

GESTIÓN DE LOS RIESGOS TECNOLÓGICOS

Luis Martín Romeral

*Consultor Senior de Gobierno TI, everis,
Paseo de la Castellana 141, 28046 Madrid*
luis.martin.romeral@everis.com

Álvaro Torres Gallego

*Gerente de Gobierno TI, everis,
Paseo de la Castellana 141, 28046 Madrid*
alvaro.torres@everis.com

Resumen

La importancia de una buena gestión de TI es de gran relevancia en el mercado, y cada día más. Un punto de crítica importancia al respecto es la gestión de riesgos tecnológicos, que en una gran medida pueden ser desencadenantes de riesgos operacionales para la empresa.

La gestión de riesgos debe ser considerada como un proceso cíclico que incluye el análisis y la priorización de riesgos. Estas actividades permiten a la organización tener una visión detallada y exacta de los riesgos, y constituyen una buena herramienta de decisión acerca de qué riesgos pueden ser gestionados en un entorno de recursos limitados (el habitual).

El principal objetivo es asegurar la continuidad del negocio. Para conseguirlo es necesario establecer un Proceso de Continuidad de los Sistemas, que nos proporcione métricas relevantes. Estas métricas deben servir de base para obtener informes y un Cuadro de Mando ejecutivo, los cuales facilitarán la toma de buenas decisiones de gestión.

Palabras Clave: Gobierno TI, Riesgo, Continuidad, Resiliencia.

Abstract

The importance of good management of IT is already high in the market, and its increasing day by day. One of the main concerns regarding IT management is the management of technology risks that trigger operational risks for the company.

Risk management should be considered as a never ending cycle, comprising analysis and prioritizing risk. Those activities allow the organization to have an accurate view of risks and an informed way to decide about what can be covered in a limited resources environment (usual situation).

The main objective is the assurance of business continuity. To achieve this it is necessary to establish a Systems Continuity Process, providing relevant metrics. These metrics should be a starting point to feed a set of reports and an executive Scorecard, giving the basis for good management decisions.

Key Words: IT Governance, Risk, Continuity, Resilience.

1. INTRODUCCIÓN

Todas las organizaciones están sufriendo cambios continuamente: nuevos requisitos, cambios en el entorno, cambios regulatorios, adquisiciones... Cuanto mayor es una empresa, mayor es el número de cambios que sufre. Así mismo, cada cambio que se produce lleva asociados una serie de riesgos que pueden derivar en resultados desde lo inocuo hasta lo desastroso. Esto ha hecho que las empresas traten de conseguir el mayor grado de resiliencia posible, es decir que sean capaces de absorber las

perturbaciones sin alterar significativamente sus características de estructura y funcionalidad, pudiendo regresar a su estado original una vez que la perturbación ha terminado.

Por desgracia no basta con conocer los riesgos a los que se enfrentan las empresas, las cosas pasan. Alguna de esas amenazas potenciales puede efectivamente tener lugar. Hay que estar preparado y disponer de planes de acción en caso de que se cumpla alguno de los riesgos identificados. La

situación se agrava cuando se pone en peligro la continuidad del negocio como consecuencia de la ocurrencia de un riesgo. Por tanto, hoy día se hace indispensable disponer de un plan de continuidad de negocio de modo que se obtenga el nivel de resiliencia deseado. Además es conveniente realizar un seguimiento del plan de modo que se tenga una visión clara de su eficacia, así como de sus puntos débiles, para poder mejorarlo de forma continua.

La Gestión de Riesgos y de la Continuidad de Servicios basados en Tecnología de la Información es de vital importancia, recogiéndose incluso en regulaciones como Sarbanes-Oxley, lo que nos obliga a adoptar una serie de principios para la gestión del Riesgo Tecnológico:

- Gestión permanente, sistemática y continua de los riesgos.
- Existencia de planes de contingencia.
- Supervisión periódica e independiente.
- Evaluación del riesgo para todo nuevo sistema o proceso.

A continuación se describirá el ciclo básico de la gestión de riesgos, así como un modelo propuesto para la gestión de la continuidad y una serie de posibles indicadores que nos ayuden a medir tanto el grado de cumplimiento como lo exitoso de nuestro sistema.

