2	12 - Realizar periódicamente evaluaciones de las vulnerabilidades existentes en el Departamento.
17	PC	2	17 - Revisar periódicamente y evaluar potenciales amenazas.

19	ORA	2	19 - Seguridad de los Documentos y Archivos - las claves de acceso deben ser cambiadas regularmente para mejorar la seguridad de los registros.
20	ORA	2	20 - Destrucción de Documentos y Archivos - asegurarse que los miembros del personal asistan a la capacitación en gestión de documentos, para asegurarse de que son conscientes de los riesgos que conlleva mantener la información durante un plazo de tiempo mayor al que se establece como necesario.
23	AR	2	23 - Llevar a cabo sesiones informativas y jornadas de entrenamiento para el personal.
28	AR	2	28 - Formación del personal respecto al uso del correo electrónico.
1	MM	2	1 - La empresa debe asegurarse al contratar servicios con terceros, que estos tengan conocimiento de los parámetros de seguridad de la organización necesarios para llevar a cabo su tarea.
16	PC	2	16- Asegurar que todo hardware, software y servicio relacionado con la función de seguridad y los controles, sea inviolable.
21	ORA	2	21 - La politica de Administración de Documentos debe tratar la temática que refiere al Ambiente fisico necesario para el Almacenamiento - esta politica debe incluir detalles en cuanto a como deben ser almacenados a fin de cumplir con la regulación existente en materia de prevención de incendios.
25	AR	2	25 - Asegurarse que los armarios estén bajo llave.
26	AR	2	26 - Establecer los procedimientos de eliminación de activos de información.
27	AR	2	27 - Establecer controles para la encriptación de información que se envie a terceros.
Proceso AI6 - Administrar cambios			
30	MM	1	30 – Debe existir un proceso formal para gestionar los cambios, que incluya al menos la categorización y priorización de los mismos.
31	MM	1	31- La evaluación del impacto de los cambios de TI (nuevas aplicaciones y tecnologías) sobre el negocio debe realizarse oportunamente, con el objetivo de contribuir a la toma de decisiones respecto a que cambios considerar y evitar sorpresas a la hora de su implantación.
37	PC	1	37 - Considerar el impacto de los proveedores de servicios contratados (por ejemplo, de infraestructura, desarrollo de aplicaciones) sobre el proceso de gestión de cambios.
38	PC	1	38 - Categorizar los cambios solicitados (por ejemplo, infraestructura, sistemas operativos, redes, software de aplicación).
39	PC	1	39 - Priorizar los cambios solicitados, asegurando que el proceso de gestión del cambio considera tanto las necesidades comerciales, como las técnicas.
40	PC	1	40 - Implementar informes sobre la situación de los cambios que incluyan métricas de desempeño, para permitir a la Dirección realizar una revisión y monitorear el estado en que se encuentran los cambios.
44	AR	1	44 – Debe realizarse una revisión periódica del Proceso de Control de Cambios.
32	OC	1	32 - Deben definirse procedimientos formales de control de cambios para manejar de forma estándar todas las solicitudes de cambios a las aplicaciones, procedimientos y procesos.
35	RACI	1	35 – Cerciorarse que los cambios de emergencia siguen el proceso de aprobación de cambios establecido en la organización.
42	ORA	2	42 - Deben aplicarse controles de validez a los cambios en las funcionalidades de las aplicaciones desarrolladas internamente.
43	AR	2	43 – Las bases de datos deben ser validadas.
45	AR	2	45 – Debe realizarse una revisión periódica de los Procedimientos de Almacenamiento de Datos.
33	OC	2	33 - Asegurarse que los cambios a implementar estén debidamente aprobados por quien solicitó el cambio.
34	OC	2	34 - Debe implementarse un sistema de seguimiento y comunicación para mantener informado a los solicitantes de los cambios y a las partes interesadas acerca del estado de los cambios a las aplicaciones, procedimientos y procesos.
36	RACI	2	36 – Los usuarios deben ser informados sobre los cambios introducidos en las aplicaciones, los procedimientos y procesos que requieren su participación.
41	PC	2	41 - Mantener actualizados los procesos de negocio, en concordancia con los cambios en el hardware o software, de modo de asegurarse que las nuevas funcionalidades o aplicaciones se utilizan.
	Referencia		Priorización
	MM	Modelo de Madurez	1 - Mayor contribución
	OC	Objetivos de Control	2 - Moderada contribución
	RACI	Matriz RACI	
	PC	Practicas de Control	
	ORA	Observaciones y Recomendaciones de Auditoria	
	AR	Análisis de Riesgos	

En este cuadro resumimos la priorización que hemos llevado adelante, como se puede observar agrupamos las oportunidades de mejora en función de la temática a la que refieren.

