Methodology for Dynamic Analysis and Risk Management on ISO27001

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

***Abstract* – The information society is increasingly dependent Information Systems Security Management (ISMS) and knowledge of the security risks associated with its assets value. However, very few risk analysis methodologies have been raised as to create systems to analyze risks in a quick and economical, and which in turn can leave this system dynamically update. This paper presents a new methodology, called MARISMA, aimed at carrying out a risk analysis simplified and dynamic, which is valid for all companies, including SMEs, and to provide solutions to the problems identified during the application of the scientific method "Action Research". This methodology is being applied directly to real cases, thus achieving a constant improvement of its processes.**

***Keyword* — 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. De esta forma, las empresas ya han tomado conciencia de que la información y los procesos que apoyan los sistemas y las redes son sus activos más importantes [6, 7]. Estos activos están sometidos a riesgos de una gran variedad, que pueden afectar de forma crítica a la empresa. Así, la importancia de la seguridad en los sistemas de información viene avalada por numerosos trabajos [8-15], por citar sólo algunos.

Algunos autores [16, 17] sugieren la realización de un análisis de riesgos como parte fundamental en la PYME, ya que deben tener en cuenta que el valor y la sanción de los datos robados o filtrados en una pequeña organización es el mismo que para una grande, y por tanto debe tener controlado el valor y los riesgos a los que esos activos están sometidos [18]. Otros autores [19] proponen la necesidad de desarrollar un nuevo modelo de análisis de riesgos (AR) pero orientándolo directamente a las PYMES, considerando que el uso de técnicas de análisis y gestión de riesgos, así como el papel de terceros, es necesario para poder garantizar la seguridad del sistema de información de las PYMES [20]. Aunque la investigación realizada se centra inicialmente en las PYMES los resultados podrían aplicarse en otros sectores como el de salud [21-23], o nuevas tecnologías como el cloud computing [24].

Estudios centrados en la evaluación de riesgos [25-27], 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 [28]. 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 [29], y que una evaluación de la situación actual requiere de herramientas de análisis de riesgos [30] 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

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

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

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

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

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

concienciación de su importancia.

Otros autores sugieren que no es suficiente con aplicar un enfoque basado en análisis y gestión de riesgos [31] 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 [32].

Otro de los aspectos que se está estudiando para su aplicación a los modelos de gestión de la seguridad y su madurez es el control de los costes asociados a la gestión de la seguridad, ya que estos pueden influir en el dimensionamiento del modelo de gestión de la seguridad. De esta forma, Mercuri [33] se propone asociar como parte fundamental del desarrollo de los SGSI los análisis de coste–beneficio (CBA) en la fase del análisis de riesgos.

Como tal, una de las cuestiones derivadas de las conclusiones es la necesidad de obtener nuevas metodologías y modelos de análisis y gestión del riesgo que permitan adaptarse a las PYMES, con el objetivo de eliminar (o al menos reducir) los inconvenientes y ayudar a estas sociedades a evaluar los riesgos a los que sus activos están expuestos y a establecer los controles de seguridad adecuados [34].

Muchos autores consideran que el punto central de los SGSI debe ser el análisis de riesgos. Entre ellas se puede destacar la propuesta de Barrientos [35] y UE CORAS (IST–2000–25031) [36, 37]. La propuesta de Barrientos [35] está basada en llevar a cabo un análisis relativo a la seguridad informática para identificar el grado de vulnerabilidad y determinar los aspectos de mejora a ser llevados a cabo en la organización con el objeto de reducir el riesgo. Por otro lado, UE CORAS (IST–2000–25031) [36, 37] está desarrollando un marco para el análisis de riesgos de seguridad que utiliza UML2, AS/NZS 4360, ISO/IEC27001, RM–ODP6, UP7 y XML8.

