Revisión Sistemática de Análisis de Riesgos Asociativos y Jerárquicos. Periodo 2014 – 2019.

A. Santos-Olmo, L. E. Sánchez, E. Álvarez, D.G. Rosado, E. Fernandez-Medina

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, mediante relaciones de asociatividad y jerarquía. De esta forma, obtendremos un análisis de riesgo de mayor calidad (y reduciendo su coste) empleando conceptos avanzados como "Algoritmos asociativos" y "Redes sociales empresariales". En este artículo presentamos los resultados obtenidos tras aplicar el método de investigación "Revisión Sistemática de la Literatura" de las propuestas científicas orientadas a análisis de riesgos TIC Asociativos y Jerárquicos, publicadas en los últimos 5 años.**

Palabras clave **— Cibersecurity, *Information Systems Security Management, ISMS*, Risk Analysis, SME, ISO27001, ISO27002, ISO27005, Magerit.**

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 [1-3]. 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. [4]. Sin embargo, la mayor parte de las empresas tienen sistemas de seguridad caóticos creados sin unas guías adecuadas, sin documentación y con recursos insuficientes [5]. Los controles clásicos se muestran por sí solos insuficientes para dar unas mínimas garantías de seguridad, en especial en sectores como el de la salud [6, 7]. 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 último, la enorme diversidad de estas herramientas y su falta de integración suponen un enorme coste en recursos para poderlas gestionar.

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 [8], el nivel de implantación con éxito de estos sistemas realmente es muy bajo [9]. 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 [5].

Algunos autores [10, 11] 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 debe tener controlado el valor y los riesgos a los que esos activos están sometidos. Otros autores [12] proponen la necesidad de desarrollar un nuevo modelo de análisis de riesgos orientándolo directamente a las PYMES.

Algunos autores [13] sugieren que no es suficiente con aplicar un enfoque basado en análisis y gestión de riesgos sino que, además de identificar y eliminar riesgos, también esta actividad se ha de realizar de manera eficiente, ahorrando dinero, consecuencia directa de una correcta gestión de la seguridad [14, 15].

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.

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, con el consiguiente deterioro de gran parte de la eficacia de los mecanismos tradicionales de protección [16].

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 trabajo 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.

En este artículo, vamos a llevar a cabo una revisión sistemática (RS) de la literatura existente en relación con las investigaciones en el campo de los Análisis de Riesgos, no

A. Santos-Olmo, Departamento I+D+i, Sicaman Nuevas Tecnologías y Marisma Shield, Tomelloso (Ciudad Real), España, Asolmo@sicaman-nt.com
L. E. Sánchez, Grupo de Investigación GSyA, Universidad de Castilla-la Mancha, Ciudad Real, España, Luisenrique@sanchezcrespo.org
E. Álvarez, Fundación In-Nova, Toledo, España, Ealvarez@in-nova.org
D.G. Rosado, Grupo de Investigación GSyA, Universidad de Castilla-la Mancha, Ciudad Real, España, David.Grosado@uclm.es
E. Fernandez-Medina, Grupo de Investigación GSyA, Universidad de Castilla-la Mancha, Ciudad Real, España, Eduardo.FdezMedina@uclm.es

https://doi.org/10.12804/si9789587844337.13

sólo con el fin de resumir las pruebas existentes en relación con este tema, sino también para proporcionar un marco en el que posicionar adecuadamente nuevas líneas de investigación.

Esta revisión sistemática se va a llevar a cabo mediante el uso de las directrices para las revisiones sistemáticas propuestas por Kitchenham [17-19], lo que se ha mostrado apropiado para investigadores de ingeniería del software. Usaremos también un modelo de protocolo de revisión desarrollado por Biolchini et al. [20], que facilita la planificación y ejecución de las revisiones sistemáticas en la ingeniería del software.

El resto del artículo se estructura de la siguiente forma: En la Sección 2 definiremos la pregunta de investigación. En la Sección 3 se explica el método de revisión, que se basa en el protocolo de investigación, y es aquí donde se definirá la estrategia de búsqueda y la selección de estudios. En la Sección 4 definiremos los datos a extraer y que se presentarán en el resumen de los estudios relevantes. En Sección 5 presentaremos los resultados de la revisión y un análisis de los mismos. Finalmente, en la última sección describiremos las principales conclusiones obtenidas.

