Libro de Actas

Actas del VII Congreso Iberoamericano de Seguridad Informática
CIBSI 2013
Panamá, República de Panamá, 29 al 31 de Octubre del 2013

Compiladores

Giovana Garrido
Jorge Ramió Aguirre
Gaspar Modelo Howard
Arturo Ribagorda Garnacho

ISBN: 978-9962-676-43-0

Facultad de Ingeniería de Sistemas Computacionales
Universidad Tecnológica de Panamá
Panamá, República de Panamá

Avales Académicos

Patrocinadores

Comité del Programa

Modelo Howard Gaspar (Chair)	Universidad Tecnológica de Panamá, Panamá
Arturo Ribagorda Garnacho (Chair)	Universidad Carlos III de Madrid, España
Jorge Ramió Aguirre	Universidad Politécnica de Madrid, España
Giovana Garrido	Universidad Tecnológica de Panamá, Panamá
Santiago Acurio	Pontificia Universidad Católica del Ecuador, Ecuador
Nicolás Antezana Abarca	Sociedad Peruana de Computación, Perú
Javier Areitio Bertolín	Universidad de Deusto, España
Waltea Baluja	Ciudad Universitaria Juan Antonio Echeverría, Cuba
Gustavo Betarte	Universidad de la República, Uruguay
Carlos Blanco	Universidad Cantabria, España
Jorge Blasco Alis	Universidad Carlos III de Madrid, España
Joan Borrell Viader	Universidad Autónoma de Barcelona, España
Pino Caballero Gil	Universidad de La Laguna, España
José Jeimy Cano	Universidad Pontificia Bolivariana, Colombia
Mauro Adriano Cansian	Universidade Estadual Paulista, Brasil
Eduardo Carozo	Universidad de Montevideo, Uruguay
Enrique Daltabuit Godas	Universidad Nacional Autónoma de México, México
José María De Fuentes	Universidad Carlos III de Madrid, España
Ángel Martín Del Rey	Universidad de Salamanca, España
Josep Domingo Ferrer	Universidad Rovera i Virgili, España
Josep Lluis Ferrer Gomilla	Universidad de las Islas Baleares, España
Angélica Flórez Abril	Universidad Pontificia Bolivariana, Colombia
Amparo Fúster	Consejo Superior de Investigaciones Científicas, España
David García	Universidad de Castilla-La Mancha, España
Luis Javier García	Universidad Complutense de Madrid, España

Comité Organizador

Nicolás Samaniego	Universidad Tecnológica de Panamá, Panamá
Jorge Ramió Aguirre	Universidad Politécnica de Madrid, España
Giovana Garrido	Universidad Tecnológica de Panamá, Panamá
Crispina Ramos	Universidad Tecnológica de Panamá, Panamá
Amarilis Alvarado	Universidad Tecnológica de Panamá, Panamá
Isabel Leguías	Universidad Tecnológica de Panamá, Panamá

INDICE

PONENCIAS CIBSI

PONENCIAS TIBETS

PRESENTACIÓN

El VII Congreso Iberoamericano de Seguridad Informática CIBSI 2013, tuvo lugar del 29 al 31 de Octubre de 2013 en la ciudad de Panamá, siendo organizado por la Facultad de Ingeniería de Sistemas Computacionales de la Universidad de Tecnológica de Panamá y la Universidad Politécnica de Madrid, España, a través de la Red Temática de Criptografía y Seguridad de la Información Criptored.

Las jornadas se desarrollaron en el Auditorio de la Universidad Tecnológica de Panamá y en el Salón de Conferencias del Edificio de Postgrado.

El evento está pensado desde la perspectiva de compartir experiencias a nivel de investigación en tecnologías de la seguridad informática, imprescindible actualmente para el desarrollo del conocimiento humano y del estado de bienestar de la sociedad. De esta manera, el propósito de CIBSI es promover y desarrollar el área de la seguridad de la Información, creando para ello un espacio tecnológico que facilite el intercambio de conocimiento y la formación de redes de colaboración en el ámbito de la investigación, el desarrollo y la innovación tecnológica.

Así mismo, se llevó a cabo el II Taller Iberoamericano de Enseñanza e Innovación Educativa en Seguridad de la Información TIBETS. Desarrollado como un espacio propio dentro del congreso CIBSI, su objetivo es la presentación de experiencias en la enseñanza y formación en seguridad de la información, innovación educativa en dichas áreas, nuevas propuestas docentes y análisis de proyectos de colaboración académica y de programas de postgrados, de forma que fomente el planteamiento de posibilidades reales de colaboraciones docentes entre países.

A partir de los objetivos antes mencionados, la participación giró en torno a los siguientes ejes temáticos: Fundamentos de la seguridad de la información; Sistemas de gestión de seguridad de la información; Riesgos, recuperación y continuidad del negocio; Normativas y legislación en seguridad; Algoritmos y protocolos criptográficos; Vulnerabilidades y criptoanálisis; Técnicas de control de acceso e identificación; Técnicas de intrusión y análisis forense; Infraestructuras de clave pública; Seguridad en redes; Hacking; Ciberdelitos.

En estas actas se recogen 20 trabajos enviados para el congreso CIBSI y 8 para el taller TIBETS, seleccionados por un Comité de Programa compuesto por 43 especialistas de una docena de países Iberoamericanos. No se incluyen, sin embargo, la conferencia magistral inaugural de CIBSI 2013 "Capacidades Esenciales para una Ciberdefensa Nacional" del Dr. Jorge López Hernández-Ardieta, la charla invitada "Confiabilidad de Cumplimiento de Tiempos de Recuperación en Continuidad de Negocios" del Dr. Julio Escobar, y la conferencia magistral inaugural de TIBETS 2013 "Presentación del Proyecto MESI: Mapa de Enseñanza de la Seguridad de la Información" del Dr. Jorge Ramió Aguirre.

Giovana Garrido, Jorge Ramió Aguirre, Gaspar Modelo Howard,

Arturo Ribagorda Garnacho

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

A. Santos-Olmo, L. E. Sánchez, E. Álvarez, E. Fernandez-Medina, M. Piattini

Abstract— **En una sociedad basada en la información, los Sistemas de Gestión de Seguridad (SGSIs) son cada vez más críticos para las empresas, pero no sólo estos sistemas, sino también la posibilidad de poder conocer con exactitud los riesgos a los que están sometidos los activos de información y el valor objetivo que tienen estos activos. El presente artículo presenta una revisión sobre el estado del arte de algunas técnicas para la evaluación de los riesgos y la tasación cuantitativa y objetiva de los activos que componen los sistemas de información, así como una nueva propuesta de metodología que busca solucionar las principales carencias detectadas durante la investigación.**

Keywords—**ISO27001, SGSI, PYMES; Analisis de riesgos; Riesgos jerárquicos y asociativos; Tasación de Sistemas de Información.**

I. Introducción

En un entorno empresarial globalizado y competitivo como el actual, las empresas dependen cada vez más de sus sistemas de información [1], 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 [2, 3]. Estos activos están sometidos a riesgos de una gran variedad, que pueden afectar de forma crítica a la empresa. Así, la importancia de la seguridad en los sistemas de información viene avalada por numerosos trabajos [4-11], por citar sólo algunos.

El problema de conocer los riesgos a los que están sometidos sus principales activos se acentúa especialmente en el caso de las pequeñas y medianas empresas, que cuentan con la limitación adicional de no tener recursos humanos y económicos suficientes para realizar una adecuada gestión [12]. Así algunos autores [13, 14] sugieren la realización de un análisis de riesgos como parte fundamental en la PYME, ya que deben tener en cuenta que el valor y la sanción de los datos robados o filtrados en una pequeña organización es el mismo que para una grande, y por tanto deben tener controlado el valor y los riesgos a los que esos activos están sometidos. Otros autores [15] proponen la necesidad de desarrollar un nuevo modelo de análisis de riesgos (AR) pero orientándolo directamente a las PYMES, considerando que el uso de técnicas de análisis y gestión de riesgos, así como el papel de terceros, es necesario para poder garantizar la seguridad del sistema de información de las PYMES.

Estudios centrados en la evaluación de riesgos [16-18], 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 TI, debido principalmente a la asignación de responsabilidades a personal sin la debida formación. Al analizar las causas por las que no se había realizado el análisis de riesgos se llegó a la conclusión de que esta tarea es a menudo compleja y requiere conocimientos especializados [19], y que una evaluación de la situación actual requiere de herramientas de análisis de riesgos [20] comerciales, las cuales no son fáciles de usar sin conocimientos técnicos adecuados.

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 [2, 3].

El tratamiento de estos riesgos de tipo asociativo adquiere también especial relevancia con la aparición del Cloud Computing, que ha alterado drásticamente la percepción de las arquitecturas de infraestructura de Sistemas de Información. Esta rápida transición hacia la "nube" supone que, desde una perspectiva de seguridad, aparezcan una serie de riesgos y vulnerabilidades desconocidas a partir de esta reubicación de los Sistemas de Información en Cloud, con el consiguiente deterioro de gran parte de la eficacia de los mecanismos tradicionales de protección [21].

Añadido a este tipo de riesgo, también es necesario gestionar los riesgos de carácter vertical en la jerarquía de empresa, donde la actividad de una empresa filial puede afectar a la empresa matriz, y viceversa.

Para otros autores, uno de los aspectos críticos a tener en cuenta cuando se implantan los sistemas de análisis y gestión del riesgo es si el proceso se realiza de manera eficiente, facilitando el ahorro de costes [22, 23], ya que estos pueden influir en el dimensionamiento del modelo de gestión de la seguridad. De esta forma, en [24] se propone asociar como parte fundamental del desarrollo de los SGSI los análisis de coste–beneficio (CBA) en la fase del análisis de riesgos. Pero aquí surge la problemática de cómo calcular de forma objetiva el valor monetario de los activos que debemos proteger. Durante la investigación, se han encontrado muy pocos estudios enfocados a la tasación de sistemas de información y

L. E. Sánchez, PROMETEO, Escuela Politécnica del Ejército extensión Latacunga (ESPEL), Latacunga (Cotopaxi), Ecuador, luisenrique@sanchezcrespo.org

A. Santos-Olmo, Departamento I+D+i, Sicaman Nuevas Tecnologías, Tomelloso (Ciudad Real), España, asolmo@sicaman-nt.com

E. Alvarez, Departamento I+D+i, Fundación In-nova S.L, Toledo, España, ealvarez@in-nova.org

E. Fernandez-Medina, Grupo de Investigación GSyA, Universidad de Castilla-la Mancha, Ciudad Real, España, Eduardo.FdezMedina@uclm.es

M. Piattini, Grupo de Investigación Alarcos, Universidad de Castilla-la Mancha, Ciudad Real, España, Mario.Piattini@uclm.es

a la obtención de formulas para calcular el valor de los activos contenidos en un sistema de información [25].

