Departamento de Tecnologías y Sistemas de Información

Universidad de Castilla-La Mancha

Ciudad Real (España)

CIBSI 2013

VII Congreso Iberoamericano de Seguridad Informática

Desarrollando una metodología para gestionar los riesgos de seguridad asociativos y jerárquicos y tasar de forma objetiva los Sistemas de Información

Antonio Santos-Olmo Parra
(asolmo@sicaman-nt.com)

Luis Enrique Sánchez Crespo
(luisenrique@sanchezcrespo.org)

Esther Álvarez
(ealvarez@in-nova.org)

Eduardo Fernández-Medina Paton
(Eduardo.FdezMedina@uclm.es)

Mario Piattini Velthuis
(Mario.Piattini@uclm.es)

Índice de la Presentación

1. Introducción
2. Trabajo relacionado
3. Framework desarrollado: MARISMA
4. Conclusiones
5. Trabajo futuro

Antonio Santos-Olmo Parra

Necesidad del análisis de riesgos en PYMES (I)

- Introducción:
  - La información es el activo más importante para una compañía.
  - El análisis de riesgos es fundamental para tener controlado el valor y los riesgos a los que los activos están sometidos.
  - Además de identificar y eliminar riesgos, esta actividad se ha de realizar de manera eficiente, ahorrando dinero y esfuerzo.
  - Los modelos de seguridad clásicos se han mostrado ineficaces.
  - La falta de seguridad es un freno para las nuevas tecnologías.
  - Surge la necesidad de obtener metodologías de análisis de riesgos adaptadas a PYMES, que les permitan evaluar los riesgos a los que sus activos están expuestos y a establecer los controles de seguridad adecuados.

Necesidad del análisis de riesgos en PYMES (II)

- Principales problemas detectados:
  - Riesgos asociativos (relación con el entorno)
  - Riesgos jerárquicos (esquema Matriz – Filiales)
  - Elevado nivel de incertidumbre en los resultados
  - Dificultad de tasación económica objetiva
  - Valoraciones no objetivas
  - Poco dinámicos ante cambios de activos, alcance, etc.
  - No se adaptan a las necesidades de las PYMES

Antonio Santos-Olmo Parra

Definiciones

- **Sistema de Gestión de la Seguridad de la Información (SGSI):**

  Se puede definir como un sistema de Gestión usado para establecer y mantener un entorno seguro de la información. Este SGSI debe tratar la puesta en práctica y el mantenimiento de procesos y de procedimientos para manejar la seguridad de la tecnología de la información.

- **Análisis de Riesgos:**

  Es un proceso sistemático para estimar la magnitud de los riesgos a los que está expuesta una organización, para saber qué decisión tomar ante una posible eventualidad. Para ello, se seleccionan e implementan salvaguardas para poder conocer, prevenir, impedir, reducir o controlar los riesgos identificados. De forma más técnica, el análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegidos se encuentran los activos.

Aspectos analizados

- Ámbito global de aplicación
- Métricas
- Técnicas cualitativas
- Técnicas cuantitativas
- Asociativo
- Jerárquico
- Orientado a PYMES
- Reutilización del conocimiento
- Dispone de Herramientas SW
- Casos prácticos
- Tasación de activos
- Control de incertidumbre
- Dinámico

Estándares y metodologías: Comparativa

Nombre	Tipo de Análisis			Criterios de Seguridad				Elementos del Modelo				Otras características deseables						
	Cuantitativo	*Cualitativo*	*Mixto*	*Confidencialidad*	*Integridad*	*Disponibilidad*	*Autenticidad*	*Activos*	*Vulnerabilidades*	*Amenazas*	*Salvaguardas*	*Orientado a PYMES*	*Dinámico*	*Reutilización del Conocimiento*	*Asociativo*	*Jerárquico*	*Tasación de activos*	*Control de la incertidumbre*
ISO 13335	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	No	No	No	No	No
ISO 27002	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	No	No	No	No	No
ISO 27005	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	No	No	No	No	No
NIST SP 800-30	Sí	Sí	No	Sí	Sí	Sí	No	No	Sí	Sí	Sí	No	No	No	No	No	No	No
AS/NZS 4290	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	No	No	No	No	No	No	No
MAGERIT	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí	No	No	No	No	No	No	No
OCTAVE	Sí	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	No	No	No	No	No	No	No
MEHARI	Sí	Sí	No	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	No	No	No	No	No	No	No
CRAMM	Sí	No	No	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	No	No	No	No	No	No	No
MARISMA	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Revisión Sistemática de metodologías (I): Estudios seleccionados

