IX Congreso iberoamericano
de seguridad informática
Universidad de Buenos Aires
Ciudad Autónoma de Buenos Aires, Argentina
1 al 3 de noviembre de 2017

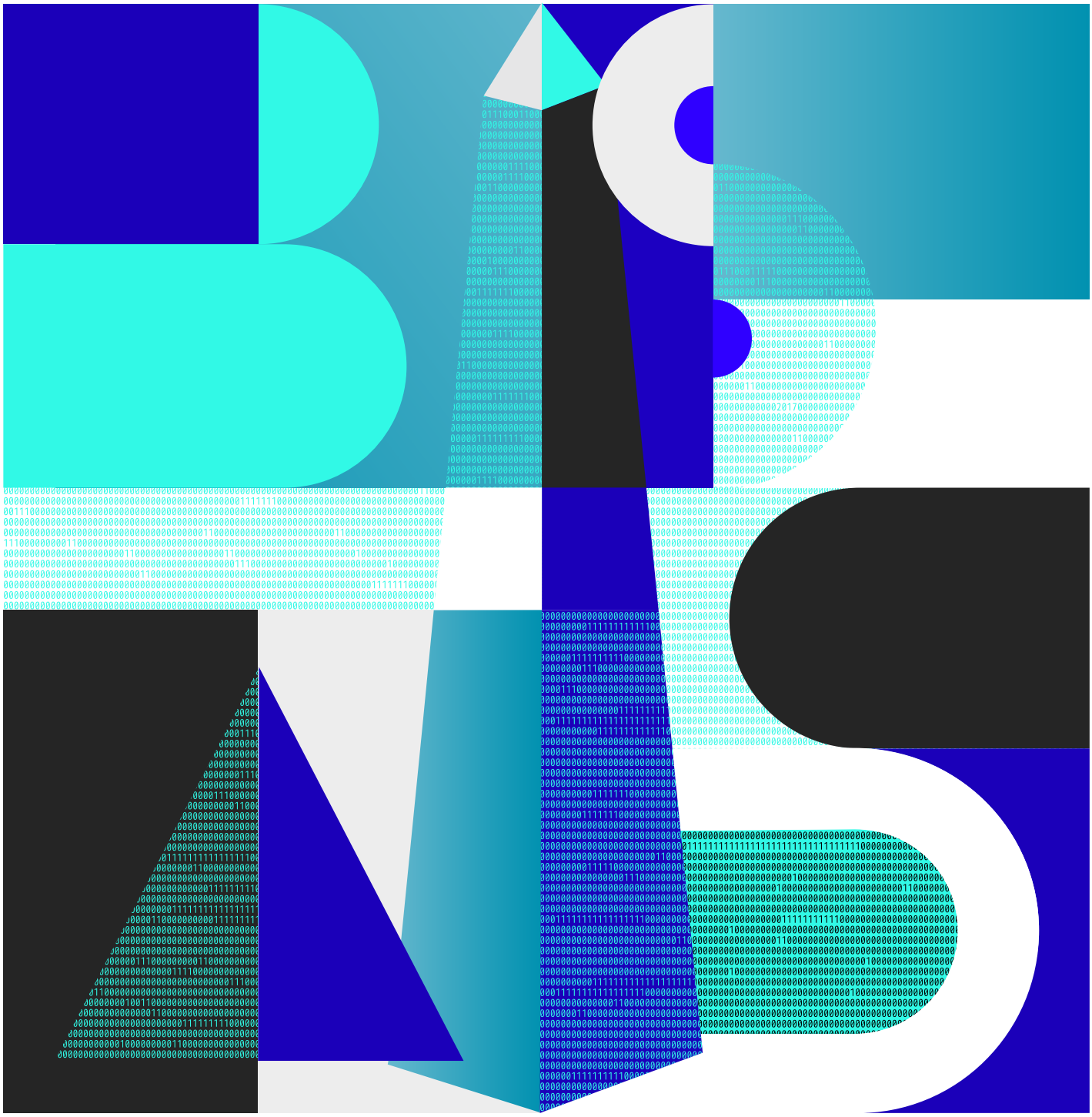
CIBSI

EU DE BA

PSI
POSGRADO EN SEGURIDAD INFORMATICA

CRIPTORED

Libro de Actas



Actas del IX Congreso Iberoamericano de Seguridad Informática
CIBSI2017, Buenos Aires, Argentina, 1 al 3 de Noviembre de 2017

Editores
Alberto E. Dams
Hugo A. Pagola
Luis E. Sánchez Crespo
Jorge Ramió Aguirre

Diseño de Tapas
Federico Dams

ISBN: en trámite

Prefacio

Del 1 al 3 de Noviembre se celebrará en la Universidad de Buenos Aires el IX Congreso Iberoamericano de Seguridad Informática - CIBSI 2017. El congreso está organizado por la Maestría en Seguridad Informática de la UBA en colaboración con la Red Temática Iberoamericana de Criptografía y Seguridad de la Información Criptored.

Este espacio permitirá a las empresas, entidades públicas, entornos militares, de defensa, centros académicos y de investigación exponer sus avances y servicios vinculados con la seguridad, facilitando el intercambio de conocimientos y la formación de redes de colaboración en este ámbito.

El congreso contará con la presencia de especialistas de Latinoamérica y de Europa entre otros de Argentina, Brasil, Colombia, Ecuador, México, Perú, Uruguay, España y Francia. Estamos muy satisfechos por el nivel de los artículos que se presentarán y el de los invitados especiales que tendremos. En esta novena edición del CIBSI, se destacan las presencias de referentes internacionales en la materia como Hugo Scolnik director de la Maestría en seguridad Informática de la UBA y Hugo Krawczyk Distinguished Research Staff Member with the Cryptography Group at the IBM T.J. Watson Research Center.

Organización de la Conferencia

Comité Organizador

Hugo Pagola, Facultad de Ingeniería Universidad de Buenos Aires, Argentina
Alberto Dams, Facultad de Ingeniería Universidad de Buenos Aires, Argentina
Jorge Ramió Aguirre, Universidad Politécnica de Madrid, España
Luis E. Sánchez Crespo, Universidad de Castilla La Mancha, España

Comité Local

Facundo Caram, FIUBA, Argentina
Luis Catanzariti, UTNfrba, Argentina
Marcia Maggiore, MUBA, Argentina
Patricia Prandini, MUBA, Argentina

Comisión de Posgrado Maestría en Seguridad Informática UBA

Mg Ing Alberto Dams, Maestria en Seguridad Informatica UBA, FIUBA, Argentina
Dr Pedro Hecht, Maestria en Seguridad Informatica UBA, Argentina
Ing Hugo Pagola, Maestria en Seguridad Informatica UBA, FIUBA, Argentina
Dr Ricardo Rivas, Maestria en Seguridad Informatica UBA, FCE-UBA Argentina
Dr Raul Saroka, Maestria en Seguridad Informatica UBA, FCE-UBA Argentina
Dr Hugo Scolnik, Maestria en Seguridad Informatica UBA, FCEN-UBA Argentina

Comité del Programa

Marco Aurélio Amaral Henriques	State University of Campinas - Unicamp, Brasil
Javier Areitio	Universidad de Deusto, España
Rodolfo Baader	Universidad de Buenos Aires, Argentina
Gustavo Betarte	Facultad de Ingeniería, Universidad de la República, Uruguay
Carlos Blanco Bueno	Universidad de Cantabria, España
Joan Borrell	Universitat Autònoma de Barcelona, España
Pino Caballero-Gil	DEIOC, Universidad de La Laguna, España
Jeimy Cano	Universidad de los Andes, Colombia
Eduardo Carozo	Universidad de Montevideo, Uruguay
Joan-Josep Climent	Universitat d'Alacant, España
Roger Clotet	Universidad Simón Bolívar, Venezuela
Alberto Dams	Universidad de Buenos Aires, Argentina
José María De Fuentes	Universidad Carlos III de Madrid, España
Josep Domingo-Ferrer	Universitat Rovira i Virgili, España
Jose-Luis Ferrer-Gomila	University of the Balearic Islands, España
Angelica Florez Abril	Universidad Pontificia Bolivariana, Colombia
Walter Fuertes	Universidad de las Fuerzas Armadas ESPE, Ecuador
Amparo Fuster-Sabater	Institute of Applied Physics, Madrid, España
Giovana Garrido	Universidad Tecnologica de Panama
Lorena González Manzano	Universidad Carlos III de Madrid, España
Juan Pedro Hecht	Universidad de Buenos Aires, Argentina

