Una visión incremental de los riesgos: de la metodología MAGERIT al modelo CMMI

Ramiro Carballo

Lead Appraiser

Caelum

Patrocinadores

Caelum
SEI Partner | Carnegie Mellon

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

Colaboradores

GRUPO SMS

DiCe

UNIVERSIDAD PONTIFICIA ICAI ICADE COMILLAS MADRID

Caelum
SEI Partner | Carnegie Mellon

SEI Partner
Carnegie Mellon

CalidaddelSoftware.com

La consultora **CAELUM** ofrece servicios para mejorar la eficiencia de las organizaciones TI dedicadas a desarrollo de productos o prestación de servicios, así como en materia de seguridad de la información.

Tiene licencia del **SEI** para prestar servicios de CMMI (formación y acreditación formal SCAMPI)

El portal **CalidaddelSoftware.com** pretende poner en contacto a personas interesadas en la mejora de procesos software y TI.

Introducción a CMMI for Development v.1.3

12, 13, 14 de Noviembre 2012. Madrid.

Los asistentes a este curso de 3 días podrán describir los componentes del modelo CMMI DEV y su relación entre sí, discutir las áreas de proceso en los modelos CMMI, y ubicar información relevante en el modelo. Comprenderán al CMMI cómo un modelo de procesos que establece un sistema de controles tempranos para la detección y eliminación de defectos. Es un requisito imprescindible para todos los participantes en una evaluación SCAMPI.

http://www.caelum.es/contents/introdev.html

Suplemento a CMMI for Services v.1.3

15 de Noviembre 2012. Madrid.

Para aquellos que asistieron con anterioridad al Curso Oficial del SEI "Introducción a CMMI DEV v.1.3", el SEI ha desarrollado este suplemento especial sobre Servicios de un día de duración, capacitando al alumno para participar como miembro del equipo evaluador en un SCAMPI del modelo CMMI for Services (CMMI SVC v.1.3.).

http://www.caelum.es/contents/suppl-svc.html

La metodología **MAGERIT** es propiedad del Ministerio de Hacienda y Administraciones Pública

Software Engineering Institute | Carnegie Mellon

El modelo **CMMI**, el método de evaluación **SCAMPI**, son marcas registradas y propiedad del Software Engineering Institute (SEI) de la Universidad Carnegie Mellon.

MAGERIT, Versión 2

MAGERIT, versión 2: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Dirección Gral. de Modernización e Impulso de la Adm. Electrónica.

Madrid, 20 de junio de 2006

- Libro_I_-_Metodo.pdf
- Libro_II_-_Catalogo_de_elementos.pdf
- Libro_III_-_Gui_de_Tecnicas.pdf

- Aplicado en
  - Esquema Nacional de Seguridad
  - ISO 27001 , Sistemas de Gestión de Seguridad de la Inf.
  - ISO 20000 (Servicios TI), CMMI, etc.

MAGERIT, el Método:

Libro I :

- Capítulo 2: Pasos conceptuales para el análisis y gestión de riesgos
- Capítulo 3: Enfoque de proyecto: roles, actividades, hitos y documentación
- Capítulo 4: Desarrollo de sistemas de información
- Capítulo 5: Consejos prácticos

