

6a. Academia de Actualización Profesional 2009 Administración de Riesgos en IT



Agenda / Contenido

Introducción conceptual sobre Administración de Riesgos Corporativos

Riesgos en IT

Key Risk Indicators

Beneficios de la Administración de Riesgos

Agenda / Contenido

Introducción conceptual sobre Administración de Riesgos Corporativos

Riesgos en IT

Key Risk Indicators

Beneficios de la Administración de Riesgos

Definición formal de Administración de Riesgos (COSO II)

“La Administración de Riesgos corporativos es un proceso efectuado por el consejo de administración de una entidad, su dirección y restante personal, aplicable a la definición de estrategias en toda la empresa y diseñado para identificar eventos potenciales que puedan afectar a la organización, gestionar sus riesgos dentro del riesgo aceptado y proporcionar una seguridad razonable sobre la consecución de objetivos de la entidad.”

Los principales puntos a resaltar de dicha definición son que la Administración de Riesgos es un **proceso** (no alcanza con una “foto” de la organización), que debe ser llevado adelante por todo el **personal**, y que se basa en la detección de eventos que puedan comprometer el cumplimiento de cualquier **objetivo** de la entidad.

Definición formal de Administración de Riesgos (COSO II)



Definición formal de Administración de Riesgos (COSO II)

Riesgo: evento que, de ocurrir, tiene un impacto negativo sobre un cierto objetivo, pudiendo impedir la creación de valor para la organización o erosionar el valor existente.

Probabilidad: indicador de la factibilidad de que el riesgo ocurra en la práctica.

Impacto: indicador de las pérdidas estimadas de cualquier índole (económicas, de imagen, de oportunidad, etc.) que puede sufrir la organización en caso de que el riesgo ocurra.

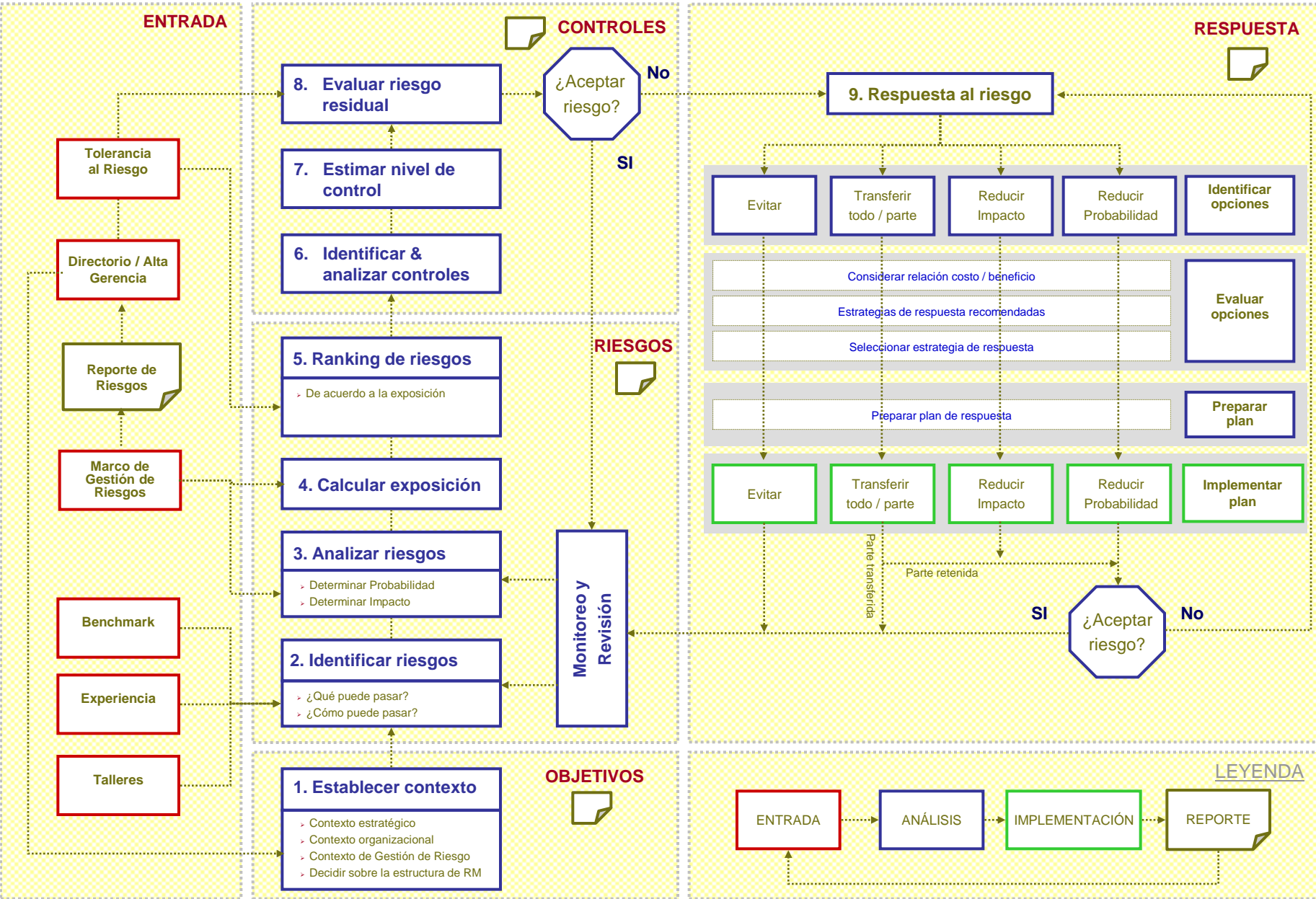
Control: toda acción tendiente a reducir la probabilidad y/o el impacto de uno o varios riesgos.

