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

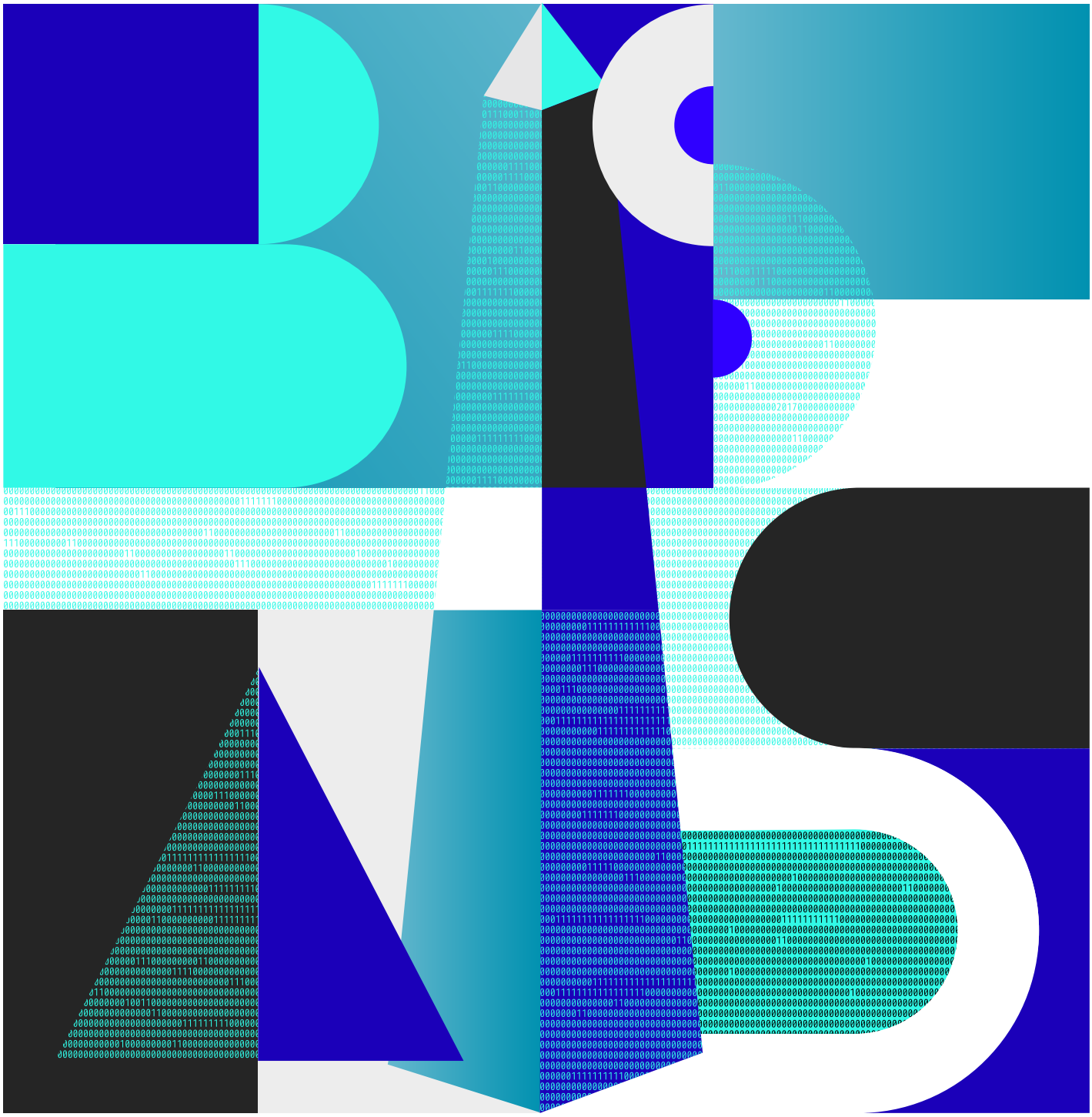
CIBSI

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 Patrones de Gestión de la Seguridad Reutilizables Utilizando MARISMA

A. Santos-Olmo, L. E. Sánchez, S. Camacho, E. Álvarez, 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 "pattern generation" 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, 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. 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 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 [18]. Aunque la investigación realizada se centra inicialmente en las PYMES los resultados podrían aplicarse en otros sectores como el de salud [19-21], o nuevas tecnologías como el cloud computing [22, 23].

Otros autores sugieren que no es suficiente con aplicar un enfoque basado en análisis y gestión de riesgos [24] sino que, además de identificar y eliminar riesgos, también este proceso se ha de realizar de manera eficiente, ahorrando dinero, consecuencia directa de una correcta gestión de la seguridad [25].

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 una metodología que permita analizar y gestionar el riesgo de seguridad [26-28], y además hemos construido una herramienta que automatiza completamente la metodología [29], y lo hemos aplicado en casos reales [30], 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.

Este artículo tiene como objetivo presentar una parte de esa metodología, en concreto el proceso de generación del análisis y el plan de tratamiento de riesgos que se ha desarrollado como parte de la metodología MARISMA, y que

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

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

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

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

tiene como objetivo principal reducir los costes de generación y mantenimiento del análisis de riesgos, al poderse generar mediante la utilización de patrones reutilizables.

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 patrones reutilizables 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 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 [31].

Entre las principales propuestas para el análisis y gestión del riesgo podemos destacar MAGERIT [32], OCTAVE [33] o CRAMM [34]. A pesar de ello, la gestión de la seguridad no puede limitarse al análisis y la gestión del riesgo [24], 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 [25]. 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 [35], 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 [36]:* Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC27001 [37] 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 [38, 39]:* 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.
- *ISO/IEC 15443 [40, 41]:* Clasifica los métodos existentes dependiendo del nivel de seguridad y de la fase del aseguramiento.
- *ISO/IEC2000/ITIL [42, 43]:* 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 [44]:* 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 [45-48]. 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 [49].

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 GEAR. 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 [19, 50], y bajo la premisa de que cualquier sistemas de Análisis de Riesgos valido para las PYMES también será extrapolable a grandes compañías.

Esta metodología asocia 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 [51].
- *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 primero de los procesos que tiene por objetivo la generación de un patrón reutilizable que permita generar y mantener análisis de riesgos de bajo coste.

IV. GEAR. Proceso de generación de patrones con Marisma.

El principal objetivo de este proceso que forma parte de la metodología MARISMA, es permitir la generación de un esquema/patrón (que es una estructura formada por los principales elementos que intervienen en un SGSI y sus relaciones para un determinado tipo de compañías que comparten características comunes – mismo sector y mismo tamaño) que pueda ser utilizado posteriormente para reducir los tiempos y costes de generación de un SGSI para una compañía.