II. Planificación de la revisión

En este apartado, 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.

A. Objeto de la pregunta.

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.

B. Premisa de la Revisión Sistemática.

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?

Las palabras y conceptos relacionados que se utilizaron para formular esta pregunta y que fueron utilizados durante la ejecución de la revisión son las siguientes:

> Risk analysis: risk analysis model, risk analysis methodology
> Risk management: risk management model, risk management methodology
> Risks: Associative risks, hierarchical risks
> Small & Medium-Sized Business: SMB, SME, PYME

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. La población a analizar se compone de las publicaciones presentes en los repositorios de las fuentes de datos seleccionadas que estén relacionadas con el objetivo de esta revisión.

Los resultados esperados de esta revisión son conocer las propuestas existentes en cuanto a análisis de riesgos asociativos y jerárquicos con orientación a PYMES, para posteriormente analizarlas y conocer qué comparten y en qué difieren, además de identificar necesidades de investigación. Las principales áreas de aplicación que se verán beneficiadas por los resultados de esta revisión sistemática son las relacionadas con la Seguridad de la Información, en especial la Gestión de la Seguridad (concretamente los análisis de riesgos), así como los expertos en seguridad. A tal fin, se proveerá un marco comparativo que permita posicionar adecuadamente las nuevas actividades de investigación en análisis de riesgos.

III. Método de la revisión

El método de revisión se basa en el protocolo de investigación. En esta etapa definimos la estrategia de búsqueda, 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.

A. 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 cuenta con libros electrónicos así como con acceso a las bibliotecas digitales de ACM, IEEE, Science@-Direct o Elsevier, entre otros; la inclusión motores de búsqueda que permitan consultas avanzadas y búsqueda por palabras clave; además, editoriales, libros, revistas y conferencias recomendadas por expertos en la materia (como los miembros de RETISTRUST1, una Red española de expertos en Seguridad de la Información).

La búsqueda de estudios primarios se llevará a cabo utilizando motores de búsqueda en web, bases de datos electrónicas y búsquedas manuales, tales como búsquedas en una revista/conferencia/libro/publicación específica o en publicaciones de investigación recomendadas por expertos en la materia.

Finalmente, la lista de fuentes inicial obtenida sobre la cual se ejecutará la revisión sistemática es la siguiente: ACM digital library, IEEE digital library, Science@Direct, Google

Scholar, SREIS symposium, ESORICS symposium, REFSQ conference, IEEE International Requirements Engineering Conference, ICSE conference, COMPSAC conference, DEXA conference, WOSIS workshop, ICCSA conference, Requirements Engineering Journal, Computer Standards & Interfaces Journal, Computers & Security.

B. 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 5 años. Los criterios de inclusión y exclusión deberían basarse en la Pregunta de investigación. 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. Como criterio de inclusión se realiza principalmente un análisis sobre el título, las palabras claves y el abstract de cada documento, de forma que podemos ver en una primera instancia cómo están relacionadas estas palabras y porqué ha sido seleccionado el estudio. Con este criterio se localizan y eliminan la mayor parte de los resultados obtenidos que no realizan aportaciones sobre análisis de riesgos en el campo de los Sistemas de Información.

El criterio de exclusión actúa sobre el subconjunto de estudios relevantes obtenidos y nos permite obtener el conjunto de estudios primarios. En esta fase nos centramos principalmente en la lectura y análisis del abstract del documento y sus conclusiones, teniendo en algunos casos que profundizar en el mismo y realizar una lectura más detallada sobre otras partes del documento, de cara a ver en más detalle de qué trata cada estudio, ver la relación real que presenta con los objetivos buscados y, si es verdaderamente relevante para la revisión, seleccionarlo como estudio primario.

C. Ejecución de la selección.

En este punto, se ejecuta la búsqueda en cada una de las fuentes seleccionadas con el fin de obtener una lista inicial de los estudios para la posterior evaluación aplicando todos los criterios y procedimientos especificados.

Los procedimientos para la selección de los estudios se aplican a todos los artículos obtenidos a fin de verificar si los estudios se ajustan a los criterios de inclusión y exclusión. Los estudios obtenidos, que corresponden exactamente con todos los criterios de inclusión y exclusión definidos previamente, se detallan en la siguiente sección.

IV. Extracción de la información.

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.

