14 BENEFICIOS PARA EL GOBIERNO EMPRESARIAL: ARTICULANDO COBIT CON ISO 27000 PARA LA EXITOSA IMPLANTACIÓN DE UN GOBIERNO DE TI*

Víctor Manuel Montaño Ardila**

Recibido: Agosto 26 de 2010 Aceptado: Septiembre 29 de 2010

RESUMEN

Concebir y mantener un adecuado modelo de Gobierno de TI es una de las grandes preocupaciones y responsabilidades de la alta gerencia en las organizaciones modernas. Son muchas las propuestas y recomendaciones que mundialmente se exponen, pero solo unas cuantas logran erigirse como las de mayor reconocimiento. Dentro de ellas se destaca el Modelo COBIT como el de mejores lineamientos para la construcción de un Gobierno de TI y la Norma ISO 27001 para la implantación de un adecuado Sistema de Gestión de Seguridad de la Información. Este artículo establece los aspectos articulables entre estos dos modelos y define bases para la construcción de un modelo robusto de Gobierno de TI a partir de la articulación de estándares de reconocimiento mundial y que les permite ser considerados como las "mejores prácticas".

PALABRAS CLAVE

Dominios, Procesos, Actividades, Objetivos de control, Gobierno de TI, Requerimientos de información, Recursos de TI, Focos de Gobierno de TI.

* Resultado parcial del Proyecto de Investigación Guías para la Implantación de un Modelo de Gobierno de Tecnología Informática para las Empresas del Sector Industrial Colombiano cumpliendo con los Lineamientos Establecidos por los Estándares Denominados como Mejores Prácticas. Grupo GICADE. Línea de Investigación: Empresa y Responsabilidad Social Empresarial.

** Ingeniero de Sistemas. Especialista en Auditoría a los Sistemas de Información. Especialista en Estudios Pedagógicos. Estudiante de Maestría en Administración de Empresas. Docente Tiempo Completo Programa de Contaduría Pública. vmontano@cuc.edu.co

GOVERNMENT BUSINESS BENEFITS: ARTICULATING WITH ISO 27000 COBIT FOR THE SUCCESSFUL IMPLEMENTATION OF IT GOVERNANCE

Víctor Manuel Montaño Ardila

ABSTRACT

Conceiving and maintaining a sufficient model for IT governance are among the primary concerns and responsibilities of upper management in modern organizations. Many proposals and recommendations for addressing these issues have been advanced worldwide, but only a select few have achieved the status of being widely known. Of the latter, the COBIT model is recognized as having the strongest guidelines for IT governance, while the ISO 27001 has been identified as the standard for implementation of information security management systems. This article describes the articulable aspects of these two models and provides a foundation for the construction of a robust model of IT governance through the joining of standards that are internationally recognized as best practices in their respective areas.

KEY WORDS

Domains, Processes, Activities, Control objectives, IT Governance, Information requirements, IT Governance focus areas.

INTRODUCCIÓN

La masiva incorporación de las tecnologías de las comunicaciones y la información al mundo de los negocios ha generado profundas transformaciones en las responsabilidades de la alta gerencia en las organizaciones.

Estamos viviendo la era del conocimiento, en la cual la información se convierte en el recurso más importante para las organizaciones y la tecnología informática, como continente y estructura para el almacenaje y procesamiento de ella, se erige como uno de los principales factores críticos de éxito, es decir, gran parte del éxito de las organizaciones modernas depende de la adecuada gestión de la tecnología informática. Por ello los expertos en administración empresarial recomiendan la necesidad de implantar procesos coordinados entre la alta gerencia y el área de TI para movilizar sus recursos de la forma más eficiente en respuesta a requisitos regulatorios, operativos o del negocio. Esto es lo que hoy se denomina *Gobierno de TI* y propende por conformar la estructura organizativa y directiva necesaria para asegurar que TI soporte y facilite el desarrollo de los objetivos estratégicos definidos.

Las organizaciones continúan efectuando importantes inversiones, con un alto y crítico componente de TI, orientadas al crecimiento o transformación del negocio. La experiencia y los resultados de un significativo volumen de investigaciones empíricas han demostrado que tales inversiones generan en las organizaciones espacios y oportunidades importantes para la creación de ventajas estratégicas cuando se gestionan dentro de un efectivo marco de gobierno. Muchas organizaciones han creado valor gracias a la selección de oportunas inversiones y la efectiva gestión desde su concepción, pasando por la implementación, hasta la realización del valor esperado; sin embargo, cuando no existe un gobierno efectivo y una buena gestión, estas inversiones generan una oportunidad igualmente significativa para erosionar o destruir valor.

La existencia de un adecuado modelo de Gobierno de TI garantiza que:

- TI se encuentra alineada con la estrategia del negocio.
- Los servicios y funciones de TI se proporcionan con el máximo valor posible o de la forma más eficiente.
- Todos los riesgos relacionados con TI son conocidos y administrados y los recursos de TI están seguros.

Es importante entender que hoy la inversión en TI no trata solamente de implementar soluciones tecnológicas, sino que se focalizan en implementar cambios y transformaciones en la organización posibilitados por TI. Esto genera mayor complejidad y mayores riesgos que en el pasado, y la aplicación de las prácticas tradicionales de gestión no son suficiente. Entonces es entendible que las inversiones de negocio basadas en TI pueden proveer grandes beneficios, pero solamente aplicando procesos de gobierno y gestión apropiados y el total compromiso de todos los niveles de dirección.

Expertos a nivel mundial han efectuado propuestas para la aplicación de un adecuado modelo de Gobierno de TI; no obstante, cada una de ellas individualmente muestra deficiencias en el tratamiento de algunos aspectos, por ello no es posible seguir pensando de forma excluyente en la adopción de un modelo propuesto. Consideramos que estableciendo aspectos comunes entre varios modelos podemos proponer la construcción de un articulado de mayor robustez que responda de forma efectiva y eficiente a las necesidades de las organizaciones modernas.

ANÁLISIS Y RESULTADOS DEL ESTUDIO

La oportunidad en la toma de decisiones, la necesidad de mantenerse permanentemente enterado de los movimientos comerciales mundiales y poder vincular a los interesados *(stakeholders)* y al entorno en general a través de los sistemas de información son intereses primordiales de las empresas modernas para asegurar su vigencia ante las exigencias de un mundo globalizado, expone Manuel Castells en sus trabajos sobre

Globalización, Tecnología, Trabajo, Empleo y Empresa.

Obtener un mayor beneficio, incrementar el volumen de sus operaciones, ofrecer propuestas de calidad superiores a la competencia y que redunden en lealtad de sus clientes, crear valor para sus propietarios y brindar un ambiente laboral motivador y de crecimiento para sus empleados son premisas alrededor de las cuales se construyen los objetivos de las organizaciones modernas y cuyo interés fundamental es mantener una competitividad sustentable en el largo plazo, afirma Fernando Grosso en la propuesta de su *Modelo para el Desarrollo de la Competitividad de la Empresa*.

Para lograr lo anteriormente expuesto las organizaciones requieren de la implantación de una infraestructura de Tecnología Informática (TI) capaz de responder de forma oportuna, efectiva, eficiente y segura a sus exigencias, es decir, la tecnología se convierte en uno de sus principales factores críticos de éxito y la dependencia continúa en aumento.

Estamos viviendo la era de la información, los tiempos en que esta se convierte en el principal recurso para las organizaciones, por ello estas deben entender y convencerse de que las tecnologías de la información forman una parte integral de ellas y no una mera función técnica; deben concientizarse de su importancia y aceptar formalmente la responsabilidad de los niveles gerenciales sobre la gestión de los sistemas de información.