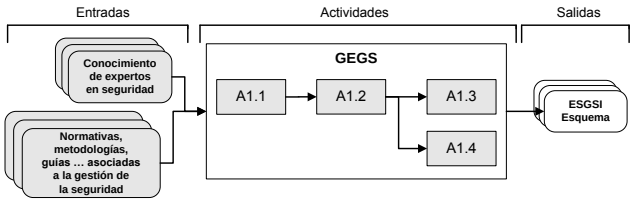


Figura 1. Esquema simplificado a nivel de actividad del subproceso GEAR.

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

- *Entradas:* Como entradas se recibirá el conocimiento del grupo de expertos del dominio de seguridad (GED) obtenido durante el proceso de implantación de SGSIs, este conocimiento es recurrente e incremental durante todo el ciclo de vida de la metodología. La segunda de las entradas estará formada por un conjunto de elementos procedentes de normativas, guías de buenas prácticas y otras metodologías existentes que serán utilizadas junto con un esquema para la construcción de un SGSI.
- *Actividades:* El subproceso estará formado por cuatro actividades. La actividad A1.2 no podrá realizarse hasta la finalización de la A1.1 ya que requiere de elementos generados por ésta para su correcto funcionamiento. La actividad A1.3 y A1.4 dependen de elementos generados por la A1.2, por lo que tendrán que esperar a la finalización de la misma. Entre las actividades A1.3 y A1.4 no existen dependencias temporales por lo que pueden ejecutarse de forma paralela.
- *Salidas:* La salida producida por este subproceso consistirá en un esquema completo formado por todos los elementos necesarios para construir un SGSI y las relaciones existentes entre estos elementos.

El generador de esquemas se puede considerar como una de las principales aportaciones de la metodología desarrollada. Así mismo representa un potente banco de pruebas para poder analizar diferentes configuraciones de SGSI sobre los modelos desarrollados, ya que permite estudiar en detalle cómo influye el elegir unos elementos u otros, o diferentes relaciones a la hora de generar un SGSI y posteriormente interactuar con él.

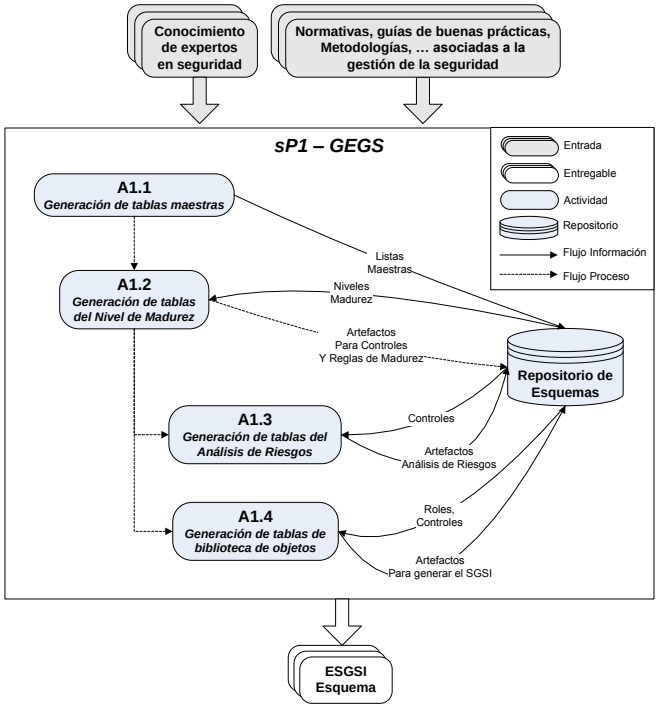


Figura 2. Esquema detallado a nivel de actividad del subproceso GEAR.

En la Figura 2 se pueden ver las actividades del subproceso de forma mucho más detallada, viendo cómo interactúan éstas con el repositorio de esquemas encargado de contener los elementos que conforman los diferentes esquemas del sistema. Aunque existen dependencias entre las diferentes actividades, no existen entregables entre ellas, ya que el resultado de cada actividad es almacenado en el repositorio, de forma que la siguiente actividad obtiene los datos necesarios del mismo.

Actualmente el repositorio de esquemas se compone de un solo elemento denominado esquema base (EB). Este esquema ha sido obtenido mediante el conocimiento adquirido por el grupo de expertos del dominio (GED) y el posterior

refinamiento por medio de la aplicación de la metodología en diversos clientes de la empresa SNT (como parte del grupo crítico de referencia). Su principal utilidad es servir de base para la creación de nuevos esquemas más especializados, con el objetivo de evitar que se tengan que crear esquemas desde cero, lo que supondría un enorme esfuerzo.

A. *Objetivos.*

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

- Incorporación de los controles y niveles de madurez necesarios para establecer el adecuado nivel de seguridad.
- Incorporación de los elementos necesarios para la realización del proceso de análisis y gestión del riesgo (tipos de activos, amenazas, vulnerabilidades y criterios de riesgo).
- Incorporación de los elementos necesarios para la realización del proceso de generación de un SGSI (procedimientos, reglamentos, plantillas, registros, instrucciones técnicas y métricas).
- Establecer relaciones entre los diferentes elementos seleccionados, con el objetivo de automatizar tareas.
- Promover la reusabilidad de los esquemas mediante la asociación de los mismos a compañías con características comunes (mismo sector de actividad empresarial, mismo tamaño), con el objetivo de reducir los tiempos y costes de generación de un SGSI.