MAGERIT: Elementos y Técnicas

Libro II : Catálogo de Elementos

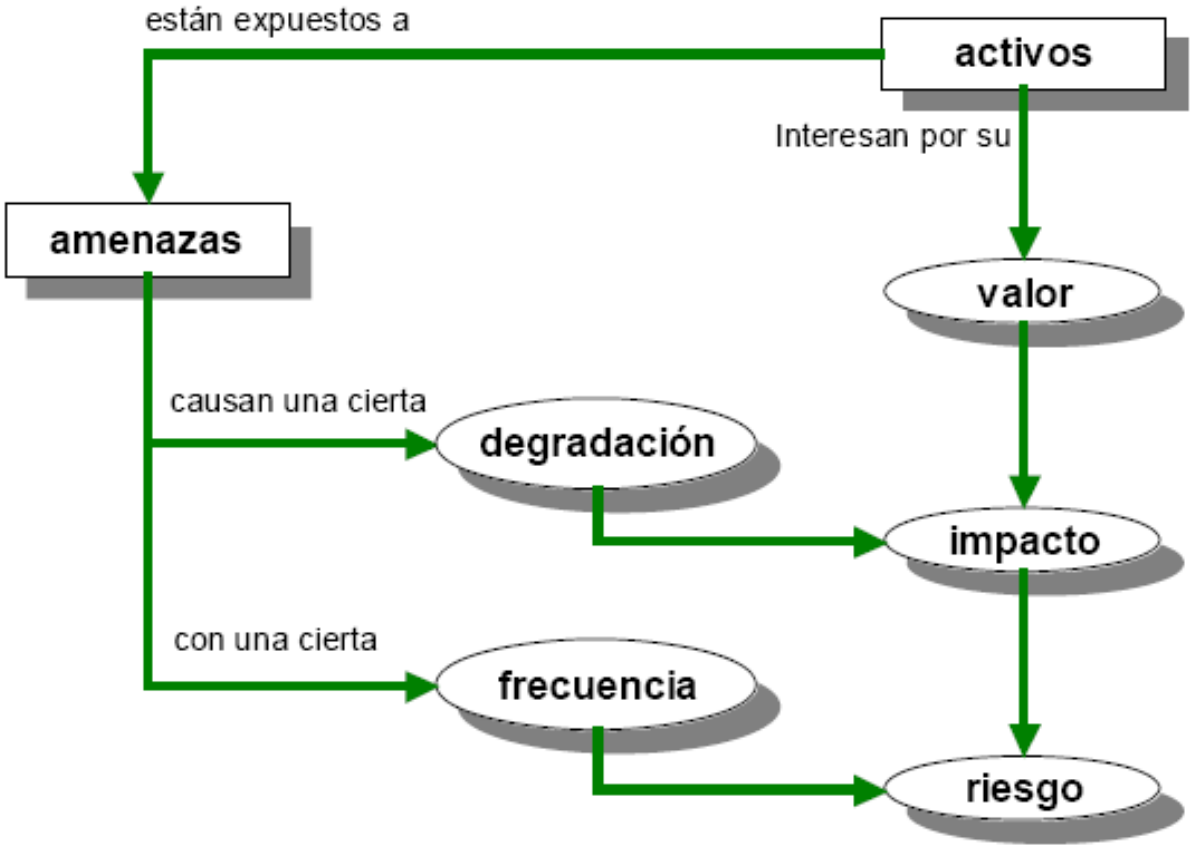
- tipos de activos
- dimensiones de valoración de los activos
- criterios de valoración de los activos
- amenazas típicas sobre los sistemas de información
- salvaguardas a considerar para proteger sistemas de información

Libro III : Guía de Técnicas

- Para el análisis de riesgos
- Para otras actividades: DFD, planificación, Delphi

MAGERIT:

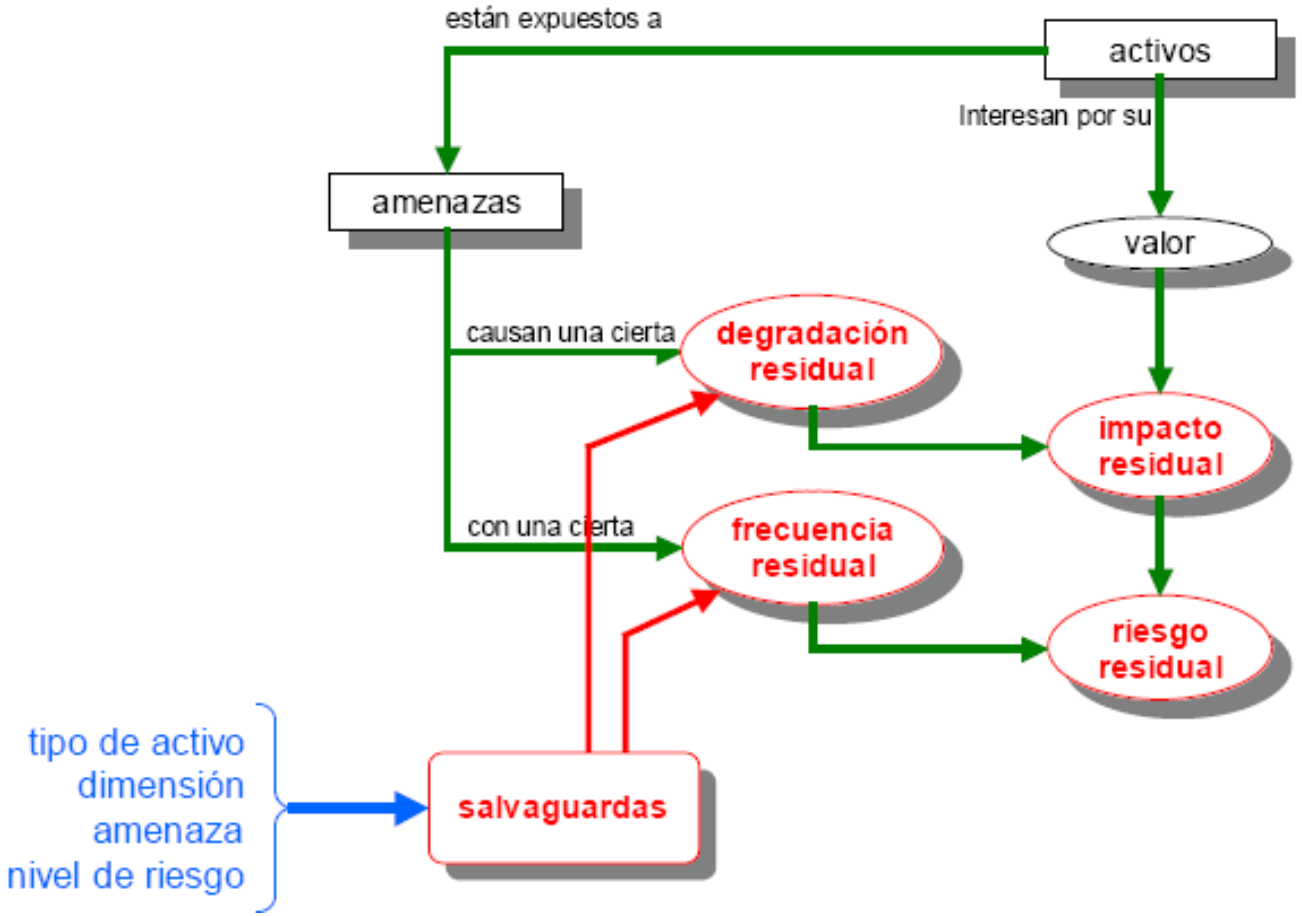
Esquema de análisis de riesgos



MAGERIT, Libro I, página 17

MAGERIT:

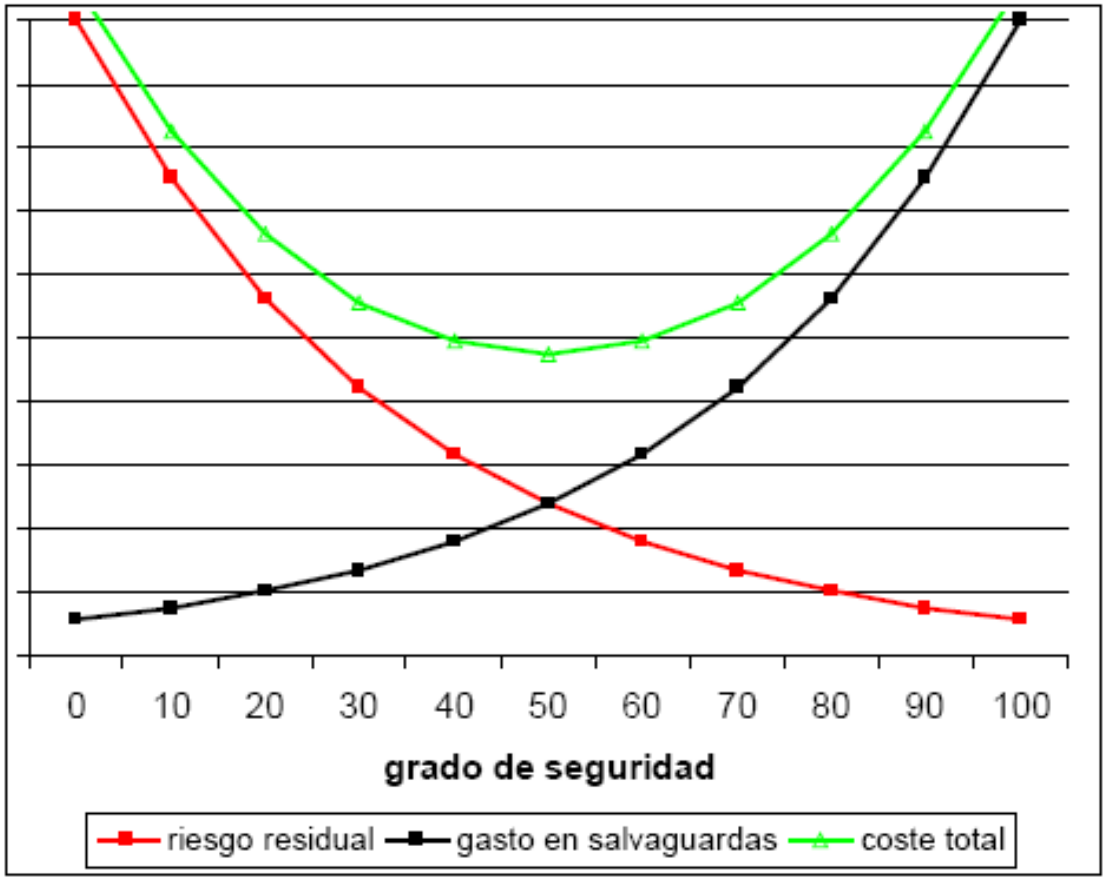
Salvaguardas



MAGERIT, Libro I, página 25

MAGERIT:

Equilibrio razonable de costes



MAGERIT, Libro I, página 28

MAGERIT:

Activos:

- El activo esencial es la **información** que maneja el sistema; o sea los datos. Y alrededor de estos datos se pueden identificar otros activos relevantes:
- Los **servicios** que se pueden prestar gracias a aquellos datos, y los servicios que se necesitan para poder gestionar dichos datos.
- Las aplicaciones informáticas (**software**) que permiten manejar los datos.
- Los equipos informáticos (**hardware**) y que permiten hospedar datos, aplicaciones y servicios.
- Los **soportes de información** que son dispositivos de almacenamiento de datos.
- El **equipamiento auxiliar** que complementa el material informático.
- Las **redes** de comunicaciones que permiten intercambiar datos.
- Las **instalaciones** que acogen equipos informáticos y de comunicaciones.
- Las **personas** que explotan u operan todos los elementos anteriormente citados

MAGERIT, Libro I, página 17

MAGERIT: enfoque de proyecto

Participantes:

- Comité de Dirección,
- Comité de Seguimiento,
- Equipo de proyecto,
- Grupos de Interlocutores,
- Promotor,
- Director de Proyecto,
- Enlace Operacional.

Desarrollo del Proyecto P1, P2, P3:

- Planificación,
- Análisis de Riesgos,
- Gestión de Riesgos

MAGERIT, Libro I, página 33

MAGERIT:

Proceso P1: Planificación

Actividad A1.1: Estudio de oportunidad
- Tarea T1.1.1: Determinar la oportunidad

Actividad A1.2: Determinación del alcance del proyecto
- Tarea T1.2.1: Objetivos y restricciones generales
- Tarea T1.2.2: Determinación del dominio y límites
- Tarea T1.2.3: Identificación del entorno
- Tarea T1.2.4: Estimación de dimensiones y coste

Actividad A1.3: Planificación del proyecto
- Tarea T1.3.1: Evaluar cargas y planificar entrevistas
- Tarea T1.3.2: Organizar a los participantes
- Tarea T1.3.3: Planificar el trabajo

Actividad A1.4: Lanzamiento del proyecto
- Tarea T1.4.1: Adaptar los cuestionarios
- Tarea T1.4.2: Criterios de evaluación
- Tarea T1.4.3: Recursos necesarios
- Tarea T1.4.4: Sensibilización

MAGERIT, Libro I, página 37

MAGERIT:

Proceso P2: Análisis de Riesgos

Actividad A2.1: Caracterización de los activos
- Tarea T2.1.1: Identificación de los activos
- Tarea T2.1.2: Dependencias entre activos
- Tarea T2.1.3: Valoración de los activos