Para las organizaciones modernas, la información y la tecnología, representan una de las inversiones más valiosas, por tanto las administraciones deben priorizar las expectativas respecto a la función de los servicios de Tecnología Informática (TI) como área de soporte o apoyo a las actividades funcionales de la empresa y meritoriamente sujeta a control sobre sus responsabilidades y los recursos asignados. El objetivo, con respecto a la tecnología informática, es aumentar su productividad, funcionalidad y masificación, incrementando la oportunidad en la entrega de información, reduciendo los costos asociados, ampliando la gama y niveles de servicio, sustentados en paradigmas de calidad, minimizando los riesgos por su aplicación y que pudieran impactar significativamente a la organización.

El establecimiento de una estructura de relaciones y procesos para dirigir y controlar la empresa con el objeto de alcanzar los objetivos corporativos y agregar valor mientras se equilibran los riesgos y el retorno sobre Tecnología Informática (TI) y sus procesos constituyen el concepto de Gobierno de TI, el cual, de acuerdo con el marco de referencia expuesto por el Modelo COBIT - Objetivos de Control para la Información y Tecnología Relacionada, es responsabilidad de los ejecutivos, del consejo de directores y consta de liderazgo, estructuras y procesos organizacionales que garantizan que TI en la empresa sostiene y extiende las estrategias y objetivos organizacionales.

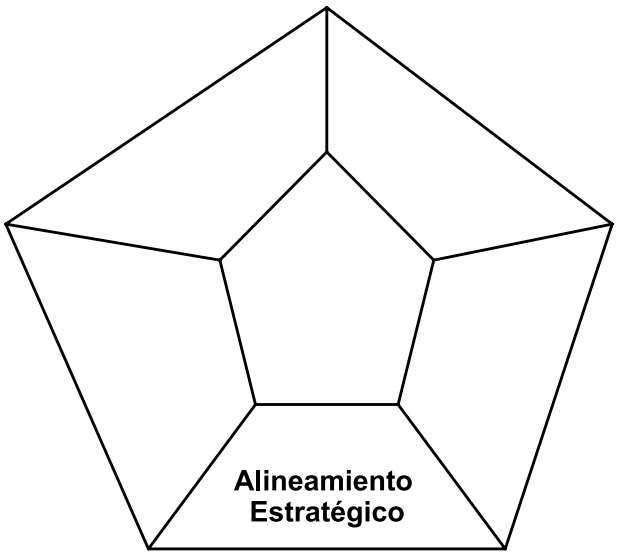
En su propuesta el Modelo COBIT y otros estándares diseñados para la organización, administración y seguridad de la información y la TI, considerados mundialmente como "Mejores Prácticas", establecen que la tecnología informática debería gestionarse como un negocio dentro del negocio cuyo objetivo principal es sostener y proveer recursos para el crecimiento y consolidación de la empresa; como consecuencia la gerencia debe entender su importancia e incluir el Gobierno de TI dentro de su agenda.

Las actividades inherentes al Gobierno de TI propuestas por el Modelo COBIT se clasifican en cinco áreas focales así: Ver Figura 1.

Alineación Estratégica se enfoca en garantizar el vínculo entre los planes de negocio y de TI; en definir, mantener y validar la propuesta de valor de TI; y en alinear las operaciones de TI con las operaciones de la empresa.

Entrega de Valor se refiere a ejecutar la propuesta de valor a todo lo largo del ciclo de en-

Figura 1.
Áreas focales del gobierno de TI



trega, asegurando que TI genere los beneficios prometidos en la estrategia, concentrándose en optimizar los costos y en brindar el valor intrínseco de TI.

Administración de Recursos se trata de la inversión óptima, así como de la administración adecuada de los recursos críticos de TI: aplicaciones, información, infraestructura y personas.

Administración de Riesgos requiere conciencia de los riesgos por parte de los altos ejecutivos de la empresa y la inclusión de las responsabilidades de administración de riesgos dentro de la organización.

Medición del Desempeño monitorea la estrategia de implementación, la terminación del proyecto, el uso de los recursos, el desempeño de los procesos y la entrega del servicio.

La aplicación de las "Mejores Prácticas" brinda tranquilidad a los diferentes niveles y funcionarios de la organización sobre el efectivo, eficiente y seguro apoyo de TI a la operatividad corporativa. ***Ver Tabla 1.***

Las organizaciones exitosas entienden los riesgos asociados con la implantación de TI y propenden por crear efectivos sistemas de control que garanticen tener seguridad razonable de que su principal recurso ***(LA INFORMACIÓN***) se encuentra adecuadamente protegida. Modelos como el COBIT, construidos para obtener una adecuada organización y administración de TI en los negocios plantean acciones y generan compromisos tendientes a proteger la información, pero sus propuestas, fundamentadas en una apropiada comunicación e información de los objetivos institucionales y la definición de políticas claras y concisas, no son suficientes para brindar la protección requerida. Por ello es necesario acudir a los lineamientos planteados por otros estándares, igualmente categorizados como "Mejores Prácticas" y tratar de encontrar puntos de articulación donde se pueda robustecer el modelo base hasta obtener una propuesta aceptable en lo relativo a protección, esto sin perder la esencia de ninguno de los modelos participantes, es decir, la existencia de un modelo no es excluyente.

En nuestro análisis hemos determinado que el Modelo COBIT se constituirá en el eje central de un robusto modelo que puede brindar mejor nivel de protección que el ofrecido de forma individual.

Tabla 1

Grupos de interés en aspectos de gestión de TI

Aspectos de alta gestión basados en Cobit	¿Quién tiene interés primario?			
	Alta Dirección	Gerencias Funcionales	Gerencia de TI	Auditoría/ Cumplimiento
Planificar y Organizar				
¿TI está alineada con las estrategias del negocio?	√	√	√	
¿La empresa está logrando el uso óptimo de los recursos internos y externos?	√	√	√	√
¿Todo el personal de la empresa entiende los objetivos de TI?	√	√	√	√
¿Se ha entendido el impacto de TI en los riesgos de la empresa? ¿Se ha establecido la responsabilidad de la gestión de los riesgos de TI?	√			
¿Se han entendido y se están gestionando los riesgos de TI?		√	√	√
¿La calidad de los sistemas es apropiada para las necesidades de la empresa?		√	√	
Adquirir e Implementar				
¿Es probable que los nuevos proyectos entreguen soluciones que satisfagan las necesidades del negocio?		√	√	
¿Es probable que los nuevos proyectos se entreguen a tiempo y dentro del presupuesto?		√	√	√
¿Los nuevos sistemas trabajarán correctamente cuando se implementen?		√	√	√
¿Los cambios serán realizados sin trastornar la actual operación del negocio?		√	√	
Entrega y Soporte				
¿Los servicios de TI se entregan en línea con los requerimientos y las prioridades del negocio?		√	√	
¿Están optimizados los costos de TI?		√	√	√
¿El personal está capacitado para utilizar los sistemas de TI en forma productiva y segura?		√	√	
¿Los sistemas de TI tienen adecuada confidencialidad, integridad y disponibilidad?		√	√	√
Monitorear y Evaluar				
¿Se puede medir el desempeño de TI y detectar los problemas antes que sea demasiado tarde?	√	√	√	
¿Los controles internos están operando eficazmente?	√			√
¿La empresa está cumpliendo las disposiciones regulatorias?	√	√	√	√
¿El gobierno de TI es eficaz?	√	√	√	√