2. CICLO DE GESTIÓN DE RIESGOS

La Gestión de Riesgos consiste en un proceso cíclico que se inicia a partir de un conjunto de información recogida de diversas fuentes (requisitos, personas, procesos de desarrollo, presupuestos, expectativas...). Toda esta información proporciona una lista de riesgos a tener en cuenta. El proceso de Gestión de Riesgos los analiza, prioriza y plantea planes de respuesta, dando como resultado el conjunto de riesgos priorizados, los planes de respuesta a dichos riesgos y un conjunto de indicadores que se utilizarán para medir el éxito del proceso, y en su caso, mejorarlo.

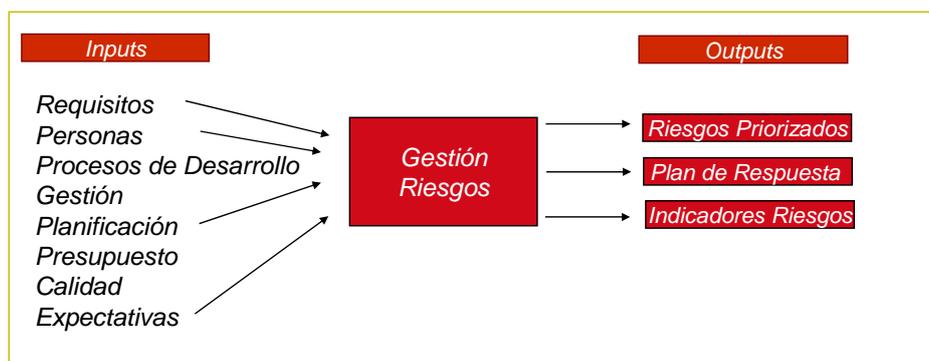


Figura 1. Gestión de Riesgos: entradas y salidas

Análisis de riesgos

Dentro del ciclo de Gestión de Riesgos tecnológicos, el análisis de riesgos consiste en un proceso sistemático para estimar la probabilidad de ocurrencia y la magnitud del

impacto de cada riesgo identificado. Para llevar a cabo este proceso es necesario partir de una lista de riesgos identificados que conviene que estén categorizados de modo que resulte más sencillo su tratamiento. Además, para disponer de una mayor criterio

a la hora de realizar el análisis, se contará con las lecciones aprendidas de que se disponga (la experiencia en análisis de riesgos resulta fundamental), estimación de costes y planificaciones.

A partir de toda esta información, se decidirá si es más conveniente utilizar una aproximación cuantitativa o cualitativa, y en base a la decisión tomada, se utilizarán herramientas tanto para evaluar las

probabilidades de ocurrencia, como el impacto que tendría la ocurrencia. De este modo se obtendría el listado de los riesgos analizados.

Para llevar a cabo este proceso se pueden utilizar diversas herramientas o mecanismos. En las siguientes figuras se ilustra un ejemplo que combina los métodos de árbol de decisión y cálculo de valor esperado.

