Metodologías para la implantación de SGSI

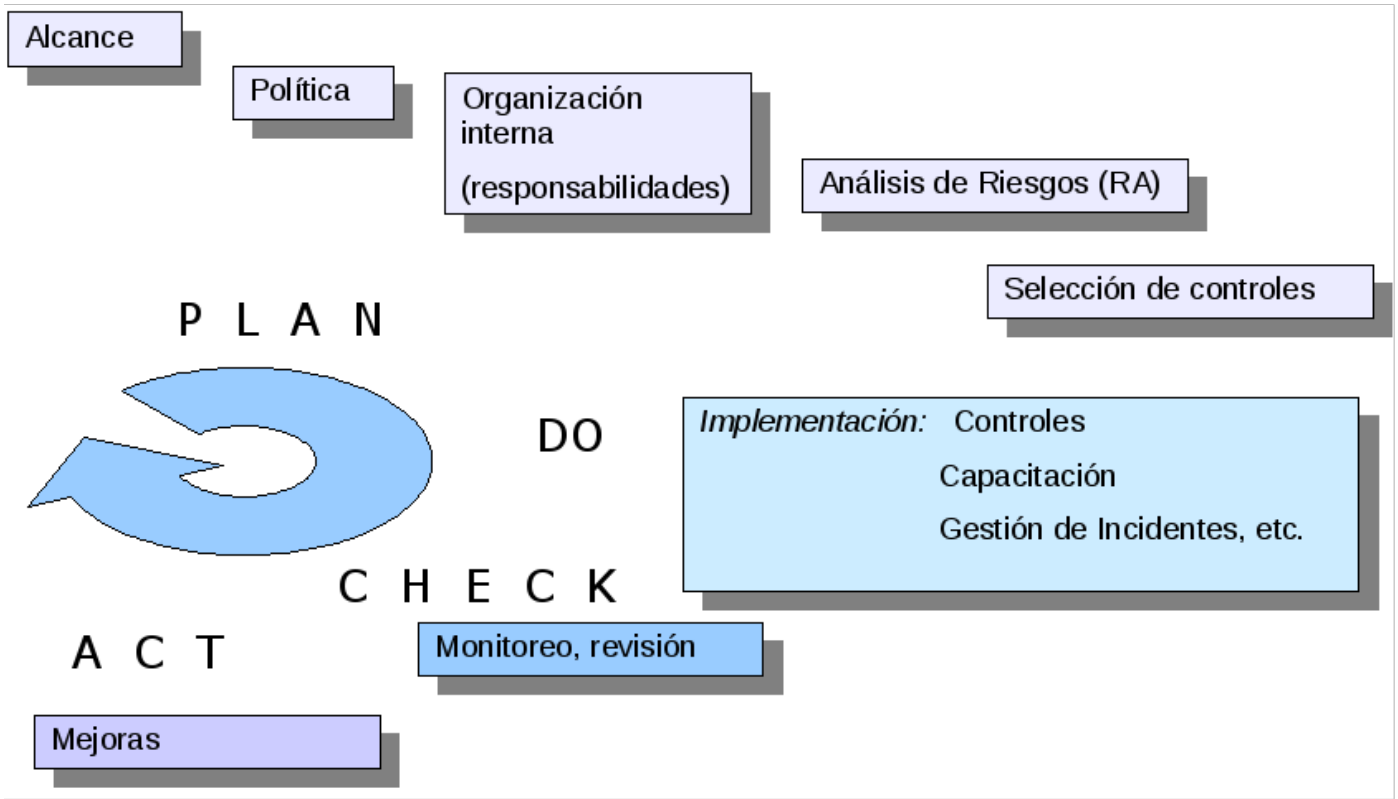
María Eugenia Corti

Grupo de Seguridad Informática
Instituto de Computación
Facultad de Ingeniería - UdelaR
mcorti@fing.edu.uy