Luis Hernandez Encinas	Institute of Physical and Information Tecnologies, España
Emilio Hernández	Universidad Simón Bolívar, Venezuela
Leobardo Hernández	Universidad Nacional Autónoma de México
Jordi Herrera	Universitat Autònoma de Barcelona, España
Monica Karel Huerta	Universidad Politécnica Salesiana, Ecuador
Angel Martin Del Rey	Universidad de Salamanca, España
Maria Vanina Martinez	Universidad Nacional del Sur in Bahia Blanca, Argentina
Vincenzo Mendillo	Universidad Central de Venezuela
Gaspar Modelo-Howard	Universidad Tecnológica de Panamá
Raul Monge	Universidad Técnica Federico Santa María, Chile
Karel Huerta Monica	Universidad Politécnica Salesiana, Ecuador
Guillermo Morales-Luna	Centro de Investigación y Estudios Avanzados, Mexico
Alfonso Muñoz	Criptored, España
Hugo Pagola	UBA - Facultad de Ingenieria, Argentina
Graciela Pataro	Universidad de Buenos Aires, Argentina
Alberto Peinado	Universidad de Malaga, España
Jose Pirrone	Universidad Catolica Andres Bello, Venezuela
Gustavo Presman	Universidad de Buenos Aires, Argentina
Jorge Ramio	Universidad Politécnica de Madrid, España
Ricardo Rivas	Universidad de Buenos Aires, Argentina
David Rosado	University of Castilla-La Mancha, España
Luis Enrique Sanchez Crespo	Universidad de Castilla La Mancha, España
Antonio Santos-Olmo Parra	Sicaman Nuevas Tecnologías
Raul Saroka	Universidad de Buenos Aires, Argentina
Hugo Scolnik	Universidad de Buenos Aires, Argentina
Pablo Silberfich	Universidad de Buenos Aires, Argentina
Jenny Torres	Escuela Politécnica Nacional, Ecuador
Urko Zurutuza	Mondragon University, España

Proceso para Generación de Análisis de Riesgo de Bajo Coste Utilizando los Patrones Reutilizables de MARISMA

L. E. Sánchez, A. Santos-Olmo, S. Camacho, I. Caballero, E. Fernandez-Medina

***Abstract* – The information society is increasingly dependent on Information Systems Security Management (ISMS) and knowledge of the security risks associated with the value of its assets. However, very few risk analysis methodologies have been produced so as to create systems with which to analyze risks in a rapid and economical manner and which can, in turn, leave this system dynamically updated. This paper presents the "generation of analysis and risk treatment plan" process of the MARISMA methodology. This process allows a reusable and low cost risk analysis to be obtained. The objective of MARISMA is to carry out a simplified and dynamic risk analysis that will be valid for all companies, including SMEs, and to provide solutions to the problems identified during the application of the "Action Research" scientific method. This methodology is being directly applied to real cases, thus allowing a constant improvement to be made to its processes.**

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

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 [6-8]. 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 [9-16], por citar sólo algunos.

Algunos autores [17, 18] sugieren la realización de un análisis de riesgos como parte fundamental en las PYMES, 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 [19].

Estudios centrados en la evaluación de riesgos [20-22], 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. Asimismo, 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/IEC27001:2013 [23]. Esto, junto con la escasa proporción 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 [24], y que una evaluación de la situación actual requiere de herramientas de análisis de riesgos [25] 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.

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

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

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

S. Camacho, Universidad Técnica Ambato, Ecuador, saracamachoestrada1@yahoo.es

I. Caballero, Grupo de Investigación Alarcos, Universidad de Castilla-la Mancha, Ciudad Real España, Ismael.Caballero@uclm.es

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

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 [26].

Las principales conclusiones obtenidas es que los modelos de análisis y gestión del riesgo son fundamentales para los SGSIs (Sistemas de Gestión de Seguridad de la Información), pero no existen metodologías que se adecuen al caso de las PYMES, y las existentes se muestran ineficientes.

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 [27-29], y además hemos construido una herramienta que automatiza completamente la metodología [30], y lo hemos aplicado en casos reales [31], 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 ésta, que define los controles que deben cumplirse. Por lo tanto, y aunque esta metodología nace para poder extenderse a otros estándares internacionales, actualmente sólo 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 nuestra propuesta para el proceso de generación de análisis y tratamiento del riesgo utilizando MARISMA. Finalmente, en la Sección 4 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 son ineficientes para 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 [32].

Entre las principales propuestas para el análisis y gestión del riesgo podemos destacar MAGERIT v3 [33], OCTAVE [34] o CRAMM [35]. A pesar de ello, la gestión de la seguridad no puede limitarse al análisis y la gestión del riesgo [36], 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 [37]. 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 [38], 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 [39]:* Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC27001 [23] y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.
- *ISO/IEC21827/SSE–CMM [40, 41]:* 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.
- *ISO/IEC 15443 [42, 43]:* Clasifica los métodos existentes dependiendo del nivel de seguridad y de la fase del aseguramiento.
- *ISO/IEC2000/ITIL [44, 45]:* 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.
- *COBIT [46]:* 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.

El principal problema de estos procesos es su complejidad para aplicarlos en el caso de las PYMES, ya que han sido concebidos para grandes empresas [47-50]. 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 [51].

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 hasta el momento.

III. METODOLOGÍA MARISMA

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 GAGR. 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 [52, 53], y bajo la premisa de que cualquier sistemas de Análisis de Riesgos valido para las PYMES también será extrapolable a grandes compañías. El objetivo de este proceso es el de generar un análisis de riesgos de bajo coste mediante la utilización de patrones reutilizables.

Mediante la metodología MARISMA, podemos asociar el análisis y la gestión del riesgo a los controles necesarios para la gestión de la seguridad y consta de tres procesos muy importantes:

- *Proceso 1 – Generación de Esquemas para el Análisis de Riesgos (GEAR -o GEGS: Generación de Esquemas para Gestión de Seguridad-):* 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 [54].
- *Proceso 2 – Generación del Análisis y Gestión del Riesgo (GAGR -o GSGS: Generación del Sistema de Gestión de Seguridad-):* 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).
- *Proceso 3 – Mantenimiento Dinámico del Análisis de Riesgos (MDAR -o MSGS: Mantenimiento del Sistema de Gestión de Seguridad-):* Mediante la utilización de las matrices generadas, las cuáles interconectan los diferentes artefactos, el sistema irá recalculando el análisis de riesgos según se produzcan incidentes de seguridad, fallen las métricas definidas o los auditores detecten "no conformidades" en los controles.

En este artículo nos centramos en el segundo de los procesos que tiene por objetivo la generación del análisis de riesgos propiamente dicho y de un plan de tratamiento de riesgos automatizado que permita generar y mantener análisis de riesgos de bajo coste.

IV. GAGR. PROCESO DE GENERACIÓN DE ANÁLISIS DE RIESGOS CON MARISMA

El principal objetivo de este subproceso es permitir la generación de los elementos que formarán el sistema de gestión de la seguridad (SGSI) para una compañía, a partir de un esquema (estructura generada mediante el subproceso GEAR) válido para un conjunto de compañías, realizando este proceso con un reducido coste.

Es importante mencionar que este subproceso ha sido desarrollado para que, a partir de un conjunto mínimo de información de la compañía (organigrama, lista de usuarios del sistema de información, roles, listas de verificación y lista de activos), se pueda generar una serie de documentos (nivel de seguridad actual, nivel de seguridad recomendable, matriz de riesgos, plan de mejora, elementos de un SGSI) que dejen el sistema de gestión completamente definido y funcional.