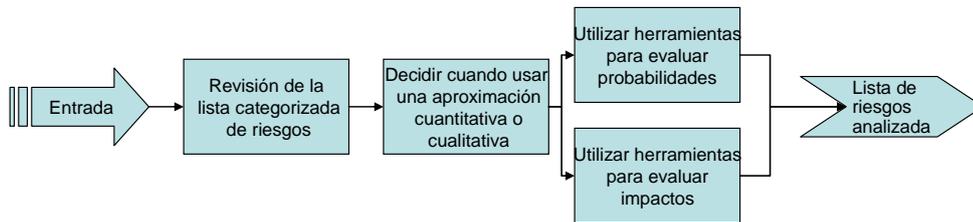


Figura 2. Proceso de análisis de riesgos

¿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 €

Figura 3. Planteamiento de caso práctico

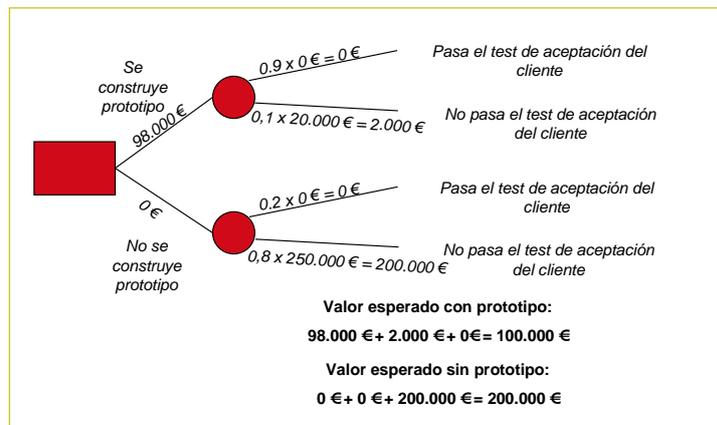


Figura 4. Árbol de decisión y valor esperado

Priorizar

El siguiente paso del ciclo consiste en priorizar los riesgos, es decir, categorizar los riesgos identificados. Se debe decidir cuales de los riesgos deben ser abordados, basado en la premisa que nunca habrá tiempo suficiente y recursos para hacer frente a todos los riesgos.

A partir de la lista de riesgos analizados y una estructura de priorización, se decide el

método que se aplicará a la hora de priorizar. Aplicando el método decidido, se priorizarán tanto oportunidades para el negocio, como los riesgos, dando como resultado un listado de oportunidades priorizadas y un listado de riesgos priorizados.

Entre otros mecanismos podemos utilizar la técnica de filtrado, como se ilustra en la figura 6.

