

# QUATIC 2001

de la Gestión de los Riesgos en los Proyectos  
a la Gestión de los Proyectos por sus Riesgos

(GR ⊂ GP)  $\wedge$  (GP ⊂ GR)

Julián Marcelo  
[jmarcelo@ati.es](mailto:jmarcelo@ati.es)

# Proyectos y sus Riesgos

---

- ◆ Conceptos básicos sobre Proyectos y Riesgos
- ◆ Generación Primera ‘casuística’, G1
- ◆ Generación Segunda ‘taxonómica’, G2
- ◆ Transición a la Generación Tercera ‘causal’, G3
- ◆ Primeros pasos de la Generación Tercera G3

# **Conceptos básicos sobre Proyectos y Riesgos**

---

- **Riesgos en los proyectos informáticos**
- **Modelos, Sistemas y Proyectos**
- **Planificación y Gestión de Sistemas y proyectos**
- **Riesgo en sistemas, proyectos y negocios**
- **Tres Generaciones**

# Riesgos en los proyectos informáticos

---

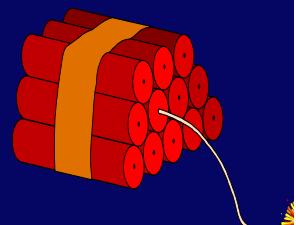
**Los estudios e informes convergen: muestran aún ahora**

**La ‘Vulnerabilidad’ de los proyectos (frecuencia de problemas)**

- **Sobre 8.380 proyectos americanos (según Standish Group)**
  - el 31% se abandona y el 53% está fuera de presupuesto o de plazo
- **También el 80% de los Proyectos británicos (según Ovum)**
  - se abandona, o está fuera de presupuesto o de plazo

**Los ‘Impactos’ en los proyectos (consecuencia de problemas)**

- **Los costes de ejecución desbordan los previstos**
- **Los tiempos de ejecución desbordan los previstos**
- **Los Sistemas resultantes**
  - no dan los beneficios anticipados (dificultad de ejecución)
  - tiene menos prestaciones que las estimadas
  - son incompatibles con la arquitectura adquirida



# Riesgos en los proyectos informáticos

---

## 10 factores de riesgo críticos en proyectos informáticos

### 1. Riesgos en los recursos

Insuficiencias de personal

Plazos y Presupuestos irreales

### 2. Riesgos en las subcontratas

Insuficiencias en suministros externos de componentes

Insuficiencias en realizaciones externas de tareas

### 3. Riesgos en los requerimientos

Desarrollo de funciones equivocadas

Desarrollo de interfaz de usuario equivocada

Especificaciones excesivas

Continuos cambios de requerimientos

### 4. Riesgos en el diseño

Insuficiencias de rendimiento del sistema al funcionar realmente

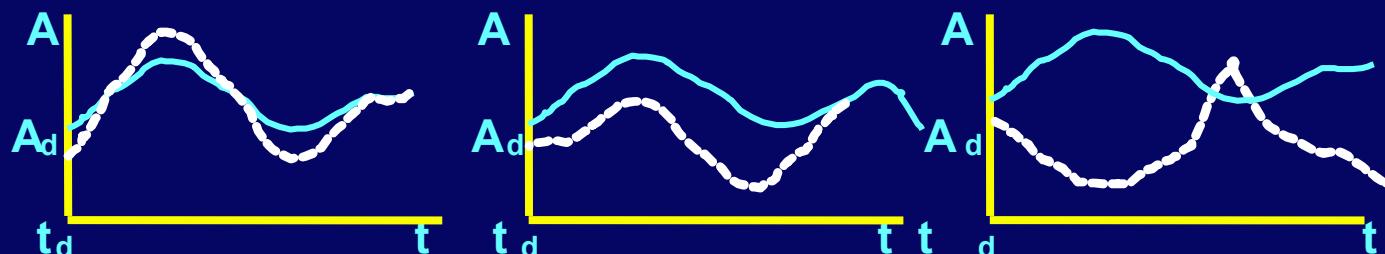
Optimismo sobre las capacidades de las tecnologías informáticas

(Fuente: Boehm 89)

# Modelos, Sistemas y Proyectos

- Un proyecto es un sistema dinámico
- En un Proyecto de desarrollo ‘informático’
  - \* Estado inicial del Sistema de Información (S.I.)
  - \* Estado final (planeado) del Sistema Informático y del S.I.
  - \* Desarrollo del proyecto informático
  - \* Estado final (alcanzado) del Sistema Informático y del S.I.
- La visión dinámica del sistema ‘proyecto’ prioriza las ‘trayectorias’  $A(t)$  de cada atributo básico A (por ejemplo el riesgo) de sus componentes. El conjunto da una visión global del **comportamiento** del sistema. Para cada A, se parte de su valor  $A_d$  en  $t = t_d$  ('hito' de decisión) y se analizan las ‘trayectorias terminales’ o ‘atractores’ (arrancando de valores  $A_d$  próximos o ‘perturbaciones’). Tres tipos de atractor:

- ‘puntual’,
- periódico
- extraño’



# Planificación y Gestión de Sistemas y proyectos

---

## Escenario

- El ritmo acelerado de cambios y las situaciones imprevistas impactan en proyectos ya iniciados o planeados.
- Los actores toman decisiones difusas, con poca información, sin tiempo de ensayo ni margen para rectificar, con impactos irreversibles por su multidimensión y globalidad.
- Se requiere anticipación que prevea una gestión flexible en tiempo real de los proyectos.

La planificación es el proceso de información que:

- anticipa las decisiones de lanzamiento de proyectos
- prepara el desarrollo de las acciones que los materializan.

La planificación, en los Sistemas de Información y Comunicaciones:

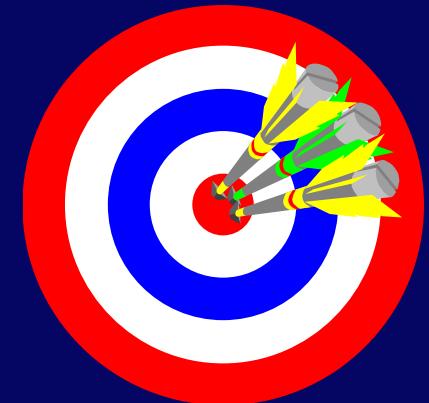
- En sentido amplio, enlaza y da coherencia entre objetivos de la organización y resultados planificados;
- En sentido estricto, permite obtener información preparatoria del lanzamiento de los proyectos.

# Riesgo en sistemas, proyectos y negocios

---

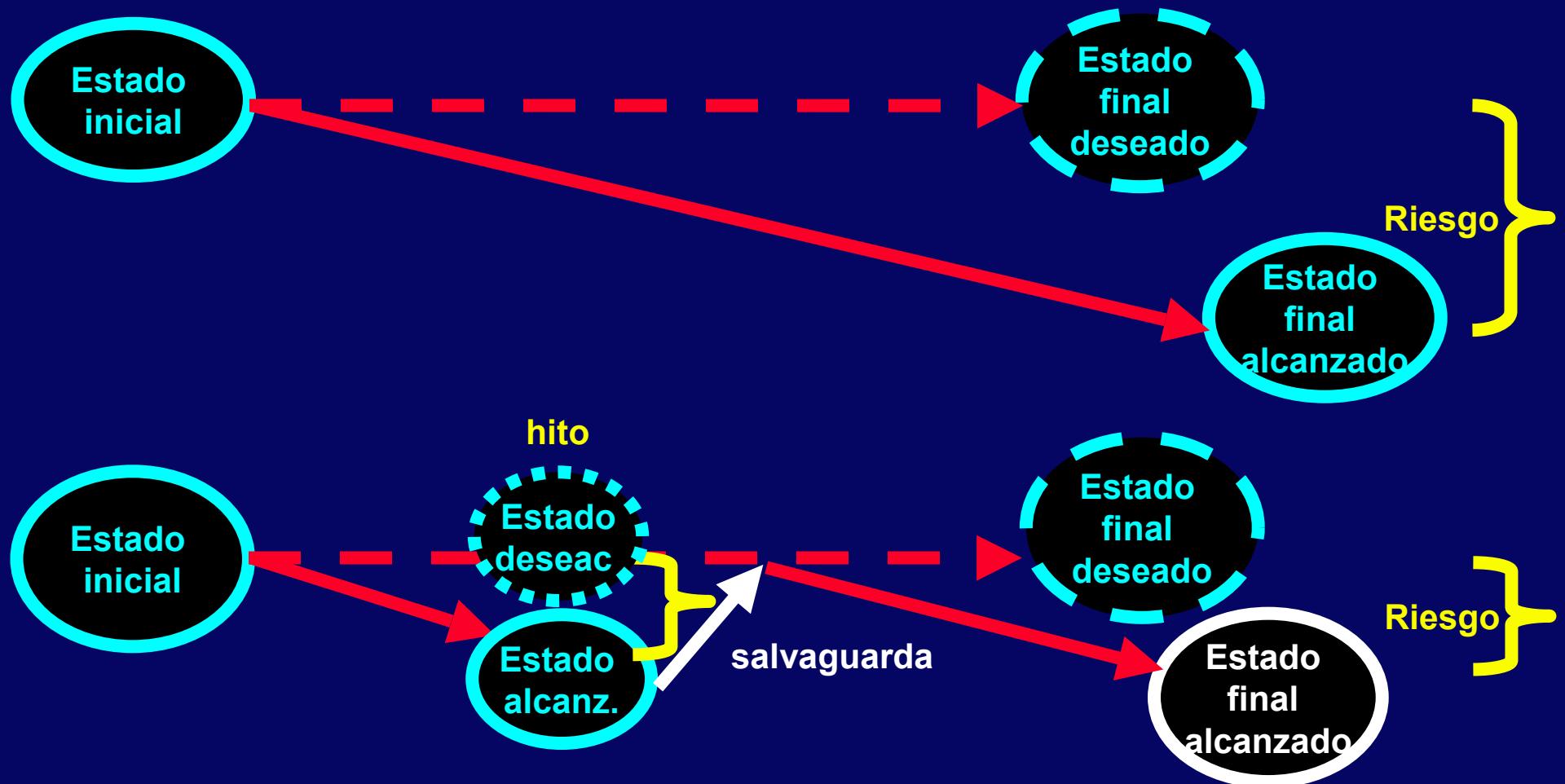
## Tres tipos de riesgos, según sus ‘dianas’