En la Figura 1 se puede ver el esquema básico de entradas, actividades y salidas que componen este subproceso:

- *Entradas:* Como entradas se recibirá un esquema de los existentes en el repositorio de esquemas, que se adecue a las características de la compañía sobre la que se quiere generar el SGSI, así como información de la empresa de tipo técnico y empresarial.
- *Actividades:* El subproceso estará formado por cuatro actividades. Las actividades A2.2 y A2.3 no podrán realizarse hasta la finalización de la A2.1 ya que requieren de elementos generados por ésta para su correcto funcionamiento. La actividad A2.4 depende de elementos generados por las actividades A2.2 y A2.3, por lo que tendrá que esperar a la finalización.
- *Salidas:* La salida producida por este subproceso consistirá en un conjunto de elementos seleccionados a partir del esquema y de la información introducida, así como un conjunto de informes con información sobre el estado actual de la compañía y las medidas que se tendrán que tomar para mejorar el nivel de gestión de la seguridad.

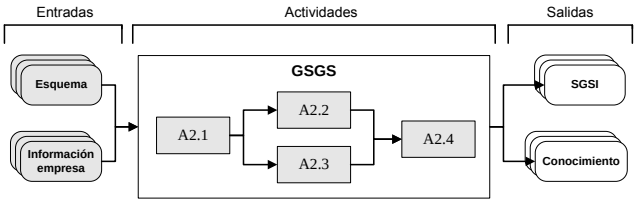


Figura 1. Esquema simplificado a nivel de actividad del subproceso GAGR.

El generador de SGSIs se puede considerar una importante aportación de la metodología desarrollada, ya que permite generar los elementos que componen el SGSI con un coste muy reducido.

En la Figura 2 se muestran las actividades del subproceso de forma mucho más detallada, viendo cómo interactúan éstas con el repositorio de SGSIs encargado de contener los elementos que conforman los diferentes SGSIs generados:

- *A2.1 – Establecimiento del marco inicial de trabajo:* Esta actividad se ocupa de tareas básicas pero necesarias para crear un marco de trabajo inicial entre el consultor de seguridad (CoS) encargado de la generación del SGSI y la compañía objetivo del mismo. Las tareas incluidas en esta actividad son: i) nombramiento de un interlocutor válido; ii) análisis

del organigrama de la compañía; iii) adaptación de la lista de usuarios del sistema de información y los roles desempeñados por cada uno de ellos al SGSI.

- *A2.2 – Establecimiento del nivel de madurez:* Esta actividad se ocupa de establecer el punto inicial en que se encuentra la compañía con respecto a la gestión de la seguridad (nivel de madurez actual) y el punto que sería deseable que la compañía alcanzara (nivel de madurez deseable).
- *A2.3 – Realización del análisis de riesgos:* Esta actividad permite identificar los activos de la compañía y obtener una evaluación del riesgo al que están sometidos estos activos, así como un plan de mejora recomendando en qué controles debe la compañía volcar sus esfuerzos para mejorar de la forma más eficiente el nivel de seguridad.
- *A2.4– Generación del SGSI:* Esta actividad tiene como objetivo generar los elementos que formarán el SGSI de la compañía a partir del esquema seleccionado y de toda la información recogida en las actividades anteriores.

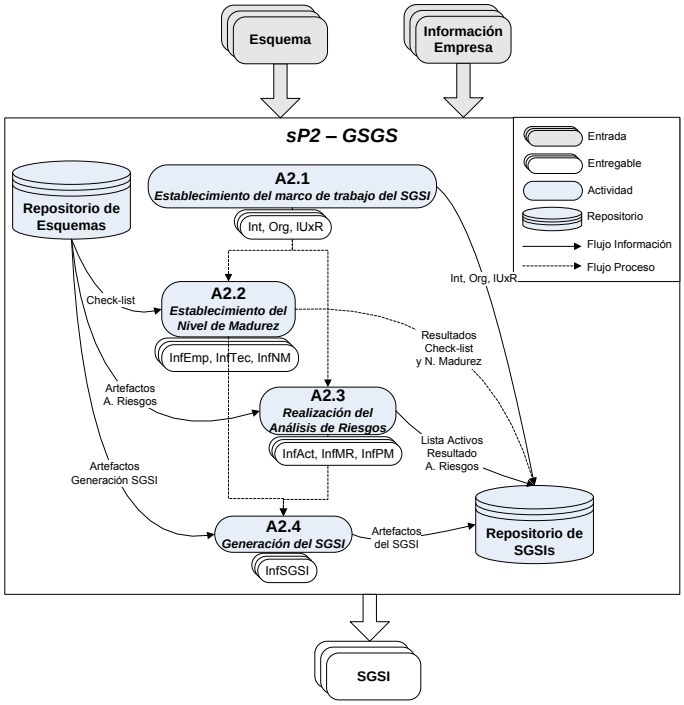


Figura 2. Esquema detallado a nivel de actividad del proceso GAGR.

Al contrario que en el subproceso GEAR, aquí la información generada, además de almacenarse en el repositorio de esquemas, genera documentos entregables para que el consultor de seguridad (Cos) y el interlocutor (Int) puedan analizar y validar los resultados obtenidos.

A. Objetivos.

Los principales objetivos que se han perseguido durante el desarrollo de las actividades que conforman este subproceso han sido:

- Incorporación de un conjunto de información básica y precisa de la compañía, que permita establecer un punto de seguridad inicial, un punto de seguridad deseado y la estructura necesaria para evolucionar la gestión de la seguridad.
- Selección del esquema adecuado para el tipo de compañía.
- Simplicidad del proceso y eficiencia en recursos, principalmente en coste y tiempo.

B. Entrada y salida.

La generación de esquemas es un subproceso cuyas entradas se componen de:

- *Un esquema base seleccionado del repositorio de esquemas:* Este esquema permitirá generar un SGSI adecuado para la compañía con un coste muy reducido.
- *Interlocutor (Int) para la compañía:* Será el interlocutor nombrado por la alta dirección para aportar toda la documentación al consultor de seguridad (CoS) a lo largo del proceso de generación del SGSI.
- *Información básica de la empresa:* La metodología desarrollada requiere sólo del organigrama de la compañía y de la lista de usuarios del sistema de información con los roles que desempeñan dentro del sistema.
- *Entrevista de información empresarial:* Lista de respuestas sobre información empresarial de la compañía, que se utilizará para determinar el máximo nivel de madurez al que debe aspirar la compañía, para evitar el sobredimensionamiento del sistema de gestión de seguridad.
- *Entrevista de información técnica:* Lista de respuestas sobre el estado del sistema de información con respecto a la seguridad, para determinar el estado actual de la seguridad del mismo.
- *Lista de activos del sistema de información:* Listado de activos del sistema de información de la compañía, intentando agrupar los activos en los menores grupos posibles para reducir los costes de generación y gestión del análisis de riesgos.

Mediante estas entradas, el conocimiento en materia de gestión de la seguridad aportado por el consultor de seguridad (CoS) y el conocimiento que tiene el interlocutor (Int) sobre la compañía, se generará la estructura del SGSI, que se almacenará en el repositorio de SGSIs y que estará formada por los siguientes elementos:

- *Tabla de usuarios del sistema de información y roles asociados (lUxR):* A partir de la lista de usuarios y roles facilitada por el interlocutor (Int), el consultor de seguridad (CoS) generará una tabla que permita asociar los usuarios del sistema de información con los roles del esquema seleccionado.
- *Organigrama de la compañía (Org):* En condiciones

normales este organigrama será idéntico al organigrama de entrada, pero puede sufrir modificaciones para adaptarlos al SGSI, por lo que también se puede considerar una salida del sistema.