Siegel [31] señala que los modelos de seguridad informática que se centran exclusivamente en modelos de eliminación de riesgos no son suficientes, y por otro lado Garigue [32] remarca que actualmente los gerentes no desean saber sólo qué se ha realizado para mitigar los riesgos, también se debe poder dar a conocer eficazmente que se ha realizado esta tarea y si se ha conseguido ahorrar dinero.

Sneza realiza un estudio sobre las PYMES considerando los resultados del análisis de riesgos como clave para garantizar que las políticas y procedimientos son realmente necesarios, llegando a la conclusión de que las PYMES deben guiarse por el riesgo de pérdidas de activos derivado del análisis de riesgos. Se debe persuadir a los propietarios de las PYMES de emprender un escenario formal basado en el análisis de riesgos y la protección de los activos de información. Los recientes hallazgos de la seguridad de la información han puesto de manifiesto una fuerte correlación entre el proceso formal de evaluación de riesgos y los gastos de la seguridad de la información [38].

Se debe tener en cuenta que el análisis de riesgos es un proceso costoso que no se puede repetir cada vez que se realiza una modificación. Por eso es importante desarrollar metodologías específicas que permitan mantener los resultados del análisis de riesgos. El proyecto de la UE Coras [36, 37] hace de este mantenimiento del análisis de riesgos el punto principal de su modelo.

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

Por lo tanto, y considerando que las PYMES representan una gran mayoría de empresas tanto a nivel nacional como internacional y son muy importantes para el tejido empresarial de cualquier país, creemos que avanzar en la investigación para mejorar los procesos de análisis y gestión del riesgo para este tipo de empresas puede generar importantes aportaciones. Esto puede contribuir a mejorar no sólo la seguridad de las PYMES, sino también su nivel de competitividad. Por este motivo, a los largo de los últimos años hemos trabajado en elaborar un proceso simplificado que permita analizar y gestionar el riesgo de seguridad en las PYMES [39-41], y además hemos construido una herramienta que automatiza completamente la metodología [42], y lo hemos aplicado en casos reales [43], 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 de metodología para el análisis y la gestión del riesgo de la seguridad orientada hacia las PYMES. 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 [44].

Entre las principales propuestas para el análisis y gestión del riesgo podemos destacar MAGERIT [45], OCTAVE [46] o CRAMM [47]. A pesar de ello, la gestión de la seguridad no

puede limitarse al análisis y la gestión del riesgo [31], 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 [32]. 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 [48], 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 [49]:* Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC27001 [28] y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC27001 [28] e ISO/IEC27002 [50] es importante para un completo entendimiento de la norma ISO/IEC 27005 [49], que es aplicable a organizaciones que tienen la intención de gestionar los riesgos que puedan comprometer la organización de la seguridad de la información [51, 52]. Su publicación revisa y retira las normas ISO/IEC TR 13335–3 [53] y ISO/IEC TR 13335–4 [54].
- *ISO/IEC21827/SSE–CMM [55, 56]:* El modelo de capacidad y madurez en la ingeniería de seguridad de sistemas describe las características esenciales de los procesos que deben existir en una organización para asegurar una buena seguridad en los sistemas, incluyendo en las fases previas un proceso orientado al riesgo, con 4 subprocesos: SSE-PA02 (Determinar el impacto), SSE-PA03 (Identificar los riesgos de seguridad), SSE-PA04 (Identificar las amenazas), SSE-PA05 (Identificar las vulnerabilidades).
- *ISO/IEC 15443 [57, 58]:* Clasifica los métodos existentes dependiendo del nivel de seguridad y de la fase del aseguramiento. La evaluación del aseguramiento se divide en proceso, producto y ambiente, mientras que las fases del análisis del riesgo son diseño/implementación, integración/verificación, réplica, transición y operación. Las fases del análisis del riesgo para CC [59] son diseño/implementación, integración/verificación, transición y operación.
- *ISO/IEC2000/ITIL [60, 61]:* ITIL ofrece un elemento para una correcta gestión de riesgos: el conocimiento actualizado y detallado de todos los activos de la organización y de las relaciones, pesos y dependencias entre ellos. Dicho conocimiento ITIL lo administra desde el proceso de gestión de la configuración de soporte al servicio, y mediante el uso de la herramienta básica sobre la que se construye una aproximación coherente a la gestión eficiente de las TI, la CMDB (Configuration Management Database). El disponer del repositorio actualizado de activos que representa la CMDB facilita la realización del análisis de riesgos en la fase de planificación del SGSI, que se utilizará como elemento de ponderación de los controles a implantar y cuya permanente actualización resultará incluso más relevante una vez el SGSI se encuentre implantado y funcionando.
- *COBIT [62]:* Es una metodología para el adecuado control de los proyectos de tecnología, los flujos de información y los riesgos que implica la falta de controles adecuados. Incluye un proceso orientado a evaluar los riesgos, en el dominio PO9. Este proceso se centra principalmente en los criterios de confidencialidad, integridad y disponibilidad, y de forma secundaría en criterios de efectividad, eficiencia, cumplimiento y confiabilidad. Por último este proceso involucra a diversos recursos del TIC (RRHH, Sistemas de Información, Tecnología, Instalaciones y Datos).