Otros investigadores [22, 23, 26] destacan la problemática de la cantidad de aspectos subjetivos que deben definirse a la hora de generar un análisis de riesgos, y que hacen que los resultados queden limitados para el uso interno de la compañía, pero que no puedan ser tenidos en cuenta por terceras partes interesadas en resultados objetivos y replicables con independencia del consultor que los realice. Así, Garigue [23] remarca en sus investigaciones que, actualmente, los gerentes no sólo desean saber qué se ha realizado para mitigar los riesgos, sino que también se debe poder dar a conocer eficaz y objetivamente cómo se ha realizado esta tarea, y si se ha conseguido ahorrar dinero. Por ello, algunos investigadores han intentado desarrollar métricas y algoritmos que permitan minimizar estos aspectos subjetivos [26].

También debemos tener en cuenta que el análisis de riesgos es un proceso costoso, y que las metodologías actuales no están pensadas para repetir el proceso cada vez que se realice una modificación. Por esto, es importante desarrollar metodologías específicas que permitan mantener los resultados del análisis de riesgos sin encarecer los costes. El proyecto de la UE Coras [27, 28] hace de este mantenimiento del análisis de riesgos el punto principal de su modelo. También las investigaciones de Alhawari [29] se han centrado en intentar reutilizar el conocimiento adquirido en las diferentes implantaciones, para intentar obtener resultados más económicos, con menor nivel de subjetividad y que permitan generar análisis de riesgos dinámicos sin incurrir en costes excesivos.

Existen otras muchas investigaciones sobre análisis de riesgos que también hemos tenido en cuenta. Entre ellas se puede destacar la propuesta de Barrientos [30] y UE CORAS (IST–2000–25031) [27, 28]. La propuesta de Barrientos [30] está basada en llevar a cabo un análisis relativo a la seguridad informática para identificar el grado de vulnerabilidad y determinar los aspectos de mejora a ser llevados a cabo en la organización con el objeto de reducir el riesgo. Por otro lado, UE CORAS (IST–2000–25031) [27, 28] está desarrollando un marco para el análisis de riesgos de seguridad que utiliza UML2, AS/NZS 4360, ISO/IEC17799, RM–ODP6, UP7 y XML8.

Por lo tanto, podemos concluir que los modelos de análisis y gestión del riesgo son fundamentales para las empresas, pero que no existen metodologías que se adecuen al caso de las PYMES, y las existentes se muestran ineficientes para este tipo de compañía. Por otro lado, las metodologías también tienen importantes carencias para empresas que no sean PYMES, al carecer de mecanismo 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.

Así, teniendo en cuenta las investigaciones y carencias detectadas por otros científicos, que validan las observaciones realizadas por nosotros en casos reales, podemos concluir que es necesario profundizar en la investigación mediante la realización de una revisión sistemática para comprobar el estado de la cuestión, y si se observa que este tipo de aspectos no son convenientemente tenidos en cuenta en las metodologías actuales, se trabajará en realizar un nuevo marco metodológico, así como en la elaboración de nuevas métricas, ontologías y algoritmos que permitan solucionar todos los problemas anteriormente mencionados.

El artículo continúa en la Sección 2, describiendo los trabajos de investigación y estándares relacionados con la investigación. En la Sección 3 se describe brevemente la metodología MARISMA. Finalmente, en la Sección 4 concluimos indicando cuál será el trabajo que desarrollaremos en el futuro y cuáles han sido las principales aportaciones de la investigación hasta el momento actual.

II. TRABAJO RELACIONADO

En esta sección se muestra el estado del arte relacionado con las diferentes propuestas de la investigación.

En nuestra investigación hemos podido comprobar que apenas hay estudios centrados en la tasación de sistemas de información [25], por lo que este capítulo se ha centrado en estudiar las principales metodologías de análisis de riesgos que se están utilizando actualmente, y en la realización de una revisión sistemática de propuestas de metodologías de análisis de riesgos, tomando como principales aspectos de las mismas los factores de jerarquía y asociatividad del riesgo, así como que estén orientadas a su implantación en PYMES. Esta sección se encuentra estructurada en tres apartados:

- En primer lugar se introducen algunos conceptos básicos sobre Análisis de Riesgos, dado que son los elementos principales que conforman la investigación.
- En segundo lugar se presenta el estado del arte de las principales metodologías y estándares de análisis de riesgos que se utilizan en la actualidad. Estos estándares y grandes metodologías se han mostrado ineficaces a la hora de implantarse en PYMES [31], por lo que lo interesante es poder extraer sus principales características de cara a ver si pueden ser adaptadas a una metodología de análisis de riesgos orientada a este tipo de compañías.
- En tercer lugar, y ya de cara a realizar un estado del arte en consonancia con los objetivos específicos de esta investigación, se presenta una revisión sistemática de las metodologías y modelos para el análisis de riesgos asociativos y jerárquicos orientados a PYMES.

A. Análisis de riesgos y seguridad de la información

Un 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 [32]. Para ello, se seleccionan e implementan salvaguardas para poder conocer, prevenir, impedir, reducir o controlar los riesgos identificados. Esto es lo que se entiende como gestión de riesgos.

De forma más técnica, el análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegidos se encuentran los activos. En coordinación con los objetivos,

estrategia y política de la organización, las actividades de gestión de riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que acepta la dirección.

Toda esta información y cómo se lleva a cabo está recogida en lo que se denomina metodologías de análisis de riesgos. Aunque es cierto que existe un gran número de metodologías para este tema, se puede decir que la mayoría tienen puntos en común. Según [32] las metodologías de análisis de riesgos tienen como punto de partida identificar formalmente los elementos a proteger o aquellos que tienen un valor para la organización, lo que se llamarán activos.

Uno de los puntos de divergencia entre las metodologías es cómo cuantificar todos estos elementos que forman parte del análisis de riesgos. Una posible clasificación se puede encontrar en [33] donde se definen tres enfoques distintos:

- *Enfoque cuantitativo:* el análisis de riesgos es una aproximación matemática al problema de cuantificar los elementos. Este enfoque requiere un gran esfuerzo de cálculo y su consecuente tiempo para la realización del mismo. Debido al arduo proceso matemático que conlleva, el enfoque cuantitativo está basado en probabilidades. La mayoría de las metodologías y de sus herramientas adjuntas usa algoritmos para calcular la frecuencia de la amenaza y probabilidad de su ocurrencia.
- *Enfoque cualitativo:* es un enfoque menos árido que el anterior. No se usan probabilidades, sino que se hacen estimaciones potenciales de pérdida. Se describen valores para los parámetros usando términos como "alto", "medio" o "bajo". El enfoque cuantitativo conlleva menos incertidumbre y tiene en consideración el conocimiento y las opiniones del personal que está inmerso en el proceso de análisis de riesgos. Este enfoque está siendo considerado más adecuado para captar los requerimientos de los sistemas.
- *Enfoque basado en conocimiento:* el análisis basado en conocimiento consiste en reutilizar el mejor método de sistemas similares. Esta visión fue ampliamente usada en los años primigenios de la informática, donde el número de activos y sus vulnerabilidades podían ser contados con los dedos de una mano.

B. Estándares y Metodologías de Análisis de Riesgos

Como se citó anteriormente, los estándares y las grandes metodologías de análisis de riesgos son bastante amplios y detallados. En este apartado se desgranan las principales características de cada una de las metodologías estudiadas, y los elementos más destacables de las mismas.

- *ISO/IEC 13335 [34]:* Inicialmente fue concebida como una serie de informes técnicos que engloban un conjunto de directrices para la gestión de la seguridad informática.
- *ISO TR 13335-4:2008 [35]* incluye una selección de salvaguardas. Dicho documento se incluyó posteriormente en la ISO 27005:2008 [36].
- ISO/IEC 27002 [37]: La ISO 27002 versa sobre la seguridad de los activos de la información, que va más allá de los propios elementos existentes en los sistemas de tecnologías de información.
- *ISO/IEC 27005 [36]:* Cimentada en los informes técnicos ISO/IEC TR 13335-3:1998 [38], ISO/IEC TR 13335-4:2000 [35] y BS 7799-3:2006 [39]. Complementa a sus normas hermanas ISO 27001 [40] e ISO 27002 [41]. En este estándar se trata la gestión de riesgos en la seguridad de la información. La metodología está especificada en [42].
- *NIST SP 800-30 [43]:* El Instituto Nacional de Normas y Tecnología (National Institute of Standards and Technology) es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. El NIST SP 800-30 contiene una guía para el Análisis y Gestión de Riesgos en los sistemas de las tecnologías de la información.
- *AS/NZS 4360 [44]:* AS/NZS 4360 es un estándar de gestión de riesgos publicado conjuntamente por Australia y Nueva Zelanda. El estándar propone una guía genérica para establecer e implementar un proceso de análisis de riesgos donde se incluye la identificación, análisis, evaluación, tratamiento y una continua monitorización del riesgo [45].
- *MAGERIT v2 [32]:* La Metodología de Análisis y GEstión de Riesgos de IT (MAGERIT) fue desarrollada por el Consejo Superior de Administración Electrónica (CSAE) y hecha pública por el Ministerio de Administraciones Públicas en 1997. Es una metodología abierta y de obligado cumplimiento por parte de las Administraciones Públicas.
- *OCTAVE [46]:* OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) es un marco desarrollado por el Instituto de Ingeniería del Software Carnegie Mellon (Pittsburgh, Pennsylvania, EEUU) para crear metodologías de Análisis y Gestión de Riesgos. Inicialmente OCTAVE fue desarrollado para empresas cuyo personal estuviera por encima de los 300. Sin embargo, se ha intentado que fuera más flexible y abarcara un rango más amplio de empresas [47].
- *MEHARI [48]:* MEHARI (Méthode Harmonisée d'Analyse de Risques) o Método de Análisis de Riesgos Armonizado, es un método de análisis y gestión de riesgos desarrollado por CLUSIF (Club de la Seguridad de la Información Francesa) y soportado por el software gestionado por la compañía Risicare.
- *CRAMM [49]:* CRAMM (CCTA Risk Assessment and Management Technology) es una metodología de análisis de riesgos desarrollada por la organización gubernamental británica CCTA (Central Communication and Telecommunication Agency).

C. Comparación de Propuestas

A continuación se mostrará una tabla comparativa con los estándares y metodologías que se han tratado para tener una visión global de ellos.