Tipo de iniciativa	Nº de estudios	Iniciativas
Proceso	6	3.7, 3.13, 3.15, 3.18, 3.19, 3.20
Framework	2	3.5, 3.6
Modelo	6	3.3, 3.8, 3.9, 3.10, 3.16, 3.21
Metodología	6	3.1, 3.2, 3.4, 3.11, 3.14, 3.17
Otros	2	3.12, 3.22
Total	**22**	-

Antonio Santos-Olmo Parra

Revisión Sistemática de metodologías (II): Comparativa

Iniciativa	Ámbito Global	Métricas	Técnicas Cualitativas	Técnicas Cuantitativas	Asociativo	Jerárquico	Orientado PYMES	Reutilización Conocimiento	Herramienta Software	Casos Prácticos	Dinámico	Tasación Activos	Control Incertidumbr
Nachtigal, S.	No	Parc.	No	No	Parc.	No	Parc.	No	No	Parc.	No	No	No
Abdullah, H	No	No	Sí	No	No	No	Sí	No	No	No	No	No	No
Arikan, A.E.	No	No	No	No	Parc.	Sí	No	No	No	Sí	No	No	No
Bagheri, E. et al.	Sí	Sí	Sí	No	No	No	No	No	No	No	No	No	No
Alhawari, S. et al.	No	No	No	No	No	No	No	Sí	No	No	No	No	No
ICES RMC	No	No	No	No	Parc.	No	No	No	No	No	No	No	No
Strecker, S et al.	Sí	No	Parc.	Parc.	No	No	No	No	No	No	No	No	No
Ma, Wei-Ming	Sí	No	No	No	Parc.	Parc.	Parc.	No	No	No	No	No	No
Feng, Nan et al.	Sí	No	Sí	Sí	Parc.	No	No	No	No	Sí	No	No	Sí
Carlsson, C. et al. and Hussain, O. et al.	No	No	Sí	Sí	Parc.	No	No	No	No	No	No	No	No
Tjoa, S. et al.	No	No	Sí	No	No	No	No	No	No	No	No	No	No
Abraham, A.	No	No	No	No	Parc.	No	No	Sí	No	No	No	No	No
Chang, She-I et al. and Wang, Ping et al.	No	Parc.	Parc.	No	Parc.	No	No	No	No	Sí	No	No	Sí
Yang, Fu-Hong	No	No	No	No	Parc.	No	No	No	No	No	No	No	No
Kumar, V. et al.	No	No	No	No	Parc.	Parc.	No	No	No	Sí	No	No	Sí
Wawrzyniak, D.	Sí	No	Sí	No	No	No	No	No	No	No	No	No	No
Lin, Mengquan et al.	Sí	Parc.	No	Sí	No	No	No	No	No	No	No	No	No
Hewett, R. et al.	No	No	No	No	Parc.	No	No	Sí	No	No	No	No	No
Lo, Chi-Chun et al.	No	Parc.	Sí	Sí	Parc.	No	No	No	No	No	No	No	No
Patel, S.C. et al.	Sí	Parc.	No	Sí	No	No	No	No	No	No	No	No	No
Yu-Ping Ou Yang et al.	Sí	Parc.	Sí	Sí	No	No	No	No	No	Sí	No	No	No
Salmeron, J.L. et al.	No	No	Sí	No	No	Parc.	No	No	No	No	No	No	No
MARISMA	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**

