Marco de Riesgos de TI

Risk IT
BASED ON COBIT®

ISACA®
Serving IT Governance Professionals

Risk IT
BASED ON COBIT®

RESUME EJECUTIVO

La información presentada ha sido traducida de los documentos en Inglés disponibles en www.isaca.org.
La utilización de términos del idioma Español en está presentación es una elección personal que puede no coincidir con la publicación de los documentos en Español de ISACA.

Un Conjunto de Guías Principales y el primer Marco de Trabajo que ayuda a las Empresas a Identificar, Gobernar y Administrar Efectivamente el Riesgo de TI

Contenido

- Definición del Universo del Riesgo
- Categorías del Riesgo
- Jerarquía de Riesgos
- Principios del Riesgo
- Modelo de Procesos de la Gestión del Riesgo
- Contenido Clave del Marco de Trabajo del Riesgo

Definición del universo del riesgo y alcance de la administración

MARCO DE RIESGOS DE TI

El riesgo debe ser visto desde una perspectiva de extremo a extremo, atravesando los silos de funcion de TI (operaciones, gestión de proyectos, desarrollo de aplicaciones, recuperación de desastres, seguridad).

El universo del riesgo describe el ambiente global del riesgo (ej. Define los límites de las actividades de gestión del riesgo). El universo de riesgo considera:

- Considera los objetivos de negocios globales, procesos de negocios y sus dependencias a través de la empresa. Describe cuáles son las aplicaciones e infraestructura de apoyo a los objetivos de negocio a través de la provisión de servicios de TI.

- Considera el ciclo de vida completo de las actividades del negocio, incluyendo los programas de transformación, investigaciones, proyectos y operaciones.

• Considera la cadena de valor de la empresa, esta incluye no solo la empresa sino tambien sus sucursales/unidades de negocio , pero tambien clientes abastecedores y proveedores de servicios.

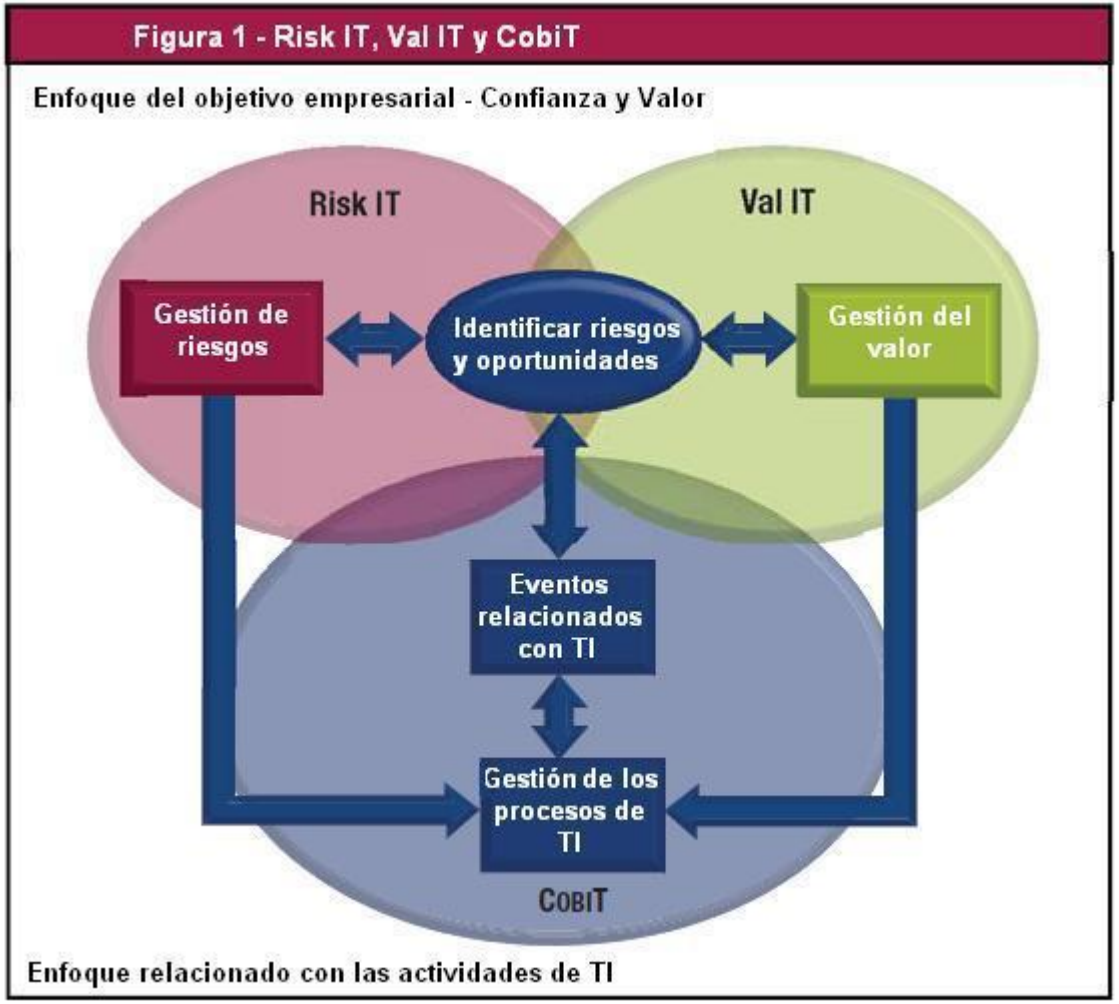
Cuándo se identifican las oportunidades de cambios del negocio relacionados con TI, el Marco VAL IT describe cómo progresar y maximizar el retorno de la inversión realizada en los mismos. El resultado de la evaluación tendrá probablemente un impacto en algunos de los procesos de TI, por lo que las flechas de la Gestión de Riesgos" y Gestión del Valor se dirigen a la "Gestión de los Procesos de TI" .