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**
ISO13335	S	S	S	S	S	S	S	S	S	S	S	N	N	N	N	N	N	N
ISO27002	S	S	N	S	S	S	S	S	S	S	S	N	N	N	N	N	N	N
ISO27005	S	S	S	S	S	S	S	S	S	S	S	N	N	N	N	N	N	N
NIST SP 800-30	S	S	N	S	S	S	N	N	S	S	S	N	N	N	N	N	N	N
AS/NZS 4360	S	S	S	S	S	S	N	S	S	S	S	N	N	N	N	N	N	N
MAGERIT	S	S	N	S	S	S	S	S	N	S	S	N	N	N	N	N	N	N
OCTAVE	S	S	S	S	S	S	N	S	S	S	S	N	N	N	N	N	N	N
MEHARI	S	S	N	S	S	S	N	S	S	S	S	N	N	N	N	N	N	N
CRAMM	S	N	N	S	S	S	N	S	S	S	S	N	N	N	N	N	N	N
MARISMA	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S

Tabla 1. Comparativa de principales metodologías y estándares de A. de Riesgos

Como se puede ver en la comparativa, ninguno de los principales estándares y metodologías de análisis de riesgos existentes en la actualidad están teniendo en cuenta los aspectos que nosotros hemos identificado en la investigación, como necesarios para la metodología de análisis de riesgo deseable. Estas características deseables se han obtenido a través de la aplicación del "método de investigación-acción" a casos reales. Se considera que cada uno de estos aspectos puede ser totalmente cumplido (Sí), o no tenido en cuenta por el modelo (No):

- *Orientado a PYMES:* Es decir, sistemas de análisis de riesgos que requieren pocos recursos para su elaboración y mantenimiento.
- *Dinámico:* Capacidad de cambiar según cambian los activos y las dependencias de estos.
- *Reutilización del conocimiento:* Capacidad de almacenar el conocimiento adquirido en diferentes implantaciones, con el objetivo de reducir los costes de generación y mantenimiento de nuevos análisis de riesgos, así como el grado de incertidumbre en la generación del mismo.
- *Asociativo:* El modelo tiene en cuenta la distribución del riesgo (por ejemplo, funciones derivadas a terceros, o realizadas por la empresa en colaboración con otras empresas) y la interrelación de la empresa con el entorno.
- *Jerárquico:* El modelo tiene en cuenta la relación jerárquica entre compañías relacionadas. (Por ejemplo, el esquema Matriz – Filiales).
- *Tasación de activos:* El análisis de riesgos permite obtener una tasación monetaria objetiva de los activos.
- *Control de incertidumbre:* El análisis de riesgos minimiza el grado de incertidumbre en la generación, es decir, la generación por parte de dos consultores de un análisis de riesgos sobre los mismos activos y los mismos interlocutores genera el mismo o parecido resultado, con desviaciones mínimas.

D. Revisión Sistemática de Metodologías de Análisis y Gestión de Riesgos Asociativos y Jerárquicos

1) Planificación de la revisión

En esta revisión sistemática se pretende localizar trabajos centrados en el desarrollo de modelos y metodologías de análisis de riesgos, con el objetivo de que puedan ser aplicadas en PYMES y puedan adaptarse a cubrir riesgos asociativos y jerárquicos. Podemos definir la pregunta de investigación de este trabajo, por tanto, de la siguiente forma:

¿Qué trabajos se han llevado a cabo para desarrollar sistemas de análisis de riesgos teniendo en cuenta riesgos jerárquicos, asociativos y aplicación en PYMES?

2) Ejecución de la selección y Extracción de la información

A continuación se ofrece una breve reseña de cada uno de los estudios seleccionados:

- *Nachtigal, S. "E-business Information Systems Security Design Paradigm and Model" [50]:* El autor propone un modelo de seguridad de la información en comercio electrónico cubriendo el diseño y gestión de la Seguridad de la Información en este tipo de negocios, y relacionándola con los sistemas de gestión relacionados con riesgos asociativos y jerárquicos.
- *Abdullah, H. "A Risk Analysis and Risk Management Methodology for Mitigating Wireless Local Area Networks (WLANs) Intrusion Security Risks" [51]:* El autor propone una Metodología de análisis y gestión de riesgos con aplicación sobre las redes WLAN. La metodología propuesta está basada en la metodología de análisis de riesgos OCTAVE. Se trata de un estudio teórico, sin contrastar resultados con aplicación de la metodología en casos prácticos.
- *Arikan, A.E. "Development of a risk management decision support system for international construction projects" [52]:* El autor propone un modelo conceptual de gestión del riesgo y un prototipo de Sistema de Soporte a las Decisiones (DSS) para gestión del riesgo en proyectos de construcción. Sin embargo, los modelos propuestos se han considerado muy interesantes de cara a ser extrapolados a Sistemas

de Información. El autor propone también un Modelo de Gestión de Riesgos de Información (IRMS) que incluye la identificación de riesgos mediante el uso integrado de una Estructura Jerárquica de Distribución de Riesgos (HRBS), planteando de esta forma la importancia de la gestión de riesgos asociativos y jerárquicos, y siendo una base de modelo adaptable a la estructura de un sistema en Cloud.

- *Bagheri, E. et al. "Astrolabe: A Collaborative Multiperspective Goal-Oriented Risk Analysis Methodology" [53]:* Los autores presentan una metodología de análisis de riesgos llamada Astrolabe, basada en el análisis causal de los riesgos de los Sistemas de Información. Se trata de un estudio teórico, sin contrastar resultados con aplicación de la metodología en casos prácticos.
- *Alhawari, S. et al. "Knowledge-Based Risk Management framework for Information Technology project" [29]:* Los autores presentan un Framework conceptual llamado Knowledge-Based Risk Management (KBRM) que emplea procesos de Gestión del Conocimiento (KM) para mejorar la eficacia de la gestión de riesgos y aumentar la probabilidad de éxito en proyectos de Tecnología de la Información (TI). Se trata de un estudio teórico, sin contrastar resultados con aplicación de la metodología en casos prácticos.
- *ICES Resource Management Committee. "Report of the Study Group on Risk Assessment and Management Advice (SGRAMA)" [54]:* El Comité destaca la importancia del análisis de riesgos en todos los campos de la ingeniería, y la necesidad de desarrollar un Framework para la gestión de riesgos, aunque centrado en los campos de exploración marina y ecología, principalmente.
- *Strecker, S et al. "RiskM: A multi-perspective modeling method for IT risk assessment" [55]:* Los autores proponen un método conceptual de modelado llamado RiskM, con el objetivo principal de cumplir con los requisitos esenciales en el ámbito de evaluación de riesgos de TI. Se trata de un estudio teórico, sin contrastar resultados con aplicación de la metodología en casos prácticos.
- *Ma, Wei-Ming. "Study on Architecture-Oriented Information Security Risk Assessment Model" [56]:* El autor desarrolla un modelo orientado a la arquitectura para la evaluación del riesgo en Seguridad de la Información (AOISRAM). Su objetivo principal es, según el autor, cubrir bastantes dificultades causadas por el modelo propuesto en la ISO 27001:2005, que es orientado a procesos. Entre otros inconvenientes, el autor destaca: distribución desigual de los recursos, pobre rendimiento de la seguridad y alto riesgo. Se trata de un estudio teórico, sin contrastar resultados con aplicación de la metodología en casos prácticos.
- *Feng, Nan et al. "An information systems security risk assessment model under uncertain environment" [26]:* Los autores proponen un modelo de evaluación de riesgos en Sistemas de Seguridad de la Información basado en la teoría de la evidencia (generalización de la teoría Bayesiana de probabilidad subjetiva). El modelo está contrastado con un caso práctico de estudio, pero es muy genérico y no está soportado por ninguna herramienta software.
- *Carlsson, C. et al. "Predictive Probabilistic and Possibilistic Models Used for Risk Assessment of SLAs in Grid Computing" [57]:* Los autores desarrollan un modelo híbrido (probabilístico y posibilístico) para la evaluación de riesgos centrado en riesgo asociado a Acuerdos de Nivel de Servicio (SLA) en entornos de computación en Grid/Cluster. También hace constar la importancia del entorno y de terceros en la evaluación del riesgo y, por tanto, la necesidad de de una gestión de riesgos asociativos, de gran importancia en sistemas en Cloud, aunque no se llega a concretar una propuesta en este sentido. Esto mismo se contrasta en Hussain, O. et al. "Semantic Similarity Model for Risk Assessment in Forming Cloud Computing SLAs" [58], donde se desarrolla un modelo para la gestión de riesgos centrado en riesgo asociado a Acuerdos de Nivel de Servicio (SLA) en entornos de Cloud Computing. El mismo autor, en el artículo "A Methodology for Transactional Risk Assessment and Decision Making in e-Business Interactions" [59] centra la importancia del análisis de riesgos en entornos de comercio electrónico, poniendo de relevancia la importancia de una evaluación de riesgos asociativos, aunque sin entrar en una propuesta que cubra la asociatividad o jerarquía en el análisis de riesgos.
- *Tjoa, S. et al. "Enhancing Business Impact Analysis and Risk Assessment applying a Risk-Aware Business Process Modeling and Simulation Methodology" [60]:* Los autores presentan una metodología de evaluación de procesos orientada al riesgo llamada ROPE (Risk-Oriented Process Evaluation). Esta metodología está orientada sobre todo al desarrollo y simulación de planes de negocio. Se trata de un estudio teórico, sin contrastar resultados con aplicación de la metodología en casos prácticos.
- *Abraham, A. "Nature Inspired Online Real Risk Assessment Models for Security Systems" [61]:* Los autores presentan las ventajas de uso de métodos de inferencia difusa (fuzzy inference) para desarrollar modelos inteligentes de evaluación de riesgos en línea (intelligent online risk assessment models). También presentan una optimización de los sistemas de inferencia difusa con el aprendizaje neuronal y el aprendizaje evolutivo para el uso de estos modelos en un entorno en línea.
- *Chang, She-I et al. "The development of audit detection risk assessment system: Using the fuzzy theory and audit risk model" [62]:* Los autores presentan un sistema de detección de riesgos en

auditoría. Para implementar el sistema, se utiliza la teoría difusa (fuzzy theory) y el modelo de riesgo de auditoría para calcular el grado de detección de riesgo que permite al personal de auditoría determinar con mayor precisión la cantidad de evidencias de auditoría reunidas y construir un sistema de evaluación de la detección de riesgos de auditoría. Este sistema se evalúa sobre un caso de prueba. La teoría difusa se emplea también en el trabajo Wang, Ping et al. "A Fuzzy Decision Model of Risk Assessment Through Fuzzy Preference Relations with Users'Confidence-interval" [63], definiendo un modelo difuso de análisis de riesgos, aunque de forma muy general. Es interesante el concepto de aplicación de modelos difusos al análisis de riesgos, aunque es necesario centrar el ámbito de aplicación en la PYME, al abarcar un marco de aplicación más general