Los formularios de información definidos para esta revisión sistemática contienen la identificación del estudio, la metodología o modelo del estudio, los resultados del estudio, los problemas del estudio y nuestras impresiones generales al respecto.

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.

4.1. Feng, Nan et al. “A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis” [21].

Los autores presentan un modelo de análisis de riesgos de seguridad con el objetivo de identificar las relaciones causales entre los factores de riesgo y analizar la complejidad y la incertidumbre de la propagación de las vulnerabilidades. Se basan en que en los sistemas de información, los riesgos de seguridad son causados por diversos factores internos y externos interrelacionados. De esta forma, una vulnerabilidad de seguridad también podría propagarse y escalar a través de las cadenas causales de los factores de riesgo a través de diferentes vías de acceso.

Los autores desarrollan una red Bayesiana para definir simultáneamente los factores de riesgo y sus relaciones causales basadas en el conocimiento a partir de los casos observados y de los expertos en el dominio.

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

4.2. Webb, J. et al. “A situation awareness model for information security risk management” [22].

Los autores proponen un modelo de análisis de riesgos de seguridad de la información consciente de la situación (SA-ISRM) para complementar el proceso de gestión del riesgo de seguridad de la información. Su objetivo es paliar las

deficiencias en la práctica de la evaluación de riesgos de seguridad de información que inevitablemente conducen a una mala toma de decisiones y estrategias inadecuadas o inapropiadas de seguridad.

De esta forma, el modelo propuesto busca responder a dichas deficiencias a través de la recogida, análisis y comunicación de la información relacionada con los riesgos de la empresa en su totalidad.

El modelo ha sido refinado y perfeccionado mediante un caso de estudio en la empresa de inteligencia de seguridad nacional de Estados Unidos.

4.3. Yongli Tang et al. "Information Security Risk Assessment Method based on Cloud Model" [23].

Los autores proponen una metodología de evaluación del riesgo en Sistemas de Información basándose en la construcción de un modelo basado en la Nube (Cloud). De esta forma, su objetivo es utilizar el "Modelo Cloud" para reducir la incertidumbre en la cuantificación de resultados del análisis de riesgos. Este modelo, por su propia naturaleza, permite tener en cuenta factores asociativos a la hora de realizar la evaluación de riesgos, empleando para ello técnicas difusas (fuzzy).

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

4.4. Vicente, E. et al. "Risk analysis in information systems: A fuzzification of the MAGERIT methodology" [24].

Los autores presentan una extensión de la metodología MAGERIT basada en modelos computacionales fuzzy (difusos) con el objetivo de reducir el grado de incertidumbre en las técnicas de medición de las metodologías tradicionales.

De esta forma, presentan una escala de términos lingüísticos para representar los valores de medición, sus dependencias y frecuencias y la degradación de los activos en entornos de Sistemas de Información.

Estas técnicas se aplican teniendo en cuenta también que la relación de activos de SI puede ser tanto interna como depender de terceras partes, lo que apoya la necesidad de trabajar con factores asociativos de cara a la evaluación y gestión de riesgos.

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

4.5. Saptarshi, M. et al. "Risk analysis using FMEA: Fuzzy similarity value and possibility theory based approach" [25].

Los autores proponen una metodología que incorpore a los procesos de análisis de riesgos las técnicas de FMEA (Failure Mode and Effect Analysis), particularmente las aproximaciones basadas en reglas y técnicas fuzzy.

El objetivo principal es utilizar estas técnicas para reducir la arbitrariedad y, con ello, la incertidumbre en el análisis de riesgos, integrando conceptos de similitud de valores de medición de los número difusos y teorías de posibilidad.

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

4.6. Abdel-Basset, Mohamed et al. "A framework for risk assessment, management and evaluation: Economic tool for quantifying risks in supply chain" [26].

Los autores proponen un framework de gestión y evaluación de riesgos basado en la aplicación de técnicas neutrosóficas. Aunque se aplica al riesgo en el ámbito de una cadena de montaje, es interesante estudiar su posible adaptación a los Sistemas de Información.

Lo interesante de esta propuesta es la introducción de la incertidumbre dentro del análisis de riesgos, así como la posibilidad de obtener valores cuantitativos de riesgo dentro de un escenario afectado por sucesos imprevistos y al que pueden afectar factores como la subjetividad, la incertidumbre o la vaguedad a la hora de obtener valores de riesgo cuantitativos y objetivos que puedan orientar procesos de tomas de decisión. Los autores emplean el Proceso Analítico Jerárquico Neutrosófico (N-AHP) para analizar los factores de riesgo identificados.

