Marco metodológico para análisis de riesgos en el manejo de información en PYMES

Autores: Luis Enrique Sánchez[1] , Antonio Santos-Olmo[1] , Eduardo Fernández-Medina[2] y Mario Piattini[2]
[1] Sicaman Nuevas Tecnologías S.L. [2] Universidad de Castilla-la Mancha.

1 INTRODUCCIÓN

En un entorno empresarial globalizado y competitivo como el actual, las empresas dependen cada vez más de sus sistemas de información, ya que se han mostrado como un factor de gran importancia para aumentar su nivel de competitividad. De esta forma, las empresas ya han tomado conciencia de que la información y los procesos que apoyan los sistemas y las redes son sus activos más importantes. Estos activos están sometidos a riesgos de una gran variedad, que pueden afectar de forma crítica a la empresa.

Estudios centrados en la evaluación de riesgos, realizados sobre organizaciones en Europa y los EE.UU, revelan que las PYMES se caracterizan por la falta de la dedicación necesaria a la seguridad de Tecnologías de la Información (TI), debido principalmente a la asignación de responsabilidades a personal sin la debida formación. Pero las PYMES no son las únicas que sufren problemas con los sistemas de análisis de riesgos; con la llegada de Internet, para las empresas es cada vez más crítico implantar controles de seguridad que les permitan conocer y controlar los riesgos a los que pueden estar sometidas. En una época en la que la colaboración es vital en la situación actual del mercado, es necesario contemplar también el riesgo derivado de la relación de la empresa con su entorno, sus circunstancias (variantes en cada momento) y con otras empresas, bien como terceras partes en algún servicio que realice la empresa o bien como co-participantes en proyectos multi-empresa. El tratamiento de estos riesgos de tipo asociativo adquiere también especial relevancia con la aparición del *Cloud Computing*, que ha alterado las arquitecturas tradicionales de Sistemas de Información.

Podemos concluir que los modelos de análisis y gestión del riesgo son fundamentales para las empresas, pero que no existen metodologías que se adecuen, y las existentes se muestran ineficientes al carecer de mecanismos de reutilización de conocimiento, adaptación al cambio, control de elementos asociativos y jerárquicos, sistemas objetivos de tasación y generación de riesgos, que como se ha visto son elementos cada vez más importantes para las compañías.

Las principales carencias detectadas utilizando los métodos científicos de "investigación-en acción" y "revisión sistemática de la literatura" fueron las siguientes: i) las PYMES requieren de metodologías de análisis de riesgos que sean de bajo coste, generación rápida y reutilicen el conocimiento; ii) las metodologías existentes entienden los activos como elementos, obviando aspectos cada vez más importantes como las inter-relaciones entre las compañías y los activos de éstas; iii) las metodologías de análisis de riesgos existentes en la actualidad generan un elevado nivel de incertidumbre, lo que limita su aplicación práctica. Dos análisis de riesgos realizados por diferentes consultores, pueden arrojar niveles de riesgo completamente diferentes, debido al elevado número de componentes subjetivos de los análisis de riesgos actuales; iv) en la era del conocimiento, la información se ha convertido en el mayor activo de las compañías, pero la carencia de sistemas objetivos de tasación monetaria de activos, así como de análisis de riesgos objetivos, hace que las compañías de seguros no puedan tasar y asegurar dichos activos.

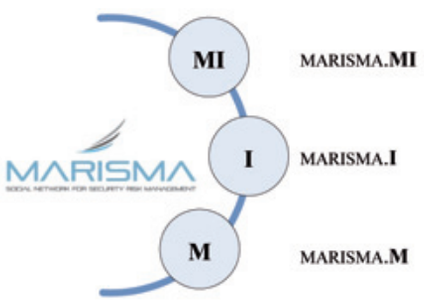

Fig. 1: Fases de la metodología

2. DESARROLLO

Nuestro principal objetivo ha sido el desarrollo de un marco de trabajo metodológico que cumpliese con las carencias detectadas. Como se puede ver en la Fig. 1, el marco metodológico que estamos construyendo, estará formado por tres componentes:

- *Modelo de Información (MI):* Contendrá el modelo de información, y estará formado por los conceptos y las bases de conocimiento del marco metodológico.
- *Indicadores (I):* Contendrá todas las métricas que nos permitirán las tasaciones económicas objetivas de los activos.
- *Metodología (M):* Contendrá la propia metodología de tasación y análisis del riesgo.

En las siguientes sub-secciones se describirán, de forma resumida, los

principales elementos y características del marco de trabajo que se está desarrollando.

2.1. Modelo de Información MARISMA.MI

La primera parte del marco metodológico que proponemos contendrá un modelo de información que recoge todos los conceptos relacionados con la nueva metodología, y que estará basado en otras investigaciones.

Para el desarrollo de estas Bases de datos de conocimento, debemos ser capaces de analizar las tres dimensiones del problema (ver Fig. 2):

- Conceptos relacionados con el campo de la tasación de activos (TA).
- Conceptos relacionados con el campo de la seguridad (S).
- Conceptos relacionados con la interrelación de compañías: Asociatividad (por ejemplo, varias empresas que participan en un proyecto) y jerarquía (por ejemplo, una empresa matriz y sus filiales) (AJ).