Definición formal de Administración de Riesgos (COSO II)

Exposición: es una función que relaciona el impacto y la probabilidad, que se utiliza a efectos de facilitar el análisis. Distinguimos entre la exposición inherente, la cual se obtiene considerando el impacto y probabilidad “naturales” de un riesgo, es decir, sin tener en cuenta el efecto de ningún control; y la exposición residual, la cual se obtiene considerando el impacto y probabilidad ajustados según los controles instalados.

Tolerancia al Riesgo: determina a partir de qué nivel la exposición residual se considera inaceptable. En otras palabras, que tanto riesgo se está dispuesto a asumir por la organización.

Introducción conceptual sobre Administración de Riesgos Corporativos



Agenda / Contenido

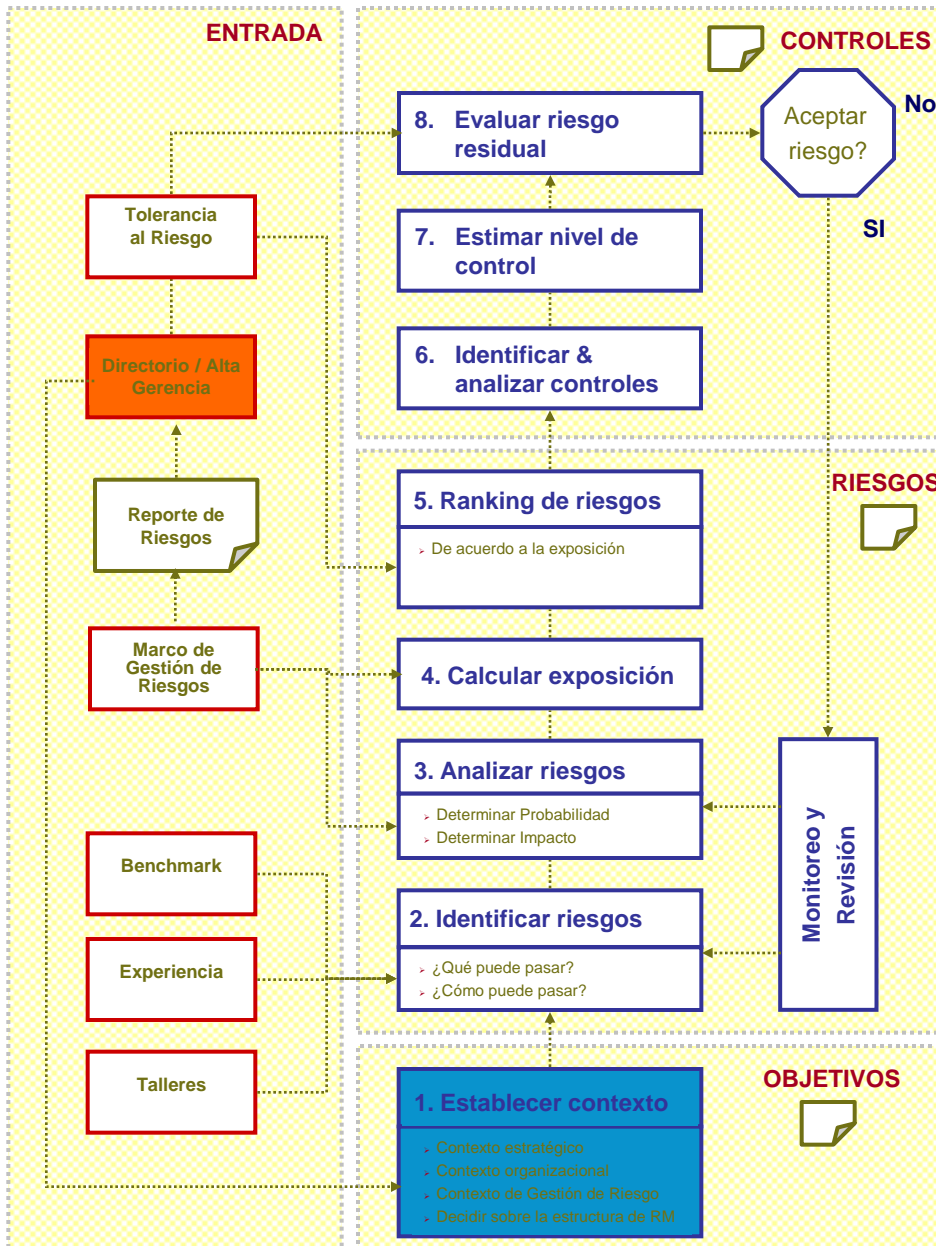
Introducción conceptual sobre Administración de Riesgos Corporativos

