

COBIT – Preguntas Frecuentes

- ¿Qué es COBIT?
- ¿Qué hay de Nuevo en COBIT 3rd. Edition?
- ¿Qué se incluye?
- ¿Por qué algunas porciones de COBIT se han juzgado como “estándar abierto”?
- ¿Cuál es el propósito de COBIT?
- ¿Quién está utilizando COBIT ?
- ¿Quiénes son los propietarios de los procesos?
- ¿Por qué fue focalizada la orientación de COBIT en el proceso en lugar de las funciones o aplicaciones?
- ¿Cuán robustos son los requerimientos del negocio?
- ¿Cuál es la calidad total de COBIT y hubo algún propietario de proceso/ejecutivo que fue parte de la revisión experta?
- ¿Cuál es la futura dirección de COBIT?
- ¿Cómo decidió ISASF/A la lista de referencias primarias?
- ¿Puedo utilizar COBIT como una declaración de criterios para conclusiones específicas de auditoría?
- ¿Son los Objetivos de Control un nivel mínimo de control o una mejor práctica?
- ¿Por qué la ausencia de Controles de Plataformas Específicas?
- ¿Dónde están los Controles de Aplicaciones?
- ¿Por qué hay superposición dentro de los Objetivos de Control?
- ¿Están vinculados los Objetivos de Control a las Guías de Auditoría y con qué grado?
- ¿Por qué no hay ninguna Declaración de Riesgo con los Objetivos de Control?
- ¿Por qué hay diferencias entre los Objetivos Detallados de Control y las Consideraciones de Control?
- ¿De qué forma puedo sugerir a la Gerencia de TI que utilice COBIT?
- ¿Es superior la Estructura COBIT a los otros Modelos de Control aceptados?
- ¿Cuál es la forma más rápida y mejor para vender COBIT a los Gerentes de TI?
- Dado que COBIT actualmente no encara los riesgos asociados del negocio, sino las declaraciones de control pro-activo a lograr, ¿se presta alguna consideración para encarar la necesidad percibida de identificar los riesgos?
- ¿Ha sido aceptado COBIT y su estructura por los CIOs?
- ¿Cómo se integran las nuevas Guías Gerenciales en la Estructura COBIT?

1) ¿Qué es COBIT?

COBIT, lanzado en 1996, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de TI. Vinculando tecnología informática y prácticas de control, COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores. Como tal, COBIT representa una estructura de control autorizada, actualizada, un conjunto de objetivos de control generalmente aceptados, y un producto agregado que posibilita la fácil aplicación de la Estructura y los Objetivos de Control - denominado las *Guías de Auditoría*. COBIT se aplica a los sistemas de información de toda la empresa, incluyendo los computadores personales, minicomputadores, *mainframes* y ambientes distribuidos. Está basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivo. Con la adición de las *Guías Gerenciales*, COBIT ahora soporta auto-evaluación del estado estratégico organizacional, identificación de acciones para mejorar los procesos de TI y monitorear el desempeño de estos procesos de TI. Desde que se liberó la 1ra edición de COBIT en 1996 se ha vendido e implementado en más de 100 países del mundo.

2) ¿Qué hay de Nuevo en COBIT 3rd. Edition?

COBIT 3rd Edition ha sido mejorado mediante la revisión / agregado de:

- Las *Guías Gerenciales*, que proveen modelos de madurez, factores críticos de éxito, indicadores claves de objetivos e indicadores claves de desempeño para los 34 procesos de TI de COBIT. Estas guías o proveen a la gerencia herramientas que permiten la auto-evaluación y poder seleccionar opciones para implementación de controles y mejoras sobre la información y la tecnología relacionada. Las guías fueron desarrolladas por un panel de 40 expertos en seguridad y control, profesionales de administración de TI y de administración de desempeño, analistas de la industria y académicos de todo el mundo.
- Nuevo material generado por el aumento (de 36 a 41) de los documentos primarios globales.
- 45 objetivos de control detallados nuevos o revisados.

Los componentes de COBIT *Resumen Ejecutivo*, *Marco*, *Objetivos de Control*, *Guías de Auditoría* y *Guías Gerenciales* han sido diseñadas como un estándar libre, disponible para bajar desde el website de ISACA. El acceso libre a este material se brinda para hacer más fácil que las organizaciones de todo el mundo utilicen y adopten COBIT y lo personalicen de acuerdo a sus propias circunstancias.