B. *Entrada y salida.*

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

- *Una selección de roles o perfiles asociados a tareas de un sistema de información*. Sólo aquellos usuarios de la compañía que se asocien con uno de esos roles se verán afectados por el SGSI. Un usuario puede tener asignados varios roles. Los roles son muy importantes dado que el correcto funcionamiento de los procedimientos del SGSI se apoya en ellos. Para la creación de esta parte del esquema base, y al estar la metodología orientada a PYMES, se han seleccionado un conjunto de los roles propuestos en COBIT [52].
- *Una selección de sectores de actividad empresarial*: Los sectores de actividad representan una división de empresas en grupos, según el trabajo que realizan. Para la creación de esta parte del esquema base, y al estar la metodología orientada a PYMES, se ha utilizado la lista de sectores propuesta por el gobierno Español en el código nacional de actividades económicas Español (CNAE) en su nivel más general.
- *Una selección de posibles niveles de madurez*: Estos niveles permitirán determinar diferentes niveles de evolución de la gestión de la seguridad en el sistema de información. La metodología está preparada para soportar el número de niveles de madurez que se deseen. Para la creación de esta parte del esquema base, y al estar la metodología orientada a PYMES, se han tenido en cuenta las investigaciones realizadas por [53] que proponen un modelo de madurez formado por 4 niveles, y las de Areiza [54] y Vicente Aceituno [55] que proponen modelos de 5 niveles, utilizando finalmente un modelo de 3 niveles parecido al propuesto [53], al ser este el que mejores resultados ha arrojado en las investigaciones.
- *Un conjunto de reglas de madurez y sus valores*: Este conjunto de reglas de madurez se utilizarán para definir el nivel de seguridad deseable para la compañía, es decir, el máximo nivel de madurez que debería poder alcanzar en base a sus características estructurales. Para desarrollar el esquema base se ha utilizado un conjunto básico de preguntas, obtenidas a partir del estudio realizado de los datos económicos de las empresas aportadas en el INE. Parte del estudio realizado con los informes estadísticos obtenidos del INE se muestra en la subsección 4.5.1.1 de este capítulo.
- *Una selección de posibles subcontroles, controles, objetivos de control y secciones asociados a niveles de madurez*: Este conjunto de controles representan las salvaguardas que actuarán y se medirán para gestionar la seguridad del sistema de información a lo largo de todo el ciclo de vida. Los controles seleccionados serán utilizados para medir el nivel de seguridad actual de la compañía y serán utilizados en el análisis de riesgos y la generación del SGSI. Para la creación de esta parte del esquema base se ha utilizado un conjunto de controles extraídos de la guía de buenas prácticas ISO/IEC27002 [56].
- *Un conjunto de listados asociados con los artefactos del análisis de riesgos (tipos de activos, vulnerabilidades, amenazas y criterios de riesgo)*: Estos elementos servirán para evaluar el riesgo al que están sometidos los activos de la compañía. El contenido de este conjunto de artefactos y las relaciones que se establecerán entre ellos es necesario para la realización del análisis de riesgos. La creación de los elementos que componen esta parte del esquema base se ha basado en el contenido de la metodología de análisis de riesgos Magerit v3 [57] y el estándar ISO/IEC27005 [58].
- *Un conjunto de listados asociados con los artefactos de generación del SGSI (reglamentos, procedimientos, plantillas, registros, instrucciones técnicas y métricas)*: Estos elementos serán los que definirán qué y cómo deben operar e interactuar los usuarios con el sistema de información de la compañía para una correcta gestión de seguridad. La creación de los elementos que componen está parte del esquema base se ha basado en: i) el contenido de la guía de buenas

prácticas ISO/IEC27002 [56] para el desarrollo de los procedimientos, reglamentos, registros, plantillas e instrucciones técnicas; ii) el contenido del estándar ISO/IEC27004 [59] para el desarrollo de los elementos de las métricas y el cuadro de mandos; y iii) el contenido del estándar ISO/IEC27001 [37] para determinar las relaciones a establecer entre los diferentes elementos de la metodología.

Mediante estas entradas y el conocimiento del arquitecto en gestión de la seguridad AGS y del grupo de expertos del dominio (GED), se generará un esquema que se almacenará en el repositorio de esquemas y que estará formado por:

- Un subconjunto de los elementos de entrada: Incluirá los niveles de madurez que tendrá el sistema, o los sectores a los que afectará el esquema, controles que se tendrán en cuenta para establecer el nivel madurez de seguridad actual, y reglas que se utilizarán para obtener el nivel de madurez.
- Una serie de matrices de asociación que permiten reducir el tiempo de generación del SGSI y que relacionan entre sí los elementos seleccionados en las entradas. Estas matrices se dividen en dos tipos: i) Análisis de riesgos: Permiten reducir el tiempo de generación del análisis de riesgos, aunque la precisión obtenida es menor que con otras metodologías como Magerit [57], pero la calidad de los resultados obtenidos es suficiente para el caso de las PYMES; ii) Generación del SGSI: Permiten que el sistema pueda generar un SGSI adecuado para la compañía, minimizando la intervención de un consultor de seguridad (CoS) y el coste asociado al mismo.

Todo este conjunto de elementos, necesarios para poder generar el sistema de gestión del sistema de información de la compañía, son incluidos en el repositorio de esquemas para el SGSI, junto con las relaciones existentes entre ellos que representan parte del conocimiento práctico aportado por el grupo de expertos del dominio (GED).

Tabla 1. Intervención de los actores en el proceso GEAR

MARISMA		
GEAR		
A2.1: Establecimiento del marco de trabajo del SGSI.		
T2.1.1	T2.1.2	T2.1.3
AGS, GED	AGS, GED	AGS, GED
A2.2: Establecimiento del nivel de madurez.		
T2.2.1	T2.2.2	T2.2.3
AGS, GED	AGS, GED	AGS, GED
A2.3: Realización del análisis de riesgos.		
T2.3.1	T2.3.2	T2.3.3
AGS, GED	AGS, GED	AGS, GED
A2.4: Generación del SGSI.		
T2.4.1	T2.4.2	
AGS, GED	AGS, GED	

Los esquemas se encuentran en constante evolución, actualizándose con los nuevos conocimientos obtenidos por el arquitecto en gestión de la seguridad (AGS) y el grupo de expertos del dominio (GED) en cada nueva implantación.

C. Actores.

En la Tabla 1 se muestra en qué actividades y tareas tendrán que intervenir cada uno de los tipos de actores definidos en la metodología.

En el subproceso GEAR participarán los siguientes tipos de actores: arquitecto en gestión de la seguridad (AGS) y el grupo de expertos del dominio (GED).

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 GEAR de la metodología MARISMA.

D.1. Actividad A1.1 – Generación de tablas maestras.

El principal objetivo de esta actividad es determinar cuáles son los elementos de carácter general que más pueden adecuarse al esquema que se está creando.

En la Figura 3 se puede ver el esquema básico de entradas, tareas y salidas que componen esta actividad:

- *Entradas:* Como entradas se recibirá el conocimiento del grupo de expertos del dominio de seguridad (GED) obtenido durante el proceso de implantación de SGSIs, y un conjunto de: i) roles (para el esquema base se han utilizados los propuestos por ISACA); ii) sectores empresariales (para el esquema base se han utilizado los propuestos en el CNAE); iii) niveles de madurez (para el esquema base se ha aplicado una variación cercana a la propuesta por [53]).
- *Tareas:* El subproceso estará formado por tres tareas independientes unas de otras. Estas tareas son: i) establecimiento de los roles del esquema; ii) establecimiento de los sectores empresariales; y iii) establecimiento de los niveles de madurez.
- *Salidas:* La salida producida por este subproceso consistirá en un subconjunto de los elementos de entrada, que se almacenarán en el repositorio de esquemas y que se corresponden con la primera parte de los elementos de los que se compondrá el esquema que se quiere generar.

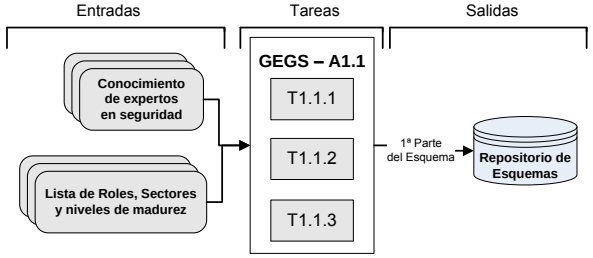


Figura 3. Esquema simplificado a nivel de tarea de la actividad A1.1.