- el riesgo en el negocio  
(de un mercado de valores, por ejemplo)  
Sus modelos enriquecen los método de análisis
- el riesgo en el sistema  
(de información, por ejemplo)  
El método MAGERIT trata Riesgos de Sistemas
- el riesgo en el proyecto  
(de construir el sistema de información, por ejemplo)  
El modelo MAGERIT ayuda a tratar Riesgos de Proyectos



# Riesgo en sistemas, proyectos y negocios

Riesgo = 'distancia' de estados finales (deseado, alcanzado)



# Tres Generaciones

---

## Tres generaciones de modelos de riesgos en proyectos

- **Primera Generación G1 (primeros 80)**

Basada en listas ‘casuísticas’ de riesgos especiales para proyectos



- **Segunda Generación G2 (primeros 90)**

Basada en modelos de procesos y eventos.

Arranca de Boehm 89 y sigue con SEI-CMM 94-96, Hall 98



- **Tercera Generación G3 (emergente)**

Arranca con Eurométodo 96, MAGERIT 97, ISPL 98

Influida por otros modelos ‘causales’ (proyectuales, ‘ecológicos’)



## **Generación Primera ‘casuística’, G1**

---

- Riesgos tecnológicos
- Listas de comprobación de riesgos

# Riesgos tecnológicos

---

## Definiciones básicas:

- Fiabilidad de un sistema:** probabilidad  $F$  de que funcione en tiempo y condiciones
- Disponibilidad:** fiabilidad potencial instantánea.
- Tasa de fallos  $I(t)$ :** probabilidad potencial de su ocurrencia durante  $dt$  si el sistema funciona en el instante  $t$ ; equivale a  $I(t) = - (dF(t)/dt)/F(t)$ ; o bien a  $F(t) = \exp(-It)$ .

## Historia:

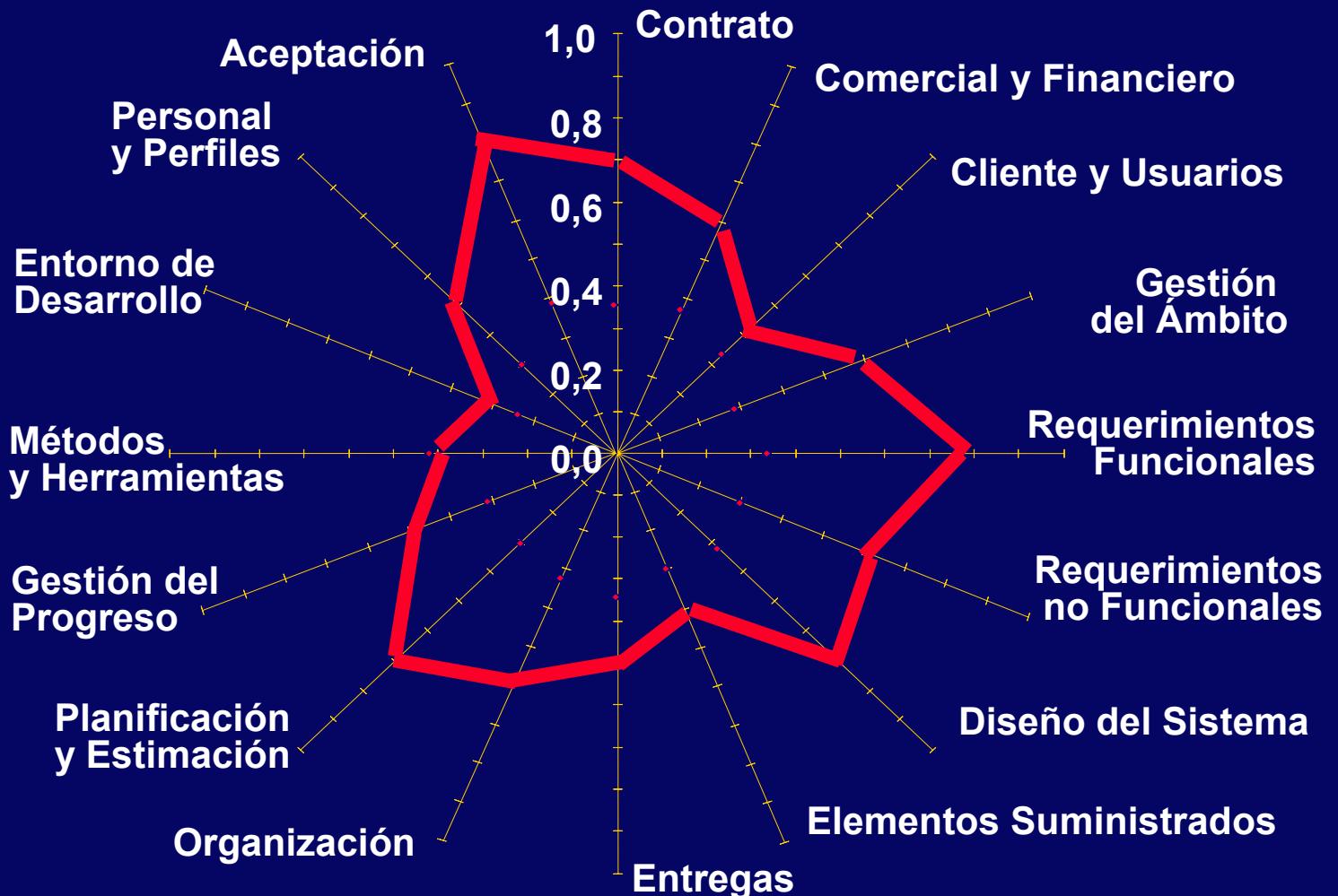
40s. La **teoría de la fiabilidad**, arranque de la Teoría del Riesgo en Sistemas complejos con el **Teorema de Lusser**: *la probabilidad de éxito (no fallo) de una cadena de componentes es el producto de las probabilidades de éxito de sus elementos* (la fiabilidad del conjunto es inferior a la de cada elemento separado; “la cadena se rompe siempre por su eslabón más débil”).

60s. **Análisis de riesgos cuantitativo (procesos markovianos)** para describir el comportamiento de sistemas complejos con fallos ensayables y sin intervención manual (aleatorios); o **cualitativo como los árboles de fallos** para sistemas híbridos con la incertidumbre de la intervención humana y la imposibilidad de probar los impactos salvo por simulación. Se define el “riesgo como una entidad con dos dimensiones: probabilidad y consecuencia(s)” o sea vulnerabilidad e impacto.

70s. **Método general de Rasmussen**. 6 etapas: Definición del proyecto de seguridad y su sistema objetivo; Análisis funcional de éste; Identificación de riesgos; Modelización del sistema; Evaluación de consecuencias; Síntesis y decisiones final.