Riesgos en IT

Key Risk Indicators

Beneficios de la Administración de Riesgos

Riesgos en IT



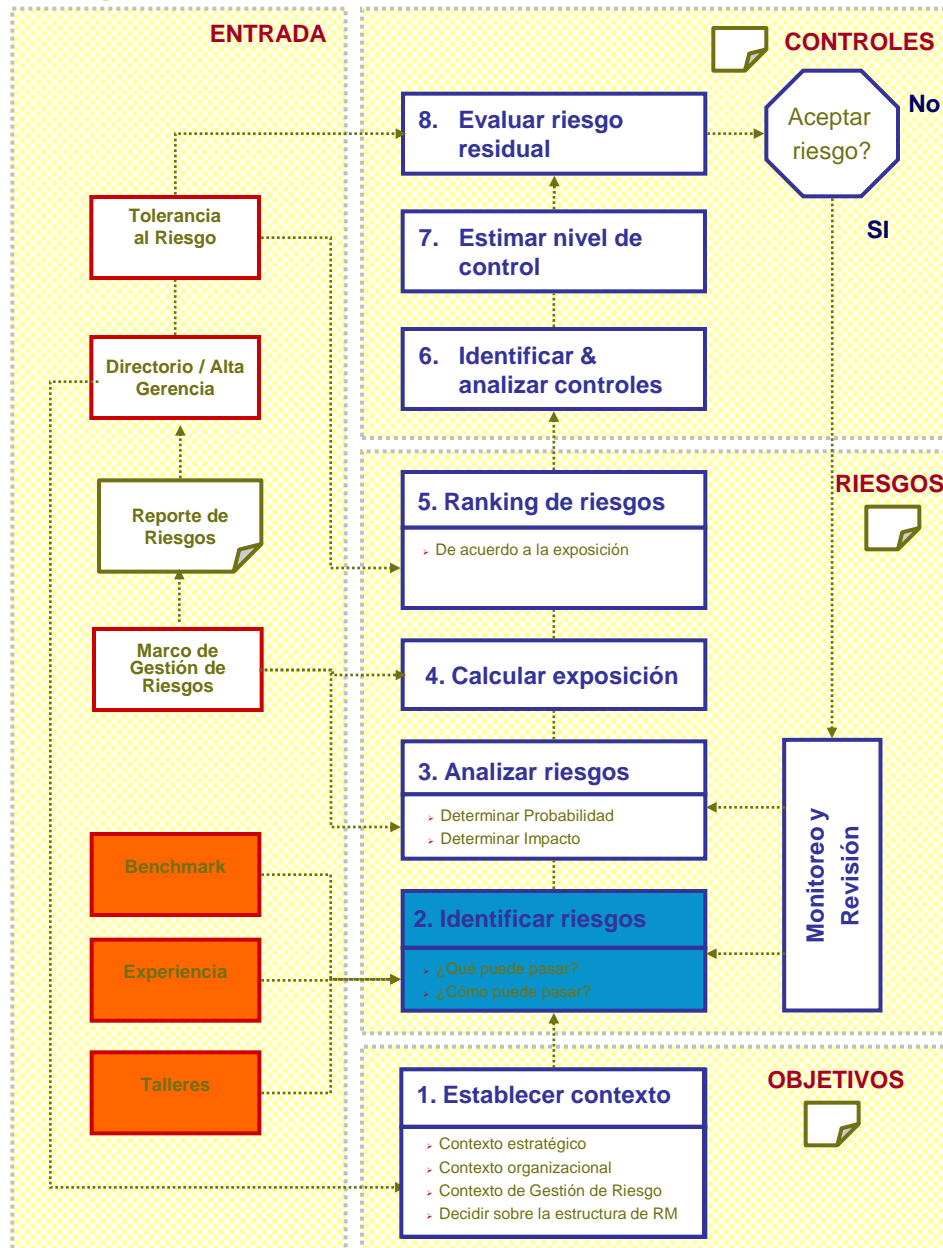
Objetivos

De acuerdo al plan estratégico de IT, la gerencia selecciona los objetivos más importantes del área.

Ejemplo: Mantener presencia en Internet en forma segura y con una performance adecuada.

Categorías de riesgos

Categoría	Ejemplos de riesgos
Plataforma tecnológica de hardware y software de base	Obsolescencia, falta de capacidad, problemas con el soporte, ...
Sistemas de aplicación	Problemas de mantenimiento, baja performance, ...
Acceso a datos	Accesos no autorizados al CPD, divulgación de información confidencial...
Utilitarios y herramientas disponibles	Baja productividad, ...
Recursos Humanos	Capacitación inadecuada, pérdida de personal clave, ...
Planificación estratégica	Falta de alineación con el negocio, no contar con planes a largo plazo, ...
Adquisición e implementación	No contar con procedimientos adecuados, falta de monitoreo / mantenimiento, ...
Desarrollo, operaciones y atención a clientes	Manuales de operación desactualizados, no involucramiento de los usuarios en el desarrollo, ...
Monitoreo	Insuficiencia de recursos, ...
Reputación e imagen	Poco entendimiento de los servicios de IT por parte de los usuarios, ...
Auditoría / revisiones externas	No contar con controles adecuados, no cumplir con las recomendaciones de auditoría, ...
Normativa / legal	Incumplimiento de contratos, incumplimiento de normas de reguladores, ...



Identificar Riesgos

A la hora de identificar riesgos es crítico contar con un proceso sistemático para lograr una lista lo más completa posible.

Ejemplo:

Plataforma tecnológica de hardware y software de base: Capacidad del hardware insuficiente (R1).

