Revisión Sistemática de Metodologías y Modelos para el Análisis y Gestión de Riesgos Asociativos y Jerárquicos para PYMES

Antonio Santos-Olmo, Luís Enrique Sánchez
Departamento de I+D+i
SICAMAN Nuevas Tecnologías
Ave María, 5. Tomelloso, Ciudad Real, Spain
{Lesanchez, Asolmo}@sicaman-nt.com

Eduardo Fernández-Medina, Mario Piattini
ALARCOS Research Group. TSI Department
Universidad de Castilla-La Mancha (UCLM)
Paseo de la Universidad, 4 – 13071 Ciudad Real, Spain
{Eduardo.FdezMedina, Mario.Piattini}@uclm.es

***Resumen*— La sociedad de la información cada vez depende más de los Sistemas de Gestión y Análisis del Riesgo al que se encuentran sometidos sus principales activos de información, y poder disponer de estos sistemas ha llegado a ser vital para la evolución de las PYMES. Sin embargo, este tipo de compañías requiere que estos sistemas estén adaptados a sus especiales características, y teniendo en cuenta la existencia de riesgos derivados no sólo de la propia PYME, sino riesgos externos de otras empresas que colaboran con ella. De esta forma, obtendremos un análisis de riesgos de mayor calidad reduciendo el coste empleando conceptos avanzados como "Algoritmos asociativos" y "Redes sociales empresariales". En este artículo, presentamos los resultados obtenidos tras realizar una revisión sistemática de metodologías y modelos para el análisis de riesgos para PYMES, y que tengan en cuenta riesgos jerárquicos y asociativos.**

PYMES; Analisis de riesgos; Risgos jerárquicos y asociativos

I. INTRODUCCIÓN

Para las empresas, es muy importante implantar controles de seguridad que les permitan conocer y controlar los riesgos a los que pueden estar sometidas [1, 2]. Pero la implantación de estos controles no es suficiente, siendo necesarios sistemas que gestionen la seguridad a lo largo del tiempo, de modo que les permitan reaccionar ágilmente ante nuevos riesgos, vulnerabilidades, amenazas, etc. [3]. Sin embargo, la mayor parte de las empresas tienen sistemas de seguridad caóticos creados sin unas guías adecuadas, sin documentación y con recursos insuficientes [4]. Los controles clásicos se muestran por sí solos insuficientes para dar unas mínimas garantías de seguridad. Las herramientas de seguridad existentes en el mercado ayudan a solucionar parte de los problemas de seguridad, pero nunca afrontan el problema de una manera global e integrada. Por lo tanto, a pesar de que la realidad ha demostrado que para que las empresas puedan utilizar las tecnologías de la información y las comunicaciones con garantías es necesario disponer de guías, métricas y herramientas que les permitan conocer en cada momento su nivel de seguridad y las vulnerabilidades que aún no han sido cubiertas [5], el nivel de implantación con éxito de estos sistemas realmente es muy bajo. Este problema 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 [4].

Algunos autores [6, 7] sugieren la realización de un análisis de riesgos como parte fundamental en la PYME. Otros autores [8] proponen la necesidad de desarrollar un nuevo modelo de análisis de riesgos 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.

Como tal, toma especial relevancia la necesidad de obtener nuevas metodologías y modelos de análisis y gestión del riesgo, que permitan adaptarse a las PYMES, con el objetivo de eliminar (o al menos reducir) los inconvenientes y ayudar a estas sociedades a evaluar los riesgos a los que sus activos están expuestos y a establecer los controles de seguridad adecuados.

Además, 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 partners tecnológicos, bien como terceras partes en algún servicio que realice la empresa o bien como co-participantes en proyectos multi-empresa.

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.

De esta manera, el objetivo principal de este artículo es realizar una revisión sistemática de los modelos y metodologías existentes o en desarrollo para el análisis y gestión de riesgos, contemplando riesgos de carácter asociativo y jerárquico, y con orientación a PYMES.

El artículo continúa en la Sección 2, describiendo brevemente la planificación de la revisión sistemática. En la Sección 3 se presentan brevemente las propuestas más relevantes seleccionadas. En la Sección 4 se analizan las propuestas seleccionadas. Finalmente, en la Sección 5 concluimos indicando cuál será el trabajo que desarrollaremos en el futuro.

II. PLANIFICACIÓN DE LA REVISIÓN

En primer lugar, en esta etapa identificamos la necesidad de la revisión indicando cuáles son sus objetivos, qué fuentes

se utilizarán para identificar los estudios primarios, si hubo algunas restricciones, cuáles son los criterios de inclusión y exclusión, qué criterios se utilizarán para evaluar la calidad de los estudios primarios y cómo se extraerán y sintetizarán los datos de los estudios.