Por otro lado, existe un pequeño conjunto de herramientas de análisis de riesgos. Actualmente la más utilizada para el análisis de riesgos es PILAR, basada en Magerit v3 [45]. Otras herramientas utilizadas son la propuesta por ENISA, que incluye un sistema de comparativas, OCTAVE–S y Octave Automated Tool, que implementan la metodología de evaluación de riesgos OCTAVE [46], CRAMM 5.2 y COBRA, etc.

El principal problema de estos procesos y herramientas es su complejidad para aplicarlos en el caso de las PYMES, ya que han sido concebidos para grandes empresas [63-66]. 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 [67].

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. Para ello se tomarán como base algunas de las normas y documentos tanto nacionales como internacionales más adecuados, como las guías para la gestión de seguridad ISO/IEC 13335 [53, 54, 68] y la metodología de análisis y gestión de riesgos Magerit [45].

III. MARISMA-AGR

Para solucionar los problemas detectados en el análisis y gestión del riesgo, se ha realizado un proceso orientado a las

PYMES y enfocado a reducir los costes de generación y mantenimiento del proceso de análisis y gestión del riesgo denominado MARISMA-AGR. Este proceso se ha obtenido mediante la aplicación del método de investigación en acción y se ha enmarcado dentro de una metodología (MARISMA) que acomete todos los aspectos relacionados con la gestión de la seguridad [21, 69], 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):* 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 [70].
- *Proceso 2 – Generación del Análisis y Gestión del Riesgo (GAGR):* 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):* 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 la Figura 1 se pueden ver de forma resumida los tres procesos que componen la metodología MARISMA, y cómo intercambian información entre ellos. La información generada en el proceso GEAR será utilizada por los otros dos procesos. De igual forma, la información generada en el proceso GAGR será necesaria para el proceso MDAR. Esto no implica que siempre se deban ejecutar los tres procesos para obtener un resultado, sino que debe existir un Esquema generado previamente por el proceso GEAR para que se pueda ejecutar el GAGR.

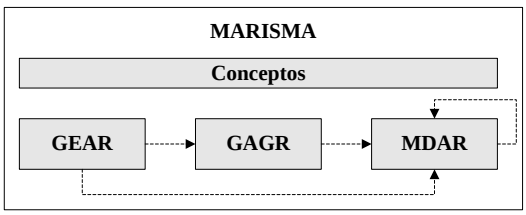

Figura 1. Esquema de procesos de MARISMA

Este apartado se divide a su vez en cuatro sub-apartados, representando cada uno de los elementos de la Figura 1. En el primero se verán una serie de conceptos o definiciones necesarias para entender el proceso. En el segundo sub-apartado se analizará el primero de los procesos que se ocupa de la generación de un esquema valido para el análisis de riesgos. En el tercer sub-apartado se analizará el segundo de los procesos que se ocupara de la generación del análisis y el plan de tratamiento de riesgos. En el último apartado se analizará el proceso que permite mantener el cuadro de riesgos actualizado de forma dinámica.