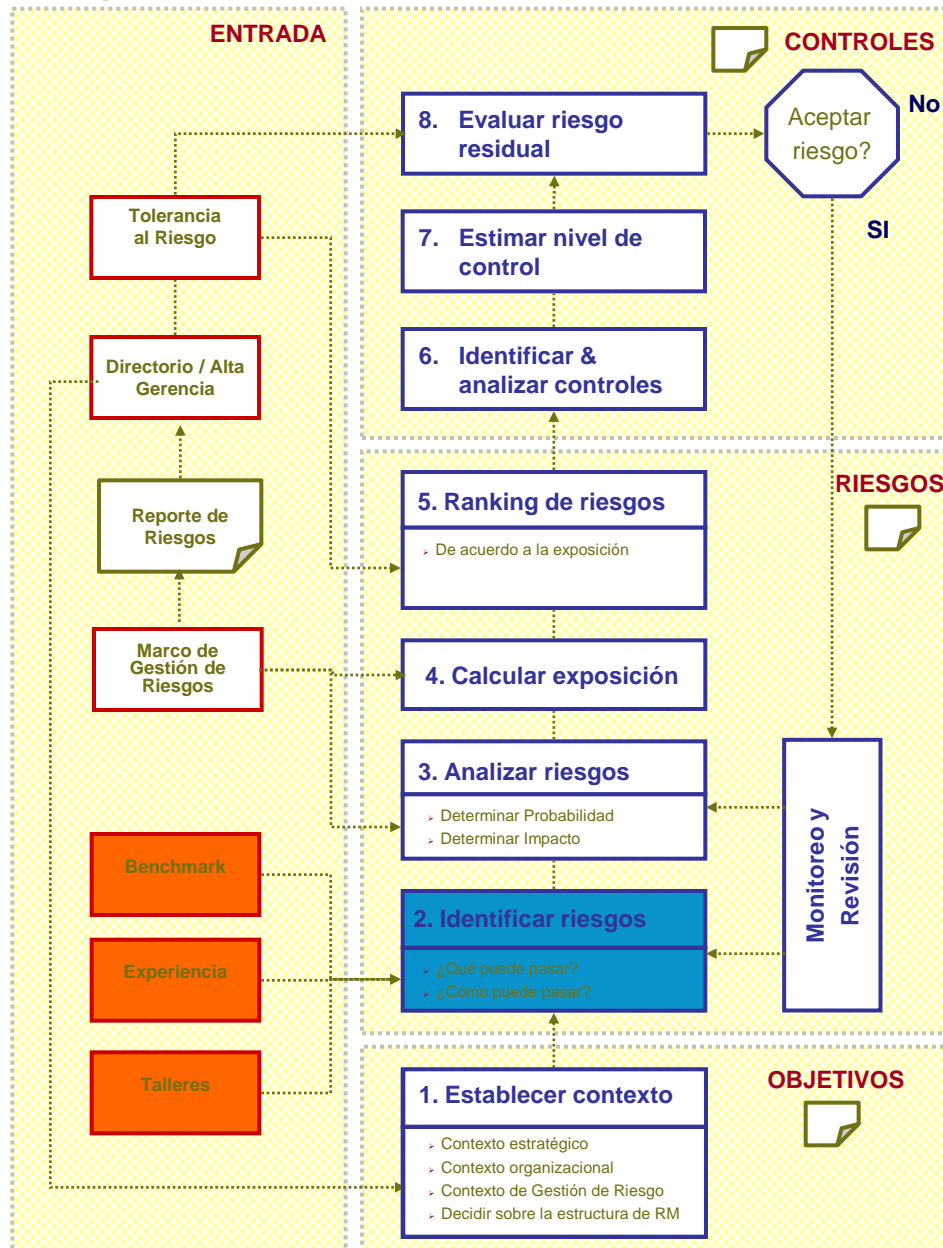
Sistemas de aplicación: -

Acceso a datos: Acceso no autorizado a información sensible (R2).

Utilitarios y herramientas disponibles: -

Recursos Humanos: No contar con personal calificado en seguridad de la información (R3).

Planificación estratégica, organización y gestión: -



Identificar Riesgos (Cont.)