Comprende las bases del Riesgo Tecnológico, sus conceptos, alcances, normas aplicables y las fases fundamentales en la aplicación del riesgo.

CIT CONSULTING INFORMATION TECHNOLOGY S.A.

MARCO DE RIESGOS DE TI

Figura 1 - Risk IT, Val IT y CobiT



CIT

Concepto de Riesgo

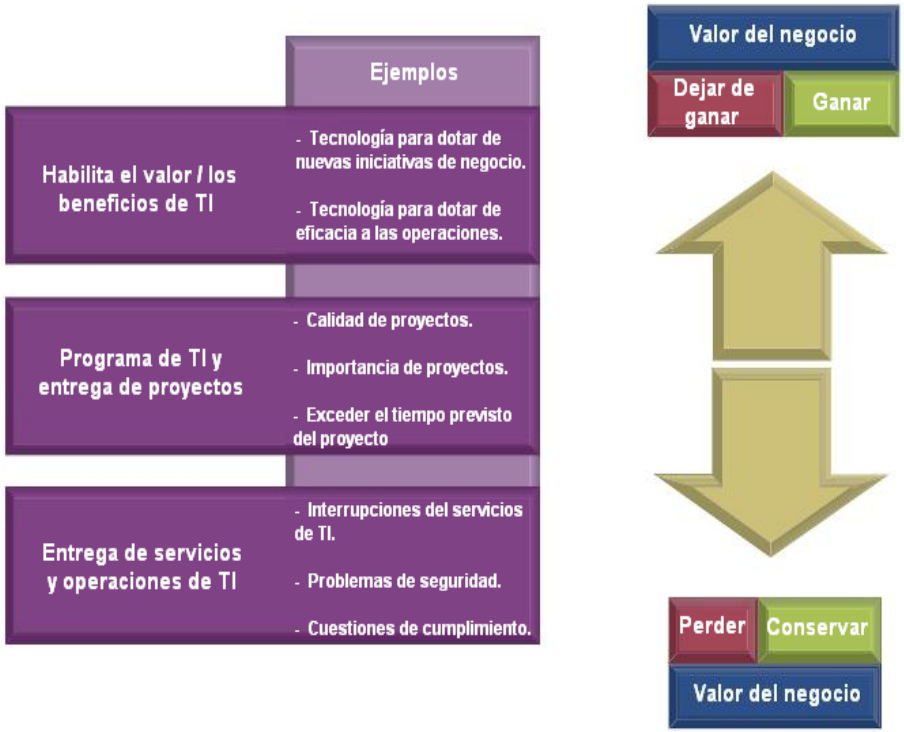
Un riesgo de TI es también un riesgo del negocio, riesgos del negocio asociados con el uso, propiedad, operación, participación, la influencia y la adopción de las TI en una organización.

Se compone de los eventos relacionados con TI que potencialmente podrían afectar el negocio. Este hecho puede ocurrir con una frecuencia y magnitud inciertas, y supone dificultades para alcanzar las metas y objetivos estratégicos. Los riesgos de TI pueden clasificarse de diversas maneras.