3) ¿Qué se incluye?

COBIT 3rd Edition contiene:

- Un *Resumen Ejecutivo*, que consiste en una Vista Ejecutiva de Antecedentes y del Marco, diseñado para proveer a la alta gerencia una descripción sucinta de los conceptos claves de COBIT.
- El *Marco o Estructura*, que ilustra e identifica los requerimientos de negocio de TI para la información mediante la introducción de objetivos de control de alto nivel.
- *Objetivos de Control*, que contienen declaraciones de resultados deseados o propósitos a lograr al implementar los 318 objetivos específicos de control detallados.
- *Guías de Auditoría*, que proveen una guía para preparar planes de auditoría y están vinculadas a los objetivos de control.
- Un *Conjunto de Herramientas de Implementación (Tool Set)*, que describe enfoques prácticos utilizados por las organizaciones que aplicaron COBIT rápida y exitosamente en sus ambientes de trabajo.
- *Guías Gerenciales*, que proveen guía para evaluar el estado de la organización, identificando las actividades críticas conducentes al éxito y midiendo el desempeño para alcanzar los objetivos de la empresa.

4) ¿Por qué algunas porciones de COBIT se han juzgado como “estándar abierto”?

- Es el deseo de ISACF que con el tiempo COBIT sea adoptado por las comunidades de auditoría y negocios como un estándar generalmente aceptado para el control de TI. Hacerlo fácilmente disponible ayuda no solo al progreso del establecimiento de COBIT como un estándar de hecho, sino que también responde al mercado.
- El intención de ISACF que los departamentos de auditoría y otros interesados en el gobierno efectivo de TI puedan adaptar COBIT según sea necesario, a las políticas y procedimientos internos propios de la empresa. Al ofrecer el material para bajarlo de la web, los individuos pueden personalizar COBIT según lo requieran para hacerlo un documento operativo aplicable a sus propias circunstancias.
- Se cree que las empresas tienen mucho para ganar si la alta gerencia comprende la importancia del gobierno y control de TI y reconoce el rol de COBIT en función efectiva. Al hacer disponible vía el web site porciones de COBIT, los departamentos de auditoría y otros interesados en el gobierno de TI tendrán acceso más fácil a la información y estarán en mejor posición para presentarlo a la gerencia y a otras partes interesadas.

En la 3ra. Edición de COBIT, se ha aumentado la cantidad de componentes estándar libres al incluir las nuevas *Guías Gerenciales*.

5) ¿Cuál es el propósito de COBIT?

El propósito de COBIT es proveer a la gerencia y a los propietarios de los procesos del negocio con un modelo de gobierno de Tecnología Informática (TI) que ayude a comprender y administrar los riesgos asociados con TI. COBIT ayuda a sortear las brechas entre los riesgos del negocio, las necesidades de control y los aspectos técnicos. Es un modelo de control para satisfacer las necesidades de gobierno de TI y asegurar la integridad de la información y de los sistemas de información.

6) ¿Quién está utilizando COBIT?

COBIT está siendo utilizado por aquellos que tienen la responsabilidad primaria por los procesos del negocio y la tecnología, por aquellos que dependen de la tecnología para la información relevante y confiable, y por aquellos que proveen calidad, confiabilidad y control de la tecnología informática.

7) ¿Quiénes son los propietarios de los procesos?

COBIT está orientado a los procesos del negocio y en consecuencia está dirigido en primer lugar a los propietarios de esos procesos. En referencia al Modelo Genérico de Negocios de Porter estamos refiriéndonos a los procesos principales (adquisiciones, operaciones, comercialización, ventas, etc.) como asimismo, a los procesos de apoyo (recursos humanos, administración, tecnología informática, etc.). Como consecuencia, COBIT no es solo para ser aplicado por el departamento de TI, sino por la empresa como un todo.