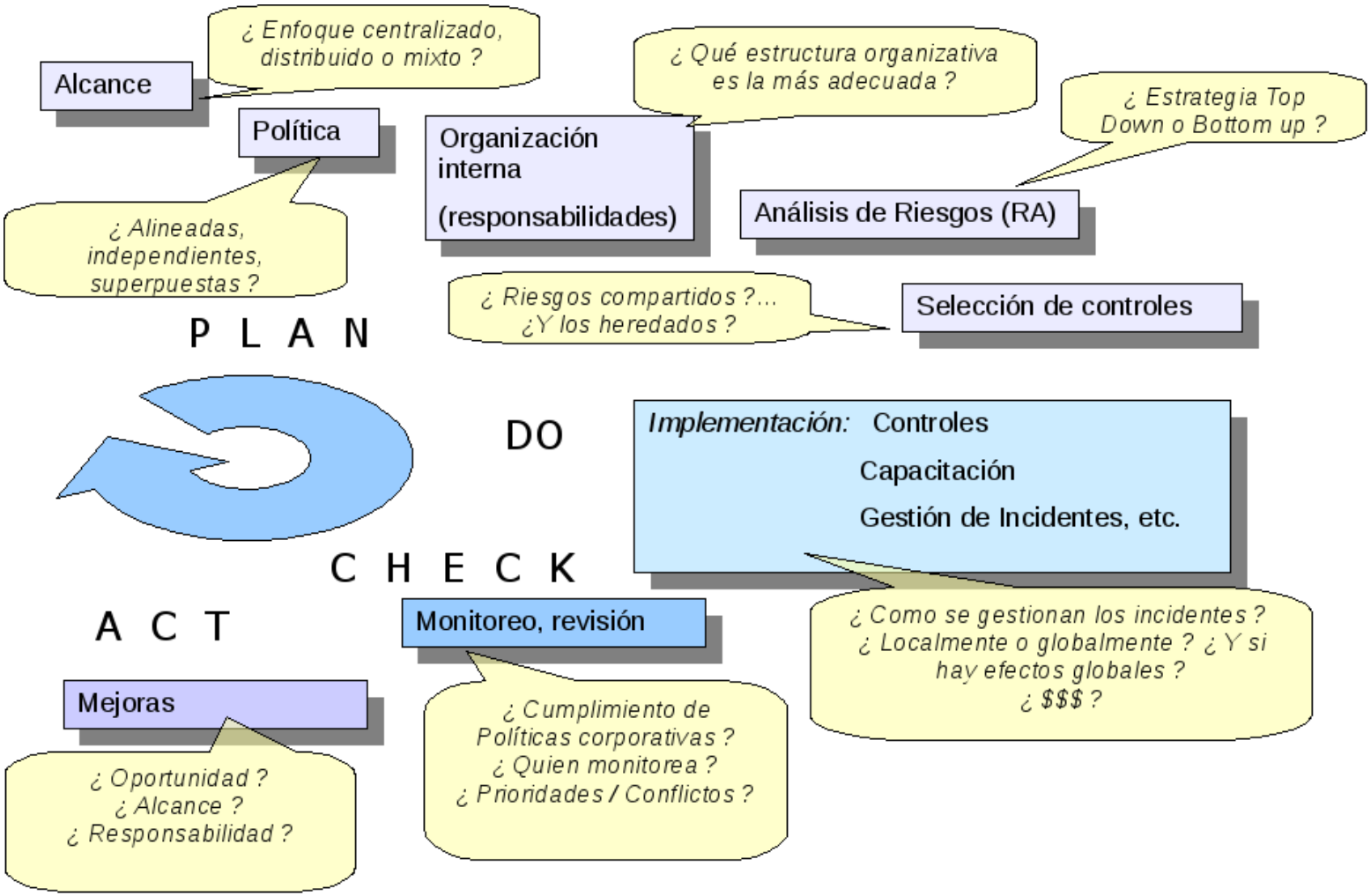
24/06/2010

Contenido

Motivación

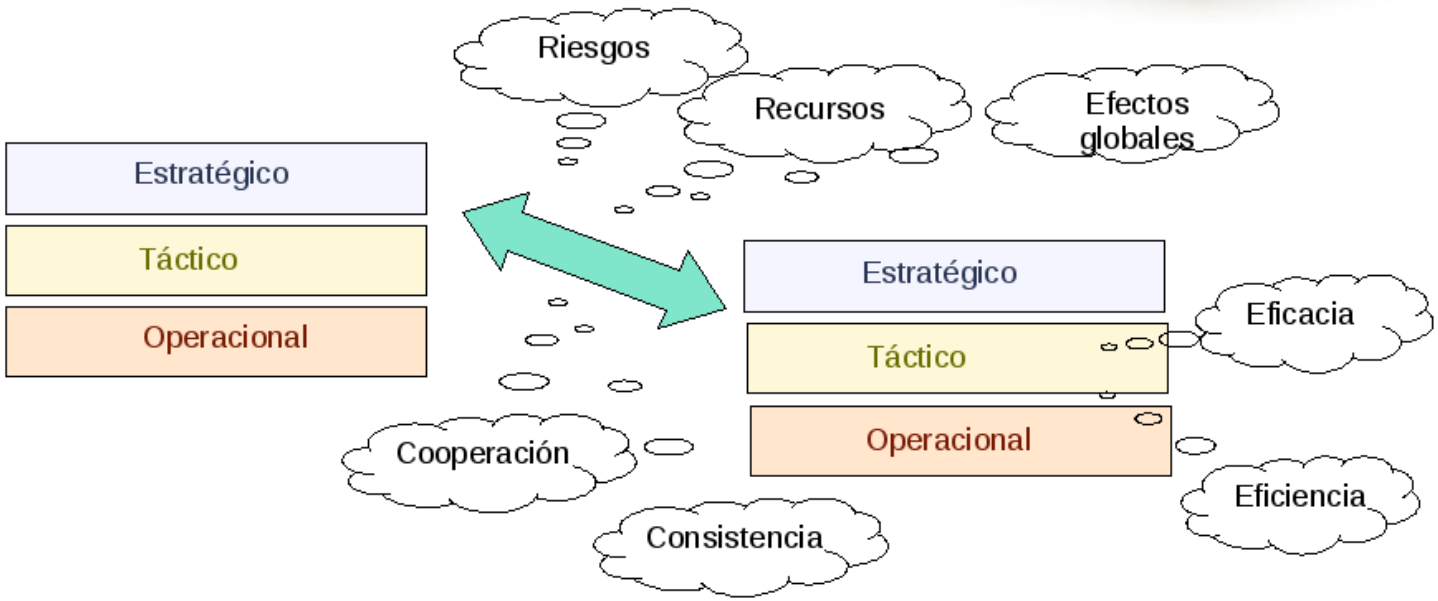

Alcance
Política
Organización interna
(responsabilidades)
Análisis de Riesgos (RA)
Selección de controles
P L A N
DO
Implementación: Controles
Capacitación
Gestión de Incidentes, etc.
C H E C K
A C T
Monitoreo, revisión
Mejoras

Motivación

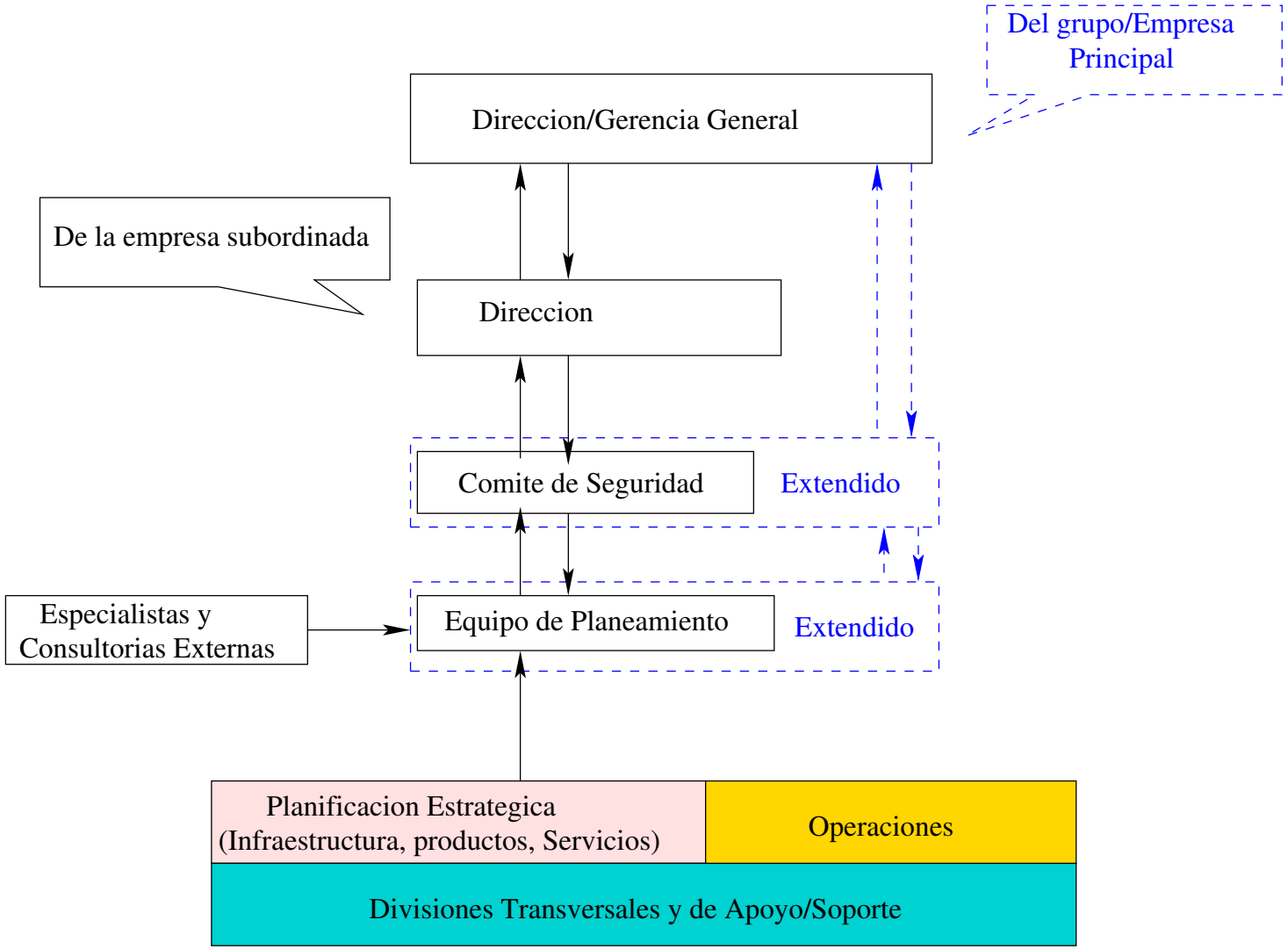

Alcance
¿ Enfoque centralizado, distribuido o mixto ?
Política
¿ Alineadas, independientes, superpuestas ?
Organización interna (responsabilidades)
¿ Qué estructura organizativa es la más adecuada ?
Análisis de Riesgos (RA)
