tecnim@p Sevilla 2006
30 mayo a 2 junio
060.es
24x7x365

Comunicación

415

MAGERIT Y LA NORMALIZACIÓN DE OTROS MODELOS DE GESTIÓN DE RIESGOS

Comunicación a completar tras las 24.00 horas del 13.3.2006.

Julián Marcelo Cocho
Dr. Ingeniero en Informática
Subdirector de Investigación del Departamento de Organización de Empresas, Economía Financiera y Contabilidad
Investigador del grupo ITIO
Universidad Politécnica de Valencia – UPV
Camino de Vera E-46022 Valencia, España
+34 96 387 76 80
jmarcelo@omp.upv.es

Julián Marcelo Cocho

1. Abstract

El Riesgo, concepto científico y utilitario ampliamente empleado desde el Renacimiento, ha adquirido una importancia creciente en una sociedad que ha de tratar extensas zonas de incertidumbre creciente con una 'cultura del riesgo' ampliamente renovada. El análisis de las convergencias de los conceptos de riesgo en múltiples sectores, incluyendo los financieros, sanitarios, técnicos o laborales, conducen a un **MGGR**, **M**odelo **G**eneral de **G**estión de **R**iesgos de todo tipo.

Este **MGGR** está en la base de la constitución en ISO de **ISO/TMB/WG**, un nuevo Grupo Especial de Trabajo especial sobre **"Risk management"**, representado en España por el Grupo AEN/GET 13 de AENOR. ISO elabora con urgencia la nueva Norma Internacional **"General Guidelines for Principles and Implementation of Risk Management"** a propuesta de Japón, Australia y Nueva Zelanda. Esta norma presenta un modelo de fondo que permite abarcar y recoger Métodos españoles de Análisis y Gestión de Riesgos en varios sectores

2. Comunicación

2.1. Hacia una 'cultura' común del riesgo

"En el actual contexto socio-económico globalizado es cada vez más fundamental que las organizaciones –sean empresas, administraciones públicas, asociaciones emprendedoras, organizaciones no-gubernamentales- puedan ejecutar procesos directivos que respondan al cambio e incertidumbre de los escenarios, a la creciente exigencia de transparencia y conocimiento de la opinión pública y de las partes interesadas, a los principios de sostenibilidad y responsabilidad social; procesos que, después de todo, buscan garantizar la existencia y el éxito de las propias organizaciones. El conjunto de las técnicas y de las metodologías dirigidas a lo que podría definir como "gestión de los procesos de la empresa" es sin duda tan complejo como articulado, también al nivel normativo, debido también a la conocida transversalidad que afecta a menudo a los dominios de conocimiento implicados en aquélla. En cualquier caso, nunca como hoy se percibe la exigencia de una mayor responsabilidad sobre los riesgos que afectan a las diversas actividades humanas. Se va consolidando una auténtica ***'cultura del riesgo'*** *basada, a su vez, en una metodología sistemática y formalizada, la llamada* ***'gestión del riesgo'*** *capaz de caracterizar el contexto, de estimar –o sea analizar y evaluar- tratar, monitorizar y comunicar los riesgos." [4]*

Así explicaba la UNI, Asociación de Normalización Italiana federada a ISO, su implicación en octubre de 2005 en la vasta operación de unificación de los diversos conceptos y modelos de Gestión del Riesgo que a principios de 2005 habían emprendido en nuestras antípodas las asociaciones australiana y japonesa federadas a ISO. En España AENOR, la Asociación Española de Normalización y Certificación, se sumaba pocos días después a un movimiento internacional que busca reorienta los dispersos procesos de unas complejas sociedades marcadas por la incertidumbre hacia el estudio y dominio comunes de la búsqueda de limitación a unas consecuencias negativas cada vez más frecuentes. El BOE de 14 de diciembre de 2005 publicó la "RESOLUCIÓN de 8 de noviembre de 2005, de la Dirección General de Desarrollo Industrial, por la que se autoriza a la Asociación Española de Normalización y Certificación, para asumir funciones de normalización en el ámbito de la gestión de riesgos.", y el 8 de enero de 2006 se celebró la reunión de constitución del GET 13. Este Grupo Especial Temporal *"cuenta con miembros procedentes de muy diversos sectores de actividad (construcción, transporte, salud, alimentación, riesgos laborales, tecnología, medio ambiente, prevención de accidentes, industria aeroespacial, líneas aéreas, tecnología de la información ...) tanto de la Universidad, como de la Administración Pública y del Sector Privado. El debate en el GET 13 se orientó a conseguir una 'comprensión común' por miembros de ámbitos sectoriales y de actuación muy diferentes en cuanto al ámbito temático en el cual se trabaja" [5].*