- *Informe empresarial (InfEmp):* Estará formado por las respuestas que el interlocutor ha dado a las preguntas de carácter empresarial realizadas por el consultor de seguridad (CoS) y a los comentarios introducidos por este último para clarificarlas.
- *Informe técnico (InfTec):* Estará formado por las respuestas que el interlocutor ha dado a las preguntas de carácter técnico realizadas por el consultor de seguridad (CoS) y a los comentarios introducidos por este último para clarificarlas.
- *Informe nivel de madurez (InfNM):* Informe con las conclusiones del consultor de seguridad (CoS) con respecto a los resultados obtenidos de las dos listas de verificación realizadas y el NMA y NMR de la compañía en el momento actual.
- *Informe de activos (InfAct):* Listado de los activos del sistema de información detectados y sus valoraciones.
- *Informe de matriz de riesgos (InfMR):* Informe sobre los riesgos existentes sobre los activos con respectos a todos los artefactos involucrados en el análisis.
- *Informe del plan de mejora (InfPM):* Informe detallado sobre los pasos que debe realizar la compañía para aumentar de la forma más eficiente posible su nivel de gestión de seguridad.
- *Informe de artefactos que componen el SGSI (InfSGSI):* Listado de todos los elementos que compondrán el SGSI (reglamentos, procedimientos, controles, etc) generado por el sistema.

Todo este conjunto de elementos, necesarios para poder generar el SGSI, son incluidos por una parte en el repositorio de SGSIs, y por otra parte se convierten en entregables que serán evaluados por el consultor de seguridad (CoS) y el interlocutor de la compañía (Int).

Tabla 1. Intervención de los actores en el proceso GAGR

MARISMA		
GAGR		
A2.1: Establecimiento del marco de trabajo del SGSI.		
T2.1.1	T2.1.2	T2.1.3
CoS, Int	CoS, Int	CoS, Int
A2.2: Establecimiento del nivel de madurez.		
T2.2.1	T2.2.2	T2.2.3
CoS, Int	CoS, Int	CoS
A2.3: Realización del análisis de riesgos.		
T2.3.1	T2.3.2	
CoS, Int	CoS	
A2.4: Generación del SGSI.		
T2.4.1	T2.4.2	
CoS	CoS, Int	

C. Actores.

En la Tabla 1 se muestra en qué actividades y tareas tendrá que intervenir cada uno de los tipos de actores definidos en la metodología. En la actividad actual participarán los siguientes tipos de actores: consultor de seguridad (CoS) y el interlocutor designado por la compañía (Int).

D. Actividades.

A continuación se describirán en detalle las entradas, salidas, relaciones y objetivos de cada una de las diferentes actividades y tareas que componen el subproceso GAGR de la metodología MARISMA.

D.1. Actividad A2.1: Establecimiento del marco de trabajo del SGSI.

El principal objetivo de esta actividad es crear un marco de trabajo inicial entre el consultor de seguridad (CoS) encargado de la generación del SGSI y el cliente (Cl). En la Figura 3 se puede ver el esquema básico de entradas, tareas y salidas que componen esta actividad:

- Entradas: Como entradas 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); ii) información de la compañía en la que se quiere implantar el SGSI.
- Tareas: El subproceso estará formado por tres tareas dependientes unas de otras. Estas tareas son: i) solicitud del interlocutor válido; ii) solicitud del organigrama de la compañía; y iii) obtención de la lista de usuarios del sistema de información y sus roles.
- Salidas: La salida producida por este subproceso consistirá en una serie de entregables (notificación de la dirección del interlocutor válido de la compañía, organigrama de la compañía, matriz de usuarios del sistema de información y roles que desempeñarán dentro 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.

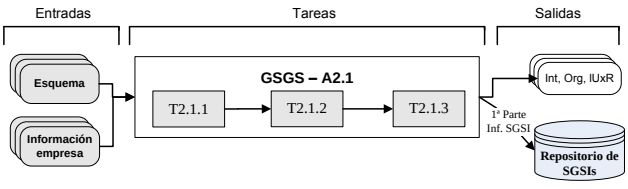


Figura 3. Esquema simplificado a nivel de tarea de la actividad A2.1.

En la Figura 4 se muestran las tareas de la actividad de forma mucho más detallada, viendo cómo interactúan éstas 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 en actividades posteriores (actividad A2.4).

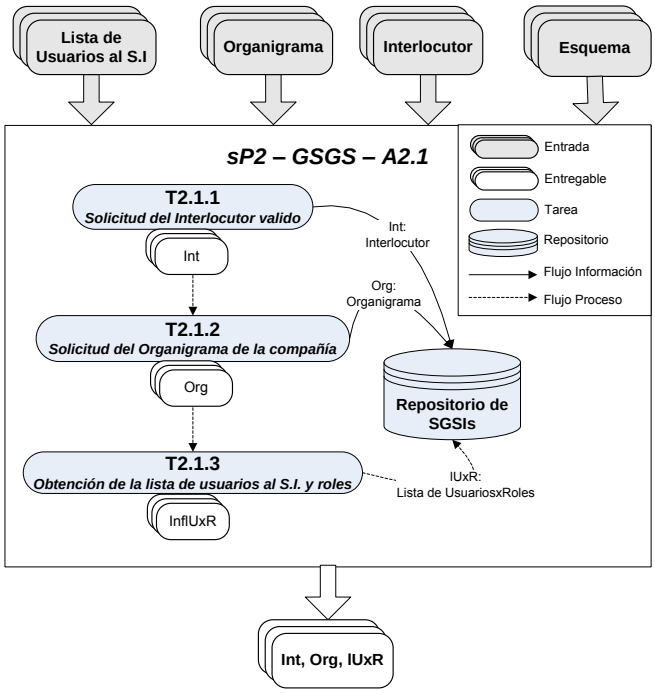


Figura 4. Esquema detallado a nivel de tarea de la actividad A2.1.

A continuación describimos el objetivo de cada una de las tareas:

- Tarea T2.1.1 – Solicitud del interlocutor válido: Para poder iniciar la actividad de generación del SGSI de la compañía, se debe identificar al interlocutor (Int) que acompañará al consultor de seguridad (Cos) durante todo el proceso de consultoría y generación del SGSI, para lo que se utilizará la tarea T2.1.1. El rol de interlocutor (Int) será ocupado por el director de informática en el caso de que la compañía disponga de un departamento de informática, y en el caso de no existir dicho departamento este rol será asumido por la persona más afín al sistema de información de la compañía. Aunque a priori esta tarea puede parecer sencilla, es de gran importancia realizar una correcta selección del interlocutor (Int) y negociar con la dirección de la compañía que esta persona disponga del tiempo necesario para garantizar que no se produzcan retrasos en la elaboración del SGSI. Por otro lado esta persona hará de intermediador entre el consultor de seguridad (CoS) y todos los otros miembros del sistema de información de la compañía, por lo que es de vital importancia que cuente con el apoyo de la dirección de la misma. Por otro lado, el interlocutor (Int) será la persona encargada de facilitar al consultor de seguridad (CoS) toda la información de la compañía que éste requiera para el desarrollo y elaboración del subproceso GAGR, por lo que tendrá que poseer tanto conocimiento técnicos como conocimientos empresariales.
- Tarea T2.1.2 – Solicitud del organigrama de la compañía: La tarea T2.1.2 se ocupa de la obtención del organigrama de la compañía, con el objetivo de centrar el marco de trabajo, delimitando el alcance del SGSI y determinando la complejidad de la empresa. En esta tarea el consultor de seguridad (CoS) deberá analizar el organigrama de la compañía para poder determinar la parte que afecta al sistema de información y cómo adaptar el SGSI a dicha estructura. Es normal en las PYMES que muchas empresas no tengan totalmente claro el organigrama de la misma, por lo que el consultor de seguridad (CoS) puede realizar una labor previa de establecimiento o clarificación de los diferentes departamentos.
- Tarea T2.1.3 – Obtención de la lista de usuarios del S.I. y roles: La tarea T2.1.3 consiste en solicitar al interlocutor (Int) la lista de trabajadores de la compañía que tienen acceso al sistema de información de la misma y los roles que desempeñan dentro de la empresa, con el objetivo de determinar cuáles de ellos están asociados al sistema de información de la compañía y correlacionarlos con los roles definidos (durante la tarea T1.1.1) en el esquema seleccionado. En las PYMES es habitual que los usuarios desempeñen varios roles a la vez, e incluso que un rol sea desempeñado por varias personas. La metodología MARISMA ha sido desarrollada pensando en este tipo de configuraciones.

D.2. Actividad A2.2: Establecimiento del nivel de madurez.