En primer orden ubicamos aquellas que a nuestro entender generan una mayor contribución al logro de las Metas de la Organización.

3.3.4 Implementación de las mejoras

Finalmente es fundamental asistir a la organización en la implementación y el posterior monitoreo de las mejoras de gestión a ser incorporadas. A efectos de contribuir a su incorporación, es conveniente mantener reuniones periódicas, para lo cual es necesario desarrollar planes de acción, definir metas a alcanzar y colaborar con los responsables dentro de la organización en todo lo relacionado con las mejoras seleccionadas..

Debido a que esta instancia escapa al planteo de nuestra propuesta de trabajo ya que no es necesario el Marco Cobit para llevarla adelante, no nos extenderemos sobre el punto.

4. CONCLUSIONES

En primer lugar, debemos mencionar que el Marco Cobit es un estándar internacional, de relativa aceptación, y que más allá de que se carece de datos más actualizados que los que constan en el anexo 1, ya de éste se desprende que en Latinoamérica son varios los países –Uruguay incluido- que lo han incorporado dentro de su regulación.
Esto, que en cierto modo constituye una conclusión previa al trabajo, muestra la relevancia que adquiere profundizar el estudio del referido documento.

Del análisis realizado del Marco Cobit nos surge que éste no incluye una metodología a seguir a efectos de su implementación; en el mismo sentido de la búsqueda de información efectuada durante nuestra investigación tampoco hemos encontrado documentación en la cual se proponga una metodología de este tipo y cuente con general aceptación

En ese sentido, se aprecia que el Marco define un conjunto de criterios, pero no establece un mecanismo para su incorporación a la gestión de la organización, por lo tanto se concluye que resulta útil plantear una propuesta metodológica de implementación.

En efecto, la magnitud de tópicos cubiertos por el Marco Cobit muestra la envergadura que puede tener un proyecto de implementación del mismo. Por lo tanto, para lograr una implementación exitosa es importante contar con una metodología apropiada que lo viabilice, la que debería estar enmarcada en las características que debería tener todo proyecto de magnitud: liderazgo desde la cúpula de la organización, adhesión e involucramiento de quienes deberán trabajar en el emprendimiento, una estructura organizativa del proyecto apropiada y definida con precisión, asignación de responsabilidades concreta, cronogramas que permitan controlar los avances y gestionar eventuales desvíos, instrumentos de apoyo apropiados y estandarizados, criterios de medición objetivos y similares.
Consideramos que la metodología desarrollada en el capítulo 3, cubre tales aspectos y amalgama las herramientas del Marco de gestión con pautas de evaluación convencionales,

que más allá de su formulación concreta es conveniente utilizar, por lo que, sin la pretensión de que sea la única opción válida, puede apoyar a una organización que se proponga implantar Cobit, en virtud de lo cual entendemos haber logrado razonablemente el objetivo planteado al encarar el trabajo.

BIBLIOGRAFIA

BCU, 2003, Comunicación 2003/179 – Instituciones de intermediación financiera – Requisitos para la Administración de las Áreas de Tecnología Informática.

BCU, 2009, CERT - Estándares Mínimos de gestión, Instituciones de intermediación Financiera.

ISACA, 2010, Cobit 5.0 Design Paper, Exposure Draft.

ITGI, 2006, Cobit Mapping: Overview of international IT Guidance, 2nd Edition.

ITGI, 2007, Cobit 4.1 (versiones en Ingles y Español).

ITGI, 2007, Cobit Control Practices: Guidance to achieve control objectives for successful IT Governance, 2nd Edition.

ITGI, 2008, IT Governance Global Status Report.