A. Definiciones previas.

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

- *Esquema:* Estructura formada por los principales elementos de un SGSI y las relaciones entre ellos, que puede ser reutilizado por un conjunto de compañías con características comunes (mismo sector y tamaño) a partir del conocimiento adquirido con la implantación de la metodología MARISMA y posteriores refinamientos [71].
- *Esquema Base:* Esquema inicial obtenido a partir del conocimiento de expertos en seguridad, que sirve como base para la elaboración de otros esquemas más específicos que puedan adecuarse a conjuntos de compañías [70].
- *SGSI:* Parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. En el caso de la metodología MARISMA el SGSI se compone entre otros de un conjunto de reglamentos que definen la política de seguridad de la compañía, procedimientos, controles, un sencillo análisis de riesgos y un cuadro de mandos que nos permite conocer cómo evoluciona el sistema.
- *Análisis de riesgos:* Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización [45]. La metodología MARISMA incluye un sencillo método para estimar el riesgo a partir de un conjunto básico de activos.
- *Activo:* Recursos del sistema de información, o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.
- *Activo de grano grueso:* La metodología MARISMA funciona bajo activos de grano grueso, que son aquellos que agrupan activos que están sometidos a las mismas amenazas, mismos criterios de riesgo, mismas vulnerabilidades y mismo valor estratégico. Dado que, por lo tanto, activarían los mismos riesgos y controles se tratan de forma unificada dentro del análisis de riesgos.
- *Activo de grano fino:* Son los activos de valor para la compañía al nivel más bajo de agregación.
- *Controles:* Mecanismos que nos permiten proteger los

activos de las amenazas que intentan aprovechar las vulnerabilidades en estos para producir un impacto sobre algún criterio de riesgo de nuestros activos de valor.

- *Sub-controles:* Divisiones a mayor detalle de los controles. En ocasiones los controles son demasiado difusos, o intentan abordar demasiada información para permitir que el usuario dé una respuesta coherente sobre el nivel de cumplimiento (Si/Parcialmente/No).
- *Amenaza:* Evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
- *Vulnerabilidad:* Debilidad o falta de control que permitiría o facilitaría que una amenaza actuase contra un activo del sistema que presenta la citada debilidad. En el caso de MARISMA, las vulnerabilidades se calculan como la ausencia o debilidad de un control en la lista de controles base, que en el esquema seleccionado para la investigación está basada en controles y sub-controles derivados de la ISO27001:2013.
- *Criterios de riesgo:* Criterios que permiten estimar el grado de exposición a que una amenaza se materialice sobre uno o más dimensiones valorables de los activos causando daños o perjuicios a la organización.
- *Matriz Amenazas x Tipos de Activos:* Es una matriz que nos permite relacionar qué amenazas afectan a las diferentes familias de activos.
- *Matriz Amenazas x Controles:* Es una matriz que permite relacionar qué controles permiten proteger a los activos frente a cada amenaza. Dado que no se ha encontrado ninguna normativa que tuviera esta matriz, se ha tenido que extraer en base a la experiencia (Know-How) de los consultores involucrados en el proceso, aplicando la metodología científica Investigación en Acción.