- *Yang, Fu-Hong et al. "A Risk Assessment Model for Enterprise Network Security" [64]:* Los autores presentan una propuesta conceptual de modelo para el análisis de riesgo de la seguridad de Sistemas de Información centrada en el ámbito de las redes locales de la empresa bajo la amenaza de infección y propagación de virus informáticos. Este modelo, llamado "Graph Model", se diseña con el objetivo de mapear en forma de grafo las infraestructuras de TI de la empresa, tanto sistemas como redes. La principal ventaja del modelo propuesto es poder reflejar de una forma gráfica el estado del riesgo en la red, y que la dirección pueda ver de forma sencilla si las inversiones realizadas en seguridad están en consonancia con el riesgo existente, o qué puntos son los más prioritarios para invertir en seguridad dentro de la red de la empresa. Se trata de un estudio teórico, sin contrastar resultados con aplicación de la metodología en casos prácticos.
- *Kumar, V. et al. "Integrated Fuzzy Approach for System Modeling and Risk Assessment" [65]:* Los autores proponen una técnica de modelado de Sistemas, incluyendo una parte de evaluación del riesgo, empleando técnicas difusas (fuzzy). El modelo está contrastado con un caso práctico de estudio, aunque centrado en riesgos medioambientales.
- *Wawrzyniak, D. "Information Security Risk Assessment Model for Risk Management" [66]:* El autor propone un modelo de evaluación y gestión del riesgo en Sistemas de Información, con el objetivo principal de que sea flexible y sencillo de utilizar. Este modelo tiene un hándicap importante, que es que su efectividad a la hora de la implantación y gestión depende en un grado muy alto del conocimiento experto del consultor, lo cual lo hace muy difícil de adaptar al caso de las PYMES.
- *Lin, Mengquan et al. "Methodology of Quantitative Risk Assessment for Information System Security" [67]:* Los autores proponen una metodología para la evaluación de riesgos en la seguridad de los Sistemas de Información. Esta metodología está basada en métodos cuantitativos de obtención de pesos de los criterios que indican la forma de evaluar la seguridad general del Sistema de Información. No se presenta tampoco la metodología completa, sino sólo los métodos de base para obtener los pesos de los criterios de evaluación.
- *Hewett, R. et al. "A Risk Assessment Model of Embedded Software Systems" [68]:* Los autores proponen una técnica para representar y evaluar los riesgos asociados al software integrado en sistemas en determinados sistemas. No se presenta tampoco la metodología completa, ni se contrastan los resultados con la aplicación en casos prácticos.
- *Lo, Chi-Chun et al. "A hybrid information security risk assessment procedure considering interdependences between controls" [69]:* Los autores proponen un procedimiento híbrido para evaluar los niveles de riesgo de la seguridad de la información bajo diferentes controles de seguridad. El procedimiento propuesto es poco flexible y fundamentalmente teórico, sin contrastar resultados con su aplicación en casos prácticos.
- *Patel, S.C. et al. "Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements" [70]:* Los autores proponen un método para evaluar la vulnerabilidad de una organización ante brechas en los sistemas de seguridad de la información. Se presenta un método cuantitativo para medir el riesgo en términos de un valor numérico llamado "grado de seguridad cibernética". El procedimiento propuesto es fundamentalmente teórico. Se aplica en un caso práctico, pero es demasiado global y sin detallar demasiado los procesos llevados a cabo para obtener los resultados. También es difícil de aplicar en el caso de las PYMES, y sobre todo a entornos Cloud, ya que requiere un alto grado de conocimiento experto para su mantenimiento, y se centra sobre todo en riesgo de ataque cibernético, siendo demasiado específico.
- *Yu-Ping Ou Yang et al. "A VIKOR technique based on DEMATEL and ANP for information security risk control assessment" [71]:* Los autores proponen un modelo de evaluación del riesgo en seguridad de la información. Se trata de un proceso desarrollado con una estrategia Plan-Do-Check-Act (PDCA), definiendo un ciclo continuo de evaluación, tratamiento, monitorización de los riesgos y mejora de la seguridad. Los autores han definido un caso de estudio para aplicar y refinar este modelo.
- *Salmeron, J.L. et al. "A multicriteria approach for risks assessment in ERP maintenance" [72]:* Los autores presentan una taxonomía general para la evaluación y gestión de riesgos que afectan a los sistemas y personal involucrado con el mantenimiento de los ERP (Enterprise Resource Planning). Los autores emplean el Proceso Analítico Jerárquico

(AHP) para analizar los factores de riesgo identificados. Se trata de un estudio teórico, sin contrastar resultados con aplicación de la metodología en casos prácticos.

3) Análisis de resultados

A continuación, en la Tabla 2, se puede ver una comparativa de las diferentes propuestas analizadas.

Se considera que los aspectos valorados se pueden cumplir de forma total, parcialmente o no haber sido abordados en el modelo. A continuación, se describe cada uno de los aspectos analizados:

- *Ámbito de aplicación:* Si el modelo se aplica de forma global a la seguridad los Sistemas de Información de una compañía, o sólo a un subconjunto de ellos.
- *Métricas:* La guía incluye mecanismos de medición de los criterios de riesgo claros, detallando información sobre su aplicación y evaluación.
- *Técnicas cualitativas:* El modelo incluye técnicas cualitativas de medición.
- *Técnicas cuantitativas:* El modelo incluye técnicas cuantitativas de medición.
- *Asociativo:* El modelo tiene en cuenta la distribución del riesgo (por ejemplo, funciones derivadas a terceros, o realizadas por la empresa en colaboración con otras empresas) y la interrelación de la empresa con el entorno.
- *Jerárquico:* El modelo tiene en cuenta la relación jerárquica entre compañías relacionadas. (Por ejemplo, el esquema Matriz – Filiales).
- *Orientado a PYMES:* El modelo ha sido desarrollado pensando en la casuística especial de las PYMES.
- *Reutiliza el conocimiento:* La guía adquiere conocimiento de las implantaciones y de la información recogida durante su utilización, de forma que este conocimiento pueda ser reutilizado para facilitar posteriores implantaciones.
- *Dispone de herramienta software:* El modelo dispone de una herramienta que lo soporte.
- *Casos prácticos:* El modelo ha sido desarrollado y refinado a partir de casos prácticos.
- *Tasación de activos:* El análisis de riesgos permite obtener una tasación monetaria objetiva de los activos.
- *Control de incertidumbre:* El análisis de riesgos minimizar el grado de incertidumbre en la generación, es decir, la generación por parte de dos consultores de un análisis de riesgos sobre los mismos activos y los mismos interlocutores genera el mismo o parecido resultado, con desviaciones mínimas.
- *Dinámico:* Capacidad de cambiar según cambian los activos y las dependencias de estos.

Estas características deseables para un modelo de análisis y gestión de riesgos asociativos y jerárquicos para PYMES se han obtenido a través de la aplicación del "método de investigación-acción" a casos reales. Se considera que cada uno de estos aspectos puede ser totalmente cumplido (Sí), parcialmente cumplido (P) o no tenido en cuenta por el modelo (No).

Iniciativa	Ámbito Global	Métricas	Técnicas Cualitativas	Técnicas Cuantitativas	Asociativo	Jerárquico	Orientado PYMES	Reutilización Conocimiento	Herramienta Software	Casos Prácticos	Dinámico	Tasación Activos	Control Incertidumbre
Nachtigal, S.	N	P	N	N	P	N	P	N	N	P	N	N	N
Abdullah, H	N	N	S	N	N	N	S	N	N	N	N	N	N
Arikan, A.E.	N	N	N	N	P	S	N	N	N	S	N	N	N
Bagheri, E.	S	S	S	N	N	N	N	N	N	N	N	N	N
Alhawari, S.	N	N	N	N	N	N	N	S	N	N	N	N	N
ICES RMC	N	N	N	N	P	N	N	N	N	N	N	N	N
Strecker, S.	S	N	P	P	N	N	N	N	N	N	N	N	N
Ma, Wei-Ming	S	N	N	N	P	P	P	N	N	N	N	N	N
Feng, Nan.	S	N	S	S	P	N	N	N	N	S	N	N	S
Carlsson, C Hussain, O.	N	N	S	S	P	N	N	N	N	N	N	N	N
Tjoa, S.	N	N	S	N	N	N	N	N	N	N	N	N	N
Abraham, A.	N	N	N	N	P	N	N	S	N	N	N	N	N
Chang, She-I Wang, Ping	N	P	P	N	P	N	N	N	N	S	N	N	S
Yang, Fu-Hong	N	N	N	N	P	N	N	N	N	N	N	N	N
Kumar, V.	N	N	N	N	P	P	N	N	N	S	N	N	S
Wawrzyniak, D.	S	N	S	N	N	N	N	N	N	N	N	N	N
Lin, Mengquan	S	P	N	S	N	N	N	N	N	N	N	N	N
Hewett, R.	N	N	N	N	P	N	N	S	N	N	N	N	N
Lo, Chi-Chun	N	P	S	S	P	N	N	N	N	N	N	N	N
Patel, S.C.	S	P	N	S	N	N	N	N	N	N	N	N	N
Yu-Ping Ou Yang et al.	S	P	S	S	N	N	N	N	N	S	N	N	N
Salmeron, J.L.	N	N	S	N	N	P	N	N	N	N	N	N	N
MARISMA	**S**	**S**	**S**	**S**	**S**	**S**	**S**	**S**	**S**	**S**	**S**	**S**	**S**

Tabla 2. Comparativa de las propuestas seleccionadas.

Se puede ver cómo ninguna de las propuestas estudiadas posee las características requeridas por las PYMES:

- No están pensadas para su aplicación en empresas de pequeño tamaño y, por tanto, con escasos recursos humanos y económicos.
- La mayoría se centran sólo en el análisis de riesgos de una parte del Sistema de Información, y casi ninguna de ellas aborda desde un punto de vista global la implantación de estos sistemas, lo que obligaría a las compañías a tener que adquirir, implementar, gestionar y mantener varias metodologías, modelos y herramientas para gestionar de forma integral los riesgos.
- La mayoría de las propuestas no tienen en cuenta la necesidad de contemplar riesgos jerárquicos y asociativos y, las que lo hacen, lo realizan desde un

punto de vista teórico, sin establecer mecanismos concretos y basados en casos prácticos para gestionar este tipo de riesgos.

- Muy pocas se han centrado en disminuir el grado de incertidumbre a la hora de calcular los riesgos.
- Casi ninguna tiene reutilización del conocimiento.
- Y ninguna ha tenido en cuenta la importancia de poder actualizarse de forma dinámica y con bajo coste, ni la posibilidad de obtener una tasación monetaria y objetiva de los activos.

Por lo tanto, es relevante realizar un nuevo marco metodológico que permita incluir todas esas características, incluyendo la automatización de las métricas para reducir los costes de mantenimiento del sistema.

III. FRAMEWORK MARISMA

El principal objetivo de esta investigación es el desarrollo de 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.

El principal problema que encuentran actualmente las compañías de seguros a la hora de valorar económicamente un sistema de información es que no cuentan con ningún mecanismo o metodología que les permita realizar una tasación económica objetiva del mismo, ni análisis de riesgos con bajo grado de incertidumbre. Actualmente, distintas personas, en base a sus propios criterios subjetivos, obtendrán tasaciones muy diferentes del valor económico de un sistema de información, y de los riesgos a que este está sometido, incluso contando con el mismo interlocutor dentro de la compañía, lo que hace imposible a día de hoy para una compañía de seguros acometer el aseguramiento económico de los sistemas de información de una empresa. Esto adquiere especialmente relevancia cuando 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 [3], y más cuando en la era del conocimiento la información se está convirtiendo en el activo más importante para las compañías y de mayor valor económico. Estos activos están sometidos a riesgos de una gran variedad, que pueden afectar de forma crítica a la empresa.