El principal objetivo de esta actividad es establecer el punto inicial en que se encuentra la compañía con respecto a la gestión de la seguridad (nivel de madurez actual) y el punto que sería deseable que la compañía alcanzara (nivel de madurez deseable). Para establecer estos niveles de seguridad se realizarán dos entrevistas, mediante cuestionarios de valores limitados. En [55] se demostraron las ventajas de realizar entrevistas mediante cuestionarios que tienen pre–establecida una serie de preguntas con un número limitado de categorías de respuesta.

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

- Entradas: Como entradas 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 cuestionarios (uno empresarial y uno técnico) que se realizarán al cliente; ii) el interlocutor (Int) válido para la compañía, el cual se encargará de responder los cuestionarios.
- Tareas: El subproceso estará formado por tres tareas. Estas tareas son: i) recogida de información

empresarial; ii) recogida de información técnica del sistema de información; y iii) obtención del nivel de madurez de la seguridad. Las Tareas T2.2.1 y T2.2.2 son independientes y por tanto podrán ser realizadas en paralelo, aunque al depender del interlocutor lo normal será procesarlas en serie. La Tarea T2.2.3 depende de los resultados anteriores y por tanto no podrá acometerse hasta que no finalicen las anteriores.

- Salidas: La salida producida por este subproceso consistirá en una serie de entregables (informe empresarial, informe técnico y resultados del nivel de madurez de la seguridad actual y deseable) 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.

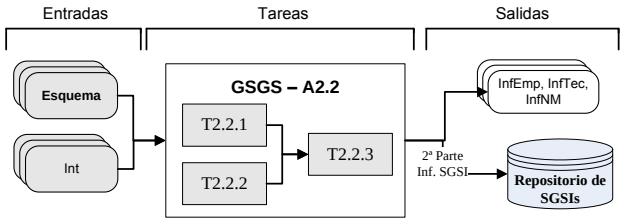


Figura 5. Esquema simplificado a nivel de tarea de la actividad A2.2.

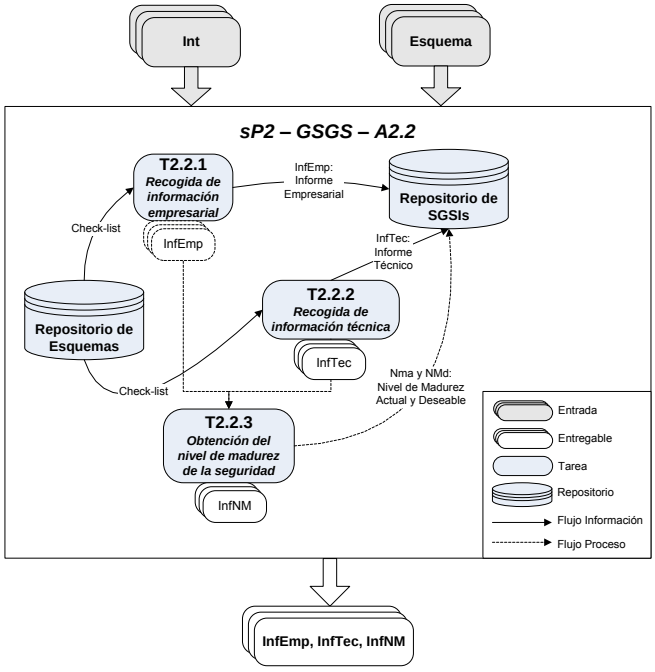


Figura 6. Esquema detallado a nivel de tarea de la actividad A2.2.

En la Figura 6 se muestran las tareas de la actividad de forma mucho más detallada, viendo cómo interactúan éstas 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 en actividades posteriores (actividad A2.4).

Mediante la definición de unas sencillas pero eficaces características de la compañía se han establecido unas reglas que permiten determinar el nivel de madurez actual de la compañía y el que sería deseable que tuviera.

Las tareas de esta actividad se apoyarán principalmente en la parte segunda del esquema seleccionado, que se corresponde con los elementos generados durante la actividad A1.2 del subproceso GEAR.

A continuación describimos el objetivo de cada una de las tareas:

- Tarea T2.2.1 – Recogida de información empresarial: El objetivo de la tarea T2.2.1 es obtener información empresarial de la compañía, mediante la realización de un sencillo cuestionario. Está información se utilizará para: i) seleccionar el esquema más adecuado para la generación del SGSI; ii) determinar el nivel de madurez deseable para la compañía, a partir de las cuestiones sobre el tamaño y el sector al que pertenece la empresa, coincidiendo con las técnicas planteadas por [22]. Así mismo el sector al que pertenece la industria es un factor determinante en la puesta en marcha de un SGSI [56, 57].

  Esta tarea consiste en la realización de un cuestionario empresarial al interlocutor (Int) de la compañía por parte del consultor de seguridad (CoS). La metodología desarrollada se basa en utilizar un conjunto de características intrínsecas a la compañía para definir el nivel de madurez máximo al que la compañía debe evolucionar desde la situación actual. Cada una de estas características o reglas de la compañía tiene asociado un conjunto de valores que permiten determinar el nivel de madurez deseable para la compañía. Estos valores de las reglas han sido determinados a partir de la experiencia obtenida en las implantaciones de SGSIs, y han sido recalibrados gracias al método científico investigación–acción.

  Para el esquema base desarrollado se ha obtenido un conjunto reducido de las características que se han considerado más destacables en las compañías: i) número de empleados, ii) facturación anual, iii) departamento de I+D+i, iv) número de empleados que utilizan el sistema de información, v) número de personas asociadas directamente al departamento de sistemas, vi) nivel de dependencia de la compañía del outsourcing del sistema de información.

  Se debe evitar que una compañía intente llegar a un nivel de madurez que suponga el sobredimensionamiento (utilizar más recursos de los necesarios, o distribuir la carga de forma errónea) en la gestión de su sistema de seguridad, ya que esto tendría consecuencias muy negativas para el conjunto del sistema porque supondría que la compañía realizaría un sobre–esfuerzo que a medio plazo derivaría en la retirada de recursos al no obtenerse los resultados deseados, lo que aumentaría el riesgo de

tener fallos graves en la gestión de la seguridad.

- Tarea T2.2.2 – Recogida de información técnica del S.I.: El objetivo de la tarea T2.2.2 es obtener información técnica de la compañía mediante la realización de un detallado cuestionario. Esta información se utilizará para: i) determinar el nivel de cumplimiento de los controles de seguridad del SGSI; ii) determinar el nivel de madurez actual de la compañía. Esta tarea consiste en la realización de un detallado cuestionario técnico al interlocutor (Int) de la compañía por parte del consultor de seguridad (CoS). Este último podrá incluir anotaciones a las respuestas del interlocutor (Int), ya que al ser éstas de tipo test para facilitar su respuesta, pueden requerir de aclaraciones adicionales que el consultor de seguridad (CoS) incluirá en el informe.
- Tarea T2.2.3 – Obtención del nivel de madurez de la seguridad: El objetivo de la tarea T2.2.3 es procesar los datos obtenidos mediante cuestionarios en las tareas T2.2.1 y T2.2.2, utilizando para ello un conjunto de ecuaciones, el algoritmo de nivel de madurez deseable (Tabla 2) y el algoritmo de nivel de madurez actual (Tabla 3).

  Para determinar el nivel de madurez deseable o recomendado de la compañía se utiliza la Ecuación 1. Los distintos elementos de esta expresión son los siguientes: i) Factores: Los factores representan un conjunto de parámetros que se han seleccionado y que afectan a la hora de determinar el nivel de madurez de gestión de la seguridad adecuado para la compañía; ii) PesoFactor: Es un parámetro corrector que permite controlar las desviaciones que pueden producir las características de compañías pertenecientes a ciertos sectores y que se calibra en el esquema según la experiencia del grupo de expertos del dominio (GED). Ej.: en el caso de compañías tecnológicas permite aumentar el peso del factor "nº de personas asociadas al S.I".