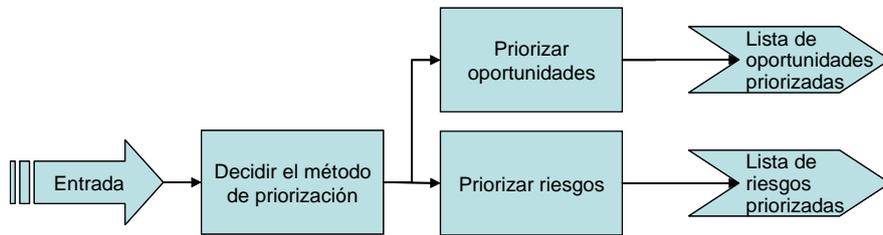


Figura 5. Proceso de priorización

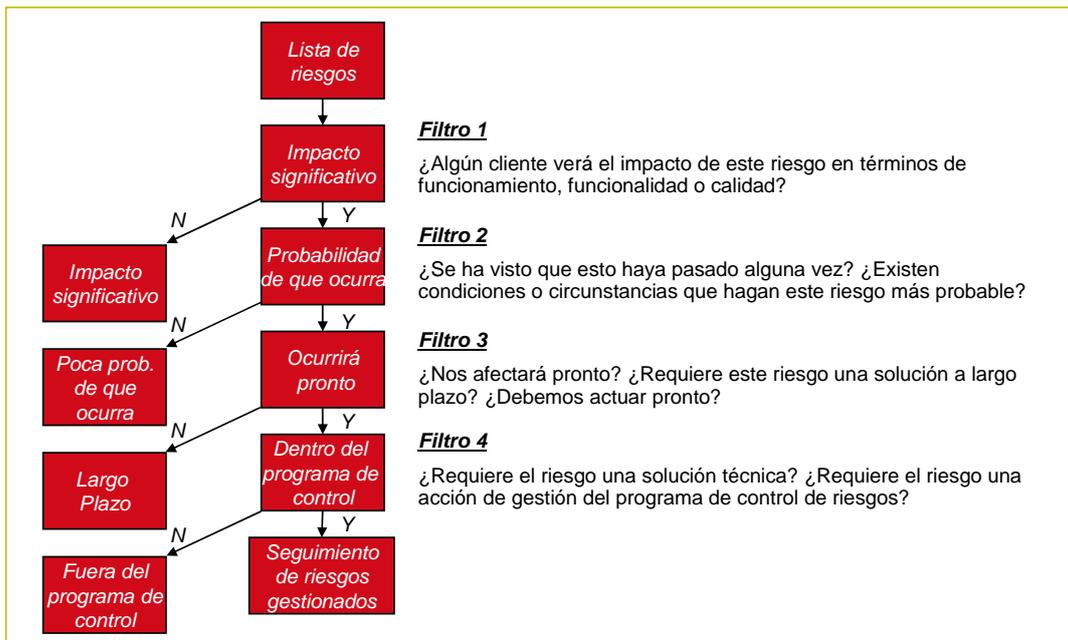


Figura 6. Filtrado de riesgos

3. LA CONTINUIDAD DEL NEGOCIO

Durante mucho tiempo el planteamiento de las empresas frente a los riesgos consistía en disponer del mejor proceso de gestión de riesgos posible. Sin embargo, con el tiempo este enfoque se ha revelado insuficiente. Esto se debe a que la preocupación del estamento directivo de la empresa, así como la de sus propietarios/accionistas, no está en que un servidor se haya caído o que la luz se haya ido o incluso que haya un terremoto... El foco de la atención está en cómo afectan estos acontecimientos a su negocio y en cuanto tiempo su negocio volverá a funcionar. La máxima es “si el negocio se para, se deja de ingresar”. Con esta máxima presente resulta imprescindible para cualquier empresa disponer de:

- Un plan de continuidad de servicio
- Un departamento/infraestructura de TI con el máximo nivel de resiliencia

En cuanto al plan de continuidad de servicio, a continuación se describen los elementos que deben componerlo:

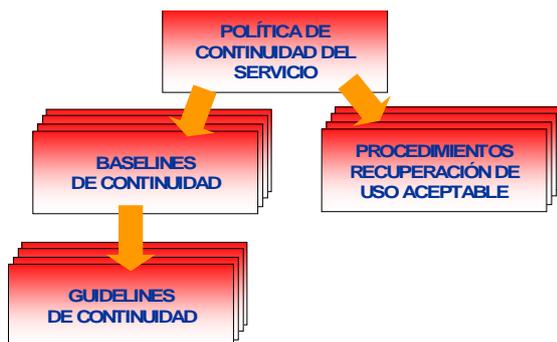


Figura 7. Plan de continuidad de servicio

Política de Continuidad del Servicio

A la hora de establecer una Política de Continuidad del Servicio es necesario hacer una aproximación de alto nivel al problema

y definir los grandes pasos que dicha política debe incluir:

- Identificación de los bienes que se desea proteger
- Determinación de quién amenaza nuestra seguridad
- Determinación de cómo se amenaza nuestra seguridad
- Implementación de medidas enfocadas a proteger los bienes de las amenazas de forma rentable
- Recursos que se van a dedicar a lograr los objetivos de seguridad
- Asignación de responsabilidades
- Revisión continua del proceso y cada vez que es detectada una debilidad en el mismo

Las características que debe cumplir una buena política son:

- Razonable y Aplicable
- Auditable
- Comprensible
- Sin contenido Técnico
- Aprobado por la alta dirección

Baselines de Continuidad

Una vez definida y aprobada la Política de Continuidad del Servicio, es necesario definir a alto nivel y de un modo global el conjunto de estándares mínimos para las especificaciones de Continuidad del Servicio para todos los departamentos/áreas. Estos estándares son los aspectos más relevantes para la Continuidad del Servicio y pueden verse como el conjunto de reglas básicas que deben ser implantadas. Dependiendo del área de implantación algunas tendrán carácter obligatorio mientras otras serán optativas.

Las baselines (o líneas base) están compuestas por un conjunto de normas y

procedimientos que detallan las diversas fases de la contingencia y el personal que debe restablecer el servicio tecnológico, con un procedimiento de respuesta ante emergencias específico diseñado para ello.

Las características que deben cumplir las Baselines son:

- Globales y no particularizables
- Aplicable
- Auditable
- Sin contenido técnico

Procedimientos de Recuperación de uso aceptable

En paralelo a las Líneas Base de Continuidad es recomendable establecer los procedimientos de recuperación de los diferentes sistemas. Estos procedimientos no constituyen el detalle de cómo se debe recuperar cada sistema en particular, lo que debe ser particularizado para cada sistema en función de los servicios que soporte. Sin embargo, sí establece las mejores prácticas y una guía de cómo se debe recuperar cada sistema.

Estos procedimientos están compuestos por un conjunto de documentos (procedimientos) operativos genéricos, que detallan las actividades a realizar para la recuperación del sistema en función de sus características. Así se detallan los procedimientos a seguir para la recuperación del entorno especificado, ya sean comunicaciones, sistemas medios o de mainframe.

Para el caso de que se disponga de un centro alternativo (lo más recomendable), en estos procedimientos se describirá la secuencia de acciones a realizar en el centro alternativo para recuperar el servicio en el caso de que se haya producido la pérdida total o parcial del mismo en el centro principal.