Conclusiones

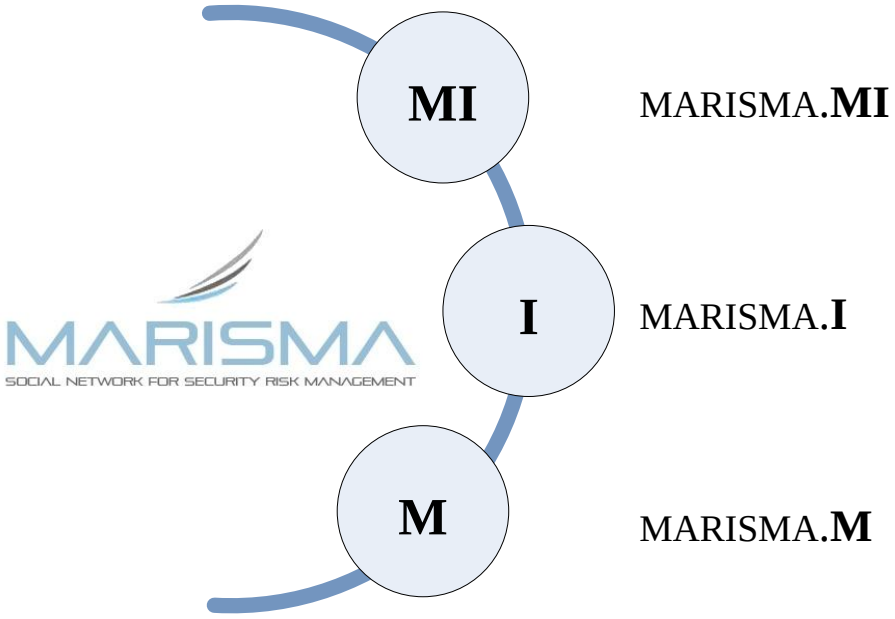
- Ninguna de las propuestas posee las características deseables
- No orientación a PYMES
- Pocas propuestas cuentan con herramientas que faciliten su gestión
- Pocas propuestas incluyen riesgos jerárquicos y asociativos
- Las que lo hacen, de forma teórica y sin base en casos reales
- Muy pocas se han centrado en disminuir el grado de incertidumbre
- Casi ninguna tiene reutilización del conocimiento
- No se tiene en cuenta la importancia de poder actualizarse de forma dinámica
- No se obtiene una tasación monetaria y objetiva de los activos

Framework propuesto: MARISMA

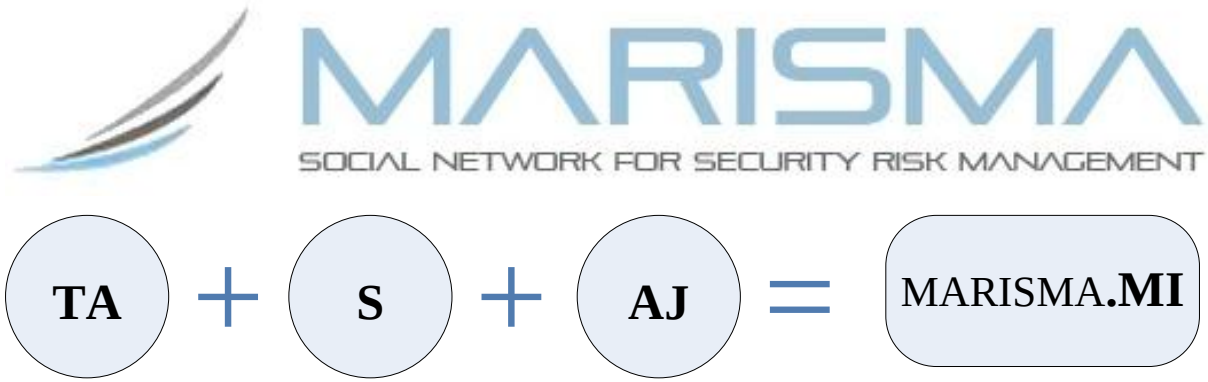
El objetivo fundamental de nuestra investigación queda expresado como:

Diseñar y construir un marco de trabajo metodológico que permita realizar análisis de riesgos con el menor grado de incertidumbre, que sean válidos para las PYMES, que sean dinámicos, controlen aspectos asociativos y jerárquicos y permitan la tasación económica y objetiva de los Sistemas de Información de una compañía