Dentro de AENOR, el Subcomité SC27 del Comité Técnico CT71 sobre Seguridad de los Sistemas de Información tiene un papel relevante, ya que había recibido directamente como tarea internacional el borrador

de la nueva norma y se había adelantado a enviar los comentarios solicitados al documento de ISO/TMB N11 "Text for 1st Working Draft -Risk Management- Guidelines for Principles and implementation of Risk management". El GET 13 de AENOR adoptó prácticamente los comentarios del SC27 con algunas adiciones y así lo envió a ISO, además de elegir en esta primera sesión como Presidente a Miguel Angel Amutio del Ministerio de Administraciones Públicas, responsable de MAGERIT versión 2 y representante elegido por el SC27 citado.

2. Contenido de la norma ISO/TMB N11

Además de las tradicionales introducciones de toda norma internacional, el borrador de la norma ISO/TMB N11 (en adelante N11) contiene actualmente 7 grandes bloques:

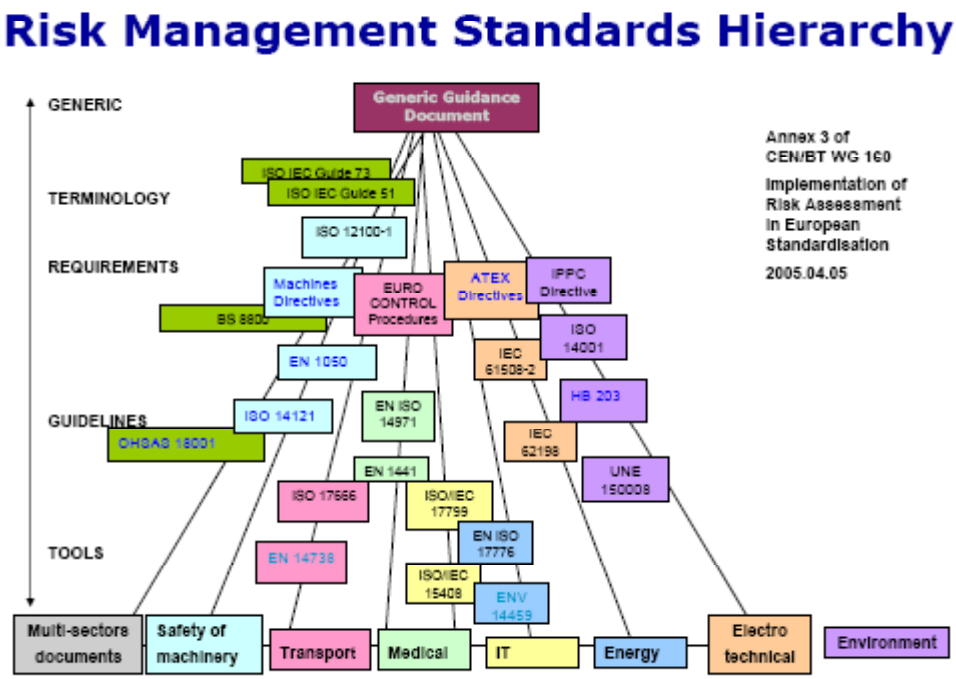
- El bloque 1 trata su Alcance
- El sucinto bloque 2 recoge otras normas anteriores que le sirven de referencia
- El amplio bloque 3 unifica y clarifica una treintena de términos, completando sus definiciones
- El bloque 4 plantea los principios de una "Buena Gestión de Riesgos"
- El sucinto bloque 5 plantea el Contexto Organizacional para la Gestión de Riesgos
- El amplísimo bloque 6 ocupa media norma con el Proceso de Gestión de Riesgos propuesto
- El corto bloque 7 aconseja la Implantación de una Gestión de Riesgos integrada en las estructuras existentes.

