Gestión de la seguridad y análisis de riesgos

Realizando una Revisión Sistemática de Metodologías ISRA orientadas a la Seguridad TIC. Periodo 2014-2019

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

***Resumen* – La sociedad de la información depende cada vez más de los Sistemas de Gestión y Análisis del Riesgo al que se encuentran sometidos sus principales activos de información. Poder disponer de estos sistemas es crítico para una correcta protección de los Sistemas de Información de las compañías. Sin embargo, hoy en día desconocemos la situación de las metodologías, modelos y estándares de riesgo TIC, así como las carencias que tienen los mismos. De esta forma, las empresas no saben cómo seleccionar el modelo de Análisis de Riesgos TIC más adecuado para su compañía. En este artículo, presentamos los resultados obtenidos tras aplicar el método de investigación "Revisión Sistemática de la Literatura" de las propuestas científicas orientadas a las llamadas Metodologías ISRA (Information Security Risk Analysis) publicadas en los últimos 5 años.**

Palabras clave — Cibersecurity, Information Systems Security Management, ISRA, Information Security Risk Analysis, ISMS, Risk Analysis.

I. Introducción

Hoy en día, los elementos digitales o las infraestructuras (computadoras, redes, contenidos, etc.), son elementos cada vez más complejos y dependientes de las TI que están en el centro de nuestras vidas y constituyen los pilares esenciales de nuestras infraestructuras de comunicación, económicas, sociales e institucionales. La seguridad y la mitigación de amenazas dentro de esos sistemas se han convertido implícitamente en una parte fundamental para el ciudadano (para preservar su privacidad), para la empresa (para proteger los activos y transacciones digitales) y para los estados (para proteger sus infraestructuras críticas y asegurar la continuidad del gobierno y servicios gubernamentales, etc.) [1-3], y en especial en ciertos sectores como el de la salud [4], o el de la educación [5].

Para proteger estos sistemas recurrimos a la gestión de la seguridad, que según [6] puede definirse como un sistema de gestión usado para establecer y mantener un entorno seguro de la información. El objetivo principal de un SGSI (Sistema de Gestión de Seguridad de la Información) es afrontar la puesta en práctica y el mantenimiento de los procesos y procedimientos necesarios para manejar la seguridad de las tecnologías de la información. Estas acciones incluyen la identificación de las necesidades de seguridad de la información y la puesta en práctica de estrategias para satisfacer estas necesidades, medir los resultados y mejorar las estrategias de protección.

La definición de un SGSI es una tarea ardua y compleja que requiere un proceso previo de definición en la compañía donde se quiere establecer. Una de las fases más importantes para la implantación de un SGSI es la de Análisis y gestión del riesgo, que para algunos investigadores es una de las fases más críticas [7].

Todas las organizaciones que utilizan tecnologías de la información tienen problemas con la seguridad de su sistema de información. El primer paso en el proceso de protección de un sistema de información es la identificación y clasificación de los recursos o activos de información que necesitan protección, porque son vulnerables a las amenazas, y para realizar este paso necesitamos contar con sistemas de análisis y gestión de riesgos adecuados [8]. Diferentes investigadores destacan que la gestión del riesgo es un proceso esencial en cualquier modelo de gestión empresarial [9, 10], y que la información es un activo valioso que se espera que esté protegido [11].

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 [12]. 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.

Actualmente se están realizando muchas investigaciones sobre análisis de riesgos, y muchas de ellas intentan comparar los métodos clásicos para ver cómo se podrían alinear [13-19]. Otros investigadores han realizado también algunos análisis comparativos de los principales estándares de riesgos con el objetivo de mejorar algunos de sus aspectos -entre ellos podemos destacar [20], o trabajos que relacionan los planes de contingencia con el análisis de riesgos [21]. Uno de los puntos de divergencia entre las metodologías se trata de cómo cuantificar todos estos elementos que forman parte del análisis

L. E. Sánchez, Grupo de Investigación GSyA, Universidad de Castilla-la Mancha, Ciudad Real, España, Luisenrique@sanchezcrespo.org

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

V. Figueroa, OPTIC – Gobierno de la Provincia, Neuquen, Argentina, vfigueroa@neuquen.gov.ar

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/si9789587844337.11

de riesgos. A continuación destacamos algunas problemáticas identificadas por otros investigadores:

- Según Alcántara [22], uno de los problemas que se presentan es que los riesgos de los activos de información tienen una naturaleza compleja. La gestión del riesgo de la seguridad de la información se aborda mediante diferentes enfoques. Existe una importante carencia sobre cómo implementar sistemas que gestionen esto riesgos.
- Para Shamala [23], la seguridad de la información se ha convertido en un elemento esencial para que las organizaciones de todo el mundo eliminen los posibles riesgos en sus sistemas de información mediante la evaluación de riesgos de seguridad de la información (ISRA). Sin embargo, la existencia de numerosos tipos diferentes de métodos de evaluación de riesgos, estándares, pautas y especificaciones disponibles hace que las organizaciones afronten de forma desalentadora la tarea de determinar el método más adecuado para satisfacer sus necesidades.
- Ford [24] destaca que, en base a su experiencia como consultor experto en la materia, la mayoría de las industrias que visita desconocen cómo abordar el tema de la Gestión de riesgos de IT, y la mayoría recurren a realizar un análisis de riesgos obligadas por regulaciones como la SOX, HIPAA, etc., y no por el valor diferencial que este tipo de sistemas le puede generar.
- Según Derakhshandeh [25], la seguridad se está convirtiendo cada vez más en un foco crítico en los sistemas de información. Con más redes, movilidad y teletrabajo, existe una mayor necesidad de una evaluación de los riesgos técnicos y de seguridad.
- Dehkhoda [26] analiza la posibilidad de unir métodos tradicionales de análisis de riesgos como IRAM2 con los análisis CBA (Cost-Benefit Analysis), ya que entiende que los unos no pueden funcionar sin los otros.
- Duricu [27], se centra en la necesidad que marca la nueva legislación europea de privacidad de datos (GDPR) de realizar un análisis de riesgos y la necesidad de crear un nuevo modelo, dado que los modelos tradicionales (OCTAVE Allegro, ISO, NIST) no se adaptan a la casuística de esta nueva legislación.
- Para Shamala [28], la seguridad de la información se ha convertido en un punto crítico para las organizaciones de todo el mundo, ya que realizan negocios en un entorno interconectado y rico en información. Por lo tanto, las organizaciones desean eliminar los posibles riesgos en sus organizaciones mediante la evaluación de riesgos de seguridad de la información (ISRA). Los ISRA les permite identificar y priorizar los activos de información y garantizar que se utilicen mecanismos de control efectivos para los activos de información de alta prioridad, pero los métodos actuales de ISRA tienen limitaciones críticas ya que adoptan simplemente una perspectiva técnica. Los métodos ISRA disponibles actualmente funcionan en una vista limitada de los activos de información, y por tanto es necesario desarrollar nuevas taxonomías de activos para ellos.
- Según Wangen [29], gran parte del debate en torno a la gestión de riesgos en seguridad de la información (InfoSec) ha sido a nivel académico, donde la cuestión de cómo los profesionales ven los problemas predominantes es un elemento esencial que a menudo se deja sin explorar. Por lo tanto, este artículo representa una visión inicial de cómo los profesionales de riesgos de InfoSec ven el campo de evaluación de riesgos de Información (ISRA). El estudio presenta los resultados de un estudio de 46 participantes donde han reunido datos sobre problemas conocidos en ISRA. También destacan que la teoría de los “cisnes negros” (eventos catastróficos poco probables) no suele ser tenida en cuenta dentro de estos sistemas. Por último los investigadores determinan que los métodos actuales no son suficientes para resolver los problemas y que son necesarios nuevos métodos más avanzados.
- Para Haythorn [30], la realización de una evaluación de riesgos es un paso esencial para las organizaciones a fin de garantizar que existan controles adecuados para proteger los activos que son críticos para las funciones comerciales. La evaluación de riesgos puede ser una tarea muy compleja, que requiere múltiples metodologías y recursos para realizar análisis cuantitativos y cualitativos basados en evidencia fáctica y opinión subjetiva. En última instancia, la organización tiene la responsabilidad del análisis preciso y las medidas de control. La necesidad de una evaluación de riesgos precisa ha creado múltiples marcos de referencia que las organizaciones pueden utilizar para cubrir sus necesidades. Es responsabilidad de los profesionales de seguridad de la información dentro de la organización analizar múltiples marcos y utilizar los métodos que sean ideales para cada caso.
- Según Pandey [31], cualquier activo de información, cuando está conectado al mundo exterior, es vulnerable a los ataques. Los ataques son causados principalmente por amenazas que tienen el potencial de explotar vulnerabilidades. Cualquier tipo de daño a estos activos causa riesgos y es uno de los factores más importantes para la organización. El riesgo de ataques maliciosos a la seguridad del software ha aumentado considerablemente y es muy necesario evitarlo. La máxima "antes es mejor" se ha convertido en el orden del día. Por lo tanto, este estudio se realizó en vista de la importancia de la evaluación de riesgos en la fase de requisitos de SDLC (Software Development Life Cycle).
- Rea-Guaman [32] destaca que, en ciberseguridad, la identificación de riesgos es una parte fundamental porque esta actividad no es exclusiva de la ciberseguridad y es difícil saber cuáles son los riesgos en esta área concreta. Este estudio tiene como objetivo identificar si existen taxonomías de riesgo en ciberseguridad.
- López [33] se centra en el Riesgo Dinámico y destaca que la aplicación de procesos de Análisis y Gestión de Riesgos en el ámbito de los Sistemas de Información es una práctica común que permite la planificación en un

momento puntual de tiempo de las acciones preventivas frente al riesgo a corto, medio o largo plazo, pero con un considerable potencial actualmente desaprovechado para facilitar la toma de decisiones en tiempo real frente a eventos o incidentes de seguridad. Este trabajo hace un recorrido por las principales corrientes que buscan sacar partido a este potencial, englobadas principalmente bajo el concepto de Análisis de Riesgos Dinámico.