De cara a hacer posible la obtención de una valoración económica objetiva de un sistema de información y de los riesgos a los que están sometidos estos activos, con el menor grado de incertidumbre, con el objetivo de permitir a una compañía aseguradora poder realizar un seguro del mismo, o permitir conocer a un tercero los riesgos que asume al ceder un activo o colaborar con la compañía, planteamos la necesidad de desarrollar un marco metodológico que permita realizar este proceso.

Como se puede ver en la siguiente ilustración, el marco metodológico estará formado por tres componentes:

- *MI:* Contendrá el modelo de información, y estará formado por las Ontologías y las bases de conocimiento del marco metodológico.
- *I:* Contendrá todas las métricas que nos permitirán las tasaciones económicas objetivas de los activos, y las reducciones del nivel de incertidumbre en la elaboración del análisis de riesgos.
- *M:* Contendrá la propia metodología de tasación y análisis y gestión del riesgo.

En las siguientes sub-secciones se irán detallando los principales elementos y características del marco de trabajo que se está desarrollando.

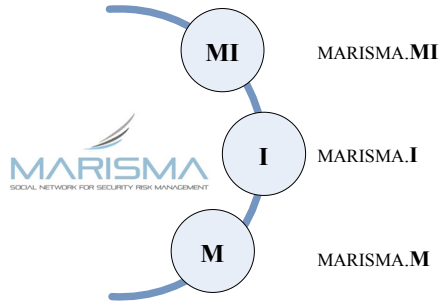


Figura 1. Fases de la metodología

A. *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 metodología que se pretende desarrollar. Estará formada por un conjunto de ontologías y una base de conocimiento, que nos permitirá reutilizar el conocimiento adquirido en diferentes implantaciones, y que estará basada en las investigaciones realizadas por [29, 68], entre otras.

Para el desarrollo de estas Ontologías, debemos ser capaces de analizar las tres dimensiones del problema:

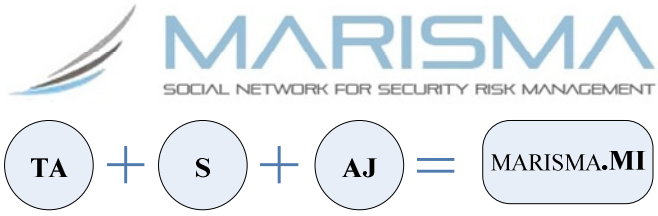


Figura 2. Dimensiones de la Ontología sobre la que se construirá la metodología

- *Conceptos relacionados con el campo de la tasación de activos (TA):* para abarcar este dominio del problema, analizaremos otras investigaciones y estándares existentes. Las investigaciones realizadas hasta el momento han concluido que existen muy pocos estudios y estándares relacionados con la materia [25]. Se ha intentando acceder a los sistemas de tasación de compañías de internet utilizados por los

"Business Angels", pero está considerada como información confidencial, por lo que no se ha podido validar su utilidad.

- *Conceptos relacionados con el campo de la seguridad (S):* para abarcar este dominio del problema, utilizaremos los principales estándares relacionados con la gestión de la seguridad de Sistemas de Información, en especial los relacionados con el análisis y gestión de riesgos (ISO27005, MAGERIT, OCTAVE, …) [32, 34, 36, 37, 43, 44, 46, 48, 49] y orientados en especial a disminuir el nivel de incertidumbre de la generación de un análisis de riesgos .
- *Conceptos relacionados con la interrelación de compañías (asociatividad y jerarquía) (AJ):* para abarcar este dominio del problema, y ante la ausencia de estándares oficiales, utilizaremos los estudios obtenidos durante la revisión sistemática, que serán complementados con los resultados prácticos obtenidos de aplicar la investigación en caso reales mediante el método científico "investigación en acción".

El conjunto resultante de analizar estos tres dominios sobre un campo común como son los sistemas de información, dará lugar a un conjunto de Ontologías que podremos aplicar sobre la metodología que estamos desarrollando.

B. *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 monetaria como en cuanto a importancia dentro de la empresa) de los activos del sistema de información.

Una vez que hemos desarrollado la primera fase del marco de trabajo y obtenida una Ontología, ésta se utilizará entre otras cosas para obtener reglas del sistema de tasación. Por último, estas reglas se utilizarán para aplicar factores derivados de las posibles relaciones de cada activo, amenaza y vulnerabilidad en cuanto a la jerarquía y asociatividad de la compañía dentro de su entorno, buscando siempre reducir el nivel de incertidumbre.

El objetivo último perseguido en esta fase es ser capaces de localizar y desarrollar indicadores y métricas que nos permitan calcular de forma semi-automática los valores de los activos y el nivel de riesgo al que están expuestos, reduciendo el nivel de incertidumbre en la elaboración del análisis de riesgos. De esta forma, esta parte de la investigación permitirá la consecución completa de los siguientes objetivos: i) Diseñar métricas para la valoración y tasación de activos de información; ii) Diseñar métricas para la valoración de las amenazas; iii) Diseñar métricas para la valoración de activos de información en base a criterios de riesgo; iv) Diseñar métricas para la valoración de controles de seguridad en base a estándares existentes y para calcular la probabilidad de ocurrencia de una vulnerabilidad.

C. *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 riesgo 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 siguiente figura:

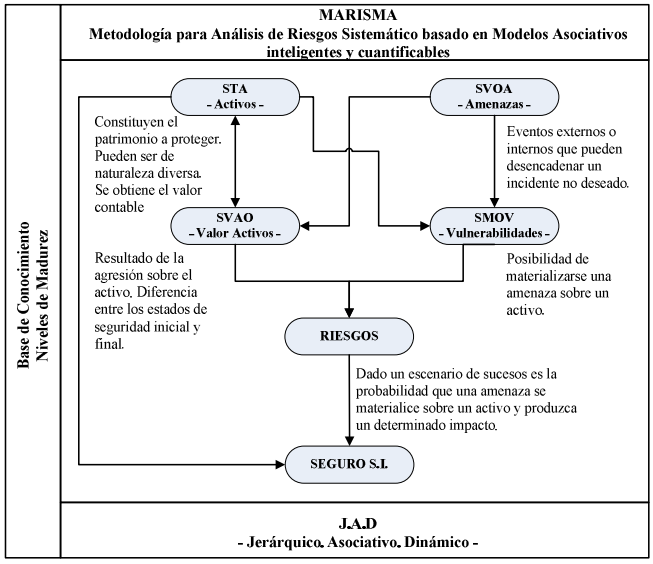


Figura 3. Esquema general de la metodología

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. Esta tasación se realizará en base a criterios totalmente objetivos, de forma que el valor de los activos no varíe si dos consultores diferentes realizan la tasación sobre los mismos activos. La tasación tendrá en cuenta también que pueden actuar sobre el valor de un activo dos tipos de factores: i) Factores jerárquicos: Por ejemplo, en el caso de una empresa filial, es posible que un determinado activo no le pertenezca, sino que sea propiedad de la matriz. O que la matriz deje ese activo a la filial mediante un leasing, con lo que sólo poseerá un porcentaje del activo; ii) Factores asociativos: Por ejemplo, un producto del cual la compañía se encargue de desarrollar el Software, siendo incorporado el Hardware por otra compañía asociada. En este caso, el valor del producto tasable para la compañía será sólo el correspondiente a la parte Software del mismo.
- *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. En este sistema será básica la Base de Conocimiento que se va alimentando de cada nueva implantación, de forma que se pueda calcular automáticamente la probabilidad de ocurrencia de una amenaza en función de la calculada previamente para otra compañía con similares características. Por ejemplo, en función del ámbito geográfico. Los valores calculados también se verán afectados por la aplicación de factores jerárquicos y asociativos.

- *Sistema de Medición Objetiva de Vulnerabilidades (SMOV):* Permite valorar mediante métricas objetivas la probabilidad de que una vulnerabilidad pueda ser explotada para una compañía. Este sistema trabaja como parte fundamental una ontología de vulnerabilidades, para cada una de las cuáles se calculará la probabilidad de ocurrencia. Este valor se calculará en función del los niveles de cobertura de los controles implantados en la compañía. De esta forma, el sistema trabajará sobre la base de un listado de controles. Para la primera versión de la metodología se empleará el listado de controles de seguridad de la Norma ISO 27001. Los valores calculados también se verán afectados por la aplicación de factores jerárquicos y asociativos.
- *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 (Confidencialidad, Integridad, Disponibilidad y Legalidad). Para ello se emplearán métricas que tomen como base estos criterios de riesgo. Los valores calculados también se verán afectados por la aplicación de factores jerárquicos y asociativos.

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. Para realizar esto, nos estamos basando en las investigaciones de Feng [26] sobre generalización de la teoría Bayesiana de probabilidad subjetiva, las del modelo híbrido (probabilístico y posibilístico) de Carlsson [57], y métodos de inferencia difusa (fuzzy inference) para desarrollar modelos inteligentes de evaluación de riesgos en línea (intelligent online risk assessment models) propuestos por Abraham [61], entre otras [62, 63, 65, 67, 69, 70, 72-74]. Todas ellas orientadas a disminuir el grado de incertidumbre en la generación del análisis de riesgos.

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. Como comentamos anteriormente, para la valoración económica de los activos nos estamos basando en las investigaciones de Lambrinoudakis [25].

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 una tercer factor: La necesidad de que la metodología sea dinámica, de forma que si hay algún cambio en el sistema (Por ejemplo, añadir un nuevo activo o un control que originalmente no se aplicaba) se puedan recalcular los valores de riesgo y tasación de una forma automática y ágil. Para definir estos aspectos nos estamos basando en las investigaciones de [50, 52, 56, 57, 65].

A continuación mostramos en detalle cada uno de los artefactos que componen la metodología.

1) Sistema de Tasación de Activos (STA)

El esquema general del Sistema de Tasación de Activos se puede ver en la Figura 4. Veremos a continuación en detalle cada una de las tareas en las que hemos dividido este sistema:

- *T1 – Lista de activos de la compañía:* En base a una ontología de activos generada en base al cálculo del valor económico de los distintos activos que pueden conformar un Sistema de Información, se obtiene un listado de los diferentes activos de la compañía para los que se calculará el valor monetario. La ontología reflejará también las propiedades de cada activo que supondrán la base del cálculo.
- *T2 – Rellenar el conjunto de propiedades de los activos:* Contando con un interlocutor de la compañía con conocimiento de su Sistema de Información, se recogerán los valores de las propiedades de cada activo de la compañía. Por ejemplo, para valorar un ordenador será necesario conocer datos concretos como: Nº años, memoria, capacidad de disco, etc.
- *T3 – Calcular el valor total del activo:* Una vez recogidos los valores de las propiedades necesarias para la valoración de cada activo, se aplicarán las métricas que permitan tasarlo de una forma objetiva. Por ahora se están tomando como base de la investigación las propuestas por Lambrinoudakis [25].
- *T4 – Aplicar factores asociativos y jerárquicos:* Sobre los valores calculados en la tarea anterior, y para cada activo, se seleccionarán los factores asociativos y jerárquicos que puedan afectarle, como describimos en el esquema general de la metodología. Estos factores se están definiendo según las investigaciones realizadas por [50, 52, 56, 57, 65].
- *T5 – Calcular el valor del activo en la compañía:* Para cada activo, se aplicarán los factores asociativos y jerárquicos seleccionados en la tarea anterior para obtener su valor económico a efectos de tasación. Se están generando nuevas métricas en base a las investigaciones anteriormente mencionadas.