El Modelo General de Gestión de Riesgos que subyace a la Norma se articula en torno a su Alcance, a la definición de sus Conceptos básicos y al Proceso de etapas y actividades que permiten aplicarla en las organizaciones.

3. Alcance de la Norma

La N11 *"proporciona el concepto, la pauta y el establecimiento de un proceso iterativo genérico para la gestión del riesgo en toda organización de cualquier tamaño... Quiere también proporcionar un documento de alto nivel para dar soporte a los estándares existentes que tratan aplicaciones específicas de riesgos; y no debe verse como substituto de los estándares internacionales sobre gestión de riesgos que se han establecido y utilizado satisfactoriamente en sectores específicos. También busca apoyar a los desarrolladores de estándares para armonizar las definiciones y los procesos de gestión de riesgos en los estándares actuales y futuros ... Puede aplicarse a una gama muy amplia de las actividades, decisiones y operaciones de cualquier entidad pública, privada o comunitaria, en grupo o individualmente... No se piensa su utilización para propósitos de certificación o contractuales".*

Este amplísimo alcance, pese a las limitaciones auto-impuestas de no sustituir normas existentes y de no emplearse para certificación de la situación de las organizaciones en materia de gestión de riesgos adecuada, puede colegirse en la siguiente jerarquía de Estándares puesta como ejemplo en la propia norma [5]:



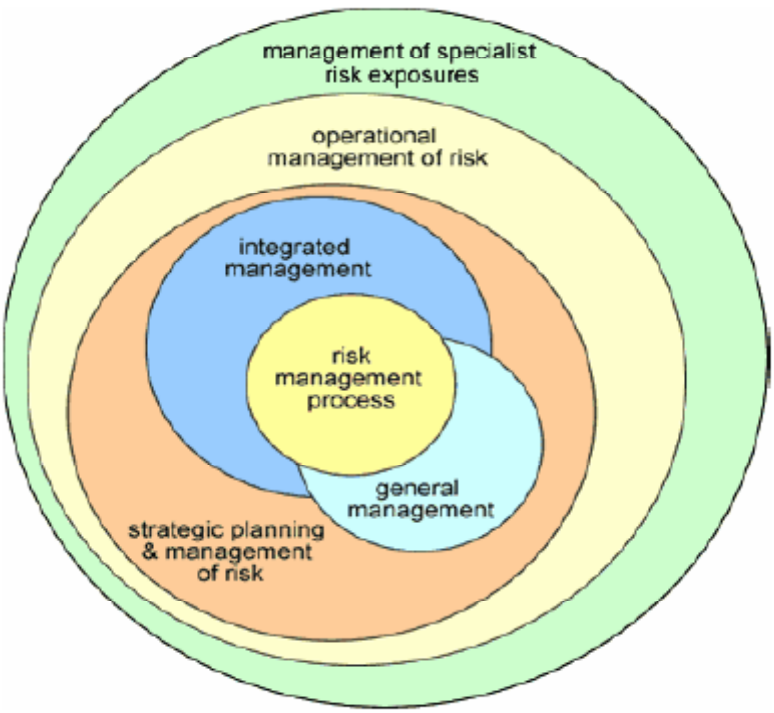
4. Unificar, clarificar y definir conceptos

La N11 ha adoptado un elenco de una treintena de conceptos y definiciones tomados de las normas vigentes. Se propone así facilitar la comunicación entre éstas y la nueva, sin dejar de buscar una mejor precisión en dicha comunicación, sobre todo en los conceptos actuales más ambiguos, como los relacionados con la posibilidad del propio riesgo.