ESTÁNDAR ISO 27000 ***(para la Gestión de la Seguridad de la Información)***

Los estándares pertenecientes a la familia de la Norma ISO 27000 apuntan a proveer lineamientos efectivos para la Gestión de la Seguridad de la Información en las organizaciones. Cada uno de los estándares pertenecientes a la familia tiene un objetivo que exponemos a continuación:

- **ISO 27000:** Contiene términos y definiciones que se emplean en toda la serie 27000.
- **ISO 27001:** Contiene la estructura y requerimientos para la implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI).
- **ISO 27002:** Establece y describe los objetivos de control y controles recomendables a tener en cuenta para la construcción de un adecuado SGSI. ***Anexo A de ISO 27001.***
- **ISO 27003:** Contiene una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases.
- **ISO 27004:** Especifica las métricas y las técnicas de medida aplicables para determinar la eficiencia y efectividad de la implantación de un SGSI y de los controles relacionados.
- **ISO 27005:** Consiste en una guía para la gestión del riesgo de la seguridad de la información y servirá, por tanto, de apoyo a la ISO 27001 y a la implantación de un SGSI.
- **ISO 27006:** Especifica el proceso de acreditación de entidades de certificación y el registro de SGSI.

El Estándar Internacional ISO 27001, diseñado por la Organización Internacional de Estandarización - ISO y la Comisión Electrotécnica Internacional - IEC, es un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI).

El propósito de un Sistema de Gestión de la Seguridad de la Información no es garantizar la seguridad –que nunca podrá ser absoluta– sino asegurar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, continua, repetible, eficiente y adaptada a los cambios que se produzcan en la organización, los riesgos, el entorno y las tecnologías.[1]

El SGSI apunta a proteger la información de la organización independientemente del medio en que se encuentre contenida y se extiende hasta la información confidencial de trabajadores y colaboradores; esta acción se logra mediante la identificación y evaluación de los riesgos asociados con la información que afectan al negocio, con el objeto de proveer actividades, procesos y procedimientos para su apropiado control, tratamiento y mejora continua evitando inversiones innecesarias producto de una errada valoración de dichos riesgos. Lo importante es proveer niveles adecuados de confidencialidad, integridad y disponibilidad de información sensitiva, lo cual es necesario para lograr resultados deseables en lo relativo a competitividad, rentabilidad, conformidad legal e imagen empresarial, es decir, facilitar la obtención de los objetivos corporativos y asegurar beneficios económicos.

Para la concepción, operatividad, mantenimiento y mejora del SGSI propuesto, el estándar ISO 27001 adopta la metodología para la *Gestión del riesgo* definida por el *estándar AS/NZ 4360* y clasifica las acciones a desarrollar dentro del ciclo de la administración PHVA (Planear - Hacer - Verificar - Actuar), de la siguiente manera: ***Ver Figura 2***.

- ✓ **Planear:** Establecer el SGSI.
- ✓ **Hacer:** Implementar y utilizar el SGSI.
- ✓ **Verificar:** Monitorear y revisar el SGSI.
- ✓ **Actuar:** Mantener y mejorar el SGSI.

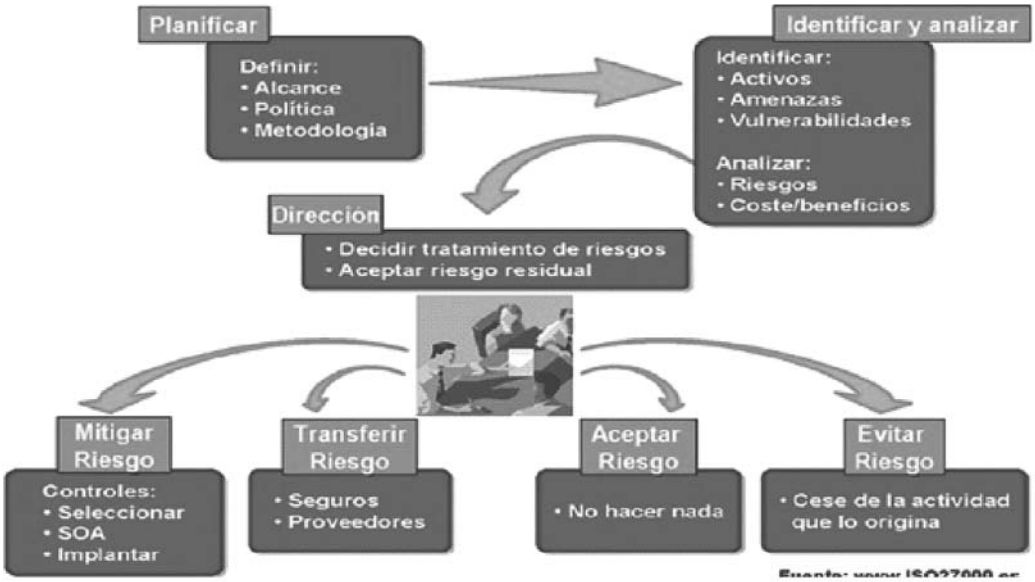
ASPECTOS ARTICULABLES ENTRE MODELO COBIT Y LA NORMA ISO 27000

El *Marco de Referencia de COBIT* consta de ob-

1. Tomado de "Preguntas más Frecuentes, doc_faq_all.pdf pág. 8", www.iso27000.es

FIGURA 2

Modelo para la Gestión de Riesgos



Fuente: www.ISO27000.es

jetivos de control de TI de alto nivel y de una estructura general para su clasificación y presentación. La teoría subyacente para la clasificación seleccionada se refiere a que existen, en esencia, tres niveles de actividades de TI al considerar la administración de sus recursos. Comenzando por la base, encontramos las actividades y tareas necesarias para alcanzar un resultado medible. Las actividades cuentan con un concepto de ciclo de vida, mientras que las tareas son consideradas más discretas.

Los procesos se definen en un nivel superior como una serie de ***actividades*** o tareas conjuntas con "cortes" naturales (de control). En el nivel más alto, los ***procesos*** son agrupados de manera natural en ***dominios***. Su agrupamiento natural es denominado frecuentemente como dominios de responsabilidad en una estructura organizacional y está en línea con el ciclo administrativo o ciclo de vida aplicable a los procesos de TI.

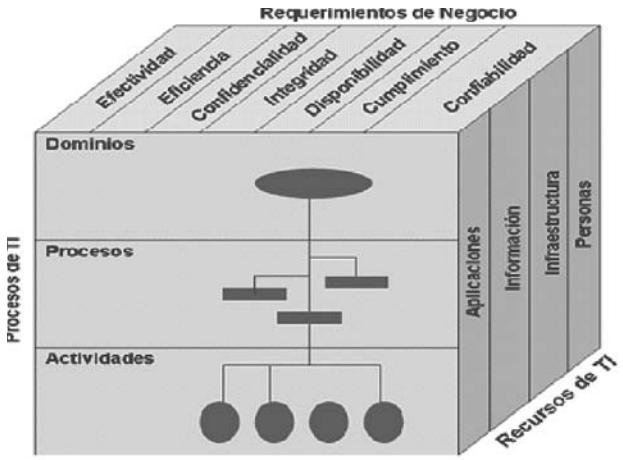
La siguiente figura muestra el Cubo de COBIT, donde puede evidenciarse la relación entre los ***Procesos de TI***, los ***Requerimientos de Información del Negocio*** y los ***Recursos de TI*** que lo soportan. En síntesis, los Recursos de TI son manejados por Procesos de TI para lograr Metas de TI que respondan a los Requerimientos del Negocio. Este es el principio básico del marco de trabajo COBIT. ***Ver Figura 3.***

La versión COBIT 4.1 dispone de cuatro dominios: Planificar y organizar, Adquirir e implantar, Entrega y soporte, y Monitorear y evaluar. Dentro de estos se encuentran distribuidos 34 procesos (10, 7, 13 y 4) respectivamente que contienen 310 actividades de control.