Este enfoque nace del hecho de que en las empresas de hoy, los propietarios de los procesos son responsables por el desempeño de sus procesos, de los cuales TI se ha convertido en una parte integrante. En otras palabras, ellos están fortalecidos pero también son responsables. Como consecuencia, los propietarios de los procesos del negocio soportan la responsabilidad final por la tecnología informática según esté distribuida dentro de los confines de sus procesos de negocio. Por supuesto, ellos harán uso de los servicios provistos por las partes especializadas tal como el tradicional departamento de TI o los terceras partes proveedores de servicios.

COBIT provee a los propietarios de los procesos del negocio una estructura, que les debería permitir controlar todas las distintas actividades subyacentes en la distribución de TI. Como resultado, sobre esta base pueden ganar una seguridad razonable de que TI contribuirá al logro de sus objetivos de negocio. Más aún, COBIT provee a los propietarios de los procesos del negocio una estructura genérica de comunicación para facilitar la comprensión y claridad entre las distintas partes involucradas en la entrega de servicios de TI.

Además, el agregado de las Guías Gerenciales en la 3ra. Edición provee a la gerencia un conjunto de herramientas que posibilita la auto-evaluación para seleccionar opciones para implementación de controles y mejoras sobre TI, y medir el logro de objetivos y el desempeño apropiado de los procesos de TI. Las Guías Gerenciales incluyen modelos de madurez, factores críticos de éxito, indicadores claves de objetivos e indicadores claves de desempeño para apoyar la toma de decisiones gerencial.

8) ¿Por qué fue focalizada la orientación de COBIT en el proceso en lugar de las funciones o aplicaciones?

La estructura COBIT ha sido organizada en 34 procesos de TI agrupando actividades interrelacionadas del ciclo de vida o tareas discretas interrelacionadas. El modelo de proceso fue preferido por varias razones. Primeramente, un proceso por su naturaleza está orientado a resultados de forma que se focaliza en el resultado final a la vez que optimiza el uso de recursos. La forma en que estos recursos están físicamente estructurados, ej: gente/habilidades en departamentos, es menos relevante en esta perspectiva. En segundo lugar, un proceso, y especialmente sus objetivos, son más permanentes en naturaleza y el riesgo no cambia tan frecuentemente como en una entidad organizacional. Tercero, la distribución de TI no puede ser confinada a un departamento en particular e involucra a usuarios y gerencia como asimismo a especialistas de TI. En este contexto, el proceso de TI se mantiene no obstante como el denominador común. En lo que se refiere a aplicaciones, ellas son tratadas dentro de la estructura COBIT como una de las cinco categorías de recursos. De ahí que deban ser administradas y controladas de forma tal de obtener la información requerida a nivel de proceso del negocio. De esta forma, los sistemas de aplicación son una parte integral de la estructura COBIT y pueden ser encarados específicamente desde el punto ventajoso de los recursos. En otras palabras, focalizando estrictamente solo en los recursos, uno podría obtener automáticamente una vista de los objetivos de COBIT respecto de las aplicaciones.

9) ¿Cuán robustos son los requerimientos de negocio?

Durante el proceso de revisión de COBIT, los gerentes senior y los CIOs les gustaba la definición de requerimientos de información de los negocios y consideraban opciones acerca de qué requerimientos eran más importantes en qué proceso. Las opciones eran difíciles y ocasionaban un debate considerable entre los expertos durante el proyecto. El principio rector había sido siempre: ¿Qué es realmente fundamental para este Objetivo de Control en este proceso? ¿Qué recurso requiere un control especial? ¿Qué requerimiento de información requiere especial atención?

10) ¿Cuál es la calidad total de COBIT y hubo algún propietario de proceso/ ejecutivo que fue parte de la revisión experta?

Para asegurar la calidad final de COBIT, se tomaron varias medidas. Las más importantes fueron:

- i. Todo el proceso de investigación fue gobernado por el COBIT Steering Committee (CSC). Más allá de preconcebir los productos finales, el CSC fue también responsable por la calidad final de estos productos.
- ii. Los resultados detallados de la investigación fueron controlados totalmente en su calidad.
- iii. Los resultados de la investigación preliminar, como asimismo la estructura, fueron expuestos a dos grupos de expertos incluyendo gerentes de negocios.
- iv. Antes de emitir los textos finales los mismos fueron distribuidos a una cantidad de especialistas para obtener sus comentarios.