- Para Ganin [34], los evaluadores y gerentes de riesgos enfrentan muchos desafíos difíciles relacionados con los nuevos sistemas cibernéticos. Entre estos desafíos se encuentran la naturaleza en constante cambio de los sistemas cibernéticos causado por los avances técnicos, su distribución a través de los dominios físicos, de información y sociocognitivos, y las complejas estructuras de red que a menudo incluyen miles de nodos.
- Según Smojver [35], numerosos métodos existentes de gestión de riesgos de seguridad de la información (ISRM) difieren mucho en su enfoque, complejidad de uso, nivel de detalle y aplicabilidad a organizaciones de diferentes tamaños y modelos de negocio. La selección de un método que se ajuste a los requisitos de una organización puede ser un proceso complejo e intensivo en recursos, con una posibilidad significativa de decisión subóptima.
- Beckers [36] destaca la importancia de constatar que los estándares de seguridad y de gestión de riesgos puede ser un desafío, en parte porque las descripciones de lo que se debe realizar suelen ser genéricas y deben ser perfeccionadas por expertos en seguridad. Eliminar esta ambigüedad requiere mucho tiempo para los expertos en seguridad, ya que tienen que interpretar todas las tareas requeridas en el estándar por su cuenta.
- Para Shedden [37] existen muchas metodologías para evaluar los riesgos de seguridad asociados con fugas no autorizadas, modificación e interrupción de información en una organización determinada. Argumentan que la orientación tradicional de estas metodologías, hacia la identificación y evaluación de los activos de información técnica, oscurece los riesgos clave asociados con el cultivo y despliegue del conocimiento organizacional. Basándose en la literatura de gestión del conocimiento, el estudio sugiere mecanismos para incorporar estas consideraciones basadas en el conocimiento en el alcance de las metodologías de riesgo de seguridad de la información.
- Según Rot [38], el riesgo relacionado con la aplicación de las tecnologías de la información en los negocios crece junto con el aumento de la correlación empresarial con sus clientes, socios comerciales y operaciones subcontratadas. El progreso tecnológico genera dependencias que evocan el crecimiento de la diversidad, la complejidad, la falta de descripción y la cantidad de factores de riesgo. En inversiones insuficientes en seguridad de la información, el tema de la gestión de riesgos de TI se vuelve más importante, concentrándose en buscar la proporción óptima entre las amenazas y los costes de la protección de los sistemas de TI. En un desarrollo tan dinámico de las Tecnologías de la Información, el tiempo necesario para una reacción apropiada ante el riesgo se acorta de forma determinante. La falta de una preparación adecuada puede llevar a la empresa al colapso, por lo que la reacción adecuada al riesgo constituye la posibilidad de supervivencia y desarrollo de la empresa. El problema de la gestión de riesgos de TI es un problema muy complejo. Una de las etapas más importantes de este proceso es el análisis de riesgos, utilizado para la optimización y la minimización de las pérdidas relacionadas con el riesgo.
- Saripalli [39] plantea la necesidad de modernizar los modelos de riesgos para que se puedan adaptar a entornos como el Cloud Computing [39]
- Por último Li y Sicari [40, 41], proponen la necesidad de avanzar en el análisis de riesgos para IoT, tanto desde el punto de vista de modernizar los modelos existentes como la necesidad de añadir sistemas inteligentes de valoración del riesgo, tales como las redes neuronales.

Toda esta información y cómo se lleva a cabo el proceso está recogido en lo que se denominan 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 [12] 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.

Después de analizar estas propuestas, vemos que es de interés el llevar a cabo una revisión sistemática (RS) de la literatura existente en relación con las Metodologías y Estándares de Análisis de riesgos que se están utilizando actualmente, su estado y evolución histórica, con el objetivo de entender su situación actual.

Como se trata de una revisión sistemática, se sintetiza el trabajo existente de forma que sea coherente [42-44]. En contraste con el proceso habitual de una revisión de la literatura, que se lleva a cabo de manera no sistemática cada vez que alguien acomete una parte particular de una investigación, una RS se desarrolla, como el término denota, de una manera formal y sistemática [45]. Esto significa que el proceso de investigación de una revisión de tipo sistemático sigue una secuencia de pasos metodológicos muy bien definida y estricta, conforme a un protocolo desarrollado apriorísticamente. Ésta se lleva a cabo en torno a un tema central, que representa el núcleo de la investigación, y que se expresa mediante el uso de una pregunta específica, previamente definida, centrado y estructurada. Los pasos metodológicos, las estrategias para recuperar la evidencia y el enfoque en la cuestión se definen explícitamente, de manera que otros profesionales pueden reproducir el mismo protocolo y también pueden juzgar la idoneidad de los estándares elegidos para el caso en cuestión.

Esta revisión sistemática se va a llevar a cabo mediante el uso de las directrices para las revisiones sistemáticas propuestas

por Kitchenham [42-44], que se han mostrado apropiadas para investigaciones de ingeniería del software. Usaremos también un modelo de protocolo de revisión desarrollado por Biolchini et al. [45], 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 de carácter general, con el objetivo de entender su estado actual y cuáles son los que se están utilizando actualmente.

B. Premisa de la Revisión Sistemática.

Podemos definir la pregunta de investigación de este trabajo, por tanto, de la siguiente forma:

> ¿Qué Metodologías y Estándares existen actualmente relacionados con el Análisis de Riesgos y en qué estado se encuentran?

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:

> "Information Security Risk Assessment", ISRA
> "Information Security Risk Management", ISRM
> Risk management: Risk assessment methodology

En el contexto de la revisión sistemática planificada se van a observar las propuestas existentes sobre modelos y metodologías de análisis de riesgos generales, 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 generales, 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.

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, las principales fuentes de 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 standard OR guidelines
AND
"Information Security Risk Assessment" OR ISRA
AND
"Information Security Risk Management" OR ISRM
AND
"risk analysis" OR "risk management" OR "risk assessment"

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 (2014 – 2019). 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 nivel general.

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.

Algunos de los artículos obtenidos han sido descartados por no ofrecer información relevante, o estar sesgados hacia algunos sectores, aun así consideramos interesantes hacer mención sobre ellos:

- Svatá, V. and M. Fleischmann, "IS/IT Risk Management in banking industry" [46]: En esta investigación el autor analiza la relación de algunos estándares de riesgos con la norma Bancaria de Basilea II para alinearlos en su aplicación al sector financiero.
- Mayer, N., P. Heymans, and R. Matulevicius. "Design of a Modelling Language for Information System Security Risk Management". [47]: En esta investigación el autor plantea la necesidad de diseñar un lenguaje formal para el análisis y gestión de riesgos de información.

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.

1.1. García, F.Y.H. and L.M.L. "Moreta. Maturity Model for the Risk Analysis of Information Assets based on Methodologies MAGERIT, OCTAVE y MEHARI; focused on Shipping Companies" [48].

En la Investigación [48, 49] se propone un nuevo modelo de madurez para el Análisis de Riesgos de los Activos de Información, derivado de las Metodologías MAGERIT, OCTAVE y MEHARI y una orientación sectorial, en concreto a empresas del sector marítimo.

La Investigación propone un modelo de mapa de control compuesto por 11 categorías a evaluar (A. Política de Riesgo, B. Responsabilidad, C. Compromiso de la Alta Dirección; D. Comunicación y Formación; E. Determinación y Valoración de los Activos de Información; F. Identificación y estimación de Amenazas; G. Estimación de Impacto; H. Evaluación del Riesgo; I. Respuesta a los Riesgos; J. Actividades de Control y K. Mejora Continua del Análisis de Riesgo) y 5 Niveles de Madurez (Nivel 1. Inicial; Nivel 2. Repetible; Nivel 3. Definido; Nivel 4. Administrado; Nivel 5. Optimizado).

1.2. Gritzalis, D., et al., "Exiting the Risk Assessment maze: A meta-survey" [50].

En la Investigación se puede ver una comparativa entre 10 metodologías de Análisis de Riesgos, con 3 criterios de comparación.