Los autores han definido un caso de estudio para aplicar y refinar este framework.

4.7. Sicari, S. et al. "A risk assessment methodology for the Internet of Things" [27].

Los autores proponen una Metodología de análisis y gestión de riesgos con aplicación sobre entornos IoT. El método propuesto (tanto cualitativo como cuantitativo) se basa la construcción de un árbol de ataques adaptado a cada escenario y en un criterio denominado valor de explotabilidad. Inicialmente, la evaluación de este valor se obtiene de forma cualitativa, considerando los niveles de dificultad de realizar un ataque contra el sistema. Estos niveles cualitativos se traducen posteriormente en valores cuantitativos concretos. El valor de explotabilidad general del sistema se calcula finalmente sobre la base de un grafo de dependencia entre las vulnerabilidades identificadas.

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. Además, requiere un alto grado de conocimiento experto para su mantenimiento, y se centra sobre todo en riesgo de ataque sobre componentes físicos, siendo demasiado específico.

4.8. Staalduinen, M.A. et al. "Functional quantitative security risk analysis (QSRA) to assist in protecting critical process infrastructure" [28].

Los autores proponen una metodología cuantitativa de evaluación de riesgos de seguridad orientada a infraestructuras críticas. Se parte de un enfoque orientado a la evaluación

concurrente de amenazas y vulnerabilidades y se introduce un modelo de riesgo "Bow Tie" mapeado en un modelo de Red Bayesiana que permite diferentes supuestos lógicos. Finalmente, se integran las probabilidades de riesgo/vulnerabilidad con valores de pérdida potencial para cuantificar el riesgo.

La importancia de procesos de análisis de riesgos adaptados a infraestructuras críticas siguiendo un modelo "Bow Tie" también se presenta por Abdo, H. et al. en "A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie – combining new version of attack tree with bowtie analysis" [29].

Aunque ambos puntos de partida se centran sobre instalaciones químicas (sobre todo de cara a preparar casos de estudio reales), las metodologías son adaptables a cualquier infraestructura crítica configurando y personalizando sus elementos, aunque es necesario el conocimiento experto para llevarla a cabo.

Los autores han definido un caso de estudio para aplicar y refinar esta metodología.

4.9. Khan, F. et al. "Dynamic risk management: a contemporary approach to process safety management" [30].

Los autores proponen un framework para la gestión dinámica de riesgos, cuya piedra angular es un proceso de evaluación dinámica de riesgos basado en una estrategia Plan-Do-Check-Act (PDCA). De esta forma, se define una evaluación inicial de riesgos, tras la que comienza un ciclo PDCA de evaluación continua.

El framework propuesto está aún en una fase muy inicial, pero lo más interesante de esta propuesta es la creciente importancia del concepto de dinamismo dentro de los procesos de evaluación de riesgos.

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

4.10. Munodawafa, F. et al. "Security risk assessment within hybrid data centers: A case study of delay sensitive applications" [31].

Los autores presentan un estudio discursivo sobre la necesidad de contar con procesos de análisis y gestión de riesgos específicamente en el ámbito de los Centros de datos. No se llega a proponer ni definir un mecanismo concreto pero pone sobre la mesa conceptos relevantes como la necesidad de incluir en la seguridad de estos Centros de datos los riesgos a los que están sometidos no sólo los servidores físicos sino también los virtuales. Este nuevo escenario entronca con las nuevas necesidades en el área del Cloud Computing, con la necesidad de convivencia de sistemas físicos clásicos con sistemas virtuales, así como en los riesgos asociativos derivados de la virtualización.

El estudio presenta una selección inicial de Riesgos y Vulnerabilidades centrados en Data centers, incluyendo algunos específicos para servidores virtuales. También se presenta un caso de estudio centrado específicamente en la evaluación de aspectos de Disponibilidad sobre un servicio de VoIP, si bien es aún muy esquemático y sin demasiado detalle.