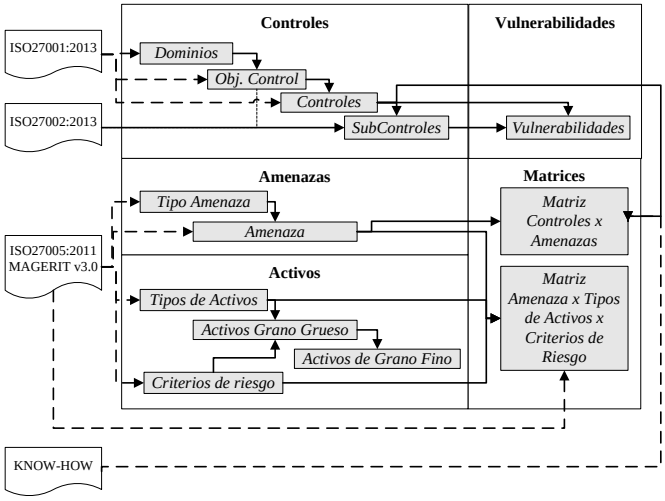

Figura 2. Elementos que componen el sistema base y sus relaciones.

En el esquema de la Figura 2 se puede ver cómo todos elementos se interrelacionan unos con otros y el origen que se ha utilizado para generar el esquema base que se está utilizando actualmente, y que básicamente parte de cuatro fuentes (ISO27001:2013, ISO27002:2013, ISO27005:2011, MAGERIT v3.0 y la Experiencia adquirida mediante la técnica de Investigación en Acción).

B. Proceso 1 – Generación de Esquemas para el Análisis de Riesgos (GEAR).

El principal objetivo de este proceso es seleccionar los elementos necesarios para poder realizar un análisis de riesgos de bajo coste sobre los activos que componen el sistema de información de la compañía que se adapte a los requerimientos de las PYMES.

Aunque el análisis de riesgos es una de las partes fundamentales en la norma ISO/IEC27001 [28] y se encuentra descrita en detalle en el estándar ISO/IEC27005 [49], 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 3 se puede ver el esquema básico de entradas, tareas y salidas que componen este proceso:

- *Entradas:* Como entrada se recibirá el conocimiento del grupo de expertos del dominio de seguridad (GED) obtenido durante el proceso de implantación de otros Análisis de Riesgos, así como un conjunto de controles para la gestión de seguridad que se encuentran almacenados en el repositorio de esquemas y un conjunto de elementos (tipos de activos, amenazas, vulnerabilidades y criterios de riesgo) necesarios para elaboración del análisis de riesgos (en el esquema base desarrollado la selección de estos elementos se ha basado en el contenido de la metodología de análisis de riesgos Magerit v3.0, y de los estándares de seguridad ISO/IEC27001:2013 [28], ISO/IEC27002: 2013 [50] y la ISO/IEC27005 [49]).

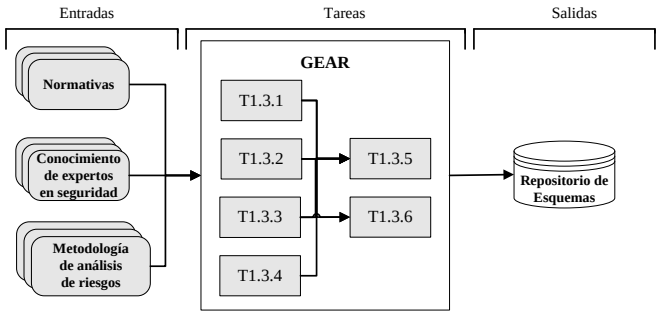

Figura 3. Esquema simplificado a nivel de tarea del proceso GEAR.

- *Tareas:* El proceso estará formado por seis tareas (ver Figura 3). Las cuatro primeras tareas son independientes y permiten seleccionar los elementos de entrada. Las otras dos tareas se ocupan de

establecer las relaciones existentes entre dichos elementos, con el objetivo de poder automatizar aspectos del análisis de riesgos y hacerlo dinámico. Estas relaciones se establecen a partir del conocimiento del grupo de expertos del dominio (GED) y de los continuos refinamientos obtenidos de la implantación de la metodología. En las siguientes subsecciones se detallarán estas tareas.

