UNIDAD DE CONTROL INTERNO
Área de investigación y Capacitación

OTROS MODELOS DE CONTROL INTERNO

Recopilado por: Lic. Luis E. Guzmán Gutiérrez, CPA

MODELO COCO (Criteria of control board)

Publicado por el Consejo para el diseño y emisión de criterios generales sobre control del Instituto Canadiense de Contadores Certificados

Objetivo: proveer un conocimiento del control como respuesta a los siguientes aspectos:

- Impacto de la tecnología y la disminución del tamaño de la estructura de las organizaciones
- Crecimiento de la demanda de información sobre la eficacia del control
- Interés de las autoridades para establecer controles que protejan las inversiones de los accionistas

MODELO COCO (Criteria of control board)

El modelo COCO provee criterios básicos para comprender y aplicar las medidas de control interno de acuerdo con las características y naturaleza de cada organización, así como para la evaluación del desempeño de los controles implantados.

Establece 20 criterios, clasificados en 4 grupos, aplicables a un apropiado sistema de control interno:

Propósito, compromiso, aptitud, evaluación y aprendizaje.

MARCO INTEGRADO DE CONTROL INTERNO PARA LATINOAMERICA (MICIL)

Se emitió en setiembre de 2004 y fue elaborado por una comisión de la Asociación Interamericana de Contabilidad (AIC) y la Federación Latinoamericano de Auditores Internos, con el propósito de tener un marco conceptual de control interno en español que se pudiera aplicar en las empresas públicas y privadas de América Latina, como respuesta al informe COSO

MARCO INTEGRADO DE CONTROL INTERNO PARA LATINOAMERICA (MICIL)

RAZONES DE IMPLEMENTACIÓN

1- En esa época había poca disponibilidad del texto “Nuevos Conceptos de Control Interno, Informe COSO”, por lo cual sus conceptos y técnicas de control interno no eran conocidas por la mayoría de los profesionales involucrados con el tema.

2- Tendencia del cambio de los modelos de planificación y ejecución de las actividades de los estados hacia una mayor participación ciudadana.

MICIL: IMPLEMENTACIÓN

Nivel global: dirigido al aparato gubernamental, sectores económicos relevantes, entidades públicas específicas, municipalidades, etc. También funciona para empresas privadas, organizaciones civiles, de interés social, entre otras.

Escala particular: se refiere a departamentos o unidades dentro de una organización.

Se requiere la creación de una cultura liderada por una persona que participa en el proceso y que debe contar con la responsabilidad social para informar sobre errores e irregularidades detectadas, ya sea a sus superiores, o bien a entes fiscalizadores o reguladores.

Aparte del enfoque económico y financiero, este modelo de control interno debe incluir el reconocimiento del ambiente de control como fundamento para que la organización funcione apropiadamente aplicando los principios éticos, de valores y transparencia que deben haberse definido a nivel estratégico.

MICIL: PROCESO DE AUTOEVALUACIÓN

AUTO EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO

La auto evaluación del control interno es una de las recomendaciones incluidas en el MICIL. Este proceso debe ser apoyado por la administración y la auditoría interna.

La auto evaluación debe considerar los resultados semestrales para evaluar el cumplimiento de objetivos intermedios o grado de avance, cuyo informe debe estar disponible para la evaluación de auditores externos de conformidad con la fecha de cumplimiento de cierre fiscal, que es otra particularidad del MICIL.

La auto evaluación se puede realizar en cualquier momento, a discreción de la persona responsable del proyecto. MICIL no establece un método o herramienta específica por aplicar.

MICIL: EVALUACIONES INDEPENDIENTES

EVALUACIÓN INDEPENDIENTE DEL SISTEMA DE CONTROL INTERNO

MICIL establece la evaluación independiente del SCI como un procedimiento obligatorio de auditoría realizado por auditores internos y externos a través de auditorías con diferentes enfoques, tanto para auditoría de estados financieros como para auditorías de gestión, de tecnología de información

La auditoría externa rendirá un informe con los resultados relevantes de su evaluación, incluyendo las fortalezas encontradas y los aspectos de mejora para fortalecer el sistema. Esta evaluación es válida para las auditoría de estados financieros como la de gestión

La evaluación del SCI está dirigida a la evaluación de los cinco componentes del control interno y los procesos o actividades relevantes para la organización.