Adquisición e implementación: -

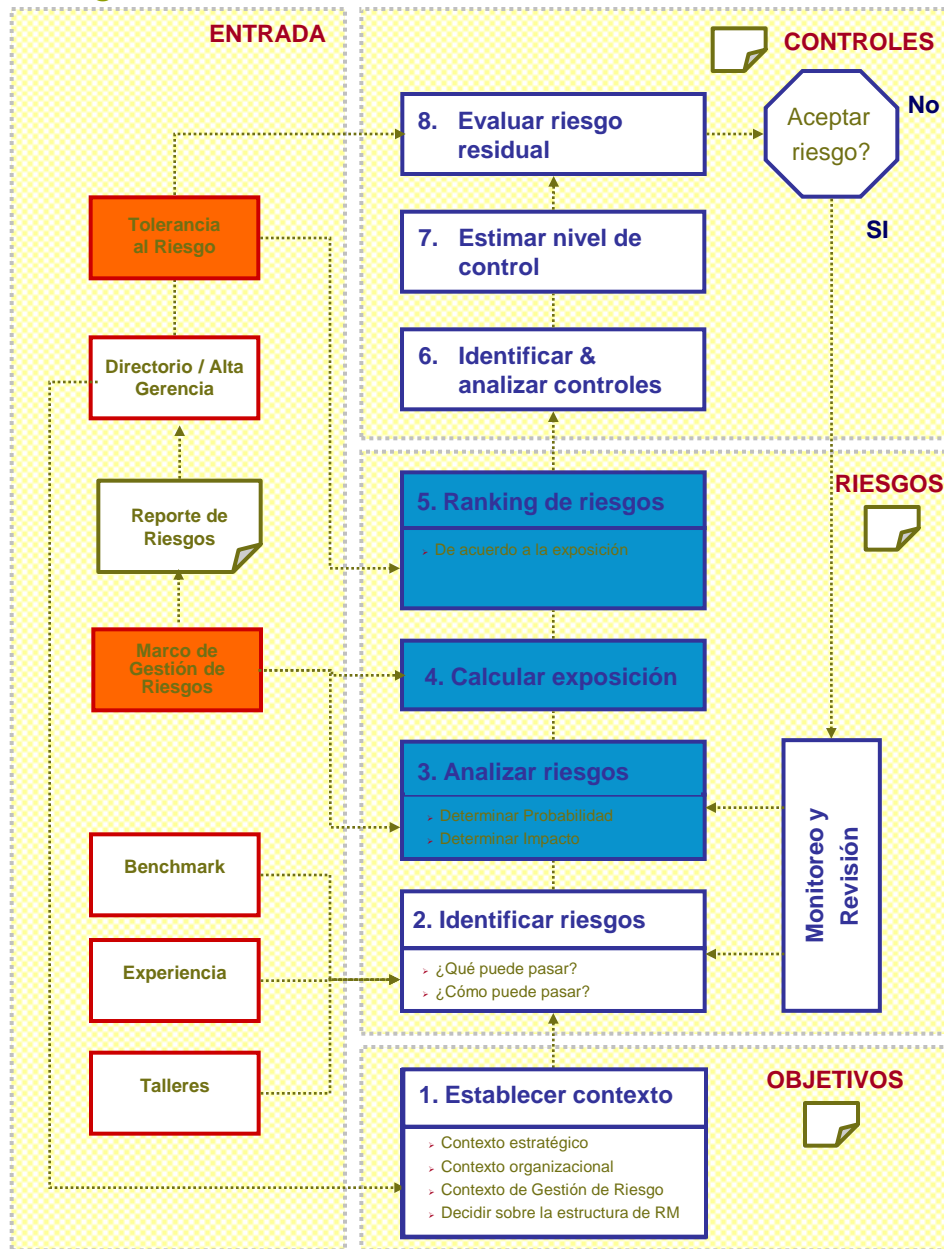
Desarrollo, operaciones y atención a clientes: -

Monitoreo: No disponer de los recursos necesarios (R4).

Reputación e imagen: No lograr un grado de calidad aceptable (R5).

Auditoría / Revisiones externas: -

Normativa / Legal: -



Evaluar Riesgos

Un aspecto relevante para estandarizar las prácticas de Administración de Riesgos es utilizar criterios lo más unificados posibles para estimar probabilidades e impactos.

De esta forma se busca minimizar (aunque es imposible de eliminar totalmente) la visión subjetiva del analista al momento de aplicar la técnica.

Evaluar Riesgos (Cont.)

Ejemplo de criterios de probabilidad

Muy Alta	<p>Muy Probable Probablemente ocurra en el año (más de 35% de probabilidad de ocurrencia)</p>	<ul style="list-style-type: none"> - Ha ocurrido en el último año - Es típico de las operaciones de este negocio - Potencialmente puede ocurrir varias veces en los próximos 5 años
Alta	<p>Probable Probablemente ocurra en los próximos 2 años (más de 25% y menos de 35% de probabilidad de ocurrencia)</p>	<ul style="list-style-type: none"> •- Ha ocurrido en los 2 últimos años •- Es típico de las operaciones de este negocio •- Potencialmente puede ocurrir varias veces en los próximos 10 años
Media	<p>Posible Probablemente ocurra en los próximos 10 años) (más del 2% y menos del 25% de probabilidad de ocurrencia)</p>	<ul style="list-style-type: none"> •- Puede ser difícil de controlar debido a alguna influencia externa •- Existen antecedentes de haber ocurrido en la empresa •- Potencialmente puede ocurrir varias veces en los próximos 15 años
Baja	<p>Poco probable (menos del 2% de probabilidad de ocurrencia)</p>	<ul style="list-style-type: none"> •- Nunca ocurrió en la región •- Sería sorprendente si ocurriera

Evaluar Riesgos (Cont.)

