MEMORIAS

VIII CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMÁTICA

III Taller Iberoamericano de enseñanza e innovación educativa en seguridad de la información

CIBSI ECUADOR 2015

10-12 NOV 2015

UNIVERSIDAD DE LAS FUERZAS ARMADAS DEL ECUADOR - ESPE

Sangolquí, ECUADOR

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Con la Organización de

ESPE-Innovativa EMPRESA PÚBLICA

CRIPTORED

fundación IN-NOVA Centro de Innovación

Memorias del VIII Congreso Iberoamericano de Seguridad Informática

CIBSI 2015

Sangolqui (Quito), Ecuador, 10 al 12 de Noviembre del 2015

Compiladores

Luis Enrique Sánchez Crespo

Walter Marcelo Fuertes Díaz

Jorge Ramió Aguirre

ISBN: 978-9978-301-61-6

Universidad De Las Fuerzas Armadas Del Ecuador -ESPE

Quito, Ecuador

Patrocinadores

SEDE

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

ORGANIZACIÓN

ESPE-Innovativa
EMPRESA PÚBLICA

CRIPTORED

Fundación IN-N-VA
Centro de Innovación

PATROCINADORES Y EXPOSITORES

POLITÉCNICA
"Ingeniamos el futuro"
CAMPUS DE EXCELENCIA INTERNACIONAL

Ministerio de Telecomunicaciones y de la Sociedad de la Información

YACHAY
CIUDAD DEL CONOCIMIENTO

BLUEHAT consultores
EXPERTOS EN CIBERSEGURIDAD...

SNR Sicaman
Nuevas Tecnologías

GSyA
Grupo de Investigación en Seguridad y Auditoría

RACKLY
Grupo de Investigación de Sistemas Distribuidos. Ciberseeuridad v Contenido

COMITÉ DEL PROGRAMA

Acurio, Santiago.	Pontificia Universidad Católica del Ecuador, ECUADOR
Antezana, Nicolás.	Sociedad Peruana de Computación, PERÚ
Areitio, Javier.	Universidad de Deusto, ESPAÑA
Baluja, Walter.	Ciudad Universitaria Juan Antonio Echeverría, CUBA
Betarte, Gustavo.	Universidad de la República, URUGUAY
Blanco, Carlos.	Universidad de Cantabria, ESPAÑA
Blasco, Jorge.	City University London, ESPAÑA
Borrell, Joan.	Universidad Autónoma de Barcelona, ESPAÑA
Caballero, Ismael.	Universidad de Castilla-la Mancha, ESPAÑA
Caballero, Pino.	Universidad de La Laguna, ESPAÑA
Cano, Jeimy José.	Universidad de Los Andes, COLOMBIA
Cansian, Adriano Mauro.	Universida de Estadual Paulista, BRASIL
Carozo, Eduardo.	Universidad de Montevideo, URUGUAY
Climent Coloma, Joan Josep.	Universitat d'Alacant, Espanya
Clotet, Roger.	Universidad Simón Bolívar, Venezuela
Daltabuit, Enrique.	Universidad Nacional Autónoma de México, MÉXICO
De Fuentes, José María.	Universidad Carlos III de Madrid, ESPAÑA
Del Rey, Ángel Martín.	Universidad de Salamanca, ESPAÑA
Ferrer, Josep Domingo.	Universidad Rovira i Virgili, ESPAÑA
Ferrer, Josep Lluis.	Universidad de Las Islas Baleares, ESPAÑA
Flórez, Angélica.	Universidad Pontificia Bolivariana, COLOMBIA
Fuertes Díaz, Walter Marcelo.	Universidad de las Fuerzas Armadas ESPE, ECUADOR
Fúster, Amparo.	Consejo Superior de Investigaciones Científicas, ESPAÑA
García, David.	Universidad de Castilla – La Mancha, ESPAÑA
García, Luis Javier.	Universidad Complutense de Madrid, ESPAÑA
Garrido, Giovana.	Universidad Tecnológica de Panamá, PANAMÁ
González Manzano, Lorena.	University Carlos III of Madrid
Hecht, Pedro.	Universidad de Buenos Aires, ARGENTINA
Henriques, Marco Aurelio.	Universidade de Campinas, BRASIL
Hernández, Emilio.	Universidad Simón Bolívar, VENEZUELA
Hernández, Leobardo.	Universidad Nacional Autónoma de México, MÉXICO
Hernández, Luis.	Consejo Superior de Investigaciones Científicas, ESPAÑA
Herrera Joancomartí, Jordi.	Universitat Autònoma de Barcelona
Karel Huerta, Monica.	Universidad Politécnica Salesiana, Ecuador

López, Javier.	Universidad de Málaga, ESPAÑA
López, Julio César.	Universidade de Campinas, BRASIL
Martínez Gasca, Rafael.	Universidad de Sevilla, ESPAÑA
Mendillo, Vincenzo.	Universidad Central de Venezuela, VENEZUELA
Merino Garcia, Jorge.	Universidad de Castilla-la Mancha, España
Miret, Josep María.	Universidad de Lleida, ESPAÑA
Modelo Howard, Gaspar,	Universidad Tecnológica de Panamá, Panamá
Monge, Raúl.	Universidad Técnica Federico Santa María, CHILE
Monteiro, Edmundo.	Universidade de Coimbra, PORTUGAL
Morales, Guillermo.	CINVESTVA Instituto Politécnico Nacional, MÉXICO
Muñoz Muñoz, Alfonso,	Criptored, ESPAÑA
Peinado, Alberto.	Universidad de Málaga, ESPAÑA
Pirrone, José.	Universidad Católica Andrés Bello (UCAB), Venezuela
Ramió, Jorge.	Universidad Politécnica de Madrid, ESPAÑA
Ramos, Benjamín.	Universidad Carlos III de Madrid, ESPAÑA
Rezk, Tamara.	INRIA, FRANCIA
Sánchez, Luis Enrique.	Universidad de Castilla-la Mancha, ESPAÑA
	Universidad de las Fuerzas Armadas ESPE, ECUADOR
Santos-Olmo Parra, Antonio.	Sicaman Nuevas Tecnologías, ESPAÑA
	Universidad de Castilla-la Mancha, ESPAÑA
Satizabal, Isabel Cristina.	Universidad Politécnica de Cataluña, España
Simoes, Paulo.	Universidade de Coimbra, PORTUGAL
Soriano, Miquel.	Universidad Politécnica de Cataluña, ESPAÑA
Tapia Recillas, Horacio.	Universidad Autónoma Metropolitana, MÉXICO
Torres Olmedo, Jenny Gabriela.	Escuela Politécnica Nacional, ECUADOR
Zurutuza, Urko.	Mondragon Unibertsitatea, ESPAÑA

ORGANIZACIÓN

PhD. Walter Marcelo Fuertes Díaz	Universidad de las Fuerzas Armadas ESPE. ECUADOR
PhD. Luis Enrique Sánchez Crespo,	Universidad de Castilla-la Mancha. ESPAÑA
	Universidad de las Fuerzas Armadas ESPE. ECUADOR
PhD. Jorge Ramió Aguirre,	Universidad Politécnica de Madrid. ESPAÑA

COMITÉ ORGANIZADOR LOGÍSTICO

MsC. Luis Recalde,	Universidad de las Fuerzas Armadas ESPE. ECUADOR
MsC. Fernando Delgado,	Fundación In-Nova. ESPAÑA
MsC Laura Gómez	Fundación In-Nova ESPAÑA
MsC. Esther Álvarez,	Fundación In-Nova. ESPAÑA
MsC Nolivos, Jaime	ESPE-Innovativa E.P,ECUADOR
MsC Quishpe, María Dolores	ESPE-Innovativa E.P,ECUADOR

COMITÉ DIFUSIÓN

PhD. David Garcia Rosado,	Universidad de Castilla-la Mancha. ESPAÑA
MsC. Antonio Santos-Olmo,	Universidad de Castilla-la Mancha. ESPAÑA

COMITÉ TÉCNICO

PhD. Walter Marcelo Fuertes Díaz	Universidad de las Fuerzas Armadas ESPE. ECUADOR
PhD. Luis Enrique Sánchez Crespo,	Universidad de las Fuerzas Armadas ESPE. ECUADOR

EDITORES

PhD. Luis Enrique Sánchez Crespo,	Universidad de Castilla La-Mancha. ESPAÑA
	Universidad de las Fuerzas Armadas ESPE. ECUADOR
PhD. Walter Marcelo Fuertes Díaz	Universidad de las Fuerzas Armadas ESPE. ECUADOR
PhD. Jorge Ramió Aguirre,	Universidad Politécnica de Madrid. ESPAÑA

CHAIR SESIONES

PhD, Angelica Flórez,	Universidad Pontificia Bolivariana, COLOMBIA
PhD. Walter Marcelo Fuertes Díaz	Universidad de las Fuerzas Armadas ESPE. ECUADOR
PhD, David García Rosado,	Universidad de Castilla – La Mancha, ESPAÑA
PhD, Pedro Hecht,	Universidad de Buenos Aires, ARGENTINA
PhD, Leobardo Hernández,	Universidad Nacional Autónoma de México, MÉXICO
PhD. Luis Enrique Sánchez Crespo,	Universidad de Castilla – La Mancha, ESPAÑA
	Universidad de las Fuerzas Armadas ESPE. ECUADOR
PhD. Jorge Ramió Aguirre,	Universidad Politécnica de Madrid. ESPAÑA

INDICE

PRESENTACIÓN

El VIII Congreso Iberoamericano de Seguridad Informática CIBSI 2015, tuvo lugar entre los días 10 al 12 de Noviembre de 2015 en la ciudad de SanGolqui (Quito), siendo organizado por el Departamento de Ciencias de la Computación de la Universidad de las Fueras Armadas y la Universidad Politécnica de Madrid, España, a través de la Red Temática de Criptografía y Seguridad de la Información Criptored.

Las jornadas se desarrollaron en el Auditorio de la Universidad de las Fuerzas Armadas y en el Salón de Conferencias del Edificio de Postgrado.

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

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

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

Para esta edición del CIBSI, se recibieron 49 trabajos, de los cuales solo el 30 fueron aceptados como “Full Paper”. En estas actas se recogen los 24 trabajos para el congreso CIBSI y 6 para el taller TIBETS, seleccionados como “Full Paper” por un Comité de Programa compuesto por 58 especialistas de una docena de países Iberoamericanos. Así como 8 artículos que se aceptaron como “Short Paper”. No se incluyen, sin embargo, la conferencia magistral inaugural de CIBSI 2015 "Seguridad de la Información, ¿en quién podemos confiar?" del Dº. David Barroso, la conferencia magistral "Metodología de Experimentación para la Ciberdefensa" de Dª. Esther Álvarez Gonzalez, y la conferencia magistral inaugural de TIBETS 2015 "Lecciones aprendidas en MESI 2.0 al horizonte de la enseñanza en ciberseguridad" del Dr. Jorge Ramió Aguirre.