En la Figura 4 se pueden ver las tareas de la actividad de forma mucho más detallada, viendo 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 puedan ser utilizados por otras tareas.

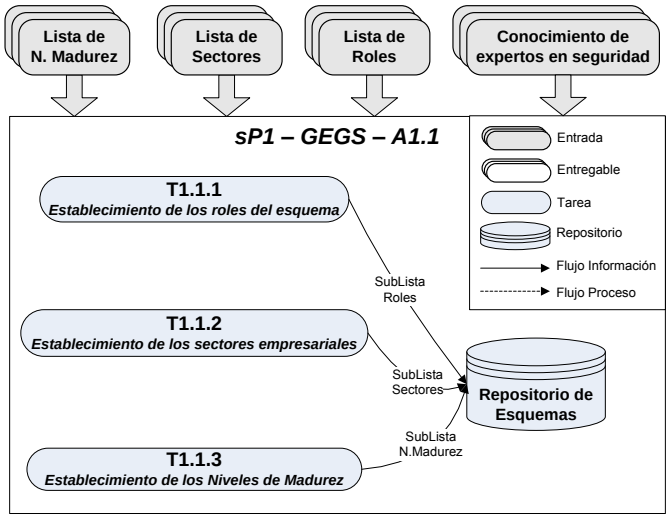


Figura 4. Esquema detallado a nivel de tarea de la actividad A1.1.

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

- *Tarea T1.1.1 – Establecimiento de los roles del esquema:* La tarea T1.1.1 se ocupa de seleccionar la lista inicial roles que se asociarán con actividades del sistema de información. En el esquema base desarrollado con la metodología se ha partido de la lista de roles para sistemas de la información, extraídos de otras metodologías como COBIT [52] de ISACA y del conocimiento adquirido por el arquitecto de gestión de la seguridad (AGS) y el grupo de expertos del dominio (GED) para seleccionar los que más se adecuan al caso de las PYMES. Para la elaboración del esquema base se ha seleccionado un subconjunto de dichos roles, que se verán en detalle en el capítulo 6 al analizar el caso de estudio.
- *Tarea T1.1.2 – Establecimiento de los sectores empresariales:* La tarea T1.1.2 se ocupa de seleccionar la lista inicial de sectores de actividad empresarial que permita incluir a cualquier tipo de compañía. En la elaboración del esquema base se utilizó como conjunto de sectores por actividad empresarial recomendado por la metodología el del CNAE Español nivel 1, que tiene 59 grupos de actividades empresariales, ya que el nivel de detalles de otros niveles superiores era demasiado grande para el caso de las PYMES (220 grupos de actividad empresarial en el caso del CNAE nivel2, 501 grupos de actividad empresarial en el caso del CNAE nivel3).
- *Tarea T1.1.3 – Establecimiento de los niveles de madurez:* La tarea T1.1.3 se ocupa de seleccionar el número de niveles de madurez del SGSI de la compañía. Para el esquema base desarrollado se analizaron diferentes modelos de madurez basados en tres, cuatro y cinco niveles [53-55]. Aun cuando la metodología propuesta admite cualquier número de niveles de madurez, los resultados de las investigaciones realizadas durante la elaboración de la metodología permitieron determinar que el número de niveles de madurez que más se adecua al caso de las PYMES era de tres.

D.2. Actividad A1.2 – Generación de tablas del nivel de madurez.

El principal objetivo de esta actividad es determinar los controles y reglas de madurez que más pueden adecuarse al esquema que se está creando, y que serán utilizados posteriormente para determinar el nivel de madurez de la seguridad de la compañía actualmente y hasta qué nivel de madurez sería aconsejable que evolucionase.

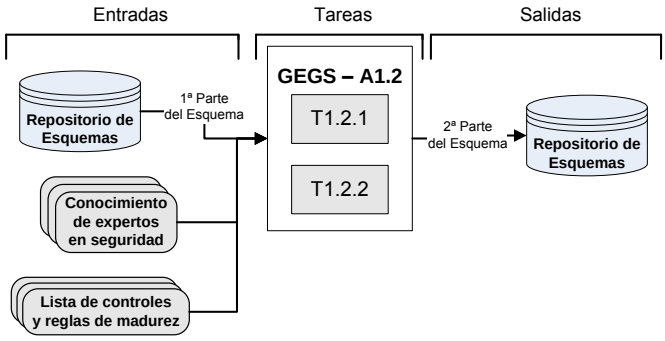


Figura 5. Esquema simplificado a nivel de tarea de la actividad A1.2.

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

- *Entradas:* Como entradas se recibirá el conocimiento del grupo de expertos del dominio de seguridad (GED) obtenido durante el proceso de implantación de SGSIs, los niveles de madurez obtenidos en la tarea T1.1.3 y un conjunto de: i) reglas de madurez, que se utilizarán para definir el nivel de seguridad deseable para la compañía, es decir, el máximo nivel de madurez que debería poder alcanzar en base a sus características estructurales (para el esquema base se han obtenido a partir de un estudio realizado sobre datos del INE y mostrado en el apartado 4.5.1.1); ii) controles de seguridad (para el esquema base se han utilizados los propuestos en la guía de buenas prácticas de la ISO/IEC27002 [56]).
- *Tareas:* El subproceso estará formado por dos tareas independientes, que tendrán que seleccionar los elementos que posteriormente se utilizarán para

determinar el nivel de madurez actual y deseable para la compañía. Estas tareas son: i) establecimiento de las reglas de madurez, establecimiento de los controles.

- *Salidas:* La salida producida por este subproceso consistirá en un subconjunto de los elementos de entrada, los cuales se almacenarán en el repositorio de esquemas y que se corresponden con la segunda parte de los elementos de los que se compondrá el esquema que se quiere generar.

En la Figura 6 se pueden ver las tareas de la actividad de forma mucho más detallada, viendo 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 puedan ser utilizados por otras tareas.

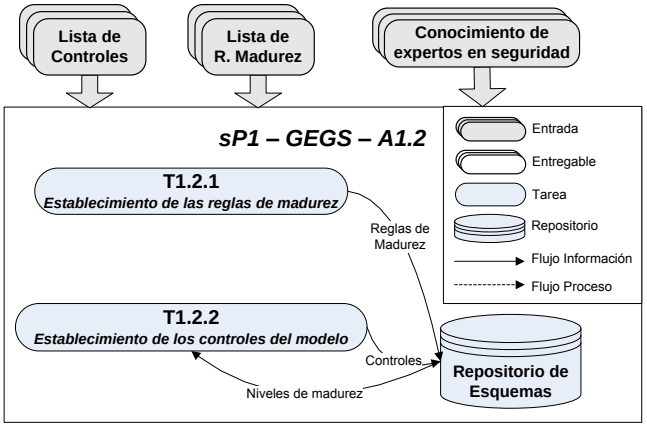


Figura 6. Esquema detallado a nivel de tarea de la actividad A1.2.