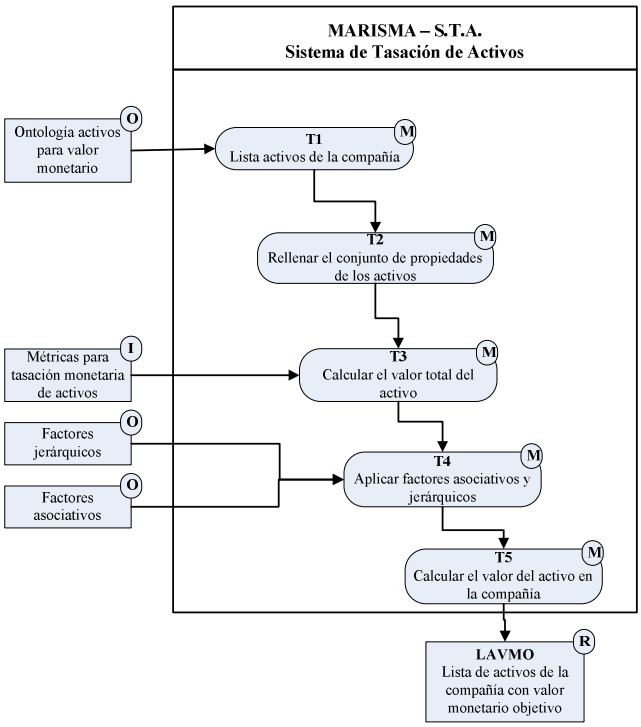


Figura 4. Esquema general del Sistema de Tasación de Activos

2) Sistema de Valoración Objetivo de Amenazas (SVOA)

El esquema general del Sistema de Valoración Objetivo de Amenazas se puede ver en la siguiente ilustración:

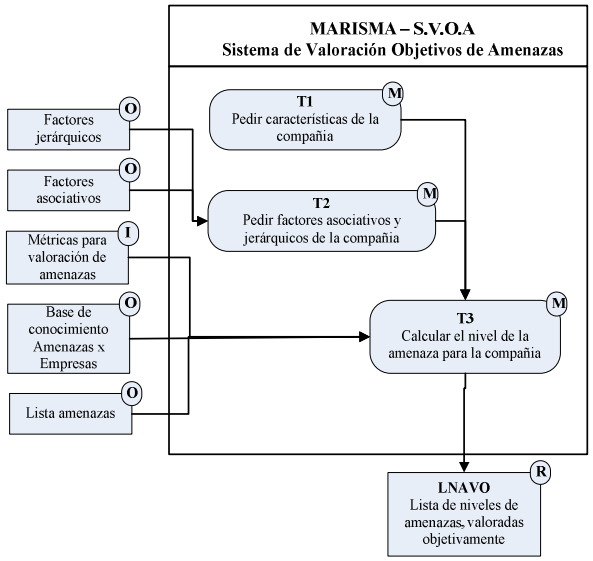


Figura 5. Esquema general del Sistema de Valoración Objetivo de Amenazas

Veremos a continuación en detalle cada una de las tareas en las que hemos dividido este sistema:

- *T1 – Pedir características de la compañía:* Contando con un interlocutor de la compañía, se recogerán las características de la empresa que permitan catalogarla, tales como situación geográfica, sector de actividad, número de empleados, etc. Este conjunto de características se obtendrá a través del método de investigación "Investigación en acción" durante la investigación.
- *T2 – Pedir factores asociativos y jerárquicos:* Para cada activo de la compañía, se seleccionarán los factores asociativos y jerárquicos que puedan afectarle, como describimos en el esquema general de la metodología. Estos factores se están definiendo según las investigaciones realizadas por [50, 52, 56, 57, 65].
- *T3 – Calcular el nivel de amenaza la compañía:* Para cada activo, se aplicarán los factores asociativos y jerárquicos seleccionados en la tarea anterior para obtener el nivel de las amenazas que pueden afectarle. Esta valoración se realizará en base a una serie de métricas que nos permitan cuantificar de forma objetiva el nivel de cada amenaza. En esta tarea será una pieza muy importante la base de conocimiento, ya que se puede reutilizar conocimiento de implantaciones anteriores para automatizar parte del cálculo. Por ejemplo, el nivel de la amenaza "Inundación" será el mismo para los activos de dos empresas del centro de España que esté alejadas de grandes núcleos acuáticos (pantanos, etc.). Esta tarea se está desarrollando en base a las investigaciones realizadas por [29, 68] y a las investigaciones que realizamos anteriormente para SGSIs.

3) Sistema de Valoración de Activos Objetivo (SVAO)

El esquema general del Sistema de Valoración de Activos Objetivo se puede ver en la siguiente ilustración:

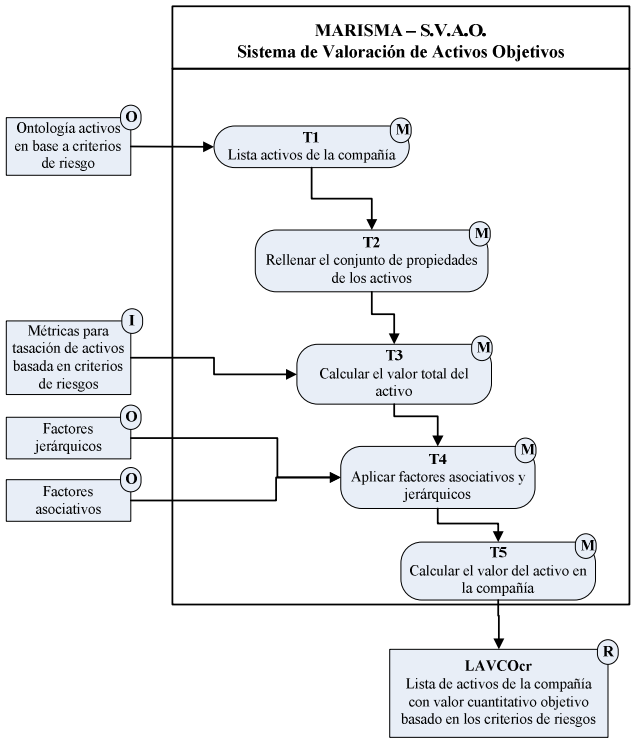


Figura 6. Esquema general del Sistema de Valoración de Activos Objetivo

Veremos a continuación en detalle cada una de las tareas en las que hemos dividido este sistema:

- *T1 – Lista de activos de la compañía:* En base a una ontología generada en base al nivel de incidencia, sobre cada uno de los distintos activos que pueden conformar un Sistema de Información, de los criterios de riesgo que hemos seleccionado en esta fase de la investigación (Confidencialidad, Integridad, Disponibilidad y Legalidad), se obtiene un listado de los diferentes activos de la compañía con el nivel de incidencia de cada uno de estos criterios calculado automáticamente. De esta forma, por ejemplo, el nivel de incidencia del criterio Confidencialidad sobre una licencia de la compañía (activo) se reflejará como "0" en la ontología.
- T2 – Rellenar el conjunto de propiedades de los activos: Contando con un interlocutor de la compañía con conocimiento de su Sistema de Información, se recogerán los valores de incidencia de los criterios de riesgo que no se hayan precalculado en la tarea anterior, para cada activo de la compañía.
- T3 – Calcular el valor total del activo: Una vez recogidos los valores de los criterios de riesgo necesarios para la valoración de cada activo, se aplicarán las métricas que permitan tasarlo de una forma objetiva. Para reducir la incertidumbre, nos estamos basando en diversas investigaciones [26, 57, 61-63, 65, 67, 69, 70, 72-74].
- T4 – Aplicar factores asociativos y jerárquicos: Sobre los valores calculados en la tarea anterior, y para cada activo, se seleccionarán los factores asociativos y jerárquicos que puedan afectarle, como describimos en el esquema general de la metodología. Estos factores se están definiendo según las investigaciones realizadas por [50, 52, 56, 57, 65].
- T5 – Calcular el valor del activo en la compañía: Para cada activo, se aplicarán los factores asociativos y jerárquicos seleccionados en la tarea anterior para obtener su valor cuantitativo basado en criterios de riesgo.

4) Sistema de Medición Objetiva de Vulnerabilidades (SMOV)

El esquema general del Sistema de Valoración de Activos Objetivo se puede ver en la siguiente Figura 7.

Veremos a continuación en detalle cada una de las tareas en las que hemos dividido este sistema:

- *T1 – Calcular el nivel de cobertura de los controles:* Permite calcular utilizando un conjunto de métricas objetivas el nivel de cobertura de los controles de seguridad implantados en el Sistema de Información de la compañía. De esta forma, la tarea trabajará sobre la base de un listado de controles. Para la primera versión de la metodología se empleará el listado de controles de seguridad de la Norma ISO 27001. Para reducir la incertidumbre, nos estamos basando en diversas investigaciones [26, 57, 61-63, 65, 67, 69, 70, 72-74].
- *T2 – Lista de vulnerabilidades:* En base a una ontología de vulnerabilidades, se selecciona un conjunto de aquellas vulnerabilidades que son susceptibles de afectar a los activos del Sistema de Información de la compañía.
- *T3 – Probabilidad de ocurrencia de la vulnerabilidad:* Una vez seleccionadas las vulnerabilidades, se aplicarán las métricas que permitan calcular la probabilidad de ocurrencia de cada vulnerabilidad de una forma objetiva. Para reducir la incertidumbre, nos estamos basando en diversas investigaciones [26, 57, 61-63, 65, 67, 69, 70, 72-74].
- *T4 – Aplicar factores asociativos y jerárquicos:* Sobre los valores calculados en la tarea anterior, y para cada activo, se seleccionarán los factores asociativos y jerárquicos que puedan afectarle, como describimos en el esquema general de la metodología. Estos factores se están definiendo según las investigaciones realizadas por [50, 52, 56, 57, 65].
- *T5 – Calcular el valor del activo en la compañía:* Para cada vulnerabilidad, se aplicarán los factores asociativos y jerárquicos seleccionados en la tarea anterior para obtener un valor objetivo cuantificando su probabilidad de ocurrencia.