Luis Enrique Sánchez Crespo

Walter Marcelo Fuertes Díaz

Jorge Ramió Aguirre

Proceso Agil para la realización de Análisis y Gestión de Riesgos sobre la ISO27001 orientado a las PYMES

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

***Abstract* – The information society is increasingly dependent on Information Security Management Systems (ISMS), and having these kind of systems has become vital for the development of SMEs. However, these companies require ISMS adapted to their special features, which would be optimized from the aspect of the resources needed to deploy and maintain them. This article presents a proposed method to develop a simplified risk analysis, which is valid for SMEs, and framed within the methodology of safety management in small and medium-sized enterprises (MARISMA). This model is being applied directly to real cases, achieving a steady improvement in its implementation.**

***Resumen* — La sociedad de la información cada vez depende más de los Sistemas de Gestión de la Seguridad de la Información (SGSI), y poder disponer de estos sistemas ha llegado a ser vital para la evolución de las PYMES. Sin embargo, este tipo de compañías requiere de SGSIs adaptados a sus especiales características, y que estén optimizados desde el punto de vista de los recursos necesarios para implantarlos y mantenerlos. En este artículo se presenta el método propuesto para realizar un análisis de riesgos simplificado, que sea válido para las PYMES, y enmarcado dentro de la metodología de gestión de la seguridad en las pequeñas y medianas empresas (MARISMA). Este modelo está siendo aplicado directamente a casos reales, consiguiendo así una constante mejora en su aplicación.**

***Keyword* — Cybersecurity, *Information Security Management Systems*, ISMS, Risk Analysis, SMEs, ISO27001, ISO27005.**

***Palabras clave* — Ciberseguridad, Sistemas de Gestión de Seguridad de la Información, SGSI, Analisis de Riesgos, PYMES, ISO27001, ISO27005.**

I. Introducción

Estudios realizados han 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 [1-3]. El problema de conocer los riesgos a los que están sometidos sus principales activos se acentúa especialmente en el caso de las pequeñas y medianas empresas, que cuentan con la limitación adicional de no tener recursos humanos y económicos suficientes para realizar una adecuada gestión [4, 5].

Pero con la llegada de Internet, para las empresas es cada vez más crítico implantar controles de seguridad que les permitan conocer y controlar los riesgos a los que pueden estar sometidas [6, 7]. Gran parte de este cambio de mentalidad en las empresas tiene su origen en el cambio social producido por Internet y la rapidez en el intercambio de información, que ha dado lugar a que las empresas empiecen a tomar conciencia del valor que tiene la información para sus organizaciones y se preocupen de proteger sus datos. De esta forma, las empresas ya han tomado conciencia de que la información y los procesos que apoyan los sistemas y las redes son sus activos más importantes [6, 7]. Estos activos están sometidos a riesgos de una gran variedad, que pueden afectar de forma crítica a la empresa. Así, la importancia de la seguridad en los sistemas de información viene avalada por numerosos trabajos [8-15], por citar sólo algunos.

Algunos autores [16, 17] 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 [18]. Otros autores [19] proponen la necesidad de desarrollar un nuevo modelo de análisis de riesgos (AR) pero orientándolo directamente a las PYMES, considerando que el uso de técnicas de análisis y gestión de riesgos, así como el papel de terceros, es necesario para poder garantizar la seguridad del sistema de información de las PYMES [20]. Aunque la investigación realizada se centra inicialmente en las PYMES los resultados podrían aplicarse en otros sectores como el de salud [21-24], o nuevas tecnologías como el cloud computing [25].

Estudios centrados en la evaluación de riesgos [26-28], realizados sobre organizaciones en Europa y los EE.UU revelan que las PYMES se caracterizan por la falta de la dedicación necesaria a la seguridad de TI, debido principalmente a la asignación de responsabilidades a personal sin la debida formación. Así mismo, la mayoría de las organizaciones carecen de políticas de seguridad y sistemas de evaluación del riesgo, llegando al caso en que el 73% de los encuestados de PYMES de UK dijo realizar en su casa la evaluación de riesgos. Menos del 10% de los encuestados afirmó usar una herramienta de análisis de riesgos, y ninguno utilizó una guía de referencia como podía ser la ISO/IEC27001 [29, 30]. Esto, junto con la escasa proporción

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

L. E. Sánchez, Universidad de Castilla-la Mancha (UCLM), España y Universidad de las Fuerzas Armadas (ESPE), Proyecto Prometeo de la SENESCYT, Ecuador, Luisenrique@sanchezcrespo.org

E. Álvarez, Fundación In-Nova, Toledo, España, Ealvarez@in-nova.org

M. Huerta, Universidad Politécnica Salesiana, Proyecto Prometeo de la SENESCYT, Ecuador, mhuerta@ieee.org

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

de organizaciones que realmente emplea especialistas en seguridad, plantea dudas sobre la manera exhaustiva o eficaz en que pueden haberse realizado dichos análisis.

Al analizar las causas por las que no se había realizado el análisis de riesgos se llegó a la conclusión de que dado que el análisis de riesgos es a menudo complejo y requiere conocimientos especializados [31], y que una evaluación de la situación actual requiere de herramientas de análisis de riesgo [32] comerciales, las cuales no son fáciles de usar sin conocimientos técnicos adecuados, es evidente que muchas PYMES no están preparadas para evaluarse los riesgos a sí mismas. Aunque algunas PYMES ya habían tomado la determinación de externalizar dicho servicio, en general la mayoría no había realizado dicha evaluación por la falta de concienciación de su importancia.

Otros autores sugieren que no es suficiente con aplicar un enfoque basado en análisis y gestión de riesgos [33] 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 [34].

Otro de los aspectos que se está estudiando para su aplicación a los modelos de gestión de la seguridad y su madurez es el control de los costes asociados a la gestión de la seguridad, ya que estos pueden influir en el dimensionamiento del modelo de gestión de la seguridad. De esta forma, Mercuri [35] se propone asociar como parte fundamental del desarrollo de los SGSI los análisis de coste–beneficio (CBA) en la fase del análisis de riesgos.

Como tal, una de las cuestiones derivadas de las conclusiones es la necesidad de obtener nuevas metodologías y modelos de análisis y gestión del riesgo que permitan adaptarse a las PYMES, con el objetivo de eliminar (o al menos reducir) los inconvenientes y ayudar a estas sociedades a evaluar los riesgos a los que sus activos están expuestos y a establecer los controles de seguridad adecuados [36].

Muchos autores consideran que el punto central de los SGSI debe ser el análisis de riesgos. Entre ellas se puede destacar la propuesta de Barrientos [37] y UE CORAS (IST–2000–25031) [38, 39]. La propuesta de Barrientos [37] está basada en llevar a cabo un análisis relativo a la seguridad informática para identificar el grado de vulnerabilidad y determinar los aspectos de mejora a ser llevados a cabo en la organización con el objeto de reducir el riesgo. Por otro lado, UE CORAS (IST–2000–25031) [38, 39] está desarrollando un marco para el análisis de riesgos de seguridad que utiliza UML2, AS/NZS 4360, ISO/IEC27001, RM–ODP6, UP7 y XML8.

Siegel [33] señala que los modelos de seguridad informática que se centran exclusivamente en modelos de eliminación de riesgos no son suficientes, y por otro lado Garigue [34] remarca que actualmente los gerentes no desean saber sólo qué se ha realizado para mitigar los riesgos, también se debe poder dar a conocer eficazmente que se ha realizado esta tarea y si se ha conseguido ahorrar dinero.

Sneza realiza un estudio sobre las PYMES considerando los resultados del análisis de riesgos como clave para garantizar que las políticas y procedimientos son realmente necesarios, llegando a la conclusión de que las PYMES deben guiarse por el riesgo de pérdidas de activos derivado del análisis de riesgos. Se debe persuadir a los propietarios de las PYMES de emprender un escenario formal basado en el análisis de riesgos y la protección de los activos de información. Los recientes hallazgos de la seguridad de la información han puesto de manifiesto una fuerte correlación entre el proceso formal de evaluación de riesgos y los gastos de la seguridad de la información [40].

Se debe tener en cuenta que el análisis de riesgos es un proceso costoso que no se puede repetir cada vez que se realiza una modificación. Por eso es importante desarrollar metodologías específicas que permitan mantener los resultados del análisis de riesgos. El proyecto de la UE Coras [38, 39] hace de este mantenimiento del análisis de riesgos el punto principal de su modelo.

Las principales conclusiones obtenidas es que los modelos de análisis y gestión del riesgo son fundamentales para los SGSIs, pero no existen metodologías que se adecuen al caso de las PYMES, y las existentes se muestran ineficientes para este tipo de compañía.

Por lo tanto, y considerando que las PYMES representan una gran mayoría de empresas tanto a nivel nacional como internacional y son muy importantes para el tejido empresarial de cualquier país, creemos que avanzar en la investigación para mejorar los procesos de análisis y gestión del riesgo para este tipo de empresas puede generar importantes aportaciones. Esto puede contribuir a mejorar no sólo la seguridad de las PYMES, sino también su nivel de competitividad. Por este motivo, a los largo de los últimos años hemos trabajado en elaborar un proceso simplificado que permita analizar y gestionar el riesgo de seguridad en las PYMES [41-44], y además hemos construido una herramienta que automatiza completamente la metodología [45], y lo hemos aplicado en casos reales [46], lo que nos ha permitido validar tanto la metodología como la herramienta.

Toda la metodología de Análisis de Riesgos desarrollada, y en especial las partes relacionadas con los controles, han sido aplicadas sobre la norma ISO/IEC27001 y en especial sobre el Anexo A de esta que define los controles que deben cumplirse. Por lo tanto, y aunque esta metodología nace para poder extenderse a otros estándares internacionales, actualmente solo se ha validado su funcionamiento sobre el estándar internacional de la ISO/IEC27001.

El artículo continúa en la Sección 2 describiendo brevemente las metodologías y modelos para el análisis y la gestión del riesgo de la seguridad y su tendencia actual. En la Sección 3 se introduce brevemente nuestra propuesta de metodología para el análisis y la gestión del riesgo de la seguridad orientada hacia las PYMES. En la Sección 4 se introduce la herramienta que da soporte al proceso. En la Sección 5 se muestran algunos resultados obtenidos al aplicar el proceso sobre un caso real. Finalmente, en la Sección 6 concluimos indicando cuál será el trabajo que desarrollaremos en el futuro.

II. Estado del Arte

Con el propósito de reducir las carencias mostradas en el apartado anterior y reducir las pérdidas que éstas ocasionan, han aparecido un gran número de procesos, marcos de trabajo y métodos para la gestión del riesgo cuya necesidad de uso para proteger de forma eficaz los activos de una compañía está siendo cada vez más reconocida y considerada por las organizaciones, pero que como se ha mostrado son ineficientes para el caso de las PYMES.