Dentro del Marco de Navegación del Modelo COBIT para cada uno de los Procesos dispuestos dentro de cada Dominio se identifican gráfica y claramente los ***Requerimientos de Información*** *(indicando su importancia con P = Primaria y S = Secundaria)*, el ***Área Focal de Gobierno de TI*** *(maneja dos tonalidades de azul para destacar el interés Primario o Secundario por cada foco)* y los ***Recursos de TI*** *(marcando con un "chulo" a los involucrados en cada proceso)* implicados. ***Ver Figura 4.***

La Norma ISO 27001 en su modelo para la construcción del Sistema de Gestión de la Seguridad de la Información - SGSI establece 11 ***Do-***

FIGURA 3
El Cubo de Cobit



Fuente: Cobit 4.1 - ISACA

FIGURA 4
Criterios de información, áreas focales y recursos del Gobierno de TI

minios (cuadros que conforman el marco de la ***Figura 5***), disponiendo para cada uno de ellos ***Objetivos de Control*** y Controles (e involucra tres recursos a saber: las ***Personas***, los ***Procesos*** y los ***Sistemas Informáticos.***

Un Sistema de Gestión de la Seguridad de la Información (SGSI) es una forma sistemática de abordar la gestión de la información empresarial para protegerla concentrándose en cuatro ***Criterios*** fundamentales:

- ✓ ***Confidencialidad:*** Acceso únicamente por autorizados.
- ✓ ***Integridad:*** Exactitud y completitud.
- ✓ ***Disponibilidad:*** Acceso de los usuarios autorizados cuando lo requieran.
- ✓ ***No Repudio:*** Suficiencia en evidencias de acciones realizadas.

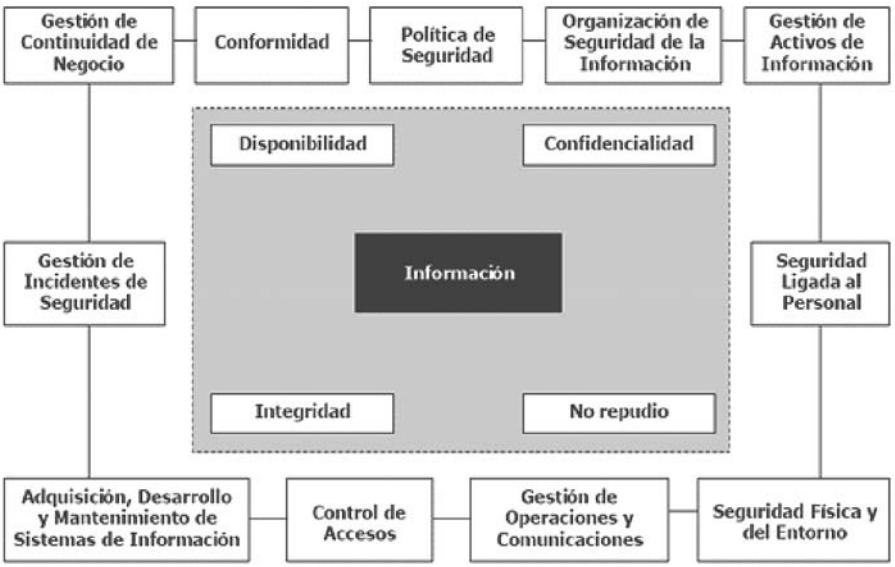
Como puede observarse los tres primeros *Criterios* igualmente son considerados directamente por el Modelo COBIT dentro de los *Requerimientos de Información del Negocio* y los elementos utilizados para el *No Repudio* pueden ser claramente identificados dentro de la propuesta de COBIT. Estos criterios constituyen los principales aspectos para la articulación de los dos modelos.

Para establecer cómo y cuáles aspectos podrán articularse entre los modelos, se analizarán todos los *Procesos* pertenecientes a cada uno de los *Dominios* establecidos en la estructura del Mo-

delo COBIT identificando aquellos donde exista coincidencia dentro de los *Requerimientos de Información* establecidos por el Modelo COBIT y los Criterios definidos por la Norma ISO 27001, las cuales son: Disponibilidad, Confidencialidad e Integridad y No Repudio.

mejorar la seguridad de la información corporativa. Expone, en distintos campos, una serie de aspectos a tratar en relación a la seguridad, los objetivos de seguridad a lograr, los controles a considerar para cada objetivo y un conjunto de "sugerencias" para cada uno de esos controles.

FIGURA 5
Dominios de la Norma ISO 27001



El beneficio de la articulación de estos dos modelos consiste en obtener una "mejor práctica" para la implantación de las actividades de control que permitirán lograr la adecuada, efectiva y eficiente implementación del proceso propuesto por el Modelo COBIT. En palabras simples la Norma ISO 27001, apropiando las recomendaciones de *Objetivos de Control* y *Controles* expuestos en la Norma ISO 27002 (Anexo A), define el **¿cómo hacerlo?** para la implantación del **¿qué hacer?** propuesto por el Modelo COBIT en cada uno de los Procesos factibles de articular.

Para claridad del lector no familiarizado con las Normas ISO 27001 e ISO 27002, considero importante hacer la siguiente aclaración para evitar confusiones conceptuales o imaginar un lapsus por parte de este escritor.

La Norma ISO 27002 es una guía para, en distintos ámbitos, conocer qué se puede hacer para

Por su parte la ISO 27001 habla de los controles de forma residual. El núcleo de la ISO 27002 queda reducido a un listado de objetivos de control y controles incluidos en un anexo (normativo, pero anexo). No aparecen en el cuerpo de la norma, porque en absoluto son la parte más importante. El foco de la ISO 27001 es la gestión de la seguridad, en forma de SISTEMA DE GESTIÓN, es decir, lo que importa en esta es que los riesgos se analicen y se gestionen, que la seguridad se planifique, se implemente y, sobre todo, se revise, se corrija y mejore.

En la ***Figura Nº 6*** presentamos un esquema de la forma como la Norma ISO 27001 plantea sus recomendaciones para concretar la implantación de un *Objetivo de Control*.

En la tabla que exponemos a continuación destacamos, por cada Dominio del Modelo CO-

FIGURA 6
Esquema del Dominio A. 8. Norma ISO 27001:2005 - Seguridad Ligada al Personal

A.8.3 ***Terminación de Contrato o Cargo de un Empleado*** **Objetivo:** Asegurar que empleados, contratistas o terceros realicen su retiro de la empresa de forma organizada.		
A.8.3.1.	Terminación de responsabilidades	***Control:*** Establecer un procedimiento con responsabilidades y funciones claramente definidas para registrar la terminación de contrato de empleados, contratistas y terceros.
A.8.3.2.	Reintegro de activos	***Control:*** Todos los empleados, contratistas o terceros que hayan prestado sus servicios a la empresa deben retornar todos los activos y herramientas que les fueron entregados para el desarrollo de sus funciones y labores.
A.8.3.3.	Remoción de los derechos de acceso	***Control:*** Todos los permisos otorgados a empleados, contratistas o terceros para acceder a los sistemas de información de la empresa deberán ser removidos al finalizar el contrato o si se efectúa alguna reasignación.