LEDESMA, C. “Cobit y su implementación en America Latina”, Marzo 2007, Revista Percepciones, (pgs 7 a 14)

ANEXO

Anexo 1 – Regulación

Como complemento, nos parece adecuado hacer referencia a la regulación existente sobre el Marco en nuestra región y en nuestro país, a los efectos de brindar un panorama de la situación actual en América Latina. Para ello citamos un articulo elaborado por la Ing. Cristina Ledesma titulado “COBIT Y SU IMPLEMENTACIÓN EN LA BANCA DE AMÉRICA LATINA”, y seguidamente haremos referencia a la regulación a nivel local.

1.1 Regulación en América Latina

Articulo publicado en la revista *Percepciones* (Capitulo ISACA Montevideo) por la Ing. Cristina Ledesma en el mes de marzo de 2007.

Cobit en América Latina

Desde hace ya algún tiempo, las entidades de controlar en América Latina han venido detectando la necesidad de establecer un marco de control estándar para las entidades financieras que nos permita medirnos, compararnos y controlarnos en forma homogénea. En los últimos años las reuniones que se llevan a cabo por representantes de estas entidades en América Latina, han acordado y promulgado, en forma conjunta, la fuerte recomendación de adoptar Cobit como marco de control de los procesos de TI. Hoy más que nunca, cuando los procesos, la información y los activos en general cruzan las fronteras geográficas a través de Internet, se hace palpable la necesidad de una metodología común.

En casi todos los países de América Latina las entidades regulatorias centrales se han promulgado con distinto énfasis (leyes, circulares, normativas) y han recomendado y promulgado la adopción de Cobit. Si bien ninguna de ellas ha tenido carácter de obligatoriedad, la certeza de ser auditados mediante este marco y las cualidades excelentes del mismo han hecho que sea adoptado en forma general.

Por lo anteriormente expuesto, hoy no se cuenta con una estadística completa de la implementación de Cobit en América Latina para distintos ámbitos empresariales, pero sí se puede estimar un valor aproximado de entre un 40 a 50 por ciento para un nivel de madurez de 2/3.
Recientemente, entidades como la Federación Latinoamericana de Bancos (FELABAN) y la Organización Latinoamericana de la Comunidad de Entidades Financieras (OLACEF) han firmado convenios con ISACA internacional para promulgar y fortalecer la adopción de Cobit. Actividades de estas instituciones, actividades del comité *Govermental Regulatory Agencies Board* (GRAB) de ISACA y las iniciativas de los capítulos locales de ISACA, en cuanto a la capacitación y fomento de Cobit, son vitales para asegurar el éxito de este emprendimiento.

Regulaciones en América Latina

- Argentina-Mendoza: el Tribunal Honorario de Mendoza adopta Cobit, como el marco de control para todas las entidades que proveen servicios contables en la provincia.

- Brasil: la Resolución 2554 del Banco Central (Bacen) define que las instituciones financieras deben tener un modelo de control y gobernabilidad de IT. Los auditores de Bacen realizan su función utilizando Cobit.

- Chile: se trata de una iniciativa con carácter de recomendación.

- Costa Rica: El Consejo Nacional de Supervisión del Sistema Financiero, mediante Artículo 12, del Acta de la Sesión 271-2001, celebrada el 14 de diciembre del 2001, con base en la recomendación del Asesor Técnico y Administrativo del CONASSIF, contenida en la carta PDC-603-2001 del 12 de diciembre del 2001. En relación con la consulta realizada por la Contraloría General de la República, mediante oficio 11889, en torno a la eventual adopción por parte de esa institución del modelo de control en el campo de Tecnología de Información (TI), conocido como Cobit, para la gestión y fiscalización de las tecnologías y sistemas de información del sector público, comunicar al Órgano Controlador que este cuerpo colegiado considera adecuada tal iniciativa, pues se trata de un estándar reconocido en el ámbito internacional que probablemente traerá beneficios, tanto para la Contraloría General de la

República como para la administración de TI, siempre y cuando se logre implementar de manera razonable y planificada.

- Paraguay: Resolución SB No. 00188/2002, por esta se implementa el Manual de Control Interno Informático para las entidades financieras. Es una de las regulaciones más fuertes, no sólo por su carácter de obligatoriedad sino también porque aplica además de a las entidades financieras a todas las firmas y personas profesionales autorizados a dar servicios de auditoria a las mismas.