En relación con los estándares más destacados se ha podido constatar que la mayor parte de ellos han intentado incorporar procesos para el análisis y la gestión del riesgo, pero que son muy difíciles de implementar y requieren una inversión demasiado alta que la mayoría de las PYMES no pueden asumir [47].

Entre las principales propuestas para el análisis y gestión del riesgo podemos destacar MAGERIT [48], OCTAVE [49] o CRAMM [50]. A pesar de ello, la gestión de la seguridad no puede limitarse al análisis y la gestión del riesgo [33], sino que además de identificar y eliminar riesgos se ha de realizar de manera eficiente, obteniendo la compañía grandes ahorros de costes como consecuencia directa de una mejor gestión de la seguridad [34]. Gracias al análisis de riesgos se podrán identificar los activos y conocer el nivel de seguridad que se debe aplicar. Los expertos también han propuesto recientemente realizar un análisis de riesgos para poder alinear las estrategias de la empresa y de la seguridad [51], ya que esto hace que la empresa pase de tomar una posición reactiva ante la seguridad a una proactiva.

Por otro lado, algunos de los principales estándares de gestión de la seguridad, han intentado incorporar dentro de sus procesos el análisis y la gestión del riesgo:

- *ISO/IEC27005 [52]:* Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC27001 [30] y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC27001 [30] e ISO/IEC27002 [53] es importante para un completo entendimiento de la norma ISO/IEC 27005 [52], que es aplicable a organizaciones que tienen la intención de gestionar los riesgos que puedan comprometer la organización de la seguridad de la información [54, 55]. Su publicación revisa y retira las normas ISO/IEC TR 13335–3 [56] y ISO/IEC TR 13335–4 [57].
- *ISO/IEC21827/SSE–CMM [58, 59]:* El modelo de capacidad y madurez en la ingeniería de seguridad de sistemas describe las características esenciales de los procesos que deben existir en una organización para asegurar una buena seguridad en los sistemas, incluyendo en las fases previas un proceso orientado al riesgo, con 4 subprocesos: SSE-PA02 (Determinar el impacto), SSE-PA03 (Identificar los riesgos de seguridad), SSE-PA04 (Identificar las amenazas), SSE-PA05 (Identificar las vulnerabilidades).
- *ISO/IEC 15443 [60, 61]:* Clasifica los métodos existentes dependiendo del nivel de seguridad y de la fase del aseguramiento. La evaluación del aseguramiento se divide en proceso, producto y ambiente, mientras que las fases del análisis del riesgo son diseño/implementación, integración/verificación, réplica, transición y operación. Las fases del análisis del riesgo para CC [62] son diseño/implementación, integración/verificación, transición y operación.
- *ISO/IEC2000/ITIL [63, 64]:* ITIL ofrece un elemento para una correcta gestión de riesgos: el conocimiento actualizado y detallado de todos los activos de la organización y de las relaciones, pesos y dependencias entre ellos. Dicho conocimiento ITIL lo administra desde el proceso de gestión de la configuración de soporte al servicio, y mediante el uso de la herramienta básica sobre la que se construye una aproximación coherente a la gestión eficiente de las TI, la CMDB (Configuration Management Database). El disponer del repositorio actualizado de activos que representa la CMDB facilita la realización del análisis de riesgos en la fase de planificación del SGSI, que se utilizará como elemento de ponderación de los controles a implantar y cuya permanente actualización resultará incluso más relevante una vez el SGSI se encuentre implantado y funcionando.
- *COBIT [65]:* Es una metodología para el adecuado control de los proyectos de tecnología, los flujos de información y los riesgos que implica la falta de controles adecuados. Incluye un proceso orientado a evaluar los riesgos, en el dominio PO9. Este proceso se centra principalmente en los criterios de confidencialidad, integridad y disponibilidad, y de forma secundaría en criterios de efectividad, eficiencia, cumplimiento y confiabilidad. Por último este proceso involucra a diversos recursos del TIC (RRHH, Sistemas de Información, Tecnología, Instalaciones y Datos).

Por otro lado, existe un pequeño conjunto de herramientas de análisis de riesgos. Actualmente las más utilizada para el análisis de riesgos es PILAR, basada en Magerit v3 [48]. Otras herramientas utilizadas son la propuesta por ENISA, que incluye un sistema de comparativas, OCTAVE–S y Octave Automated Tool, que implementan la metodología de evaluación de riesgos OCTAVE [49], CRAMM 5.2 y COBRA, etc.

El principal problema de estos procesos y herramientas es su complejidad para aplicarlos en el caso de las PYMES, ya que han sido concebidos para grandes empresas [66-69]. Se justifica en repetidas ocasiones que la aplicación de este tipo de procesos para las PYMES es difícil y costosa. Además, las organizaciones, incluso las grandes, tienden más a adoptar grupos de procesos relacionados como un conjunto que a tratar

los procesos de forma independiente [70].

Por lo tanto, y como conclusión de este apartado, se puede decir que es pertinente y oportuno abordar el problema de desarrollar un nuevo proceso para el análisis y gestión del riesgo de la seguridad para los sistemas de información en las PYMES, así como una herramienta que soporte este proceso, tomando como base la problemática a que este tipo de compañías se enfrenta y que ha llevado a continuos fracasos en los intentos de implantación en este tipo de empresas. Para ello se tomarán como base algunas de las normas y documentos tanto nacionales como internacionales más adecuados, como las guías para la gestión de seguridad ISO/IEC 13335 [56, 57, 71] y la metodología de análisis y gestión de riesgos Magerit [48].

III. MARISMA-AGR

Para solucionar los problemas detectados en el análisis y gestión del riesgo, se ha realizado un proceso orientado a las PYMES y enfocado a reducir los costes de generación y mantenimiento del proceso de análisis y gestión del riesgo denominado MARISMA-AGR. Este proceso se ha obtenido mediante la aplicación del método de investigación en acción y se ha enmarcado dentro de una metodología (MARISMA) que acomete todos los aspectos relacionados con la gestión de la seguridad [21, 72].

Esta metodología asocia el análisis y la gestión del riesgo a los controles necesarios para la gestión de la seguridad y consta de dos fases muy importantes:

- *Fase I:* Se establece una estructura de relaciones entre los diferentes elementos involucrados en el análisis del riesgo y los controles necesarios para gestionar la seguridad. Estas relaciones se establecen mediante el conocimiento adquirido en las diferentes implantaciones, que es almacenado en una estructura denominada esquema para ser reutilizado con posterioridad, reduciendo los costes de generación de este proceso [73].
- *Fase II:* Mediante la selección del esquema más adecuado y la identificación de un pequeño conjunto de los principales activos se obtiene un detallado mapa de la situación actual (análisis del riesgo) y un plan de recomendaciones de cómo mejorarlo (gestión del riesgo).

Este apartado se divide en tres subapartados. En el primero se verán una serie de definiciones necesarias para entender el proceso. En el segundo subapartado se analizará la primera fase del proceso. En el último subapartado se analizará la segunda fase del subproceso.

A. *Definiciones previas.*

A continuación, se describen los principales conceptos, que intervienen en la metodología:

- *Esquema:* Estructura formada por los principales elementos de un SGSI y las relaciones entre ellos, que puede ser reutilizado por un conjunto de compañías con características comunes (mismo sector y tamaño) a partir del conocimiento adquirido con la implantación de la metodología MARISMA y posteriores refinamientos [74].
  - *Esquema Base:* Esquema inicial obtenido a partir del conocimiento de expertos en seguridad, que sirve como base para la elaboración de otros esquemas más específicos que puedan adecuarse a conjuntos de compañías [73].
- *SGSI:* Parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. En el caso de la metodología MARISMA el SGSI se compone entre otros de un conjunto de reglamentos que definen la política de seguridad de la compañía, procedimientos, controles, un sencillo análisis de riesgo y un cuadro de mandos que nos permite conocer cómo evoluciona el sistema (ver Figura 1).

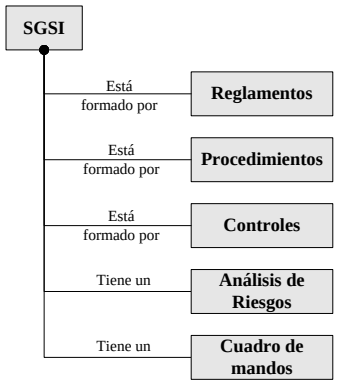


Figura 1. Esquema de los componentes de un SGSI.

- *Análisis de riesgos:* Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización [48]. La metodología MARISMA incluye un sencillo método para estimar el riesgo a partir de un conjunto básico de activos.
  - *Activo:* Recursos del sistema de información, o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.
  - *Amenaza:* Evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
  - *Vulnerabilidad:* Debilidad o falta de control que permitiría o facilitaría que una amenaza actuase contra un activo del sistema que presenta la citada debilidad.
  - *Criterios de riesgo:* Criterios que permiten estimar el grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

B. MARISMA-AGR Actividad 1: Análisis de riesgos como parte de un Esquema.

El principal objetivo de esta actividad es seleccionar los elementos necesarios para poder realizar, en actividades posteriores de la metodología, un análisis de riesgos básico y de bajo coste sobre los activos que componen el sistema de información de la compañía que se adapte a los requerimientos de las PYMES.

Esta actividad está basada en el principio de que los elementos que participan en un análisis de riesgos y sus relaciones tienen un alto grado de coincidencia cuando se aplican en PYMES que tienen características parecidas (mismo sector y mismo tamaño), por lo que se pueden establecer dichas relaciones a priori eliminando el coste de tener que analizarlas una por una mediante una labor de consultoría en cada caso. Aun cuando existan diferencias entre unas y otras, éstas son irrelevantes con respecto a la configuración final del SGSI obtenido para el caso de las PYMES, dado que este tipo de empresas priorizan el coste a obtener un resultado con un alto grado de precisión.

Aunque el análisis de riesgos es una de las partes fundamentales en la norma ISO/IEC27001 [30] y se encuentra descrita en detalle en el estándar ISO/IEC27005 [52], el principal objetivo del análisis de riesgos incluido en la metodología desarrollada es que sea lo menos costoso posible, utilizando una serie de técnicas y matrices predefinidas, aunque obteniendo un resultado con la suficiente calidad.

En la Figura 2 se puede ver el esquema básico de entradas, tareas y salidas que componen esta actividad:

- *Entradas:* Como entrada se recibirá el conocimiento del grupo de expertos del dominio de seguridad (GED) obtenido durante el proceso de implantación de SGSIs, así como un conjunto de controles para la gestión de seguridad que se encuentran almacenados en el repositorio de esquemas y un conjunto de elementos (tipos de activos, amenazas, vulnerabilidades y criterios de riesgo) necesarios para elaboración del análisis de riesgos (en el esquema base desarrollado la selección de estos elementos se ha basado en el contenido de la metodología de análisis de riesgos Magerit y del estándar ISO/IEC27005 [52]).