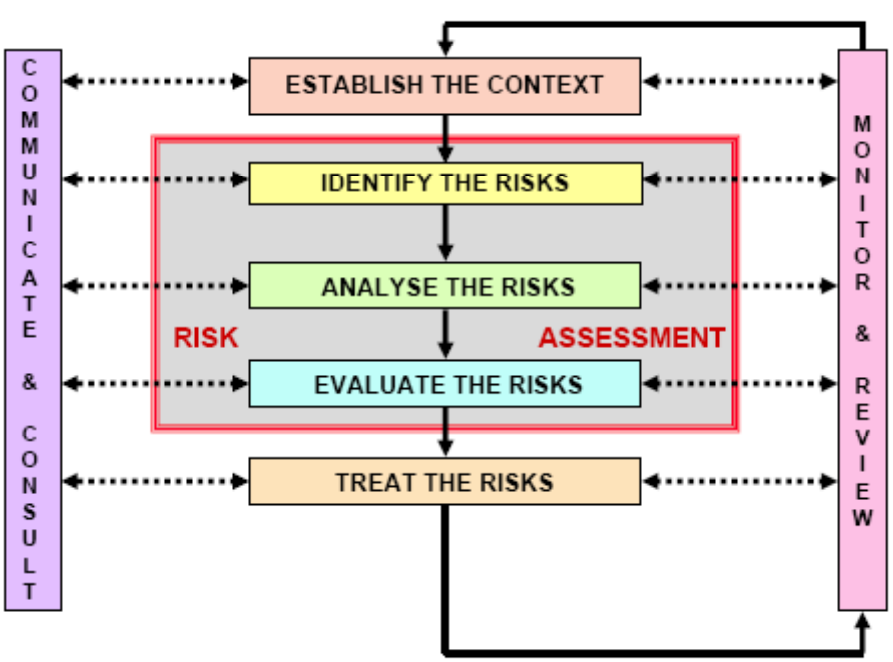
Retomando la terminología y definiciones que utiliza MAGERIT en su Submodelo de Entidades, puede observarse una amplísima semejanza que va a necesitar sólo muy ligeras adaptaciones, debidas a la ampliación sobre todo del alcance de la nueva norma a campos más amplios al de los Sistemas de información.

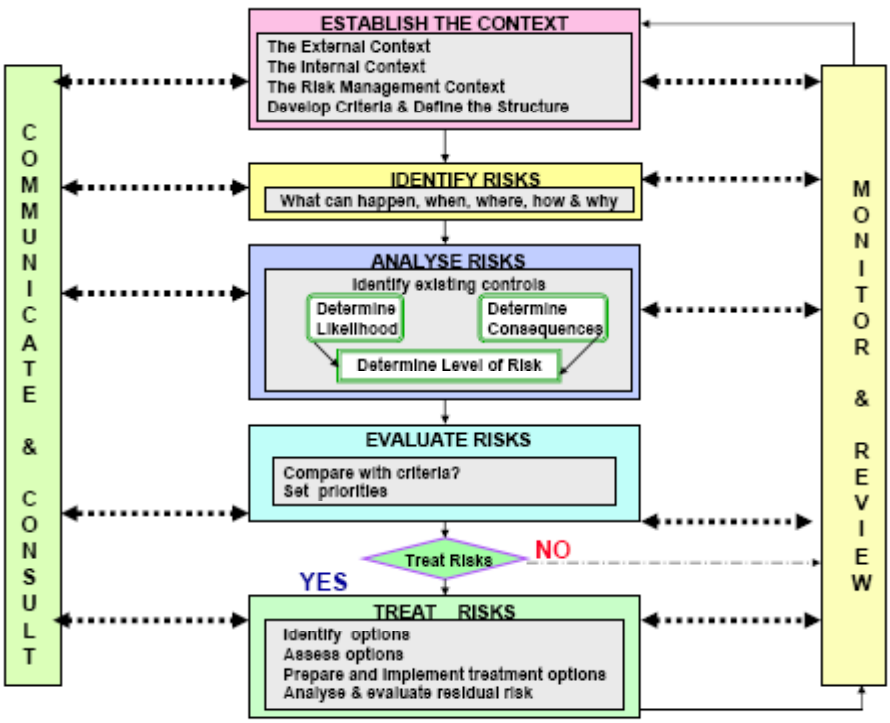
- Los **Activos** en MAGERIT se amplían en N11 a los **Objetivos** (del Dominio considerado, por supuesto)
- Las **Amenazas** en MAGERIT se amplían en N11 a **Eventos o Azares**
- Los **Impactos** en MAGERIT se amplían en N11 a **Consecuencias** (sean pérdidas en también ganancias positivas en ciertos casos)
- La definición de **Riesgo** en MAGERIT se amplía en N11 a la "***ocurrencia de algo que tenga una consecuencia en los objetivos".***