Las Guías Gerenciales fueron desarrolladas por un panel mundial consistente en 40 expertos en seguridad y control, profesionales de administración de TI y de administración de desempeño, analistas de la industria y académicos que participaron en un taller residencial conducido por facilitadores profesionales. Los productos del taller pasaron a través de un proceso de aseguramiento de calidad y fueron expuestos para revisión. Sin embargo, debe enfatizarse que estas guías se mantuvieron genéricas, generalmente aplicables y no proveen normas específicas de la industria. Las organizaciones necesitarán en muchos casos personalizar este conjunto general de directivas a su propio ambiente.

Por sobre todo, la experiencia muestra que el modelo COBIT apela a la administración del negocio en su conjunto y a que ellos aprecien el valor agregado del mismo en vista a mejorar su control sobre TI. En este sentido, estamos confiados en que, más allá de la satisfacción del cliente, se ha alcanzado el nivel de calidad requerido.

11) ¿Cuál es la dirección futura de COBIT?

Como con cualquier investigación amplia e innovadora, COBIT será actualizado cada 3 años. Esto asegurará que el modelo y la estructura permanezcan vigentes. La validación también permite asegurar que los 41 materiales de referencia primarios no hayan cambiado, y, si hubieran cambiado, reflejar eso en el documento.

12) ¿Cómo decidió ISASF/A la lista de referencias primarias?

La lista de referencias primarias fue desarrollada en un consenso colectivo basado en la experiencia de los profesionales que participaron en la investigación, revisión experta y esfuerzos de aseguramiento de calidad del Comité de Conducción de COBIT.

13) ¿Puedo utilizar COBIT como una declaración de criterios para conclusiones específicas de auditoría?

Sí, basando las Guías de Auditoría firmemente en los Objetivos de Control aparta la opinión del auditor de la conclusión de auditoría, reemplazándola por un criterio autorizado. COBIT está basado en 41 documentos de estándares y mejores prácticas para Tecnología Informática de cuerpos que establecen estándares (tanto públicos como privados) de todo el mundo. Estos incluyen documentos de Europa, Canadá, Australia, Japón y los Estados Unidos. Como COBIT contiene todos los estándares mundiales pertinentes identificables al momento, es “todo incluido” (all-inclusive) en relación a los estándares de control de TI. Como resultado, COBIT puede ser utilizado como un documento de referencia de fuente autorizada, para brindar criterios sobre controles de TI en las auditorías.

14) ¿Son los Objetivos de Control un nivel mínimo de control o una mejor práctica?

Son tanto niveles mínimos de control como mejores prácticas, porque estamos aún a nivel de objetivos de control, no aún a nivel de guías de control o prácticas de control. Esto será encarado en fases futuras del proyecto COBIT, en donde el ambiente de la empresa, los objetivos específicos del negocio, el nivel de seguridad que uno desea lograr, el grado de riesgo que uno desea aceptar, etc., determinarán cómo serán traducidos los objetivos de control para un proceso al nivel correcto de control.

Como todas estas opciones no son auto-evidentes, y porque el proceso de selección de controles puede ser oneroso y consumidor de tiempo, deberán ciertamente desarrollarse y promoverse estándares de niveles mínimos de seguridad y control.

15) Por qué la ausencia de Controles de Plataformas Específicas?

Los objetivos de control de COBIT son genéricos en naturaleza y están tratando con actividades o tareas dentro de los procesos de TI. De esta forma, por una parte los mismos son independientes de la plataforma. Por otra parte, sin embargo, ellos son la estructura general dentro de la cual deben definirse los controles más específicos relacionados con las plataformas. En los hechos, los objetivos de control generales deberían permanecer válidos independientemente de si uno está controlando por ejemplo una plataforma *mainframe* o una plataforma de automatización de oficinas. Es obvio que ciertos aspectos requerirán más énfasis en un ambiente determinado.

16) ¿Dónde están los Controles de Aplicaciones?

Los controles de aplicaciones han sido totalmente integrados en el modelo COBIT. Esta opción se ha tomado considerando que COBIT está orientado a los procesos del negocio y que a este nivel los controles de aplicaciones son

meramente parte de los controles totales a ser ejercidos sobre los sistemas de información y la tecnología relacionada. Sin embargo, en la mayoría de los casos esta parte no puede ser tercerizada. De ahí que la pregunta "¿Dónde están los controles de aplicaciones?" es de importancia fundamental.