¿ Estrategia Top Down o Bottom up ?
¿ Riesgos compartidos ?... ¿Y los heredados ?
Selección de controles
P L A N
DO
Implementación: Controles
Capacitación
Gestión de Incidentes, etc.
¿ Como se gestionan los incidentes ? ¿ Localmente o globalmente ? ¿ Y si hay efectos globales ? ¿ $$$?
C H E C K
Monitoreo, revisión
¿ Cumplimiento de Políticas corporativas ? ¿ Quien monitorea ? ¿ Prioridades / Conflictos ?
A C T
Mejoras
¿ Oportunidad ? ¿ Alcance ? ¿ Responsabilidad ?

Enfoque

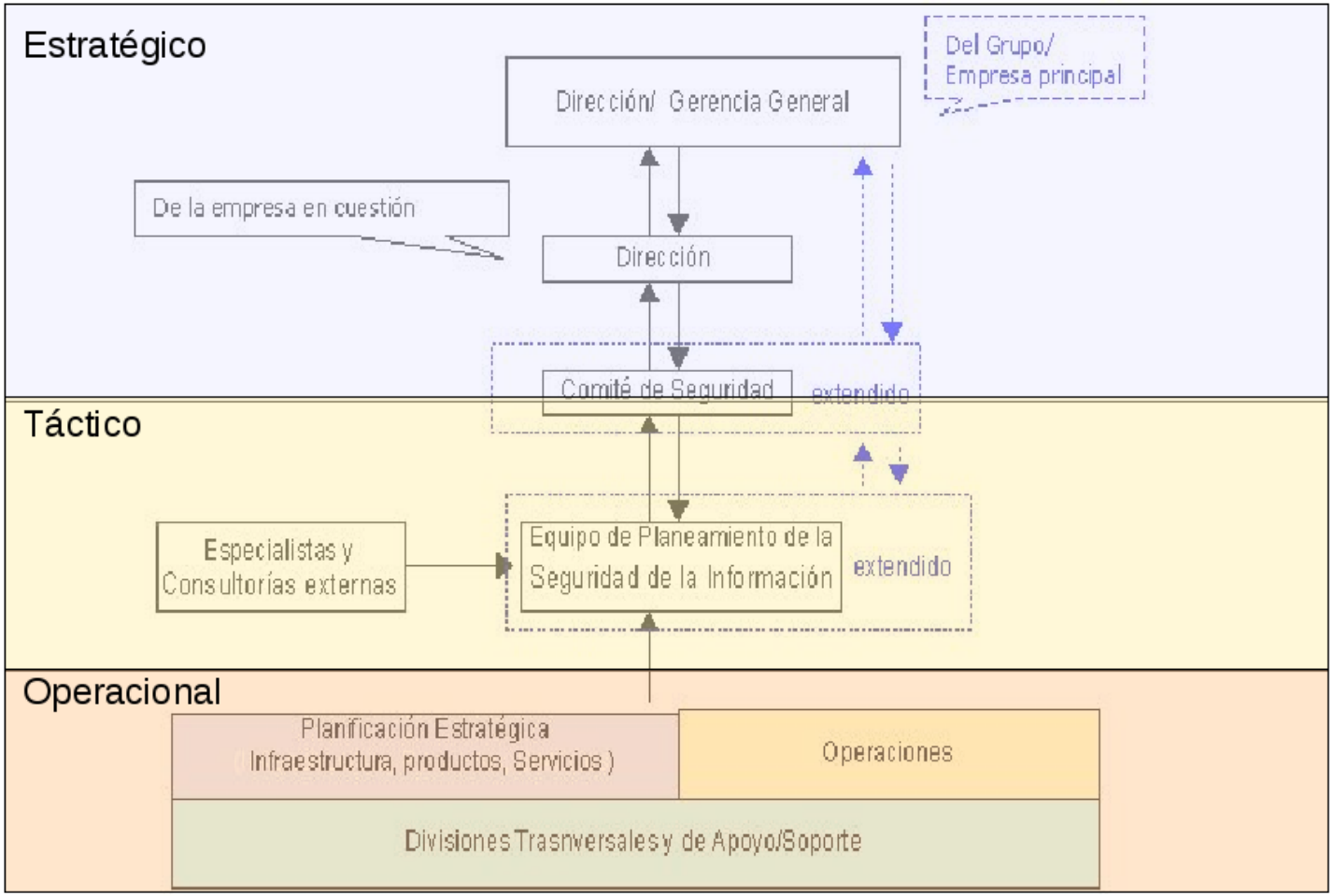
- Mixto: SGSI relacionados e integrados con autonomía operativa
- Sistémico
- Diferentes capas de abstracción