Categorías del Riesgo

CATEGORIAS DE RIESGOS DE TI

Figura 2 - Categorías de los riesgos de TI



CIT

Categoría de los Riesgos de TI

• Beneficios de TI / valor de la habilitación del riesgo de TI - Asociados con la ausencia de las oportunidades para utilizar la tecnología, con el fin de mejorar la eficiencia o efectividad de los procesos de negocio o como un facilitador para nuevas iniciativas de negocio.

• Programa de TI y el riesgo de ejecución de proyectos - Asociado con la contribución de las TI para nuevos o mejores soluciones de negocios , por lo general en la forma de proyectos y programas. Esto se vincula a la gestión de las inversiones de cartera (como se describe en el marco de VAL IT).

• Las operaciones de TI y el riesgo de la prestación de servicios - Asociado con la disponibilidad, estabilidad, protección y recuperabilidad de todos los servicios de TI, que pueden ocasionar la destrucción o la reducción de valor para la organización.

Los riesgos de TI siempre existen, sean o no detectados o reconocidos por la organización.

Que hacemos?

Se realiza una vista inicial de los riesgos generales o de alto nivel que la Compañía debe enfrentar, de acuerdo a factores definidos, que van a determinar la criticidad general de la entidad (o funciones o procesos), lo cual ayudará a conocer por donde se comenzará el primer análisis de riesgo.

Marco basado en:

El marco de RISK IT se basa en los principios de gestión de los riesgos organizacionales (ERM), las normas y marcos como COSO ERM 2 y AS/NZS 43603 (que pronto serán complementados o sustituidos por la norma ISO 31000) y provee información acerca de cómo aplicar estos principios a las TI. RISK IT aplica los conceptos generalmente aceptados de los principales estándares y marcos, así como los principales conceptos de la gestión de otros riesgos de TI, relacionados con las normas.

Jerarquía de Riesgos

JERARQUIA DE RIESGOS

Figura 3 - Riesgos de TI en la jerarquía de riesgos

RISK IT es el riesgo comercial, es decir, el riesgo de los negocios asociados con el uso, la propiedad, la operación, la participación, la influencia y la adopción de las TI dentro de una organización. Se compone de eventos relacionados con IT que podrían afectar a la organización. Esto incluye tanto la frecuencia y la magnitud incierta, la creación de problemas en el cumplimiento de metas y objetivos estratégicos, así como la incertidumbre en la búsqueda de oportunidades.

CIT

Propósito del marco de trabajo

El marco de Riesgos de TI explica los riesgos y permite a los usuarios:

• Integrar la gestión de los riesgos en el ERM de la organización, esto permitirá que se tomen decisiones conscientes sobre el retorno de los riesgos.

• Tomar decisiones con conocimiento acerca de la magnitud del riesgo, el apetito de riesgo y la tolerancia al riesgo de la organización.

• Entender cómo responder a los riesgos.

El Marco provee de:

• Un marco de proceso de punta a punta para gestión de riesgos de TI correcta.

• Orientación para los profesionales, incluyendo herramientas y técnicas para entender y gestionar los riesgos concretos para las operaciones de negocio. Esto incluye una lista genérica de campo común, los panoramas relacionados con la TI potencialmente adversos del riesgo que podrían afectar la realización de los objetivos de negocio.

Principios del Riesgo

Figura 5 - Principios de los riesgos de TI

PRINCIPIOS DEL MARCO DE RIESGOS DE TI

El marco de RISK IT se basa en los riesgos de TI. En otras palabras, el riesgo organizacional está relacionado con el uso de las TI. La conexión con la organización se basa en los principios en los que se construye el marco, es decir, el gobierno efectivo de la organización y gestión de los riesgos de TI.