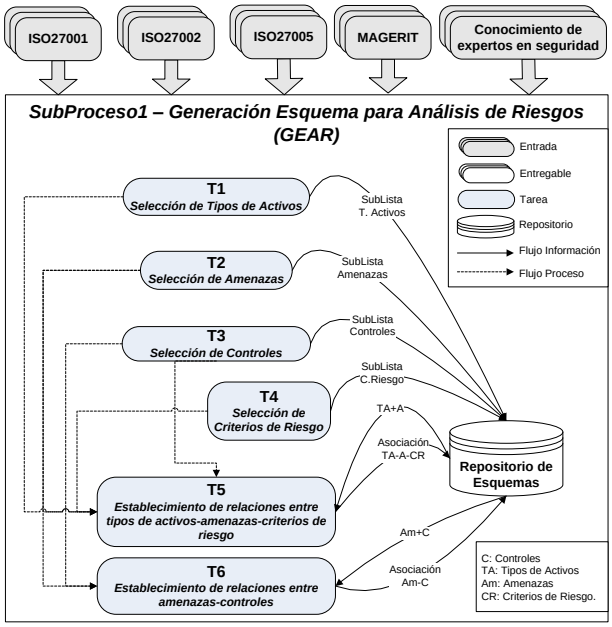

Figura 4. Esquema detallado a nivel de tarea del proceso GEAR

- *Salidas:* La salida producida por este proceso consistirá en un subconjunto de los elementos de entrada y las relaciones establecidas entre ellos, los cuales se almacenarán en el repositorio de esquemas.

En la Figura 4 se pueden ver las tareas del proceso de forma mucho más detallada, mostrando cómo interactúan éstas con el repositorio de esquemas encargado de contener los elementos que conforman los diferentes esquemas del sistema. No existen entregables entre las diferentes tareas, ya que el resultado de cada tarea es almacenado en el repositorio, para que pueda ser utilizado por otras tareas, siendo el resultado final un Esquema. En el caso que estamos siguiendo el esquema generado se ha denominado "Esquema Base ISO27001:2013" al tomar esta norma como base generadora.

A continuación, se analizarán una por una las diferentes tareas de las que se compone el proceso GEAR propuesto en la nueva metodología y los valores que estos elementos pueden tomar para el esquema base generado inicialmente.

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

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

  La selección del conjunto de tipos de activos que conforma el esquema base actual está basada en la metodología de análisis de riesgos Magerit v3.0 [45] y en el estándar ISO/IEC27005 [49]. Para el esquema actual se ha definido un conjunto de 10 tipos de activos.

- *Tarea T1.3.2 – Selección de amenazas:* Se ocupa de seleccionar el conjunto de amenazas que formarán parte del esquema que se está construyendo. Una amenaza se define como un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos [45]. 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 v3.0 [45] y en el estándar ISO/IEC27005 [49]. Estas amenazas están agrupadas en un conjunto de categorías: Desastres naturales; De origen industrial; Errores y fallos no intencionados; Ataques intencionados. Para el esquema actual se han definido un conjunto de 57 amenazas asociadas a 4 tipos de amenazas.

- *Tarea T1.3.3 – Selección de controles:* Se ocupa de seleccionar el conjunto de controles que formarán parte del esquema que se está construyendo y permitirá dar cumplimiento al concepto de vulnerabilidad, definida está 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 [45]. Por lo tanto, a partir del nivel de incumplimiento de los controles podemos cuantificar el nivel de la vulnerabilidad para ese control. Estos controles 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 controles 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 controles que conforma el esquema base está basada en la norma ISO/IEC27001:2013, lo que nos permite extraer un conjunto de 114 controles. Pero durante la aplicación del método científico investigación-acción se vio que si sólo se preguntaba a los usuarios de una empresa en base a esos controles sobre un total de 3 respuestas posibles (Si, Parcialmente o No), el grado de error e incertidumbre obtenido era muy elevado, obteniendo incluso las tres respuestas para el mismo control. Por ello se decidió complementar dicha tarea extrayendo un nivel de sub-controles (preguntas de grano fino) utilizando para ello la norma ISO/IEC27002:2013, lo que permitía reducir el grado de error y obtener con mayor certeza el grado de cumplimiento de los controles. Para el esquema actual se han obtenido unos 1.000 sub-controles que se asocian con los 114 controles.