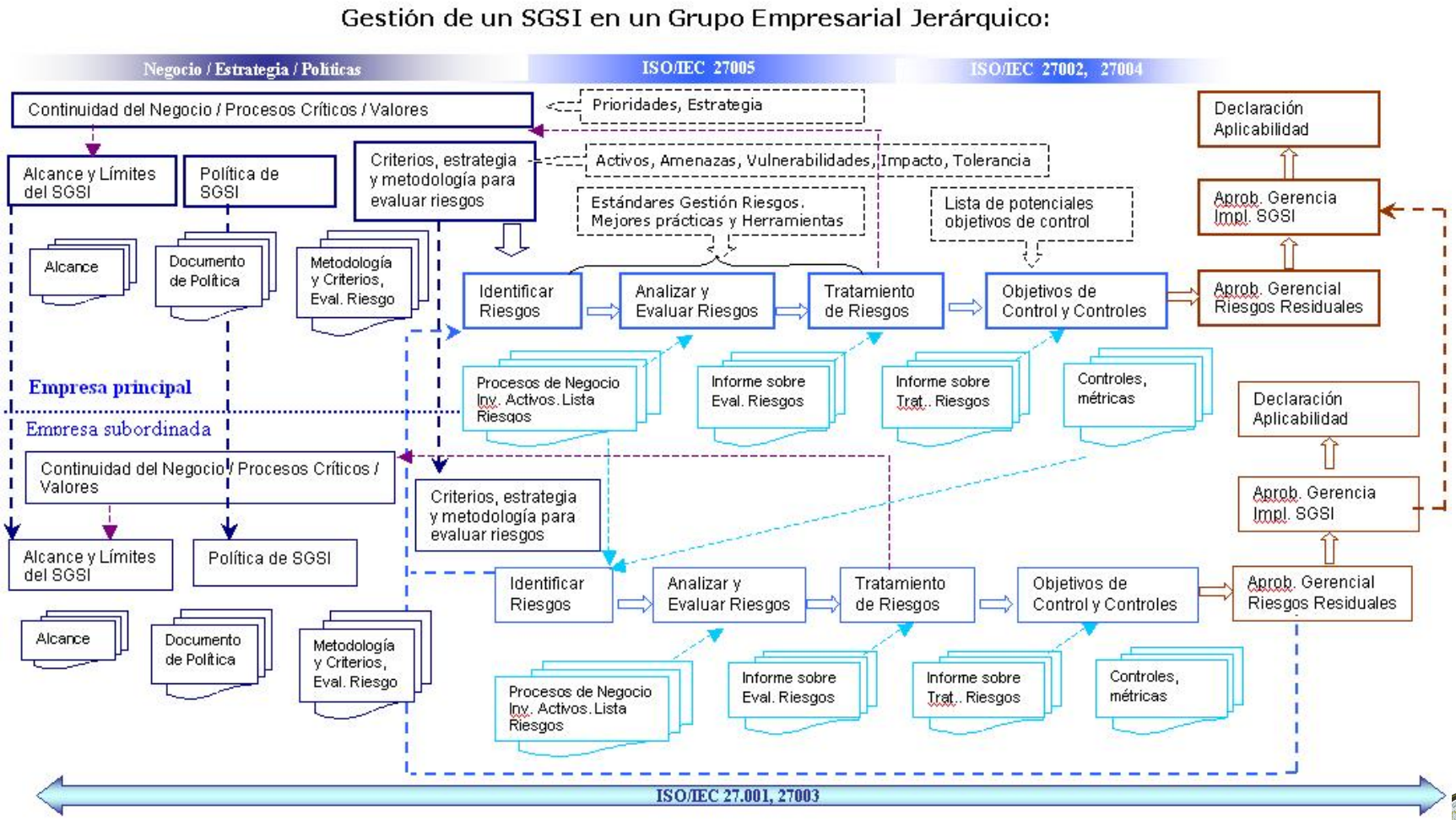
Organigrama de Seguridad



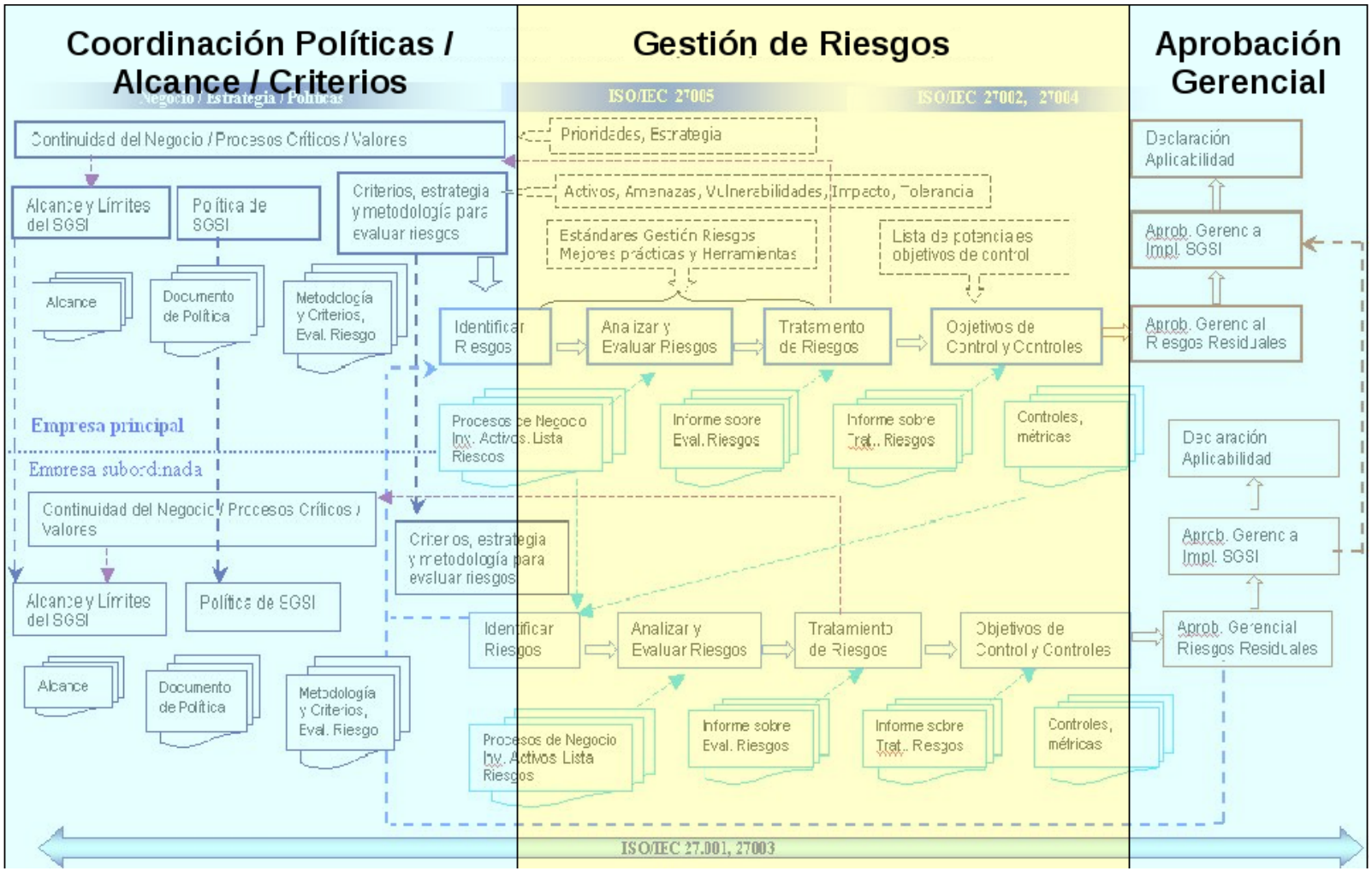
Organigrama de Seguridad



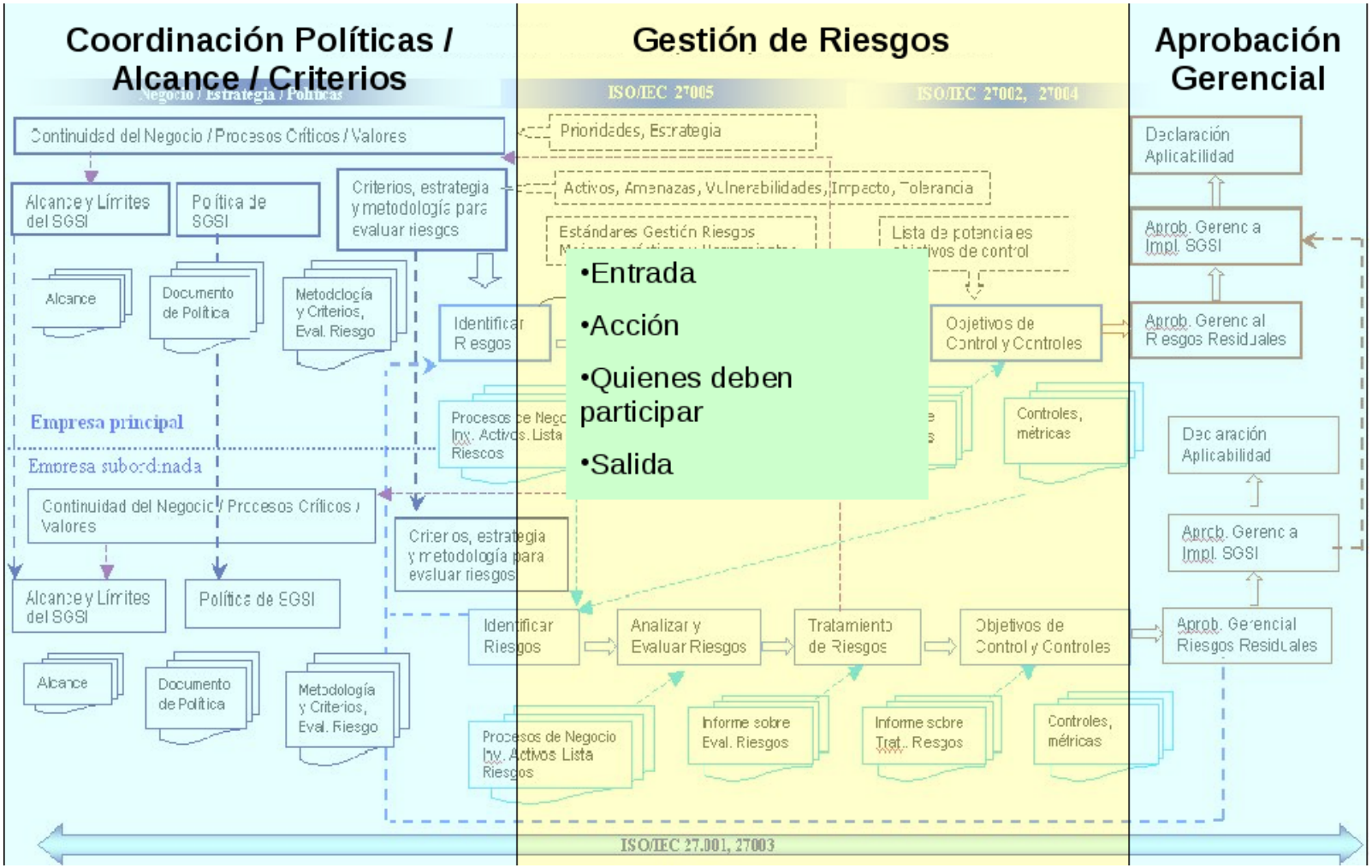
Síntesis Gráfica



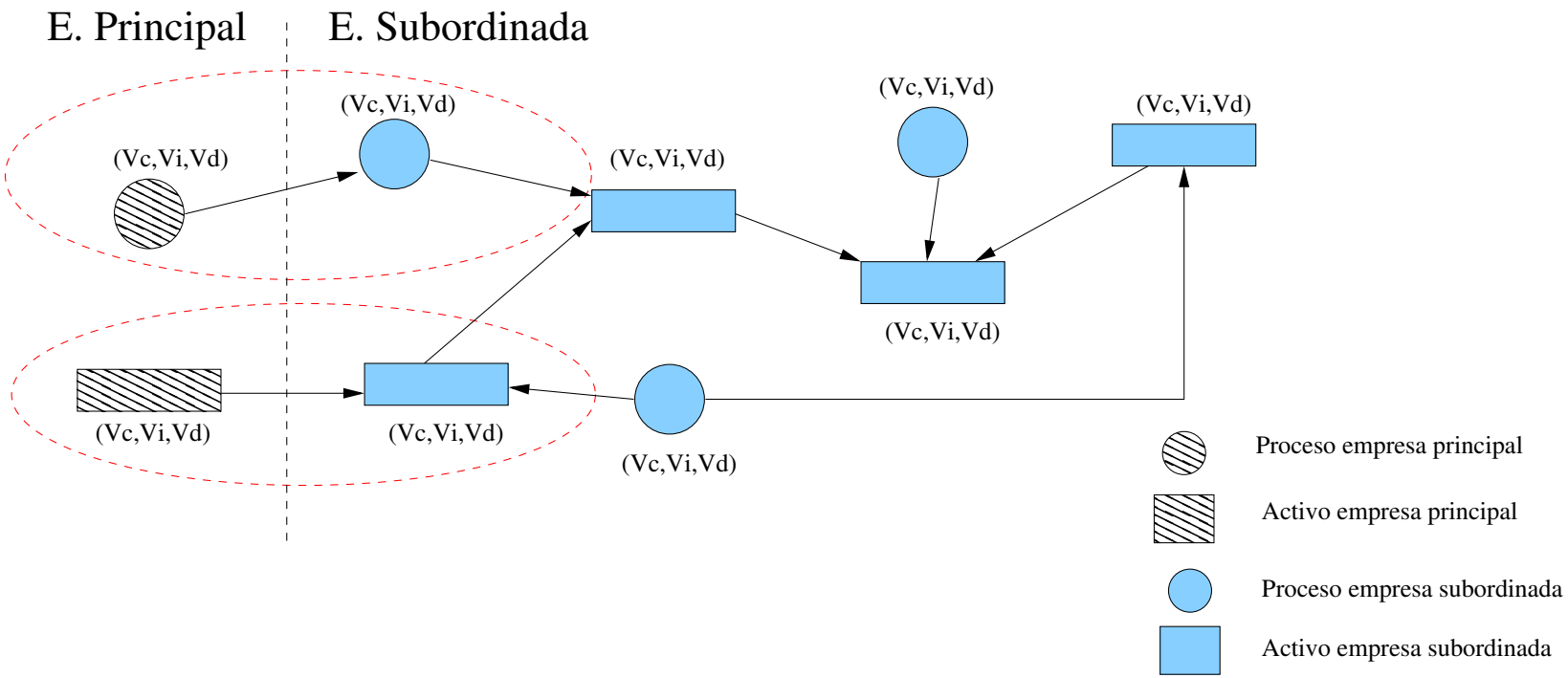
Síntesis Gráfica



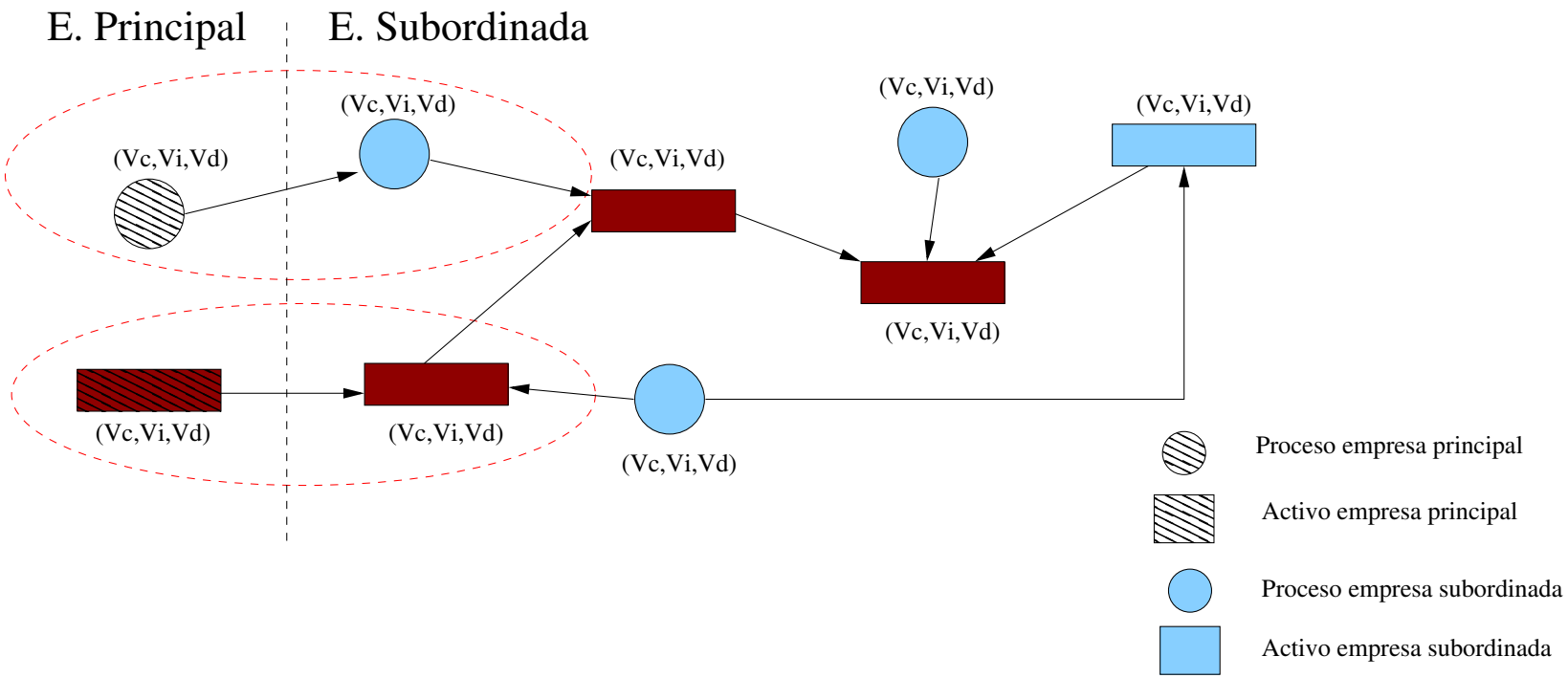
Síntesis Gráfica



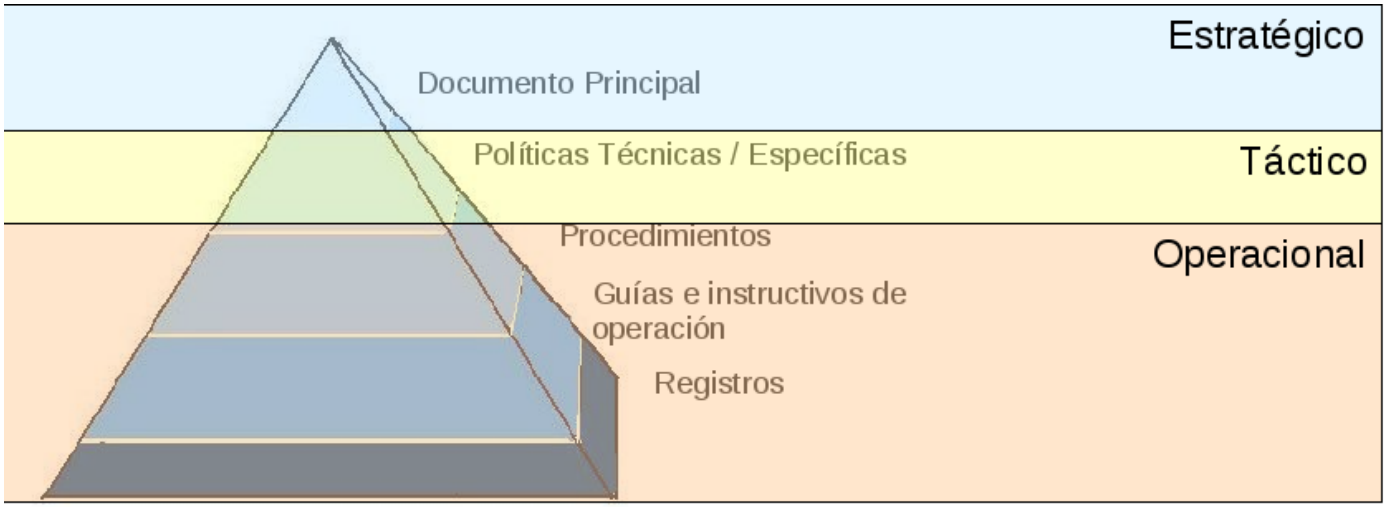
Grafo de Valoración y Dependencia de Activos



Grafo de Valoración y Dependencia de Activos



Documentación



- Facilita la comprensión, y la abstracción de los detalles técnicos y operativos.
- Separaración de los conceptos medulares de detalles de implementación
- Mantenibilidad.
- Facilita la integración. Documento principal será común (corporativo), o una extensión.
- Flexibilidad para la definición de políticas específicas y locales

Propuesta de Software de Apoyo

- `Workflow:` que comprenda la naturaleza jerárquica del grupo empresarial
- Vistas o capas de abstracción
- Gestión de roles
- Gestión de riesgos: `Top Down` con intervenciones `Bottom Up`
- Gestión de documentación
- Valoración de activos y dependencia (grafos)
- Gestión de dependencias inter-empresariales
- Revaloraciones

Conclusiones

- Una estructura empresarial compleja requiere de una metodología de implantación específica
- Enfoque sistémico, con dirección jerárquica y gerenciamiento distribuido
- Gestión en diferentes niveles: Estratégico, Táctico y Operacional
- Mecanismos de comunicación y cooperación bien definidos para cada fase de la implantación y mantenimiento
- Estructura organizacional de Seguridad de la Información
- Software de apoyo facilita la implantación
- Metodología propuesta conforme a la ISO/IEC 27001

Trabajo Futuro

- Validación de la metodología. Confirmación experimental.
- Especificación y desarrollo del software sugerido