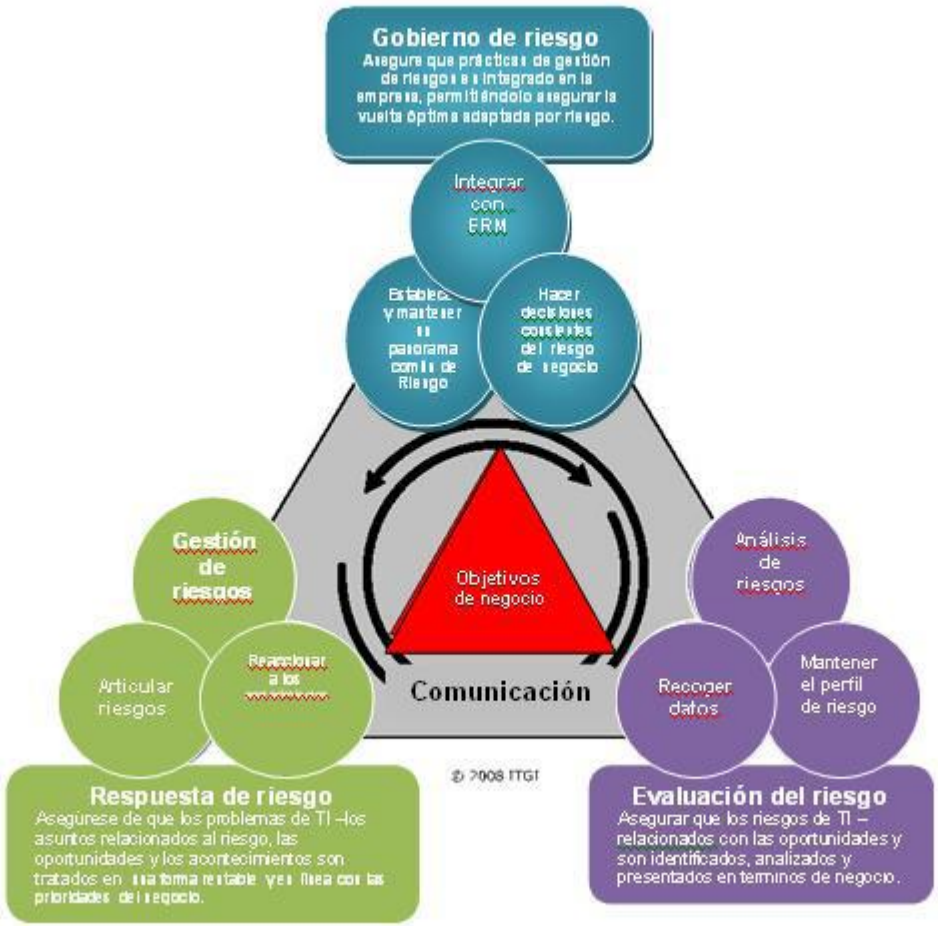
Principios

- Alinear siempre con los objetivos organizacionales.
- Alinear la gestión de las TI con el riesgo organizacional relacionado con el total de ERM.
- Balance de los costes y los beneficios de la gestión de los riesgos de TI.
- Promover la comunicación abierta y equitativa de los riesgos de TI.
- Establecer el tono correcto desde un enfoque de arriba abajo, definiendo y haciendo cumplir la responsabilidad del personal con los niveles de tolerancia aceptables y bien definidos.
- Son un proceso continuo y parte de las actividades diarias.

Modelo de Procesos de la Gestion de Riesgo de TI

MARCO DEL RIESGO DE TI

Figura 6 – Marco del riesgo de TI



Ámbitos o Dominios del Modelo de Procesos de Riesgos de TI

El modelo se divide en tres ámbitos o dominios: gobernanza del riesgo, evaluación de riesgos y respuesta de riesgos, cada uno con tres procesos:

• Gobierno del riesgo (GR)
- RG1 Establecer y mantener una vista de riesgo común.
- RG2 Integrar con ERM.
- RG3 Tomar decisiones conscientes de los riesgos del negocio.

• Evaluación de riesgos (RE)
- RE1 Recoger datos.
- RE2 Analizar los riesgos.
- RE3 Mantener perfil de riesgo.

• Respuesta de riesgos (RR)
- RR1 Riesgo articulado
- RR2 Manejar riesgos
- RR3 Reaccionar a acontecimientos

Contenido Clave del Marco de Trabajo de Riesgo de TI

El contenido clave del marco de riesgo de TI incluye:

El modelo se divide en tres ámbitos o dominios: gobernanza del riesgo, evaluación de riesgos y respuesta de riesgos, cada uno con tres procesos:

Elementos de la Gestión del riesgo

En el **Gobierno del Riesgo**: El apetito y la tolerancia al riesgo, responsabilidades y rendición de cuentas sobre la gestión de riesgos de TI, sensibilización y comunicación y cultura del riesgo.

En la **Evaluación del Riesgo**: Describe el impacto del negocio y los escenarios de riesgo.

En la **Respuesta del Riesgo**: Los indicadores claves de riesgo (KRI) y las definiciones y priorización de la respuesta del riesgo.

Risk IT

BASED ON COBIT®

info@consultinginformationtechnology.com
www.consultinginformationtechnology.com

CIT