- **Formulación de la pregunta**: Se define la pregunta de investigación de forma que se focalice el área de interés del trabajo y queden definidos tanto el problema a tratar como sus principales características. 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?

  En el contexto de la revisión sistemática planificada se van a observar las propuestas existentes sobre modelos y metodologías de análisis de riesgos, haciendo especial hincapié en aquéllas orientadas a trabajo con riesgos asociativos, riesgos jerárquicos y/u orientadas a PYMES, extrayendo las más importantes y procediendo a un posterior análisis y comparación de las mismas.
- **Selección de fuentes:** El objetivo de esta fase es seleccionar las fuentes que se usarán para realizar la ejecución de la búsqueda de estudios primarios. El criterio para la selección de las fuentes de búsqueda será la posibilidad de consultar los documentos en Internet o en la biblioteca digital de la Universidad de Castilla-La Mancha, que contengan estudios en inglés, así como la inclusión motores de búsqueda que permitan consultas avanzadas y búsqueda por palabras clave. La lista de fuentes obtenida sobre la cual se ejecutará la revisión sistemática es la siguiente: Science Direct, ACM digital library, IEEE digital library, SCOPUS, Scholar Google y DBLP.
- **Selección de estudios:** Una vez que se han sido definidas las fuentes, es necesario describir el proceso y el criterio que vamos a seguir en la ejecución de la revisión para la selección y evaluación de los estudios. En primer lugar, se combinaron las palabras clave seleccionadas con conectores AND y OR para obtener la cadena de búsqueda, como se muestra a continuación:

  methodology OR model
  AND
  associative OR hierarchical
  AND
  “risk analysis” OR “risk management” OR “risk assessment"
  AND
  SMB OR SME OR PYME

  El procedimiento para la selección de estudios empleado comienza con la adaptación de la cadena de búsqueda al motor de búsqueda de la fuente y la ejecución de la consulta, limitando la búsqueda a trabajos publicados en los últimos 7 años. El criterio de inclusión actúa sobre los resultados obtenidos al ejecutar la búsqueda sobre la fuente, permitiéndonos realizar una primera selección de documentos que serán considerados en el contexto de la revisión como candidatos a convertirse en estudios primarios. El criterio de exclusión actúa sobre el subconjunto de estudios relevantes obtenidos y nos permite obtener el conjunto de estudios primarios. En esta fase seleccionamos como estudios primarios, por ejemplo, aquéllos centrados en la aplicación de algún estándar como ISO 27001 al ámbito del análisis de riesgos en PYMES o trabajos que definen metodologías ágiles de gestión del riesgo o tienen en cuentas riesgos asociativos o ambientales.

III. EJECUCIÓN DE LA SELECCIÓN Y EXTRACCIÓN DE INFORMACIÓN

En este punto, se ejecuta la revisión sistemática en cada una de las fuentes seleccionadas aplicando todos los criterios y procedimientos especificados. La información extraída de los estudios debe contener las técnicas, métodos, procesos, medidas, estrategias o cualquier tipo de iniciativa para la adaptación del análisis, gestión o evaluación de riesgos a un alcance abordable por las PYMES, o manejar riesgos asociativos o jerárquicos. A continuación se ofrece una breve reseña de cada uno de los estudios seleccionados mostrados en la sección anterior, de acuerdo con la información extraída obtenida a través de los formularios de información creados:

1. *Nachtigal, S. “E-business Information Systems Security Design Paradigm and Model” [9].*

El autor propone un modelo de seguridad de Sistemas de Información centrado en organizaciones basadas en el comercio electrónico. De esta forma, 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. También desarrolla una Metodología de Seguridad en Procesos de e-Business (e-BPSM), destacando la dificultad de definir un modelo propio de Gestión del Riesgo dada la problemática de que dicho riesgo dependa de factores no controlados por la organización, como partners tecnológicos o usuarios no controlados. Así, se reconoce la importancia de una gestión de riesgos asociativos y jerárquicos.

2. *Abdullah, H. “A Risk Analysis and Risk Management Methodology for Mitigating Wireless Local Area Networks (WLANs) Intrusion Security Risks” [10].*

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, aunque sólo tomándola como

base debido a la gran cantidad de tiempo necesario para aplicar dicha metodología, lo que hace que su implantación en PYMES sea inviable debido a la cantidad de tiempo y recursos (humanos y económicos) necesarios para su aplicación.

Se trata de un estudio teórico, sin contrastar resultados con aplicación de la metodología en casos prácticos.

