everis

attitude makes the difference

Medición de riesgos tecnológicos: un enfoque práctico

VIII Conferencia Anual de la Asociación Española de Métricas de Sistemas Informáticos

1 de octubre 2007

Introducción

"Riesgo Operacional es el riesgo de pérdidas directas o indirectas que resultan de procesos internos inadecuados o de fallos en los mismos, fallos humanos, de sistemas y como consecuencia de sucesos externos"

En los últimos años, la incidencia del Riesgo Operacional ha crecido fuertemente debido a cambios en el Marco Competitivo, en el Marco Regulatorio y en la Operativa

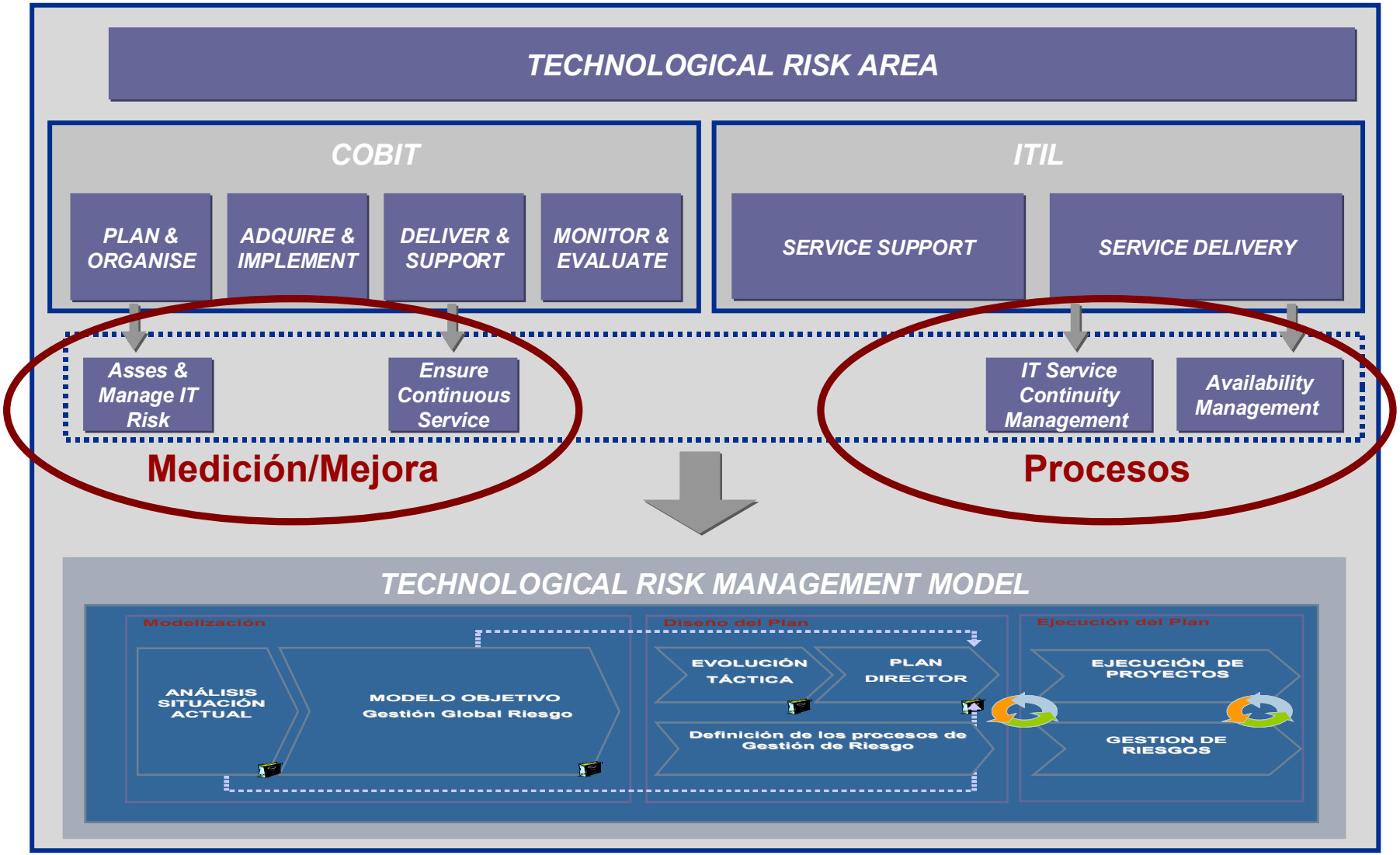
Es necesario que exista una integración a nivel global entre los distintos componentes que conforman el riesgo operacional con el resto de los riesgos asociados a las organizaciones y con los requisitos del negocio.