- Uruguay: el 12 de septiembre del 2003, el Banco Central del Uruguay emitió la Comunicación No. 2003/179 de referencia “Instituciones de Intermediación Financiera- Requisitos para la Administración de las Áreas de Tecnología Informática”; en esta se pone en conocimiento a las instituciones financieras que para la administración de las áreas de tecnología deberán adoptar un sistema de buenas prácticas. La Superintendencia de Instituciones de Intermediación Financiera (SIIF) evalúa y audita los procesos de TI del mercado uruguayo utilizando Cobit.

- Venezuela: si bien no esta formalizado como exigencia a las instituciones financieras, el órgano supervisor emplea Cobit en sus revisiones y auditoria.

Conclusiones

Si bien Cobit es un marco general, su flexibilidad y versatilidad nos permite adaptarlo a cualquier tipo y tamaño de empresa, realizando una implementación gradual y progresiva acorde a los recursos disponibles y acompasando la estrategia empresarial.
Es también muy adaptable e integrable con estándares más específicos como ISO 17799, ISO 9000, ISO 27000, CMM, ITIL, etc.; es el único marco de referencia reconocido internacionalmente como líder en el mercado. Para dar una idea más completa, es el único marco de referencia no corporativo sobre dirección global de la administración de los recursos de tecnología de la información reconocido de manera pública y aplicado de manera oficial.
Si bien aún no es requerido formalmente en forma regulatoria, es un estándar de facto en toda Latinoamérica y es una fuerte recomendación en los ámbitos financieros.
Es parte de la misión de ISACA, la divulgación de Cobit y apoyo en la implementación como

forma de promover la eficiencia y buena gestión de los procesos de tecnología que nos permita compararnos y mejorar día a día en pos de la concreción de los Objetivos de Negocio. En el futuro, continuaremos viendo el crecimiento de Cobit en sus facetas de administración y dirección de los recursos de tecnología. Aparecerán nuevas herramientas de la familia de productos Cobit y nuevos recursos con los cuales mejorar la administración. Se continuará refinando el producto en sí, mejorando la calidad de sus referencias cruzadas, su relacionamiento con otros modelos, estándares y normas. Se procurará institucionalizar y mejorar la calidad de las versiones en otras lenguas y, sin duda, continuará el esfuerzo fundamental del ITGI en la difusión del uso de esta importante base de dirección.

Cristina Ledesma
Gerente de Seguridad y Continuidad del Negocio
de Citibank Uruguay

1.2 Regulación en Uruguay

En nuestro país la regulación referente al Marco Cobit ha sido exclusivamente materia de competencia del Banco Central del Uruguay (BCU), a continuación citamos la *Comunicación Nº 2003/179* del año 2003 y los *Estándares Mínimos de Gestión para Instituciones de Intermediación Financiera (CERT)* publicado en abril de 2009.

C O M U N I C A C I O N N ° 2003/179 del BCU - Ref.: Instituciones de Intermediación Financiera - Requisitos para la Administración de las Áreas de Tecnología Informática.

Se pone en conocimiento de las Instituciones de Intermediación Financiera que para la administración de las **Áreas de Tecnología Informática** deberán adoptar un **Sistema de Gestión** que contemple las mejores prácticas de administración en esta materia. A tales efectos deberán considerar como guía los principios establecidos en el marco de referencia **C.O.B.I.T.** (Control Objectives for Information and Related Technology) emitido por la **Information Systems Audit and Control Foundation** (ISACA) de los Estados Unidos de América.

La Superintendencia de Instituciones de Intermediación Financiera evaluará dicho sistema de gestión, considerando los cuatro dominios descriptos en **C.O.B.I.T.** que a continuación se detallan:

1. **Planificación y Organización -** Comprende los aspectos estratégicos y tácticos y analiza la forma en que las Tecnologías de Información contribuyen al logro de los objetivos del negocio. También refiere a la planificación, comunicación y administración de la consecución de los objetivos estratégicos, poniendo énfasis en la coordinación entre la alta dirección, las áreas usuarias de los servicios de Tecnología de Información y el área de Tecnología de Información.

2. **Adquisición e Implementación -** Contempla la identificación, desarrollo o adquisición de soluciones tecnológicas y su posterior implementación e integración en el proceso del negocio. Abarca asimismo los cambios y el mantenimiento de los sistemas existentes, de forma de garantizar la continuidad de su ciclo de vida.