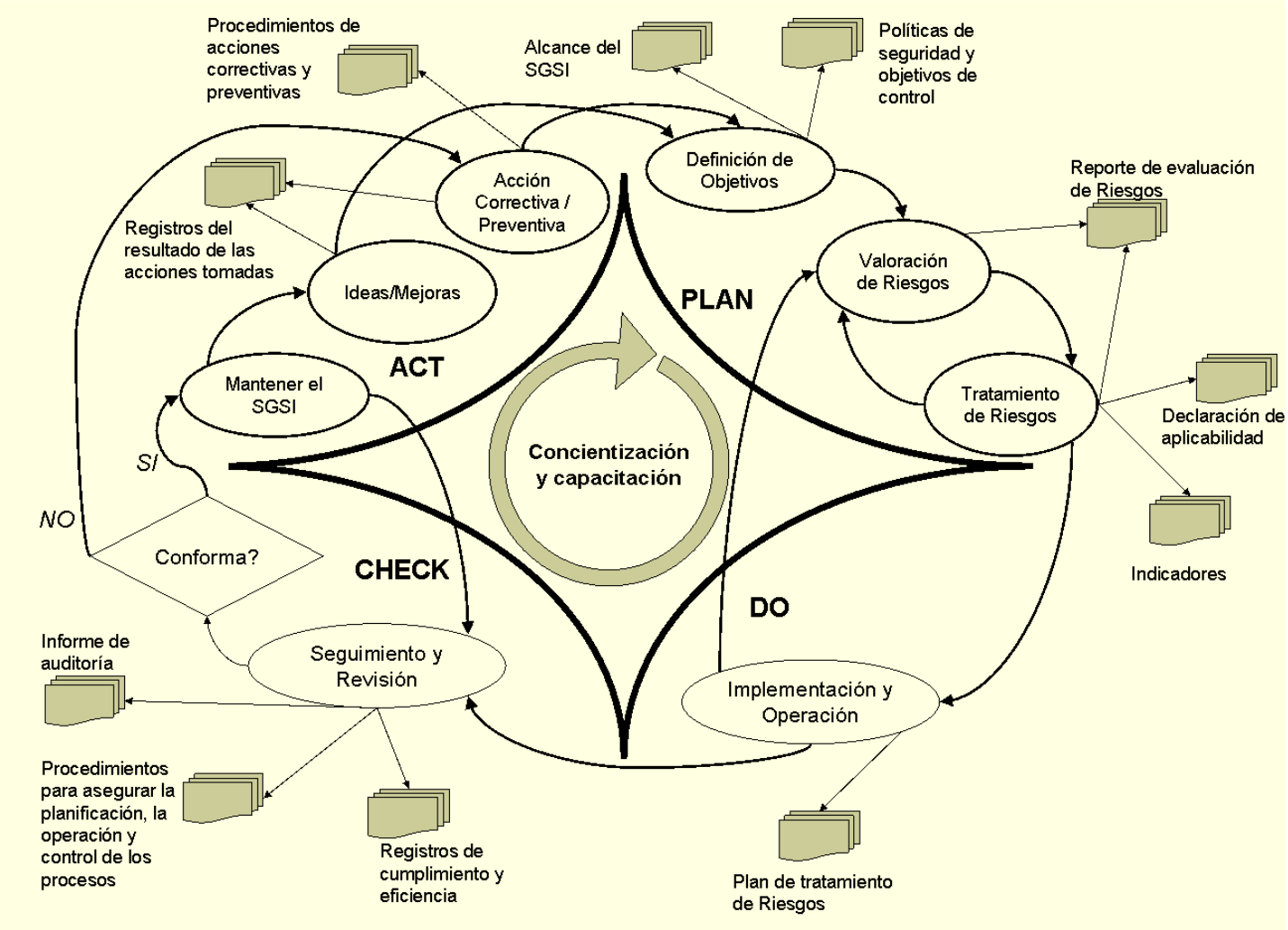
Motivación

- Contribuir a la elaboración de herramientas y metodologías que faciliten la implementación y mejora continua de SGSI
- Identificar metodologías y procedimientos adecuados a las características de las PyMEs uruguayas
- Cubrir organizaciones carentes de metodologías o prácticas de seguridad específicos o generales
- Especificación de requerimientos de software para una herramienta de automatización de la implantación y mejora continua de SGSI

Características de las PyMEs

- Estructura organizacional jerárquica poco compleja
- Infraestructura informática de pocos recursos y desactualizada
- 67 % del software no legalizado
- Pocos recursos humanos dedicados
- Conectadas a Internet
- Nivel de seguridad de la información nulo o mínimo

Síntesis Gráfica



Etapa de Planificación

- Definir el alcance del SGSI
- Definir la política del SGSI
- Formación del equipo de trabajo

- Definir método para valoración de riesgos
- Identificar riesgos
- Evaluar riesgos

- Identificar y evaluar opciones
- Selección de controles y objetivos de control
- Definir indicadores

Identificar Activos

- Identificar Categorías
- identificar Propietarios

Categoría	Nombre	Características	Propietario
HW	PT	Puestos de Trabajo	
	SABD	Servidor de Base de Datos	
SW	SisteFact	Sistema de facturación y control de stock	

Identificar Activos

- Identificar Categorías
- identificar Propietarios

Categoría	Nombre	Características	Propietario
HW	PT	Puestos de Trabajo	
	SABD	Servidor de Base de Datos	
SW	SisteFact	Sistema de facturación y control de stock	

- Determinar Dependencias

	SistFact	SistSueldos	SistContab
SUELDOS		X	
PROD	X		X
CLIENTES	X		

Identificar Activos (Cont.)

- Definir Escala

Valor		Criterio
10	muy alto	daño muy grave a la organización
7-9	alto	daño grave a la organización
4-6	medio	daño importante a la organización
1-3	bajo	daño menor a la organización
0	despreciable	irrelevante a los efectos prácticos

Identificar Activos (Cont.)

- Definir Escala

Valor		Criterio
10	muy alto	daño muy grave a la organización
7-9	alto	daño grave a la organización
4-6	medio	daño importante a la organización
1-3	bajo	daño menor a la organización
0	despreciable	irrelevante a los efectos prácticos

- Valorar

Dependencias

Sea SUP(B) = $\{A_i, A_i \rightarrow B\}$
$Valor\_acumulado(B) = max(valor(B), max_i[valor(A_i)])$
$A_i \in SUP(B)$

	Disponibilidad	Integridad	Confidencialidad
SABD	5	6	4
FW-Web	4	4	3

Identificar Amenazas

- Determinar Escala

Frecuencia	**Valor**	**Tasa**	**Escala**
A diario	Muy frecuente	100	4
Mensualmente	Frecuente	10	3
Una vez al año	Normal	1	2
Cada varios años	Poco frecuente	1/10	1

Identificar Amenazas

- Determinar Escala

Frecuencia	**Valor**	**Tasa**	**Escala**
A diario	Muy frecuente	100	4
Mensualmente	Frecuente	10	3
Una vez al año	Normal	1	2
Cada varios años	Poco frecuente	1/10	1

- Estimar Frecuencia y Degradación

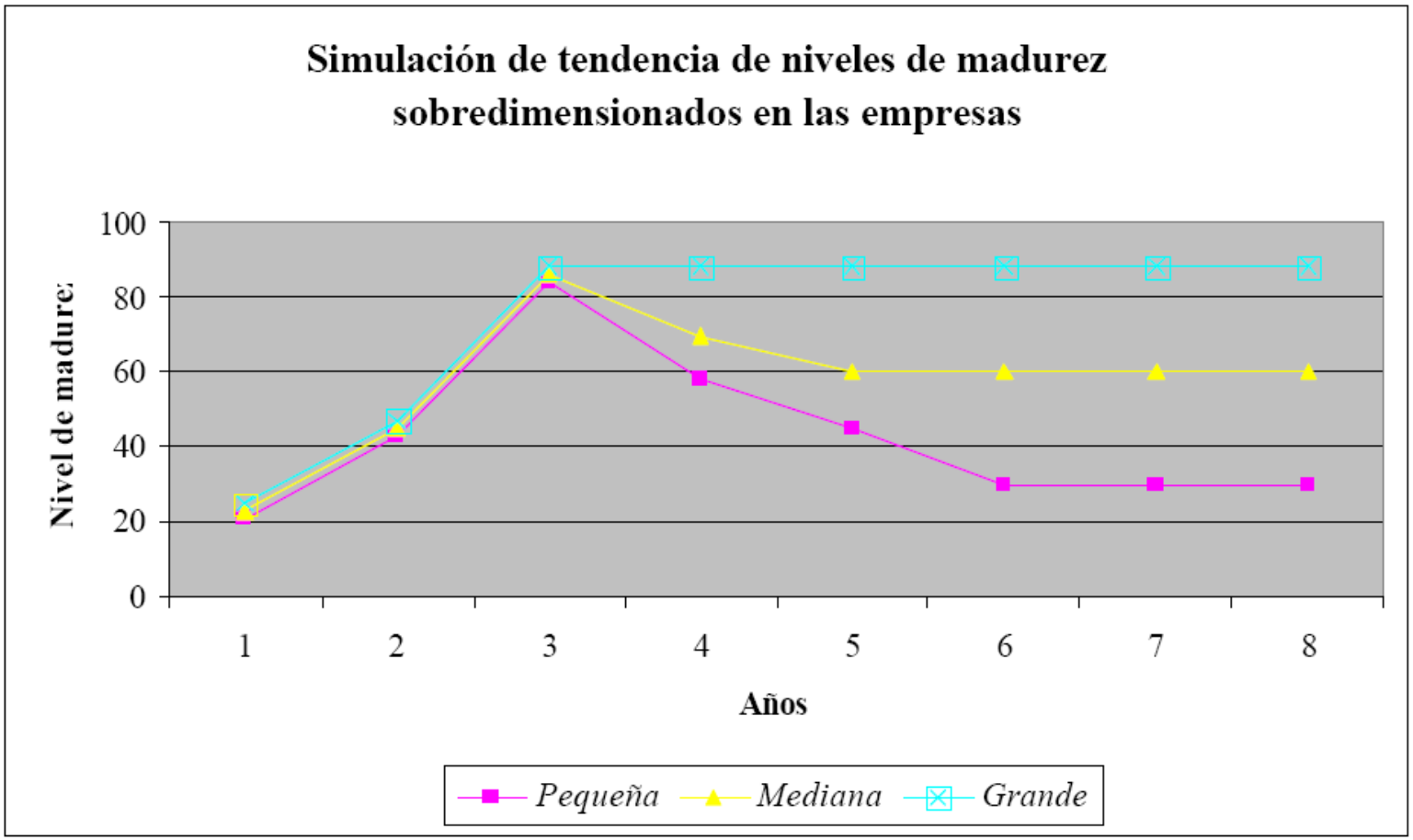
Activo/Categoría	**Amenaza**	**Frecuencia**	**Degradación**		
			Disp.	**Int.**	**Conf.**
HW	Alteraciones eléctricas	3	100 %	50 %	
	Robo	1	100 %		100 %