4.11. Panchal, D. et al. "A new fuzzy methodology-based structured framework for RAM and risk analysis" [32].

Los autores proponen un framework para la realización de análisis de riesgos que sustenta sus procesos de análisis de riesgos en técnicas de FMEA (Failure Mode and Effect Analysis), particularmente las aproximaciones basadas en reglas y técnicas fuzzy.

El objetivo principal es utilizar estas técnicas para reducir la arbitrariedad y, con ello, la incertidumbre en el análisis de riesgos. De esta forma se utiliza un enfoque Fuzzy Lambda – Tau (FLT) para calcular los parámetros de confiabilidad, disponibilidad y mantenibilidad (RAM) del sistema.

El estudio se centra en el ámbito de una planta de proceso químico, aunque es lo suficientemente genérico como para adaptarse a cualquier tipo de Sistema de Información. En todo caso, refuerza la creciente importancia de procesos de análisis de riesgo específicos para Infraestructuras críticas.

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

4.12. Sangaiah, A.K. et al. "Towards an efficient risk assessment in software projects–Fuzzy reinforcement paradigm" [33].

Los autores proponen un acercamiento basado en técnicas fuzzy como base para el futuro desarrollo de un framework de evaluación de riesgos que permita manejar la incertidumbre y evaluar de forma eficiente los riesgos en el ámbito del desarrollo de proyectos software, de forma que puedan guiar un proceso de tomas de decisiones eficiente a lo largo del Ciclo de vida del proyecto.

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

4.13. Wangen, G. et al. "A framework for estimating information security risk assessment method completeness" [34].

Los autores proponen un framework llamado CURF (Core Unified Risk Framework) cuyo objetivo es comparar métodos de evaluación de riesgos de sistemas de información.

La propuesta es interesante por plantear la necesidad de que este framework sea dinámico, permitiendo adaptarse a nuevas características y tareas de los métodos revisados. Además, entre sus criterios de comparación de métodos de análisis de riesgo incluye como factores clave que se adapte a Cloud Computing y que tenga en cuenta la Reutilización del conocimiento.

4.14. Zhang, H. et al. “An Integrated Approach to Risk Assessment for Special Line Shunting Via Fuzzy Theory” [35].

Los autores presentan un proceso de evaluación de riesgos basado en técnicas fuzzy con el objetivo principal de obtener valores de riesgo fiables en entornos sujetos a factores ambientales que condicen a obtener resultados de riesgo incompletos o involucran altos niveles de incertidumbre.

Aunque el estudio se aplica específicamente al ámbito ferroviario, sus conceptos son fácilmente extrapolables al campo de las TI donde la incertidumbre es también un factor clave en los procesos de Análisis de riesgos. De esta forma, se redunda en la importancia de la reducción de incertidumbre de cara a obtener resultados fiables, así como en otros conceptos muy interesantes como son la utilización tanto de técnicas cualitativas como cuantitativas.

El estudio también incide en la necesidad de tener en cuenta las relaciones jerárquicas y define un caso de estudio para aplicar este proceso.

V. ANÁLISIS DE RESULTADOS.

Los resultados de la revisión sistemática se muestran en la siguiente tabla, que resume la cantidad de estudios por iniciativa:

Tipo de iniciativa	Nº de estudios	Iniciativas
Proceso	1	4.14
Framework	5	4.6, 4.9, 4.11, 4.12, 4.13
Modelo	2	4.1, 4.2
Metodología	5	4.3, 4.4, 4.5, 4.7, 4.8
Otros	1	4.10
Total	14	-

Tabla 1: Resultados por iniciativa

Como podemos ver en la tabla anterior, hay muchos nuevos frameworks, procesos, modelos y metodologías que intentan facilitar la gestión, evaluación y/o el análisis de riesgos teniendo en cuenta factores como la flexibilidad o simplicidad de su aplicación (necesaria para poder aplicarlos al ámbito de la PYME), o considerando la importancia de gestionar los riesgos jerárquicos y asociativos, imprescindible para Cloud Computing o IoT, por ejemplo. También se empieza a ver la necesidad de controlar el riesgo en sistemas asociados de forma específica a Infraestructuras críticas.

Sin embargo, muy pocos trabajos describen casos de estudio complejos que muestren la posibilidad y los beneficios obtenidos de aplicar el modelo o metodología propuestos en la práctica.