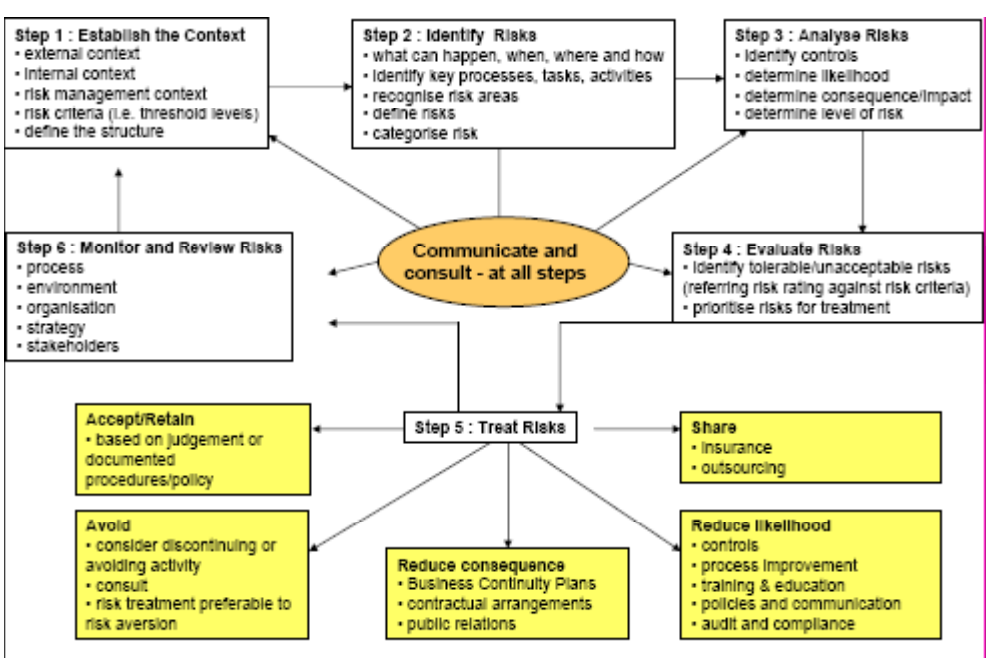
5. El Proceso General de Gestión de Riesgos



Proceso de Gestión de Riesgos

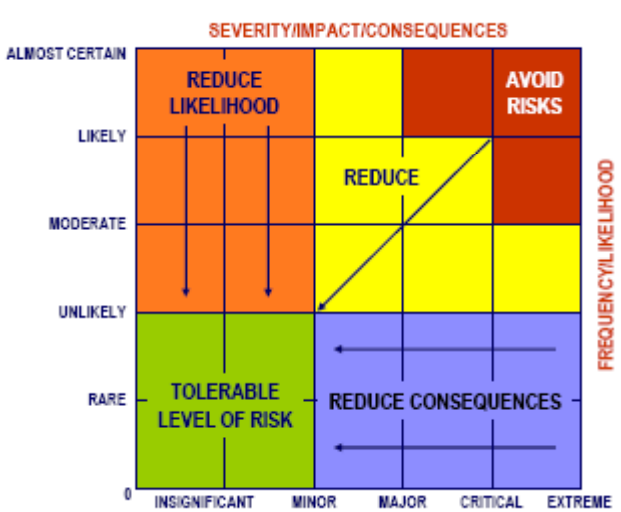



ESTABLISH THE CONTEXT
The External Context
The Internal Context
The Risk Management Context
Develop Criteria & Define the Structure
IDENTIFY RISKS
What can happen, when, where, how & why
ANALYSE RISKS
Identify existing controls
Determine Likelihood
Determine Consequences
Determine Level of Risk
EVALUATE RISKS
Compare with criteria?
Set priorities
Treat Risks
NO
YES
TREAT RISKS
Identify options
Assess options
Prepare and implement treatment options
Analyse & evaluate residual risk
COMMUNICATE & CONSULT
MONITOR & REVIEW