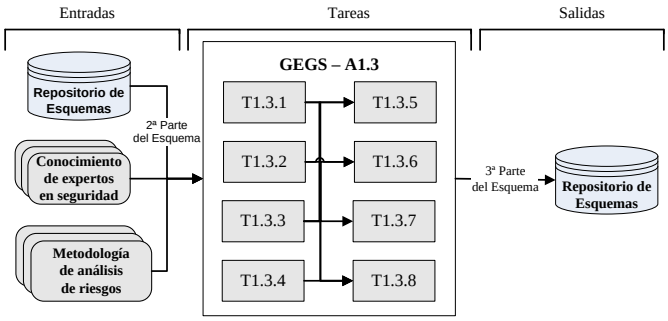


Figura 2. Esquema simplificado a nivel de tarea de la actividad A1.3.

- *Tareas:* El subproceso estará formado por ocho tareas: i) selección de tipos de activos; ii) selección de amenazas; iii) selección de vulnerabilidades; iv) selección de criterios de riesgo; v) establecimiento de relaciones entre tipos de activos y vulnerabilidades; vi) establecimiento de relaciones entre amenazas y vulnerabilidades; vii) establecimiento de relaciones entre amenazas y controles; viii) establecimiento de relaciones entre tipos de activos, vulnerabilidades y criterios de riesgo. Las cuatro primeras tareas son independientes y permiten seleccionar los elementos de entrada. Las otras cuatro tareas se ocupan de establecer las relaciones existentes entre las familias de elementos de las tareas: i) T1.3.1 – Selección de tipos de activos; ii) T1.3.2 - Selección de amenazas; iii) T1.3.3 – Selección de vulnerabilidades; iv) T1.3.4 – Selección de criterios de riesgo.

  Estas relaciones se establecen a partir del conocimiento del grupo de expertos del dominio (GED) y de los continuos refinamientos obtenidos de la implantación de la metodología. En las siguientes subsecciones se detallarán estas tareas.

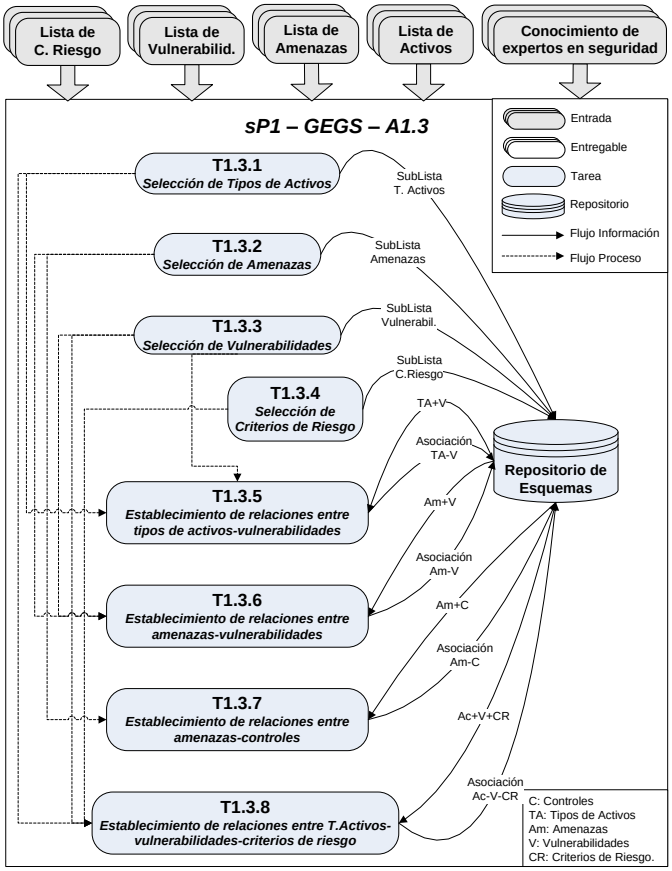


Figura 3. Esquema detallado a nivel de tarea de la actividad A1.3.

- *Salidas:* La salida producida por este subproceso consistirá en un subconjunto de los elementos de entrada y las relaciones establecidas entre ellos, los cuales se almacenarán en el repositorio de esquemas y que se corresponden con la tercera parte de los

elementos de los que se compondrá el esquema que se quiere generar.

En la Figura 3 se pueden ver las tareas de la actividad de forma mucho más detallada, mostrando cómo interactúan éstas con el repositorio de esquemas encargado de contener los elementos que conforman los diferentes esquemas del sistema. No existen entregables entre las diferentes tareas, ya que el resultado de cada tarea es almacenado en el repositorio, para que pueda ser utilizado por otras tareas.

A continuación, se analizarán uno por uno los diferentes elementos (tipos de activos, amenazas, vulnerabilidades, impactos y riesgo y matrices de asociación) de los que se compone el análisis de riesgos propuesto en la nueva metodología y los valores que estos elementos pueden tomar.

- *Tarea T1.3.1 – Selección de tipos de activos:* Se ocupa de seleccionar el conjunto de tipos de activos que formarán parte del esquema que se está construyendo. Los tipos de activos se utilizarán posteriormente para diversas tareas: i) agrupar los activos del sistema de información; ii) se relacionarán con otros elementos del análisis de riesgos para facilitar la automatización del mismo.

  El conjunto de tipos de activos será seleccionado en base a las metodologías, normas, etc que se determinen como entradas de la tarea y al conocimiento adquirido por el grupo de expertos del domino (GED) a lo largo de la implantación.

  La selección del conjunto de tipos de activos que conforma el esquema base está basado en la metodología de análisis de riesgos Magerit v3.0 [48] y en el estándar ISO/IEC27005 [52]. Para el esquema actual se ha definido un conjunto de 23 tipos de activos.

- *Tarea T1.3.2 – Selección de amenazas:* Se ocupa de seleccionar el conjunto de amenazas que formarán parte del esquema que se está construyendo. Una amenaza se define como un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos [48]. Estas amenazas se relacionarán en tareas posteriores con otros elementos del análisis de riesgos, con el objetivo de poder automatizar y reducir los costes a la hora de evaluar el riesgo al que están sometidos los activos de un sistema de información.

  El conjunto de amenazas será seleccionado en base a las metodologías, normas, etc que se determinen como entradas de la tarea y al conocimiento adquirido por el grupo de expertos del domino (GED) a lo largo de la implantación.

  La selección del conjunto de amenazas que conforma el esquema base está basada en la metodología de análisis de riesgos Magerit [48] y en el estándar ISO/IEC27005 [52]. Estas amenazas están agrupadas en un conjunto de categorías: naturales, accidentales, ataques intencionados, errores no intencionados, personal. Para el esquema actual se han definido un conjunto de 51 amenazas asociadas a 6 tipos de amenazas.

- *Tarea T1.3.3 – Selección de vulnerabilidades:* Se ocupa de seleccionar el conjunto de vulnerabilidades que formarán parte del esquema que se está construyendo. Una vulnerabilidad se define como una debilidad o falta de control que permitiría o facilitaría que una amenaza actuase contra un activo del sistema que presenta la citada debilidad [48]. Estas vulnerabilidades se relacionarán en tareas posteriores con otros elementos del análisis de riesgos, con el objetivo de poder automatizar y reducir los costes a la hora de evaluar el riesgo al que están sometidos los activos de un sistema de información.

  El conjunto de vulnerabilidades será seleccionado en base a las metodologías, normas, etc, que se determinen como entradas de la tarea y al conocimiento adquirido por el grupo de expertos del domino (GED) a lo largo de la implantación.

  La selección del conjunto de vulnerabilidades que conforma el esquema base está basada en la metodología de análisis de riesgos Magerit [48] y en el estándar ISO/IEC27005 [52]. Para el esquema actual se han definido un conjunto de 48 vulnerabilidades.

- *Tarea T1.3.4 – Selección de criterios de riesgo:* Se ocupa de seleccionar el conjunto de criterios de riesgo que formarán parte del esquema que se está construyendo. Los criterios de riesgo se definen como aquellos criterios que permiten estimar el grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. Estos criterios de riesgo se relacionarán en tareas posteriores con otros elementos del análisis de riesgos, con el objetivo de poder automatizar y reducir los costes a la hora de evaluar el riesgo al que están sometidos los activos de un sistema de información.

  El conjunto de criterios de riesgo será seleccionado en base a las metodologías, normas, etc que se determinen como entradas de la tarea y al conocimiento adquirido por el grupo de expertos del domino (GED) a lo largo de la implantación.

  La selección del conjunto de criterios de riesgo que conforma el esquema base está basada en la metodología de análisis de riesgos Magerit [48] y en el estándar ISO/IEC27005 [52], aunque se ha simplificado ya que el conjunto ofrecido por Magerit [48] se muestra demasiado complejo para la estructura sencilla de las PYMES, por lo que para el modelo se han seleccionado los más importantes, prescindiendo del resto (aunque la metodología puede soportar un conjunto de criterios de riesgo más complejo). El conjunto de criterios de riesgo definidos para el esquema base está formado por cuatro criterios

(confidencialidad, integridad, disponibilidad y legalidad).

- *Tarea T1.3.5 – Establecer relaciones entre tipos de activos y vulnerabilidades:* Se ocupa de establecer las relaciones existentes entre los elementos que componen el conjunto de tipos de activos y los elementos que componen el conjunto de vulnerabilidades para un esquema determinado.

  El objetivo principal de este conjunto de asociaciones es establecer relaciones entre los elementos del SGSI para poder realizar una evaluación del riesgo de bajo coste en la actividad A2.3.

  Estas asociaciones se establecen por el grupo de expertos del dominio (GED) en base al conocimiento adquirido en diferentes implantaciones del SGSI.

  Para el esquema base actual, se han establecido 237 relaciones entre el conjunto de tipos de activos y el conjunto de vulnerabilidades del esquema, en base al conocimiento adquirido a lo largo de la investigación.

- *Tarea T1.3.6 – Establecer relaciones entre amenazas y vulnerabilidades:* Se ocupa de establecer las relaciones existentes entre los elementos que componen el conjunto de amenazas y los elementos que componen el conjunto de vulnerabilidades para un esquema determinado.

  El objetivo principal de este conjunto de asociaciones es establecer relaciones entre los elementos del SGSI para poder realizar una evaluación del riesgo de bajo coste en la actividad A2.3.

  Estas asociaciones se establecen por el grupo de expertos del dominio (GED) en base al conocimiento adquirido en diferentes implantaciones del SGSI.

  Para el esquema base actual, se han establecido 79 relaciones entre el conjunto de amenazas y el conjunto de vulnerabilidades, en base al conocimiento adquirido a lo largo de la investigación.