Las características que deben cumplir los Procedimientos son:

- Fundamentalmente técnicos
- Particularizables

Guidelines de Continuidad

Por último las Guidelines o Guías de Continuidad proporcionan los documentos suplementarios y plantillas de las Líneas Base de Continuidad. Estas Guías proporcionan el detalle particularizado para cada área/departamento sobre cómo recuperar el servicio IT.

Han de contemplar la plantilla del Plan de Contingencia donde se hace referencia a toda la documentación de los pilares de Gestión de Continuidad del Servicio IT. Deben contener las plantillas a completar ante cualquier simulacro de contingencia o prueba de mantenimiento, así como las distintas plantillas a completar para disponer de los contactos (internos/externos) ante una contingencia.

Las principales guías son:

- Descripción de Pruebas de Contingencia
- Pruebas de Contingencia
- Simulacro de Emergencias
- Plan de Contingencia
- Plantillas del Plan de Pruebas
- Plantillas de Contactos.
- Plantillas de Organización ante Contingencia

Las características que deben cumplir las Guidelines son:

- Plantillas de uso
- 100% particularizadas

4. MEDICIÓN DE LA CONTINUIDAD

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 verán plasmadas en un Cuadro de Mando que permita realizar un seguimiento detallado y continuo.



Figura 8. Elementos del Plan de Continuidad de Servicio

Una vez lanzadas las iniciativas orientadas a obtener un programa de continuidad del servicio IT, cumplimiento normativo y gestión de riesgos, se plantea la necesidad de ‘medir’ el grado de cumplimiento y eficacia de las iniciativas llevadas a cabo. De este modo se revela crítico proceder a la definición de métricas y del Cuadro de Mando, fundamentalmente orientados a medir la Continuidad del Servicio TI y la resiliencia.

El programa de definición e implantación de métricas busca proveer de los siguientes beneficios:

- Facilitar la toma de decisiones.
- Permitir mejorar en las responsabilidades (accountability), mostrando de forma precisa los controles técnicos, operativos o administrativos no implantados o implementados incorrectamente.

- Usar el resultado del análisis de métricas con los responsables de programas y de sistemas para aislar problemas, justificar peticiones de presupuesto en base a evidencia cuantitativa y orientar recursos especialmente en las áreas que necesitan mejorar.

Tipos de Indicadores

De acuerdo al nivel de madurez de la compañía en aspectos relativos a la Continuidad del Servicio TI, nos centraremos los siguientes tipos de métricas:

- Métricas de implementación: permiten medir la implementación de la Continuidad del Servicio TI. 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 TI dirigida y apoyada por la alta gerencia de la organización que marque la estrategia corporativa. Además deberá tener desarrollados los procedimientos (o en fase de construcción) y se estará planteando ‘medir’ el grado de implantación de dichos controles.
- Métricas de efectividad/eficiencia: permiten medir los resultados obtenidos por el desarrollo de servicios de continuidad. Una vez implantado los controles y las métricas de implementación, se puede plantear medir el grado de implantación de los procedimientos.
- Métricas de impacto: permiten medir el impacto operativo o de negocio de los eventos de la Continuidad del Servicio TI. La organización debe medir cómo están impactando todos

aquellos controles que están ya implementados, y son efectivos y eficientes.

¿Cómo definir las Métricas?

A la hora de definir indicadores, una primera aproximación, posiblemente la más cómoda, consiste en recurrir a los indicadores ya definidos por ISACA ("ISACA- IS AUDITING GUIDELINE- BUSINESS

CONTINUITY PLAN (BCP)"). Así, si tomamos como modelo de referencia COBIT podemos obtener los 8 procesos indicados que son representativos a la hora de gestionar y auditar los BCP de una organización.