Control de Objetivos para Tecnologías de la Información y Relacionadas (COBIT)

Definido por el Instituto de Gobierno de Tecnologías de la Información, es un estandar abierto desarrollado y promovido y aceptado en buenas prácticas de seguridad de TI, con el fin de apoyar las necesidades gerenciales en cuanto al seguimiento de los niveles apropiados de seguridad de TI que deben cumplir las organizaciones.

COBIT

Administración efectiva de las tecnologías de información y comunicaciones: crítica para el éxito y la supervivencia de las organizaciones

Origen de la naturaleza crítica:

- La creciente dependencia de la información y de los sistemas que proporcionan dicha información
- La creciente vulnerabilidad y un amplio espectro de amenazas, tales como las de ambiente web y la guerra de información

COBIT

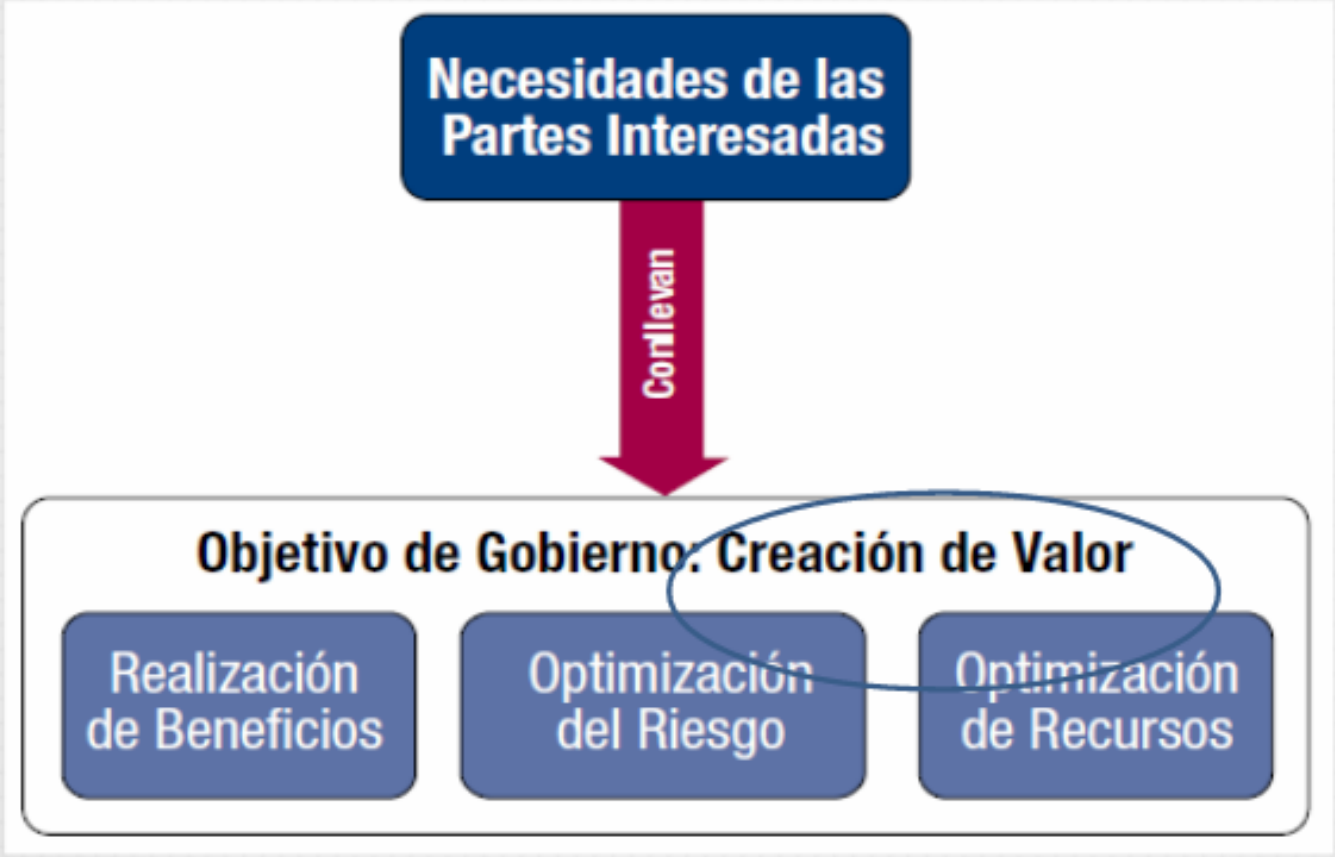
Origen de la naturaleza crítica:

- La escala y el costo de las inversiones actuales y futuras en información y en TI
- El potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas del negocio, crear nuevas oportunidades y reducir costos
- La información y la tecnología que la soporta son los activos mas valiosos en muchas organizaciones.

COBIT

Principio 1. Satisfacer las Necesidades de las Partes Interesadas

- Las empresas existen para **crear valor** para sus accionistas.



Fuente: ISACA CHAPTER MONTEVIDEO

COBIT

Riesgos de TI

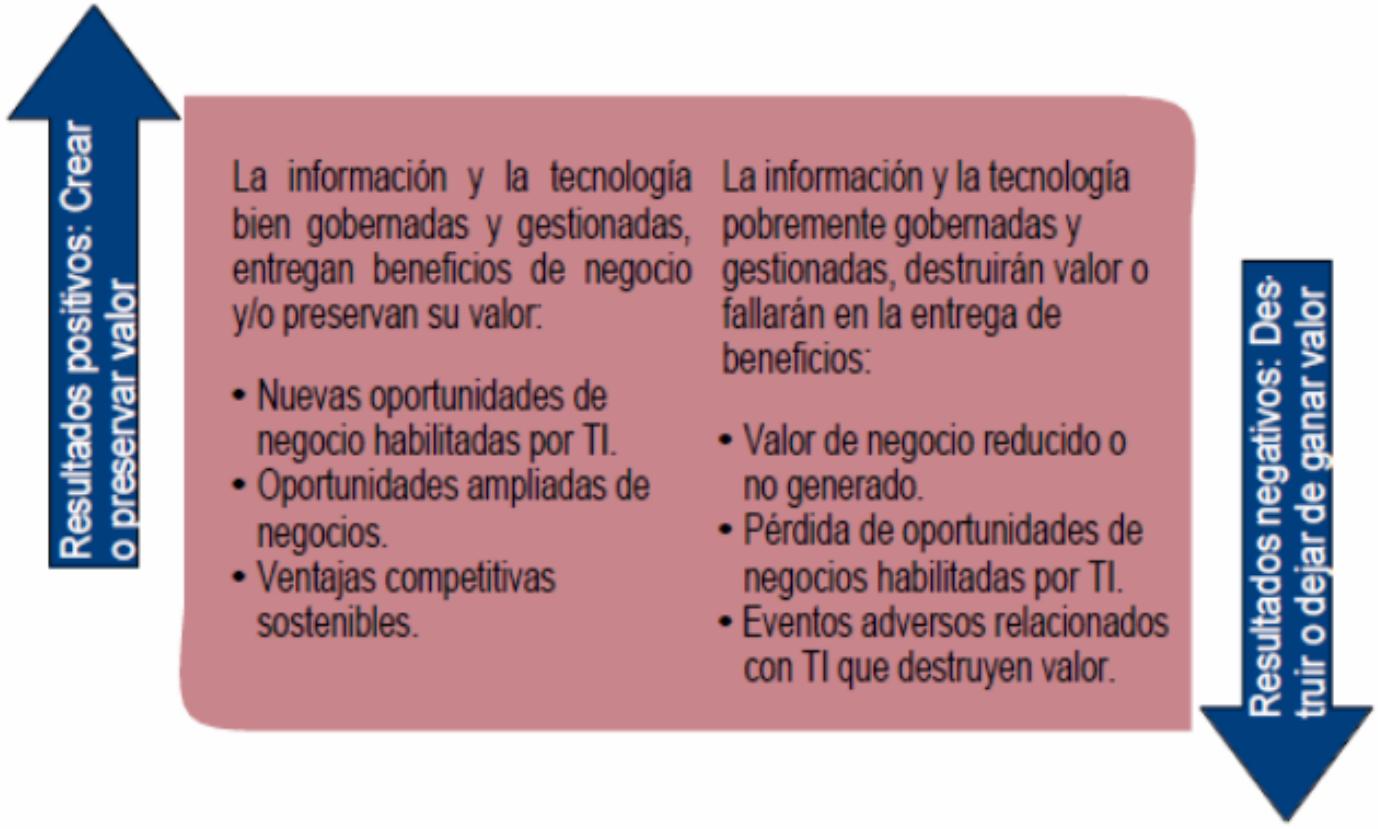