Se analizan las siguientes metodologías de Análisis de Riesgos: EBIOS, MEHARI, OCTAVE, IT-Grundschutz, MAGERIT, CRAMM, HTRA, NIST SP800, RiskSafe Assessment y CORAS.

Se analizan las siguientes dimensiones: Si incluye las cuatro fases del análisis de riesgos (1. Preparación; 2. Identificación del Riesgo; 3. Análisis del Riesgo; y 4. Evaluación del Riesgo); El modelo de cálculo del riesgo; y el tipo de Análisis que realiza (Cualitativo o Cuantitativo).

El articulo también muestra otras tablas comparativas interesantes entre las metodologías que incluyen su vinculación con otros estándares y costes asociados con el soporte y el software. Finalmente, muestra un análisis de características como: la facilidad de uso, el ciclo de vida de sus versiones, los objetivos respecto al tamaño de las empresas, software que la soporta, adaptabilidad, etc.

1.3. Mrksic Kovacevic, S., "Smart homes from a Risk Management perspective" [51].

En la Investigación podemos ver el trabajo de Tesis realizado sobre una maestría especializada en "Risk Assessment and Management".

Dentro de esta tesis de maestría, el autor analiza y compara diferentes metodologías y estándares de análisis de riesgos, en particular: OCTAVE Allegro, FAIR, NIST CSF, RaMEX, ISRAM, CORAS y CIRA.

De cada una de ellas se analiza: i) Tipo de metodología; ii) Nivel; iii) Tiempo de implantación; iv) Fortalezas; v) Debilidades; y vi) Perspectivas individuales, empresariales y gubernamentales.

1.4. Wangen, G., C. Hallstensen, and E. Snekkenes, "A framework for estimating information security risk assessment method completeness" [52, 53].

En la Investigación podemos ver cómo se plantea la dificultad de comparar los diferentes métodos al no existir criterios unificados de comparación. Por ello se propone la creación de un marco unificado de comparación (Core Unified Risk Framework – CURF), que permitirá comparar diferentes modelos.

Dentro de esta investigación se compararon los siguientes modelos de riesgos: CIRA, CORAS, CRAMM, FAIR, NSMROS, OCTAVE A, ISO27005, NIST 800-30, RISK IT, RAIS y CRDF.

Para cada uno de los modelos se analizan en detalle: i) Los problemas relacionados con la identificación de riesgos; ii) La estimación del riesgo; iii) Problemas relacionados con la Evaluación del riesgo; y iv) Problemas de la Integridad del Riesgo.

1.5. Novoa, H.A. and C.R. Barrera, "Metodologías para el análisis de riesgos en los sgsi" [54].

En la Investigación podemos ver una pequeña comparativa entre algunas de las principales metodologías de Análisis de Riesgos. En concreto, se analiza OCTAVE, MAGERIT, MEHARI, NIST SP 800-30, CORAS, CRAMM y EBIOS, analizando su ámbito de aplicación y las ventajas y desventajas de cada una de ellas, orientándolas a su aplicación en los SGSI, aunque el análisis que se realiza es superficial y no entra a identificar las principales problemáticas que pueden tener estos modelos metodológicos en su aplicación real.

1.6. Santonja Lillo, J., "Análisis y correlación entre probabilidad e impacto de los riesgos" [55].

En la Investigación se realiza una comparativa entre algunas de las principales metodologías de Análisis de Riesgos. En particular, se analizan Octave (las tres versiones), Magerit, Mehari, Cramm y NIST SP 800:30, analizando las ventajas y desventajas de cada una de ellas y las fases que cubren.

Las fases han sido catalogadas en: Caracterización del Sistema, Identificación de Amenazas, Identificación de Vulnerabilidades, Análisis de Controles, Determinación de la Probabilidad, Análisis de Impacto, Determinación del Riesgo, Recomendaciones de Control, Documentación de los resultados, Establecimiento de Parámetros y Necesidades de Seguridad.

1.7. Hashim, N.A., et al., "Risk Assessment Method for Insider Threats in Cyber Security: A Review" [56].

En la Investigación se realiza una comparación entre NIST SP 800-30, OCTAVE, FRAP y CRAMM, mencionando las principales investigaciones que las referencian, así como el tipo de metodología, las fases principales de cada una de ellas y los recursos que requiere su implementación. Dentro de esta investigación, su principal conclusión es que el método que mejor aceptación tiene de los evaluados fue el del NIST por su orientación práctica y su simplicidad, aunque no está exento de deficiencias que deben abordarse.

1.8. Bergvall, J. and L. Svensson, "Risk analysis review" [57].

En la Investigación se realiza una comparación entre Attack trees (método de los investigadores), CRAMM, ISRAM, OCTAVE Allegro, COBRA, Mehari, Magerit y CORAS, clasificándose estas metodologías de Análisis de Riesgos en base a un conjunto de características, que incluyen: Recursos necesarios, número de problemas identificados, tipo de AR (Cuantitativo y Cualitativo) y si tiene soporte para la toma de decisiones (es decir, que establezcan claramente qué acciones son necesarias para mitigar los riesgos).

En las conclusiones de la investigación se destaca que la mayoría de los métodos evaluados carecían de soporte a la decisión, es decir, no especificaban de forma clara las acciones que debían implementarse para mitigar los riesgos, en particular CRAMM, ISRAM, MEHARI y MAGERIT. Esto dio lugar a que cada una de las compañías que formó parte de la investigación (Ericsson, SAAB, Tage Rejmes Bil AB, etc.)

había implementado el análisis de riesgos con métodos diferentes y no unificados.

También se identifica la necesidad de elevados conocimientos para implantar métodos como CRAMM, ISRAM, MEHARI y CORAS.

1.9. Abbass, W., A. Baina, and M. Bellafkih. "Using EBIOS for risk management in critical information infrastructure" [58].

En la Investigación podemos ver la utilización de la metodología EBIOS para la gestión del riesgo dentro de la Infraestructuras Críticas, y dentro del artículo se muestra una comparativa de diferentes metodologías de riesgos. En concreto, se centra en la comparación de OCTAVE, EBIOS, MEHARI, CRAMM y CORAS, analizando características como la fecha de creación, soporte, herramientas, monitorización del riesgo, metodologías de análisis y documentación disponible de las mismas.

La principal conclusión que obtiene es que, a pesar del proceso estructurado, los resultados de los métodos de Análisis de Riesgos son en gran medida informales y no suelen ser suficientemente analíticos. Esta informalidad muestra una falta de automatización, razonamiento y trazabilidad del proceso de Análisis de Riesgos.

1.10. ENISA. "Inventory of Risk Management / Risk Assessment Methods" [59].

En [59] la Agencia Europea para la Ciberseguridad analiza las principales metodologías de Análisis de Riesgos que se utilizan dentro del Marco de la Unión Europea, mostrando sus principales características.

En particular se analizan las siguientes metodologías: Austrian IT Security Handbook, Cramm, Dutch A&K Analysis, Ebios, ISAMM, ISF Methods, ISO/IEC 13335-2, ISO/IEC 17799, ISO/IEC 27001, IT-Grundschutz, Magerit, Marion, Mehari, MIGRA, Octave, RiskSafe Assessment y NIST SP800-30.

Para cada una de ellas se analizan las siguientes dimensiones: Información general, Nivel de referencia del producto, Tarjeta de identidad del producto, Alcance y Características desde el punto de vista de los usuarios.

1.11. Pan, L. and A. Tomlinson, "A systematic review of information security risk assessment" [60].

En [60] se hace una revisión de las publicaciones científicas asociadas al análisis de riesgos, pero centradas en las metodologías NIST SP800-30, ISO27005/ISO27001, OCTAVE e ISRAM. Determina que estos mecanismos de análisis de riesgos tienen importantes carencias, como por ejemplo que no pueden abordar algunos factores importantes, como son la fuga de activos, los activos creados por los usuarios y el conocimiento crítico. También analiza las desventajas de estos modelos a la hora de obtener puntuaciones de riesgo objetivas. Por último plantean la necesidad de investigar los ISRA desde la perspectiva económica, como el análisis de coste-beneficio y la teoría de juegos.

1.12. Shameli-Sendi, A., R. Aghababaei-Barzegar, and M. Cheriet, "Taxonomy of information security risk assessment (ISRA)" [61]

En esta investigación los autores presentan una taxonomía para la evaluación de riesgos de seguridad, construida a partir del análisis de 125 artículos publicados entre 1995 y 2014.

Destacan que uno de los mayores problemas que han encontrado es que, aunque se investiga mucho sobre el riesgo, la mayoría de los modelos propuestos están basados en taxonomías antiguas, dejando a un lado la necesidad de considerar nuevos criterios relacionados con el cambio de tecnologías y del nivel de conocimiento de los atacantes.

Analiza algunas de las principales metodologías de riesgos, como CRAMM, CORAS, OCTAVE, MAGERIT, Microsoft Security Risk Management Guide, MEHARI, ISO27005, NIST SP800-30 y un grupo de proyectos de investigación en riesgos.

Sobre ellos, evalúa la perspectiva con respecto al riesgo, las técnicas utilizadas, valoración, entradas y salidas, valoración de recursos, medición de riesgo y fases de riesgo.