3. **Entrega y Soporte -** Refiere a la entrega o prestación efectiva de los servicios que son requeridos al área de Tecnología de Información, abarcando la operación tradicional de los sistemas, los aspectos de seguridad, de continuidad de las operaciones, de recuperación y de capacitación, así como todos los procedimientos y procesos que sean necesarios.
4. **Monitoreo -** Los procesos de Tecnología de Información deben ser evaluados en forma regular, para asegurar el cumplimiento de los requerimientos, calidad, seguridad y requerimientos de control. Este dominio contempla la participación de las auditorías interna y externa, a efectos de garantizar la independencia de los juicios y conclusiones elaborados por la gerencia de Tecnología de Información vinculados a los controles efectuados sobre los procesos.

A los efectos de esta evaluación la Superintendencia considerará la aplicación de procedimientos que contemplen una adecuación gradual a la directiva de carácter general atendiendo las características particulares de cada entidad.

ESTANDARES MINIMOS DE GESTION PARA INSTITUCIONES DE INTERMEDIACION FINANCIERA (CERT)

Con el propósito de realizar una evaluación Integral de las instituciones de intermediación financiera, el BCU creo una metodología de calificación denominada CERT.

A continuación hacemos una breve referencia al documento:

El objetivo del CERT es sintetizar la evaluación, por componente y en forma general, de tres aspectos:

− Si existe alguna debilidad en uno de los componentes que requiera atención prioritaria por parte de la Institución

− En qué etapa de resolución se encuentra dicha debilidad

− El impacto potencial de la debilidad encontrada sobre la capacidad de la institución de mantener niveles de solvencia prudenciales en el corto plazo.

Para aplicar la calificación CERT a una entidad, los Supervisores analizarán los siguientes componentes:

C – El Gobierno Corporativo

E – Evaluación económico-financiera

R – Riesgos

T – Tecnología

En particular el componente Tecnológico refiere a la confiabilidad y eficacia de los sistemas de información como herramientas de la gestión, y la gestión de los riesgos tecnológicos.

El CERT establece que los estándares para la evaluación de las áreas de **Tecnología de Información (TI)** tienen como base el conjunto de principios conocido como **COBIT**, en particular los vinculados al dominio de Adquisición e Implementación. Los restantes dominios han sido contemplados en los estándares de Gobierno Corporativo y de Riesgo Operacional.

Anexo 2 – Relacionamiento con otros Marcos y Estándares

A continuación citamos una serie de Marcos y Estándares que dan soporte al Marco Cobit y asimismo son útiles a efectos de buscar oportunidades de mejora, ya que muchos de ellos tratan temáticas específicas.

El cuadro siguiente, muestra la relación entre dichos Marcos y Estándares y los Dominios de Cobit. Como podemos observar el Informe COSO y los Estándares ISO/IEC 17799, FIPS PUB 200, NIST 800, son los que están más relacionados.

Cuadro A.2.1 – Resumen de la relación entre diferentes Marcos y Estándares y los Dominios del Marco de gestión Cobit

	PO	AI	DS	ME
COSO	+	+	0	0
ITIL	0	0	+	-
ISO/IEC 17799	0	+	+	0
FIPS PUB 200	0	+	+	0
ISO/IEC 13335	0	0	0	-
ISO/IEC 15408	-	0	-	-
PRINCE2	0	-	-	-
PMBOK	0	-	-	-
TickIT	-	+	-	0
CMMI	-	+	-	0
TOGAF 8.1	0	-	-	-
IT BPM	0	-	0	-
NIST 800-14	0	+	+	0

(+) Frecuentemente relacionado
(0) Moderadamente relacionado
(-) Raramente ó no relacionado

Seguidamente realizamos una breve descripción de cada uno de ellos:

• COSO

Committee of Sponsoring Organisations of the Treadway Commission (COSO) *Internal Control—Integrated Framework* es un informe que consta de cuatro volúmenes. Se dedica a mejorar la calidad de la información financiera y la ética a través de un control interno efectivo.

• **ITIL**

La IT Infrastructure Library (ITIL) es una serie de ocho libros y se conoce como la única práctica consistente e integral para la gestión de servicios de TI, a efectos de ofrecer servicios de TI de alta calidad. Cabe acotar que ITIL no es un estándar.

• **ISO/IEC 17799:2005**

Constituye un Código de Prácticas para la Gestión de Seguridad de la Información, es un estándar internacional. El objetivo de la norma es proporcionar información a los responsables de la aplicación de seguridad de la información dentro de una organización.