Figura 5 — Categorías de riesgo de TI

Fuente: ISACA, *The Risk IT Framework*, 2009, figura 2

COBIT

Dualidad del Riesgo

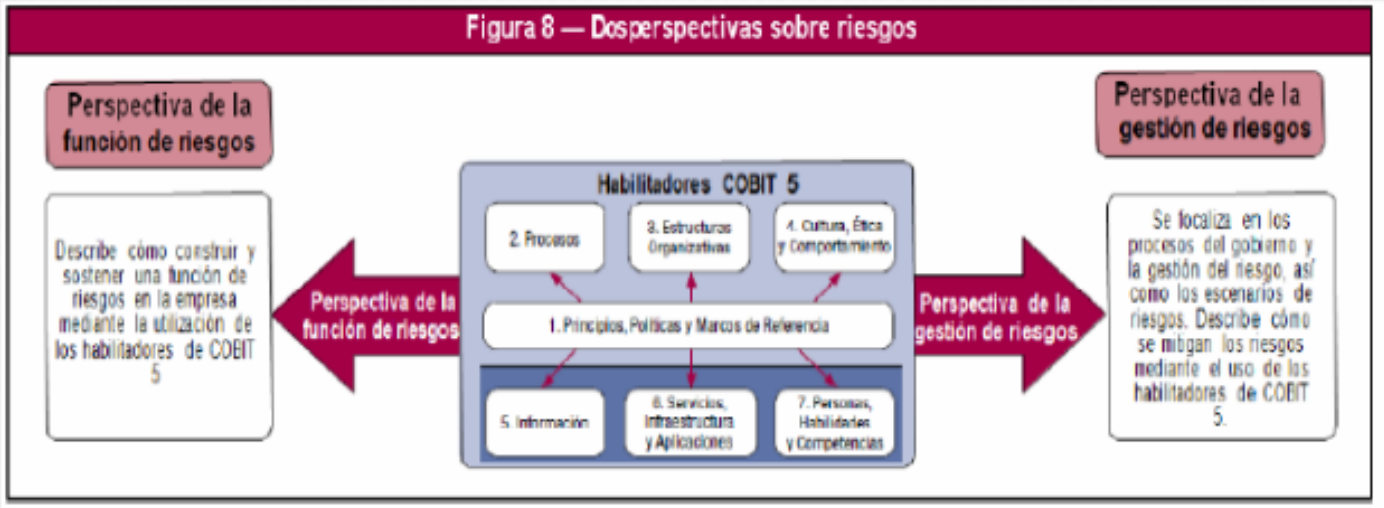
Figura 6 — Dualidad del riesgo



Fuente: ISACA CHAPTER MONTEVIDEO

COBIT

Perspectivas sobre Riesgos

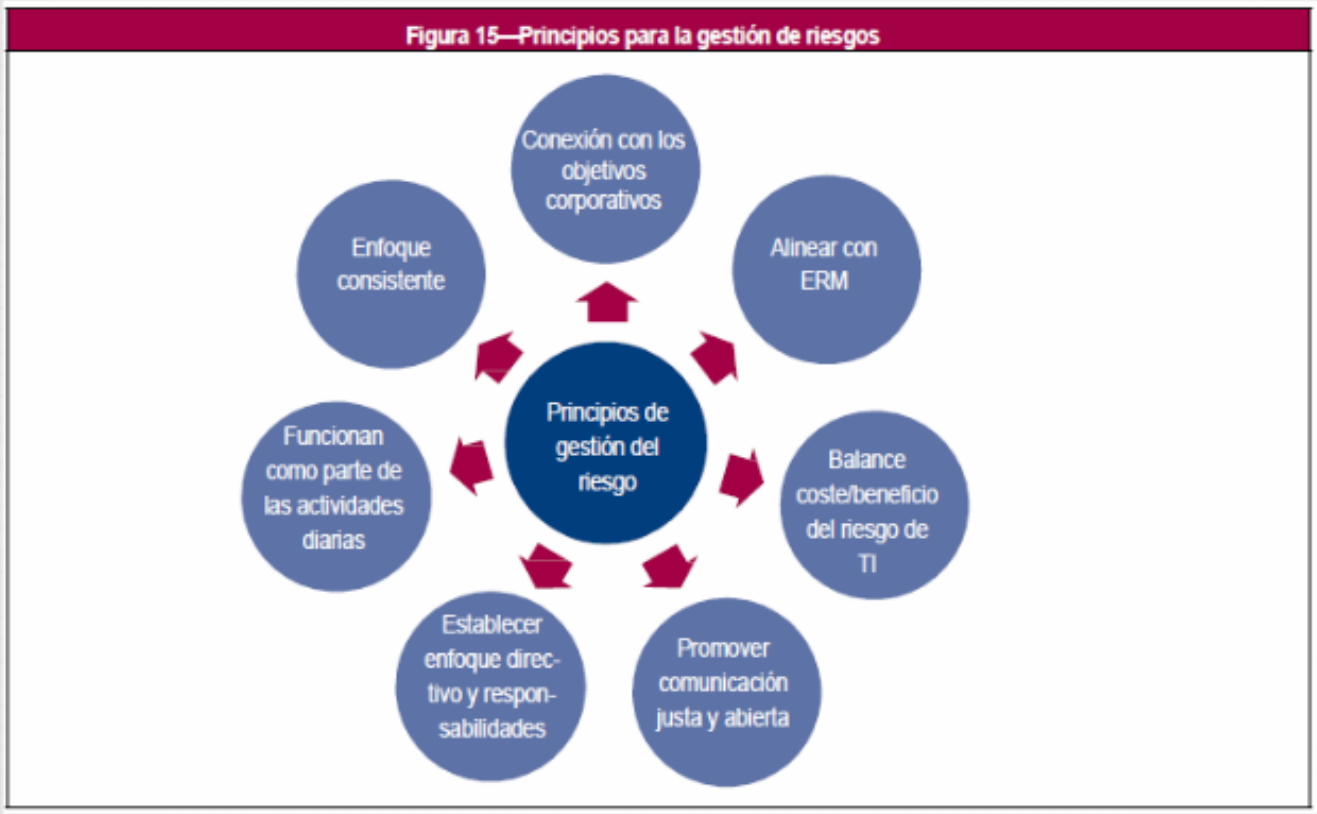