Step 1 : Establish the Context
• external context
• internal context
• risk management context
• risk criteria (i.e. threshold levels)
• define the structure
Step 2 : Identify Risks
• what can happen, when, where and how
• identify key processes, tasks, activities
• recognise risk areas
• define risks
• categorise risk
Step 3 : Analyse Risks
• identify controls
• determine likelihood
• determine consequence/impact
• determine level of risk
Step 6 : Monitor and Review Risks
• process
• environment
• organisation
• strategy
• stakeholders
Communicate and consult - at all steps
Step 4 : Evaluate Risks
• identify tolerable/unacceptable risks (referring risk rating against risk criteria)
• prioritise risks for treatment
Accept/Retain
• based on judgement or documented procedures/policy
Step 5 : Treat Risks
Share
• insurance
• outsourcing
Avoid
• consider discontinuing or avoiding activity
• consult
• risk treatment preferable to risk aversion
Reduce consequence
• Business Continuity Plans
• contractual arrangements
• public relations
Reduce likelihood
• controls
• process improvement
• training & education
• policies and communication
• audit and compliance

Consequence **Likelihood**

	Rare	Unlikely	Possible	Likely	Almost certain
Catastrophic	High	Very High	Very High	Very High	Very High
Significant	High	High	Very High	Very High	Very High
Major	Tolerable	High	High	Very High	Very High
Moderate	Low	Tolerable	Tolerable	High	High
Minor	Low	Low	Tolerable	Tolerable	Tolerable
Insignificant	Very Low	Low	Low	Tolerable	Tolerable
Negligible	Very Low	Very Low	Low	Tolerable	Tolerable



6. Conclusión

6.1. Agradecimientos

El autor agradece al Ministerio de Administraciones Públicas, a la Generalitat Valenciana y a AENOR la autorización para citar, resumir o reproducir partes públicas de borradores y documentos.

6.2. Referencias

1. MAGERIT, Método de Análisis y GEstión de Riesgos en Sistemas de Información, es el modelo oficial del Consejo Superior de Administración Electrónica para la Administración General del Estada y entidades anejas. La actual versión 2 puede verse en: http://www.csi.map.es/csi/pg5m20.htm. La primera versión se editó por Presidencia de Gobierno en 1997.
2. MAGRIP, Modelo de Análisis y Gestión de Riesgos en Proyectos, es un Proyecto de Investigación del Grupo de Investigación ITIO (Integración de las Tecnologías de la Información en la Organizaciones) del Departamento de Organización de Empresas, Economía Financiera y Contabilidad de la Universidad Politécnica de Valencia, dentro de su Línea de Investigación sobre Riesgos
3. MAGERIL, "Modelo de Análisis y GEstión de Riesgos Laborales en PYMES Valencianas del Sector del Mueble", es un Proyecto de investigación financiado durante los años 2005 y 2006 por la Conselleria de Empresa, Universidad y Ciencia de la Generalitat Valenciana (referencia GV05/053), llevado a cabo por el Grupo de Investigación ITIO (Integración de las Tecnologías de la Información en la Organizaciones) del Departamento de Organización de Empresas, Economía Financiera y Contabilidad de la Universidad Politécnica de Valencia.
4. Borghesi A. (Università degli Studi di Verona, Presidente del Comité Científico de ARIMAS, Aca demic Risk Management Association); Cibien, M. (UNI) Gestión del riesgo y normalización a la búsqueda de un punto de encuentro, 4/10/2005)