El siguiente diagrama muestra un ejemplo de cómo definir las métricas a utilizar:

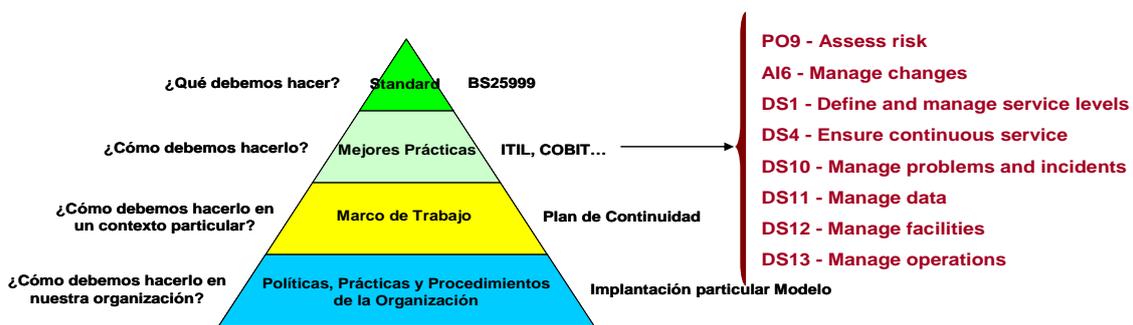


Figura 9. Definición de métricas

4.3 Pilares de las Métricas

Las métricas están sustentadas en cuatro pilares fundamentalmente:

- **Procesos Corporativos:** es necesario conocer cómo se están implementando los diferentes procedimientos de gestión de los sistemas.
- **Operaciones:** es necesario conocer cómo se están operando los sistemas basándose en los procesos definidos.
- **Tecnología:** es necesario conocer cómo la Tecnología está soportando la continuidad del servicio y el nivel de resiliencia deseado.
- **Auditoría:** es necesario medir cómo la evaluación continua de los controles (auditorías periódicas) proporciona mejoras en los sistemas.

5. CONCLUSIONES

En el entorno competitivo actual, desde hace ya algunos años, la mera posesión de tecnología no supone por sí misma una ventaja competitiva para las empresas. Es la gestión de esa tecnología la que puede ser diferencial, con especial énfasis en la gestión de los riesgos derivados del uso de Tecnología de la Información. Estos riesgos constituyen una parte importante, y cada vez más, del riesgo operativo (el derivado de simplemente existir y operar como empresa) ya que la simbiosis entre las operaciones de las empresas y el uso de TI es cada vez más intensa.

En ese sentido, existen técnicas maduras de gestión de riesgos que nos pueden servir de ayuda a la hora de identificarlos, de analizarlos y de priorizarlos. Es decir,

“separar el trigo de la paja” ya que en un entorno de recursos limitados no podemos abarcarlo todo.

El objetivo final no es la gestión del riesgo en sí misma sino lograr un alto grado de continuidad del negocio y de resistencia ante cambios o eventualidades (la citada resiliencia). Para lograr ese objetivo, además de ponernos en camino, debemos ser capaces de controlar que el camino que recorremos es el adecuado. Nuestra brújula en ese camino serán unas métricas adecuadas de Continuidad del Servicio, convenientemente

explotadas en informes y Cuadros de Mando ya que el objetivo de medir no es meramente medir sino tomar buenas decisiones apoyadas en datos fiables y relevantes.

6. REFERENCIAS

- [1] Information Systems Audit and Control Association, IS Auditing Guideline Business Continuity Plan (BCP)
- [2] IT Governance Institute, COBIT 4.1

Llamada a la participación Revista Procesos y Métricas

Uno de los principales objetivos de esta revista es que aquellas entidades y organizaciones interesadas **participen** en ella. Y por ello le instamos tanto a usted como a su institución para que realicen contribuciones, o envíen sus comentarios y sugerencias. Actualmente estamos abiertos a la recepción de trabajos para el próximo número que cubra los siguientes tópicos:

- Artículos académicos.
- Casos prácticos o casos de éxito (success histories) de aplicación de métricas y procesos de tecnologías de la información en organizaciones
- Artículos de difusión que traten conceptos teóricos, básicos, novedosos, etc... explicados de forma amena, o que traten aspectos relacionados con la difusión y empleo de ciertas técnicas, métricas o procesos.
- Información sobre noticias, eventos, etc...

La revista se edita en formato electrónico y papel (ambas con ISSN propio), y es accesible a través de su web: <http://www.aemes.fi.upm.es/rpm/rpm.php>. Consulte la 'Guía para Autores' publicada en este número o visite la web para más información sobre el formato de las contribuciones.

Esperamos sus contribuciones en: rpm@aemes.org