Por otra parte, como se puede ver en la Tabla 2, después de nuestro análisis hemos llegado a la conclusión de que cada una de las iniciativas seleccionadas nos ofrece aspectos muy importantes que tienen que ver con los requisitos de análisis de riesgos en Sistemas de Información. Estas son características que pueden ser utilizadas como base para el desarrollo de una metodología que incluya todas las características deseadas.

Iniciativa	Ámbito	Técnica/ Modelo base	Principales contribuciones
Feng, Nan	Global	Redes Bayesianas	- Análisis de la incertidumbre de propagación de debilidades
Webb, J.	Global	-	- Procesos de toma de decisiones - Mejora de los procesos de recogida, análisis y comunicación de información relativa a riesgos - Caso de estudio
Yongli Tang	Global	Modelo Cloud Técnicas difusas	- Modelo basado en la Nube - Gestión de riesgos asociativos
Vicente, E.	Global	Técnicas difusas	- Reducción del grado de incertidumbre - Importancia del entorno y de terceros en la evaluación de riesgos
Saptarshi, M.	Global	FMEA	- Reducción del grado de incertidumbre
Abdel-Basset, Mohamed	-	N-AHP	- Gestión de la incertidumbre - Uso de AHP para analizar factores de riesgo e impacto - Caso de estudio
Sicari, S.	IoT	-	- Valor de explotabilidad de vulnerabilidades - Grafos de vulnerabilidad
Staalduinen, M.A. Abdo, H.	Infraestructuras Críticas	- Modelos Bow Tie - Redes Bayesianas	- Análisis concurrente de riesgos y vulnerabilidades - Caso de estudio
Khan, F.	Global	-	- Evaluación dinámica del riesgo
Munodawafa, F.	Data Centers	-	- Análisis de riesgos en virtualización - Riesgos en Data centers fuera de la infraestructura del SI pero que forman parte de ella
Panchal, D.	Infraestructuras Críticas	FMEA	- Reducción del grado de incertidumbre
Sangaiah, A.K.	Desarrollo de Software	Técnicas difusas	- Reducción del grado de incertidumbre
Wangen, G.	Global	-	- Reutilización del conocimiento - Importancia de la Evaluación dinámica del riesgo y los entornos en la Nube
Zhang, H.	-	Técnicas difusas	- Reducción del grado de incertidumbre - Factores jerárquicos para valoración de probabilidad e impacto de los riesgos

Tabla 2: Principales contribuciones de las propuestas seleccionadas

En la Tabla 3 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.
- Cloud Computing: El modelo tiene en cuenta la aplicación en entornos de Cloud Computing.

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 (S), parcialmente cumplido (P) o no tenido en cuenta por el modelo (N).

Iniciativa	Ámbito Global	Métricas	Técnicas Cualitativas	Técnicas Cuantitativas	Asociativo	Jerárquico	Orientado PYMES	Reutilización Conocimiento	Herramienta Software	Casos Prácticos	Cloud Computing
Feng, Nan	S	S	N	S	S	N	N	N	N	N	N
Webb, J.	S	N	N	N	S	N	N	N	N	S	N
Yongli Tang	S	S	S	S	S	N	N	N	N	N	S
Vicente, E.	S	S	S	N	S	N	N	N	N	N	P
Saptarshi, M.	S	S	S	N	S	N	N	N	N	N	N
Abdel-Basset, Mohamed	N	N	N	S	P	N	N	N	N	S	N
Sicari, S.	N	P	S	S	N	N	N	N	N	S	N
Staalduinen, M.A. Abdo, H.	N	N	N	S	N	N	N	N	N	S	N
Khan, F.	S	N	N	N	N	N	N	P	N	N	N
Munodawafa, F.	N	N	N	N	P	N	N	N	N	P	S
Panchal, D.	S	P	S	N	N	N	N	N	N	N	N
Sangaiah, A.K.	N	S	S	N	N	N	N	N	N	N	N
Wangen, G.	S	N	N	N	S	N	N	S	N	N	N
Zhang, H.	N	S	S	S	N	S	N	N	N	N	N
MARISMA	**S**	**S**	**S**	**S**	**S**	**S**	**S**	**S**	**S**	**S**	**S**

Tabla 3: 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. Adicionalmente, las pocas aplicaciones que han intentado abordar todo el Sistema de Información requieren de una gestión compleja y de un mantenimiento costoso, con una necesidad importante de conocimiento experto para poder mantener el sistema de gestión y evaluación de riesgos, lo que hace que no sean adecuadas para las PYMES.
- 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.