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

- *Tarea T1.2.1 – Establecimiento de las reglas de madurez:* La tarea T1.2.1 se ocupa de seleccionar el conjunto de reglas que permitirán posteriormente establecer el nivel de madurez de la seguridad del sistema de información más adecuado para la compañía. El esquema base se ha desarrollado inicialmente con un sencillo conjunto de seis de reglas con tres a cuatro valores seleccionables cada una. Este conjunto, aunque sencillo, se ha mostrado eficiente a la hora de determinar el nivel de madurez adecuado para las PYMES.
- *Tarea T1.2.2 – Establecimiento de los controles:* La tarea T1.2.2 se ocupa de seleccionar un conjunto de controles que servirán posteriormente para diversas tareas: i) servir de salvaguardas para el SGSI; ii) medir el nivel de madurez de la gestión de la seguridad actual de la compañía; iii) establecer un plan de mejora de la gestión de la seguridad; iv) y seleccionar los elementos que compondrán el SGSI de la compañía.

Con el objetivo de obtener una mayor precisión a la hora de determinar el cumplimiento de los controles, estos son divididos en subcontroles que permitan determinar con la mayor precisión posible el cumplimiento o no de un aspecto de seguridad muy concreto. La idea de dividir en el mayor número posible de preguntas cada control de la norma está orientada a obtener la mayor precisión con la menor complejidad. Con el uso de subcontroles, los usuarios sólo tienen que responder con una sencilla lista de valores (no aplica, si, parcialmente, no) a cada una de la preguntas, permitiendo obtener un nivel de cumplimiento de los controles [0 – 100%] mucho más preciso que si las cuestiones se realizaran a nivel de control.

Para el desarrollo del esquema base se ha utilizado la guía de buenas prácticas ISO/IEC27002 [56], de la cual se ha extraído la lista de controles, obteniendo 896 subcontroles que permiten determinar de forma muy precisa la seguridad del sistema de información de una compañía. Inicialmente la investigación se realizó con la guía de buenas prácticas ISO/IEC17799:2000 [60] obteniendo un cuestionario de 735 preguntas o subcontroles.

Aunque el número de subcontroles puede parecer muy elevado para el caso de las PYMES, no es así dado que es una tarea que se realiza una sola vez a lo largo del SGSI y que las preguntas y respuestas requeridas son muy sencillas.

D.3. Actividad A1.3 – Generación de tablas del nivel de madurez.

El principal objetivo de esta actividad es seleccionar los elementos necesarios para poder realizar, en actividades posteriores de la metodología, un análisis de riesgo 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 [37] y se encuentra descrita en detalle en el estándar ISO/IEC27005 [58], 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 7 se puede ver el esquema básico de entradas, tareas y salidas que componen esta actividad:

- *Entradas:* Como entradas se recibirá el conocimiento del grupo de expertos del dominio de seguridad (GED) obtenido durante el proceso de implantación de SGSIs, los controles seleccionados en la tarea T1.2.2 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 [57] y del estándar ISO/IEC27005 [58]).

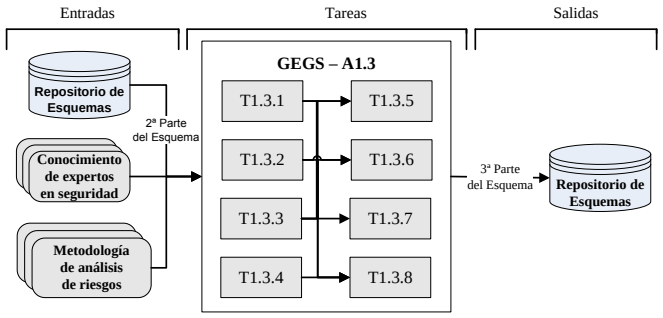


Figura 7. Esquema simplificado a nivel de tarea de la actividad A1.3.

- *Tareas:* El subproceso estará formado por ocho tareas. Estas tareas son: 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 T1.3.1 a T1.3.4. 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.
- *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 8 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 puedan ser utilizados por otras tareas.

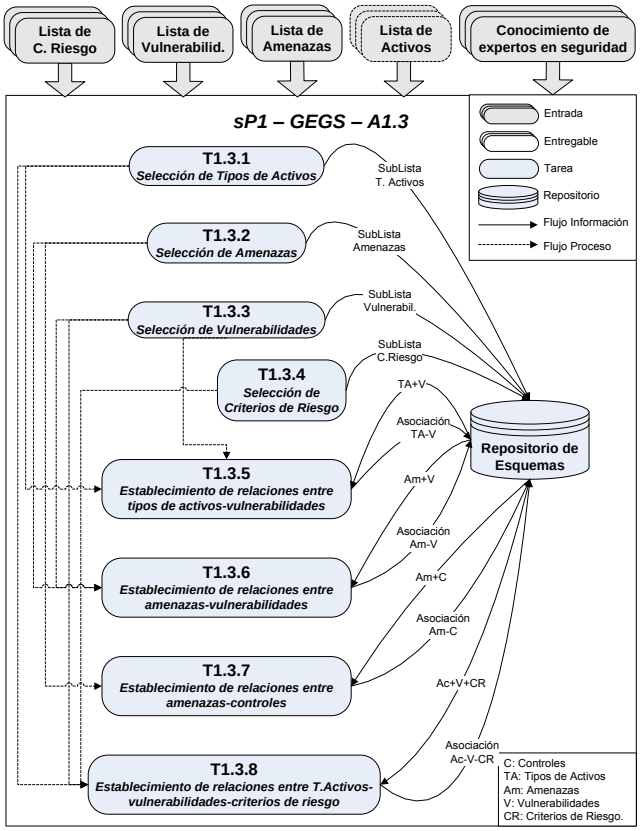


Figura 8. Esquema detallado a nivel de tarea de la actividad A1.3.

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:* La tarea T1.3.1 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 [57] y en el estándar ISO/IEC27005 [58]. Para el esquema actual se ha definido un conjunto de 23 tipos de

activos.

- *Tarea T1.3.2 – Selección de amenazas:* La tarea T1.3.2 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 [57]. 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 [57] y en el estándar ISO/IEC27005 [58]. 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:* La tarea T1.3.3 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 [57]. 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 [57] y en el estándar ISO/IEC27005 [58]. Para el esquema actual se han definido un conjunto de 48 vulnerabilidades.
- *Tarea T1.3.4 – Selección de criterios de riesgo:* La tarea T1.3.4 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 [57] y en el estándar ISO/IEC27005 [58], aunque se ha simplificado ya que el conjunto ofrecido por Magerit [57] 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 elementos: i) Confidencialidad: Característica que evita el acceso o la divulgación de información a individuos o procesos no autorizados; ii) Integridad: La integridad está vinculada a la fiabilidad funcional del sistema de información, su eficacia para cumplir las funciones del sistema; iii) Disponibilidad: Característica que previene la denegación no autorizada de accesos a los activos; iv) Legalidad: Se trata de evaluar la importancia del activo con respecto al cumplimiento de la legislación vigente.
- *Tarea T1.3.5 – Establecer relaciones entre tipos de activos y vulnerabilidades:* La tarea T1.3.5 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:* La tarea T1.3.6 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:* La tarea T1.3.7 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:* La tarea T1.3.8 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 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.