Actividad A2.2: Caracterización de las amenazas
- Tarea T2.2.1: Identificación de las amenazas
- Tarea T2.2.2: Valoración de las amenazas

Actividad A2.3: Caracterización de las salvaguardas
- Tarea T2.3.1: Identificación de las salvaguardas existentes
- Tarea T2.3.2: Valoración de las salvaguardas existentes

Actividad A2.4: Estimación del estado de riesgo
- Tarea T2.4.1: Estimación del impacto
- Tarea T2.4.2: Estimación del riesgo
- Tarea T2.4.3: Interpretación de los resultados

MAGERIT, Libro I, página 37

MAGERIT:

Proceso P3: Gestión de Riesgos

Actividad A3.1: Toma de decisiones
- Tarea T3.1.1: Calificación de los riesgos

Actividad A3.2: Plan de seguridad
- Tarea T3.2.1: Programas de seguridad
- Tarea T3.2.2: Plan de ejecución

Actividad A3.3: Ejecución del plan
- Tarea T3.3.*: Ejecución de cada programa de seguridad

MAGERIT, Libro I, página 37

CMMI: el modelo de mejora

CMMI : Capability Maturity Model Integration v.1.3

3 constelaciones: *www.sei.cmu.edu/cmmi*

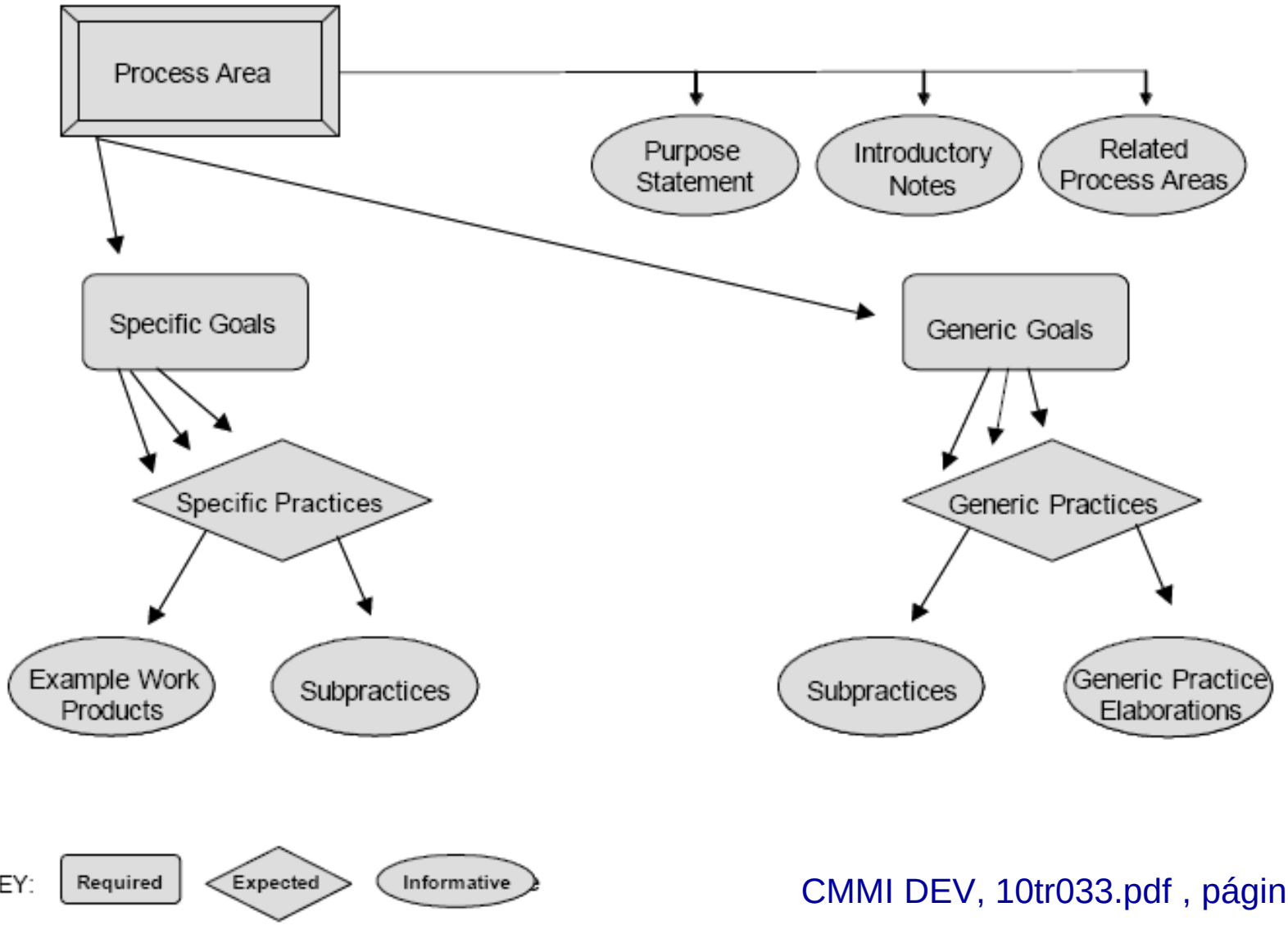
- CMMI DEV: Desarrollo de Software, *10tr033.pdf*
- CMMI SVC: Servicios, *10tr034.pdf*
- CMMI ACQ: Adquisiciones, *10tr032.pdf*