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

VI. Conclusiones.

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, que sean válida para las 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 [36-40].

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 (Khan [30] han intentado 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.
- Aunque está creciendo el número de propuestas que inciden en la necesidad de tener en cuenta factores como el dinamismo, la reutilización del conocimiento y la reducción de la incertidumbre a la hora de realizar un análisis de riesgos, son muy pocas las traslaciones prácticas de dichas propuestas a casos reales y se encuentran en fases muy iniciales.

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 todo tipo de compañías, y en espacial para el caso de las PYMES.

Todos los estándares y propuestas para la evaluación y gestión de riesgos estudiados 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 ha sido co-financiada por los proyectos *GENESIS - Security Government of Big Data and Cyber Physics Systems ((SBPLY/17/180501/000202)* financiado por el "JCCM- Consejería de Educación, Cultura y Deportes, y Fondos FEDER", del proyecto ECLIPSE – Enhancing Data Quality and Security for Improving Business Processes and Strategic Decisions in Cyber Physical Systems (RTI2018-094283-B-C31) financiado por la "Ministerio Economía, Industria y Competitividad y fondos FEDER", y ha contado con el apoyo de las empresas Marisma Shield S.L (www.emarisma.com) y Sicaman Nuevas Tecnologías (www.sicaman-nt.com).

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] Vivas, T., A. Zambrano, and M. Huerta. *Mechanisms of security based on digital certificates applied in a telemedicine network*. in *2008 30th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*. 2008. IEEE.

[4] 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.

[5] 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.

[6] Huerta, M., et al. *Implementation of a open source security software platform in a telemedicine network*. in *Proceedings of the 9th WSEAS international conference on Advances in e-activities, information security and privacy*. 2010. World Scientific and Engineering Academy and Society (WSEAS).

[7] Pirrone, J. and M. Huerta. *Security Mechanism for Medical Record Exchange Using Hippocratic Protocol*. in *World Congress on Medical Physics and Biomedical Engineering 2018*. 2019. Springer.

[8] 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.

[9] Huerta, M., et al. *Design of a building security system in a university campus using RFID technology*. in *2017 IEEE 37th Central America and Panama Convention (CONCAPAN XXXVII)*. 2017.

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

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

[12] 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.

[13] 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.

[14] Garigue, R. and M. Stefaniu, *Information Security Governance Reporting.* Information Systems Security, 2003. **sept/oct**: p. 36-40.

[15] Mercuri, R.T., *Analyzing security costs.* Communications of the ACM, 2003. **46**: p. 15-18.