NRM=Σ(PesoFactor*(ValoraciónFactor/ValorMáximoFactor))/ Σ(PesoFactor)

- Si el resultado está entre 0 – 0.25 se debe aplicar sólo el nivel1 de madurez.
- Si el resultado está entre 0.25 – 0.75 se debe aplicar hasta el nivel2 de madurez.
- Si el resultado está entre 0.75 – 1 se debe aplicar hasta el nivel3 de madurez.

Ecuación 1. Nivel de madurez recomendado.

Cada sector de los definidos tiene asociada una matriz de pesos. Esta matriz es fundamental para evitar que las casuísticas de ciertos sectores determinen un nivel de seguridad superior al que realmente puede soportar la infraestructura de la compañía. En condiciones normales el valor inicial establecido para un peso será de 0.50 unidades, para restar peso a un valor se reducirá a 0.25 y para eliminarlo se establecerá un valor de 0. En caso de querer darle mayor importancia se subirá a 0.75 y si el factor se considera fundamental para ese sector, se puede subir el valor del peso a 1. Por ejemplo, en el caso de una compañía de energías renovables el valor de su departamento de I+D+i es fundamental para su evolución, por lo que el peso de este factor debe ser el máximo posible.

Tabla 2. Pseudocódigo del algoritmo del nivel de madurez recomendado.

Algoritmo: Nivel de madurez deseable.

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 calcula el nivel de la compañía como la suma de la valoración x peso de la reglas de madurez de la compañía, entre la valoración máxima a la que se puede acceder.

2º.– Se normaliza el resultado: Nivel1 = 0.00 a 0.25; Nivel2 = 0.25 a 0.75; Nivel3 = 0.75 a 1.00

Una vez determinado el nivel de madurez deseable para la compañía, se determinará el nivel de madurez actual de la misma.

NSCn = Σ(VS)/ NSn

- ***NSCn:*** Nivel de cumplimiento de seguridad de un control para un nivel dado.
- ***VS:*** Valor del subcontrol.
- ***NSn:*** Número de subcontroles para un control y para un nivel dado.

Ecuación.2. Nivel de cumplimiento de la seguridad de un control para un nivel.

Para determinar el nivel de madurez actual de la compañía se determinará primero el nivel de cumplimiento de un control. Este nivel de cumplimiento se puede establecer para cada nivel de madurez (Ecuación 2) o para todos los controles que componen el SGSI (Ecuación 3). Una vez establecido el nivel de cumplimiento de seguridad de cada control, se puede establecer el nivel de cumplimiento a nivel de empresa para cada nivel de madurez (Ecuación 4) o para toda la empresa (Ecuación 5).

NSC = Σ(NSn)/ NNM

- ***NSC:*** Nivel de cumplimiento de seguridad de un control.
- ***NSn:*** Número de subcontroles para un control y para un nivel dado.
- ***NNM:*** Número de niveles del modelo de madurez.

Ecuación 3. Nivel de cumplimiento de la seguridad de un control.

El nivel de cumplimiento de un control para un nivel dado Ecuación 2) se utilizará en la tarea T2.3.2 para determinar el plan de mejora.

$NSEn = \Sigma(NSCn)/ NCn$
• ***NSEn:*** Nivel de cumplimiento de seguridad de la empresa para un nivel. • ***NSCn:*** Nivel de cumplimiento de seguridad de un control para un nivel. • ***NCn:*** Número de controles del nivel.

Ecuación 4. Nivel de cumplimiento de la seguridad para un nivel.

$NSE = \Sigma(NSC)/ NC$
• ***NSE:*** Nivel de cumplimiento de seguridad de la empresa. • ***NSC:*** Nivel de cumplimiento de seguridad de un control. • ***NC:*** Número de controles.

Ecuación 5. Nivel de cumplimiento de la seguridad de la empresa.

El resultado obtenido se debe normalizar para obtener el nivel de madurez actual, mediante la aplicación de los límites establecidos. El algoritmo que permite determinar el nivel de madurez actual se puede ver en la Tabla 3.

Tabla 3. Pseudocódigo del algoritmo del nivel de madurez actual.

Algoritmo: Nivel de madurez actual.
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 calcula el nivel de cobertura para cada control como la suma de los valores de sus subcontroles entre el número de subcontroles por el valor máximo.
2º.– El nivel actual será el nivel más bajo que tenga un control con nivel de cobertura inferior al 90%.
3º.– Se normaliza el resultado: Nivel1 = 0.00 a 0.25; Nivel2 = 0.25 a 0.75; Nivel3 = 0.75 a 1.00

D.3. Actividad A2.3: Realización 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.

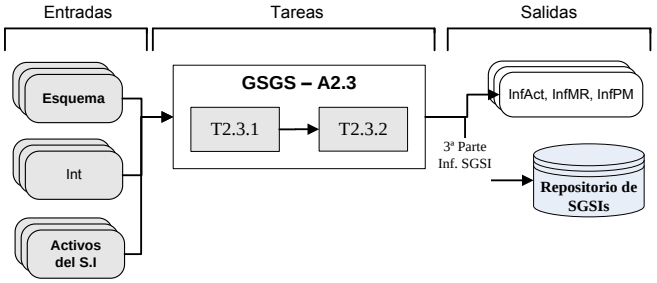


Figura 7. Esquema simplificado a nivel de tarea de la actividad A2.3.

En la Figura 7 se puede ver el esquema básico de entradas, tareas y salidas que componen esta actividad:

- Entradas: Como entradas 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 es dependiente de la T2.3.1, por lo que no podrá ejecutarse hasta la finalización de ésta.
- Salidas: La salida producida por este subproceso consistirá en una serie de entregables (informe de activos del sistema de información, matriz de riesgos a los que están sometidos los activos del sistema de información y el 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 8 se pueden ver las tareas de la actividad de forma mucho más detallada, viendo 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 en actividades posteriores (actividad A2.4).

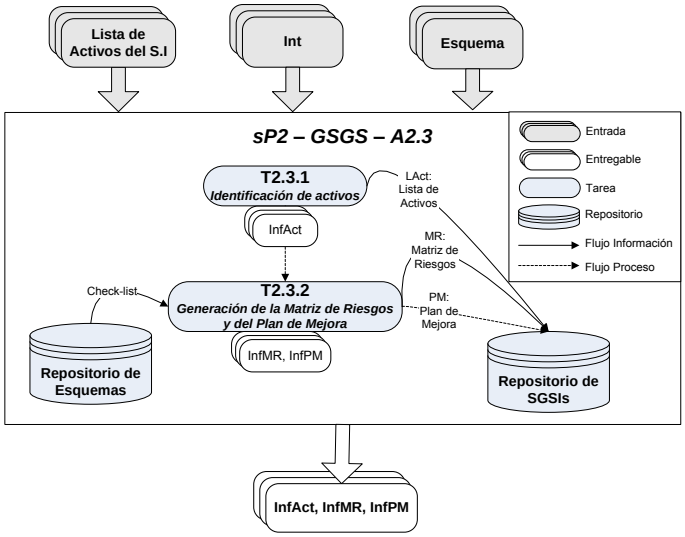


Figura 8. Esquema detallado a nivel de tarea de la actividad A2.3.

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 [58] tomando como referencia la ISO/IEC27002 [59] y en la metodología de análisis de riesgos Magerit v3 [33].

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.

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 [33] y algunos aspectos de los análisis de riesgos clásicos, 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.

Las tareas de esta actividad se apoyarán principalmente en la parte tercera del esquema seleccionado y en la lista de controles obtenida en el subproceso GEAR.

A continuación describimos el objetivo de cada una de las tareas:

- 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 es que se busca que los activos sean lo más generales (grano grueso), frente a MAGERIT que 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: i) Nivel: Nivel de Madurez de la seguridad; ii) Nombre y descripción del activo; iii) Coste del activo: valor cuantitativo que tendría la pérdida del activo para la compañía; iv) Valor estratégico: valor cualitativo que tendría la pérdida del activo; v) Tipo de activo; vi) Amenaza; vii)

Vulnerabilidad; viii) Criterios de riesgo; ix) 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]; x) 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]; xi) 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 6) y xii) 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 en un nivel de madurez determinado, y que se obtiene a partir de las Ecuaciones 7 y 8. 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.

$$NR = P * NA$$

- ***NR:*** Nivel de riesgo.
- ***P:*** Probabilidad de ocurrencia de las vulnerabilidades.
- ***NA:*** Nivel de la amenaza.