BIT, los Procesos articulables con la Norma ISO 27002. Expondremos la declaración del Proceso, los Focos de Gobierno de TI hacia los que apunta, los Requerimientos de Información que satisface, los Recursos involucrados y los Objetivos de Control de la Norma ISO 27002 que poseen información suficiente y necesaria para apoyar la implantación de cada actividad establecida en cada proceso. Para las dos primeras columnas antepondremos a cada ítem una P (Primaria) o una S (Secundaria) para señalar el grado de importancia de cada uno de ellos.

COBIT 4.1. Dominio: Planificar y Organizar - PO			
PO2: Definir la arquitectura de información			
La función de los sistemas de información crea y actualiza periódicamente el modelo de información del negocio y define los sistemas apropiados para optimizar el uso de esta información. Esto abarca el desarrollo de un diccionario de datos y las reglas de sintaxis de datos de la organización, el esquema de clasificación de los datos y los niveles de seguridad. Este proceso mejora la calidad de la gestión de toma de decisiones, al garantizar la entrega de información confiable y segura, facilitando la racionalización de los recursos de sistemas de información para satisfacer adecuadamente las estrategias empresariales. Este proceso de TI también es necesario para consolidar la responsabilidad de reportar el estado de la integridad y la seguridad de los datos, ampliando la eficacia y el control del intercambio de información entre las aplicaciones y la organización.			
Focos de Gobierno de TI	**Requerimientos de Información**	**Recursos Involucrados**	**Objetivos de Control de ISO/IEC 27002:2005**
P. Alineación Estratégica P. Administración de Recursos S. Administración de Riesgos S. Entrega de Valor	P. Eficiencia P. Integridad S. Efectividad S. Confidencialidad	• Aplicaciones • Información	7. Gestión de Activos 10. Gestión de Comunicaciones y Operaciones 11. Control de Acceso
PO3: Determinar la orientación tecnológica			
La función de servicios de información determina la dirección tecnológica para apoyar al negocio. Esto requiere la creación de un plan de infraestructura tecnológica y un consejo de arquitectura que establece y gestiona expectativas claras y realistas de lo que la tecnología puede ofrecer en términos de productos, servicios y mecanismos de entrega. El plan se actualiza periódicamente y abarca aspectos tales como la arquitectura de sistemas, dirección tecnológica, planes de adquisición, estándares, estrategias de migración y contingencia. Esto permite una respuesta oportuna a los cambios en el entorno competitivo, las economías de escala sobre el personal y las inversiones en sistemas de información, así como una mejor interoperabilidad de plataformas y aplicaciones.			

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Administración de Recursos S. Alineación Estratégica S. Administración de Riesgos S. Entrega de Valor	P. Efectividad P. Eficiencia	• Aplicaciones • Infraestructura	5. Política de Seguridad 6. Aspectos Organizativos de Seguridad de Información 10. Gestión de Comunicaciones y Operaciones 11. Control de Acceso 14. Gestión de la Continuidad del Negocio

PO4: Definir los procesos, organización y relaciones de TI

Una organización de TI está definida con base en las necesidades de personal, las aptitudes, funciones, obligación de rendir cuentas, autoridad, roles, responsabilidades y la supervisión. Esta organización se incrusta en un marco de procesos de TI que garantice la transparencia y el control, así como la participación de altos ejecutivos y la gerencia de la organización. Un comité de estrategia asegura que la junta de supervisión de TI, y uno o más comités de dirección en el que participan las áreas de negocios y de TI, determinen la priorización de los recursos de TI de acuerdo a las necesidades del negocio. Se habilitan los procesos, las políticas y los procedimientos administrativos para todas las funciones, con especial atención al control y garantía de calidad, gestión de riesgos, seguridad de la información, propiedad de datos y sistemas, y la segregación de funciones. La TI es involucrada en los procesos relevantes de decisión para asegurar el soporte oportuno de los requerimientos del negocio.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Administración de Recursos P. Administración de Riesgos S. Alineación Estratégica	P. Efectividad P. Eficiencia	• Personas	6. Aspectos Organizativos de Seguridad de Información 7. Gestión de Activos 8. Seguridad ligada a los Recursos Humanos 9. Seguridad Física y Ambiental 10. Gestión de Comunicaciones y Operaciones 15. Cumplimiento

PO5: Gestionar la inversión en TI

Se establece y mantiene un marco de gestión del programa de inversiones facilitadas por TI, que abarca los costos, beneficios, prioridades dentro del presupuesto, un proceso formal de presupuestación y gestión contra el presupuesto. Las partes interesadas son consultadas para identificar y controlar los costos y beneficios totales dentro del contexto de los planes estratégicos y tácticos de TI, ejecutando acciones correctivas cuando se necesiten. El proceso fomenta la asociación entre TI y las partes interesadas de la empresa, facilita el uso eficaz y eficiente de los recursos de TI y promueve la transparencia y la rendición de cuentas sobre el costo total de propiedad (TCO), la realización de beneficios y el ROI de las inversiones facilitadas por TI.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Entrega de Valor S. Administración de Riesgos S. Alineación Estratégica S. Medición del Desempeño	P. Efectividad P. Eficiencia S. Cumplimiento	• Personas • Aplicaciones • Infraestructura	6. Política de Seguridad 13. Gestión de Incidentes en Seguridad de Información

PO6: Comunicar las aspiraciones y dirección de la gerencia

La gerencia desarrolla un marco de control de TI en la empresa, define y comunica las políticas. Se implementa un programa de comunicación permanente, aprobado y apoyado por la dirección, para articular la misión, los objetivos de servicio, las políticas y procedimientos, etc. La comunicación apoya el logro de los objetivos de TI y asegura el conocimiento y la comprensión de los riesgos de TI y del negocio, los objetivos y la dirección. El proceso garantiza el cumplimiento de las leyes y regulaciones vigentes.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Administración de Riesgos P. Alineación Estratégica	P. Efectividad S. Cumplimiento	• Información • Personas	5. Política de Seguridad 6. Aspectos Organizativos de Seguridad de Información 7. Gestión de Activos 8. Seguridad ligada a los Recursos Humanos 9. Seguridad Física y Ambiental 10. Gestión de Comunicaciones y Operaciones 11. Control de Acceso 12. Adquisición, Desarrollo y Mantenimiento de SI 15. Cumplimiento

PO7: Gestión de los recursos humanos de TI

Se forma y mantiene una plantilla competente para la creación y entrega de servicios de TI al negocio. Esto se logra a través de prácticas definidas y acordadas que apoyen el reclutamiento, el entrenamiento, la evaluación del desempeño, la promoción y los ceses. Este proceso es crítico, ya que las personas son un activo importante; el buen gobierno y el entorno de control interno dependen en gran medida de la motivación y competencia del personal.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Administración de Recursos P. Alineación Estratégica S. Medición del Desempeño S. Administración de Riesgos	P. Efectividad P. Eficiencia	• Personas	8. Seguridad ligada a los Recursos Humanos