1.13. Ruan, K. – "Introducing cybernomics: A unifying economic framework for measuring cyber risk". [62]

En esta investigación el autor analiza diferentes modelos de riesgos como ITIL, COBIT, ISO/IEC 27005:2011, ISF (SPRINT y SARA), OCTAVE, NIST 800-53, NIST 800-37, ISO/IEC 31000:2009, COBRA, CORAS, BPIRM, ISRAM, CRAMM, BSI Guide y CORA, y sobre ellos analiza las problemáticas y limitaciones existentes que se resumen en:

- Los métodos actuales se centran en la tecnología y dejan de lado otros factores como las personas, procesos y factores de riesgo socioeconómicos.
- Las estimaciones más precisas a menudo requieren acceso a datos y conocimiento que una sola entidad no posee.
- Los marcos de evaluación de riesgos predominantes como ISO / IEC 27002 están estructurados en función de dominios de control de seguridad, que no son lo suficientemente efectivos para evaluar la preparación de una entidad hacia un conjunto de escenarios de pérdida de alto riesgo desarrollados en torno a activos digitales críticos.
- La proliferación de metodologías de evaluación de riesgos en ausencia de un punto de referencia común ha causado inconsistencias indeseables en la medición del riesgo cibernético.

De esta forma, es necesario plantear otros puntos de vista diferentes para el análisis de riesgos que tenga en cuenta riesgos externos, mayor objetividad, etc.

1.14. Madhavan, K. and R. ManickaChezian, "International Journal of Engineering Sciences & Research Technology a Study on Information Security and Risk Management in IT Organizations". [63]

El enfoque del presente estudio fue analizar 14 metodologías de análisis de riesgos en detalle y reconocer algunos criterios comunes, con el objetivo de ayudar a las

empresas en la toma de decisiones de cuál puede ser más adecuada para su negocio.

Las metodologías elegidas fueron: IT Grundschutz (BSI 2008), "Standard of Good Practice" (ISF 2005), CRAMM, OCTAVE-O, OCTAVE-A, COBIT, CORAS, ISM3, NIST SP 800-30, ITIL, EBIOS, MEHARI, GAISP y LRAM.

1.15. Radanliev, P., et al., "Economic impact of IoT cyber risk-analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance". [64]

En esta investigación se realiza un análisis de 16 métodos de Análisis de Riesgos y su orientación y validez para los sistemas IoT.

Los métodos analizados fueron: ITIL, COBIT, ISO27005:2011, ISF (SPRINT y SARA), OCTAVE, NIST SP 800-37, NIST SP 800-53, ISO/IEC 31000:2009, COBRA, CORAS, BPIRM, ISRAM, CRAMM, BSI Guide, BS7799 y CORA.

Los resultados de esta investigación conducen a la conclusión de que existen muchos desafíos para comprender los tipos y la naturaleza del riesgo cibernético y sus dependencias / interacciones orientadas a los IoT.

Por otro lado, el estudio concluye que las metodologías clásicas no se adaptan a los riesgos IoT y que es necesario desarrollar nuevas métricas y métodos de valoración de riesgos.

1.16. Acevedo, N. and C. Satizábal. "Risk management and prevention methodologies: a comparison". [65, 66]

Los investigadores analizan algunas metodologías de gestión y prevención de riesgos (OCTAVE, CORAS, AS/NZS 4360:1999, IS/IEC 27005, CRAMM, MAGERIT, 2 versiones de NIST y BID), realizando una comparación de las etapas que incluyen y determinando si tienen en cuenta el factor humano en el análisis y tratamiento de riesgos.

Entre las conclusiones que obtienen es que solo el 42.85% de las metodologías de gestión de riesgos estudiadas incluyen el factor humano, siendo el NIST la metodología más completa, pero debe completarse con otras metodologías como la BID (Banco Interamericano de Desarrollo - Diagnóstico, prevención y control de la corrupción en los programas de metodología de seguridad cívica).

De las siete metodologías de gestión de riesgos estudiadas, sólo tres consideran el factor humano (Octave, Magerit y la metodología de gestión de riesgos del NIST) y cuatro no lo consideran de manera explícita (CORAS, la metodología del estándar australiano, la NTC-ISO/IEC 27005 y CRAMM).

1.17. Devia, G.A.V. and C.J. Pardo, "Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT". [67]

La investigación destaca la importancia cada vez mayor del análisis de riesgos, y por ello presenta la armonización de modelos de riesgos de TI (e.g., CRAMM, COBIT, EBIOS, ITIL V3 MAGERIT, OCTAVE, RISK IT) y algunas normas enfocadas en brindar soporte a los riesgos (e.g., ISO/IEC 27000, ISO/IEC 27005, ISO/IEC 31010, AS/NZS ISO 31000, BS 7799-3:2006, y UNE 71504:2008), realizando un análisis comparativo, de alto y bajo nivel, que permite conocer las características más comunes y representativas de cada uno de ellos.

El análisis realizado permitió evidenciar que la mayoría de las normas y modelos tienen puntos en común, aunque algunas normas presentan procesos más detallados, con un nivel más profundo que otros modelos. Asimismo, se observó que hay normas y modelos con similitudes en la definición de sus procesos, tales como actividades similares entre sí. Por otra parte, también se encontraron algunas actividades que complementaban y mejoraban las descripciones de otras actividades, dando como resultado la característica en la que un modelo es capaz de soportar a otro modelo.

La gestión de riesgos permite evitar el fracaso de proyectos de desarrollo de software, estimulando la terminación del mismo de modo que se incrementa la calidad en los proyectos entregados, reduciendo costos y cumpliendo con las necesidades del cliente, lo que impacta positivamente en su satisfacción. Una buena gestión de riesgos tiene como habilidad entregar a tiempo los productos esperados a partir de las metas que se plantearon y con el cronograma de actividades establecido.

1.18. Alhajri, R.M., et al. "Dynamic Interpretation Approaches for Information Security Risk Assessment". [68]

El investigador plantea la necesidad de analizar los modelos de riesgos para prever los riesgos probables y llegar a las contramedidas apropiadas, y para ello analiza modelos como OCTAVE, CRAMM, FRAP e ISRAM, además de algunos modelos de investigación.

Las conclusiones que presenta determinan que el factor determinante básico es que el enfoque de evaluación de riesgos más importante es el que incorpora las tres dimensiones de seguridad: confidencialidad, integridad y accesibilidad.

1.19. Korman, M., et al. "Overview of enterprise information needs in information security risk assessment". [69].

Según los investigadores, los métodos para la evaluación de riesgos en seguridad de la información sugieren a los usuarios recopilar y considerar conjuntos de información de entrada, a menudo notablemente diferentes, tanto en tipo como en tamaño, lo que suele hacer que los análisis de riesgos de las mismas compañías, sobre el mismo alcance y en igual de circunstancias sean diferentes.

Para explorar estas diferencias, este estudio compara doce métodos de análisis de riesgos (IT-Grundschutz, TRA-1, TRITF, CORAS, ISO/IEC27005, MEHARI, TSRMG, MAGERIT, OCTAVE, MG-3, NIST RMF, HMG IA), y se analiza cómo sus sugerencias de entrada se corresponden con los conceptos de ArchiMate, un lenguaje de modelado ampliamente utilizado para la arquitectura empresarial.

Como conclusión, determinan que varios factores podrían explicar las diferencias en las sugerencias de entrada entre los métodos. Por un lado, proporcionar sugerencias detalladas

puede beneficiar a los analistas, ya que identificar información que sea verdaderamente relevante para una evaluación de riesgos es una tarea difícil que merece una visión considerable y un pensamiento amplio. Por otro lado, sugerencias muy detalladas podrían sesgar cognitivamente a los analistas para seguir un esquema establecido que no sea necesariamente completo o equilibrado, lo que podría llevar a pasar por alto elementos de relevancia que de otro modo probablemente se identificarían. Esto último podría pesar especialmente a la luz de los constantes cambios de tecnologías y amenazas. Una alternativa podría ser invitar a los analistas a que identifiquen qué es lo más relevante para el objetivo específico de la evaluación en el día que se ésta realice.

1.20. Fulford, J.E., "What Factors Influence Companies' Successful Implementations of Technology Risk Management Systems". [70]

El artículo critica el poco éxito empresarial que tienen las metodologías de análisis de riesgos desarrolladas puramente en el ámbito académico, que no han sido aplicadas en la práctica. Para ello analiza algunas metodologías como OCTAVE, CRAMM, ISO27001, ISRAM, FAIR, CORAS, así como otras metodologías que están en fase de investigación.

Las conclusiones extraídas de las comparaciones de las metodologías y modelos de gestión de riesgos tecnológicos investigados durante la revisión de la literatura incluyeron:

- Algunos métodos de análisis de riesgos (como CORAS y FAIR) utilizan aspectos de diseño de otras metodologías de riesgo y son muy complementarios con las metodologías en uso.
- Los profesionales han desarrollado modelos que típicamente incluyen métodos cuantitativos, pero estos generalmente carecen de un método matemático componente de análisis, como un modelo estadístico, lo que limita la capacidad de esos modelos para determinar las relaciones e impactos de eventos de riesgo operacional de seguridad y tecnología para las operaciones de TI.
- Los modelos profesionales generalmente se construyen para usuarios experimentados con amplios conocimientos de dominio.