Para la prestación de servicios de IT se deben integrar los aspectos de Riesgo Operacional/Tecnológico que cumpla con los requisitos de Seguridad, Resilience, Disponibilidad, Eficacia y Rendimiento requeridos.

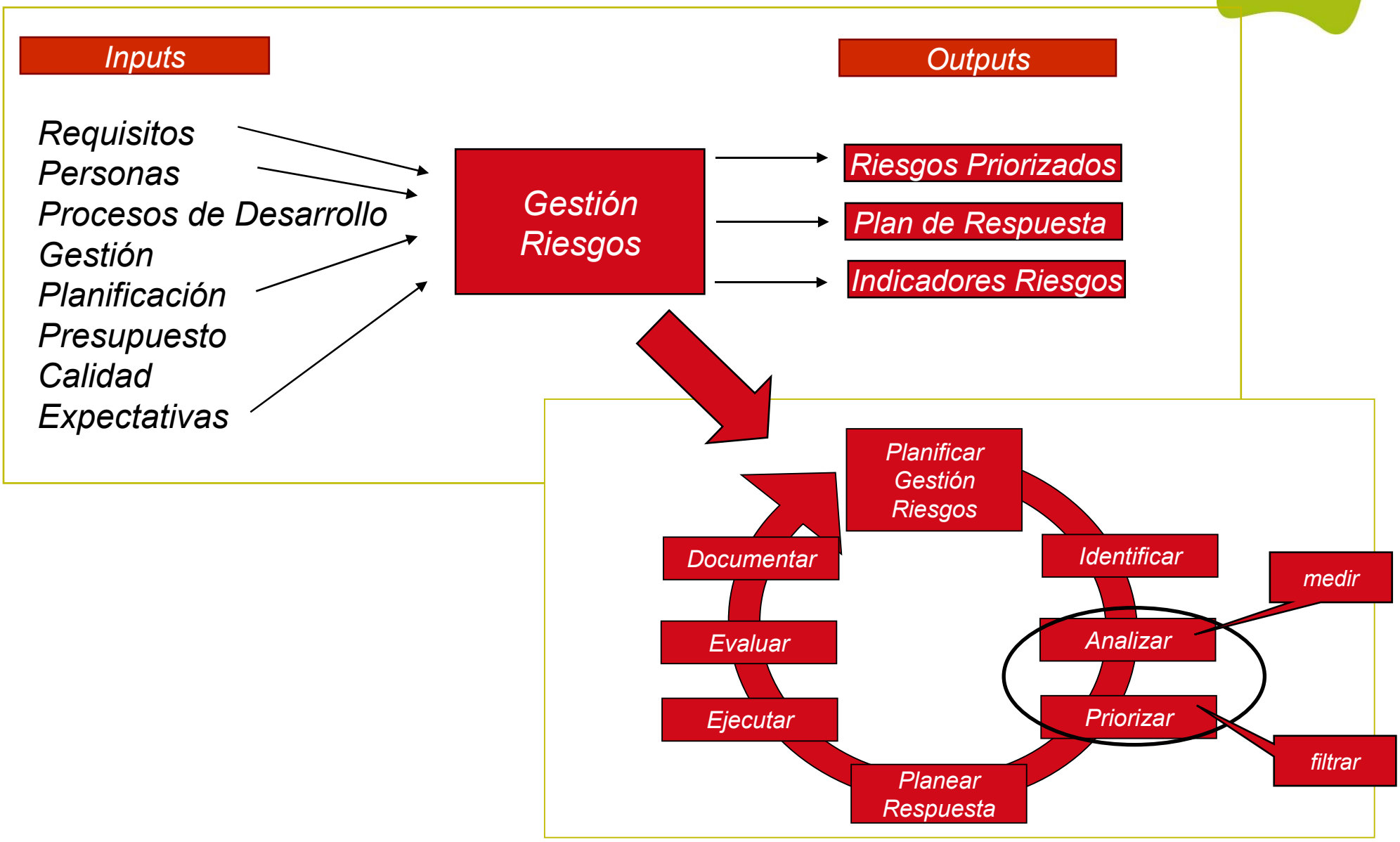
Ejemplo Mercado Financiero

Enfoque: marco metodológico

Enlace entre la organización gestora de riesgos tecnológicos (personas) y el modelo de gestión de riesgos tecnológicos (proceso)