# Listas de comprobación de riesgos

**Modelo G1**  
de **Análisis**  
de riesgos  
de Sema:  
partiendo  
de una  
lista de  
unas 200  
preguntas,  
16 factores  
de riesgo  
tratan:



## **Generación Segunda ‘taxonómica’, G2**

---

- **Modelo de Boehm**
- **Modelo de Hall y su relación con el de madurez de SEI-CMM**
- **Modelo de Riesgos del SEI**
- **Modelo SPR de mejora de capacidad en la gestión del riesgo**

# Modelo de Boehm (análisis de riesgos G2)

---

## Riesgos

### 1. Riesgos en los recursos generales

Insuficiencias de personal

Plazos y presupuestos irreales

### 2. Riesgos en las subcontratas

Insuficiencia en suministro externos de componentes - - - - - - - - J K

Insuficiencia en realizaciones externas de tareas - B - D - - - - J

### 3. Riesgos en los requerimientos

Desarrollo de Funciones equivocadas - - - - F - H

Desarrollo de Interfaz de usuario equivocada - - - - F - H

Especificaciones excesivas - - - D - FG H

Continuo cambio de requerimientos - - - - E - - - I

### 4. Riesgos en el diseño

Insuficiencia de rendimiento en funcionamiento real - - - - - - - - - K

Forzamiento/optimismo sobre capacidades informáticas - - - - - H - J K L

## Técnicas

# Modelo de Boehm (análisis de riesgos G2)

---

## Técnicas (medidas, salvaguardas)

- A) **Contratar las personas clave** proactivamente
- B) **Construir equipos** proactivamente (desarrollar valores compartidos, ...)
- C) **Estimar los plazos y presupuestos** ‘reactivamente’ (con fondo para riesgos)
- D) **Diseñar ‘forfait’** proactivamente: usar el presupuesto/plazo fijo para priorizar los requerimientos; diseñar con arquitectura que permita retrasar lo no obligatorio; modular la funcionalidad entregada para adecuarla al presupuesto/plazo disponible.
- E) **Desarrollar incrementalmente** las funcionalidades (requerimientos prioritarios...)
- F) **Desarrollar por prototipos** (o sea, subconjuntos para ‘comprar’ información)
- G) **Reducir requerimientos** usando las priorizaciones desarrolladas para D, E), F).
- H) **Analizar la misión:** análisis organizacional, coste-beneficio, ingeniería del usuario
- I) **Encapsular la información** para reducir requisitos volátiles y reutilizar software
- J) **Comprobar los referentes y auditar** por expertos externos antes de decidir
- K) **Ingenierizar rendimientos** con técnicas para simular, modelar, prototipar, afinar
- L) **Analizar las capacidades de las tecnologías informáticas** para resolver FCE.

# Modelo de Hall (análisis de riesgos G2)

---

- Gestión del Riesgo: proceso con dos actividades principales:
  - la Evaluación del riesgo
  - el Control del riesgo
- Gestión del Riesgo: genera estrategia para decidir
- Gestión del Riesgo: basada en 9 teorías
  - **Razona sobre la vulnerabilidad** -probabilidad de riesgo- usando las Teorías de probabilidad, de incertidumbre y la de portfolio:
  - **Razona sobre el impacto** -consecuencia del riesgo-, usando las Teorías de la utilidad, de juegos, del caos y/o la creatividad.
  - **Combina vulnerabilidad e impacto en el tiempo**, usando la Teoría de la decisión y el Teorema de Bayes para elecciones dinámicas.

# Modelo de Hall (análisis de riesgos G2)

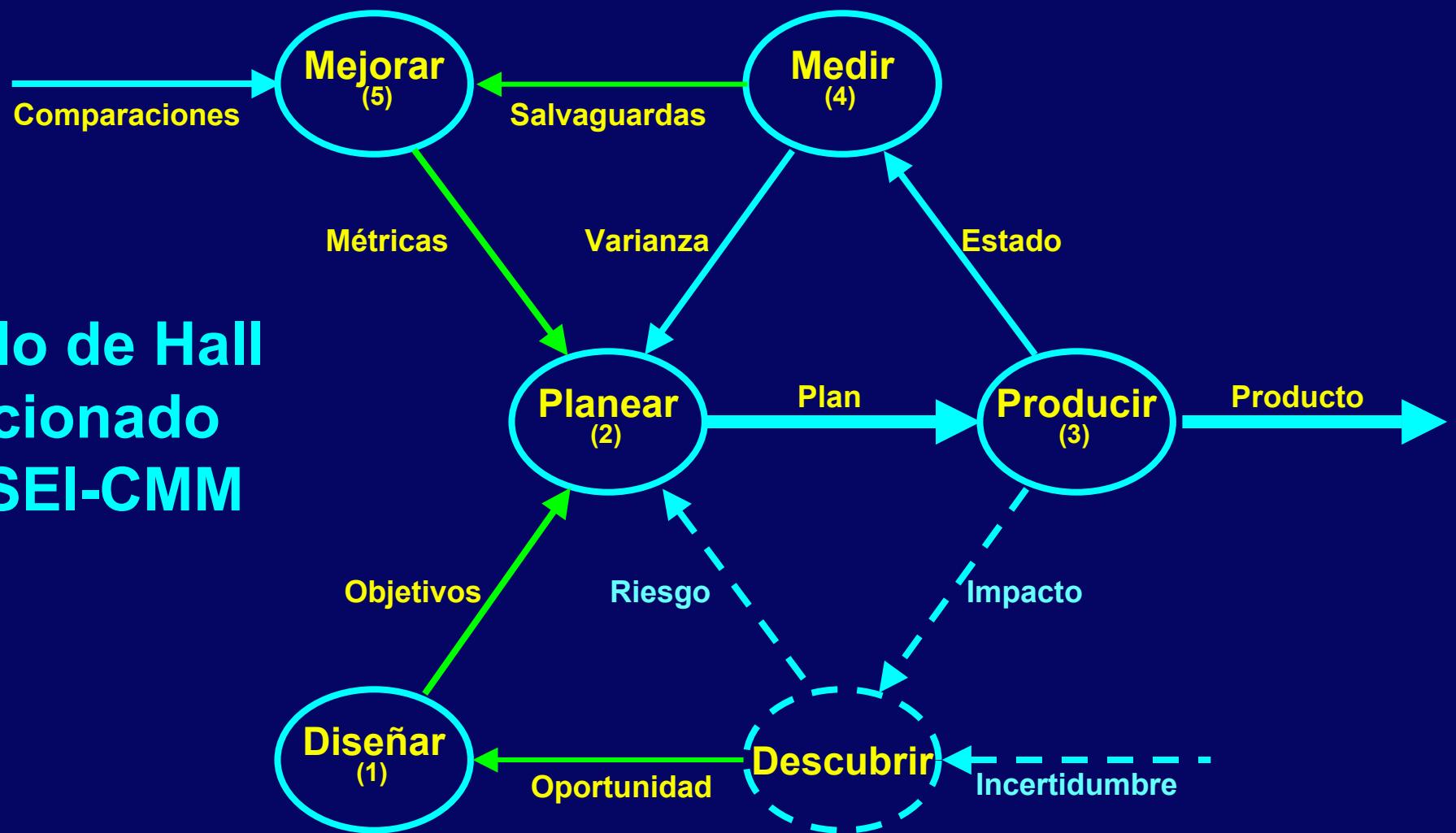
---

El Modelo 6-D de las 6 disciplinas PPMMDD soporta la mejora continua del proceso SEI (Humphrey) o modelo de madurez CMM:

- **Diseñar:** transformar ideas en objetivos, creando y difundiendo la visión organizacional (*CMM-SEI nivel 1*)
- **Planear:** confrontar los recursos disponibles y los requerimientos derivados de los objetivos del proyecto (*CMM-SEI nivel 2*)
- **Producir:** implementar el plan para lograr el producto (*CMM nivel 3*)
- **Medir:** comparar los resultados esperados y los realiza (*CMM nivel 4*)
- **Mejorar:** aprender de experiencias como cambiar el plan (*CMM nivel 5*)
- **Descubrir:** concienciar sobre el futuro, razona sobre posibilidades con resultados inciertos buenos (oportunidades) o malos (riesgos).

# Modelo de Hall (análisis de riesgos G2)

Modelo de Hall  
relacionado  
con SEI-CMM



# Modelo de Hall (análisis de riesgos G2)

---

Ciertas organizaciones de software tienen un concepto del riesgo en sentido revolucionario de oportunidad y soportan

- la mejora continua (modelo basado en la conciencia del pasado)
- la reingeniería (modelo basado en la conciencia de futuro).

*Es falaz elegir entre ambos modelos. Sólo la coexistencia de la conciencia de pasado y futuro con el ciclo completo PPMMDD optimiza productos existentes y capitaliza nuevas oportunidades.*

El modelo 6-D forma 4 ciclos de ‘conciencia’:

- |              |                |             |
|--------------|----------------|-------------|
| • ciclo PPM: | lo conocido    | lógica      |
| • ciclo MMP: | lo pasado      | memoria     |
| • ciclo PPD: | lo desconocido | imaginación |
| • ciclo DDP: | lo futuro      | emoción     |