Fuente: ISACA CHAPTER MONTEVIDEO

COBIT

Principios para la Gestión de Riesgos

Figura 15—Principios para la gestión de riesgos



Fuente: ISACA CHAPTER MONTEVIDEO

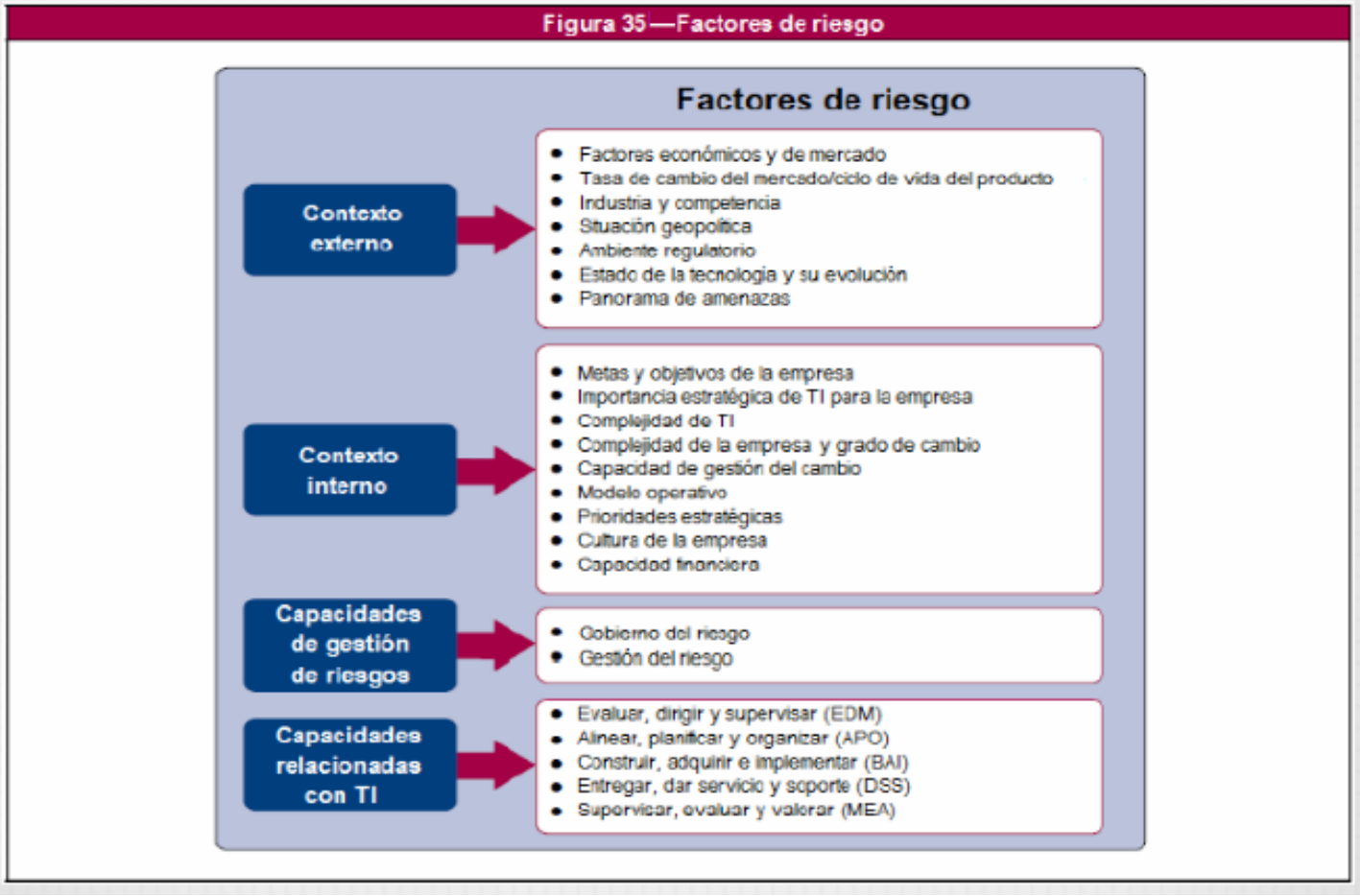
COBIT

Líneas de Defensa contra el Riesgo

Fuente: ISACA CHAPTER MONTEVIDEO