Modelo de Gestión de Riesgos Tecnológicos

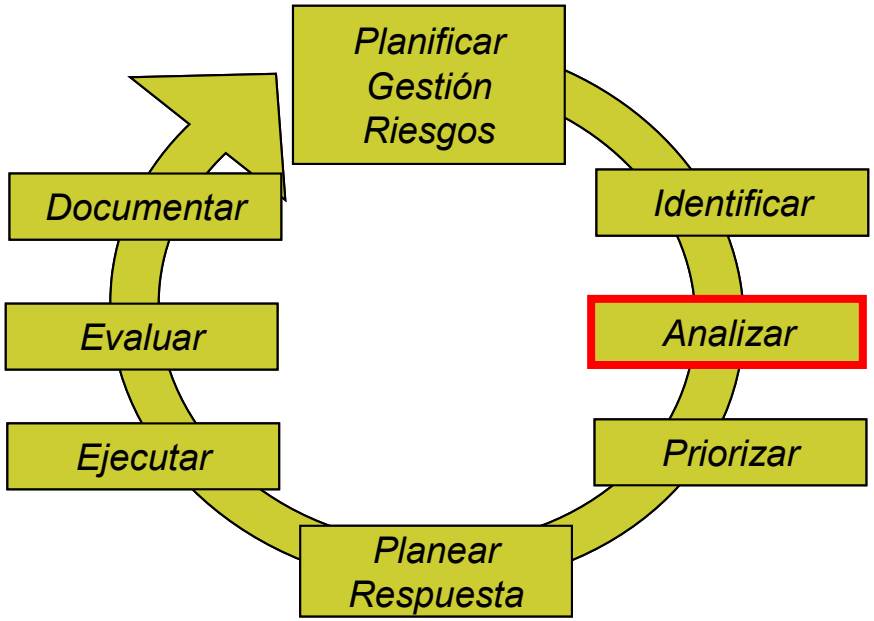


Analizar Riesgos

Análisis de riesgos es:

- El proceso sistemático de estimar la probabilidad de ocurrencia y la magnitud del impacto para cada riesgo

- Un proceso que reduce la incertidumbre al respecto de la ocurrencia de los riesgos contemplados



Ejemplo: Análisis de Valor Esperado

Presupuesto del proyecto A = 5.000.000 €

Lista completa de los riesgos del proyecto A

Riesgo	*Probabilidad*	*x*	*Impacto*	*=*	*Valor esperado*
Los proveedores están de huelga durante el proyecto	*50%*		*+ 500.000 €*		*+ 250.000 €*
El prototipo funciona perfectamente la primera vez	*20%*		*- 200.000 €*		*- 40.000 €*
Tormenta de nieve en marzo	*90%*		*+ 5.000 €*		*+ 4.500 €*

Valor esperado total para los riesgos = 214.500 €

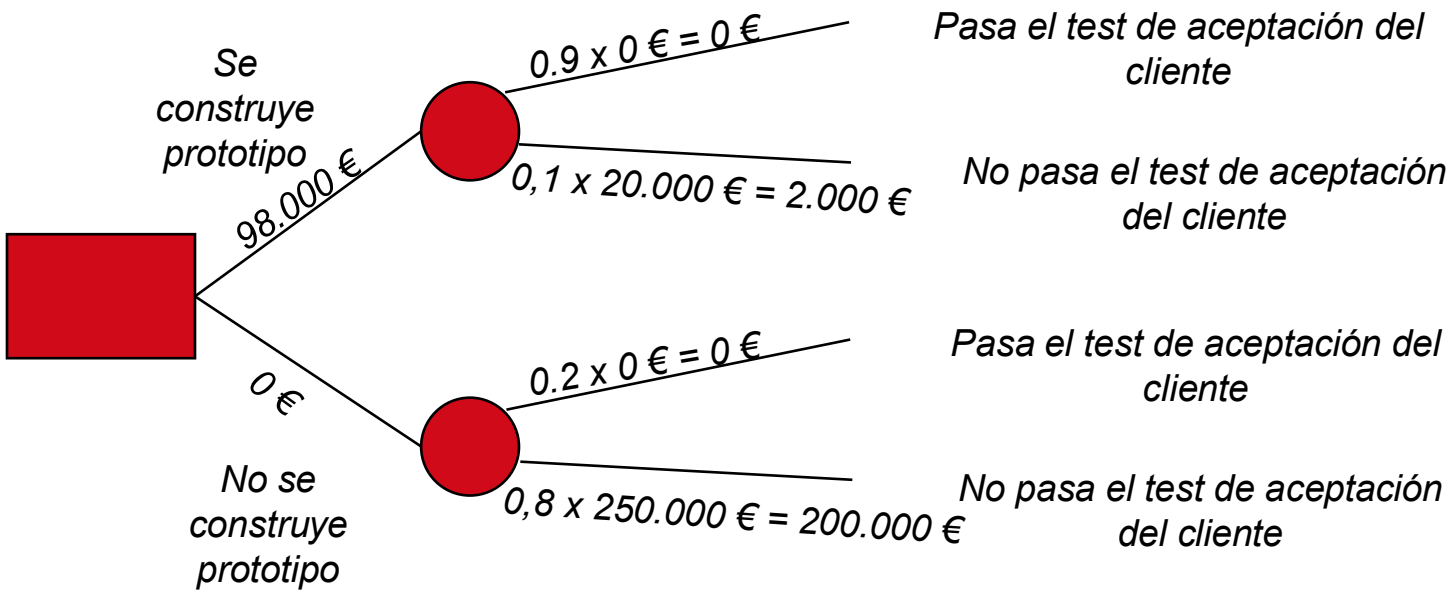
Presupuesto ajustado del proyecto A = 5.214.500 €