3. *Bagheri, E. et al. "Astrolabe: A Collaborative Multiperspective Goal-Oriented Risk Analysis Methodology" [11].*

Los autores presentan una metodología de análisis de riesgos llamada Astrolabe, basada en el análisis causal de los riesgos de los Sistemas de Información. Su objetivo es permitir a los analistas, por un lado, alinear el estado actual del sistema con sus objetivos y, por otro, identificar las vulnerabilidades o riesgos que amenazan la estabilidad del sistema, guiando el análisis de riesgos a través de sus fases, para que se lleve a cabo una investigación casi completa de los riesgos del sistema..

Se trata de un estudio teórico, sin contrastar resultados con aplicación de la metodología en casos prácticos.

4. *Alhawari, S. et al. "Knowledge-Based Risk Management framework for Information Technology project" [12].*

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.

5. *Strecker, S et al. "RiskM: A multi-perspective modeling method for IT risk assessment" [13].*

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. Para ello, parten de la involucración y participación de los interesados como factores clave de éxito para la evaluación de riesgos de TI.

Se trata de un estudio teórico, sin contrastar resultados con aplicación de la metodología en casos prácticos.

6. *Ma, Wei-Ming. "Study on Architecture-Oriented Information Security Risk Assessment Model" [14].*

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.

7. *Feng, Nan et al. "An information systems security risk assessment model under uncertain environment" [15].*

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). De esta forma, toman como base que, dado que existe una gran incertidumbre en el proceso de evaluación de riesgos en Sistemas de Seguridad de la Información (ISS), el manejo de la incertidumbre es de gran importancia para la eficacia de la evaluación de riesgos.

El modelo está contrastado con un caso práctico de estudio, pero es muy genérico y no está soportado por ninguna herramienta software.

8. *Abraham, A. "Nature Inspired Online Real Risk Assessment Models for Security Systems" [16].*

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.

La definición y aplicación de estos modelos se centran en la evaluación de riesgos en la detección de intrusos en entornos móviles, aunque puede ser interesante evaluar la posibilidad de su aplicación a ámbitos más generales de los Sistemas de Información, así como su aplicación al Cloud Computing.

9. *Chang, She-I et al. "The development of audit detection risk assessment system: Using the fuzzy theory and audit risk model" [17].*

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" [18], 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

10. *Yang, Fu-Hong et al. "A Risk Assessment Model for Enterprise Network Security" [19].*

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.

11. *Wawrzyniak, D. "Information Security Risk Assessment Model for Risk Management" [20].*

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.

12. *Lin, Mengquan et al. "Methodology of Quantitative Risk Assessment for Information System Security" [21].*

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.

La base de la metodología es la obtención y asignación de los pesos a los distintos criterios de evaluación. Sin embargo, esta aproximación depende mucho del conocimiento experto para la definición y gestión de los criterios de evaluación.

No se presenta tampoco la metodología completa, sino sólo los métodos de base para obtener los pesos de los criterios de evaluación.

13. *Hewett, R. et al. "A Risk Assessment Model of Embedded Software Systems" [22].*

Los autores proponen una técnica para representar y evaluar los riesgos asociados al software integrado en sistemas en determinados sistemas.

La técnica de representación propuesta está basada en diagramas de flujo dinámico. La parte más interesante de este trabajo es la representación gráfica y la integración del entorno y sistemas externos en la evaluación de los riesgos, así como la apuesta por la reutilización del conocimiento en sucesivas aplicaciones del modelado.

No se presenta tampoco la metodología completa, ni se contrastan los resultados con la aplicación en casos prácticos.

14. *Patel, S.C. et al. "Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements" [23].*

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.

15. *Yu-Ping Ou Yang et al. "A VIKOR technique based on DEMATEL and ANP for information security risk control assessment" [24].*

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.

16. *Salmeron, J.L. et al. "A multicriteria approach for risks assessment in ERP maintenance" [25].*

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.

IV. ANÁLISIS DE RESULTADOS

A continuación, en la Tabla 1 se puede ver una comparativa de las diferentes propuestas analizadas, comparadas con la propuesta futura que pretende abordarse. 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.