COBIT

Factores de Riesgo



Fuente: ISACA CHAPTER MONTEVIDEO

COBIT

Estructura de Escenario de Riesgos

Fuente: ISACA CHAPTER MONTEVIDEO

COBIT

Ejemplo de Escenario de Riesgos

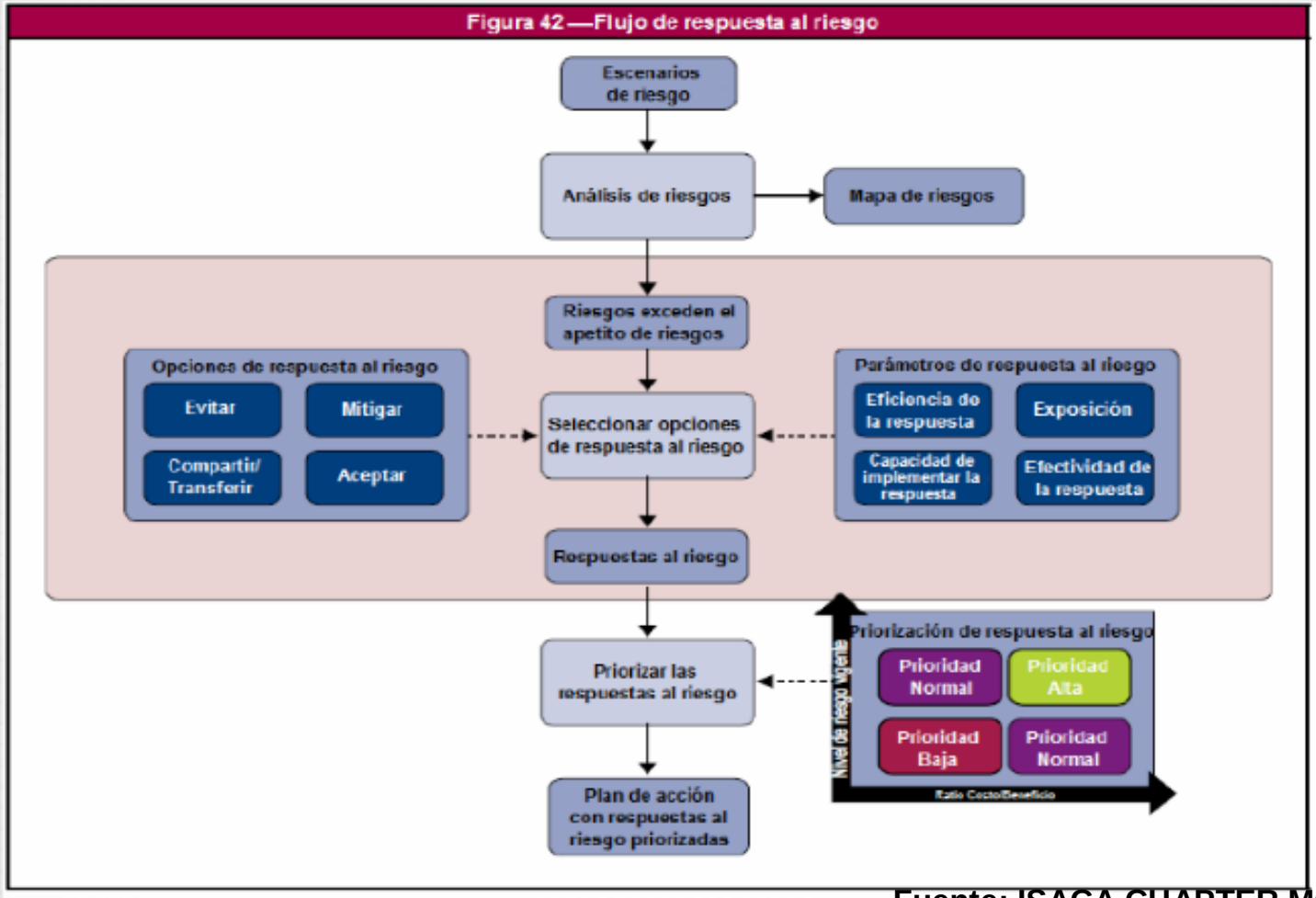
Figura 38—Ejemplo de escenarios de riesgos *(cont.)*