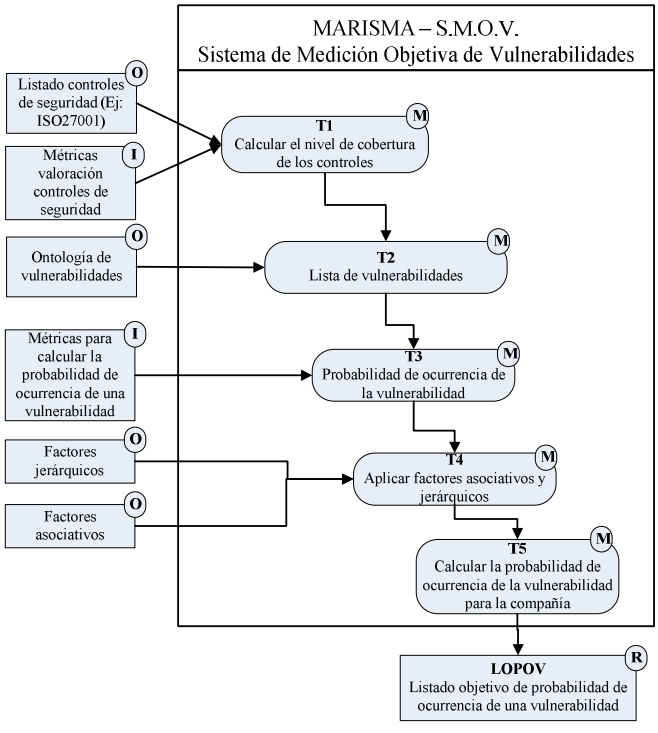


Figura 7. Esquema general del Sistema de Valoración de Activos Objetivo

IV. CONCLUSIONES Y TRABAJOS FUTUROS

En este trabajo se ha propuesto MARISMA, 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.

Durante la investigación, se han estudiado las principales metodologías existentes en el mercado relacionadas con la generación de análisis de riesgos y se ha realizado una revisión sistemática de los diferentes modelos y metodologías para el análisis y gestión de riesgos, con el objetivo de estudiar las propuestas centradas en riesgos asociativos y jerárquicos orientadas a PYMES.

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, ya que constituye un requisito básico para alcanzar la misión y los objetivos organizacionales en un entorno altamente competitivo.

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.

Se ha podido validar durante la investigación la problemática de aplicar las metodologías existentes en el caso de las PYMES, ya que estas han sido concebidas para grandes empresas, siendo la aplicación de este tipo de metodologías y modelos difícil y costosa para las PYMES [75-79].

El problema principal de todos los modelos de análisis y gestión riesgos existentes es que no están teniendo éxito a la hora de implantarse en PYMES, debido principalmente a que:

- Unos fueron desarrollados pensando en organizaciones grandes (Grandes estándares como CRAMM [49], ISO/IEC 27005 [36], MAGERIT [32], OCTAVE [47], NIST SP 800-39 [80], MEHARI [48] o COBIT [81]) y en las estructuras organizativas asociadas a éstas.
- Otros [50, 51, 56] han intentando simplificar el modelo para que pudiera ser apto para compañías con recursos limitados, pero son modelos incompletos que sólo afrontan parte del problema, o intentan aportar unas guías básicas de los pasos a realizar, pero sin entrar en cómo evaluar y gestionar realmente los riesgos de una forma en la que el propio personal técnico de la empresa se pueda involucrar. Además, la mayoría son modelos teóricos y están todavía en desarrollo.
- La mayoría de las propuestas no tienen en cuenta la necesidad de contemplar riesgos jerárquicos y asociativos, factores cruciales en la estructura y funcionamiento actual de las empresas (en el que cada vez tiene más peso el uso de sistemas en Cloud), sobre todo de las PYMES.
- No existen formas objetivas de realizar un análisis de riesgo, dejando gran parte de la responsabilidad a los consultores, de forma que los resultados no tienen validez para terceros.
- La valoración económica de los activos de información es subjetiva, al no existir formas objetivas de valorarlo.

De esta forma, creemos que la investigación propuesta es el inicio de una propuesta detallada y ambiciosa, ya que solucionará gran parte de la problemática existente con las metodologías actuales y tendrá una clara aplicación práctica.

Las ventajas de la investigación propuesta son claras; la posibilidad de poder tener mecanismos de tasación de sistemas de información y de análisis de riesgos que sean objetivos, con coste reducidos y que tengan en cuenta las interrelaciones de los activos supone un cambio radical en la forma de ver los análisis de riesgo, ya que estos se convierten en herramientas útiles para los terceros (ej: las aseguradoras) y posibilita que las compañías tengan mecanismos objetivos de comparación de los riesgos cuando contratan un proyecto a otra compañías.

Todos los estándares y propuestas para la evaluación y gestión de riesgos estudiados en este trabajo son muy importantes, y sus aportaciones serán tenidas en cuenta para el desarrollo de una metodología que incluya todas las características deseadas.

AGRADECIMIENTOS

Esta investigación es parte del proyecto PROMETEO financiado por la Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT) del Gobierno de Ecuador, y los proyectos MEDUSAS (IDI-20090557) y ORIGIN (IDI-2010043) financiado por el CDTI y el FEDER, BUSINESS (PET2008-0136) concedido por el Ministerio Español de Ciencia y Tecnología y MARISMA (HITO-2010-28), SISTEMAS (PII2I09-0150-3135) y SERENIDAD (PII11-0327-7035) financiado por la Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-la Mancha.

Referencias

[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] Dhillon, G. and J. Backhouse, *Information System Security Management in the New Millennium.* Communications of the ACM, 2000. **43**(7): p. 125-128.

[4] Brinkley, D. and R. Schell, *What Is There to Worry About? An Introduction to the Computer Security Problem*, in *Information Security, An Integrated Collection of Essays*, M. Abrams, S. Jajodia, and H. Podell, Editors. 1995, IEEE Computer Society: California.

[5] Chung, L., et al., *Non-functional requirements in software engineering*2000, Boston/Dordrecht/London: Kluwer Academic Publishers.

[6] Dhillon, G., *Information Security Management: Global challenges in the new millennium*2001: Idea Group Publishing.

[7] Ghosh, A., C. Howell, and J. Whittaker, *Building Software Securely from the Ground Up.* IEEE Software, 2002. **19**(1): p. 14-16.

[8] Hall, A. and R. Chapman, *Correctness by Construction: Developing a Commercial Secure System.* IEEE Software, 2002. **19**(1): p. 18-25.

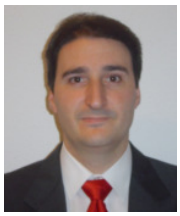
[9] Jürjens, J. *Towards Development of Secure Systems using UML*. in *International Conference on the Fundamental Approaches to Software Engineering (FASEiTAPS)*. 2001. Springer.
[10] Masacci, F., M. Prest, and N. Zannone, *Using a security requirements engineering methodology in practice: The compilanse with the Italian data protection legislation.* Computer Standards & Interfaces, 2005. **27**: p. 445-455.
[11] Walker, E., *Software Development Security: A Risk Management Perspective.* The DoD Software Tech. Secure Software Engineering, 2005. **8**(2): p. 15-18.
[12] Wiander, T. and J. Holappa, *Theoretical Framework of ISO 17799 Compliant. Information Security Management System Using Novel ASD Method.*, in *Technical Report*, V.T.R.C.o. Finland, Editor 2006.
[13] Volonino, L. and S. Robinson. *Principles and Practice of Information Security*. in *1 edition, Anderson, Natalie E.* 2004. New Jersey, EEUU.
[14] Michalson, L., *Information security and the law: threats and how to manage them.* Convergence, 2003. **4**(3): p. 34-38.
[15] Spinellis, D. and D. Gritzalis. *Information Security Best Practise Dissemination: The ISA-EUNET Approach*. in *WISE 1:First World Conference on Information Security Education*. 1999.
[16] Dimopoulos, V., et al. *Approaches to IT Security in Small and Medium Enterprises*. in *2nd Australian Information Security Management Conference, Securing the Future*. 2004. Perth, Western Australia: 73-82.
[17] 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.
[18] 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.
[19] Shaw, M., *What makes good research in software engineering?* International Journal on Software Tools for Technology Transfer (STTT), 2002. **4**(1): p. 1-7.
[20] Dimopoulos, V., et al. *Factors affecting the adoption of IT risk analysis*. in *Proceedings of 3rd European Conference on Information Warfare and Security*. 2004. Royal Holloway, University of London: 28-29 June 2004.
[21] Zissis, D. and D. Lekkas, *Addressing cloud computing security issues.* Future Generation Computer Systems, 2012. **28**(3): p. 583-592.
[22] Siegel, C.A., T.R. Sagalow, and P. Serritella, *Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security.* Security Management Practices, 2002. **sept/oct**: p. 33-49.
[23] Garigue, R. and M. Stefaniu, *Information Security Governance Reporting.* Information Systems Security, 2003. **sept/oct**: p. 36-40.
[24] Mercuri, R.T., *Analyzing security costs.* Communication of the ACM, 2003. **46**: p. 15-18.
[25] Lambrinoudakis, C., et al., *A formal model for pricing information systems insurance contracts.* Computer Standards & Interfaces, 2005. **27**(5): p. 521-532.
[26] Feng, N. and M. Li, *An information systems security risk assessment model under uncertain environment.* Applied Soft Computing, 2011. **11**(7): p. 4332-4340.
[27] Lund, M.S., F.d. Braber, and K. Stolen, *Proceedings of the Seventh European Conference On Software Maintenance And Reengineering (CSMR'03).* IEEE, 2003.
[28] Fredriksen, R., et al. *The CORAS framework for a model-based risk management process*. in *21st International Conference on Computer Safety, Reliability and Security (Safecomp 2002)*. 2002. Springer: LNCS 2434.
[29] Alhawari, S., et al., *Knowledge-Based Risk Management framework for Information Technology project.* International Journal of Information Management, 2012. **32**(1): p. 50-65.
[30] Barrientos, A.M. and K.A. Areiza, *Integration of a safety management system withan information quality management system.*, in *Master's thesis*2005, Universidad EAFIT.
[31] Spinellis, D. and D. Gritzalis. *nformation Security Best Practise Dissemination: The ISA-EUNET Approach*. in *WISE 1:First World Conference on Information Security Education*. 1999.
[32] MageritV2, *Methodology for Information Systems Risk Analysis and Management (MAGERIT version 2)*, 2006, Ministerio de Administraciones Públicas (Spain).
[33] Vidalis, S., *A critical discussion of risk and threat analysis methods and methodologies*, 2003.
[34] ISO/IEC13335, *ISO/IEC 13335, Information Technology - Security Techniques - Management of Information and Communications Technology Security*, 2004.
[35] ISO/IEC13335-4, *ISO/IEC TR 13335-4, Information technology -- Guidelines for the management of IT Security -- Part 4: Selection of safeguards.*, 2000.
[36] ISO/IEC27005, *ISO/IEC 27005. Information Technology - Security Techniques - Information Security Risk Management Standard*, 2008.
[37] ISO/IEC27002, *ISO/IEC 27002:2005, the international standard Code of Practice for Information Security Management (en desarrollo).* 2007.
[38] ISO/IEC13335-3, *ISO/IEC TR 13335-3, Information technology -- Guidelines for the management of IT Security -- Part 3: Techniques for the management of IT Security.*, 1998.
[39] BS7799, *BS 7799: Information security management systems.* , 2006, British Standards Institute (BSI).
[40] ISO/IEC27001, *ISO/IEC 27001, Information Technology - Security Techniques Information security management systemys - Requirements.*, 2005.
[41] ISO/IEC27002, *ISO/IEC 27002, Information Technology - Security Techniques - The international standard Code of Practice for Information Security Management.*, 2007.
[42] ISO/IEC27005, *ISO/IEC 27005, Information Technology - Security Techniques - Information Security Risk Management Standard (under development).* 2008.
[43] Stoneburner, G., A. Goguen, and A. Feringa. *Risk Management Guide for Information Technology Systems, NIST SP 800-30*. 2009.
[44] 4360:2004, A.N., *Standars Australia and Standards New Zealand*. Risk Management2004, Sydney, NSW.
[45] Konus, J. and D. Minoli, *Information Technology Risk Management in Enterprise Environments.*, N.J.W. Hoboken, Editor 2010.
[46] OCTAVE. *CERT – Software Engineering Institute, Carnegie Mellon*. 2009; Available from: http://www.cert.org/octave/.
[47] Alberts, C.J. and A.J. Dorofee, *OCTAVE Criteria, Version 2.0*, 2001.
[48] MEHARI. *Club de la Sécurité de l'Information Français*. 2009; Available from: https://www.clusif.asso.fr/.
[49] CRAMM. *Siemens Enterprise Communications Ltd. "CRAMM toolkit"*. 2009; Available from: http://www.cramm.com/.
[50] Nachtigal, S., *E-business Information Systems Security Design Paradigm and Model.* Royal Holloway, University of London, Technical Report, 2009: p. 347.
[51] Abdullah, H., *A Risk Analysis and Risk Management Methodology for Mitigating Wireless Local Area Networks Intrusion Security Risks.* University of Pretoria, 2006: p. 219.
[52] Arikan, A.E., *Development of a risk management decision support system for international construction projects.* Middle East Technical University, 2005: p. 118.
[53] Bagheri, E. and A.A. Ghorbani, *Astrolabe: A Collaborative Multiperspective Goal-Oriented Risk Analysis Methodology.* IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART A: SYSTEMS AND HUMANS, 2009. **39**(1): p. 66-85.
[54] Committee, I.R.M., *Report of the Study Group on Risk Assessment and Management Advice (SGRAMA).* 2006.
[55] Strecker, S., D. Heise, and U. Frank, *RiskM: A multi-perspective modeling method for IT risk assessment.* Inf Syst Front, 2010(13): p. 595–611.
[56] Ma, W.-M., *Study on Architecture-Oriented Information Security Risk Assessment Model.* ICCCI 2010, Part III, LNAI 6423, 2010: p. 18–226.
[57] Carlsson, C. and R. Fullér, *Predictive Probabilistic and Possibilistic Models Used for Risk Assessment of SLAs in Grid Computing.* IPMU 2010, Part II, CCIS 81, 2010: p. 747–757.
[58] Hussain, O., H. Dong, and J. Singh, *Semantic Similarity Model for Risk Assessment in Forming Cloud Computing SLAs.* OTM 2010, Part II, LNCS 6427, 2010: p. 843–860.
[59] Hussain, O., et al., *A Methodology for Transactional Risk Assessment and Decision Making in e-Business Interactions.* 2009 IEEE International Conference on e-Business Engineering, 2009: p. 157-164.
[60] Tjoa, S., S. Jakoubi, and G. Quirchmayr, *Enhancing Business Impact Analysis and Risk Assessment applying a Risk-Aware Business Process Modeling and Simulation Methodology.* IEEE Computer Society DOI 10.1109, 2008: p. 179-186.
[61] Abraham, A., *Nature Inspired Online Real Risk Assessment Models for Security Systems.* EuroISI 2008, LNCS 5376, 2008.
[62] Chang, S.-I., et al., *The development of audit detection risk assessment system: Using the fuzzy theory and audit risk model.* Expert Systems with Applications, 2008. **35**(3): p. 1053-1067.
[63] Wang, P., et al., *A Fuzzy Decision Model of Risk Assessment Through Fuzzy Preference Relations with Users'Confidence-interval.* IEEE Computer Society AINA'06, 2006.