PO8: Gestión de la calidad

Un Sistema de Gestión de Calidad (SGC) es desarrollado y mantenido, incluyendo estándares y procesos de adquisición y desarrollo probados. Esto es posible por la planificación, implementación y el mantenimiento del SGC mediante requerimientos, procedimientos y políticas claras de calidad. Los requisitos de calidad son establecidos y comunicados mediante indicadores cuantificables y alcanzables. La mejora continua se consigue a través del monitoreo permanente, el análisis y la actuación sobre las desviaciones, y comunicando los resultados a las partes interesadas. La gestión de la calidad es esencial para asegurar que TI entregue valor al negocio, la mejora continua y la transparencia para los accionistas.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Alineación Estratégica S. Administración de Riesgos S. Entrega de Valor	P. Efectividad P. Eficiencia S. Integridad S. Confiabilidad	• Personas • Aplicaciones • Infraestructura • Información	6. Aspectos Organizativos de Seguridad de Información 12. Adquisición, Desarrollo y Mantenimiento de SI

PO9. Evaluar y gestionar los riesgos de TI

Se crea y mantiene un marco de gestión de riesgo que documenta un nivel común y consensuado de riesgos de TI, estrategias de mitigación y riesgos residuales. Se identifica, analiza y evalúa cualquier impacto potencial en las metas de la organización causado por un evento no planificado. Se adoptan estrategias de mitigación de riesgo para minimizar el riesgo residual a un nivel aceptable. El resultado de la evaluación es entendible para las partes interesadas y expresado en términos financieros para permitirles alinear el riesgo a un nivel de tolerancia aceptable.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Alineación Estratégica S. Administración de Riesgos	P. Confidencialidad P. Integridad P. Disponibilidad S. Efectividad S. Eficiencia S. Cumplimiento S. Confiabilidad	• Personas • Aplicaciones • Infraestructura • Información	5. Política de Seguridad 13. Gestión de Incidentes en Seguridad de Información 14. Gestión de la Continuidad del Negocio

COBIT 4.1. Dominio: Adquirir e Implementar - AI

AI1: Identificar soluciones automatizadas

La necesidad de una nueva aplicación o función requiere de análisis previo a la adquisición o construcción para asegurar que se satisfagan los requerimientos del negocio de una manera eficaz y eficiente. Este proceso cubre la definición de necesidades, consideración de fuentes alternas, revisión de factibilidades tecnológica y económica, ejecución de análisis de riesgo y de costo-beneficio, concluyendo en una decisión final para "hacer" o "comprar". Todos estos pasos permiten que las organizaciones minimicen el costo de adquirir e implementar soluciones mientras se asegura el logro de sus objetivos.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Alineación Estratégica P. Entrega de Valor S. Administración de Riesgos S. Administración de Recursos	P. Efectividad S. Eficiencia	• Aplicaciones • Infraestructura	6. Aspectos Organizativos de Seguridad de Información 8. Seguridad ligada a los Recursos Humanos 10. Gestión de Comunicaciones y Operaciones 11. Control de Acceso 12. Adquisición, Desarrollo y Mantenimiento de Si

AI2: Adquirir y mantener software aplicativo

Las aplicaciones se hacen disponibles en línea con los requerimientos del negocio. Este proceso cubre el diseño de las aplicaciones, la inclusión correcta de los controles de aplicación y los requerimientos de seguridad, así como el desarrollo y la configuración alineados con los estándares. Esto le permite a las organizaciones apoyar apropiadamente sus operaciones de negocios con las aplicaciones automatizadas correctas.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Alineación Estratégica P. Entrega de Valor S. Administración de Riesgos	P. Efectividad P. Eficiencia S. Integridad S. Confiabilidad	• Aplicaciones	6. Aspectos Organizativos de Seguridad de Información 7. Gestión de Activos 10. Gestión de Comunicaciones y Operaciones 11. Control de Acceso 13. Gestión de Incidentes en Seguridad de Información 15. Cumplimiento

AI3: Adquirir y mantener infraestructura tecnológica

Las organizaciones tienen procesos para la adquisición, implementación y actualización de su infraestructura tecnológica, lo que requiere un enfoque planificado para la adquisición, el mantenimiento y la protección de la infraestructura, en línea con estrategias tecnológicas consensuadas, y la provisión de ambientes de desarrollo y prueba. Esto asegura la disponibilidad continua de soporte tecnológico para las aplicaciones del negocio.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Administración de Recursos	S. Efectividad P. Eficiencia S. Integridad S. Disponibilidad	• Infraestructura	9. Seguridad Física y Ambiental 10. Gestión de Comunicaciones y Operaciones 12. Adquisición, Desarrollo y Mantenimiento de SI

AI4: Facilitar la operación y el uso

La disponibilidad del conocimiento sobre los sistemas nuevos requiere la producción de documentación y manuales para usuarios y para TI, a la vez que proporciona entrenamiento para asegurar el uso y operación adecuados de las aplicaciones y la infraestructura.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
S. Alineación Estratégica P. Entrega de Valor S. Administración de Riesgos S. Administración de Recursos	S. Integridad S. Disponibilidad P. Efectividad P. Eficiencia S. Cumplimiento S. Confiabilidad	• Aplicaciones • Infraestructura • Personas	10. Gestión de Comunicaciones y Operaciones 13. Gestión de Incidentes en Seguridad de Información

AI5: Adquirir recursos de TI

Se necesita adquirir recursos de TI, incluyendo al personal, hardware, software y servicios, lo que requiere de la definición y cumplimiento de los procedimientos de adquisiciones, selección de proveedores, definición de aspectos contractuales y la adquisición propiamente dicha, asegurando que la organización tenga todos los recursos de TI de forma oportuna y económica.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
S. Entrega de Valor P. Administración de Recursos	S. Efectividad P. Eficiencia S. Cumplimiento	• Personas • Aplicaciones • Infraestructura • Información	6. Aspectos Organizativos de Seguridad de Información 10. Gestión de Comunicaciones y Operaciones 12. Adquisición, Desarrollo y Mantenimiento de SI

AI6: Gestionar cambios

Todos los cambios relacionados con la infraestructura y aplicaciones dentro del entorno de producción, inclusive los mantenimientos de emergencia y los parches, se gestionan formalmente y de modo controlado. Los cambios (inclusive sobre procedimientos, procesos y parámetros de servicio y de sistema) son registrados, evaluados y autorizados antes de su implementación y comparados contra los resultados luego de su implementación. Esto asegura una mitigación de los riesgos que afectan negativamente la estabilidad o integridad del entorno de producción.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
S. Entrega de Valor P. Administración de Recursos	P. Integridad P. Disponibilidad P. Efectividad P. Eficiencia S. Confiabilidad	• Personas • Aplicaciones • Infraestructura • Información	10. Gestión de Comunicaciones y Operaciones 11. Control de Acceso 12. Adquisición, Desarrollo y Mantenimiento de SI

AI7: Instalar y acreditar soluciones y cambios

Los nuevos sistemas necesitan entrar en operación una vez que se ha completado el desarrollo, lo que requiere de pruebas adecuadas en un entorno dedicado con datos de prueba relevantes, la definición del despliegue e instrucciones de migración, la planificación de la liberación, el paso a producción y una revisión luego de su implementación. Esto asegura que los sistemas en operación estén alineados con las expectativas y resultados acordados.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Entrega de Valor S. Administración de Recursos S. Alineación Estratégica S. Medición del Desempeño S. Administración de Riesgos	S. Integridad S. Disponibilidad P. Efectividad S. Eficiencia	• Personas • Aplicaciones • Infraestructura • Información	6. Aspectos Organizativos de Seguridad de Información 8. Seguridad ligada a los Recursos Humanos 10. Gestión de Comunicaciones y Operaciones 12. Adquisición, Desarrollo y Mantenimiento de SI