Ref.	Categoría de escenario de riesgos	Tipo de riesgo			Ejemplos de escenarios	
		Habilitación de Beneficio/Valor de TI	Entrega de Programas y proyectos de TI	Entrega de operaciones y servicios de TI	Ejemplos de escenarios negativos	Ejemplos de escenarios positivos
0201	Gestión del ciclo de vida de los programas/proyectos (inicio, aspectos económicos, entrega, calidad y finalización de los programas/ proyectos)	P	P	S	No se completan los proyectos con fallas (debido a costos, demoras, arrastres en el alcance, prioridades cambiantes de negocios).	Los proyectos fallidos o irrelevantes se detienen en forma oportuna.
0202		S	P	S	El presupuesto para proyectos de TI se encuentra excedido.	Se completa el proyecto de TI dentro del presupuesto acordado.
0203		S	P		Ocasionalmente, se tienen entregas tardías de los proyectos de TI por un departamento interno de desarrollo.	La entrega del proyecto se realiza a tiempo.
0204		P	P	S	Rutinariamente, existen importantes retrasos en la entrega de proyectos de TI.	La ruta crítica de los proyectos se gestiona en forma acordada y la entrega es oportuna.
0205		P	P	S	Existen demoras excesivas en proyectos de desarrollo externalizado de TI.	La comunicación con terceros asegura la entrega oportuna según alcance y calidad acordados.
0206		P	P		Los programas/proyectos fallan debido a la falta de involucramiento activo de las partes interesadas (incluyendo al patrocinador) durante su ciclo de vida.	La gestión de cambios en el ciclo de vida del programa/proyecto se conduce apropiadamente para informar a las partes interesadas del avance y para el entrenamiento de usuarios futuros.

Fuente: ISACA CHAPTER MONTEVIDEO

COBIT

Flujo de Respuesta al Riesgo



Fuente: ISACA CHAPTER MONTEVIDEO

COBIT

Ejemplo de Escenarios de Riesgos
Código Malicioso

Figura 38—Ejemplo de escenarios de riesgos *(cont.)*

Ref.	Categoría de escenario de riesgos	Tipo de riesgo: Habilitación de Beneficio/Valor de TI	Tipo de riesgo: Entrega de Programas y proyectos de TI	Tipo de riesgo: Entrega de operaciones y servicios de TI	Ejemplos de escenarios negativos	Ejemplos de escenarios positivos
1501	Código malicioso	S		P	Se ha producido una intrusión de código malicioso en los servidores operativos críticos.	La infraestructura de TI se protege de forma apropiada a través de firewalls y monitoreo continuo de la red, para asegurar la ejecución de las actividades diarias.
1502		S		P	Las computadores portátiles se infectan frecuentemente con código malicioso.	
1503		S		P	Un empleado insatisfecho implementa una bomba lógica que produce la pérdida de datos.	
1504		S		P	Roban los datos de la compañía a través de accesos no autorizados obtenidos mediante ataques de "phishing".	

Fuente: ISACA CHAPTER MONTEVIDEO

Beneficios de COBIT

- Mejor alineación, con base en su enfoque de negocios
- Visión entendible para la gerencia de lo que hacen los recursos de tecnología de información
- Propiedad y responsabilidades claras, con base en su orientación a procesos
- Aceptación general de terceros y reguladores
- Entendimiento compartido entre todos los Interesados, con base en un lenguaje común
- Cumplimiento de los requerimientos COSO para el ambiente de control de TI