[64] Yang, F.-H., C.-H. Chi, and L. Liu, *A Risk Assessment Model for Enterprise Network Security.* ATC 2006, LNCS 4158, 2006: p. 293 – 301.
[65] Kumar, V., M. Schuhmacher, and M. García, *Integrated Fuzzy Approach for System Modeling and Risk Assessment.* MDAI 2006, LNAI 3885, 2006: p. 227 – 238.
[66] Wawrzyniak, D., *Information Security Risk Assessment Model for Risk Management.* TrustBus 2006, LNCS 4083, 2006: p. 21–30.
[67] Lin, M., Q. Wang, and J. Li, *Methodology of Quantitative Risk Assessment for Information System Security.* CIS 2005, Part II, LNAI 3802, 2005: p. 526 – 531.
[68] Hewett, R. and R. Seker, *A Risk Assessment Model of Embedded Software Systems.* 29th Annual IEEE/NASA Software Engineering Workshop (SEW'05), 2005: p. 8.
[69] Lo, C.-C. and W.-J. Chen, *A hybrid information security risk assessment procedure considering interdependences between controls.* Expert Systems with Applications, 2012. **39**(1): p. 247-257.
[70] Patel, S.C., J.H. Graham, and P.A.S. Ralston, *Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements.* International Journal of Information Management, 2008. **28**(6): p. 483-491.
[71] Ou Yang, Y.-P., H.-M. Shieh, and G.-H. Tzeng, *A VIKOR technique based on DEMATEL and ANP for information security risk control assessment.* Information Sciences, (0).
[72] Salmeron, J.L. and C. Lopez, *A multicriteria approach for risks assessment in ERP maintenance.* Journal of Systems and Software, 2010. **83**(10): p. 1941-1953.
[73] Deng, Y., et al., *Risk analysis in a linguistic environment: A fuzzy evidential reasoning-based approach.* Expert Systems with Applications, 2011. **38**(12): p. 15438-15446.
[74] Ngai, E.W.T. and F.K.T. Wat, *Fuzzy decision support system for risk analysis in e-commerce development.* Decision Support Systems, 2005. **40**(2): p. 235-255.
[75] Batista, J. and A. Figueiredo, *SPI in very small team: a case with CMM.* Software Process Improvement and Practice, 2000. **5**(4): p. 243-250.
[76] Hareton, L. and Y. Terence, *A Process Framework for Small Projects.* Software Process Improvement and Practice, 2001. **6**: p. 67-83.
[77] Calvo-Manzano, J.A., et al., *Experiences in the Application of Software Process Improvement in SMES.* Software Quality Journal., 2004. **10**(3): p. 261-273.
[78] Tuffley, A., B. Grove, and M. G., *SPICE For Small Organisations.* Software Process Improvement and Practice, 2004. **9**: p. 23-31.
[79] Mekelburg, D., *Sustaining Best Practices: How Real-World Software Organizations Improve Quality Processes.* Software Quality Professional, 2005. **7**(3): p. 4-13.
[80] NIST, *Security Metrics Guide for Information Technology Systems*, 2004.
[81] COBITv4.0, *Cobit Guidelines, Information Security Audit and Control Association*, 2006.

Luis Enrique Sánchez is PhD and MsC in Computer Science and is an Professor at the Escuela Politécnica del Ejército (ESPE) of Latacunga (Ecuador), MSc in Information Systems Audit from the Polytechnic University of Madrid, and Certified Information System Auditor by ISACA. He is the Director of Professional Services and R&D departments of the company Sicaman Nuevas Tecnologías S.L. COIICLM board or committee member and responsible for the professional services committee. His research activities are management security system, security metrics, data mining, data cleaning, and business intelligence. He participates in the GSyA research group of the Department of Computer Science at the University of Castilla- LaMancha, in Ciudad Real (Spain). He belongs to various professional and research associations (COIICLM, ATI, ASIA, ISACA, eSEC, INTECO, etc).

Antonio Santos-Olmo is MsC in in Computer Science and is an Assistant Professor at the Escuela Superior de Informática of the Universidad de Castilla- La Mancha in Ciudad Real (Spain) (Computer Science Department, University of Castilla La Mancha, Ciudad Real, Spain), MSc in Information Systems Audit from the Polytechnic University of Madrid, and Certified Information System Auditor by ISACA. He is the Director of Software Factory departments of the company Sicaman Nuevas Tecnologías S.L. His research activities are management security system, security metrics, data mining, data cleaning, and business intelligence. He participates in the GSyA research group of the Department of Computer Science at the University of Castilla- LaMancha, in Ciudad Real (Spain). He belongs to various professional and research associations (COIICLM, ATI, ASIA, ISACA, eSEC, INTECO, etc).

Esther Álvarez President of Private Foundation Innova and Research of the UPM. Consultant in strategic communications programs radio, mobile and wireless both public and private sectors and in civil and military. Currently a member of the board of the Delegation of COIT (Association of Telecommunications Engineers) CLM, representative of Castilla La Mancha in the groups of the free and COIT New Technologies of the National Coordinator of the Treatment Research Chair in Digital Image at the Madrid Polytechnic University of Madrid. PhD in Information Systems specializing in Business ETSI Industriales (UPM) and the Specialty Program Communications Signals, Systems and Radiocommunications Department SSR ETSI Telecomunicaciones (UPM). It Telecommunications Engineering from UPM. Specialty Communications..



Eduardo Fernández-Medina holds a PhD. and an MSc. in Computer Science from the University of Sevilla. He is Professor at the Escuela Superior de Informática of the University of Castilla-La Mancha in Ciudad Real (Spain) (Computer Science Department, University of Castilla La Mancha, Ciudad Real, Spain)- his research activity being in the field of security in information systems, and particularly in security in business processes, databases, datawarehouses, and web services. Fernández-Medina is co-editor of several books and chapter books on these subjects, and has published several dozens of papers in national and international conferences (BPM, UML, ER, ESORICS, TRUSTBUS, etc.). He is author of several manuscripts in national and international journals (Decision Support Systems, Information Systems, ACM Sigmod Record, Information Software Technology, Computers & Security, Computer Standards and Interfaces, etc.). He leads the GSyA research group of the Department of Computer Science at the University of Castilla-La Mancha, in Ciudad Real, Spain and belongs to various professional and research associations (ATI, AEC, AENOR, etc.).

Mario Piattini is MSc and PhD in Computer Science from the Technical University of Madrid and is a Certified Information System Auditor (CISA) and Certified Information Security Manager by ISACA (Information System Audit and Control Association). He is a professor in the Department of Computer Science at the University of Castilla-La Mancha, in Ciudad Real, Spain. Author of several books and papers on databases, software engineering and information systems, he leads the ALARCOS research group of the Department of Computer Science at the University of Castilla-La Mancha, in Ciudad Real, Spain. He is author of several books and papers on databases, security, software engineering and information systems. He leads the ALARCOS research group of the Department of Computer Science at the University of Castilla- La Mancha, in Ciudad Real (Spain). His research interests are: advanced database design, database quality, software metrics, object-oriented metrics and software maintenance.