# Modelo G2 de análisis de riesgos

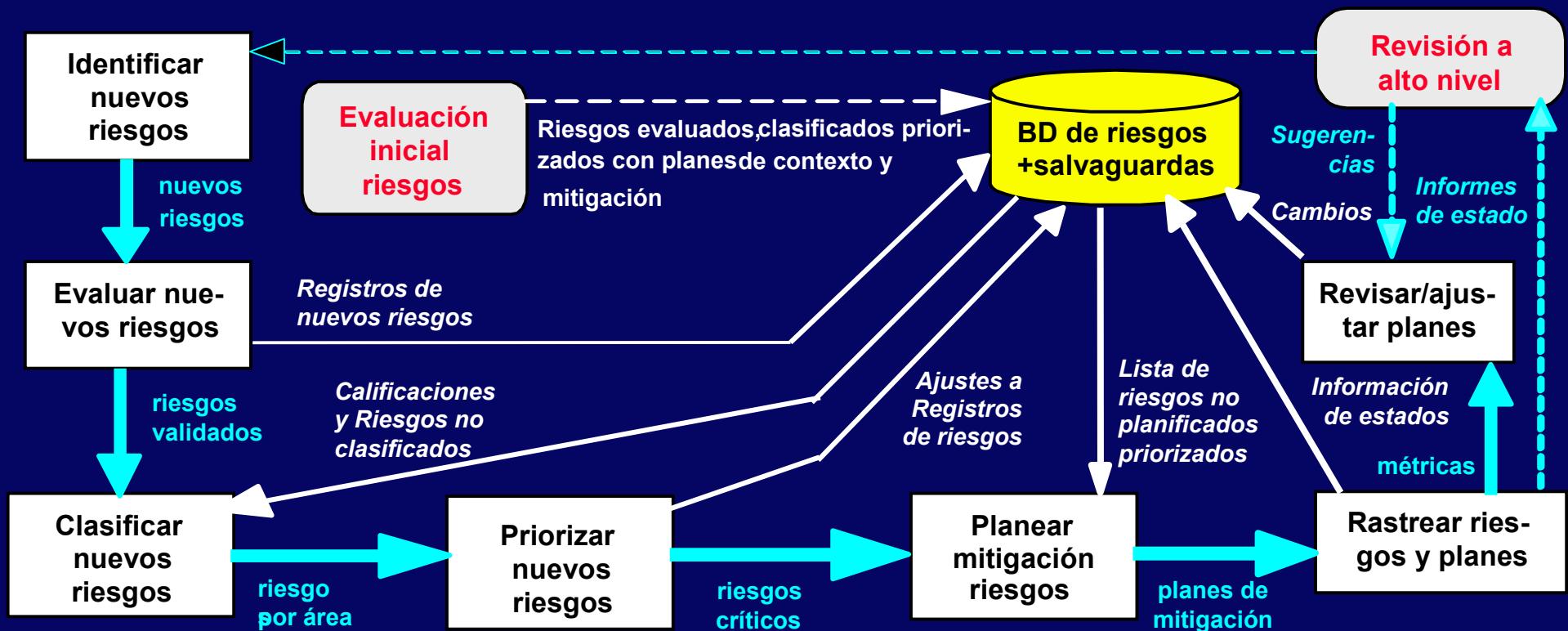
## Hall



# Modelo de Riesgos del SEI

El complejo **Modelo de Riesgos del SEI** se articula en dos grandes bloques:

- La **Adquisición de software** (CMM)
- La **Gestión o Paradigma de Riesgos del Software** con 4 elementos: Gestión Continua CRM y Conjunta TRM, Evaluación SRE y Métrica de Riesgos



# Modelo SPR de mejora de capacidad (C.Jones)

---

Según C.Jones, "**un proyecto es un 'éxito' si no da sorpresas**"; es un:

- 'éxito' absoluto si:** 1) funciona técnicamente bien; 2) se ha desarrollado rápidamente; 3) añade valor al negocio.
- 'fracaso' absoluto si:** 1) se cancela; 2) se entrega sin funcionar o con defectos que lo inutilicen; 3) lleve a litigios graves por incumplimiento.
- 'éxito' relativo si cumple:** 1) su plazo y coste por bajo de sus proyectos concurrentes y/o <115% de lo previsto, 2) a satisfacción del cliente.
- 'fracaso' relativo si:** 1) incumple objetivos de plazo y coste en >150%; 2) su mala calidad impide que el cliente lo use 6 meses tras la entrega.

Un proyecto pasará de '**fracaso**' a '**éxito**' relativos siguiendo 3 reglas:

- Más vale prevenir que curar
- Un problema descubierto temprano facilita su recuperación
- Un problema se cura rara vez si se deja sin tratar.

Jones acaba en un **modelo de maduración de capacidad** con 6 etapas que centran: 1) la gestión de los proyectos; 2) el personal técnico y métodos de eficacia probada; 3) la introducción de nuevas tecnologías y herramientas; 4) la infraestructura; 5) la reusabilidad, 6) liderazgo de la industria.

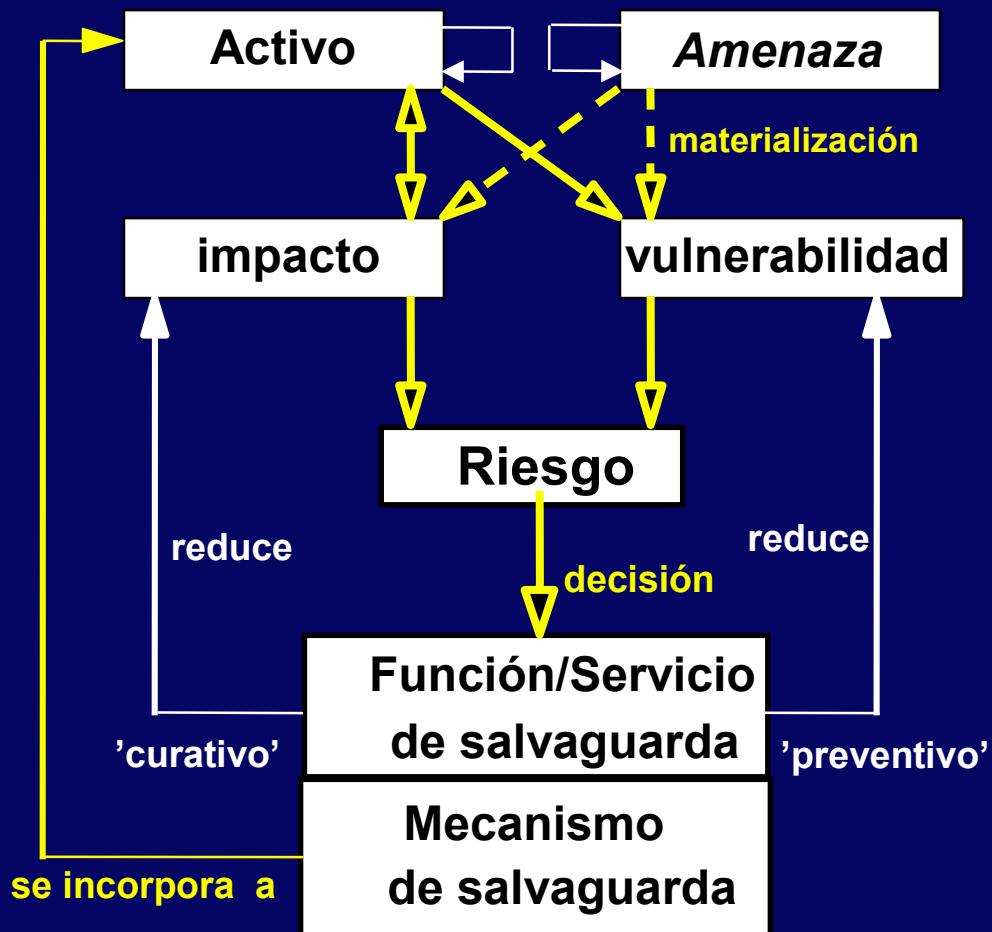
## Transición a la Generación Tercera ‘causal’, G3

---

- **Modelo MAGERIT de Gestión de Riesgos en Sistemas adaptado a Proyectos**
- **Modelo de eventos de MAGERIT-Proyectos**
- **Modelo McFarlan**

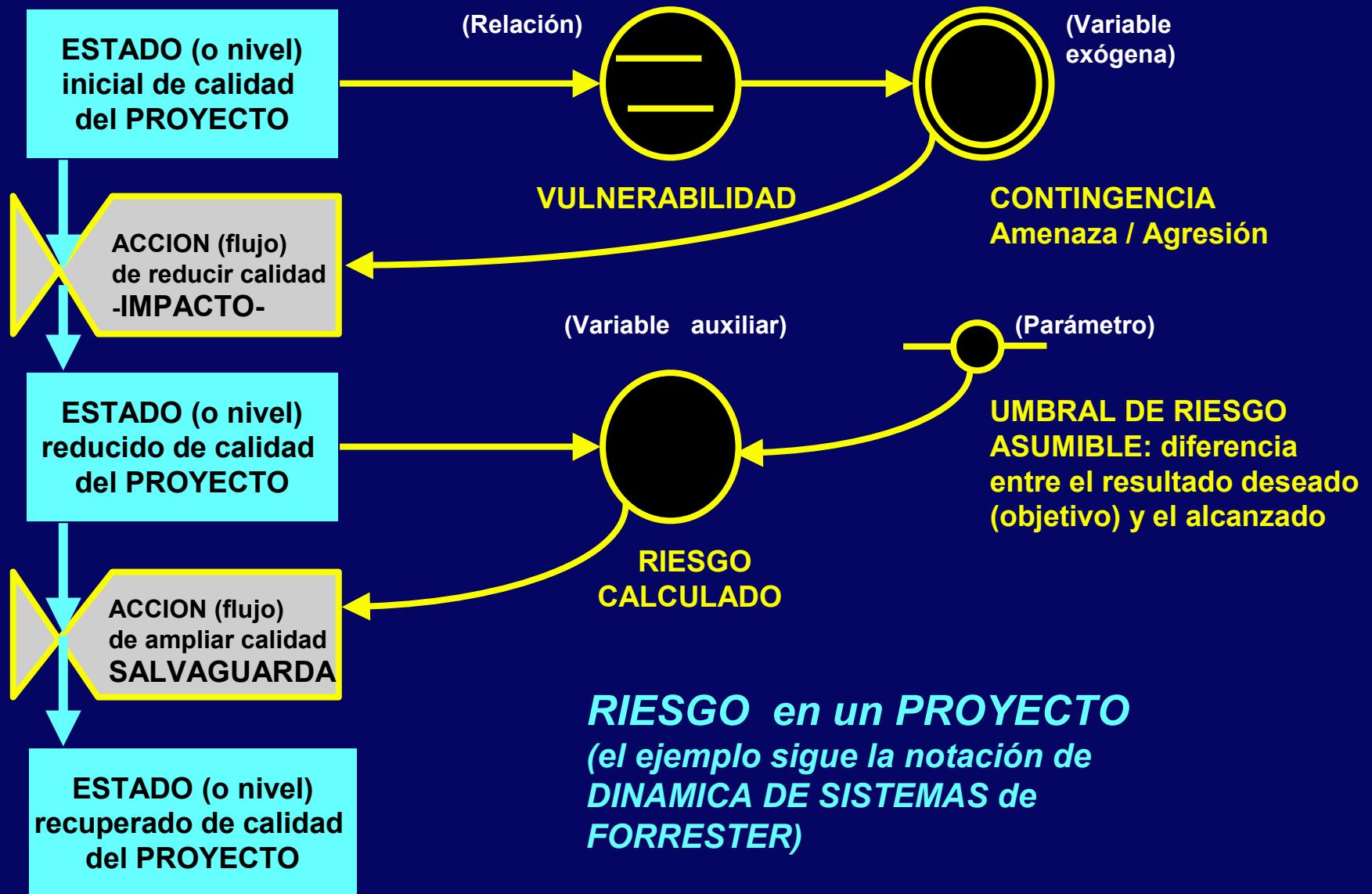
# Modelo MAGERIT de Análisis de Riesgos en Sistemas