D.4. Actividad A1.4 – Generación de tablas de la biblioteca de artefactos.

El principal objetivo de esta actividad es seleccionar los elementos necesarios para poder realizar, en actividades posteriores de la metodología, el subconjunto de estos elementos que conformarán el SGSI para una compañía y las relaciones existentes entre ellos.

Esta actividad está basada en el principio de que la estructura de las PYMES con características parecidas (mismo sector y mismo tamaño) comparte la mayor parte de relaciones en cuanto a los elementos que componen un SGSI, 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, estas son irrelevantes con respecto a la configuración final del SGSI obtenido para el caso de las PYMES, dado que estas priorizan el coste a obtener un resultado con un alto grado de precisión.

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

- *Entradas:* Como entradas se recibirá el conocimiento del grupo de expertos del dominio de seguridad (GED) obtenido durante el proceso de implantación de SGSIs, los controles seleccionados en la tarea T1.2.2 que se encuentran almacenados en el repositorio de esquemas y un conjunto elementos (reglamentos, procedimientos, plantillas, registros, instrucciones técnicas y métricas) necesarios para elaboración de un SGSI. En el esquema base desarrollado la selección de estos elementos se ha basado en: i) el contenido de la guía de buenas prácticas ISO/IEC27002 [56] para el desarrollo de los procedimientos, reglamentos, registros, plantillas e instrucciones técnicas; ii) el contenido del estándar ISO/IEC27004 [59] para el desarrollo de los elementos de las métricas y el cuadro de mandos; y iii) el contenido del estándar ISO/IEC27001 [37] para determinar las relaciones a establecer entre los diferentes elementos de la metodología.

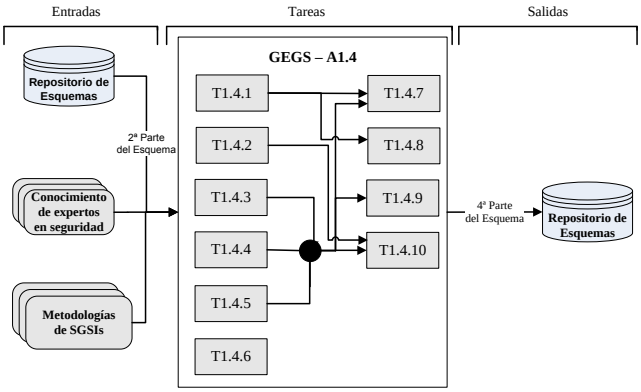


Figura 9. Esquema simplificado a nivel de tarea de la actividad A1.4.

- *Tareas:* El subproceso estará formado por diez tareas. Estas tareas son: i) selección de reglamentos; ii) selección de procedimientos; iii) selección de registros; iv) selección de plantillas; v) selección de instrucciones técnicas; vi) selección de métricas; vii) establecimiento de relaciones entre reglamentos y artefactos; viii) establecimiento de relaciones entre reglamentos y controles; ix) establecimiento de relaciones entre artefactos y controles; x) establecimiento de relaciones entre procedimientos y artefactos. Las seis primeras tareas son independientes y permiten seleccionar los elementos de entrada. Las otras cuatro tareas representan las relaciones existentes entre las familias de elementos de las tareas T1.4.1 a

T1.4.5. 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.

- *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 cuarta parte de los elementos de los que se compondrá el esquema que se quiere generar.

En la Figura 10 se pueden ver las tareas de la actividad de forma mucho más detallada, viendo 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 puedan ser utilizados por otras tareas.

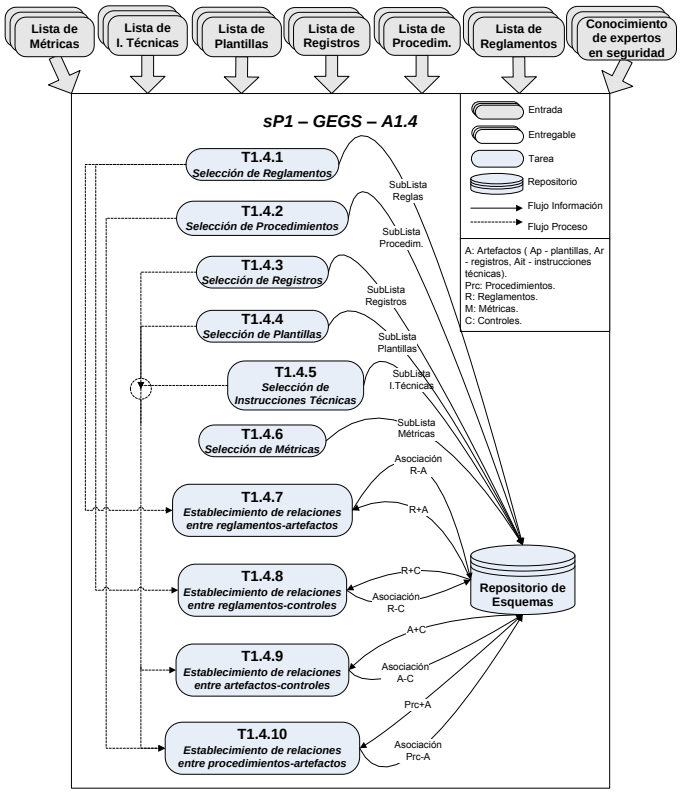


Figura 10. Esquema detallado a nivel de tarea de la actividad A1.4.