- *Tarea T1.3.7 – Establecer relaciones entre amenazas y controles:* Se ocupa de establecer las relaciones existentes entre los elementos que componen el conjunto de amenazas y los elementos que componen el conjunto de controles para un esquema determinado.

  El objetivo principal de este conjunto de asociaciones es establecer relaciones entre los elementos del SGSI para poder realizar una evaluación del riesgo de bajo coste en la actividad A2.3.

  Estas asociaciones se establecen por el grupo de expertos del dominio (GED) en base al conocimiento adquirido en diferentes implantaciones del SGSI.

  Para el esquema base actual, se han establecido 1014 relaciones entre el conjunto de amenazas y el conjunto de controles del esquema actual, en base al conocimiento adquirido a lo largo de la investigación.

- *Tarea T1.3.8 – Establecer relaciones entre tipos de activos, vulnerabilidades y criterios de riesgo:* Se ocupa de establecer las relaciones existentes entre los elementos que componen el conjunto de tipos de activos, los elementos que componen el conjunto de vulnerabilidades y los elementos que componen el conjunto de criterios de riesgo para un esquema determinado.

  El objetivo principal de este conjunto de asociaciones es establecer relaciones entre los elementos del SGSI (ver Figura 4) para poder realizar una evaluación del riesgo de bajo coste en la actividad A2.3.

  Estas asociaciones se establecen por el grupo de expertos del dominio (GED) en base al conocimiento adquirido en diferentes implantaciones del SGSI.

  Para el esquema base actual, se han establecido 345 relaciones entre el conjunto de tipos de activos, el conjunto de vulnerabilidades y el conjunto de criterios de del esquema actual, en base al conocimiento adquirido a lo largo de la investigación.

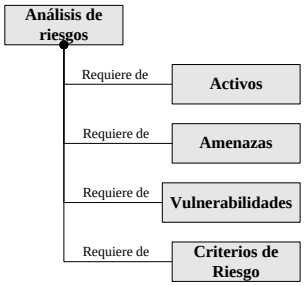


Figura 4. Esquema de los componentes del análisis de riesgos.

C. *MARISMA-AGR Actividad 2: Aplicación del Análisis de Riesgos.*

El principal objetivo de esta actividad es establecer una evaluación de los riesgos a los que se encuentran sometidos los principales activos del sistema de información de la compañía sobre la que se quiere implantar el SGSI, así como proponer un plan al responsable de seguridad (Cl/RS) para gestionar los riesgos de la forma más eficiente posible.

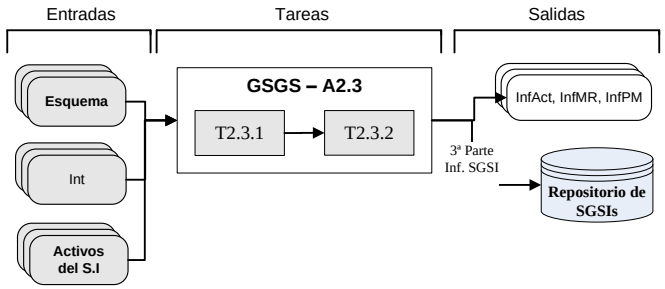


Figura 5. Esquema simplificado a nivel de tarea de la actividad A2.3.

En la Figura 5 se puede ver el esquema básico de entradas, tareas y salidas que componen esta actividad:

- *Entradas:* Como entrada se recibirá: i) un esquema de los existentes en el repositorio de esquemas, que será seleccionado por el consultor de seguridad (CoS) en base a las características de la compañía (sector y tamaño de la misma), del que se obtendrán los elementos necesarios para la realización del análisis de riesgos (listado de controles, listado tipos de activos, listado de amenazas, listado de vulnerabilidades, listado de criterios de riesgo, relaciones entre los tipos de activos y las vulnerabilidades, relaciones entre las amenazas y las vulnerabilidades, relaciones entre las amenazas y los controles y relaciones entre los tipos de activos, las vulnerabilidades y los criterios de riesgo); ii) el interlocutor (Int) válido para la compañía, el cual se encargará de definir los activos; iii) un conjunto de activos del sistema de información, lo más generalistas posible (grano grueso).
- *Tareas:* El subproceso estará formado por dos tareas. Estas tareas son: i) identificación de activos; y ii) generación de la matriz de riesgos y el plan de mejora. La tarea T2.3.2 (Generación de la matriz de riesgos y del plan de mejora) es dependiente de la T2.3.1 (Identificación de activos), por lo que no podrá ejecutarse hasta la finalización de ésta.
- *Salidas:* La salida producida por este subproceso consistirá en una serie de entregables (InfAct - Informe de activos del sistema de información, InfMR - Matriz de riesgos a los que están sometidos los activos del sistema de información y el InfPM - Plan de mejora recomendado por la metodología para afrontar las mejoras en la gestión de la seguridad del SGSI) para que el consultor de seguridad (CoS) pueda analizarlos. La información contenida en estos entregables será almacenada en el repositorio de SGSIs para que posteriormente pueda utilizarse en la generación de los elementos que componen el SGSI de la compañía.

En la Figura 6 se pueden ver las tareas de la actividad de forma mucho más detallada, mostrando cómo interactúan con el repositorio de SGSIs encargado de contener los elementos que conforman los SGSIs. Cada tarea generará un entregable para su análisis por parte del consultor de seguridad (CoS) y almacenará la información para que sea utilizada posteriormente en la actividad A2.4 (Generación del SGSI).

El desarrollo de esta actividad está basado en los propuestos por Stephenson que se centran en la sinergia entre la prueba técnica y el análisis de riesgos tomando como referencia la ISO/IEC27002 [53] y en la metodología de análisis de riesgos Magerit v3 [48].

Estas metodologías suelen producir rechazo en el caso de las PYMES debido a que éstas las perciben como demasiado complejas, a que requieren un enorme compromiso por parte de los miembros de la compañía y a que los costes asociados a los mismos no son aceptados por las compañías. Por ello, la metodología MARISMA simplifica el proceso de evaluación del riesgo para adecuarlo a las PYMES.

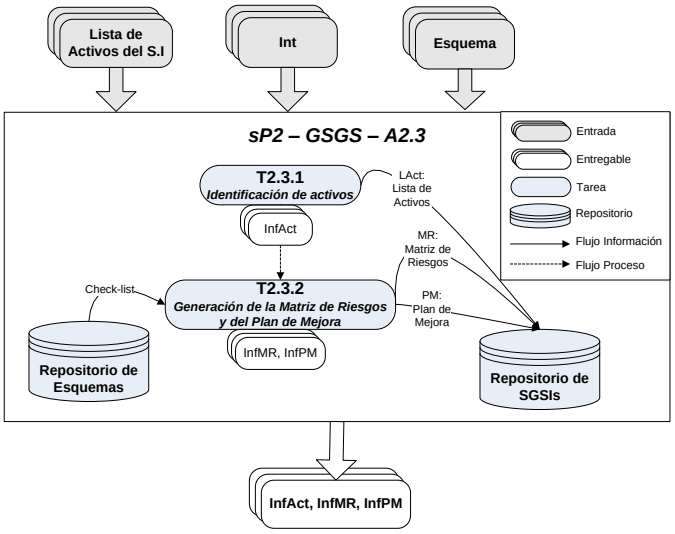


Figura 6. Esquema detallado a nivel de tarea de la actividad A2.3.

Las principales bases sobre las que se define esta actividad son: flexibilidad, simplicidad y eficiencia en costes (humanos y temporales). Se trata pues de una actividad que pretende identificar con el menor coste posible los activos de la compañía y los riesgos asociados, usando para ello los resultados generados en las actividades anteriores y unos sencillos algoritmos.

La parte de análisis de riesgos de la metodología desarrollada toma algunos aspectos de Magerit v3 [48] y algunos aspectos de los análisis de riesgos clásicos (Figura 7), pero en todo momento tiende a la simplificación.

Para que esta actividad funcione de forma coherente se deben tener en cuenta las condiciones especiales de las PYMES, en las que los usuarios no suelen tener ni el tiempo ni los conocimientos adecuados para aplicar de forma eficiente metodologías de análisis de riesgos, ni para determinar de forma adecuada los activos de los sistemas de información.

Al igual que en las actividades anteriores, cuando se trata de PYMES no se busca la opción óptima sino una opción razonablemente buena que permita grandes reducciones de tiempos a la hora de obtener el resultado [75].

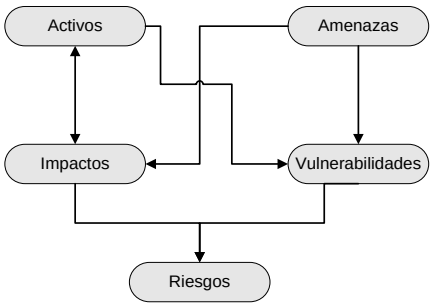


Figura 7. Esquema general del análisis de riesgos.

Las tareas de esta actividad se apoyarán principalmente en la parte tercera del esquema seleccionado, que se corresponde con la generada durante la actividad A1.3 (Generación de las tablas del análisis de riesgos) y en la lista de controles obtenida en la tarea T1.2.2 (Establecimiento de los controles del modelo) del subproceso GEGS (Generación de Esquemas).

A continuación mostramos las tareas que componen la actividad:

- *Tarea T2.3.1 – Identificación de activos:* El objetivo de la tarea T2.3.1 es obtener un conjunto de los activos que componen el sistema de información de la empresa. Los activos definidos son el objetivo principal hacia el que se enfoca el SGSI, ya que son los elementos que se pretenden proteger, porque suponen valor para la compañía y en la mayor parte de los casos son su factor diferenciador con respecto a la competencia.

  Una de las diferencias principales que presenta el método para la evaluación del riesgo presentado en la metodología frente a Magerit [48] es que se busca que los activos sean lo más generales (grano grueso), mientras que Magerit intenta identificarlos de forma clara y precisa (grano fino).

  En las PYMES se debe intentar definir un conjunto muy pequeño y básico de activos, ya que su sistema de información no permite la protección discriminada de activos de baja atomicidad, ni puede soportar el coste de gestión de los mismos. Por lo tanto, en esta tarea se buscarán activos generales que se puedan valorar de forma sencilla tanto desde el punto de vista cuantitativo como cualitativo.

  En esta tarea el consultor de seguridad (CoS) deberá ayudar el interlocutor (Int) a identificar el conjunto de activos de valor que componen el S.I. de la compañía.

  Los resultados generados en esta tarea son fundamentales para poder realizar una evaluación del riesgo y un plan de mejora en la tarea T2.3.2.

- *Tarea T2.3.2 – Generación de matriz de riesgos y plan de mejora:* El objetivo de la tarea T2.3.2 es realizar una evaluación de los riesgos a los que están sometidos los activos de la empresa definidos en la tarea T2.3.1.