Marco de Trabajo



Modelo de Información

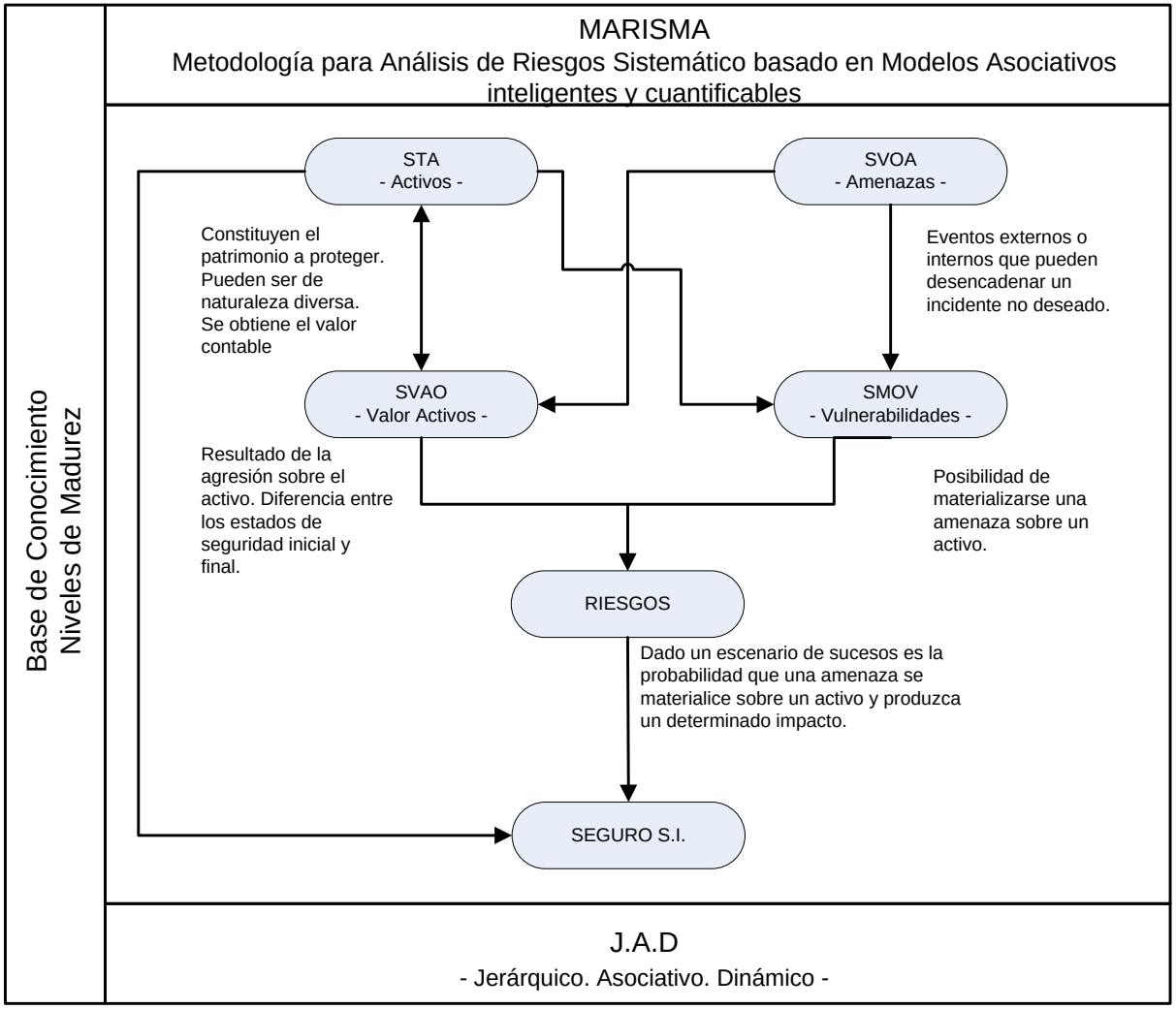


Indicadores

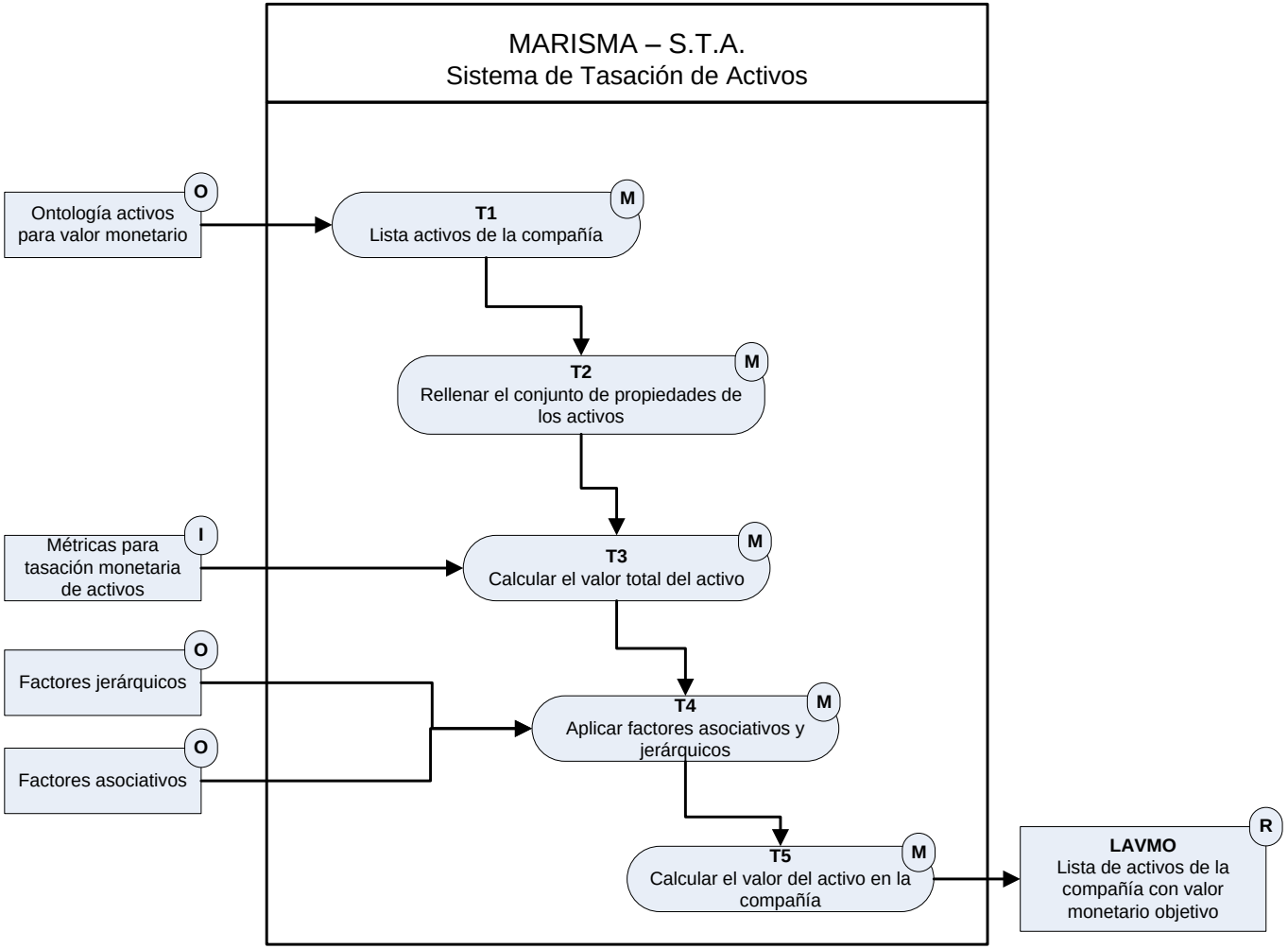
MARISMA.**I**

- Valoración y tasación de activos
- Valoración de amenazas
- Valoración de activos en base a criterios de riesgo
- Valoración de controles de seguridad