Ejemplo de criterios de impacto

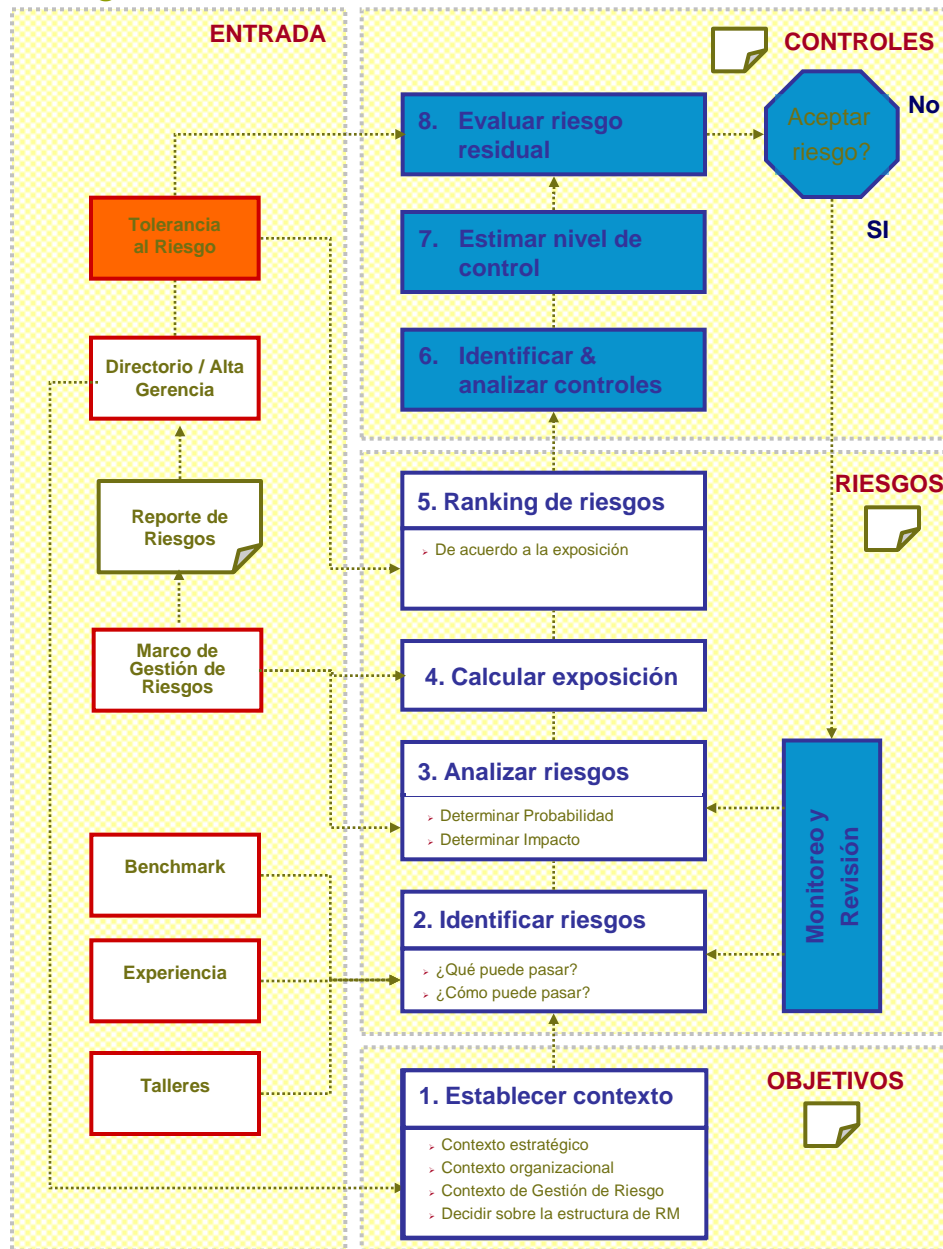
Muy Alto	Representa una situación donde se esperan pérdidas económicas o de imagen muy significativas	<ul style="list-style-type: none"> •- Servicios críticos no disponibles •- Prácticamente todos los clientes afectados •- Expectativas de juicios •- Pérdida de total de confianza
Alto	Representa una situación donde se esperan pérdidas económicas o de imagen moderadas	<ul style="list-style-type: none"> •- Degradación significativa en servicios críticos •- Número significativo de clientes afectados •- Expectativas concretas de multas / compensaciones
Medio	Representa una situación donde se produce algún impacto menor a los clientes	<ul style="list-style-type: none"> •- Pérdida de algunos servicios no críticos •- Algunos clientes afectados •- Posibles multas / compensaciones menores
Bajo	Representa una situación que afecta a algunos servicios internos	<ul style="list-style-type: none"> •- Degradación tolerable de servicios •- Algunos clientes internos afectados

Evaluar Riesgos (Cont.)

Riesgo	Probabilidad (inherente)	Impacto (inherente)
Capacidad del hardware insuficiente (R1)	Media	Alto
Acceso no autorizado a información sensible (R2)	Muy Alta	Muy Alto
No contar con personal calificado (R3)	Media	Medio
No disponer de los recursos necesarios (R4)	Alta	Alto
No lograr un grado de calidad aceptable (R5)	Alta	Medio

Evaluar Riesgos (Cont.)

		Tolerancia al Riesgo			
Probabilidad	Muy Alta				R2
	Alta		R5	R4	
	Media		R3	R1	
	Baja				
		Bajo	Medio	Alto	Muy Alto
		Impacto			



Evaluar Controles

En este punto se identifican y se evalúan los controles instalados que disminuyen la probabilidad y/o impacto de los riesgos analizados.