• **FIPS PUB 200**

La Ley "Federal Information Processing Standards (FIPS) 200 Publication"- Requisitos mínimos de seguridad para la Información Federal y los Sistemas de Información es un estándar nacional de los EE.UU. La norma se refiere a la especificación de los requisitos mínimos de seguridad para la información federal en los EE.UU. y para los sistemas de información.

• **ISO/IEC TR 13335**

Denominado "Tecnologías de la Información - Directrices para la Gestión de la seguridad informática" es un informe técnico elaborado con el objetivo de proporcionar orientación sobre los aspectos de la gestión de la seguridad de TI.

• **ISO/IEC 15408:2005**

La norma internacional ISO/IEC 15408:2005 de Técnicas de Seguridad - Criterios de evaluación de seguridad de TI; se basa en los Criterios Comunes para la Evaluación de la Seguridad de la Tecnología de la Información 2.0, publicado por la Comunidad Europea en 1991.

• **PRINCE2**

Projects in Controlled Environments (PRINCE) - Proyectos en ambientes controlados, proporciona un método estructurado para la gestión eficaz de los proyectos. El objetivo es

definir un método de gestión de proyectos para proporcionar un marco, considerando la gran variedad de actividades que se requieren dentro de un proyecto.

• **PMBOK**

Guía para el Project Management Body of Knowledge (PMBOK) es descrito como la suma de conocimientos dentro de la profesión de gestión de proyectos. Proporciona y promueve un lenguaje común para la discusión, la elaboración y la ejecución de proyectos.

• **TickIT**

Es un esquema para la evaluación y certificación del sistema de gestión de la calidad del software que tiene la organización.

• **CMMI**

La publicación Capability Maturity Model Integration (CMMI) es un documento de mejores prácticas utilizado como guía para la mejora de procesos. Ofrece modelos para la ingeniería de sistemas, el desarrollo integrado de productos y procesos y para el proveedor de recursos.

• **TOGAF 8.1**

The Open Group Architecture Framework (TOGAF) (o Esquema de Arquitectura de Open Group, en español) es un esquema de Arquitectura Empresarial que proporciona un enfoque para el diseño, planificación, implementación y gerenciamiento de la arquitectura empresarial de información.

• **IT BPM**

El Manual de referencia de Protección de TI (IT BPM) es un manual que recomienda salvaguardas de seguridad estándar para los sistemas de TI para satisfacer los requisitos de protección de la información y los activos..

• **NIST 800-14**

La publicación de Principios y Prácticas Generalmente Aceptados para la Seguridad de los Sistemas de Tecnología de Información es un conjunto de principios y prácticas para establecer y mantener la seguridad del sistema. Fue elaborado por la US National Institute of

Standards and Technology

Por último, se expone una relación desagregada entre cada uno de estos marcos y estándares y los diferentes procesos del Marco Cobit.

Cuadro A.2.2 – Resumen de la relación entre diferentes Marcos y Estándares y los Procesos del Marco de gestión Cobit