2.2. Indicadores MARISMA.I

La segunda etapa para el desarrollo de nuestra metodología se centrará en el estudio y desarrollo de un conjunto de indicadores, reglas de negocio y métricas vinculadas a los procesos seguridad de los sistemas de información. Uno de los objetivos de esta fase es facilitar que pueda determinarse de forma semiautomática la valoración (tanto económica como en cuanto a importancia dentro de la empresa) de los activos del sistema de información. En resumidas cuentas, se desarrollarán fórmulas y variables que permitan tasar el Sistema de Información de una organización.

2.3. Metodología MARISMA.M

La tercera parte del marco de trabajo que estamos desarrollando contiene la metodología que se aplicará para 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, reutilización del conocimiento, dinamismo y que sea válida para las PYMES. El esquema general de la metodología se puede ver en la Fig. 3.

La metodología MARISMA está constituida por los siguientes artefactos:

- *Sistema de Tasación de Activos (STA):* permite, a partir de la lista de activos de la compañía, obtener una tasación económica de los mismos.
- *Sistema de Valoración Objetivo de Amenazas (SVOA):* permite valorar, en base a métricas objetivas, la probabilidad de ocurrencia de cada posible amenaza que puede afectar a cada uno de los activos de la compañía. Por ejemplo, la probabilidad de un acceso no autorizado a la red de la compañía.
- *Sistema de Medición Objetiva de Vulnerabilidades (SMOV):* permite valorar mediante métricas objetivas la probabilidad de que una vulnerabilidad pueda ser explotada para una compañía. Por ejemplo, el nivel de control que se tiene actualmente en el acceso físico a las instalaciones.
- *Sistema de Valoración de Activos Objetivo (SVAO):* permite dar un valor, de forma cuantitativa y objetiva, a cada uno de los activos de la compañía sobre la base de los principales criterios de riesgo. Por ejemplo, la importancia para la compañía de la confidencialidad de sus datos.

En función de las valoraciones obtenidas por los sistemas SMOV (Probabilidad de ocurrencia de vulnerabilidades) y SVAO (Valoración de activos en base a criterios de riesgo), podemos obtener un valor de riesgo objetivo para cada uno de los activos de la compañía, en base a las amenazas que pueden afectar a un activo y su nivel de seguridad.

Una vez calculado un valor de riesgo objetivo para cada activo, se podría utilizar como base para el cálculo del seguro del Sistema de Información de la compañía, ya que contamos también con la valoración económica objetiva de cada activo, calculada previamente en el sistema STA. De esta forma, se puede calcular un valor económico del Sistema de Información en base al valor económico calculado de cada activo y la fortaleza de los controles que protegen su seguridad. Este valor se puede emplear por una compañía aseguradora para calcular una cuota de seguro para el Sistema de Información.

Como hemos visto, los factores jerárquicos y asociativos se aplican a todos y cada uno de los sistemas que conforman el núcleo de la metodología. Asimismo, para el diseño y aplicación de la misma es necesario contar con un tercer factor: la necesidad de que la metodología sea dinámica, de forma que si hay algún cambio en el sistema se puedan recalcular los valores de riesgo y tasación de una forma automática y ágil.

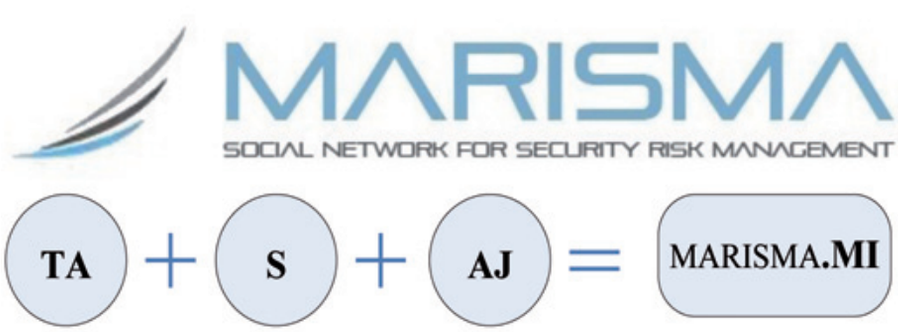

Fig. 2: Dimensiones de la Base de conocimiento sobre la que se construirá la metodología