## Modelo de Entidades de MAGERIT -Método de Análisis y Gestión de Riesgos para Sistemas- adaptado a Proyectos



- **Activo:** Éxito del proyecto
- **Amenazas:** Factores de Riesgo
- **Vulnerabilidad:** probabilidad de que se materialice cada factor de riesgo
- **Impacto:** consecuencia de que se materialice cada factor de riesgo
- **Riesgo:** composición de Impactos en los activos y vulnerabilidades en sus amenazas
- **Salvaguardas:** medidas técnicas y/u organizativas para reducir el riesgo bajo un umbral aceptable

# Modelo de eventos de MAGERIT-Proyectos



# Modelo McFarlan G2 de gestión de riesgos

---

## Tres factores de riesgo

1. **Experiencia en la tecnología aplicable (*factor subjetivo interno*):** la familiarización del equipo con el hardware, sistema operativo, gestores (DB, DC) y lenguajes comprende también la absorción de experiencia externa, p.ej. como formación
2. **Estructuración del proyecto (*factor subjetivo externo*):** Los objetivos iniciales del proyecto y sus resultados dependen de la claridad de los **requerimientos** trasladados por la organización ‘cliente’ al equipo de desarrollo.
3. **Tamaño del proyecto (*factor objetivo, no reducible*):** Importa sobre todo la **envergadura** del proyecto (en coste años-hombre) relativo al tamaño de los que el equipo desarrolla normalmente.

# Modelo McFarlan G2 de gestión de riesgos

## Tipos de proyectos, según factores y grado de riesgo

Inexperiencia tecnológica	0	0	0	0	1	1	1	1
Desestructuración	.0	.0	.1	.1	.0	.0	.1	.1
Tamaño	..0	..1	..0	..1	..0	..1	..0	..1
Composición de factores	000	001	010	011	100	101	110	111
RIESGO	0	1	2	3	4	5	6	7

Métrica en los factores: 0 = bajo 1 = alto

Métrica en el riesgo:

0 = muy bajo

1 = bajo

2 = muy bajo (y poco manejable)

3 = bajo (y poco manejable)

4 = bajo-medio

5 = medio

6 = alto

7 = muy alto

# Modelo McFarlan G2 de gestión de riesgos

---

## Salvaguardas: herramientas/métodos de gestión del proyecto

- **Integración interna (en el equipo):** mecanismos de comunicación y control, jefatura experimentada, trabajo conjunto anterior, reuniones, actas, revisiones técnicas, participación en objetivos, asistencia externa
- **Integración externa (con los clientes-usuarios):** comunicación en varios niveles (dirección de proyecto y comité conjunto, reuniones, actas); autoformación, autoinstalación; participación en: los cambios, el equipo del proyecto, decisión de fechas clave, proceso de aprobación
- **Planificación formal:** estimación previa de secuencias-recursos (gant factibilidad, hitos, normas, aprobación, auditoría) + **Control formal de resultados:** mecanismos de estima del progreso y no conformidades; acciones correctoras a tiempo (informes, disciplinas de control de cambios, reuniones en los hitos, informes de desvíos al plan).

# Modelo McFarlan G2 de gestión de riesgos

## Salvaguardas de gestión para los factores subjetivos de riesgo

### Combinación de los factores

Inexperiencia.tecnológica / Desestructuración	0/0	0/1	1/0	1/1
Salvaguardas				
- Integración externa (con clientes):	0	1	0	1
- Integración interna (equipo):	0	0	1	1
- Planificación/Control:	0	0	1	1

### Proyecto con:

inexperiencia/ desestructuración baja/ baja	0/0
⇒ permite: equipo no experimentado (0); planificación+control fácil (0)	
inexperiencia/ desestructuración baja/ alta	0/1
⇒ exige: gestión agresiva para integrar usuario (1); planif+contr.fácil (0)	
inexperiencia/ desestructuración alta/ baja	1/0
⇒ exige: liderazgo e integración en el equipo (1); planif+contr.difícil (1)	
inexperiencia/ desestructuración alta/ alta	1/1
⇒ exige: liderazgo e integración en el equipo (1); colchón de recursos	

# Modelo McFarlan G2 de gestión de riesgos

---

## Perfil de riesgos en la cartera de proyectos de una entidad

**El riesgo global está en relación con la estrategia de negocio**

- **En las entidades que usan las TI estratégicamente:  
(visión del riesgo visto como oportunidad)**
  - cartera de riesgo bajo => poca ventaja competitiva
  - cartera de riesgo alto => disruptpciones potenciales del negocio
- **En las entidades que usan las TI sólo de ‘soporte’ del negocio**
  - cartera de riesgo bajo => el equipo se desentrena y aburre
  - cartera de riesgo alto => crece el riesgo de inversión