1.21. Chen, F., "An Investigation and Evaluation of Risk Assessment Methods in Information systems". [71]

Los investigadores realizan una revisión de diferentes métodos de análisis de riesgos y de algunas dimensiones, y presentan un marco de trabajo para ayudar a las empresas a elegir el método que más se adapta a sus circunstancias.

Entre los métodos elegidos para el análisis están: OCTAVE, CORAS, CORA, COBRA, Risk Watch, FRAP, COSO ERM y @Risk. Para el análisis posterior, no se tendrá en cuenta ni Risk Watch, ni @Risk, al ser estos herramientas para análisis de riesgos, y no metodologías orientadas al riesgo TIC.

Dentro de las características los investigadores analizan: el objetivo, alcance, flexibilidad, alineamiento con otras normas, precio, tipología, tiempo de implantación, factor humano y usabilidad.

1.22. Pan, L., "Application of a Financial Quantitative Risk Model to Information Security Risk Assessment". [72]

Los investigadores destacan que muchas organizaciones no pueden identificar sus activos, y mucho menos calcular el riesgo asociado. Esta investigación argumenta que se necesita un nuevo enfoque para la evaluación de riesgos y presenta una alternativa basada en modelos financieros.

Platean también que los estándares de gestión de seguridad de la información son esenciales para la seguridad de la información, ya que permiten contar con un marco completo para asegurar los datos en un nivel apropiado.

Se examinaron cuatro estándares ISRA comúnmente utilizados: OCTAVE, FAIR, ISO 27005 y NIST SP800-30. FAIR presta mayor atención a los métodos de cálculo del análisis de riesgos, mientras que la ISO 27005 prefiere proporcionar un marco completo para la evaluación de riesgos.

Sin embargo, el primer inconveniente de estos ISRA es que son difíciles de ejecutar en periodos cortos, o con seguimientos diario. Son procesos costosos y que requieren rellenar entrevistas y cuestionarios, seguidos por expertos. El segundo problema es que son demasiado genéricos para todos los riesgos de seguridad de la información.

1.23. Nurse, J.R., S. Creese, and D. De Roure, "Security risk assessment in Internet of Things systems". [73]

Según los investigadores, los sistemas clásicos de protección ya no son adecuados para los entornos IoT, ya que a medida que aumenta la complejidad, la omnipresencia y la automatización de los sistemas tecnológicos, particularmente con el Internet de las cosas (IoT), existe un fuerte argumento sobre la necesidad de nuevos enfoques para evaluar el riesgo y generar confianza. Estos riesgos podrían estar relacionados con los altos grados de conectividad presentes o el acoplamiento de sistemas digitales, ciberfísicos y sociales, por lo que es necesario analizar los modelos existentes y plantear nuevas alternativas que consideren la dinámica y la singularidad de IoT, pero manteniendo el rigor de las mejores prácticas en la evaluación de riesgos.

Para ello analizan métodos como NIST SP800-30, ISO/IEC 27001, OCTAVE y su orientación hacia el IoT.

1.24. Agrawal, V., "A Comparative Study on Information Security Risk Analysis Methods". [74]

El investigador destaca que el análisis de riesgos es una parte integral de la práctica de gestión y un elemento esencial del buen gobierno corporativo. Hay muchos métodos de análisis de riesgos disponibles en la actualidad, y es una tarea tediosa para una organización (particularmente una pequeña y mediana empresa) elegir el método adecuado. Otro problema, es que aunque hay muchos métodos y herramientas disponibles en este dominio, existen muy pocos inventarios que estén estructurados de acuerdo con un conjunto de propiedades comunes.

Por lo tanto el investigador analiza cuatro métodos de análisis de riesgos y los compara a partir de un conjunto de atributos genéricos como: entrada, resultado, propósito, esfuerzo, escalabilidad, metodología, etc.

Los métodos analizados son: CORAS, CIRA, ISRAM e IS (IS Risk Analysis Based on Business Model).

1.25. Wangen, G.B., "Cyber Security Risk Assessment Practices: Core Unified Risk Framework". [75].

Los investigadores consideran que las evaluaciones de riesgos permiten reducir la incertidumbre con respecto a eventos futuros con el fin de tomar las mejores decisiones posibles y controlar el riesgo. En la industria, el objetivo es encontrar el equilibrio adecuado en la toma de riesgos en relación con el apetito y la tolerancia al riesgo de la organización. Demasiados controles de seguridad inhibirán la funcionalidad del negocio, y lo contrario conducirá a una exposición inaceptable. Por lo tanto, la investigación aborda varios aspectos de las prácticas de evaluación y gestión de riesgos de seguridad informática y cibernética (ISRA) y contribuye a nuevos problemas de investigación, métodos, modelos y conocimiento dentro de la disciplina.

Entre los desafíos dentro del campo de ISRM destacan la necesidad de elegir entre diferentes métodos ISRA sin una premisa clara, y con una literatura sobre el tema de los problemas en ISRM bastante dispersa.

El estudio encontró que los principales problemas de ISRM según los expertos estaban en la comunicación de riesgos, las medidas de seguridad y el retorno de las inversiones. Mientras que para la evaluación y el análisis de riesgos, encontraron que los problemas clave son la aplicación de métodos cuantitativos y cualitativos, la necesidad de experiencia y la evaluación de activos.

La investigación propone además combinar los métodos cuantitativos (estadísticos) y cualitativos (basado en el conocimiento subjetivo) para poder modelar el ataque y estimar el riesgo. El enfoque se centra en estimaciones cualitativas de activos, vulnerabilidades, amenazas, controles y resultados asociados, junto con un análisis estadístico del riesgo.

Los modelos de riesgos analizados son: CIRA, CORAS, CRAMM, FAIR, NSMROS, OCTAVE-A, ISO27005, NIST SP800-30, Risk IT, RAIS y CRDF.

1.26. MUKAMA, J., "Risk Analysis as a Security Metric for Industrial Control Systems". [76].

Según los investigadores, a medida que avanza el tiempo y la tecnología, las personas se vuelven más dependientes de los servicios proporcionados por los Sistemas de Control Industrial (ICS). Utilizados principalmente en las industrias de infraestructura crítica, los ICS han realizado y habilitado cientos de servicios esenciales para las personas, el público y las organizaciones a diario.

Para mitigar los riesgos que pueden surgir debido a las vulnerabilidades introducidas en el sistema, los investigadores realizaron una comprensión más profunda de los diferentes ICS, revisaron una serie de enfoques de análisis de riesgos existentes y los categorizamos en términos de su objetivo general, si son cualitativos o enfoques cuantitativos, las etapas de la gestión de riesgos abordados y el alcance en términos de los problemas que abordaron.

Finalmente concluyeron que no existe ningún método de riesgos que sea totalmente adecuado a los ICS, pero que se pueden utilizar NIST y CORAS como enfoques subyacentes para desarrollar un Marco de Análisis de Riesgo Modificado para sistemas ICS (MRAF-ICS). Este marco asigna pesos a todos los activos del sistema para enfatizar la importancia / criticidad del activo en el sistema general. Utiliza el enfoque de modelado de amenazas, FMEA y HAZOP para identificar exhaustivamente las amenazas, los peligros y las vulnerabilidades en el sistema.

Para la investigación se tuvieron en cuenta los siguientes métodos: CRAMM, CORAS, OCTAVE, MEHARI, CSMRA, FMEA&FMECA, HAZOP, HMRM-CI, NIST SP800-30 y ARMS.

1.27. Oppliger, R., G. Pernul, and S. Katsikas, "New Frontiers: Assessing and Managing Security Risks". [77].

Como hemos visto, existen múltiples investigaciones que destacan que el análisis cuantitativo de riesgos, como se requiere para la evaluación y la gestión de riesgos, funciona mejor en la teoría que en la práctica, y que se necesitan algunos enfoques alternativos [78].

Basado en ese problema se planteó este artículo, y otros asociados, que permitió a los autores realizar un estudio sobre la gestión de riesgos en general, así como sobre el valor intrínseco de la evaluación de riesgos. La mayoría de los investigadores que participaron estuvieron de acuerdo con la hipótesis inicial: los enfoques actualmente implementados para la evaluación de riesgos no funcionan en la práctica y son difíciles o imposibles de aplicar en el campo. Hay una serie de razones para esto, que se pueden ver en el artículo de la IEEE Security & Privacy [78] y que se pueden resumen en que el uso de la teoría de probabilidad y las estadísticas en un campo en constante cambio como la ciberseguridad no tiene sentido.

Tambien analiza la comparación de métodos de hace Wangen [13] sobre OCTAVE, ISO/IEC 27005:2011 y NSMROS. Oppliger sostiene que la elección de un método sobre otro influye enormemente en el proceso de evaluación resultante.