A continuación, se analizarán uno por uno los diferentes elementos (reglamentos, procedimientos, plantillas, registros, instrucciones técnicas y métricas) de los que se compone el SGSI propuesto en la nueva metodología:

- *Tarea T1.4.1 – Selección de reglamentos:* La tarea T1.4.1 se ocupa de seleccionar el conjunto de reglamentos que formarán parte del esquema que se está construyendo. Los reglamentos se utilizarán posteriormente para diversas tareas: i) establecer asociaciones con otros elementos del SGSI (tareas T1.4.7 y T1.4.8); ii) generar el SGSI (tarea T2.4.1); iii) servir de base para el procedimiento de denuncia de la tarea T3.2.2; iv) actualizar los niveles de seguridad de los controles de seguridad que componen el SGSI (actividad A3.3). El conjunto de reglamentos 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. Un reglamento está formado por un conjunto de reglas, cada una de las cuales está asociada con otros artefactos del SGSI. Su cumplimiento es necesario para el correcto funcionamiento del SGSI generado. El incumplimiento de una regla afecta a todos los elementos que componen el SGSI, los cuales a su vez están asociados con los controles que componen el cuadro de mandos de seguridad del sistema, con lo que al incumplirse una regla se degradan los controles de seguridad asociados a la misma. De esta operativa se ocupa la actividad A3.3 y permite mantener actualizado el nivel de seguridad del sistema de forma automática. La selección del conjunto de reglamentos que conforma el esquema base, está basada en la guía de buenas prácticas ISO/IEC27002 [56]. Para el esquema actual se han definido un conjunto de 264 reglas, aunque lo normal es que al generarse el SGSI de la compañía durante la actividad A2.4, se seleccione solo un pequeño conjunto de reglas para formar parte del SGSI.
- *Tarea T1.4.2 – Selección de procedimientos:* La tarea T1.4.2 se ocupa de seleccionar el conjunto de procedimientos que formarán parte del esquema que se está construyendo. Los procedimientos se utilizarán posteriormente para diversas tareas: i) establecer asociaciones con otros elementos del SGSI (tareas T1.4.10); ii) generar el SGSI (tarea T2.4.1); iii) servir de base a los procedimientos que forman el SGSI (actividad A3.2); iv) actualizar los niveles de seguridad de los controles de seguridad que componen el SGSI (actividad A3.3). El conjunto de procedimientos 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. Un procedimiento está formado por un conjunto de fases que a su vez tienen asociados. La selección del conjunto de reglamentos que conforma el esquema base está basada en la guía de buenas prácticas ISO/IEC27002 [56] y el contenido del estándar ISO/IEC27001 [37]. Para el esquema actual se han definido un conjunto de 50 procedimientos, aunque lo normal es que al generarse el SGSI de la compañía durante la actividad A2.4, se seleccione sólo un pequeño conjunto de procedimientos para formar parte del SGSI.
- *Tarea T1.4.3 - Selección de registros:* La tarea T1.4.3 se ocupa de seleccionar el conjunto de registros que formarán parte del esquema que se está construyendo.

Los registros se utilizarán posteriormente para diversas tareas: i) establecer asociaciones con otros elementos del SGSI (tareas T1.4.7, T1.4.9 y T1.4.10); ii) generar el SGSI (tarea T2.4.1); iii) servir de base a los procedimientos que forman el SGSI (actividad A3.2); iv) actualizar los niveles de seguridad de los controles de seguridad que componen el SGSI (actividad A3.3). El conjunto de registros 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 registros que conforma el esquema base está basada en la guía de buenas prácticas ISO/IEC27002 [61] y el contenido del estándar ISO/IEC27001 [37]. Los registros que se utilizarán en el SGSI generado dependerán de los procedimientos que formen parte de ese SGSI.

- *Tarea T1.4.4 – Selección de plantillas:* La tarea T1.4.4 se ocupa de seleccionar el conjunto de plantillas que formarán parte del esquema que se está construyendo. Las plantillas suelen contener documentos formales necesarios para el cumplimiento de los procedimientos. Las plantillas se utilizarán posteriormente en las mismas tareas que los registros. El conjunto de plantillas 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 plantillas que conforma el esquema base está basada en la guía de buenas prácticas ISO/IEC27002 [61] y el contenido del estándar ISO/IEC27001 [37]. Las plantillas que se utilizarán en el SGSI generado dependerán de los procedimientos que formen parte de ese SGSI.
- *Tarea T1.4.5 – Selección de instrucciones técnicas:* La tarea T1.4.5 se ocupa de seleccionar el conjunto de instrucciones técnicas que formarán parte del esquema que se está construyendo. Las instrucciones técnicas son documentos técnicos de apoyo para la ejecución de los procedimientos. Las instrucciones técnicas se utilizarán posteriormente en las mismas tareas que los registros y las plantillas. El conjunto de instrucciones técnicas 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 instrucciones técnicas que conforma el esquema base está basada en la guía de buenas prácticas ISO/IEC27002 [56] y el contenido del estándar ISO/IEC27001 [37]. Las instrucciones técnicas que se utilizarán en el SGSI generado dependerán de los procedimientos que formen parte de ese SGSI.
- *Tarea T1.4.6 – Selección de métricas:* La tarea T1.4.6 se ocupa de seleccionar el conjunto de métricas que formarán parte del esquema que se está construyendo. Las métricas permiten conocer o estimar el valor de ciertas características del sistema de información. Las métricas seleccionadas se utilizarán para la actividad A3.3. El conjunto de métricas 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 métricas que conforma el esquema base está basada en el estándar ISO/IEC27004 [59].
- *Tarea T1.4.7 – Establecer relaciones entre reglamentos y artefactos:* La tarea T1.4.7 se ocupa de establecer las relaciones existentes entre los elementos que componen el conjunto de reglamentos y los elementos que componen el conjunto de artefactos (procedimientos, plantillas, registros e instrucciones técnicas) para un esquema determinado. El objetivo principal de este conjunto de asociaciones es establecer relaciones entre los elementos del SGSI para poder generar de forma automática los componentes que deben formar parte del SGSI (actividad A2.4). Este conjunto de relaciones es utilizado por el algoritmo de generación del SGSI (actividad A2.4) para, a partir de la información generada en las actividades A1.2 y A1.3, generar la estructura del SGSI de la compañía. Para el esquema base actual, se han establecido 762 relaciones entre el conjunto de reglas y el conjunto de artefactos, en base al conocimiento adquirido a lo largo de la investigación.
- *Tarea T1.4.8 – Establecer relaciones entre reglamentos y controles:* La tarea T1.4.8 se ocupa de establecer las relaciones existentes entre los elementos que componen el conjunto de reglamentos 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 generar de forma automática los componentes que deben formar parte del SGSI (actividad A2.4). Este conjunto de relaciones es utilizado por el algoritmo de generación del SGSI (actividad A2.4) para generar la estructura del SGSI de la compañía. Para el esquema base actual, se han establecido 431 relaciones entre el conjunto de reglas y el conjunto de controles, en base al conocimiento adquirido a lo largo de la investigación.
- *Tarea T1.4.9 – Establecer relaciones entre artefactos y controles:* La tarea T1.4.9 se ocupa de establecer las relaciones existentes entre los elementos que componen el conjunto de artefactos (procedimientos, plantillas, registros e instrucciones técnicas) 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 generar de forma automática los componentes que deben formar parte

del SGSI (actividad A2.4). Estas asociaciones se establecen por el grupo de expertos del dominio (GED) en base al conocimiento adquirido en diferentes implantaciones del SGSI. Este conjunto de relaciones es utilizado por el algoritmo de generación del SGSI (actividad A2.4) para generar la estructura del SGSI de la compañía. Para el esquema base actual, se han establecido 449 relaciones entre el conjunto de artefactos y el conjunto de controles, en base al conocimiento adquirido a lo largo de la investigación.