Método de evaluación:

- SCAMPI A: MDD, *11hb001.pdf*
- Handbook SCAMPI B o C, *05hb005.pdf*
- ARC, *11tr006.pdf*

"risks" aparece 267 veces

CMMI: componentes del modelo



CMMI DEV, 10tr033.pdf , página 22

CMMI: las áreas de proceso

CMMI DEV

The 22 process areas are presented in alphabetical

- Causal Analysis and Resolution (CAR)
- Configuration Management (CM)
- Decision Analysis and Resolution (DAR)
- Integrated Project Management (IPM)
- Measurement and Analysis (MA)
- Organizational Process Definition (OPD)
- Organizational Process Focus (OPF)
- Organizational Performance Management (OPM
- Organizational Process Performance (OPP)
- Organizational Training (OT)
- Product Integration (PI)
- Project Monitoring and Control (PMC)
- Project Planning (PP)
- Process and Product Quality Assurance (PPQA
- Quantitative Project Management (QPM)
- Requirements Development (RD)
- Requirements Management (REQM)
- Risk Management (RSKM)
- Supplier Agreement Management (SAM)
- Technical Solution (TS)
- Validation (VAL)
- Verification (VER)

CMMI SVC

The 24 process areas are presented in alphabetical orc

- Capacity and Availability Management (CAI
- Causal Analysis and Resolution (CAR)
- Configuration Management (CM)
- Decision Analysis and Resolution (DAR)
- Incident Resolution and Prevention (IRP)
- Integrated Work Management (IWM)
- Measurement and Analysis (MA)
- Organizational Process Definition (OPD)
- Organizational Process Focus (OPF)
- Organizational Performance Management (
- Organizational Process Performance (OPP
- Organizational Training (OT)
- Process and Product Quality Assurance (PI
- Quantitative Work Management (QWM)
- Requirements Management (REQM)
- Risk Management (RSKM)
- Supplier Agreement Management (SAM)
- Service Continuity (SCON)
- Service Delivery (SD)
- Service System Development (SSD)[7]
- Service System Transition (SST)
- Strategic Service Management (STSM)
- Work Monitoring and Control (WMC)
- Work Planning (WP)

CMMI ACQ

The 22 process areas are presented in alphabetica

- Agreement Management (AM)
- Acquisition Requirements Development (ARD)
- Acquisition Technical Management (ATM)
- Acquisition Validation (AVAL)
- Acquisition Verification (AVER)
- Causal Analysis and Resolution (CAR)
- Configuration Management (CM)
- Decision Analysis and Resolution (DAR)
- Integrated Project Management (IPM)
- Measurement and Analysis (MA)
- Organizational Process Definition (OPD)
- Organizational Process Focus (OPF)
- Organizational Performance Management (OPI
- Organizational Process Performance (OPP)
- Organizational Training (OT)
- Project Monitoring and Control (PMC)
- Project Planning (PP)
- Process and Product Quality Assurance (PPQA
- Quantitative Project Management (QPM)
- Requirements Management (REQM)
- Risk Management (RSKM)
- Solicitation and Supplier Agreement Developme