Ejemplo: Árbol de Decisión (I)

¿Debemos construir un prototipo del nuevo producto *simulador de vuelo*? Los requerimientos del simulador estuvieron débilmente definidos. Como resultado, existe el riesgo de que el producto final no pasará el test de aceptación del cliente. Un prototipo generalmente reduciría sustancialmente el coste de solucionar las no conformidades del test de aceptación del cliente.

Coste de construir el nuevo prototipo	98.000 €
Probabilidad de pasar el test de aceptación del cliente	
con prototipo	90 %
sin prototipo	20 %
Costes de solucionar las no conformidades del test	
con prototipo	20.000 €
sin prototipo	250.000 €

Ejemplo: Árbol de Decisión (II)



Valor esperado con prototipo:

98.000 € + 2.000 € + 0€ = 100.000 €

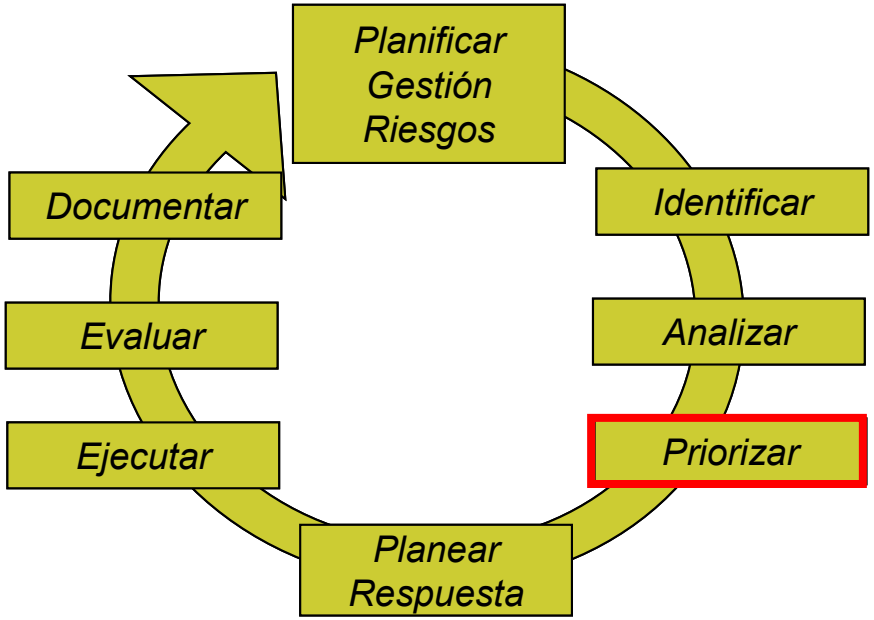
Valor esperado sin prototipo:

0 € + 0 € + 200.000 € = 200.000 €

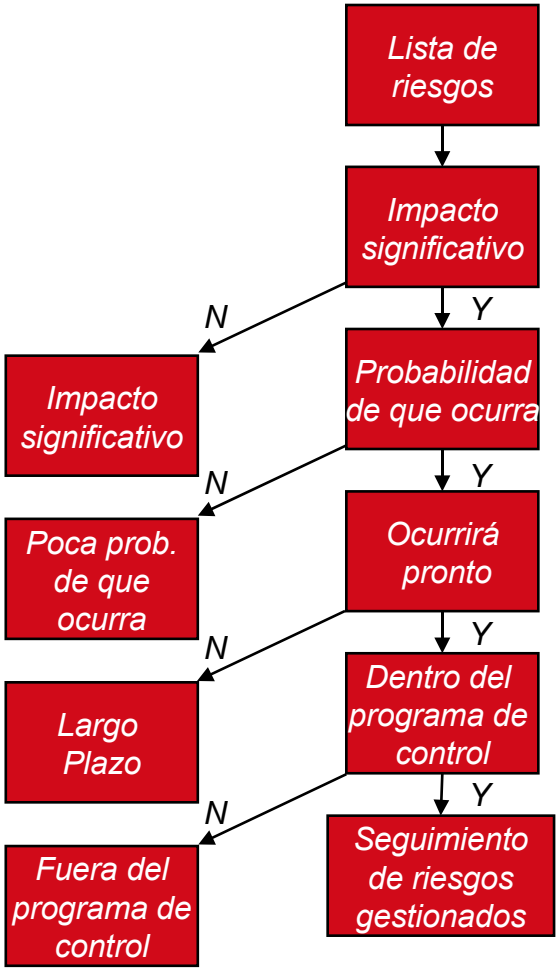
Priorización de Riesgos

- Priorizar riesgos es el proceso de categorizar los riesgos identificados

- Se debe decidir cuáles de los riesgos deben ser atacados, basado en la premisa que nunca habrá tiempo suficiente y recursos para hacer frente a todos los riesgos



Filtrado de Riesgos Gestionados



Filtro 1

¿Algún cliente verá el impacto de este riesgo en términos de funcionamiento, funcionalidad o calidad?

Filtro 2

¿Se ha visto que esto haya pasado alguna vez? ¿Existen condiciones o circunstancias que hagan este riesgo más probable?

Filtro 3

¿Nos afectará pronto? ¿Requiere este riesgo una solución a largo plazo? ¿Debemos actuar pronto?

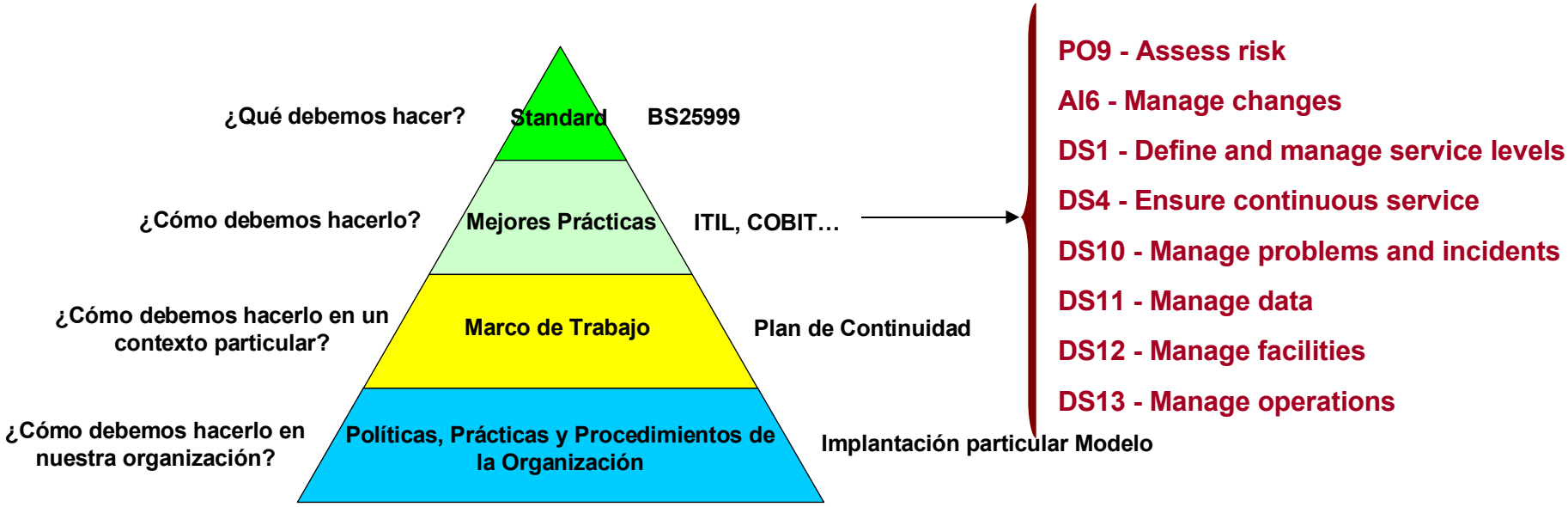
Filtro 4

¿Requiere el riesgo una solución técnica? ¿Requiere el riesgo una acción de gestión del programa de control de riesgos?

Objetivo: la Continuidad del Servicio

El objetivo es definir un conjunto de métricas e indicadores significativos que muestren el estado de los Sistemas de Gestión de la Continuidad del Servicio IT. Estas métricas se han de plasmar en un Cuadro de Mando que permita realizar un seguimiento detallado y continuo.