- *Tarea T1.4.10 – Establecer relaciones entre procedimientos y artefactos:* La tarea T1.4.10 se ocupa de establecer las relaciones existentes entre los elementos que componen el conjunto de procedimientos y el conjunto de artefactos (plantillas, registros e instrucciones técnicas) para un esquema determinado. El objetivo principal de este conjunto de asociaciones es establecer relaciones entre los elementos del SGSI para poder generar de forma automática los componentes que deben formar parte del SGSI (actividad A2.4). Estas asociaciones se establecen por el grupo de expertos del dominio (GED) en base al conocimiento adquirido en diferentes implantaciones del SGSI. Este conjunto de relaciones es utilizado por el algoritmo de generación del SGSI (actividad A2.4) para generar la estructura del SGSI de la compañía. Para el esquema base actual, se han establecido 176 relaciones entre el conjunto de procedimientos y el conjunto de artefactos, en base al conocimiento adquirido a lo largo de la investigación.

V. Conclusiones.

En este artículo se ha presentado el proceso de generación de patrones reutilizables para la generación de análisis de riegos 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, mediante la utilización de patrones reutilizables se consigue este objetivo.

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.

Tanto las características ofrecidas por el proceso como su orientación a las PYMES han sido aspectos muy bien recibidos, 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.

Actualmente tres de las actividades presentadas han sido implementadas dentro de la herramienta eMARISMA y aplicadas con éxito en empresas de España y Colombia.

El proceso MARISMA-AGR cumple con los objetivos propuestos, así como con los principios que según la OCDE [62] 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 security2011: 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 engineering2000, Boston/Dordrecht/London: Kluwer Academic Publishers.
[10] Dhillon, G., Information Security Management: Global challenges in the new millennium2001: 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] Sánchez, L.E., et al., Managing Security and its Maturity in Small and Medium-sized Enterprises. J. UCS, 2009. 15(15): p. 3038-3058.
[20] 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.
[21] 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.
[22] 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.
[23] Tariq, M.I. and V. Santarcangelo. Analysis of ISO 27001: 2013 Controls Effectiveness for Cloud Computing. in ICISSP. 2016.
[24] 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.
[25] Garigue, R. and M. Stefaniu, Information Security Governance Reporting. Information Systems Security, 2003. sept/oct: p. 36-40.
[26] 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).
[27] 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.
[28] 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.
[29] 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.
[30] 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.
[31] Gupta, A. and R. Hammond, Information systems security issues and decisions for small businesses. Information Management & Computer Security, 2005. 13(4): p. 297-310.
[32] V3, M., Methodology for Information Systems Risk Analysis and Management (MAGERIT version 3), 2012, Ministerio de Administraciones Públicas (Spain).
[33] Alberts, C.J. and A.J. Dorofee, Managing Information Security Risks: The OCTAVE Approach., ed. A.-W.P. Co.2002.
[34] CRAMMv5.0, CRAMM v5.0, CCTA Risk Analysis and Management Method., 2003.
[35] Gerber, M. and R. Von Solms, Management of risk in the information age. Computers & Security, 2005. 24(1): p. 16-30.
[36] ISO/IEC27005, ISO/IEC 27005:2011, Information Technology - Security Techniques - Information Security Risk Management Standard (under development). 2011.
[37] ISO/IEC27001, ISO/IEC 27001:2013, Information Technology - Security Techniques Information security management systemys - Requirements., 2013.
[38] SSE-CMM, Systems Security Engineering Capability Maturity Model (SSE-CMM), Version 3.0. Department of Defense. Arlington VA. 326., 2003.
[39] ISO/IEC21827, ISO/IEC 21827:2008, Information technology - Systems Security Engineering - Capability Maturity Model (SSE-CMM), 2008, ISO/IEC. p. 123.
[40] 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.
[41] ISO/IEC15443-2, ISO/IEC TR 15443-2:2012, Information technology -- Security techniques -- A framework for IT security assurance -- Part 2: Assurance methods., 2012.
[42] ISO/IEC20000-1, ISO/IEC 20000-1:2011, Information technology - Service management - Part 1: Specification., 2011.
[43] ISO/IEC20000-2, ISO/IEC 20000-2:2012, Information technology - Service management - Part 2: Code of practice., 2012.
[44] COBITv5.0, Cobit Guidelines, Information Security Audit and Control Association, ISACA, Editor 2013.
[45] 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.
[46] Hareton, L. and Y. Terence, A Process Framework for Small Projects. Software Process Improvement and Practice, 2001. 6: p. 67-83.
[47] Tuffley, A., B. Grove, and M. G, SPICE For Small Organisations. Software Process Improvement and Practice, 2004. 9: p. 23-31.
[48] 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.
[49] Mekelburg, D., Sustaining Best Practices: How Real-World Software Organizations Improve Quality Processes. Software Quality Professional, 2005. 7(3): p. 4-13.
[50] 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.
[51] 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.
[52] COBITv4.0, Cobit Guidelines, Information Security Audit and Control Association, 2006.
[53] Eloff, J. and M. Eloff, Information Security Management - A New Paradigm. Annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology SAICSIT´03, 2003: p. 130-136.

[54] Areiza, K.A., et al., Hacia un modelo de madurez para la seguridad de la información. IV Congreso Internacional de Auditoría y Seguridad de la Información, 2005b. Dic (2005).
[55] ISM3, Information security management matury model (ISM3 v.2.0), 2007, ISM3 Consortium.
[56] ISO/IEC27002, ISO/IEC 27002:2013, the international standard Code of Practice for Information Security Management (en desarrollo). 2013.
[57] MageritV3, Methodology for Information Systems Risk Analysis and Management., in Ministerio de Hacienda y Administraciones Públicas2012: Spain.
[58] ISO/IEC27005, ISO/IEC 27005, Information Technology - Security Techniques - Information Security Risk Management Standard (under development). 2008.
[59] ISO/IEC27004, ISO/IEC FCD 27004, Information Technology - Security Techniques - Information Security Metrics and Measurement (under development). 2009.
[60] ISO/IEC17799, ISO/IEC 17799, Information Technology - Security Techniques - Code of practice for information security management, 2000.
[61] ISO/IEC27002, ISO/IEC 27002, Information Technology - Security Techniques - The international standard Code of Practice for Information Security Management., 2007.
[62] 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 a Professor at the Universidad of Castilla-la Mancha (Ciudad Real, Spain), MSc in Information Systems Audit from the Polytechnic University of Madrid, and Certified Information System Auditor by ISACA. He is the Director of Professional Services and R&D departments of the company Sicaman Nuevas Tecnologías S.L. COIICLM board or committee member and responsible for the professional services committee. His research activities are management security system, security metrics, data mining, data cleaning, and business intelligence. He participates in the GSyA research group of the Department of Computer Science at the University of Castilla- LaMancha, in Ciudad Real (Spain).

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.

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).

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.