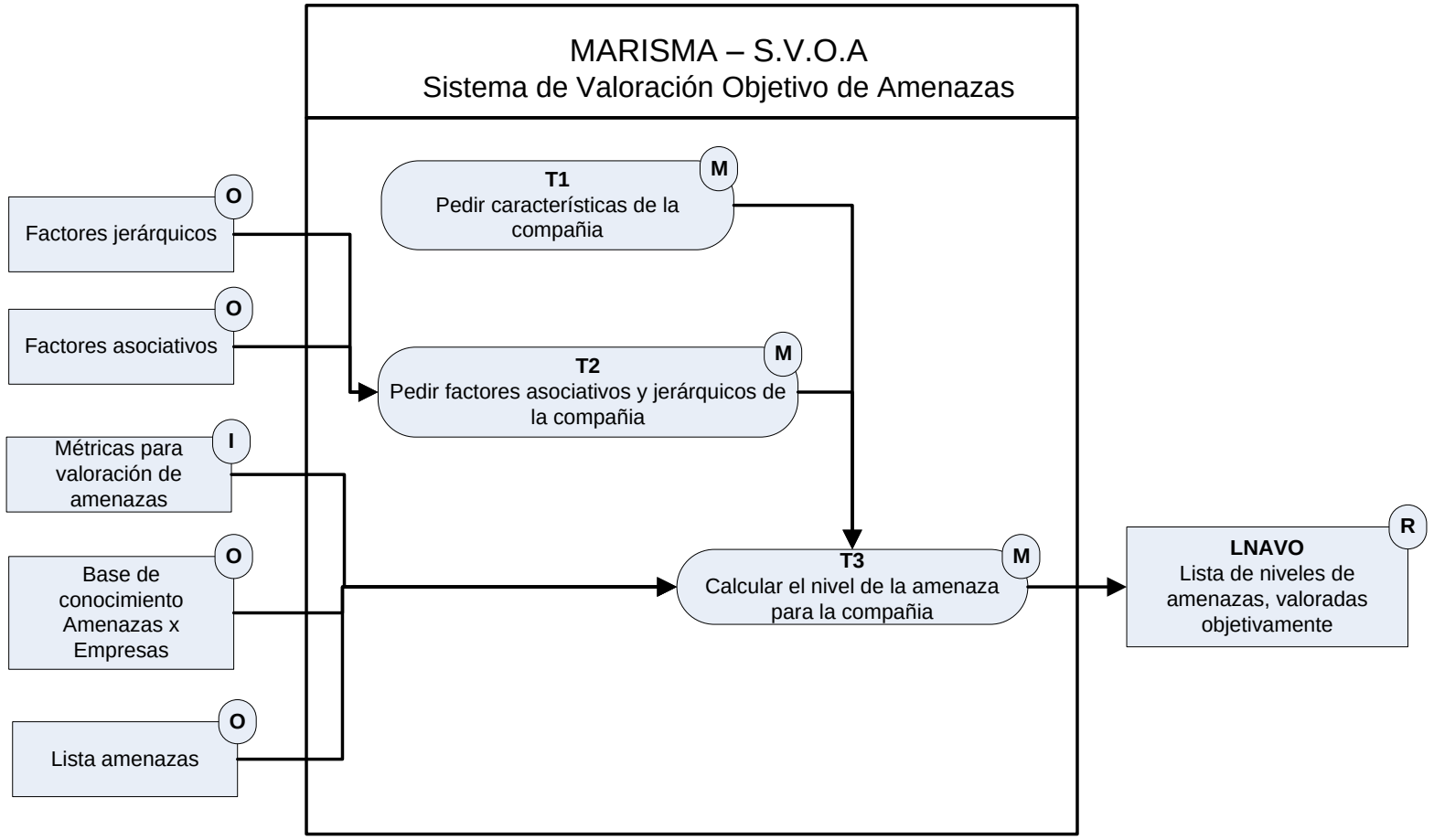
Metodología



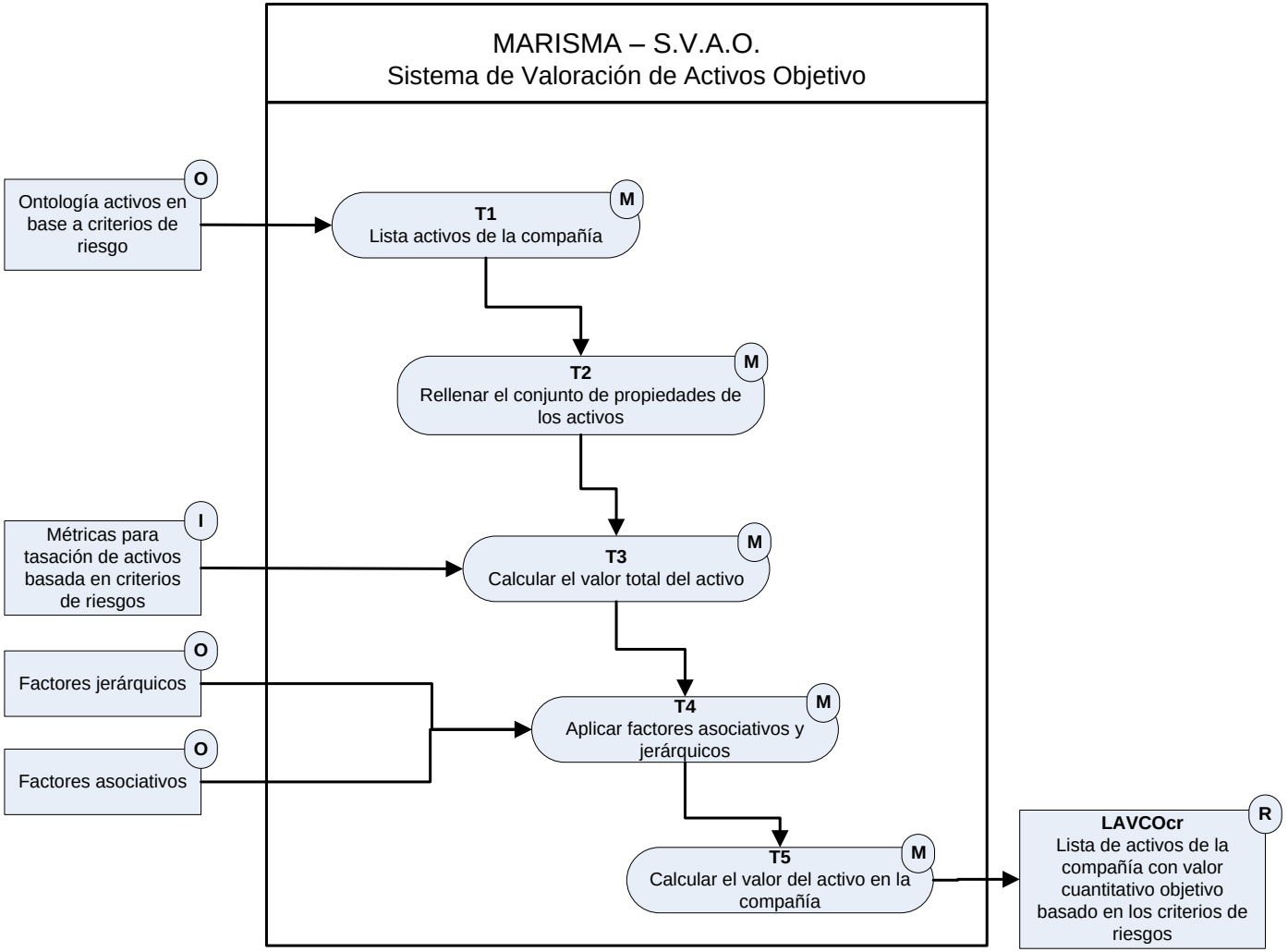
MARISMA: Sistema de Tasación