Otra investigación analizada en el artículo es la de Burnap [79], que plantea el problema de que los métodos actuales de análisis de riesgos están planteados para sistemas independientes, pero los sistemas actuales son interdependientes y complejos. Lo que se requiere para manejar con éxito tales sistemas desde una perspectiva de evaluación de riesgos actualmente no se comprende bien.

Finalmente, analiza las investigaciones de Rossebo [80, 81] el cual presenta una nueva propuesta de análisis de riesgos diseñada para sistemas IoT, que tiene una aplicabilidad mucho más amplia y que puede motivar más investigaciones en este área. Al establecer un conjunto de requisitos para comparar los métodos de evaluación de riesgos existentes para el sector energético, los autores pudieron evaluar los métodos existentes, lo que les permitió identificar la necesidad de un cuarto método, la Metodología de Gestión de Riesgos SEGRID (SRMM), que podría proporcionar un marco de gestión de riesgos para sistema IoT.

V. ANÁLISIS DE RESULTADOS.

En esta sección analizaremos los resultados obtenidos y catalogaremos las características de cada una de las metodologías, estándares y guías asociadas al Análisis de Riesgos que hemos encontrado.

En total se han analizado 27 artículos científicos del periodo 2014-2019, que han permitido identificar 40 métodos, guías y estándares clásicos asociados al Análisis de Riesgos TIC y a nuevos aspectos específicos como el IoT, Smart Grid o ICS, que podríamos considerar la evolución futura de este tipo de sistemas.

En la Tabla 1 podemos ver los 40 modelos identificados durante la revisión sistemática, junto con la organización, país de origen y el número de artículos donde ha aparecido.

Modelo Análisis de Riesgos	Origen	Organización	País	Nº Apariciones Investigaciones Relacionadas
ARMS (Automated Risk Management System)	Gubernamental	Defence R&D Canada – Ottawa	Canadá	1 [76]
AS/NZS 4360 / ISO31000:2009 (incluye las guías HB)	Gubernamental	Council of Standards Australia	Australia y Nueva Zelanda	4 [64-67]
Austrian IT Security Handbook (Manual austriaco de seguridad informática)	Gubernamental	Bundeskanzleramt (Cancillería federal austríaca)	Austria	1 [59]
BPIRM (Business Process: Information Risk Management)	Empresarial	KPMG	Reino Unido	2 [62, 64]
CIRA (Conflicting Incentives Risk Analysis)	Universidad	Desarrollo como Tesis Doctoral por Lisa Rajbhandari, bajo el nombre de "Conflicting Incentives" as an Alternative Notion of Risk.	Noruega	5 [51-53, 74, 75]
COBRA (The Consultative, Objective and Bi-functional Risk Analysis)	Empresarial	C & A Systems Security Ltd.	Reino Unido	4 [57, 62, 64, 71]
CORA (Cost-Of-Risk Analysis)	Empresarial	International Security Security, Lcd.	Estados Unidos	3 [62, 64, 71]
CORAS (Construct a platform for Risk Analyisis of Security Critical Systems)	Empresarial	C&A Systems Security LTD. Information Society Technologies (IST) Programme (Commission of the European Communities, Directorate-General Information Society)	Reino Unido	19 [50-54, 57, 58, 61-66, 69-71, 74-76]
COSO ERM (*Enterprise Risk Management — Integrated Framework)*	Organización	Committee of Sponsoring Organizations of the Treadway Commission	Estados Unidos	1 [71]
CRAMM (Central computer and Telecommunication Agency Risk Analysis and Management Method)	Gubernamental	CCTA británica (Agencia Central de Comunicaciones y Telecomunicaciones) Insight Consulting	Reino Unido	19 [50, 52-59, 61-67, 70, 75, 76]
Dutch A&K Analysis (Análisis holandés A&K)	Gubernamental	Ministerio holandés de asuntos internos	Países Bajos	1 [59]
EBIOS (Expression of Needs and Identification of Security Objectives)	Gubernamental	ANSSI (Agence nationale de la sécurité des systèmes d'information) DCSSI (Dirección Central de Seguridad de los Sistemas de información)	Francia	6 [50, 54, 58, 59, 63, 67]
FAIR (Factor Analysis of Information Risk)	Empresarial	FAIR Institute	Estados Unidos	6 [51-53, 70, 72, 75]
FRAP (Facilitated Risk Assessment Process)	Universitario	Peltier and Associates	Estados Unidos	3 [56, 68, 71]
GAISP (Generally Accepted Information Security Principles)	Organización	Information Systems Security Association International (ISSA)	Estados Unidos	1 [63]
HMG-IA (HMG IA Standard No. 1 Technical Risk Assessment)	Gubernamental	National Technical Authority for Information Assurance	Reino Unido	1 [69]
IS RA on BM (IS Risk Analysis Based On Business Model)	Gubernamental	Korea Advances Institute of Science and Technology	Corea	1 [74]
ISAMM (Information Security Assessment and Monitoring Method)	Empresarial	Telindus N.V	Bélgica	1 [59]
ISF Method: "Standard of good Practice", IRAM, IRAM2, SARA, SPRINT , FIRM	Organización	ISF (Information Security Forum) ISF asociación internacional de más de 260 empresas líderes y organizaciones del sector público	Reino Unido	4 [59, 62-64]
ISO/IEC Baselines (incluye ISO/IEC	Organización	ISO	Internacional	16 [52, 53, 59-62, 64-67,

27001 - BS7799-2:2002, ISO/IEC: 27002 - ISO/IEC 17799:2005, ISO/IEC 27005 - ISO/IEC 13335-2/3, BS 7799-3:2006)			(organización con sede en Suiza)		69, 70, 72, 73, 75, 77]
ISRAM (Information Security Risk Analysis Method)	Universidad	National Research Institute of Electronics & Cryptology & TurkeybGebze Institute of Technology	Turquia	8	[51, 57, 60, 62, 64, 68, 70, 74]
IT-Grundschutz (IT Baseline Protection Manual)/BSI Standard 100-2-3	Gubernamental	Oficina Federal de Seguridad de la Información (BSI)	Alemania	6	[50, 59, 62-64, 69]
ITIL (The IT Infraestructura Library)	Organización	Office of Government Commerce (OGC)	Reino Unido	4	[62-64, 67]
LRAM (Livermore Risk Analyisis Methodology)	Universidad	Lawrence Livermore National Laboratory (University of California)	Estados Unidos	1	[63]
MAGERIT (Methodology for Information Systems Risk Analysis and Management)	Gubernamental	Ministerio de Administraciones Públicas (Ministerio de Administraciones Públicas de España)	España	12	[48-50, 54, 55, 57, 59, 61, 65-67, 69]
MARION (Metodología de análisis de información y optimización de datos por Niveau)	Gubernamental	CLUSIF	Francia	1	[59]
MCRDF (Microsoft Cloud Risk Decision Framework)	Empresarial	Microsoft	Estados Unidos	3	[52, 53, 75]
MEHARI (Me´thode Harmonise´e d'Analyse de Risques—Harmonised Risk Analysis Method)	Organización	CLUSIF (Francia) transmitido por CLUSIQ (Canadá)	Francia	10	[49, 50, 54, 55, 57-59, 61, 63, 69]
MG-2 (A Guide to Security Risk Management for Information Technology Systems) & MG-3 (A Guide to Risk Assessment and Safeguard Selection for Information Technology Systems)	Organización	CSE (Communications Security Establishment)	Canadá	1	[69]
Microsoft's Security Risk Management Guide	Empresarial	Microsoft	Estados Unidos	2	[61, 69]
MIGRA (Metodologia Integrata per la Gestione del Rischio Aziendale) - (anteriormente se denominaba Defender)	Empresarial	AMTC / Elsag Datamat S.p.A	Italia	1	[59]
NIST Family: NIST CSF / NIST RMF / NIST SP800-30 / NIST SP800 – 37 / NIST SP800–39 / NIST SP800 - 53	Organización	Instituto Nacional de Estándares y Tecnología (NIST)	Estados Unidos	20	[50-56, 59-66, 69, 72, 73, 75, 76]
NSMROS (Norwegian National Security Authority Risk and Vulnerability Assessment)	Gubernamental	Norwegian Security Act	Noruega	4	[52, 53, 75, 77]
OCTAVE (The Operationally Critical Threat, Asset, and Vulnerability EvaluationSM)/ Octave-S / Octave-A (Allegro)	Universidad	Universidad Carnegie Mellon, SEI (Instituto de Ingeniería de Software)	Estados Unidos	29	[48-73, 75-77]
RAIS (Risk Assessment of Information Systems)	Gubernamental	Norwegian Data Protection Authority's (Datatilsynet)	Noruega	3	[52, 53, 75]
RaMEX (Risk Analysis and Management expert system)	Universidad	University of Birminghan	Reino Unido	1	[51]
Risk IT - ISACA / COBIT Risk (Control Objectives for Information and Related Technology)	Empresarial	ISACA	Estados Unidos	8	[52, 53, 62-64, 67, 69, 75]
RiskSafe Assessment	Empresarial	Platinum Squared Ltd	Reino Unido	2	[50, 59]
SRMM (SEGRID Risk Management Methodology) - SEGRID (Security for Smart Electricity GRIDs)	Gubernamental	ETSI (The European Telecommunications Standards Institute)	UE	1	[77]
TRA (Threat and Risk Assessment Methodology) & HTRA (Harmonized Threat and Risk Assessment Methodology)	Gubernamental	Communications Security Establishment Canada (CSEC) and the Royal Canadian Mounted Police (RCMP)	Canada	2	[50, 69]