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
Nachtigal, S.	No	P	No	No	P	No	P	No	No	P
Abdullah, H	No	No	Sí	No	No	No	Sí	No	No	No
Bagheri, E. et al.	Sí	Sí	Sí	No	No	No	No	No	No	No
Alhawari, S. et al.	No	No	No	No	No	No	No	Sí	No	No
Strecker, S et al.	Sí	No	P		No	No	No	No	No	No
Ma, Wei-Ming	Sí	No	No	No	P	P	P	No	No	No
Feng, Nan et al.	Sí	No	Sí	Sí	P	No	No	No	No	Sí
Abraham, A.	No	No	No	No	P	No	No	Sí	No	No
Chang, She-I et al. and Wang, Ping et al.	No	P	P	No	P	No	No	No	No	Sí
Ngai, E.W.T. et al.	No	P	Sí	No	P	No	No	No	Sí	Sí
Yang, Fu-Hong	No	No	No	No	P	No	No	No	No	No
Wawrzyniak, D.	Sí	No	Sí	No	No	No	No	No	No	No
Lin, Mengquan et al.	Sí	P	No	Sí	No	No	No	No	No	No
Hewett, R. et al.	No	No	No	No	P	No	No	Sí	No	No
Patel, S.C. et al.	Sí	P	No	Sí	No	No	No	No	No	No
Yu-Ping Ou Yang et al.	Sí	P	Sí	Sí	No	No	No	No	No	Sí
Salmeron, J.L. et al.	No	No	Sí	No	No	P	No	No	No	No

Tabla 1: Comparativa de las propuestas seleccionadas

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

V. CONCLUSIONES Y TRABAJO FUTURO

En este artículo 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.

En numerosas fuentes bibliográficas se detecta y resalta la dificultad que supone para las PYMES la utilización de las metodologías y modelos de análisis de riesgos tradicionales, que han sido concebidos para grandes empresas, siendo la aplicación de este tipo de metodologías y modelos difícil y costosa para las PYMES [26-30].

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, ISO/IEC 27005, MAGERIT, OCTAVE, NIST SP 800-39, Mehari, COBIT o ERMF) y en las estructuras organizativas asociadas a éstas. Otros (Abdullah, Wei-Ming Ma, Nachtigal) 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.*

De esta forma, se puede concluir que es relevante realizar un nuevo modelo que permita incluir todas las características citadas como deseables de cara a su implantación en PYMES.

Todas las propuestas para la evaluación y gestión de riesgos estudiadas en este artículo son muy importantes, y sus aportaciones serán tenidas en cuenta para el desarrollo de una metodología que incluya todas las características deseadas.

AGRADECIMIENTOS

Agradecimiento especial a todo el equipo informática del hospital Virgen de la Salud de Toledo, que ha participado en el desarrollo de la investigación y ha servido

de centro piloto para la implantación del mismo. Esta investigación es parte de 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] Kluge, D. *Formal Information Security Standards in German Medium Enterprises.* in *CONISAR: The Conference on Information Systems Applied Research.* 2008.

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

[3] Barlette, Y. and V. Vladislav. *Exploring the Suitability of IS Security Management Standards for SMEs*. in *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*. 2008. Waikoloa, HI, USA.

[4] 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.

[5] 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.

[6] Michalson, L., *Information security and the law: threats and how to manage them.* Convergence, 2003. **4**(3): p. 34-38.

[7] Volonino, L. and S. Robinson. *Principles and Practice of Information Security*. in *1 edition, Anderson, Natalie E*. 2004. New Jersey, EEUU.

[8] 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.

[9] Nachtigal, S., *E-business Information Systems Security Design Paradigm and Model.* Royal Holloway, University of London, Technical Report, 2009: p. 347.

[10] Abdullah, H., *A Risk Analysis and Risk Management Methodology for Mitigating Wireless Local Area Networks Intrusion Security Risks.* University of Pretoria, 2006: p. 219.

[11] 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.

[12] Alhawari, S., et al., *Knowledge-Based Risk Management framework for Information Technology project.* International Journal of Information Management, 2012. **32**(1): p. 50-65.

[13] 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.

[14] Ma, W.-M., *Study on Architecture-Oriented Information Security Risk Assessment Model.* ICCCI 2010, Part III, LNAI 6423, 2010: p. 18–226.

[15] Feng, N. and M. Li, *An information systems security risk assessment model under uncertain environment*. Applied Soft Computing, 2011. **11**(7): p. 4332-4340.

[16] Abraham, A., *Nature Inspired Online Real Risk Assessment Models for Security Systems.* EuroISI 2008, LNCS 5376, 2008.

[17] 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.

[18] 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.

[19] 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.

[20] Wawrzyniak, D., *Information Security Risk Assessment Model for Risk Management*. TrustBus 2006, LNCS 4083, 2006: p. 21–30.

[21] 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.

[22] 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.

[23] 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.

[24] 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).

[25] 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.

[26] 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.

[27] Hareton, L. and Y. Terence, *A Process Framework for Small Projects.* Software Process Improvement and Practice, 2001. **6**: p. 67-83.

[28] Tuffley, A., B. Grove, and M. G, *SPICE For Small Organisations.* Software Process Improvement and Practice, 2004. **9**: p. 23-31.

[29] 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.

[30] Mekelburg, D., *Sustaining Best Practices: How Real-World Software Organizations Improve Quality Processes.* Software Quality Professional, 2005. **7**(3): p. 4-13.