COBIT 4.1. Dominio: Entregar y dar soporte - DS

DS1: Definir y gestionar los niveles de servicio

La definición documentada de acuerdos sobre los servicios de TI y los niveles de servicio facilita la comunicación efectiva entre la gerencia de TI y los clientes del negocio respecto de los servicios requeridos. Este proceso también incluye el monitoreo y el reporte periódico y oportuno a los interesados sobre el cumplimiento de los niveles de servicio, facilitando el alineamiento entre los servicios de TI y los requisitos relacionados con el negocio.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Entrega de Valor P. Administración de Recursos P. Alineación Estratégica P. Medición del Desempeño	S. Integridad S. Disponibilidad P. Efectividad P. Eficiencia S. Cumplimiento S. Confiabilidad S. Confidencialidad	• Personas • Aplicaciones • Infraestructura • Información	10. Gestión de Comunicaciones y Operaciones

DS2: Gestionar los servicios de terceros

La necesidad de asegurar que los servicios de terceros (proveedores, vendedores y asociados) cumplan con los requerimientos del negocio requiere un proceso de gestión de terceros. Este proceso se realiza definiendo claramente los roles, responsabilidades y expectativas en los acuerdos con terceros así como la revisión y monitoreo de tales acuerdos en busca de eficacia y cumplimiento. La gestión eficaz de servicios de terceros minimiza el riesgo de negocio asociado con el incumplimiento de proveedores.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Entrega de Valor P. Administración de Riesgos S. Administración de Recursos S. Medición del Desempeño	S. Integridad S. Disponibilidad P. Efectividad P. Eficiencia S. Cumplimiento S. Confiabilidad S. Confidencialidad	• Personas • Aplicaciones • Infraestructura • Información	6. Aspectos Organizativos de Seguridad de Información 8. Seguridad ligada a los Recursos Humanos 10. Gestión de Comunicaciones y Operaciones 12. Adquisición, Desarrollo y Mantenimiento de SI 15. Cumplimiento

DS3: Gestionar el desempeño y la capacidad

La necesidad de gestionar el desempeño y la capacidad de los recursos de TI requiere de un proceso para su revisión periódica, lo que incluye pronosticar necesidades futuras basándose en requerimientos de carga de trabajo, almacenamiento y contingencia. Este proceso provee la garantía de que los recursos de información que soportan los requerimientos del negocio estén disponibles en forma continua.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
S. Entrega de Valor P. Administración de Recursos S. Alineación Estratégica S. Medición del Desempeño S. Administración de Riesgos	S. Disponibilidad P. Efectividad P. Eficiencia	• Aplicaciones • Infraestructura	10. Gestión de Comunicaciones y Operaciones

DS4: Garantizar la continuidad del servicio

La necesidad de proveer servicios continuos de TI requiere del desarrollo, mantenimiento y prueba de planes de continuidad de TI, utilizar almacenamiento de respaldo fuera de las instalaciones y proporcionar entrenamiento periódico sobre el plan de continuidad. Un proceso eficaz de servicio continuo minimiza la probabilidad y el impacto de una interrupción de un servicio crítico de TI en funciones y procesos clave del negocio.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Entrega de Valor P. Administración de Riesgos S. Administración de Recursos S. Alineación Estratégica S. Medición del Desempeño	P. Disponibilidad P. Efectividad S. Eficiencia	• Personas • Aplicaciones • Infraestructura • Información	6. Aspectos Organizativos de Seguridad de Información 10. Gestión de Comunicaciones y Operaciones 14. Gestión de la Continuidad del Negocio

DS5: Garantizar la seguridad de los sistemas

La necesidad de mantener la integridad de la información y proteger los activos de TI precisa de un proceso de gestión de seguridad, lo que incluye establecer y mantener los roles, las responsabilidades, políticas, los estándares y procedimientos de seguridad de TI, además, realizar monitoreos de seguridad y pruebas periódicas e implementar acciones correctivas para identificar debilidades de seguridad o incidentes. Una gestión efectiva de seguridad protege todos los activos de TI para minimizar el impacto de vulnerabilidades de seguridad e incidentes en el negocio.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Administración de Riesgos	P. Integridad P. Confidencialidad S. Disponibilidad S. Cumplimiento S. Confiabilidad	• Personas • Aplicaciones • Inflaestructura • Información	5. Política de Seguridad 6. Aspectos Organizativos de Seguridad de Información 8. Seguridad ligada a los Recursos Humanos 9. Seguridad Física y Ambiental 10. Gestión de Comunicaciones y Operaciones 11. Control de Acceso 12. Adquisición, Desarrollo y Mantenimiento de SI 13. Gestión de Incidentes en Seguridad de Información 15. Cumplimiento

DS7: Educar y entrenar a los usuarios

La educación efectiva de todos los usuarios de TI, incluidos a los que trabajan en TI, requiere identificar las necesidades de formación de cada grupo de usuarios, la definición y ejecución de una estrategia para una formación eficaz y la medición de los resultados. Un programa de formación eficaz aumenta el uso seguro de la tecnología reduciendo los errores de usuario, aumentando la productividad e incrementando el cumplimiento de los controles clave, tales como las medidas de seguridad del usuario.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Entrega de Valor S. Administración de Riesgos S. Administración de Recursos S. Alineación Estratégica	P. Efectividad S. Eficiencia	• Personas	8. Seguridad ligada a los Recursos Humanos

DS8: Gestionar la mesa de servicios y los incidentes

La respuesta oportuna y eficaz a las consultas y los problemas de los usuarios de TI requiere de una mesa de servicios y un proceso de gestión de incidentes bien diseñados y ejecutados. La mesa de servicios registra y escala incidentes, analiza tendencias y la causa raíz, y brinda soluciones. Los beneficios en el negocio incluye el aumento de la productividad a través de la solución rápida de los requerimientos del usuario. Además, la empresa puede abordar las causas básicas (como la formación deficiente de usuarios) a través de una presentación eficaz de informes.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Entrega de Valor S. Medición del Desempeño	P. Efectividad P. Eficiencia	• Personas • Aplicaciones	13. Gestión de Incidentes en Seguridad de Información 14. Gestión de la Continuidad del Negocio

DS9: Administrar la configuración

Asegurar la integridad de las configuraciones de hardware y software requiere el establecimiento y mantenimiento de un repositorio exacto y completo de configuraciones. Este proceso incluye la recolección de información de configuración inicial, el establecimiento de líneas de base, la verificación y auditoría de la información de configuración y la actualización del repositorio de configuración, según sea necesario. Una gestión de la configuración eficaz facilita una mayor disponibilidad del sistema, minimiza los problemas de producción y resuelve los problemas más rápidamente.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Administración de Recursos P. Entrega de Valor S. Administración de Riesgos	P. Efectividad S. Eficiencia S. Disponibilidad S. Confiabilidad	• Aplicaciones • Infraestructura • Información	7. Gestión de Activos 10. Gestión de Comunicaciones y Operaciones 11. Control de Acceso 12. Adquisición, Desarrollo y Mantenimiento de SI 15. Cumplimiento

DS10: Gestionar problemas

La gestión eficaz de problemas requiere de la identificación y clasificación de los problemas, el análisis de la causa raíz y la solución de problemas. También incluye la formulación de recomendaciones para la mejora, el mantenimiento de registros de problemas y la revisión de la situación de las acciones correctivas. Un proceso de gestión eficaz de problemas maximiza la disponibilidad del sistema, mejora los niveles de servicio, reduce costos y mejora la comodidad y la satisfacción del cliente.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Entrega de Valor S. Administración de Riesgos S. Medición del Desempeño	P. Efectividad P. Eficiencia S. Disponibilidad	• Personas • Aplicaciones • Inflaestructura • Información	13. Gestión de Incidentes en Seguridad de Información