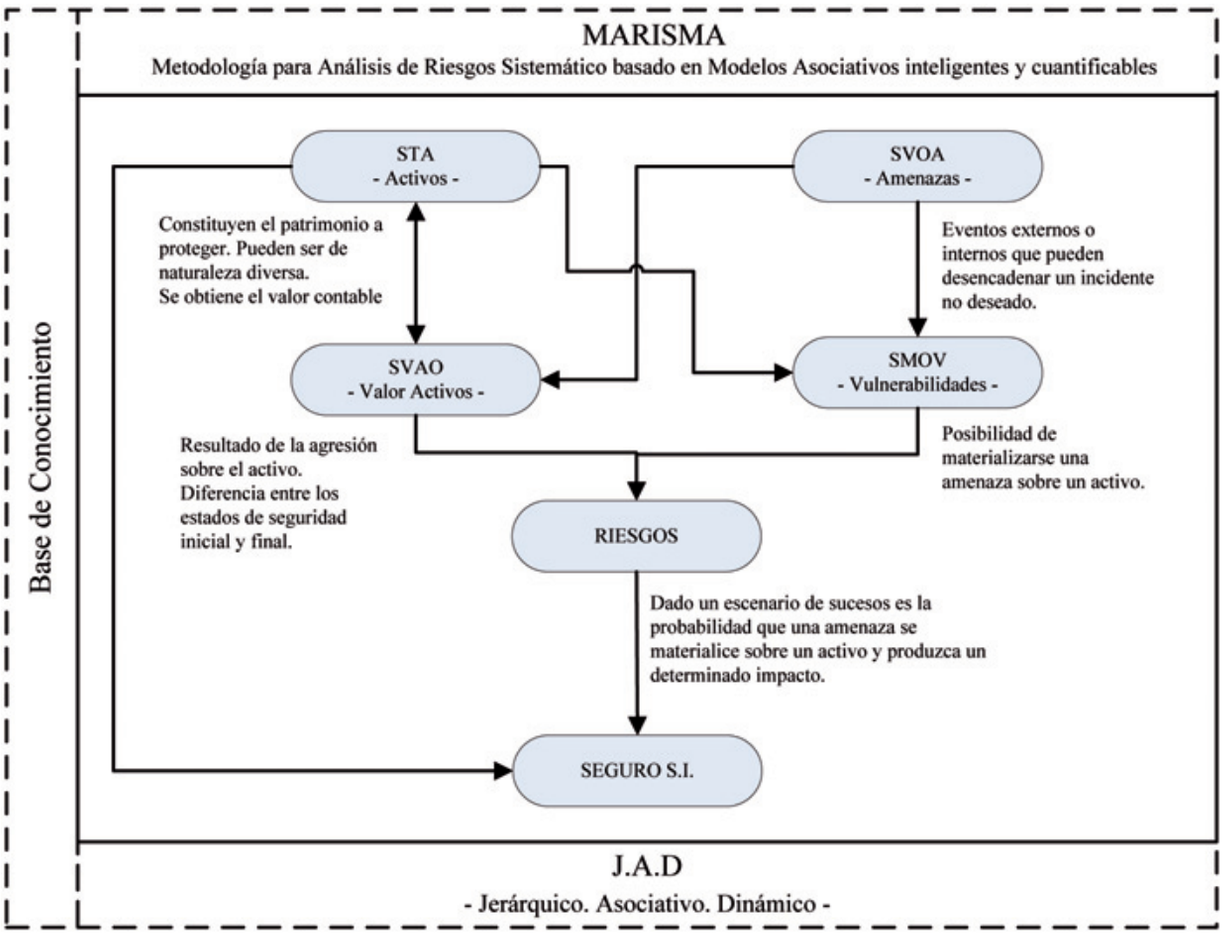

Fig. 3: Esquema general de la metodología

3. CONCLUSIONES

Durante la investigación se han estudiado las principales metodologías existentes en el mercado relacionadas con la generación de análisis de riesgos de los sistemas de información. Como resultado de esta revisión se ha podido establecer la importancia que tiene la gestión y el análisis de los riesgos sobre la seguridad de los Sistemas de Información en el desempeño y evolución sostenible de las empresas. Además, se han realizado reuniones y entrevistas en empresas privadas y sectores como el asegurador, para establecer las necesidades reales de las empresas y terceros, de forma que la investigación tenga una clara aplicación práctica.

De los resultados de la investigación y de la experiencia práctica, podemos concluir que en la era del conocimiento es crítico que las empresas gestionen de forma adecuada sus activos de información y cuenten con sistemas de gestión de seguridad que les permitan proteger de una forma correcta estos activos.

4. PARA SABER MÁS

1. Wiander, T. *Implementing the ISO/IEC 17799 standard in practice – experiences on audit phases.* in *AISC '08: Proceedings of the sixth Australasian conference on Information security.* 2008. Wollongong, Australia.
2. Kluge, D. *Formal Information Security Standards in German Medium Enterprises.* in *CONISAR: The Conference on Information Systems Applied Research.* 2008.
3. Holappa, J. and T. Wiander, *Practical Implementation of ISO 17799. Compliant Information Security Management System Using Novel ASD Method.*, in *Technical Report*, V.T.R.C.o. Finland, Editor 2006.
4. Llvonen, L. *Information Security Management in Finnish SMEs.* in *5th European Conference on Information Warfare and Security National Defence College.* 2006. Helsinki, Finlan: 1-2 June 2006.
5. Dhillon, G. and J. Backhouse, *Information System Security Management in the New Millennium.* Communications of the ACM, 2000. 43(7): p. 125-128.
6. Nachtigal, S., *E-business Information Systems Security Design Paradigm and Model.* Royal Holloway, University of London, Technical Report, 2009: p. 347.
7. Zissis, D. and D. Lekkas, *Addressing cloud computing security issues.* Future Generation Computer Systems, 2012.