Ecuación 6. Nivel de riesgo.

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

- ***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.
- ***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 7. Nivel de cobertura de un control para el par activo–amenaza.

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

- ***NCAA:*** 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:*** Siendo NAA el número de amenazas que afectan al activo.

Ecuación 8. 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 Tabla 4).

Tabla 4. Pseudocódigo del algoritmo de matriz de riesgos.

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 de cada control de la ISO/IEC27002 por niveles.

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 [1–7].

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 Tabla 5). 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 seguridad óptimo.

Tabla 5. Pseudocódigo del algoritmo del plan de mejora.

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 asumible (3)

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.– Si => Salir del ciclo.

1.2.2º.– No => 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.*

D.1. Actividad A2.4: Generación del SGSI.

El principal objetivo de esta actividad es generar los elementos que compondrán el SGSI para la compañía y obtener la aprobación del interlocutor (Int) designado por la compañía del resultado obtenido, o en caso contrario tomar las medidas pertinentes para subsanar las deficiencias (mediante la alteración del esquema seleccionado, la selección de otro esquema más adecuado, o corrigiendo las entradas del subproceso).

En la Figura 9 se puede ver el esquema básico de entradas, tareas y salidas que componen esta actividad:

- Entradas: Como entradas 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 generación del SGSI (listado de controles, listado de reglamentos, listado de procedimientos, listado de registros, listado de plantillas, listado de instrucciones técnicas, listado de métricas, relaciones entre los reglamentos y los artefactos, relaciones entre los reglamentos y los controles, relaciones entre los artefactos y los controles, relaciones entre los procedimientos y los artefactos); ii) el interlocutor (Int) válido para la compañía, el cual se encargará de validar y aprobar el resultado obtenido; iii) los entregables generados durante las actividades anteriores del subproceso GAGR para su aprobación por parte del interlocutor; iv) el contenido del repositorio de SGSIs, generado durante las actividades anteriores del subproceso GAGR.
- Tareas: El subproceso estará formado por dos tareas. Estas tareas son: i) generación de los objetos del SGSI; y ii) presentación de resultados al interlocutor. La tarea T2.4.2 es dependiente de la T2.4.1, por lo que no podrá ejecutarse hasta la finalización de ésta.
- Salidas: La salida producida por este subproceso consistirá en: i) la aprobación de los entregables obtenidos durante las actividades anteriores del subproceso GAGR; ii) conocimiento para que el grupo de expertos del dominio (GED) pueda refinar los esquemas del subproceso GEAR; iii) los elementos que forman el SGSI de la compañía (un cuadro de mandos que indicará el nivel de seguridad para cada control relacionado con la gestión de seguridad de la compañía; un conjunto de reglamentos, plantillas e instrucciones técnicas válidos para esa compañía en el momento actual; un conjunto de métricas; un conjunto de usuarios asociados a roles, que podrán ejecutar en función de su perfil una serie de procedimientos para interactuar con el sistema de información de la compañía; y un conjunto de reglamentos que se deben cumplir para el buen funcionamiento del SGSI).

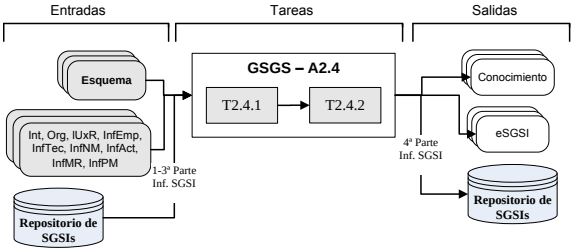


Figura 9. Esquema simplificado a nivel de tarea de la actividad A2.4.

En la Figura 10 se muestran las tareas de la actividad de forma mucho más detallada, viendo cómo interactúan éstas con el repositorio de SGSIs encargado de contener los elementos que conforman los SGSIs.

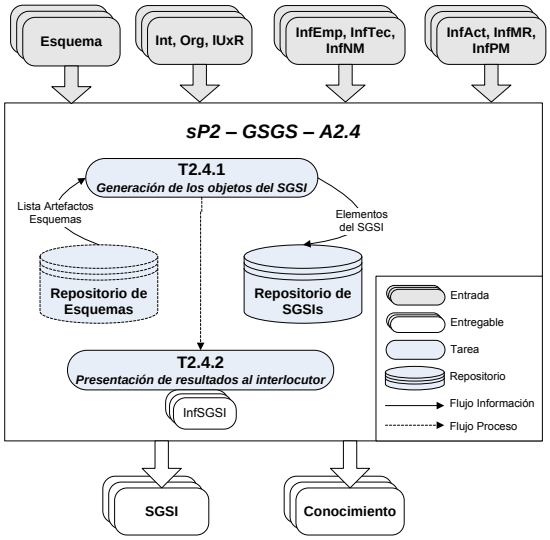


Figura 10. Esquema detallado a nivel de tarea de la actividad A2.4.

Las tareas de esta actividad se apoyarán principalmente en la parte cuarta del esquema seleccionado, que se corresponde con la generada durante la actividad A1.4, y en la lista de controles obtenida en la tarea T1.2.2 del subproceso GEAR.

A continuación describimos el objetivo de cada una de las tareas:

- Tarea T2.4.1 – Generación de los objetos del SGSI: El principal objetivo de la tarea T2.4.1 es la selección de los elementos (reglamentos, procedimientos y controles) que compondrán el SGSI de la compañía a partir del esquema seleccionado y de los datos obtenidos en las actividades anteriores del subproceso GAGR. Esta tarea no requiere de información adicional a la ya obtenida, generando de forma totalmente automática el SGSI adecuado para la compañía mediante el algoritmo de generación de SGSIs (aSGSI). Este algoritmo (Ver Tabla 6) toma como base las matrices de relaciones establecidas en el esquema seleccionado con la finalidad de activar los reglamentos y procedimientos que estén asociados a los controles del nivel de madurez recomendado para la compañía que se determinó en la actividad A2.2 (por ejemplo para una compañía que debe alcanzar un nivel2 de madurez pero que actualmente se encuentra en el nivel 1, el sistema activará sólo aquellos procedimientos que se vean afectados por los controles de nivel 1 y nivel 2 cuyo nivel de cumplimiento en el momento actual sea superior al 75%. El resultado final de esta actividad será un conjunto de reglamentos y un conjunto de procedimientos que deberán cumplirse para mejorar el nivel de seguridad de la compañía. El SGSI será dinámico, adaptándose a los cambios en los niveles de cobertura de los controles y en los niveles de seguridad según evolucione el sistema. La evolución del sistema se medirá mediante: i) un conjunto de métricas definidas sobre el conjunto de elementos del SGSI; ii) un sistema de denuncias por violación de las normativas vigentes; y iii) mediante auditorías periódicas externas. Los procedimientos seleccionados pueden estar asociados a varios niveles de madurez, algunos de los cuales sean superiores al actual o al deseable, por lo que el sistema tendrá siempre en cuenta el nivel de madurez más bajo.
- Tarea T2.4.2 – Presentación de resultados al interlocutor: En la tarea T2.4.2 se recoge toda la información y entregables obtenidos durante las tareas anteriores del subproceso GAGR y se le presenta al interlocutor (Int) para análisis y aprobación. El interlocutor (Int), junto con el consultor de seguridad (CoS), analizará los resultados obtenidos y determinará posibles cambios que tengan que realizarse. En caso de ser necesario realizar cambios, el consultor de seguridad (CoS) enviará las modificaciones pertinentes al grupo de expertos del dominio (GED) para que modifiquen el esquema o creen uno nuevo que se adapte a las necesidades de la compañía. Una vez alterado el esquema se volverán a realizar las tareas del subproceso GAGR hasta que el resultado sea aceptado por el interlocutor (Int) y el consultor de seguridad (CoS).

Tabla 6. Pseudocódigo del algoritmo de generación del SGSI.