Tabla 1. Modelos identificados durante la revisión sistemática

A continuación, vamos a extraer de forma resumida las principales necesidades y problemas identificados durante la revisión sistemática:

- Controles: Los controles deben formar parte del Análisis de Riesgo, y no sólo de la Gestión del Riesgo: Gran parte de las metodologías consideran que los controles son ajenos al análisis de riesgos, y no lo consideran hasta la fase de gestión de riesgos [75].
- Capacidad Sectorial: Importancia de tener la capacidad en las metodologías de adaptarse a sectores específicos [48].
- Estructuras comunes de riesgo que soporten diferentes metodologías: Ante la diversidad de marcos de trabajo, ser capaces de crear una estructura común que pueda unificar las diferentes metodologías de riesgos [71].
- Los sistemas de riesgos son el núcleo de los sistemas de Gestión de Seguridad [72].
- La simplicidad y la orientación práctica es importante para las empresas [56-58, 72, 75, 77].
- Los métodos deben tener mecanismos de soporte a la toma de decisiones [57].
- Los resultados del análisis de riesgos son informales y poco analíticos, obteniendo puntuaciones de riesgo subjetivas [58, 60].
- Necesidad de contar con orientaciones y perspectivas económicas del análisis de riesgos [60].
- Necesidad de taxonomías de riesgos actualizadas y adecuadas a las nuevas tecnologías (ICSs, IoT, Smart Grids, …) [61, 64, 73, 76].
- Se dejan de lado perspectivas como personas, procesos y factores de riesgo socioeconómicos [61, 65, 66].
- Necesidad de contar con escenarios de riesgos [61].
- Herramientas: Necesidad de contar con herramientas que faciliten el cumplimiento de las metodologías [71].
- Necesidad de poder contar con mecanismos de selección de metodologías de análisis de riesgos según la compañía [69].
- Necesidad de contar con métricas adecuadas [72].
- Necesidad de que las metodologías académicas se validen en entornos reales [70].
- Necesidad de metodologías adaptadas a las PYMES [74].
- Necesidad de catálogos de elementos, estructurados y que puedan compartirse entre las diferentes metodologías [74].

VI. Conclusiones.

En este artículo se han analizado diferentes metodologías, procesos y estándares de análisis de riesgos TIC (ISRA), extrayendo más de 40 modelos que suelen referenciar y analizar los investigadores actualmente.

De los modelos encontrados, se han identificados unas 20 carencias de relevancia que destacan los investigadores sobre los modelos actuales.

Estás carencias se complementan con otros aspectos relevantes que hemos encontrado al analizar los propios modelos de riesgo, entre las que podemos destacar:

- Sorprende comprobar que metodologías muy referenciadas y recomendadas como CRAMM ya no tienen páginas web accesibles, y que gran parte de la información facilitada por ENISA sobre las metodologías de análisis de riesgos está ya obsoleta.
- Existen muchos modelos de los analizados que no han sido actualizados en los últimos 10 años, y aun así se siguen utilizando.
- Se han identificado tímidas propuestas para modernizar los análisis de riesgos ante los nuevos retos como el Cloud, IoT, ICSs, etc. Sin embargo, hasta ahora han tenido poco recorrido.
- La mayoría de los modelos encontrados tienen una complejidad alta o media de implantación, no considerándose adecuados para PYMES.
- La mayoría de los modelos se orientan a cubrir las tres dimensiones base (confidencialidad, integridad y disponibilidad), dejando de lado el resto de criterios.

Podemos concluir por lo tanto, que ahora mismo existen importantes carencias dentro de los modelos de Análisis de Riesgos existentes que deben ser afrontadas, desarrollando nuevas metodologías que permitan adaptarse a las circunstancias cambiantes de las TIC.

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] Le Grand, G. and E. Adar. *White cyber knight–a Risk Assessment tool for network resilience evaluation*. in *the proceedings of the International Workshop on Complex Network and Infrastructure Protection (CNIP'06), Rome*. 2006.

[2] 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.

[3] 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).

[4] 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.

[5] 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.

[6] Eloff, J. and M. Eloff, *Information Security Management - A New Paradigm.* Annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology SAICSIT´03, 2003: p. 130-136.

[7] Steve, E., *An Introduction to information systems risk management*. SANS Institute InfoSec Reading Room. **16**: p. 2011.

[8] Bača, M. and F. Varaždin, *The risk assessment of information system security*. Fakultet organizacije i informatike, Sveučilište u Zagrebu.< dostupno na http://cuc. carnet. hr/cuc2004/program/radovi/a5_baca/a5_full. pdf>,[očitano 07.10. 2010], 2004.

[9] Restrepo, L.O. and F.J.V. Duque, *Gestión de riesgos en eTOM. Un análisis comparativo con los estándares de riesgo corporativo*. Revista Logos, Ciencia & Tecnología, 2017. **9**(1): p. 85-99.

[10] Ortiz Restrepo, L., V. Duque, and F. Javier, *Gestión de riesgos en eTOM. Un análisis comparativo con los estándares de riesgo corporativo.* Revista Logos Ciencia & Tecnología, 2017. **9**(1): p. 85-99.

[11] Chen, T.M., *Information security and risk management*, in *Encyclopedia of Multimedia Technology and Networking, Second Edition*2009, IGI Global. p. 668-674.

[12] Magerit_V2, *Methodology for Information Systems Risk Analysis and Management (MAGERIT version 2)*, 2005, Ministerio de Administraciones Públicas (Spain).

[13] Wangen, G., *Information security risk assessment: a method comparison.* Computer, 2017. **50**(4): p. 52-61.

[14] Fakrane, C. and B. Regragui. *Interactions and Comparison of It Risk Analysis Methods*. in *2018 4th International Conference on Cloud Computing Technologies and Applications (Cloudtech)*. 2018.

[15] Jeannot, F., *Méthodologies d'évaluation et gestion de risques en sécurité.* Montréal, Canada, Mai 2018, R518, v1.0, 2018.

[16] Benavides Sepúlveda, A.M. and C.A. Blandón Jaramillo, *Modelo de sistema de gestión de seguridad de la información basado en la norma NTC ISO/IEC 27001 para instituciones públicas de educación básica de la comuna Universidad de la ciudad de Pereira Alejandra.* 2017.

[17] Bornman, W.G., *Information security risk management: a holistic framework*, 2004, University of Johannesburg.

[18] Refsdal, A., B. Solhaug, and K. Stølen, *Cyber-risk management*, in *Cyber-Risk Management*2015, Springer. p. 33-47.

[19] Zudin, R., *Analysis of information risk management methods.* University of Jyväskylä, 2014.

[20] Carrillo Sánchez, J.P., *Guía y análisis de gestión de riesgos en la adquisición e implantación de equipamiento y servicios de tecnologías de información y comunicaciones para proyectos de alcance nacional*, 2012, Quito: EPN, 2012.

[21] Pacheco Pozo, D.C., *Propuesta de un plan de contingencia de TI para la empresa LOGICIEL*, 2016, Quito, 2016.

[22] Alcántara, M. and A. Melgar, *Risk management in information security: a systematic review.* Journal of Advances in Information Technology Vol, 2016. **7**(1).

[23] Shamala, P., et al., *Collective information structure model for information security risk assessment (ISRA).* Journal of Systems and Information Technology, 2015. **17**(2): p. 193-219.

[24] Ford, M., *IT Risk Management Systems Play a Key Role in Sustaining and Promoting Business Growth.* University of Westminster, MSc Information Security, London, England, 2014.

[25] Derakhshandeh, S. and N. Mikaeilvand, *New framework for comparing information security risk assessment methodologies.* Australian Journal of Basic and Applied Sciences, 2011. **5**(9): p. 160-166.

[26] Dehkhoda, D., *Combining IRAM2 with Cost-BenefitAnalysis for Risk Management: Creating a hybrid method with traditional and economic aspects*, 2018: Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology.

[27] Duricu, A., *Data Protection Impact Assessment (DPIA) and Risk Assessment in the context of the General Data Protection Regulation (GDPR)*, E.a.S.E. Department of Computer Science, Luleå University of Technology Editor 2019.

[28] Shamala, P. and R. Ahmad. *A proposed taxonomy of assets for information security risk assessment (ISRA)*. in *2014 4th World Congress on Information and Communication Technologies (WICT 2014)*. 2014. IEEE.

[29] Wangen, G. *An initial insight into information security risk assessment practices*. in *2016 Federated Conference on Computer Science and Information Systems (FedCSIS)*. 2016. IEEE.

[30] Haythorn, M., *Information Security Risk Assessment Methods, Frameworks and Guidelines.* East Carolina University, 2013.