de Activos (STA)



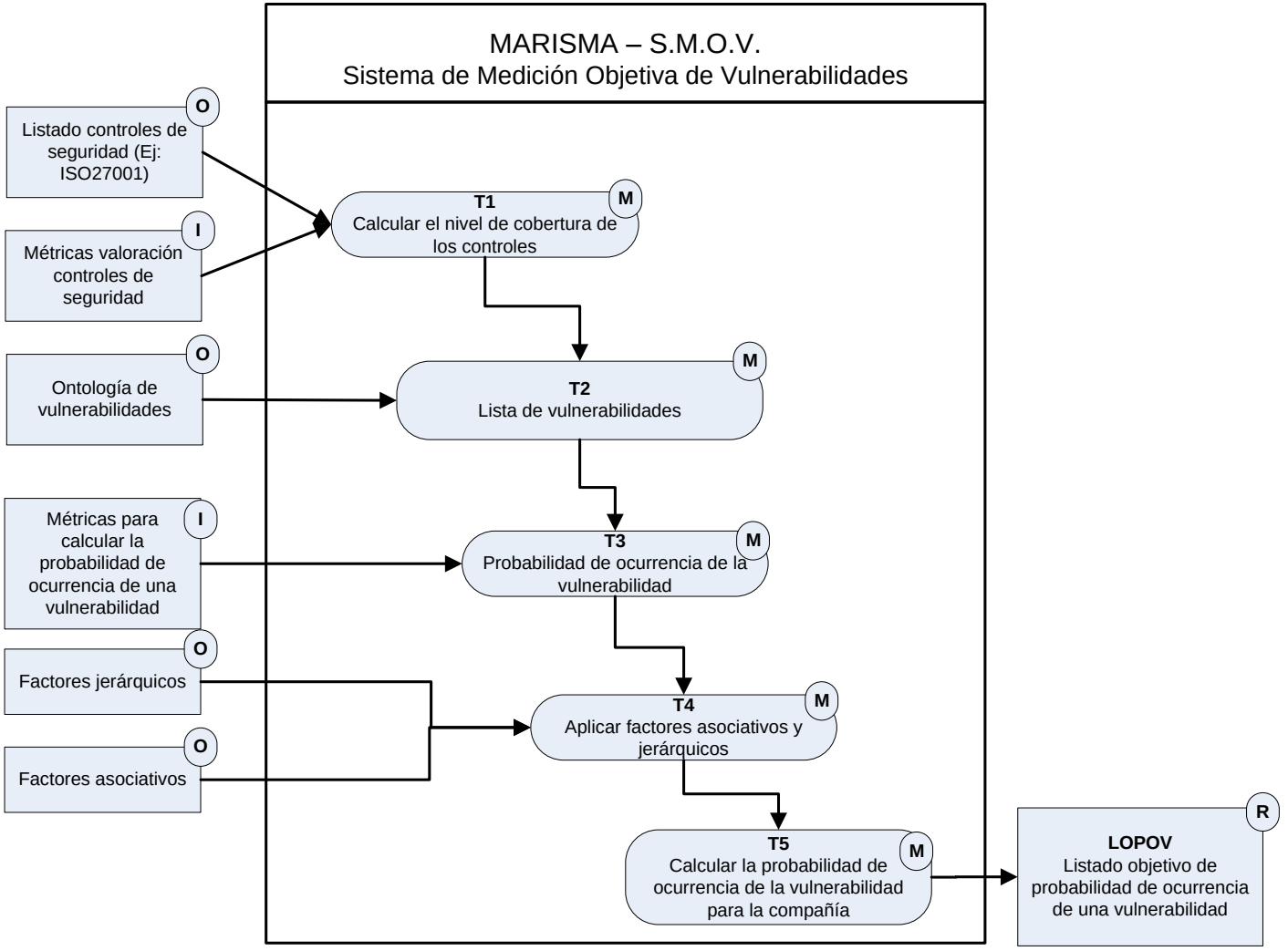
MARISMA: Sistema de Valoración Objetivo de Amenazas (SVOA)