DS11: Gestionar datos

La gestión eficaz de datos precisa de la identificación de las necesidades de datos. El proceso de gestión de datos también incluye el establecimiento de procedimientos eficaces para la gestión de la biblioteca de medios, *backup*, restauración y una adecuada eliminación de los medios. La gestión de datos ayuda a garantizar la calidad, oportunidad y disponibilidad de los datos del negocio.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Entrega de Valor P. Administración de Riesgos P. Administración de Recursos	P. Integridad P. Confiabilidad	• Información	9. Seguridad Física y Ambiental 10. Gestión de Comunicaciones y Operaciones 12. Adquisición, Desarrollo y Mantenimiento de SI 15. Cumplimiento

DS12: Gestionar el ambiente físico

La protección de equipos informáticos y del personal requiere de instalaciones físicas bien diseñadas y bien administradas. El proceso de gestionar el ambiente físico incluye definir las condiciones físicas del sitio, seleccionar las instalaciones adecuadas, diseñar procesos eficaces para el monitoreo de factores ambientales y gestionar el acceso físico. La gestión eficaz del ambiente físico reduce las interrupciones del negocio por daños a los equipos informáticos y al personal.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Administración de Riesgos S. Administración de Recursos	P. Integridad P. Disponibilidad	• Infraestructura	6. Aspectos Organizativos de Seguridad de Información 9. Seguridad Física y Ambiental

DS13: Gestionar las operaciones

El procesamiento completo y preciso de los datos requiere una gestión eficaz de los procedimientos de procesamiento de datos y mantenimiento cuidadoso del hardware. Este proceso incluye la definición de políticas operativas y procedimientos para una gestión eficaz del procesamiento planificado, protegiendo la información sensitiva, monitoreando el desempeño de la infraestructura y asegurando el mantenimiento preventivo del hardware. La gestión eficaz de operaciones ayuda a mantener la integridad de los datos y reduce los retrasos en el negocio y los costos operativos.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Administración de Recursos	P. Efectividad P. Eficiencia S. Integridad S. Disponibilidad	• Personas • Aplicaciones • Infraestructura • Información	9. Seguridad Física y Ambiental 10. Gestión de Comunicaciones y Operaciones

COBIT 4.1. Dominio: Monitorear y Evaluar - ME

ME1: Monitorear y evaluar el desempeño de TI

La gestión eficaz del desempeño de TI requiere un proceso de monitoreo que incluye la definición de indicadores relevantes de desempeño, el reporte oportuno y sistemático del desempeño, y la acción inmediata sobre las desviaciones. Es necesario el monitoreo para asegurarse que las cosas se hacen bien y están alineadas con el conjunto de direcciones y políticas.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Medición del Desempeño S. Entrega de Valor S. Administración de Riesgos S. Administración de Recursos S. Alineación Estratégica	S. Integridad S. Disponibilidad P. Efectividad P. Eficiencia S. Cumplimiento S. Confiabilidad	• Personas • Aplicaciones • Infraestructura • Información	10. Gestión de Comunicaciones y Operaciones

ME2: Monitorear y evaluar el control interno

Establecer un programa eficaz de control interno de TI requiere de un proceso de monitoreo bien definido. Este proceso incluye monitoreo y reporte de excepciones de control, resultados de las auto-evaluaciones y revisiones de terceros. Un beneficio clave del monitoreo del control interno es que proporciona garantías con respecto a operaciones eficaces y eficientes y el cumplimiento de las leyes y regulaciones.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Entrega de Valor P. Administración de Riesgos	S. Integridad S. Disponibilidad P. Efectividad P. Eficiencia S. Cumplimiento S. Confiabilidad S. Confidencialidad	• Personas • Aplicaciones • Infraestructura • Información	5. Política de Seguridad 6. Aspectos Organizativos de Seguridad de Información 10. Gestión de Comunicaciones y Operaciones 15. Cumplimiento

ME3: Garantizar el cumplimiento de requisitos externos

Una supervisión eficaz del cumplimiento exige el establecimiento de un proceso de revisión para garantizar la conformidad con leyes, reglamentos y requisitos contractuales. Este proceso incluye la identificación de los requerimientos de cumplimiento, optimización y evaluación de la respuesta, asegurando que los requisitos se han cumplido y por último, integrando el reporte de cumplimiento de TI con el resto de la empresa.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Administración de Riesgos P. Alineación Estratégica	P. Cumplimiento S. Confiabilidad	• Personas • Aplicaciones • Infraestructura • Información	6. Aspectos Organizativos de Seguridad de Información 15. Cumplimiento

ME4: Proporcionar gobierno de TI

Establecer un marco de gobierno eficaz incluye la definición de las estructuras organizativas, procesos, liderazgo, roles y responsabilidades para asegurar que las inversiones en TI estén alineadas y entregadas conforme con las estrategias y los objetivos de la empresa.

Focos de Gobierno de TI	Requerimientos de Información	Recursos Involucrados	Objetivos de Control de ISO/IEC 27002:2005
P. Medición del Desempeño P. Entrega de Valor P. Administración de Riesgos P. Administración de Recursos P. Alineación Estratégica	S. Integridad S. Disponibilidad P. Efectividad P. Eficiencia S. Cumplimiento S. Confiabilidad S. Confidencialidad	• Personas • Aplicaciones • Infraestructura • Información	5. Política de Seguridad 6. Aspectos Organizativos de Seguridad de Información 10. Gestión de Comunicaciones y Operaciones

CONCLUSIÓN

El Modelo COBIT se erige a nivel mundial como el más importante modelo o "mejor práctica" para la implantación de un adecuado Gobierno de TI; no obstante, las propuestas que realiza en cada uno de los procesos quedan en el nivel del ¿qué hacer?, es decir, los responsables de implementar procesos de Gobierno de TI en las organizaciones sienten que obtienen excelentes luces para el desarrollo de su labor, pero en ocasiones no les es fácil definir ¿cómo hacer? para satisfacer dichas propuestas. Es aquí donde surge la necesidad de analizar cada uno de los requerimientos planteados por COBIT y determinar cuál estándar, de los muchos existentes en el mercado mundial, permitirá responder acordemente a este interrogante.

El Modelo COBIT y la Norma ISO 27001 constituyen independientemente las mejores prácticas para cada uno de los aspectos que dieron origen a su concepción y desarrollo, pero logrando la articulación de ellos y quizás fortaleciendo más sus propuestas con la participación de otros estándares, se logrará conformar un modelo para Gobierno de TI excepcionalmente robusto y de total satisfacción para los requerimientos de las organizaciones modernas.

BIBLIOGRAFÍA

Isaca (2007). IT Assurance Guide. Using Cobit.

Isaca (2008). Aligning CobiT® 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit. A Management Briefing From ITGI and OGC.

Isaca (2008). Valor para la Empresa: Buen Gobierno de las Inversiones en TI.

Isaca (2009). Cobit Control Practices. Guidance to achieve Control Objetives for Successful IT Governance.

Isaca (2009). The COBIT Maturity Model in a Vendor Evaluation Case.

Isaca (2010). Cobit 4.1. Marco de Trabajo, Objetivos de Control, Directrices Gerenciales, Modelos de Madurez.

ISO (2009). Estándar ISO/IEC 27001-2005.

http://www.youtube.com/watch?v=37zvCvb31cw

http://www.youtube.com/watch?v=yQ0lPa79bHo