El modelo de referencia se construye a partir del **COBIT** y la **BS25999**. En concreto, se basa en los 8 procesos indicados por la ISACA que son representativos a la hora de gestionar y auditar los Planes de Continuidad de Negocio de una organización. Esta información es proporcionada por "ISACA- IS AUDITING GUIDELINE- BUSINESS CONTINUITY PLAN (BCP)"



Dimensiones de la Continuidad del Servicio

Dimensiones de Continuidad del Servicio	Descripción de la Dimensión	Ref. Cobit
Dimensión del Marco de Continuidad	Desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización. Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio.	DS4.1 DS4.2
Dimensión de Riesgos	Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación.	DS4.3
Dimensión del Mantenimiento y Distribución	Exhortar a la gerencia de TI a definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua los requerimientos actuales del negocio. Determinar que existe una estrategia de distribución definida y administrada para asegurar que los planes se distribuyan de manera apropiada y asegurar, y que estén disponibles entre las partes involucradas y autorizadas cuando y donde se requiera.	DS4.4 DS4.7
Dimensión de Pruebas y Formación	Probar el plan de continuidad de TI de forma regular para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable. Asegurarse de que todas las partes involucradas reciban sesiones de capacitación de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre.	DS4.5 DS4.6
Dimensión Técnica	Planear las acciones a tomar durante el período en que TI está recuperando y reanudando los servicios. Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio.	DS4.8 DS4.9

Tipos de Métricas de Continuidad

• **Métricas de implementación**: permiten ***medir la implementación*** de la Continuidad del Servicio IT. Esta es la ***primera métrica*** que se debería implementar en una organización. Es importante destacar que para poder llegar a implementar esta métrica la organización ha debido previamente disponer de una política de Continuidad del Servicio IT dirigida y apoyada por la alta gerencia de la organización que marque la estrategia corporativa. Además deberá tener desarrollado los procedimientos (o en fase de construcción) y se estará planteando 'medir' el grado de implantación de dichos controles.

• **Métricas de efectividad/ eficiencia**: ***medir los resultados*** obtenidos por la prestación de servicios de continuidad. Una vez implantado los controles y las métricas de implementación, Produban se puede plantear medir el grado de implantación de los procedimientos.

• **Métricas de impacto**: permite medir el ***impacto operativo o de negocio*** de los eventos de la Continuidad del Servicio IT. Por último la organización debe medir cómo están impactando todos aquellos controles que están ya implementados, y son efectivos y eficientes.

Ejemplo de Métricas de Continuidad

Por ejemplo para la dimensión técnica:

Dimensión Técnica → Planear las acciones a tomar durante el período en que TI está recuperando y reanudando los servicios. Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio.

❑ **Métricas de implementación**:

- ✓Existen roles y personas asignadas nominalmente para la recuperación del servicio IT.
- ✓Existen planes de continuidad de TI. Entendiendo Plan de Continuidad como conjunto de procedimientos exhaustivos para la recuperación de los sistemas.
- ✓Existen centro de respaldo alternativo y distante.

❑ **Métricas de efectividad/ eficiencia**:

- ✓ % de componentes de infraestructura críticos con monitoreo de disponibilidad automatizado.
- ✓ % de SLA de disponibilidad que se cumplen.
- ✓ % de almacenamiento de respaldos críticos y sensitivos fuera de las instalaciones.

❑ **Métricas de impacto**:

- ✓% de servicios críticos del negocio que dependen de TI, cubiertos por un plan de continuidad.
- ✓ # de horas perdidas por usuario por mes debido a interrupciones no planeadas.
- ✓Frecuencia en la interrupción de servicios de sistemas críticos.

Cuadro de Mando: Ejemplo (I)

Introducción de Datos

CUADRO DE MANDO

DS4 - Garantizar la Continuidad del Servicio

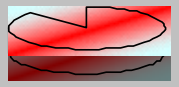
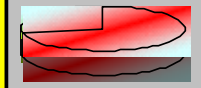
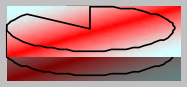
MI - Métricas de Implementación	Seleccione un valor de la lista
Existe un IT Marco de trabajo de continuidad. Es necesario conocer si los planes de continuidad del servicio de las diferentes áreas son consistentes entre sí y existe un marco que englobe todos.	2 - Existen planes locales con coordinación parcial.
Existen planes de continuidad de TI. Entendiendo Plan de Continuidad como conjunto de procedimientos exhaustivos para la recuperación de los servicios.	2 - Existe y está parcialmente documentado.
¿Cómo se recuperan los recursos de TI?. Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación.	3 - Se recuperan los servicios de un modo global.
Existen Políticas, Estándares y Procedimientos.	3 - El proceso es sólido y completo, se aplican las mejores prácticas internas.
Existe alguna herramienta de gestión del Plan de Continuidad del Servicio.	2 - Existe un plan para el uso y estandarización de las herramientas para automatizar el PCN
Existen roles y personas asignadas nominalmente para la recuperación del servicio IT.	3 - Están aceptadas y funcionan de modo que se permite al propietario del proceso descargar sus responsabilidades.
Existen centro de respaldo alternativo y distante	4 - Si y está distante