**La Cultura corporativa de la entidad influye en la visión del riesgo**

# Primeros pasos de la Generación Tercera G3

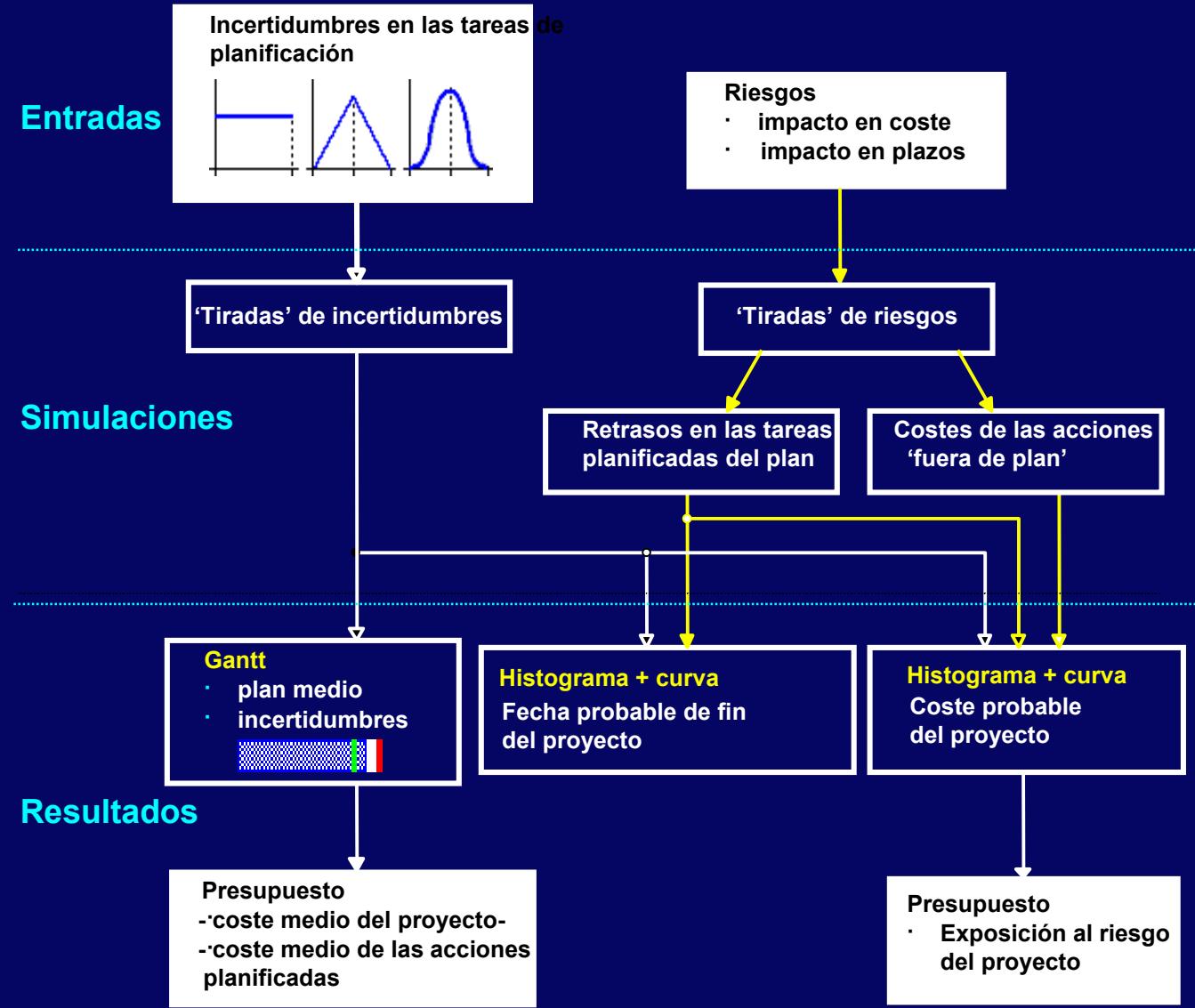
---

- **Modelo RiskMan e iniciativa RiskDriver**
- **Modelo DriveSPI**
- **Modelo Eurométodo**
- **Modelo ISPL**
- **Modelo PRisk**

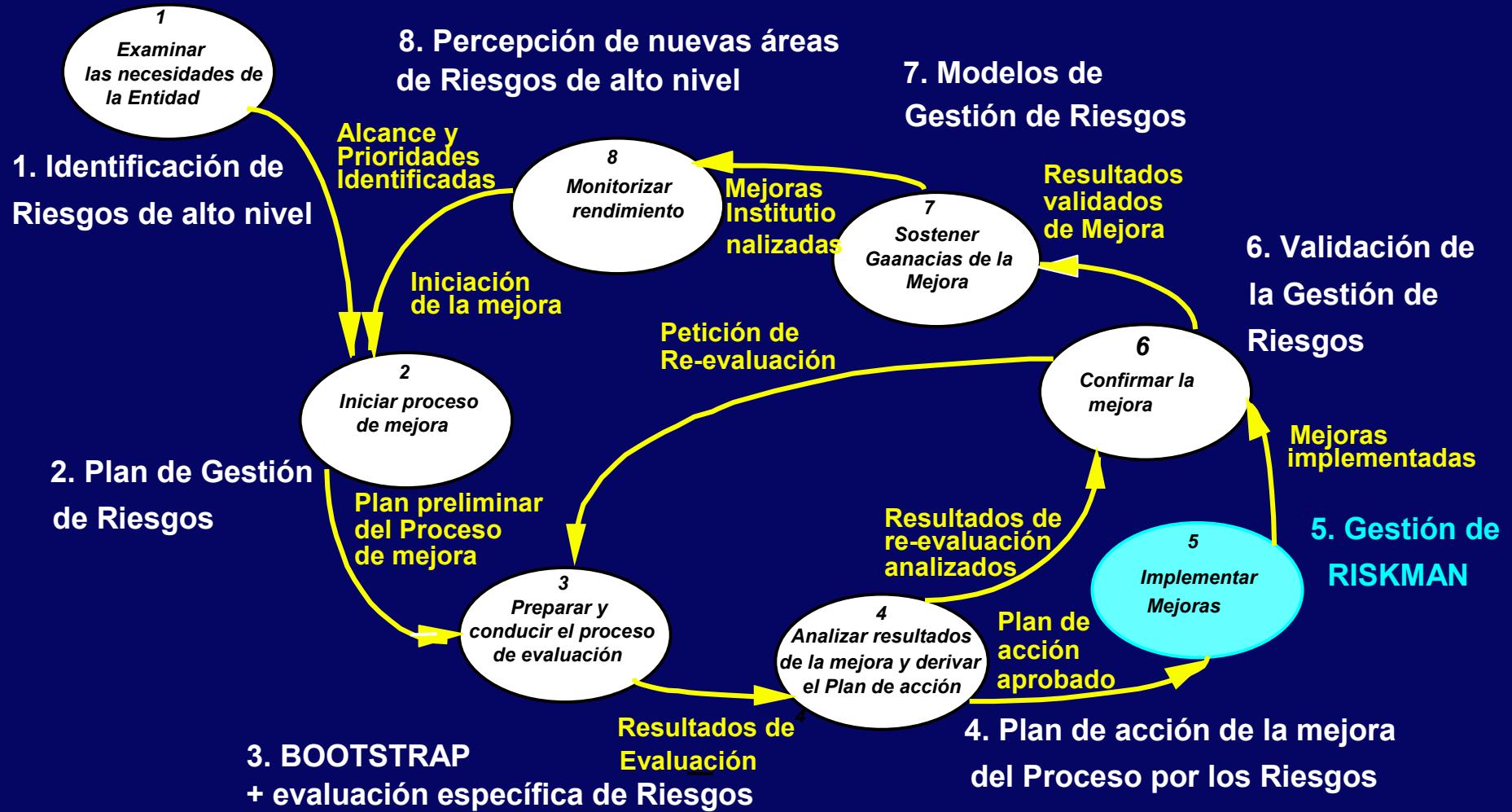
# Modelo RiskMan e iniciativa RiskDriver

## Modelo RiskMan (programa Eureka) +Iniciativa RiskDriver

Tras las Etapas de Identificación y Evaluación de los riesgos (con técnicas clásicas), se simulan varios planes para organizar la mejor generación inicial de medidas y el control mejor de los riesgos durante el desarrollo del proyecto.



# Modelo DriveSPI



# Modelo Eurométodo G3 de gestión de riesgos

Eurométodo clasifica 39 Factores de riesgo en 2 dimensiones:

- **Dos Dominios:** Dominio Objetivo; Dominio del Proyecto
- **Dos 'megafactores' de riesgo** Complejidad; Incertidumbre
- **39 Factores de riesgo:** Factores de Complejidad 16  
Factores de incertidumbre 23

- 24 del dominio objetivo:

Sistema de Información

5 12

Subsistema Informático

5 2

- 15 del dominio de proyecto: tareas

2 3

estructura

2 3

actores

1 1

tecnología

1 2

- Heurística

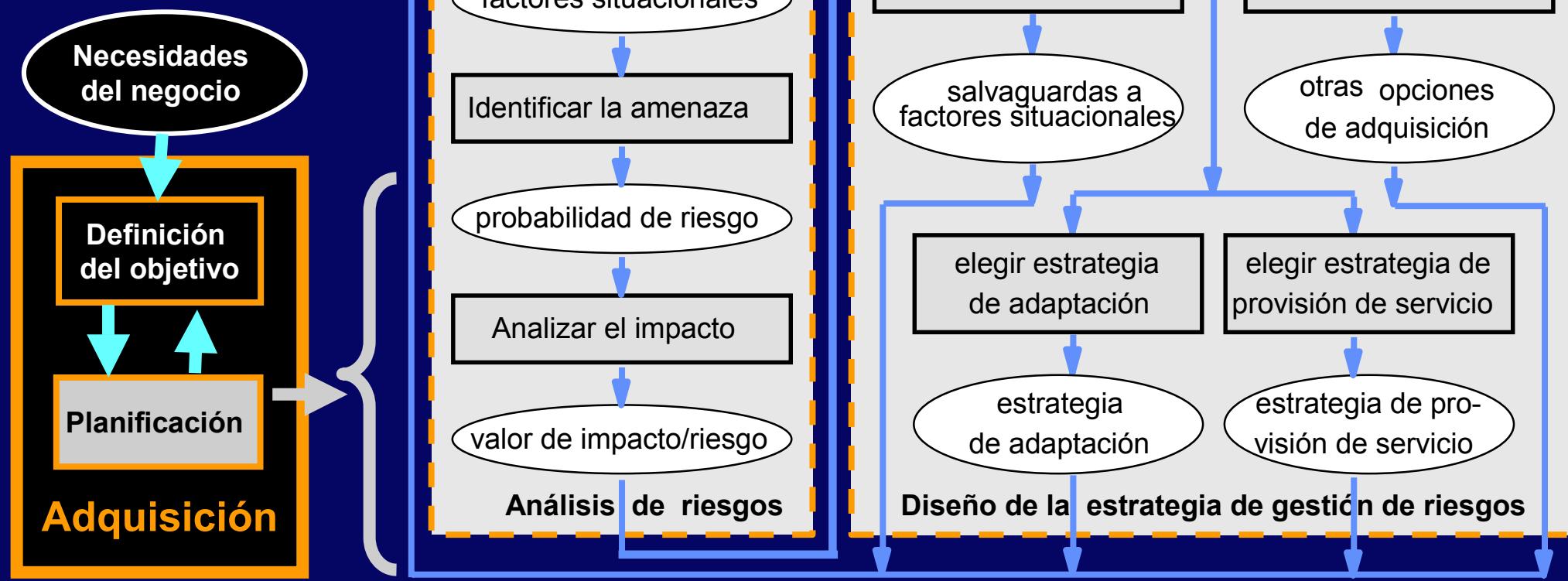


- **Gestión de Riesgos:** se compone de:

- **Análisis de riesgos;**
- **Planificación de la Gestión de Riesgos** (estrategia de desarrollo y propuesta de hitos de decisión);
- **Supervisión de riesgos** (mide si las salvaguardas tienen éxito)

# Modelo Eurométodo G3 de gestión de riesgos

## Submodelo Eurométodo de procesos



# Modelo Eurométodo G3 de gestión de riesgos

---

## 4 bloques de Medidas de Salvaguarda

### 1 Medidas específicas para factores de complejidad:

- reducir la vulnerabilidad de cada factor (dominio Objetivo)

### 2 Medidas específicas para factores de incertidumbre:

- usar la tabla que relaciona los factores con 16 riesgos -a reducir-
- cambiar 6 factores incertidumbre individuales (5 + Sistema Informático)

### 3 Medidas generales de Control del proyecto

- En cada área de trabajo (*desarrollo, calidad, configuración*), 3 opciones según *frecuencia, formalización, responsabilidad de cliente*

### 4 Medidas globales en enfoques-hitos-recursos del plan de entregas

- En Construcción e Instalación según *complejidad, incertidumbre y plazos rígidos*
  - Opción de una vez, sólo si incertidumbre baja y complejidad baja/moderada
  - Opción incremental si sube la complejidad y se reducen los plazos
  - Opción evolutiva para incertidumbre alta, plazos reducidos y muchos cambios
- En Descripción del Sistema: combina *modo de operación* (analítica/experimental) *con cooperación entre actores* (guiada-por-expertos/ participativa). Es descripción
  - Analítica + guiada por los expertos si hay complejidad alta en la información de los procesos (con plazos duros y actores heterogéneos)
  - Experimental + participativa si incertidumbre alta
  - Experimental + guiada por los expertos si la participativa no es factible

# Modelo ISPL G3 de gestión de riesgos de los servicios

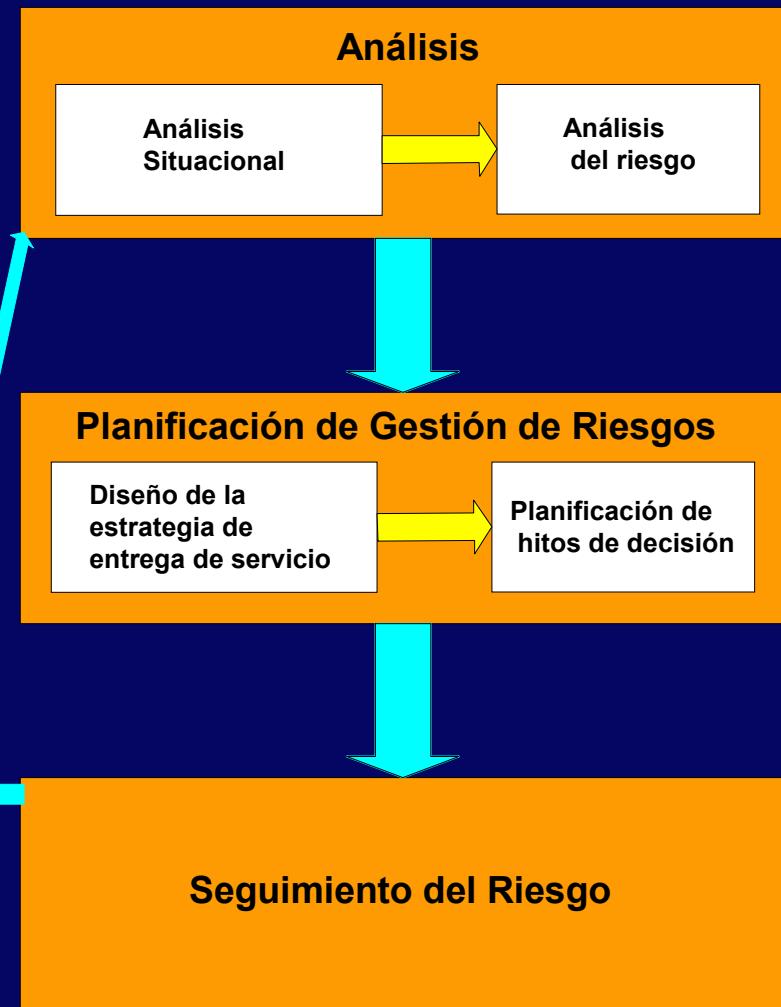
## Submodelo ISPL de procesos

### Tipos de Servicio:

- servicio continuado
- proyecto

### Desarrollo de un Servicio:

- instalación del servicio (*proyecto*)
- ejecución del servicio (*s. continuado*)
- retirada del servicio (*proyecto*)



# Modelo ISPL G3 de gestión de riesgos de los servicios

## Submodelo ISPL de componentes

### Entregables

#### 1. Del Contrato

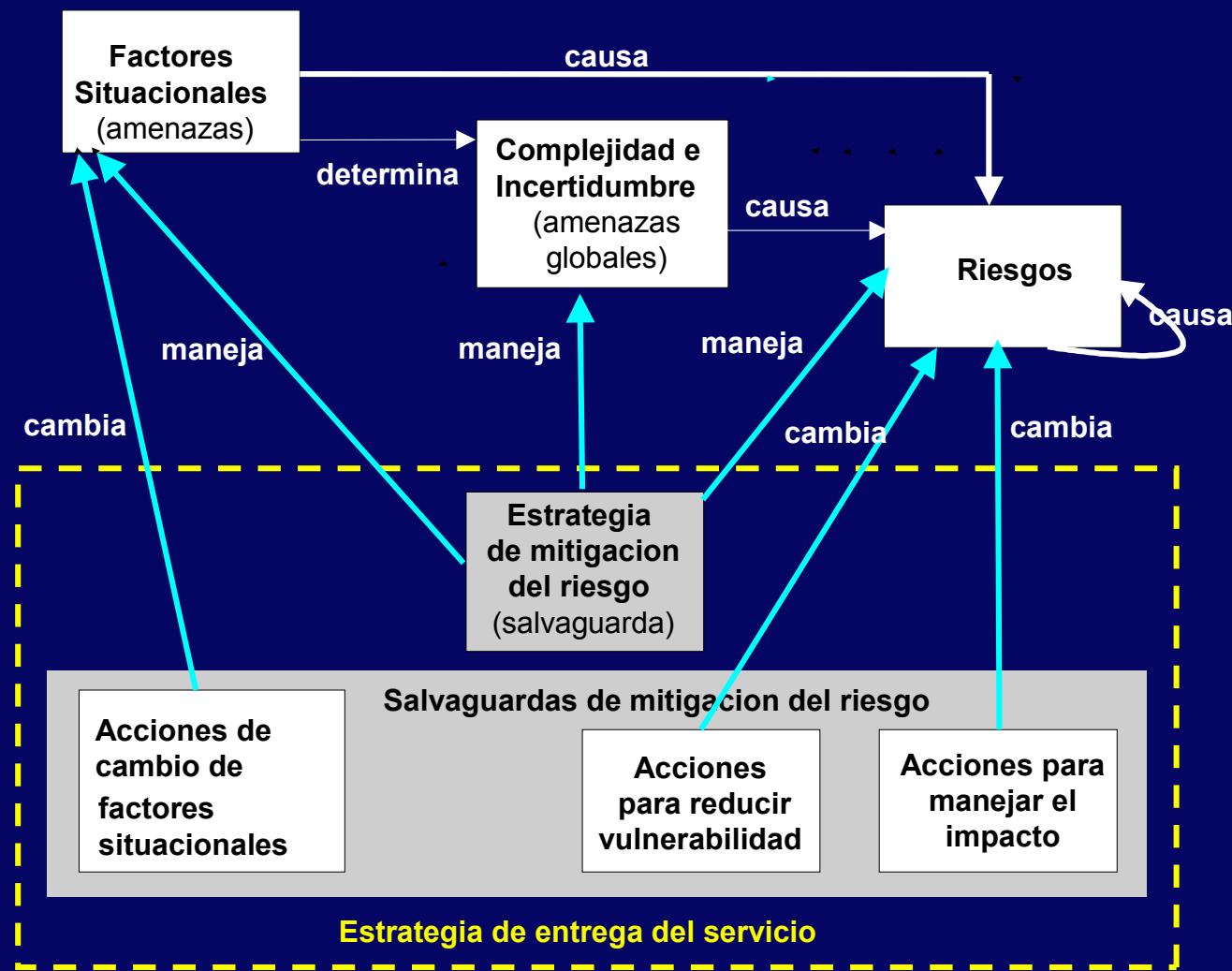
- de la licitación
- de los hitos de decisión

#### 2. De Gestión del Servicio

- Plan
- Informe

#### 3. Del Objeto del Servicio

- producto descriptivo
- producto operacional



# Modelo PRisk de gestión del proyecto por sus riesgos

---

## PRISK, modelo nuclear para gestión de proyectos por sus riesgos

- **Ampliado:** incluye fases de oferta y contrato, se orienta al servicio y se vincula a métodos de estimación (temprana, FPÁ, PFOO)
- **Bilateral:** recoge los intereses de las partes: cliente, proveedor, subcontratista
- **Completo:** con cálculo de riesgo para clasificar los críticos y con causalidad amenazas-medidas para incrustar en el plan las preventivas y revisar los hitos

**PRISK actúa a lo largo de todo el proyecto, en sus Fases de:**

- Planificación pro-activa (sus acciones de salvaguarda previenen los riesgos)
- Seguimiento re-activo (sus acciones de salvaguarda curan los riesgos)
- Acabado, recogiendo métricas y parámetros para proyectos sucesivos

**En PRISK la aplicación de medidas se atiene al tipo de riesgo; p.ej.:**

- Si es '**3 I**' -**Intencional, Inteligente, Interno-** (~ factores de riesgo) el proveedor toma medidas de gestión en el marco del cliente y de la situación del proyecto.