Los sistemas y datos de aplicaciones son tratados dentro de la estructura COBIT como dos de las cinco categorías de recursos. Están para entregar la información requerida a nivel de proceso del negocio. De esta forma, sistemas de aplicación y datos son una parte integral de la estructura COBIT y pueden ser encarados específicamente a través del punto ventajoso recurso. Al hacer esto, uno nota que muchos procesos CobiT tratan los controles de aplicación y continúan con esto a través de todo el ciclo de vida, desde la concepción hasta la operación.

Aparte de la vista general de los recursos, hay un proceso "Administrar Datos " donde se pueden encontrar los controles tradicionales de transacciones y archivos. No obstante, uno debería considerar que estos controles por si mismos ya no son suficientes para controlar efectivamente los sistemas de aplicación y los datos.

Cuando se integra COBIT en la organización de uno, deben tomarse en cuenta los elementos mencionados. En este sentido, se requiere agregar controles específicos de plataforma a los objetivos de control genéricos. Las plataformas deben interpretarse en forma amplia en este sentido, (ej: automatización de oficinas, telecomunicaciones, data warehouse, etc.). Los procesos COBIT que van a ser revisados en este caso, son aquellos relacionados con la categoría de recursos "tecnología".

17) ¿Por qué hay superposición dentro de los Objetivos de Control?

La superposición en los Objetivos de Control, aunque no ocurre muy a menudo, fue intencional. Algunos objetivos de control trascienden los dominios y procesos y en consecuencia deben ser repetidos para asegurar que existen en cada dominio y proceso. Algunos objetivos de control están pensados para ser controles cruzados de uno con otro y en consecuencia deben ser repetidos para asegurar su aplicación consistente en más de un dominio o proceso. Por lo tanto, aunque percibido como superposición, COBIT intencionalmente repite algunos objetivos de control para asegurar una cobertura apropiada de estos controles de TI.

18) ¿Están vinculados los Objetivos de Control a las Guías de Auditoria y con qué grado?

Los objetivos han sido desarrollados desde una orientación de proceso porque la gerencia está buscando un consejo pro-activo sobre cómo encarar el problema de mantener TI bajo control. Balancear costo y riesgo es el siguiente problema a encarar (ej: realizar una selección conciente de si implementar y cómo cada objetivo de control). Los futuros productos COBIT encararán acabadamente esta

selección, aun cuando se mantenga el principio pro-activo – los objetivos de control deberían ser aplicados en primer lugar para lograr un criterio de control de la información (efectividad, eficiencia, confidencialidad, disponibilidad, integridad, cumplimiento y confiabilidad). El vínculo es el proceso. Los objetivos de control ayudan a la gerencia a establecer control sobre el proceso, las guías de auditoría asisten al auditor o asesor proveyendo seguridad de que el proceso está actualmente bajo un control tal que los requerimientos de información necesarios para lograr los objetivos del negocio serán satisfechos. En referencia a la estructura de control representada por el modelo cascada, las guías de auditoría pueden ser vistas como proveyendo una retroalimentación desde los procesos de control hacia atrás a los objetivos de negocio. Los objetivos de control son la guía yendo hacia abajo de la cascada para lograr tener el proceso de TI bajo control. Las guías de auditoría son la guía para ir hacia arriba de la cascada con la pregunta: "¿Hay seguridad de que el objetivo de negocio va a ser logrado? Algunas veces las guías de auditoría son traducciones directas de los objetivos de control; más a menudo las guías buscan evidencias de que el proceso está bajo control.

19) ¿Por qué no hay ninguna Declaración de Riesgo con los Objetivos de Control?

La provisión de declaraciones de riesgo fue seriamente considerada y analizada durante la investigación y la fase de revisión del proyecto inicial de COBIT, pero no retenida porque la gerencia prefirió el enfoque pro-activo (los objetos son para ser logrados) por sobre el enfoque reactivo (los riesgos deben ser mitigados). En enfoque de riesgo viene al final de las guías de auditoría cuando se sustancia el riesgo de no implementar los controles. En la aplicación de COBIT, el enfoque de riesgo es ciertamente útil cuando la gerencia decide qué controles implementar o cuando los auditores deciden qué objetivos de control revisar. Ambas decisiones dependen totalmente del ambiente de riesgo.