ME - Métricas de efectividad / eficiencia	Seleccione un valor de la lista
Tiempo transcurrido entre las pruebas de papel del plan de continuidad de TI.	2 - Mas de 1 años.
Tiempo transcurrido entre pruebas funcionales (parciales-servicio) del plan de continuidad de TI.	3 - Cada 1 año.
Tiempo transcurrido entre las pruebas totales (CPD) del plan de continuidad de TI.	3 - Cada 1 año.
Capacitación por año de cada empleado de TI.	2 - El 25% de los empleados han recibido alguna formación
% de componentes de infraestructura críticos con monitoreo de disponibilidad automatizado.	4 - Entre 76% - 100%
Frecuencia de revisión del plan de continuidad de TI.	2 - Se revisa anualmente
% de SLA de disponibilidad que se cumplen.	4 - Entre 76% - 100%
% de almacenamiento de respaldos críticos y sensitivos fuera de las instalaciones	4 - Entre 76% - 100%
# veces activado el Plan	3 - 1 al año

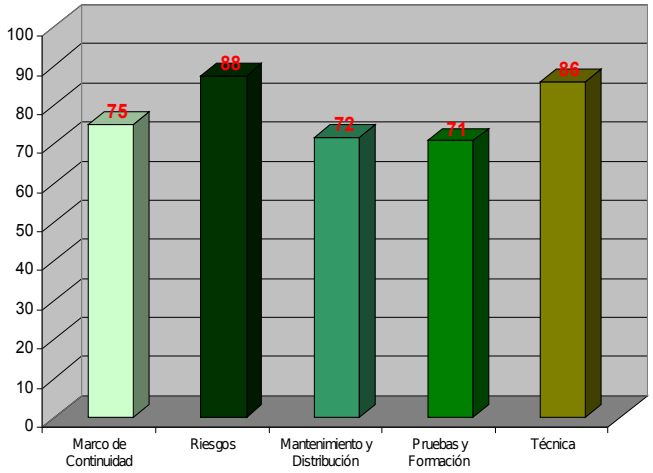
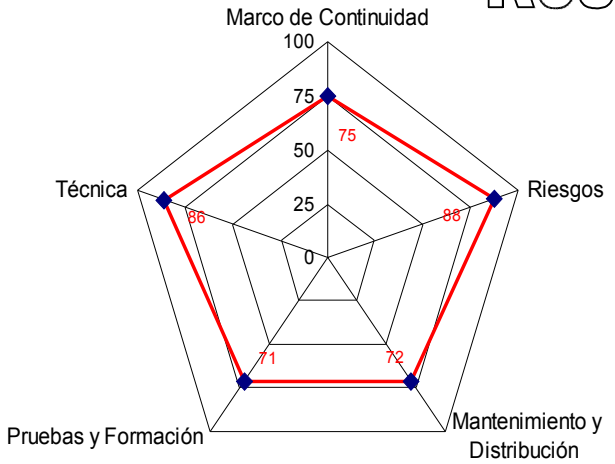
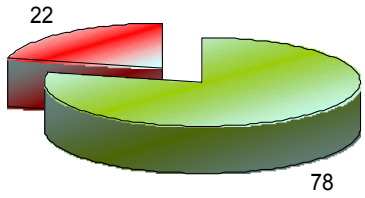
MP - Métricas de Impacto	Seleccione un valor de la lista
% de servicios críticos del negocio que dependen de TI, cubiertos por un plan de continuidad.	4 - Entre 76% - 100%
# de horas perdidas por usuario por mes debido a interrupciones no planeadas.	3 - 2 h./mes
Frecuencia en la interrupción de servicios de sistemas críticos.	3 - Una interrupción al año.

Cuadro de Mando: Ejemplo (II)

PANEL DE CONTROL	Grado de Cumplimiento		Informe Detallado
SERVICIO:	Excelente	100 75	
FECHA:	Bueno	74 51	
COMPLETADO POR:	Bajo	50 0	