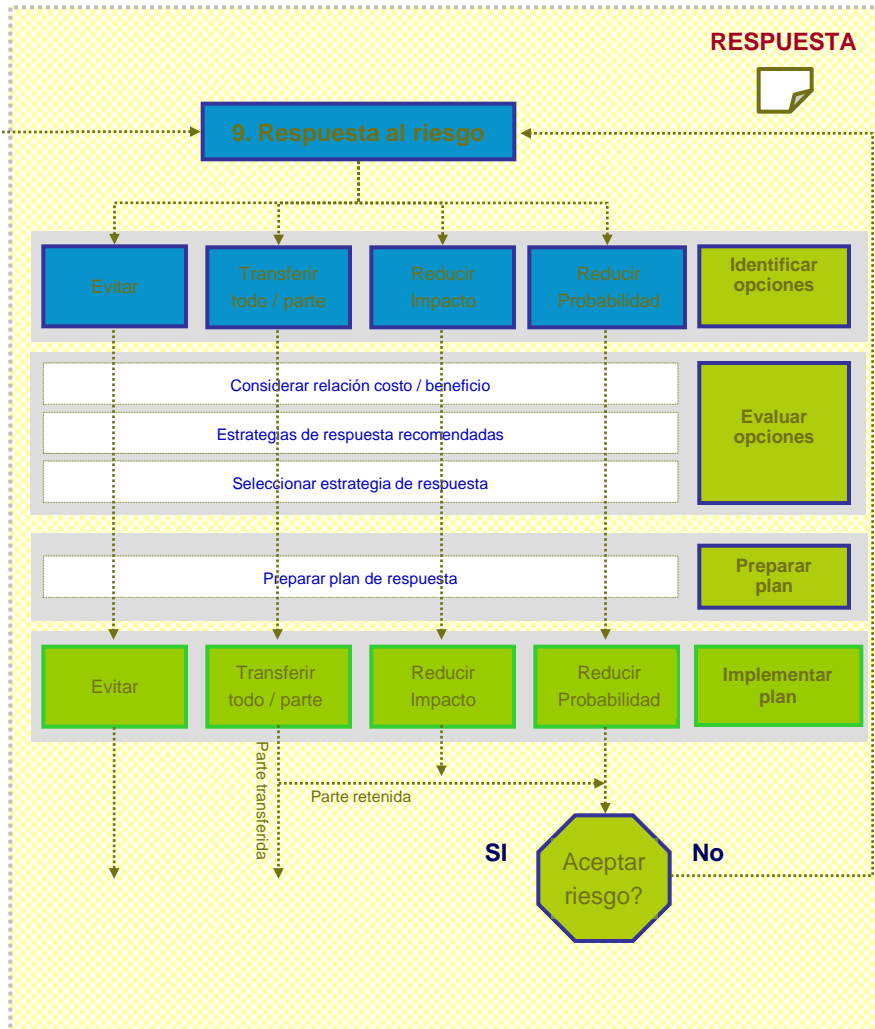
Es posible entonces estimar la exposición residual para clasificar nuevamente los riesgos (residuales) y determinar cuáles son tolerables -hay que monitorear- y cuáles no -hay que elaborar una respuesta-

Evaluar Riesgos residuales

Riesgo	Controles	Probabilidad (residual)	Impacto (residual)
Capacidad del hardware insuficiente (R1)		Media	Alto
Acceso no autorizado a información sensible (R2')	Estructura de Control Interno, DMZ	Baja	Muy Alto
No contar con personal calificado (R3)		Media	Medio
No disponer de los recursos necesarios (R4)		Alta	Alto
No lograr un grado de calidad aceptable (R5)		Alta	Medio

Evaluar Riesgos (Cont.)

		Tolerancia al Riesgo			
Probabilidad	Muy Alta				R2
	Alta		R5	R4	
	Media		R3	R1	
	Baja				R2'
		Bajo	Medio	Alto	Muy Alto
		Impacto			