  Esta tarea requiere de los datos generados durante la actividad A1.3 y de los activos identificados en la tarea T2.3.1 para generar una matriz riesgos que muestre de forma detallada los riesgos a los que está sometido cada activo y un plan de mejora que determine cómo acometer estos riesgos.

  El plan de mejora se soporta sobre los resultados obtenidos de la matriz de riesgos. La matriz de riesgos y el plan de mejora son utilizados por el consultor de seguridad (CoS) para determinar y analizar medidas adicionales y urgentes que deban tomarse en la compañía para mitigar riesgos elevados sobre los activos de información de la compañía.

  El primer objetivo de esta tarea es generar una matriz de riesgo que nos permita conocer los riesgos a los que está sometido cada activo de la compañía en cada nivel de madurez y para cada elemento del análisis de riesgos (amenazas, vulnerabilidades y criterios de riesgo). El resultado será una tabla con las siguientes columnas:

  - Nivel: Nivel de Madurez de la seguridad.
  - Nombre y descripción del activo.
  - Coste del activo: valor cuantitativo que tendría la pérdida del activo para la compañía.
  - Valor estratégico: valor cualitativo que tendría la pérdida del activo.
  - Tipo de activo.
  - Amenaza.
  - Vulnerabilidad.
  - Criterios de riesgo.
  - Nivel de la amenaza (NA): Se determina teniendo en cuenta el impacto que produciría sobre un activo la explotación de una amenaza. La escala tendrá valores comprendidos entre [bajo = 1, medio = 2, alto =3].
  - Nivel de probabilidad (P): Se define como la probabilidad de ocurrencia de una vulnerabilidad en función de criterios empíricos. La escala tendrá valores comprendidos entre [bajo = 1, medio = 2, alto =3].
  - Nivel de riesgo (NR): La definición del nivel de riesgo (NR) se obtiene a partir de la probabilidad (P) de ocurrencia (vulnerabilidad) y el nivel de la amenaza (NA) (ver Ecuación 1).

NR = P * NA
Siendo: • ***NR:*** Nivel de riesgo. • ***P:*** Probabilidad de ocurrencia de las vulnerabilidades. • ***NA:*** Nivel de la amenaza.

Ecuación 1. Nivel de riesgo.

El valor obtenido en el nivel de riesgo (NR) se multiplicara por el valor del activo y se gestionará según la Tabla I y se moverá en un rango comprendido entre 1 (menor riesgo) y 27 (mayor riesgo). Se ha determinado que el nivel del riesgo residual (NRR), es decir, el que tiene actualmente la compañía, nunca debe ser superior al nivel de riesgo aceptable (NRA), que es al que debe tender la compañía. Para la metodología se ha considerado que el NRA sea menor o igual a 4. Si el NR fuera superior al NRA, se procede a la selección de salvaguardas para la reducción del riesgo, realizando el proceso de forma recursiva hasta conseguir que el nivel de riesgo de la compañía sea el adecuado.

TABLA I. NIVELES DE RIESGO

NRA=<4	NA	Bajo			Medio			Alto		
	P	B	M	A	B	M	A	B	M	A
Valor activo	B	1	2	3	2	4	6	3	6	9
	M	2	4	6	4	8	12	6	12	18
	A	3	6	9	6	12	18	9	18	27

- *Nivel de control o cobertura:* Es el nivel de cumplimiento de un control de seguridad con respecto a un activo determinado, sometido a una amenaza, y que se obtiene a partir de las Ecuaciones 2 y 3. Este dato es fundamental para poder obtener el plan de mejora, ya que el sistema utilizará el valor de NCCAA para planificar el orden en que deben mejorarse los controles para minimizar los riesgos.

$$NCCAA(x,y,z) = \Sigma(VACAM)/NCAM$$

Siendo:

- ***NCCAA:*** Nivel de cobertura o cumplimiento que ofrecen los controles actuales ubicados en el sistema para un activo X frente a una amenaza Y con respecto al nivel de seguridad Z.
- ***NCAM:*** Número de controles afectados por la amenaza para ese nivel.
- ***VACAM:*** Valor actual del control afectado por la amenaza para cada uno de los niveles.

Ecuación 2. Nivel de cobertura de un control para el par activo–amenaza.

$$NCCA = \Sigma(NCCAA)/NAA$$

Siendo:

- ***NCCA:*** Nivel de cobertura que ofrecen los controles actuales ubicados en el sistema para un activo X frente a cualquier amenaza.
- ***NCCAA:*** Nivel de cobertura que ofrecen los controles actuales ubicados en el sistema para un activo X frente a una amenaza Y con respecto al nivel de seguridad Z.
- ***NAA:*** Número de amenazas que afectan al activo.

Ecuación 3. Nivel de cobertura de un control para un activo.

Para poder obtener de una forma sencilla el riesgo al que está sometido cada activo y el nivel de cobertura de cada control, se utilizará el algoritmo de Matriz de Riesgos (aMR) (ver Figura 8).

Algoritmo: Matriz de riesgos.

Esquema = Se selecciona el esquema de trabajo.

Empresa = Se selecciona la compañía sobre la que se realizará el SGSI.

SGSI = Se selecciona el SGSI para esa compañía.

Instancia del SGSI = Se selecciona la instancia concreta del SGSI.

1º.– Se obtiene el nivel de cobertura o cumplimiento de cada control de la ISO/IEC27002 por niveles, es decir el ***NCCA.***

2º.– Se obtiene el impacto de las amenazas para cada activo y nivel, mediante la asociación de las matrices con tipos de activos x amenazas x controles, obteniendo el nivel de cobertura media de los controles asociados al activo, la amenaza y el nivel y normalizando dichos controles como [>=0.75 – 1.00] => Impacto = Bajo, [>=0.25 – 0.75<] => Impacto = Medio, [>=0.00 – 0.25<] => Impacto = Alto.

3º.– Se obtiene la probabilidad de ocurrencia de una vulnerabilidad sobre un activo y un nivel, mediante la asociación de las matrices con tipos de activos x vulnerabilidades x amenazas x controles, obteniendo el nivel de cobertura media de los controles asociados al activo, la vulnerabilidad y el nivel y normalizando dichos controles como [0.75 – 1.00] => Probabilidad de ocurrencia = Bajo, [0.25 – 0.75] => Probabilidad de ocurrencia = Medio, [0.00 – 0.25] => Probabilidad de ocurrencia = Alto.

4º.– Se obtiene la matriz de riesgo, para obtener el nivel de riesgo de cada activo teniendo en cuenta las vulnerabilidades, amenazas y criterios de riesgos a los que está sometido, así como el nivel de cobertura de los controles asociados a éste. Para ello se multiplican todas las matrices asociadas activo x tipo activo x amenazas x vulnerabilidades x criterios riesgo x controles, asociados a las probabilidades de impacto y ocurrencia obtenidas en los puntos anteriores que determinarán el nivel de riesgo [1–27].

Figura 8. Pseudocódigo del algoritmo de matriz de riesgos.

Algoritmo: Plan de mejora.

Esquema = Se selecciona el esquema de trabajo.

Empresa = Se selecciona la compañía sobre la que se realizará el SGSI.

SGSI = Se selecciona el SGSI para esa compañía.

Instancia del SGSI = Se selecciona la instancia concreta del SGSI.

1º.– Mientras el nivel de riesgo sea mayor que el riesgo aceptable (NRA=<4)

1.1º.– Se recalcula la matriz de riesgo ordenada por nivel ascendente y riesgo descendente.

1.2º.– Queda algún elemento en la matriz de los niveles alcanzables cuyo riesgo sea inaceptable.

1.2.1º.– No => Salir del ciclo.

1.2.2º.– Si => Siguiente ciclo.

1.3º.– Se selecciona el primer registro de la matriz.

1.4º.– Se obtienen los controles asociados a ese registro de la matriz.

1.5º.– Se selecciona el control que menos nivel de cobertura tenga.

1.6º.– Se emite la recomendación completa de la evolución que supondría aplicar el control.

1.7º.– Se actualiza el control a nivel de cumplimiento = total, para que al recalcular la matriz se actualicen todos los pesos.

2º.– Fin ciclo.

Aclaración: *Con la modificación de cada control, se recalcula nuevamente toda la matriz, porque los niveles de riesgos se pueden ver alterados.*

Figura 9. Pseudocódigo del algoritmo del plan de mejora.

Una vez que se ha obtenido la matriz de riesgos, se utilizará junto con la información generada en las tareas anteriores para obtener el plan de mejora, mediante la aplicación del algoritmo del *Plan de Mejora (aPM)* (ver Figura 9).

Este algoritmo funciona de forma recursiva, determinando el activo de mayor riesgo en el menor nivel de madurez, y aplicando el control que permita mejorarlo con el menor coste, para posteriormente recalcular todo el proceso y seleccionar el siguiente mejor, hasta llegar al nivel de gestión de seguridad óptimo.

IV. HERRAMIENTA Y SU APLICACIÓN EN CASOS REALES.

Se ha desarrollado una aplicación capaz de dar soporte al proceso de análisis y gestión de riesgos, diseñado para las PYMES. Esta aplicación está dividida en dos zonas, que se ocupan de dar soporte a cada una de las actividades del proceso MARISMA-AGR.

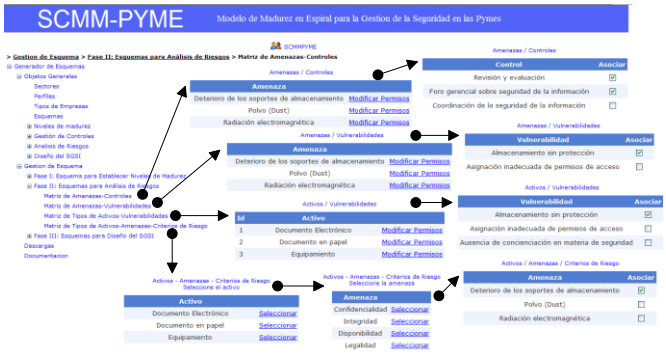


Figura 10. A1 – Pantalla de matrices del AR.

Dentro de la zona de gestión de esquemas de la aplicación se encuentra la gestión de "análisis de riesgos", que permitirá configurar los diferentes componentes básicos del análisis de riesgos añadiendo o eliminado nuevos elementos a estos componentes. Esta zona se corresponde con la primera actividad del proceso de AGR.

En la Figura 10 se puede ver cómo se asocian los componentes básicos del análisis de riesgos para establecer las relaciones entre ellos, que permitirán reducir los tiempos de generación del análisis de riesgos.

La realización del análisis de riesgos, al estar basada en la metodología desarrollada, tiene como única tarea destacable la introducción de los activos del sistema de información de la compañía (Figura 11), que deberán cuantificarse. Esta zona se corresponde con la segunda actividad del subproceso MARISMA-AGR.