20) ¿Por qué hay diferencias entre los Objetivos Detallados de Control y las Consideraciones de Control?

Los objetivos de control se focalizan en objetivos de control detallados específicos asociados con cada proceso de TI. Ellos son definidos en base a una cantidad de fuentes, comprendiendo los estándares internacionales relativos a controles sobre TI que proveen la visión del especialista en control. Las consideraciones de control, tal como se actualizaron en la 3ra. Edición de COBIT, proveen la visión gerencial y están alineados con los factores críticos de éxito para el control incluidos en las Guías Gerenciales.

21) ¿De qué forma puedo sugerir a la Gerencia de TI que utilice COBIT?

Como CobiT está orientado al negocio, es indicado utilizarlo para comprender los objetivos de control de TI para administrar los riesgos del negocio relacionados con TI:

1. Comience con sus objetivos de negocio en la Estructura
2. Seleccione los procesos de TI y objetivos de control apropiados a su empresa entre los Objetivos de Control
3. Opere desde su plan de negocio
4. Evalúe sus procedimientos y resultados con las Guías de Auditoría
5. Evalúe el estado de su organización, identifique las actividades críticas conducentes al éxito y mida el desempeño para alcanzar los objetivos de la empresa con las Guías Gerenciales.

22) ¿Es superior la Estructura COBIT a los otros Modelos de Control aceptados?

Algunos modelos enfatizan sobre el control del negocio y otros sobre aspectos de seguridad de TI, pero sólo COBIT intenta tratar los aspectos específicos de control de TI desde la perspectiva del negocio. Se debe destacar que COSO fue utilizado como material fuente para el modelo de negocio de CobiT. Por último, CobiT no significa reemplazar a ninguno de los modelos de control existentes. Se intenta proveer más detalle en el ambiente de TI trabajando sobre las fortalezas de los otros modelos de control.

23) ¿Cuál es la forma más rápida y mejor para vender COBIT a los Gerentes de TI?

Como lo señala el resto de las Herramientas de Implementación, la cultura organizacional es de vital importancia. Una cultura pro-activa será más receptiva que una que no lo es. Sin embargo, considere enfatizar los aspectos del negocio y el hecho de que COBIT no se pierde en terminología técnica. Además, señale que COBIT fue diseñado de la forma en que piensa un gerente de TI, y que uno de sus mayores beneficios es que todo está documentado en un solo lugar.

Además, con el agregado de las Guías Gerenciales, COBIT brinda a la gerencia nuevas capacidades para sustentar la auto-evaluación del estado organizacional, comparación con las mejores prácticas de la industria, alineamiento con los objetivos de la empresa, toma de decisiones de implementación y monitoreo del desempeño. Los modelos de madurez, factores críticos de éxito, indicadores claves de objetivos e indicadores claves de desempeño provistos en estas guías pueden asistir a la gerencia para el mejor alineamiento de TI con la estrategia general de la empresa asegurando que TI sea un facilitador para el logro de los objetivos de la empresa.

24) Dado que COBIT actualmente no encara los riesgos asociados del negocio, sino las declaraciones de control pro-activo a lograr, ¿se presta alguna consideración para encarar la necesidad percibida de identificar los riesgos?

El riesgo es encarado de manera penetrante en todo COBIT y aún más en la 3ra. Edición con el advenimiento de las Guías Gerenciales. Un conductor principal de los procesos de control y aseguramiento es el modelo de Gobierno de TI que ahora es cubierto ampliamente en COBIT y en la estructura de las Guías Gerenciales.

El gobierno de TI se refiere a los objetivos genéricos de la empresa de medir beneficios y administrar riesgos. La misma idea, administración de riesgos como un objetivo de la empresa, fue no obstante, ya capturado por COBIT antes, porque COBIT establece que TI necesita proveer información a la empresa que debe tener las características requeridas para permitir el logro de los objetivos. Mientras los criterios relacionado con seguridad, de disponibilidad, integridad y confidencialidad, pueden ser más fácilmente asociado con riesgos, no lograr los objetivos de la empresa o no proveer los criterios requeridos son riesgos que la empresa necesita controlar.