**La aplicación de PRISK hace en cada Riesgo un Control '3 R'**

- **Residual**, llevado bajo un umbral definido, pero sin descuidar su control;
- **Repetido**, mientras haya causas fuera del control del Jefe de proyecto;
- **Registrado**, como traza y para aprendizaje del proyecto para los sucesivos.

# Modelo PRisk de gestión del proyecto por sus riesgos

## Interpretación de la Complejidad del Sistema S y la Incertidumbre del entorno E

La estructura del ecosistema ES se describe por el triplete  $\langle S, E, M \rangle$  donde

$S = \{p(s_i)\}$  probabilidades de los estados  $s_i$  del sistema S;

$E = \{p(e_k)\}$  probabilidades de los estados  $e_k$  del entorno E;

$M = \{p(s_i, e_k)\}$  probabilidades de los estados del ecosistema ES

$$p(s_i, e_k) = p(s_i/e_k)p(e_k) = p(e_k/s_i)p(s_i) \geq 0$$

$p(s_i/e_k)$  = probabilidad de que S ocupe  $s_i$  compatible con que E ocupe  $e_k$  (dado).

**Entropía** de un conjunto de n probabilidades:  $H[p(i)] = - \sum_n p(i) \log_2 p(i)$  en bits

**Complejidad de S** = entropía de su estructura (estados) que mide la 'alcanzabilidad' de sus alternativas:  $H[S] = - \sum_n p(s_i) \log_2 p(s_i)$

**Incertidumbre de E** = entropía de su estructura  $H[E] = - \sum_m p(e_k) \log_2 p(e_k)$

La complejidad de S u la incertidumbre de E se relacionan en su frontera.

**Entropía H del S para un estado ej de E:**  $H[S/E=e_j] = - \sum_n p(s_i/e_j) \log_2 p(s_i/e_j)$

**H media para los  $e_k$ :**  $H[S/E] = \sum_m p(e_k) H[S/E=e_k] = - \sum_{nm} p(s_i, e_k) p(e_k) \log_2 p(s_i/e_k)$  = diversidad de alternativas de S condicionadas por una incertidumbre dada de E.

$H[E/S] =$  diversidad simétrica de alternativas de E =  $- \sum_{mn} p(e_k/s_i) p(s_i) \log_2 p(e_k/s_i)$ .

# Modelo PRisk de gestión del proyecto por sus riesgos

Visión dual del conjunto (Entorno.Sistema) y del megasistema ES (Ecosistema)

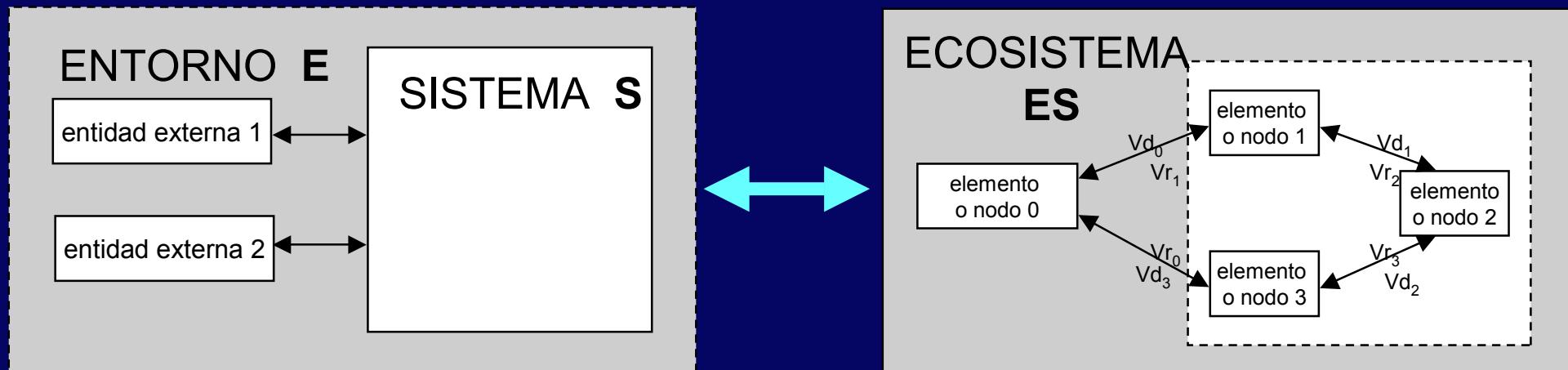
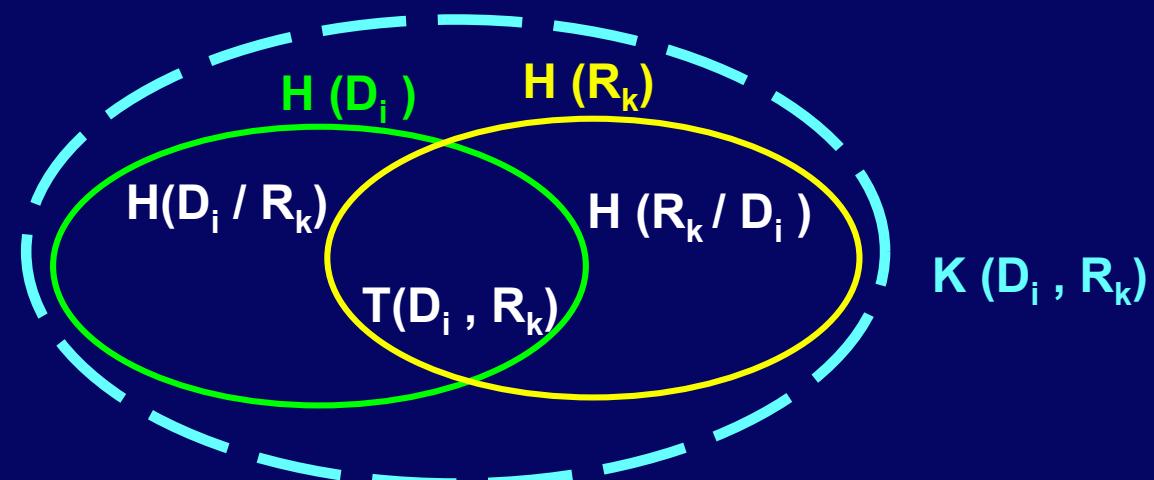


Diagrama de Venn para relacionar  
- las Entropías H,  
- la Transmisión T  
- y la Conectividad K



# Modelo PRisk de gestión del proyecto por sus riesgos

---

## Evolución, adaptación y estrategia de 'supervivencia' (modelo ecobiológico)

- Todas las ecuaciones expresan sólo propiedades estadísticas de ES, S o E, independientes de la **megacomplejidad de ES** (**complejidad de S + incertidumbre de E**)
- La interacción entre S y E se transmite por un 'canal virtual' matriz de probabilidades condicionales  $\{p(s_i|e_k)\}$ : una 'actividad informacional'  $s_i$  se manifiesta en S siempre que E 'emite' la actividad  $e_k$  = capacidad de S para percibir que pasa en E y responder
- La posibilidad de adaptación de S al E es la estabilidad de las estructuras de S y E en un esquema M de modificación, dada por el E con mayor incertidumbre donde S sobreviviría indefinidamente (haciendo  $\text{Max } H[E]$  con todos los posibles M):

$$T[E,S] = H[E] - H[E/S] = H[S] = H[S/E] = T[S,E] \text{ se convierte en } H[E] = \max\{T[E,S] + H[E/S]\}$$

Este 'intervalo de seguridad' de la capacidad de S para soportar la incertidumbre de E mide la adaptabilidad de S. Se demuestra que la **maximización de  $H[E,S]$**  lleva a una estabilidad del ES así 'adaptado' con una 'micro-entropía' > la 'macro-entropía'  $H[S]$ .

- La adaptación 'interna' de S es la tendencia a predecir y conseguir su complejidad más probable, compatible con un E dado (asignando las probabilidades estructurales que hagan  $\text{Max } H[S]$  (**base de una teoría de la evolución de los sistemas complejos**)). **Complejidad de S + su poder de anticipación sobre E = incertidumbre de E + impacto de S sobre E.** Para que una catástrofe imprevisible (desviación de la incertidumbre de E) no haga peligrar la complejidad de S, S evoluciona buscando la independencia de E. Pero no se aisla: aumenta su poder de anticipación y/o reduce su impacto sobre E.

# Modelo PRisk de gestión del proyecto por sus riesgos