A partir de los activos y los resultados obtenidos del nivel de cumplimiento de los controles de la ISO/IEC27002 [53], el modelo genera una completa matriz de los riesgos de la compañía de forma totalmente automática, para que el responsable de seguridad pueda tener un mapa completo de los riesgos, vulnerabilidades, amenazas y el nivel de cobertura de cada uno de los activos que componen el sistema de información de la compañía.

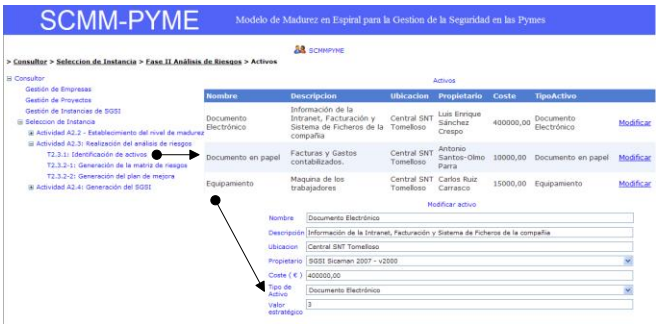


Figura 11. A2 – Pantalla de realización del AR.

La matriz generada por el modelo MARISMA para el caso real de la compañía Sicaman Nuevas Tecnologías (SNT) consta de 711 registros, pero por motivos de tamaño aquí se presentan sólo los 10 primeros. Como se puede ver en la Tabla II, la matriz de riesgos contiene una información muy completa sobre los riesgos actuales a los que está sometido el sistema de información de la compañía, que puede ser de gran utilidad para el responsable del departamento de informática y para el responsable de seguridad de cara a tomar decisiones.

TABLA II. MATRIZ DE RIESGOS DE SNT

Nivel	Nombre	Descripción	Coste (€)	Valor Estratégico	Tipo de Activo	Amenaza	Vulnerabilidad	Criterios de Riesgo	Impacto	Vulnerabilidad	Nivel de Riesgo	Nivel de Control
N1	Hw	Servidor	50,000	3	Hw	Fallo del hardware (soporte físico)	Servicio de mantenimiento inadecuado	D	A	M	6	0.21
N1	Hw	Servidor	50,000	3	Hw	Acción industrial	Servicio de mantenimiento inadecuado	D	M	M	5	0.69
N1	Hw	Servidor	50,000	3	Hw	Daño premeditado	Controles de acceso físico a las instalaciones inadecuados o inexistentes	D	M	M	5	0.65
N1	Hw	Servidor	50,000	3	Hw	Fallo/error de mantenimiento	Formación en materia de seguridad insuficiente	D	M	M	5	0.68

La matriz de riesgos contiene información detallada de los activos para cada nivel de madurez, y de cómo se ven afectados éstos según el tipo del activo, las amenazas a la que están sometidos dichos activos, las vulnerabilidades existentes y los criterios de riesgos que se han tomado en cuenta para

este activo. A partir de toda esta información se valora el impacto de cada amenaza sobre un activo, y la probabilidad de ocurrencia de cada vulnerabilidad, lo que permite establecer un nivel de riesgo que se asociará al nivel de control de la compañía para determinar cómo acometer posteriormente un plan de mejora.

A partir de la matriz de riesgos, el sistema es capaz de proponer una serie de pasos para aumentar el nivel de seguridad de la compañía en el menor tiempo posible, incluidos en un plan de mejora (Tabla III). Para ello, y mediante un algoritmo recursivo basado en los riesgos de los activos, analiza los controles que deben acometerse en cada momento para llegar a un nivel de riesgo aceptable.

Para el caso de SNT, el sistema requiere de 48 pasos para alcanzar un nivel de riesgo aceptable para el S.I. de la compañía. Por motivos de espacio se muestran solo los primeros pasos del plan de mejora.

TABLA III. PLAN DE MEJORA PARA SNT

Paso 1: El nivel actual de la compañía es nivel1 con un riesgo máximo en este nivel de 6. El activo más afectado por este riesgo es: hardware (servidores) cuya pérdida tendría un coste para la organización de 50.000€ y cuyo valor estratégico para la compañía es de 3 sobre 7, siendo el tipo del activo "hardware". El nivel de riesgo de este activo para la amenaza "fallo del hardware (soporte físico)" es de 6 contando actualmente el sistema con un nivel de cobertura de controles de 0.21, por lo que se recomienda acometer la activación del control [10.7.2] (retirada de soportes.).
Paso 2: El nivel actual de la compañía es nivel 1 con un riesgo máximo en este nivel de 6. El activo más afectado por este riesgo es: hardware (servidores) cuya pérdida tendría un coste para la organización de 50.000€ y cuyo valor estratégico para la compañía es de 3 sobre 7, siendo el tipo del activo "hardware". El nivel de riesgo de este activo para la amenaza "fallo del hardware (soporte físico)" es de 6 contando actualmente el sistema con un nivel de cobertura de controles de 0.21, por lo que se recomienda acometer la activación del control [10.5.1] (copias de seguridad de la información.).
Paso 3: El nivel actual de la compañía es nivel 1 con un riesgo máximo en este nivel de 5. El activo más afectado por este riesgo es: medios de soporte (copias de seguridad.) cuya pérdida tendría un coste para la organización de 100.000€ y cuyo valor estratégico para la compañía es de 3 sobre 7, siendo el tipo del activo "medios de soporte". El nivel de riesgo de este activo para la amenaza "fallo en la ruta de los mensajes" es de 5 contando actualmente el sistema con un nivel de cobertura de controles de 0.50, por lo que se recomienda acometer la activación del control [12.3.1] (política de uso de los controles criptográficos.).

V. CONCLUSIONES.

En este artículo se ha presentado la propuesta de un proceso para realizar el análisis y gestión del riesgo en las PYMES denominado MARISMA-ARG, que permite soportar los resultados generados durante la investigación y que cumple con los objetivos perseguidos.

El análisis de riesgos para las PYMES deberá tener un coste de generación y mantenimiento muy reducido, aún a costa de sacrificar precisión en el mismo, pero siempre manteniendo unos resultados con la calidad suficientes.

Se ha definido cómo se puede utilizar este proceso y las mejoras que ofrece con respecto a otros modelos que afrontan el problema de una forma más precisa y detallada, pero también más costosa, lo que no las hace válidas para el caso de las PYMES.

Las características ofrecidas por el proceso y su orientación a las PYMES ha sido muy bien recibida, y su aplicación está resultando muy positiva ya que permite a este tipo de empresas realizar una adecuada gestión del riesgo al que están sometidos los activos de su sistema de información. Además, con este proceso se obtienen resultados a corto plazo y se reducen los costes que supone el uso de otros procesos, consiguiendo un mayor grado de satisfacción de la empresa.

El proceso MARISMA-AGR cumple con los objetivos propuestos, así como con los principios que según la OCDE [76] debe seguir todo proceso de evaluación del riesgo, según el cual el sistema debe tener la capacidad de autoevaluar su riesgo de forma continuada en el tiempo, proponiendo medidas.

Finalmente, se considera que el trabajo realizado debe ser ampliado con nuevas especificaciones, nuevos esquemas, mejorando los algoritmos de análisis y gestión del riesgo de forma que puedan ofrecer planes más detallados y profundizando en el proceso con nuevos casos de estudio.

La mayor parte de las futuras mejoras del proceso se están orientando a mejorar la precisión del mismo, pero siempre respetando el principio de coste de recursos, es decir, se busca mejorar el proceso sin incurrir en costes de generación y mantenimiento del análisis de riesgos.

AGRADECIMIENTOS

Esta investigación ha sido co-financiada es parte por los proyectos SIGMA-CC (TIN2012-36904) y GEODAS (TIN2012-37493-C03-01) financiados por el "Ministerio de Economía y Competitividad y Fondo Europeo de Desarrollo Regional FEDER" (España), del proyecto SERENIDAD (PEII14-2014-045-P) financiados por la "Consejería de Educación, Ciencia y Cultura de la Junta de Comunidades de Castilla-la Mancha y el Fondo Europeo de Desarrollo Regional FEDER" (España), del proyecto "Plataformas Computacionales de Entrenamiento, Experimentación, Gestión y Mitigación de Ataques a la Ciberseguridad - Código: ESPE-2015-PIC-019" financiado por la ESPE y CEDIA (Ecuador), y del proyecto PROMETEO financiado por la Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT) del Gobierno de Ecuador.

Referencias

[1] Wiander, T. *Implementing the ISO/IEC 17799 standard in practice – experiences on audit phases.* in *AISC '08: Proceedings of the sixth Australasian conference on Information security*. 2008. Wollongong, Australia.

[2] Johnson, M., *Cybercrime: Threats and Solutions*, 2014.

[3] Von Solms, R., *Information security management: processes and metrics*, 2014.

[4] Wiander, T. and J. Holappa, *Theoretical Framework of ISO 17799 Compliant. Information Security Management System Using Novel ASD Method.*, in *Technical Report*, V.T.R.C.o. Finland, Editor 2006.

[5] Whitman, M. and H. Mattord, *Principles of information security*2011: Cengage Learning.

[6] Kluge, D. *Formal Information Security Standards in German Medium Enterprises.* in *CONISAR: The Conference on Information Systems Applied Research.* 2008.

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

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

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

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

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

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

[13] Jürjens, J. *Towards Development of Secure Systems using UML*. in *International Conference on the Fundamental Approaches to Software Engineering (FASEiTAPS)*. 2001. Springer.

[14] Masacci, F., M. Prest, and N. Zannone, *Using a security requirements engineering methodology in practice: The compílanse with the Italian data protection legislation.* Computer Standards & Interfaces, 2005. **27**: p. 445-455.

[15] Walker, E., *Software Development Security: A Risk Management Perspective*. The DoD Software Tech. Secure Software Engineering, 2005. **8**(2): p. 15-18.

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

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

[18] Cholez, H. and F. Girard, *Maturity assessment and process improvement for information security management in small and medium enterprises.* Journal of Software: Evolution and Process, 2014. **26**(5): p. 496-503.

[19] Spinellis, D. and D. Gritzalis. *Information Security Best Practise Dissemination: The ISA-EUNET Approach*. in *WISE 1:First World Conference on Information Security Education*. 1999.

[20] Candiwan, C. *Analysis of ISO27001 Implementation for Enterprises and SMEs in Indonesia*. in *The International Conference on Cyber-Crime Investigation and Cyber Security (ICCICS2014)*. 2014. The Society of Digital Information and Wireless Communication.

[21] Sánchez, L.E., et al., *Managing Security and its Maturity in Small and Medium-sized Enterprises.* J. UCS, 2009. **15**(15): p. 3038-3058.