Evaluar Impacto y Riesgo

- Impacto = valor x degradación
- Riesgo = impacto x probabilidad de ocurrencia

Categoría	**Activo**	**Amenaza**	**Disp.**		**Int.**		**Conf.**		
			I	***R***	***I***	***R***	***I***	***R***	***RA***
Aplicativos	SistFact/SistContab	Errores de usuarios	1	4	4	16	2	6	26
	SistFact/SistContab	Virus	1	4	4	16	1	4	24

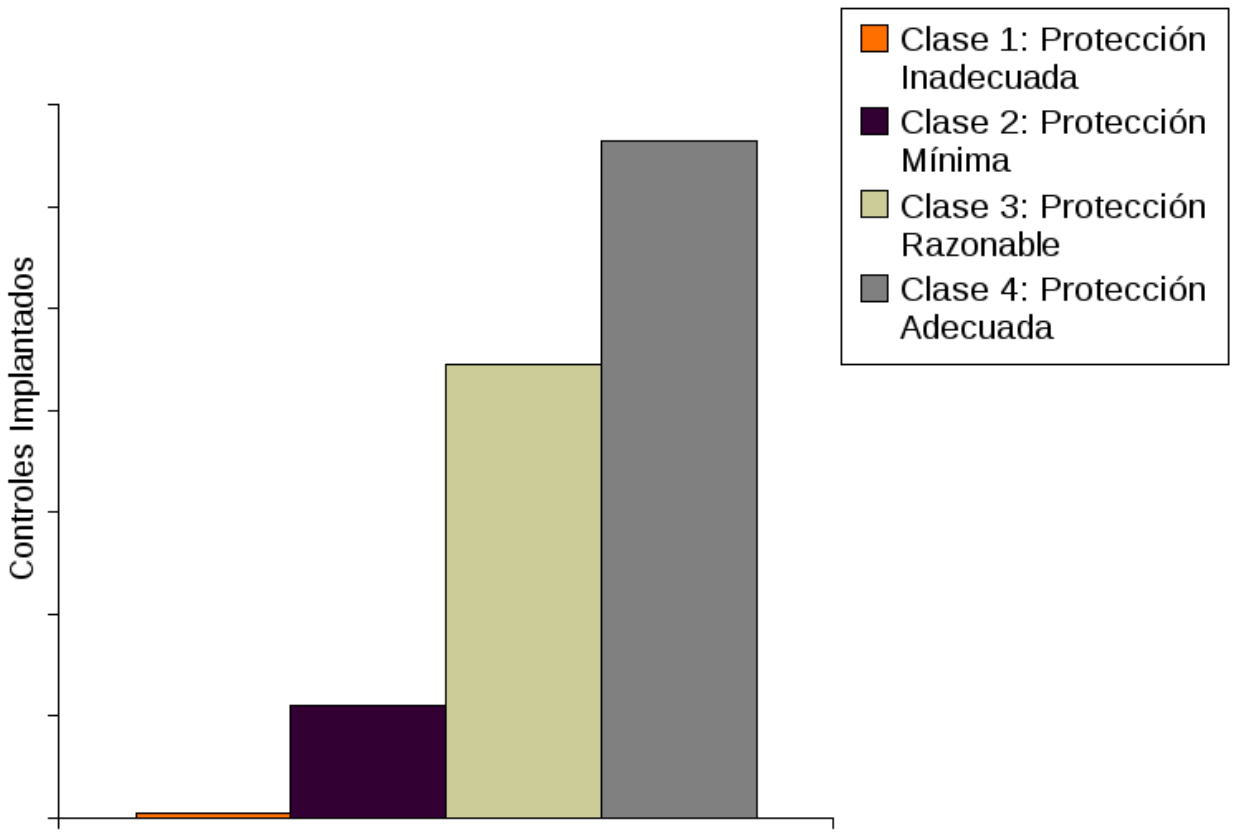
Tratamiento de Riesgos



[1]

[1] D. Villafranca et al., "Hacia un modelo de gestión de la información para la pequeña y mediana empresa con la ISO/IEC 17799", CIBSI'05

Clases de Protección



Etapa de Implementación

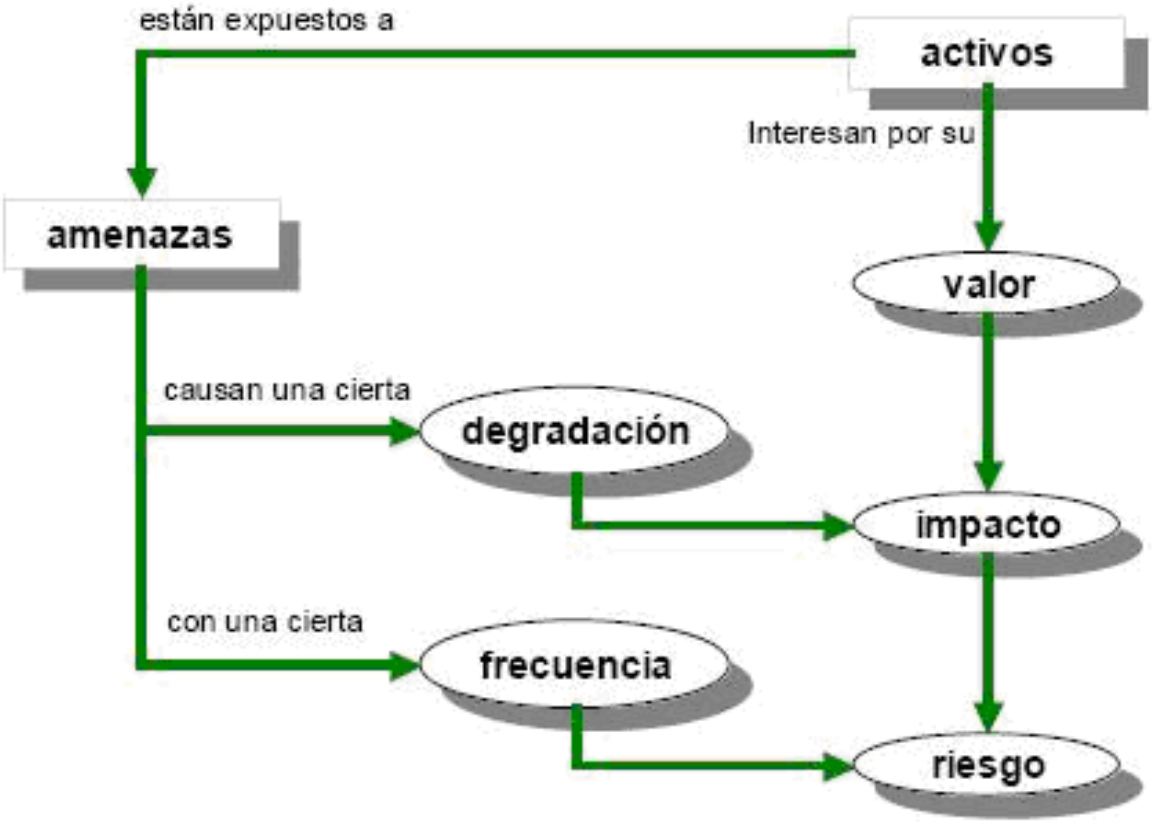
Conclusiones

- Metodología pensada para PyMEs Uruguayas
- Propone una partición de actividades, contribuyendo a clarificar la visión global del proceso
- Refina el proceso de diseño de soluciones para el tratamiento de riesgos
- Define en cada etapa la documentación resultante
- Capacitación y concientización un proceso continuo
- Especificación de requerimientos de software de automatización de actividades