En la sección 'sustanciar' de las Guías de Auditoria se brindan ejemplos específicos. El objetivo de esa sección es documentar para la gerencia lo que puede suceder, o ha sucedido, como resultado de no tener vigente un control efectivo. Más prácticamente, se definió un proceso completo para cubrir la evaluación de riesgos. (Ver PO9 – Evaluar Riesgos).

En conclusión, el riesgo es encarado en la Estructura de una forma pro-activa, ej: focalizando en objetivos, porque el riesgo primario que debe ser administrado es el de no lograr los objetivos. En segundo lugar, la sección 'sustanciar' de las Guías de Auditoria proveen ejemplos de estos riesgos para cada proceso. Esta es la información de riesgos que está buscando el profesional de control y aseguramiento. Finalmente, del conjunto de los objetivos de TI, un proceso completo de TI está dedicado a la evaluación de riesgo.

25) ¿Ha sido aceptado COBIT y su estructura por los CIOs (Directores de Tecnología Informática)?

Sí, ha sido aceptado en muchas organizaciones globalmente y se continúan documentando nuevos casos. Sin embargo, no debe sorprender a nadie que en esas entidades en que el CIO ha adoptado COBIT como una estructura utilizable de TI, esto ha sido consecuencia directa de uno o más “Campeones” COBIT dentro del Departamento(s) de Auditoria y/o TI.

El agregado de las Guías Gerenciales debería también aumentar la aceptación de COBIT tanto por la gerencia de la empresa como de TI. El énfasis en alinear TI con los objetivos de la empresa, la auto-evaluación y la medición del desempeño asegurará que COBIT sea visto no sólo como una estructura de

control, sino también como suministrador de un conjunto de herramientas para mejorar la efectividad de los recursos de información y TI. La integración de las Guías Gerenciales con la Estructura COBIT y los Objetivos de Control proveerá un énfasis adicional para que la gerencia utilice COBIT como el modelo autorizado, actualizado y establecido para el control y gobierno de TI.

26) **¿Cómo se integran las nuevas Guías Gerenciales (o Pautas Gerenciales) en la Estructura COBIT?**

Comenzando con la Estructura COBIT, la aplicación de estándares y guías internacionales y la investigación sobre las mejores prácticas condujeron al desarrollo de los Objetivos de Control. Las Guías de Auditoria fueron desarrolladas para evaluar si estos Objetivos de Control estaban apropiadamente implementados. Sin embargo, la gerencia necesita una aplicación similar de la Estructura para permitir que se realicen auto-evaluaciones y selecciones para implementar y mejorar el control sobre la información y la tecnología relacionada.

Las Guías Gerenciales proveen las herramientas para cumplir con esto. Fueron desarrolladas para cada uno de los 34 objetivos de control de alto nivel, con una perspectiva de administración de procesos y medición de desempeño. Los modelos de madurez, los factores críticos de éxito, los indicadores claves de objetivos y los indicadores claves de desempeño son provistos por las guías para soportar los procesos gerenciales de toma de decisiones. Las consideraciones de control de los objetivos de control de alto nivel han sido actualizadas para reflejar, sin mapear uno a uno, los factores críticos de éxito del objetivo de control.

El desarrollo de las Guías Gerenciales trajo a consideración la necesidad de soportar los requerimientos de:

- La gerencia de la empresa y de TI, con un conjunto de nuevas herramientas de administración de procesos, reconociendo al mismo tiempo el beneficio de utilizar una estructura de control establecida, autorizada y actualizada, como COBIT.
- El profesional de seguridad y control, con una base para potenciar y desarrollar los procesos existentes orientados a controles para proveer servicios y valor adicionales en respaldo de los objetivos de la empresa.
- Las Guías Gerenciales asumen poco conocimiento de las estructuras de control en general, y de COBIT en particular, por parte de la gerencia de la empresa y de TI. Las mismas utilizan la misma estructura que los Objetivos de Control y las Guías de Auditoria para soportar las necesidades del profesional de seguridad y control. Por medio del contenido y del formato de presentación hay una diferenciación apropiada, no obstante también existe integración y sinergia en la 3ra. Edición de COBIT para atender las necesidades de ambas audiencias.