CobiT Process	COSO	ITIL	ISO/IEC 17799	FIPS PUB 200	ISO/IEC TR 13335	ISO/IEC 15408	PRINCE2	PMBOK	TickIT	CMMI	TOGAF 8.1	IT BPM	NIST 800-14
PO 1	+	-	-	-	-	-	-	-	-	-	-	-	-
PO 2	+	-	+	+	+	-	-	-	-	-	+	-	+
PO 3	+	+	+	+	+	-	-	-	-	-	+	+	+
PO 4	+	+	+	+	+	-	-	-	-	-	+	-	+
PO 5	+	+	-	-	-	-	+	+	-	-	-	-	-
PO 6	+	-	+	+	+	-	-	-	-	-	-	+	+
PO 7	+	-	+	+	-	-	-	-	-	-	-	-	+
PO 8	-	-	-	-	-	+	+	+	+	+	-	-	-
PO 9	+	-	+	+	+	-	+	+	-	+	-	-	+
PO 10	-	-	-	-	-	-	+	+	-	+	-	-	-
AI 1	+	-	-	-	+	-	-	-	+	-	+	-	+
AI 2	+	-	+	+	-	+	-	-	+	+	-	-	+
AI 3	+	-	+	+	-	+	-	-	+	-	-	+	+
AI 4	+	+	+	+	-	+	-	-	+	-	-	-	+
AI 5	-	-	-	-	-	-	-	+	+	-	-	-	-
AI 6	+	+	+	+	+	-	-	-	+	+	-	-	+
AI 7	+	+	+	+	+	-	-	-	+	+	-	-	+
DS 1	+	+	-	-	-	-	-	-	-	-	+	-	-
DS 2	-	+	+	+	-	-	-	-	-	-	-	-	+
DS 3	+	+	+	+	-	-	-	-	-	-	-	-	+
DS 4	+	+	+	+	+	-	-	-	-	-	-	+	+
DS 5	+	+	+	+	+	+	-	-	-	-	-	+	+
DS 6	-	+	-	-	-	-	-	-	-	-	-	-	-
DS 7	+	-	+	+	+	-	-	-	-	+	-	-	+
DS 8	-	+	+	+	-	-	-	-	-	-	-	-	+
DS 9	+	+	+	+	-	-	+	-	-	+	-	-	+
DS 10	-	+	-	+	-	-	-	-	-	+	-	-	+
DS 11	+	+	+	+	+	+	-	-	-	+	-	+	+
DS 12	+	-	+	+	+	+	-	-	-	-	-	+	+
DS 13	-	-	+	-	-	-	-	-	-	-	-	-	+
ME 1	-	-	+	-	-	-	-	-	+	+	-	-	+
ME 2	-	-	+	+	+	+	-	-	+	-	-	+	+
ME 3	+	-	-	-	-	-	-	-	-	-	-	-	-
ME 4	+	-	+	+	-	-	-	-	-	-	-	-	+

(+) Frecuentemente relacionado
(-) Raramente o no relacionado

Anexo 3 – Encuesta del IT Governance Institute

En 2007, el IT Governance Institute (ITGI) encargó a PricewaterhouseCoopers (PWC) llevar a cabo la tercera encuesta mundial sobre gerenciamiento de TI, cuyos resultados se exponen en este IT Governance Global Status Report - 2008.

Planteamiento de la encuesta

La Unidad de Encuestas Internacionales de PWC, realizó cerca de 750 entrevistas a personas que ocupan cargos de Dirección, como ser Director Ejecutivo (CEO) o Director de la gestión de la Información (CIO) en todo el mundo.

Objetivos del proyecto

El propósito de la investigación fue llegar a los miembros de la alta dirección para determinar su sentido de las prioridades y las medidas adoptadas en relación con el gerenciamiento de TI, así como su necesidad de herramientas y servicios para ayudar a asegurar una gestión eficaz de TI.

Este objetivo de alto nivel se traduce en los siguientes objetivos más detallados:

1. Relevar y analizar el grado en que el concepto de gerenciamiento de TI es reconocido, establecido y aceptado dentro de las reuniones de Directorio y sobre todo por los Directores de gestión de la Información.
2. Determinar el nivel de experiencia en gerenciamiento de TI existente y que Marcos son conocidos y son (o serán) adoptados.
3. **Medir el grado en que un marco propio de ITGI, los *Objetivos de Control para la información y tecnologías relacionadas* (COBIT), se selecciona y cómo es percibido.**

Citamos las principales conclusiones de la Encuesta a los efectos de nuestro trabajo

- La importancia de TI sigue aumentando.
- La comunicación entre el Departamento de TI y los Usuarios está mejorando lentamente.

- Las buenas prácticas de gerenciamiento de TI son conocidas y aplicadas, pero no universalmente.
- Se están tomando medidas o se están realizando planes para poner en práctica las actividades de gerenciamiento de TI.
- **Respecto a Cobit:**

a. La concientización ha superado el 50% (Cuadro A.3.1) y la adopción y uso siguen representando alrededor del 30% de los encuestados (Cuadro A.3.2).