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

[23] Puma, J.P., et al. *Mobile Identification: NFC in the Healthcare Sector*. in *Andean Region International Conference (ANDESCON), 2012 VI*. 2012.

[24] Vivas, T., et al., *Aplicación de Mecanismos de Seguridad en una Red de Telemedicina Basados en Certificados Digitales*, in *IV Latin American Congress on Biomedical Engineering 2007, Bioengineering Solutions for Latin America Health*, C. Müller-Karger, S. Wong, and A. La Cruz, Editors. 2008, Springer Berlin Heidelberg. p. 971-974.

[25] Alebrahim, A., D. Hatebur, and L. Goeke. *Pattern-based and ISO 27001 compliant risk analysis for cloud systems*. in *Evolving Security and Privacy Requirements Engineering (ESPRE), 2014 IEEE 1st Workshop on*. 2014.

[26] Dimopoulos, V., et al. *Approaches to IT Security in Small and Medium Enterprises*. in *2nd Australian Information Security Management Conference, Securing the Future*. 2004. Perth, Western Australia: 73-82.

[27] Holappa, J. and T. Wiander, *Practical Implementation of ISO 17799. Compliant Information Security Management System Using Novel ASD Method.*, in *Technical Report*, V.T.R.C.o. Finland, Editor 2006.

[28] Llvonen, L. *Information Security Management in Finnish SMEs*. in *5th European Conference on Information Warfare and Security National Defence College*. 2006. Helsinki, Finlan: 1-2 June 2006.

[29] ISO/IEC17799, *ISO/IEC 17799, Information Technology - Security Techniques - Code of practice for information security management*, 2000.

[30] ISO/IEC27001, *ISO/IEC 27001:2013, Information Technology - Security Techniques Information security management systemys - Requirements.*, 2013.

[31] Shaw, M., *What makes good research in software engineering?* International Journal on Software Tools for Technology Transfer (STTT), 2002. **4**(1): p. 1-7.

[32] Dimopoulos, V., et al. *Factors affecting the adoption of IT risk analysis*. in *Proceedings of 3rd European Conference on Information Warfare and Security*. 2004. Royal Holloway, University of London: 28-29 June 2004.

[33] 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.

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

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

[36] Bugdol, M. and P. Jedynak, *Integration of Standardized Management Systems*, in *Integrated Management Systems*2015, Springer International Publishing. p. 129-160.

[37] Barrientos, A.M. and K.A. Areiza, *Integration of a safety management system withan information quality management system.*, in *Master's thesis*2005, Universidad EAFIT.

[38] Lund, M.S., F.d. Braber, and K. Stolen, *Proceedings of the Seventh European Conference On Software Maintenance And Reengineering (CSMR'03).* IEEE, 2003.

[39] Fredriksen, R., et al. *The CORAS framework for a model-based risk management process*. in *21st International Conference on Computer Safety, Reliability and Security (Safecomp 2002)*. 2002. Springer: LNCS 2434.

[40] ISBS, *Information Security Breaches Survey 2006*. Department of Trade and Industry2006, UK.

[41] Sánchez, L.E., et al. *Security Management in corporative IT systems using maturity models, taking as base ISO/IEC 17799.* in *International Symposium on Frontiers in Availability, Reliability and Security (FARES'06) in conjunction with ARES*. 2006. Viena (Austria).

[42] Sánchez, L.E., et al. *MMISS-SME Practical Development: Maturity Model for Information Systems Security Management in SMEs.* in *9th International Conference on Enterprise Information Systems (WOSIS'07).* 2007b. Funchal, Madeira (Portugal). June.

[43] Sánchez, L.E., et al. *Developing a model and a tool to manage the information security in Small and Medium Enterprises*. in *International Conference on Security and Cryptography (SECRYPT'07).* 2007a. Barcelona. Spain.: Junio.

[44] Sánchez, L.E., et al. *Developing a maturity model for information system security management within small and medium size enterprises.* in *8th International Conference on Enterprise Information Systems (WOSIS'06)*. 2006. Paphos (Chipre). March.

[45] Sánchez, L.E., et al. *SCMM-TOOL: Tool for computer automation of the Information Security Management Systems*. in *2nd International conference on Software and Data Technologies (ICSOFT'07).* . 2007c. Barcelona-España Septiembre.

[46] Sánchez, L.E., et al. *Practical Application of a Security Management Maturity Model for SMEs Based on Predefined Schemas.* in *International Conference on Security and Cryptography (SECRYPT'08).* 2008. Porto–Portugal.

[47] Gupta, A. and R. Hammond, *Information systems security issues and decisions for small businesses.* Information Management & Computer Security, 2005. **13**(4): p. 297-310.

[48] V3, M., *Methodology for Information Systems Risk Analysis and Management (MAGERIT version 3)*, 2012, Ministerio de Administraciones Públicas (Spain).

[49] Alberts, C.J. and A.J. Dorofee, *Managing Information Security Risks: The OCTAVE Approach.*, ed. A.-W.P. Co.2002.

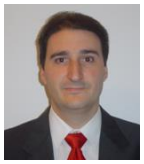
[50] CRAMMv5.0, *CRAMM v5.0, CCTA Risk Analysis and Management Method.*, 2003.
[51] Gerber, M. and R. Von Solms, *Management of risk in the information age*. Computers & Security, 2005. **24**(1): p. 16-30.
[52] ISO/IEC27005, *ISO/IEC 27005:2011, Information Technology - Security Techniques - Information Security Risk Management Standard (under development).* 2011.
[53] ISO/IEC27002, *ISO/IEC 27002:2013, the international standard Code of Practice for Information Security Management (en desarrollo).* 2013.
[54] Disterer, G., *Iso/iec 27000, 27001 and 27002 for information security management*. 2013.
[55] Beckers, K., et al., *Supporting the Development and Documentation of ISO 27001 Information Security Management Systems through Security Requirements Engineering Approaches*, in *Engineering Secure Software and Systems*, G. Barthe, B. Livshits, and R. Scandariato, Editors. 2012, Springer Berlin Heidelberg. p. 14-21.
[56] ISO/IEC13335-3, *ISO/IEC TR 13335-3, Information technology -- Guidelines for the management of IT Security -- Part 3: Techniques for the management of IT Security.*, 1998.
[57] ISO/IEC13335-4, *ISO/IEC TR 13335-4, Information technology -- Guidelines for the management of IT Security -- Part 4: Selection of safeguards.*, 2000.
[58] SSE-CMM, *Systems Security Engineering Capability Maturity Model (SSE-CMM), Version 3.0. Department of Defense. Arlington VA. 326.*, 2003.
[59] ISO/IEC21827, *ISO/IEC 21827:2008, Information technology - Systems Security Engineering - Capability Maturity Model (SSE-CMM)*, 2008, ISO/IEC. p. 123.
[60] ISO/IEC15443-1, *ISO/IEC TR 15443-1:2012, Information technology -- Security techniques -- A framework for IT security assurance -- Part 1: Overview and framework.*, 2012.
[61] ISO/IEC15443-2, *ISO/IEC TR 15443-2:2012, Information technology -- Security techniques -- A framework for IT security assurance -- Part 2: Assurance methods.*, 2012.
[62] ISO/IEC-CCv3.1, *Common Criteria for Information Technology Security Evaluation.*, 2007.
[63] ISO/IEC20000-1, *ISO/IEC 20000-1:2011, Information technology - Service management - Part 1: Specification.*, 2011.
[64] ISO/IEC20000-2, *ISO/IEC 20000-2:2012, Information technology - Service management - Part 2: Code of practice.*, 2012.
[65] COBITv5.0, *Cobit Guidelines, Information Security Audit and Control Association*, ISACA, Editor 2013.
[66] Batista, J. and A. Figueiredo, *SPI in very small team: a case with CMM.* Software Process Improvement and Practice, 2000. **5**(4): p. 243-250.
[67] Hareton, L. and Y. Terence, *A Process Framework for Small Projects.* Software Process Improvement and Practice, 2001. **6**: p. 67-83.
[68] Tuffley, A., B. Grove, and M. G, *SPICE For Small Organisations.* Software Process Improvement and Practice, 2004. **9**: p. 23-31.
[69] 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.
[70] Mekelburg, D., *Sustaining Best Practices: How Real-World Software Organizations Improve Quality Processes.* Software Quality Professional, 2005. **7**(3): p. 4-13.
[71] ISO/IEC13335-5, *ISO/IEC TR 13335-5, Information technology -- Guidelines for the management of IT Security -- Part 5: Management guidance on network security.*, 2001.
[72] Santos-Olmo, A., et al., *A Systematic Review of Methodologies and Models for the Analysis and Management of Associative and Hierarchical Risk in SMEs*, in *9th International Workshop on Security in Information Systems (WOSIS12) In conjunction with 11th International Conference on Enterprise Information Systems (ICEIS12).*2012: Wroclaw, Poland. p. 117 -124.
[73] Sanchez, L.E., et al., *ISMS Building for SMEs through the Reuse of Knowledge.* Small and Medium Enterprises: Concepts, Methodologies, Tools, and Applications, 2013: p. 394.
[74] Sánchez, L.E., et al. *Building ISMS Through Knowledge Reuse.* in *7th International Conference on Trust, Privacy & Security in Digital Business (TRUSTBUS'10).* 2010. Bilbao, Spain.
[75] Santos-Olmo, A., et al., *Desirable Characteristics for an ISMS Oriented to SMEs.*, in *8th International Workshop on Security in Information Systems (WOSIS11) In conjunction with 11th International Conference on Enterprise Information Systems (ICEIS11)*2011: Beijing, China. p. 151-158.
[76] OECD, *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.*, O.f.E.C.-o.a.D. (OECD). Editor 2002: Paris.

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 an Professor at the Universidad de las Fuerzas Armadas (ESPE) of Latacunga (Ecuador), MSc in Information Systems Audit from the Polytechnic University of Madrid, and Certified Information System Auditor by ISACA. He is the Director of Professional Services and R&D departments of the company Sicaman Nuevas Tecnologías S.L. COIICLM board or committee member and responsible for the professional services committee. His research activities are management security system, security metrics, data mining, data cleaning, and business intelligence. He participates in the GSyA research group of the Department of Computer Science at the University of Castilla-LaMancha, in Ciudad Real (Spain).

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).

Monica Karel Huerta is PhD in Telematic Engineering from Polytechnic University of Catalonia (Spain) in 2006 with the distinction of Cum-laude. Also she is MSc in Biomedical Engineering and Electrical Engineer from Simon Bolivar University (USB) in 1999 and 1994 respectively. She was Professor, Dean of Graduate Studies and Coordinator of the Doctorate in Engineering at USB. She was the founder of Networks and Telematics group in USB. She is a senior member of the IEEE, and belongs at Women in Engineering, Communications and Engineering in Medicine and Biology societies. She is currently professor at the Salesian University (Ecuador).



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.