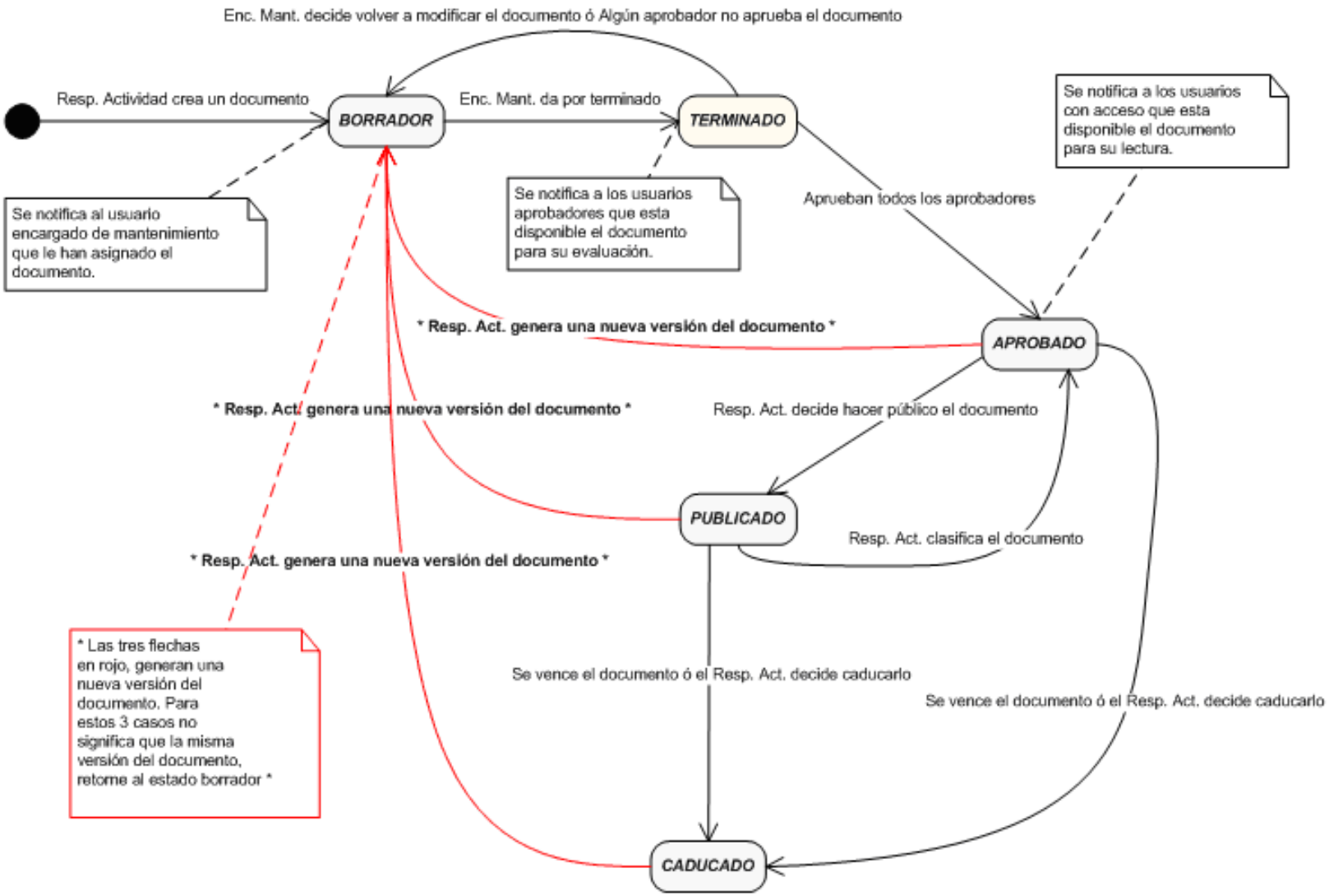
Principales Funcionalidades

- Gestión de usuarios, grupos y permisos
- Gestión de la documentación
- Automatización de actividades del SGSI
  - Generar Documento de Alcance y política de seguridad
  - Alta de categorías de activos, identificación de activos, dependencia de activos
  - Identificación de amenazas, asociar amenaza a activo
  - Evaluación de impacto y riesgo
  - Alta controles, asociar control a activo-amenaza, asignar indicador a control
  - Generar documento de aplicabilidad
  - Reporte de evaluación de riesgos
  - Calculo de impacto y riesgo residual, Gráfica comparativa de riesgo acumulado y residual
  - Reporte de implementación de controles
- Notificaciones

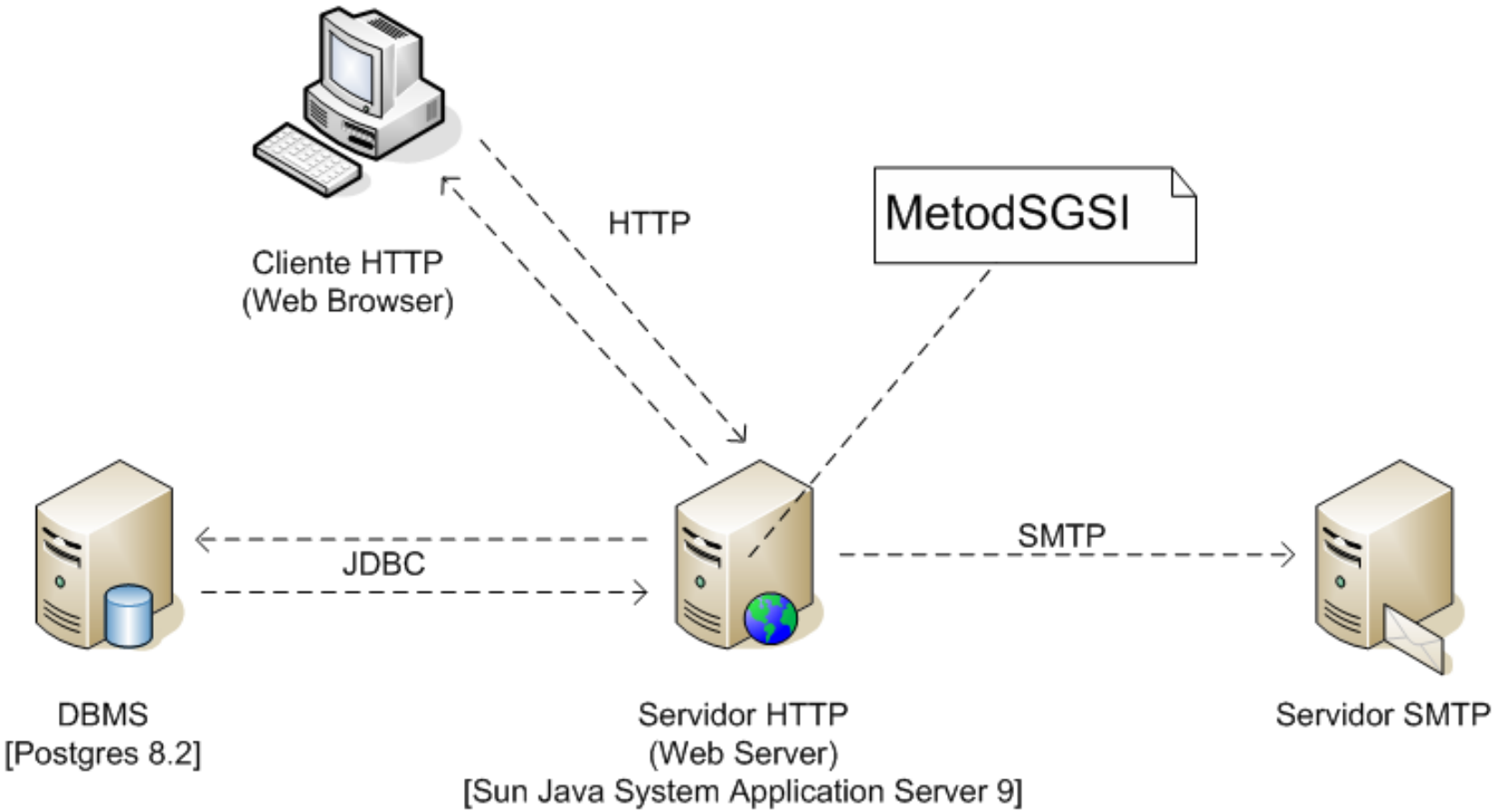
Principales Funcionalidades (Cont.)



Gestión de la documentación



Arquitectura y diseño del sistema



Tecnologías utilizadas

- Sun Java System Application Server 9

- Postgres 8.2

- Netbeans IDE 6.0 M10

  - Visual Java Server Faces

Demo

Demo

Conclusiones

- Prototipo que implementa la metodología especificada
- Desarrollado con tecnologías de código abierto
- Genera y gestiona la documentación
- Gestión centralizada del SGSI
- Módulo de notificación

Referencias


G. Pallas,
Metodología de Implantación de un SGSI en un grupo empresarial jerárquico,
Tesis de Maestría, 2010.


M.Corti, G. Pallas,
Metodología de Implantación de un SGSI en grupos empresariales de relación jerárquica,
IV Congreso Iberoamericano de Seguridad Informática, 2009.


M. Gelós, N. De Maio,
Automatización de Actividades de Implantación y Mejora Continua de un SGSI,
Tesis de Grado, 2007.

Referencias (Cont.)


M. Corti,
Análisis y Automatización de la Implantación de SGSI en Empresas Uruguayas,
Tesis de Maestría, 2006.


G.Betarte, M.Corti, R. de la Fuente,
Hacia una implementación exitosa de un SGSI,
III Congreso Iberoamericano de Seguridad Informática, 2005.

Gracias por su tiempo

Metodologías para la implantación de SGSI

María Eugenia Corti

Grupo de Seguridad Informática
Instituto de Computación
Facultad de Ingeniería - UdelaR
mcorti@fing.edu.uy

24/06/2010