Ref. Cobit	Objetivos	Dimensiones de Continuidad del Servicio	% MI	% ME	% MP	Grado Cumplimiento		Descripción
DS4.1 DS4.2	IT Marco de trabajo de continuidad Planes de continuidad de TI	Dimensión del Marco de Continuidad	50	75	100	75		Desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización. Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio.
DS4.3	Recursos críticos de TI	Dimensión de Riesgos	75	100	88	88		Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación.
DS4.4 DS4.7	Mantenimiento del plan de continuidad de TI Distribución del plan de continuidad de TI	Dimensión del Mantenimiento y Distribución	63	65	88	72		Exhortar a la gerencia de TI a definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua los requerimientos actuales del negocio. Determinar que existe una estrategia de distribución definida y administrada para asegurar que los planes se distribuyan de manera apropiada y asegurar, y que estén disponibles entre las partes involucradas y autorizadas cuando y donde se requiera.
DS4.5 DS4.6	Pruebas del plan de continuidad de TI Entrenamiento del plan de continuidad de TI	Dimensión de Pruebas y Formación	75	63	75	71		Probar el plan de continuidad de TI de forma regular para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable. Asegurarse de que todas las partes involucradas reciban sesiones de capacitación de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre.
DS4.8 DS4.9	Recuperación y reanudación de los servicios de TI. Almacenamiento de respaldos fuera de las instalaciones	Dimensión Técnica	75	100	83	86		Planear las acciones a tomar durante el período en que TI está recuperando y reanudando los servicios. Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio.

Cuadro de Mando: Ejemplo (III)

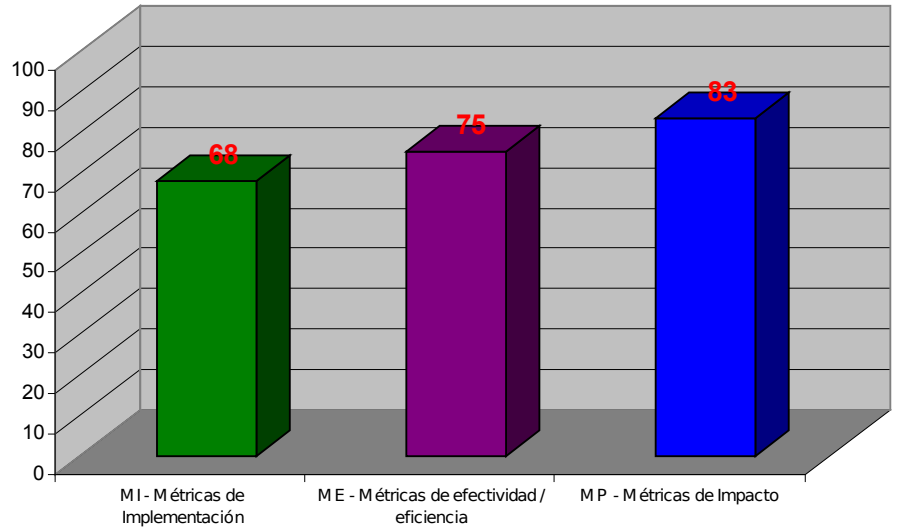
Diagrma de Barras Grado de cumplimiento de los controles de Continuidad del Servicio IT por tipo de Dimensión	Diagrma de Red Grado de cumplimiento de los controles de Continuidad del Servicio IT por tipo de Dimensión	Grado de cumplimiento global
		Resumen Ejecutivo 

Dimensiones de Continuidad del Servicio	Descripción de la Dimensión
Dimensión del Marco de Continuidad	Desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización. Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el
Dimensión de Riesgos	Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación.
Dimensión del Mantenimiento y Distribución	Exhortar a la gerencia de TI a definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua los requerimientos actuales del negocio. Determinar que existe
Dimensión de Pruebas y Formación	Probar el plan de continuidad de TI de forma regular para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable. Asegurarse de que todas las partes involucradas recib
Dimensión Técnica	Planear las acciones a tomar durante el período en que TI está recuperando y reanudando los servicios. Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI

Cuadro de Mando: Ejemplo (IV)

Diagrma de Barras Grado de cumplimiento de los controles de Continuidad del Servicio IT por tipo de Métrica

Resumen Ejecutivo



Tipo de Métrica	Descripción de la Métrica
Implementación	Permiten medir la implementación de la política de la Gestión de la Continuidad del Servicio TI. Esta es la primera métrica que se debería implementar en cualquier organización. Es importante destacar que para poder llegar implementar esta métrica deberá tener desarrollada los procedimientos (o en fase de
Efectividad / Eficiencia	Medir los resultados obtenidos por el delivery de servicios de continuidad. Una vez implantado los controles y las métricas de de implementación, la organización se puede plantear medir el grado de implantación de los procedimientos.
Impacto	Permite medir el impacto operativo o de negocio de los eventos relacionados con la continuidad del servicio IT. Por último Produban debe medir cómo están impactando todos aquellos controles que están ya implementados y son efectivos y eficiente.

attitude makes the difference

Álvaro M. Torres Gallego

Gerente IT Governance

Alvaro.torres.gallego@everis.com

www.everis.com