Visión incremental de la mejora

Table 3.1 Comparison of Capability and Maturity Levels

Level	*Continuous Representation Capability Levels*	*Staged Representation Maturity Levels*
Level 0	Incomplete	
Level 1	Performed	Initial
Level 2	Managed **PP** **PMC**	Managed **PP** **PMC**
Level 3	Defined **RSKM**	Defined **RSKM**
Level 4		Quantitatively Managed
Level 5		Optimizing

CMMI DEV, 10tr033.pdf , página 35

CMMI: Gestión de Riesgos
Riesgos en PP y PMC (WP y WMC) (NIVEL 2)

PP SP 2.2 Identify Project Risks

(Identify and analyze project risks)

Project planning risk identification and analysis typically include the following:

- Identifying risks
- Analyzing risks to determine the impact, probability of occurrence, and time frame in which problems are likely to occur
- Prioritizing risks

PMC SP 1.3 Monitor Project Risks

(Monitor risks against those identified in the project plan)

Examples of risk status include the following:

- A change in the probability that the risk occurs
- A change in risk priority

CMMI DEV, 10tr033.pdf , página 303

CMMI: Gestión de Riesgos

Gestión de Riesgos en RSKM (NIVEL 3)

SG 1 Prepare for Risk Management

- SP 1.1 Determine Risk Sources and Categories
- SP 1.2 Define Risk Parameters
- SP 1.3 Establish a Risk Management Strategy

SG 2 Identify and Analyze Risks

- SP 2.1 Identify Risks
- SP 2.2 Evaluate, Categorize, and Prioritize Risks

SG 3 Mitigate Risks

- SP 3.1 Develop Risk Mitigation Plans
- SP 3.2 Implement Risk Mitigation Plans

GG1 : Achieve Specific Goals

CMMI DEV, 10tr033.pdf , página 362

CMMI: Gestión de Riesgos RSKM

Prácticas genéricas en RSKM

GP 2.1. Establish an Organizational Policy

GP 2.2. Plan the Process

GP 2.3. Provide Resources

GP 2.4. Assign Responsibility (and authority)

GP 2.5. Train People

GP 2.6. Control Work Products

GP 2.7. Identify and Involve Relevant Stakeholders

GP 2.8. Monitor and Control the Process

GP 2.9. Objectively Evaluate Adherence

GP 2.10. Review Status with Higher Level Management

GG2 : Institucionalizar un proceso gestionado

CMMI: Gestión de Riesgos RSKM

GG3: Institucionalizar un proceso definido

Prácticas genéricas en RSKM

GP 3.1. Establish a Defined Process (Establish and maintain the description of a defined process)

GP 3.2. Collect Process Related Experiences (Collect process related experiences derived from planning and performing the process to support the future use and improvement of the organization's processes and process assets)

CMMI: Alta Madurez

4 áreas de proceso en niveles 4 y 5

El análisis estadístico de los procesos nos permite mejorar con el fin de conseguir los objetivos de calidad y rendimiento de la organización

Ramiro Carballo Gutiérrez
SCAMPI v.1.3 Lead Appraiser
(ID# 1201018-03)
rcarballo@caelum.es
Móv.: 639078817

www.linkedin.com/in/ramirocarballo

Caelum Information & Quality Technologies, S. L.
Paseo de las Delicias 38, 1º Dcha.
28045 Madrid
www.caelum.es
www.CalidaddelSoftware.com
Tlf.: 918312029

CSTIC 2012

Dominando los riesgos se compite mejor

18 de Septiembre de 2012 #CSTIC12

Patrocinadores

Caelum

SEI Partner | Carnegie Mellon

GOBIERNO DE ESPAÑA

MINISTERIO DE DEFENSA

Organizador

ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

AEC

COMITÉ DE LOS SISTEMAS Y LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Patronos de la AEC:

Aena

aena aeropuertos

AENOR

fundación enresa

renfe

Colaboradores

grupo SMS

DiCe

UNIVERSIDAD PONTIFICIA ICAI ICADE COMILLAS MADRID

Cooperadores

ati

CONCITI.org