Algoritmo: Generación del SGSI.

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 la lista de controles con su nivel de cobertura.

2º.– Se obtiene el nivel actual de la compañía. El nivel actual será el primer nivel que tenga un control para ese nivel con un cumplimiento de la cobertura menor del 90%.

3º.– Se determina el nivel deseable de la compañía a partir del perfil de la misma.

4º.– Se obtiene la lista de controles existentes entre el nivel 1 y el nivel actual, que son los que obligatoriamente se deben cumplir.

5º.– Se obtiene la lista de controles existentes entre el nivel actual y el nivel deseable que además tengan un nivel de cobertura superior al 75%, ya que a medio plazo se deberán cumplir y actualmente ya se cumplen en gran medida.

6º.– A partir del conjunto de controles seleccionados se activarán, usando la matriz de objetos x controles, los: procedimientos relacionados, instrucciones técnicas, registros, plantillas y reglamentos.

7º.– A partir del conjunto de controles seleccionados se activarán las instrucciones técnicas relacionadas usando la matriz de objetos x controles.

8º.– A partir del conjunto de controles seleccionados se activarán los registros relacionados usando la matriz de objetos x controles.

9º.– A partir del conjunto de controles seleccionados se activarán las plantillas relacionadas usando la matriz de objetos x controles.

10º.– A partir del conjunto de controles seleccionados se activarán las normas relacionadas usando la matriz de normas x controles.

11º.– Se insertan en esa instancia los objetos y normas seleccionados, que conformarán el SGSI de la compañía.

V. CONCLUSIONES.

En este artículo se ha presentado el proceso de generación y tratamiento de análisis de riesgos de bajo coste que se ha desarrollado como parte de la metodología MARISMA, el cual permite soportar los resultados generados durante la investigación y que cumple con los objetivos perseguidos, especialmente la capacidad de generarse y mantenerse actualizado a lo largo del tiempo con un bajo coste en recursos humanos y económicos, lo que suponía dos de los grandes problemas de este tipo de sistemas para todas las compañías en la que se realizó la investigación.

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 suficiente.

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 PYMES.

El proceso ha sido validado con más de 20 compañías de España y Colombia, facilitadas por la empresa Sicaman

nuevas Tecnologías S.L. 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.

El proceso MARISMA-AGR cumple con los objetivos propuestos, así como con los principios que según la OCDE [60] 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.

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 por los proyectos *SEQUOIA – Security and Quality in Processes with Big Data and Analytics* (TIN2015-63502-C3-1-R) financiados por el *"*Ministerio de Economía y Competitividad y Fondo Europeo de Desarrollo Regional FEDER", del proyecto ERAVAC ISO25000 (13/16/IN/4/014) financiados por la "Consejería de Economía, Empresas y Empleo" y 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 ha contado con la participación de la empresa Sicaman Nuevas Tecnologías (www.sicaman-nt.com) que ha permitido validar los resultados.

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]. Haufe, K., et al., *ISMS core processes: A study*. Procedia Computer Science, 2016. **100**: p. 339-346.

[9]. 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.

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

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

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

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

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

[15]. 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.

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

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

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

[19]. 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.

[20]. 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.

[21]. 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.

[22]. 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.

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

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

[25]. 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.

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

[27]. 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).

[28]. 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.

[29]. 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.

[30]. 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.
[31]. 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.
[32]. Gupta, A. and R. Hammond, *Information systems security issues and decisions for small businesses.* Information Management & Computer Security, 2005. **13**(4): p. 297-310.
[33]. V3, M., *Methodology for Information Systems Risk Analysis and Management (MAGERIT version 3)*, 2012, Ministerio de Administraciones Públicas (Spain).
[34]. Alberts, C.J. and A.J. Dorofee, *Managing Information Security Risks: The OCTAVE Approach.*, ed. A.-W.P. Co.2002.
[35]. CRAMMv5.0, *CRAMM v5.0, CCTA Risk Analysis and Management Method.*, 2003.
[36]. 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.
[37]. Garigue, R. and M. Stefaniu, *Information Security Governance Reporting.* Information Systems Security, 2003. **sept/oct**: p. 36-40.
[38]. Gerber, M. and R. Von Solms, *Management of risk in the information age.* Computers & Security, 2005. **24**(1): p. 16-30.
[39]. ISO/IEC27005, *ISO/IEC 27005:2011, Information Technology - Security Techniques - Information Security Risk Management Standard (under development).* 2011.
[40]. SSE-CMM, *Systems Security Engineering Capability Maturity Model (SSE-CMM), Version 3.0. Department of Defense. Arlington VA. 326.*, 2003.
[41]. ISO/IEC21827, *ISO/IEC 21827:2008, Information technology - Systems Security Engineering - Capability Maturity Model (SSE-CMM)*, 2008, ISO/IEC. p. 123.
[42]. 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.
[43]. ISO/IEC15443-2, *ISO/IEC TR 15443-2:2012, Information technology -- Security techniques -- A framework for IT security assurance -- Part 2: Assurance methods.*, 2012.
[44]. ISO/IEC20000-1, *ISO/IEC 20000-1:2011, Information technology - Service management - Part 1: Specification.*, 2011.
[45]. ISO/IEC20000-2, *ISO/IEC 20000-2:2012, Information technology - Service management - Part 2: Code of practice.*, 2012.
[46]. COBITv5.0, *Cobit Guidelines, Information Security Audit and Control Association*, ISACA, Editor 2013.
[47]. 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.
[48]. Hareton, L. and Y. Terence, *A Process Framework for Small Projects.* Software Process Improvement and Practice, 2001. **6**: p. 67-83.
[49]. Tuffley, A., B. Grove, and M. G, *SPICE For Small Organisations.* Software Process Improvement and Practice, 2004. **9**: p. 23-31.
[50]. 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.
[51]. Mekelburg, D., *Sustaining Best Practices: How Real-World Software Organizations Improve Quality Processes.* Software Quality Professional, 2005. **7**(3): p. 4-13.
[52]. Sánchez, L.E., et al., *Managing Security and its Maturity in Small and Medium-sized Enterprises.* J. UCS, 2009. **15**(15): p. 3038-3058.
[53]. 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.
[54]. 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.
[55]. Fontana, A. and J. Frey, *The Interview*, in *The SAGE Handbook of Qualitative Research. 3rd edition*, N.L. Denzin, Y, Editor 2005: Thousand Oaks, SAGE Publication. p. 695-727.
[56]. Chang, S.E. and C.B. Ho, eds. *Organizational factors to the effectiveness of implementing information security management*. Industrial Management & Data Systems. Vol. 106. 2006. 345-361.
[57]. Hong, K.S., et al., *An empirical study of information security policy on information security elevation in Taiwan*, in *Information Management & Computer Security*2006. p. 104-115.
[58]. Stephenson, P., *Forensic Análisis of Risks in Enterprise Systems.* Law, Investigation and Ethics, 2004. **sep/oct**: p. 20-21.
[59]. ISO/IEC27002, *ISO/IEC 27002:2013, the international standard Code of Practice for Information Security Management (en desarrollo).* 2013.
[60]. 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.

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. 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. He participates in the GSyA research group of the Department of Computer Science at the University of Castilla- LaMancha.

Sara Camacho Estrada is a Juris Doctor, Master in Information Technology and Multimedia Education, Master in Higher Education, Teaching and Administration. Director of the Languages Center for two periods at the Universidad Técnica de Ambato in Ecuador. Vice-dean of the Education Faculty at the Universidad Técnica de Ambato in Ecuador. Author and director of the TEFL Master´s program at the Universidad Técnica de Ambato in Ecuador. Author of a wide variety of programs like interactive software for learning English, international accreditations, and language learning programs.

Ismael Caballero has an MSc and PhD in Computer Science from the Escuela Superior de Informa´tica of the Castilla-La Mancha University in Ciudad Real. He actually works as an assistant professor in the Department of Information Systems and Technologiesat the University of Castilla-La Mancha, and he has also been working in the R&D Department of Indra Sistemas since 2006. His research interests are focused on information quality management, information quality in SOA, and Global Software Development.

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 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.