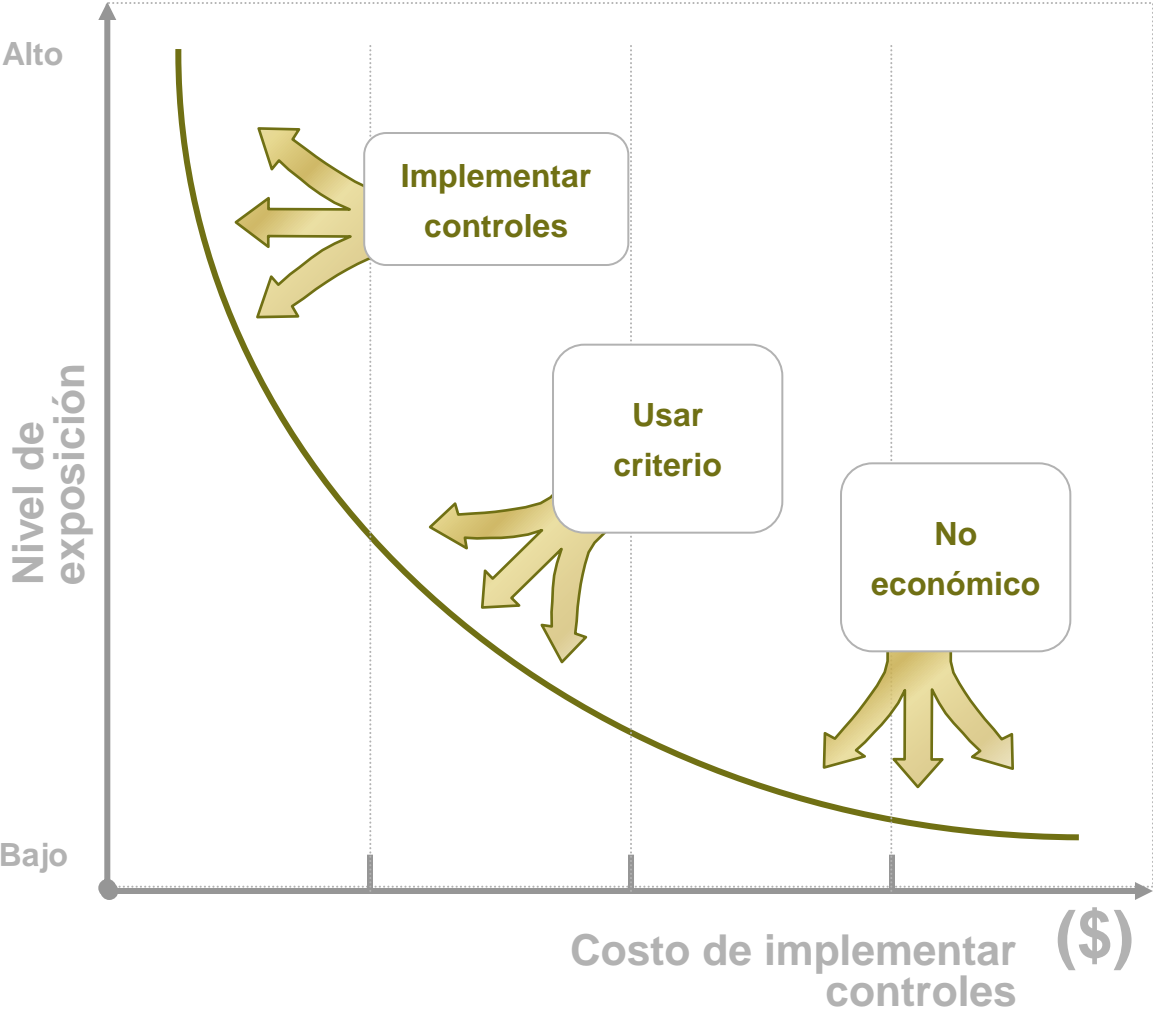
Respuesta a los riesgos

En líneas generales los riesgos que queden marcados como “Aceptables” no requerirán acciones adicionales mientras que los que queden como “Atención” requerirán de un monitoreo adecuado para garantizar que se mantengan en dicho nivel (o se reduzcan).

Por otra parte, cualquier riesgo cuya exposición residual resulte “Inaceptable” requerirá de la preparación de un Plan de Acción para su corrección/mejora/mitigación.

Ejemplo: Contratar servicio de monitoreo a un tercero.

Respuesta a los Riesgos (Cont.)



Agenda / Contenido

Introducción conceptual sobre Administración de Riesgos Corporativos

Riesgos en IT

Key Risk Indicators

Beneficios de la Administración de Riesgos

Definición de KRI

Se trata de mediciones cuantitativas o cualitativas que proporcionan un mayor conocimiento de los riesgos potenciales permitiendo identificar un aumento de la exposición más allá de los valores aceptables.

Para que resulten útiles deben estar disponibles de manera oportuna.

Ejemplo 1

Objetivo de IT – Crear y mantener un nivel de seguridad elevado contra intrusiones externas en los sistemas.

Medición – Número de intrusiones realizadas con éxito.

Medida objetivo y tolerancia – objetivo: 0 por mes, tolerancia: 0 por mes.

Evento posible – Acceso de individuos no autorizados a los sistemas de la empresa a través de conexiones de Internet.

Definición de KRI (Cont.)

Ejemplo 2

Objetivo de IT – Mantener estable el personal altamente calificado.

Medición – Porcentaje de rotación del personal altamente calificado.

Medida objetivo y tolerancia – objetivo: rotación del personal altamente calificado < 10%, tolerancia: 2%

Evento posible – Los mejores empleados renuncian.

Agenda / Contenido

Introducción conceptual sobre Administración de Riesgos Corporativos

Riesgos en IT

Key Risk Indicators

Beneficios de la Administración de Riesgos

Beneficios esperados

- Alinear el riesgo aceptado y la estrategia
- Mejorar las decisiones de respuesta a los riesgos
- Reducir las sorpresas y pérdidas operativas
- Identificar y gestionar la diversidad de riesgos para toda el área
- Aprovechar las oportunidades
- Mejorar la utilización de capital

Nuestra Visión
Ser la Firma líder
en servicios profesionales,
referente del mercado.

©2009 PricewaterhouseCoopers Ltda., PricewaterhouseCoopers, PricewaterhouseCoopers International Business Services Ltda., Shaw Faget & Asociados, Shaw Faget & Asociados International Business Services Ltda. y PW Software Ltda. Todos los derechos reservados. PricewaterhouseCoopers se refiere a las firmas uruguayas de PricewaterhouseCoopers Ltda., PricewaterhouseCoopers, PricewaterhouseCoopers International Business Services Ltda., Shaw Faget & Asociados, Shaw Faget & Asociados International Business Services Ltda. y PW Software Ltda. o, según requiera el contexto, a la red de firmas miembro de PricewaterhouseCoopers International Limited, cada una de las cuales es una entidad legal separada e independiente.

PRICEWATERHOUSECOOPERS 