[31] Pandey, S. and K. Mustafa, *Risk Assessment Framework (RAF).* International Journal of Advanced Research in C. Sc., 2010. **1**(3).

[32] Rea-Guaman, A., et al. *Systematic Review: Cybersecurity Risk Taxonomy*. in *International Conference on Software Process Improvement*. 2017. Springer.

[33] López, D., O. Pastor, and L.J.G. Villalba, *Concepto y Enfoques sobre el Análisis y la Gestión Dinámica del Riesgo en Sistemas de Información.* Actas de la XII Reunión Espanola de Criptologıa y Seguridad de la Información (RECSI 2012), Donostia-San Sebastián, Espana, 2012.

[34] Ganin, A.A., et al., *Multicriteria decision framework for cybersecurity risk assessment and management.* Risk Analysis, 2017.

[35] Smojver, S. *Selection of information security risk management method using analytic hierarchy process (ahp)*. in *Central European Conference on Information and Intelligent Systems*. 2011. Faculty of Organization and Informatics Varazdin.

[36] Beckers, K., et al., *ISMS-CORAS: A structured method for establishing an ISO 27001 compliant information security management system*, in *Engineering Secure Future Internet Services and Systems*2014, Springer. p. 315-344.

[37] Shedden, P., et al. *Towards a knowledge perspective in information security risk assessments–an illustrative case study*. in *Proceedings of the 20th Australasian Conference on Information Systems*. 2009.

[38] Rot, A. *Enterprise information technology security: risk management perspective*. in *Proceedings of the World Congress on Engineering and Computer Science*. 2009.

[39] Saripalli, P. and B. Walters. *Quirc: A quantitative impact and risk assessment framework for cloud security*. in *2010 IEEE 3rd international conference on cloud computing*. 2010. Ieee.

[40] Li, S., et al., *An improved information security risk assessments method for cyber-physical-social computing and networking.* IEEE Access, 2018. **6**: p. 10311-10319.

[41] Sicari, S., et al., *A risk assessment methodology for the Internet of Things.* Computer Communications, 2018. **129**: p. 67-79.

[42] Kitchenham, B., *Procedures for performing systematic reviews.* Keele, UK, Keele University, 2004. **33**(2004): p. 1-26.

[43] 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.

[44] Budgen, D. and P. Brereton. *Performing systematic literature reviews in software engineering*. in *Proceedings of the 28th international conference on Software engineering*. 2006. ACM.

[45] 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.

[46] Svatá, V. and M. Fleischmann, *IS/IT Risk Management in banking industry.* Acta oeconomica pragensia, 2011. **19**(3): p. 42-60.

[47] Mayer, N., P. Heymans, and R. Matulevicius. *Design of a Modelling Language for Information System Security Risk Managem*. 2007.

[48] García, F.Y.H. and L.M.L. Moreta. *Maturity Model for the Risk Analysis of Information Assets based on Methodologies MAGERIT, OCTAVE y MEHARI; focused on Shipping Companies*. in *2018 7th International Conference On Software Process Improvement (CIMPS)*. 2018. IEEE.

[49] Holguín García, F.Y., *Modelo de madurez para el análisis de riesgos de los activos de información basado en las metodologías MAGERIT, OCTAVE y MEHARI; con enfoque a empresas navieras*, 2018: Repositorio digital de la Universidad de Especialidades Espíritu Santo, UEES, Ecuador.

[50] Gritzalis, D., et al., *Exiting the Risk Assessment maze: A meta-survey.* ACM Computing Surveys (CSUR), 2018. **51**(1): p. 11.

[51] Mrksic Kovacevic, S., *Smart homes from a Risk Management perspective*, 2018, University of Stavanger, Norway.

[52] Wangen, G., C.V. Hallstensen, and E.A. Snekkenes, *A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework.* 2017.

[53] 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.

[54] Novoa, H.A. and C.R. Barrera, *Metodologías para el análisis de riesgos en los sgsi.* Publicaciones e Investigación, 2015. **9**: p. 73-86.

[55] Santonja Lillo, J., *Análisis y correlación entre probabilidad e impacto de los riesgos.* Repositorio Institucional de la Universidad de Alicante, España., 2019.

[56] Hashim, N.A., et al., *Risk Assessment Method for Insider Threats in Cyber Security: A Review.* Risk, 2018. **9**(11).
[57] Bergvall, J. and L. Svensson, *Risk analysis review*, 2015: Linköpings Universitet, Linköping, Sweden.
[58] Abbass, W., A. Baina, and M. Bellafkih. *Using EBIOS for risk management in critical information infrastructure*. in *2015 5th World Congress on Information and Communication Technologies (WICT)*. 2015. IEEE.
[59] ENISA_(e). *Inventory of Risk Management / Risk Assessment Methods*. 2019 02/08/2019].
[60] Pan, L. and A. Tomlinson, *A systematic review of information security risk assessment.* International Journal of Safety and Security Engineering, 2016. **6**(2): p. 270-281.
[61] Shameli-Sendi, A., R. Aghababaei-Barzegar, and M. Cheriet, *Taxonomy of information security risk assessment (ISRA).* Computers & Security, 2016. **57**: p. 14-30.
[62] Ruan, K., *Introducing cybernomics: A unifying economic framework for measuring cyber risk.* Computers & Security, 2017. **65**: p. 77-89.
[63] Madhavan, K. and R. ManickaChezian, *International Journal of Engineering Sciences & Research Technology a Study on Information Security and Risk Management in it Organizations.* International Journal OF Engineering Sciences & Research TEchnology (IJESRT). 2015.
[64] Radanliev, P., et al., *Economic impact of IoT cyber risk-analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance.* The Institution of Engineering and Technology (IET), England., 2018.
[65] Acevedo, N. and C. Satizábal, *Risk management and prevention methodologies: a comparison.* Sistemas & Telemática, 2016. **14**(36): p. 39-58.
[66] Satizábal, C., *Risk management and prevention methodologies: a comparison.* Sistemas & Telemática, vol.14, núm. 36, pp. 39-58, Universidad ICESI,Cali, Colombia, 2016.
[67] Devia, G.A.V. and C.J. Pardo, *Hacia un modelo para la gestión de riesgos de TI en MiPyMEs: MOGRIT.* Sistemas & Telemática, 2014. **12**(30): p. 35-48.
[68] Alhajri, R.M., et al. *Dynamic Interpretation Approaches for Information Security Risk Assessment*. in *2019 International Conference on Computer and Information Sciences (ICCIS)*. 2019. IEEE.
[69] Korman, M., et al. *Overview of enterprise information needs in information security risk assessment*. in *2014 IEEE 18th International Enterprise Distributed Object Computing Conference*. 2014. IEEE.
[70] Fulford, J.E., *What Factors Influence Companies' Successful Implementations of Technology Risk Management Systems?* Muma Business Review, 2017. **1**(13): p. 157-169.
[71] Chen, F., *An Investigation and Evaluation of Risk Assessment Methods in Information systems.* Chalmers Univ. Technol. Goteborg, 2015: p. 1-83.
[72] Pan, L., *Application of a Financial Quantitative Risk Model to Information Security Risk Assessment.* School of Mathematics and Information Security Royal Holloway, University London., 2018.
[73] Nurse, J.R., S. Creese, and D. De Roure, *Security risk assessment in Internet of Things systems.* IT Professional, 2017. **19**(5): p. 20-26.
[74] Agrawal, V., *A Comparative Study on Information Security Risk Analysis Methods.* Journal of Computers, 2017. **12**(1): p. 57-67.
[75] Wangen, G.B., *Cyber Security Risk Assessment Practices: Core Unified Risk Framework.* Norges teknisk-naturvitenskapelige U., 2017.
[76] MUKAMA, J., *Risk Analysis as a Security Metric for Industrial Control Systems.*, in *Master's thesis in Computer Systems and Networks.*2016, Chalmers University of Technology.
[77] Oppliger, R., G. Pernul, and S. Katsikas, *New Frontiers: Assessing and Managing Security Risks.* Computer, 2017. **50**(4): p. 48-51.
[78] Oppliger, R., *Quantitative risk analysis in information security management: a modern fairy tale.* IEEE Security & Privacy, 2015. **13**(6): p. 18-21.
[79] Burnap, P., et al., *Determining and Sharing Risk Data in Distributed Interdependent Systems.* Computer, 2017. **50**(4): p. 72-79.
[80] Rossebø, J.E., et al., *An enhanced risk-assessment methodology for smart grids.* Computer, 2017. **50**(4): p. 62-71.
[81] Rossebo, J.E., F. Fransen, and E. Luiijf. *Including threat actor capability and motivation in risk assessment for Smart GRIDs*. in *2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG)*. 2016. IEEE.

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).

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.

Victor Figueroa is Bachelor in Information Technology and MSc in Information Security. Is a Security Information Professor at the University of Siglo21 (Cordoba, Argentina). He is the Cybersecurity Director of Neuquen State (Argentina), working on development of Cibersecurity Information Policies, Risk Management and Incident Responses in Public Sector. He is currently a researcher in the field of Information Security Management Systems, and Information System Risk Analysis (ISRA).

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.