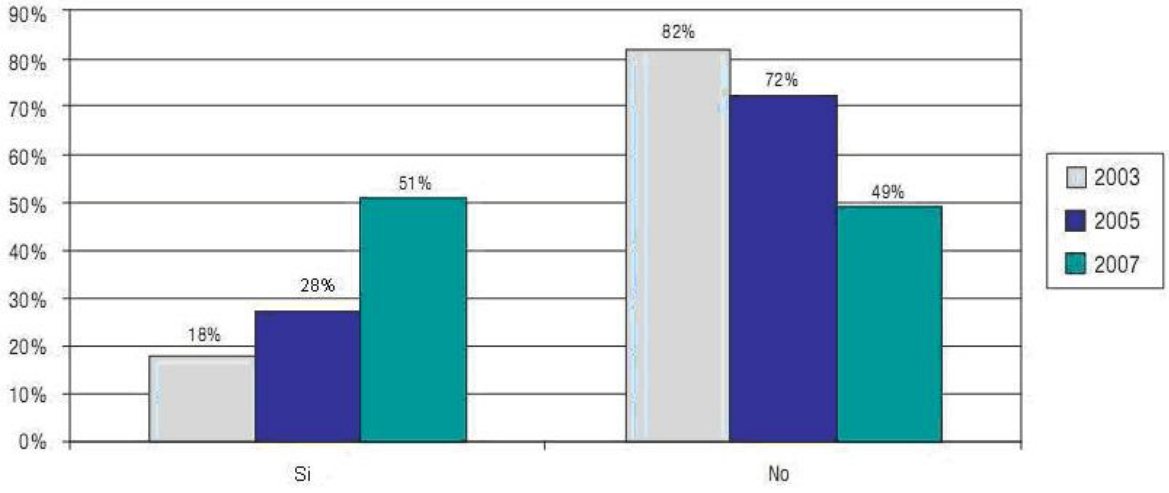
b. Entre 25% y 35% de los encuestados aplica Cobit al pie de la letra o representa la fuente de consulta principal (Cuadro A.3.3).

c. Aproximadamente el 50% de los encuestados indican que Cobit es una de las fuentes de referencia (Cuadro A.3.3).

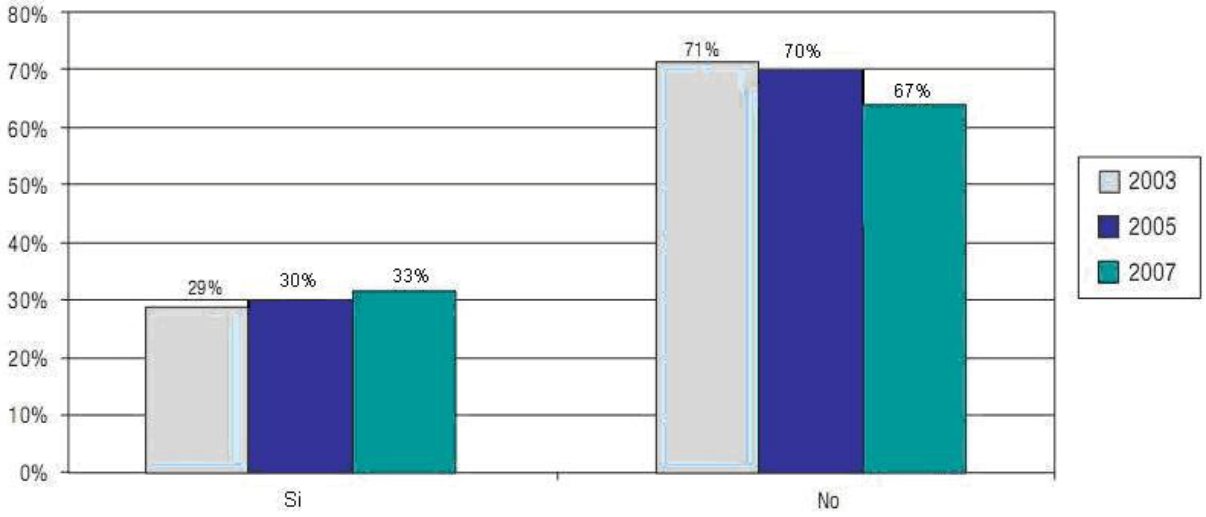
d. En general, existe gran reconocimiento respecto a Cobit. En promedio, tan sólo un 8% de los encuestados no utiliza el Marco (Cuadro A.3.3)

Es preciso mencionar, que para evitar sesgos en los resultados, los investigadores excluyeron en esta sección de la encuesta, a todos los usuarios del Marco Cobit.

Cuadro A.3.1 – Conciencia personal sobre la existencia del Marco Cobit



Cuadro A.3.2 – Uso del Marco Cobit en organizaciones conscientes de su existencia



Cuadro A.3.3 – Uso del Marco Cobit