MARISMA: Sistema de Valoración de Activos Objetivo (SVAO)



MARISMA: Sistema de Medición Objetiva de Vulnerabilidades (SMOV)



Conclusiones (I)

- Se ha propuesto un marco de trabajo que permite la tasación objetiva de un sistema de información y la generación de un análisis de riesgos objetivo que tenga en cuenta aspectos asociativos y jerárquicos y sea de bajo coste en su generación y mantenimiento
- Estudio de las principales metodologías existentes en el mercado y revisión sistemática de los diferentes modelos y metodologías para el análisis y gestión de riesgos
- No orientación a PYMES
- La mayoría están centradas en aspectos concretos de los SI (ERP, WLAN, e-Commerce,…)
  - Gestionar e integrar varios modelos de análisis de riesgos para una aplicación global
  - Integración de distintas herramientas

Conclusiones (II)

- Los modelos que cubren un ámbito global dependen en gran medida del conocimiento experto
  - Nula autonomía para el mantenimiento en PYMES
  - Necesidad de expertos para mantener el sistema de gestión y evaluación de riesgos
  - Alto coste económico y en recursos
- Pocas propuestas incluyen riesgos jerárquicos y asociativos
- Resultados de valoración no objetivos:
  - Valoración de riesgos subjetiva: Sin validez ante terceros.
  - Valoración económica subjetiva.
- Todas las propuestas estudiadas son muy importantes para la investigación.

Trabajo futuro

- Completar la revisión sistemática en relación con las métricas de tasación de sistemas de información.
- Diseñar Ontologías
- Completar la base de conocimiento basada en esquemas que interconecten los diferentes elementos y permitan la reutilización del conocimiento.
- Diseñar métricas para la tasación de activos, valoración de activos en base a criterios de riesgo y valoración de amenazas.
- Continuar con el diseño de métricas para la valoración de controles de seguridad en base a estándares existentes y para calcular la probabilidad de ocurrencia de una vulnerabilidad.
- Diseñar algoritmos:
  - Calcular niveles de riesgo en base a las dependencias jerárquicas y asociativas.
  - Generar de forma semiautomática la valoración del SI, los niveles de riesgo asociados a los activos y un plan de mejora propuesto para la compañía.
- Continuar con la generación de módulos para la herramienta.
- Continuar con la validación en casos reales.

Desarrollando una metodología para gestionar los riesgos de seguridad asociativos y jerárquicos y tasar de forma objetiva los Sistemas de Información

Gracias por su atención