[16] Zissis, D. and D. Lekkas, *Addressing cloud computing security issues.* Future Generation Computer Systems, 2012. **28**(3): p. 583-592.
[17] Brereton, P., et al., *Lessons from applying the systematic literature review process within the software engineering domain.* Journal of Systems and Software, 2007. **80**(4): p. 571-583.
[18] Kitchenham, B., *Procedures for performing systematic reviews.* Keele, UK, Keele University, 2004. **33**(2004): p. 1-26.
[19] Kitchenham, B. and S. Charters, *Guidelines for performing systematic literature reviews in software engineering version 2.3.* Engineering, 2007. **45**(4ve): p. 1051.
[20] Biolchini, J., et al., *Systematic review in software engineering.* System Engineering and Computer Science Department COPPE/UFRJ, Technical Report ES, 2005. **679**(05): p. 45.
[21] Feng, N., H.J. Wang, and M. Li, *A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis.* Information Sciences, 2014. **256**(0): p. 57-73.
[22] Webb, J., et al., *A situation awareness model for information security risk management.* Computers & Security, 2014. **44**(0): p. 1-15.
[23] Yongli, T., et al. *Information security risk assessment method based on cloud model*. in *Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conf. on Infor. and Comm. Technologies (ISSC 2014/CIICT 2014). 25th IET*. 2014.
[24] Vicente, E., A. Mateos, and A. Jiménez-Martín, *Risk analysis in information systems: A fuzzification of the MAGERIT methodology.* Knowledge-Based Systems, 2014. **66**(0): p. 1-12.
[25] Mandal, S. and J. Maiti, *Risk analysis using FMEA: Fuzzy similarity value and possibility theory based approach.* Expert Systems with Applications, 2014. **41**(7): p. 3527-3537.
[26] Abdel-Basset, M., et al., *A framework for risk assessment, management and evaluation: Economic tool for quantifying risks in supply chain.* Future Generation Computer Systems, 2019. **90**: p. 489-502.
[27] Sicari, S., et al., *A risk assessment methodology for the Internet of Things.* Computer Communications, 2018. **129**: p. 67-79.
[28] van Staalduinen, M.A., et al., *Functional quantitative security risk analysis (QSRA) to assist in protecting critical process infrastructure.* Reliability Engineering & System Safety, 2017. **157**: p. 23-34.
[29] Abdo, H., et al., *A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie–combining new version of attack tree with bowtie analysis.* Computers & Security, 2018. **72**: p. 175-195.
[30] Khan, F., et al., *Dynamic risk management: a contemporary approach to process safety management.* Current opinion in chemical engineering, 2016. **14**: p. 9-17.
[31] Munodawafa, F. and A.I. Awad, *Security risk assessment within hybrid data centers: A case study of delay sensitive applications.* Journal of Information Security and Applications, 2018. **43**: p. 61-72.
[32] Panchal, D., et al., *A new fuzzy methodology-based structured framework for RAM and risk analysis.* Applied Soft Computing, 2019. **74**: p. 242-254.
[33] Sangaiah, A.K., et al., *Towards an efficient risk assessment in software projects–Fuzzy reinforcement paradigm.* Computers & Electrical Engineering, 2018. **71**: p. 833-846.
[34] Wangen, G., C. Hallstensen, and E. Snekkenes, *A framework for estimating information security risk assessment method completeness.* International Journal of Information Security, 2018. **17**(6): p. 681-699.
[35] Zhang, H. and Q. Sun, *An Integrated Approach to Risk Assessment for Special Line Shunting Via Fuzzy Theory.* Symmetry, 2018. **10**(11): p. 599.
[36] Batista, J. and A. Figueiredo, *SPI in very small team: a case with CMM.* Software Process Impr. and Practice, 2000. **5**(4): p. 243-250.
[37] Hareton, L. and Y. Terence, *A Process Framework for Small Projects.* Software Process Improvement and Practice, 2001. **6**: p. 67-83.
[38] Tuffley, A., B. Grove, and M. G, *SPICE For Small Organisations.* Software Process Improvement and Practice, 2004. **9**: p. 23-31.
[39] 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.
[40] Mekelburg, D., *Sustaining Best Practices: How Real-World Software Organizations Improve Quality Processes.* Software Quality Professional, 2005. **7**(3): p. 4-13.

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).

Luis Enrique Sánchez is PhD and MsC in Computer Science and is a Professor at the Universidad 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 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).

Esther Álvarez President of Private Foundation In-nova 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).

David G. Rosado has an MSc and PhD. in Computer Science from the University of Málaga (Spain) and from the University of Castilla-La Mancha (Spain), respectively. His research activities are focused on security for Information Systems and Cloud Computing. He has published several papers in national and international conferences on these subjects, and he is co-editor of a book and chapter books. Author of several manuscripts in national and international journals (Information Software Technology, System Architecture, Network and Computer Applications, etc.). He is member of Program Committee of several conferences and workshops nationals and internationals such as ICEIS, ICCGI, CISIS, SBP, IAS, SDM, SECRYPT, COSE and international journals such as Internet Research, JNCA, KNOSYS, JKSU, and so on. He is a member of the GSyA research group of the Information Systems and Technologies Department at the University of Castilla-La Mancha, in Ciudad Real, Spain.

Eduardo Fernández-Medina holds a PhD. and an MSc. in Computer Science from the University of Sevilla. He is associate Professor at the Escuela Superior de Informática of the University of Castilla-La Mancha at Ciudad Real (Spain), his research activity being in the field of security in databases, datawarehouses, web services and information systems, and also in security metrics. Fernández-Medina is co-editor of several books and chapter books on these subjects, and has several dozens of papers in national and international conferences (DEXA, CAISE, UML, ER, etc.). Author of several manuscripts in national and international journals (Information Software Technology, Computers And Security, Information Systems Security, etc.), he is director of the GSyA research group of the Information Systems and Technologies Department at the University of Castilla-La Mancha, in Ciudad Real, Spain.