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

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

  La selección del conjunto de criterios de riesgo que conforma el esquema base está basada en la metodología de análisis de riesgos Magerit v3.0 [45] y en el estándar ISO/IEC27005 [49], El conjunto de criterios de riesgo definidos para el esquema base está formado por cinco criterios (C - Confidencialidad, I - Integridad, D – Disponibilidad, A - Autenticidad y T - Trazabilidad).

- *Tarea T1.3.5 – Establecimiento de relaciones entre [Tipos de activos] x [Amenazas] x [Criterios de Riesgo]:* Se ocupa de establecer las relaciones existentes entre los elementos que componen el conjunto de tipos de activos y sus criterios de riesgo asociados y los elementos que componen el conjunto de amenazas.

  El objetivo principal de este conjunto de asociaciones es establecer relaciones entre los elementos del Análisis de Riesgos para poder realizar una evaluación del riesgo de bajo coste en el proceso siguiente.

  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 ha utilizado la matriz de relaciones definidas en Magerit v3.0 y se ha adaptado al esquema en base al conocimiento adquirido a lo largo de la investigación. Se han definido 275 relaciones para está matriz.

- *Tarea T1.3.6 – Establecimiento de relaciones entre [Amenazas] x [Controles]:* Se ocupa de establecer las relaciones existentes entre los elementos que componen el conjunto de amenazas y los elementos que componen el conjunto de controles/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 el siguiente proceso.

  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 468 relaciones entre el conjunto de amenazas y los objetivos de control, en base al conocimiento adquirido a lo largo de la investigación.

C. Proceso 2: Aplicación del Análisis de Riesgos.

El principal objetivo de este proceso 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 y con el menor esfuerzo y coste.

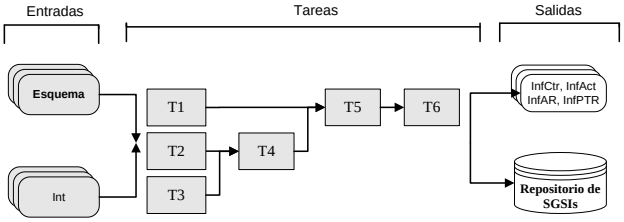

Figura 5. Esquema simplificado a nivel de tarea del proceso GAGR.

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

- *Entradas:* Como entrada se recibirá: i) un esquema de los existentes en el repositorio de esquemas, que será seleccionado por el consultor de seguridad (CoS) en base a las características de la compañía (sector y

tamaño de la misma), del que se obtendrán los elementos necesarios para la realización del análisis de riesgos (listado de controles, listado tipos de activos, listado de amenazas, relaciones entre los elementos anteriores); y ii) el interlocutor (Int) válido para la compañía, que se encargará de definir los activos.

- *Tareas:* El proceso estará formado por seis tareas. Las tareas 1, 2 y 3 pueden ejecutarse de forma independiente. La tarea 4 requiere del resultado de las tareas 2 y 3 para poder procesarse. La tarea 5 requiere del resultado de las tareas 1 y 4. Finalmente la tarea 6 requiere del resultado de la tarea 5.
- *Salidas:* La salida producida por este subproceso consistirá en una serie de entregables (InfCtr – Informe del checklist realizado sobre el sistema a nivel de cumplimiento de controles; InfAct - Informe de activos del sistema de información; InfAR - Matriz de riesgos a los que están sometidos los activos del sistema de información y el InfPTR - 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.

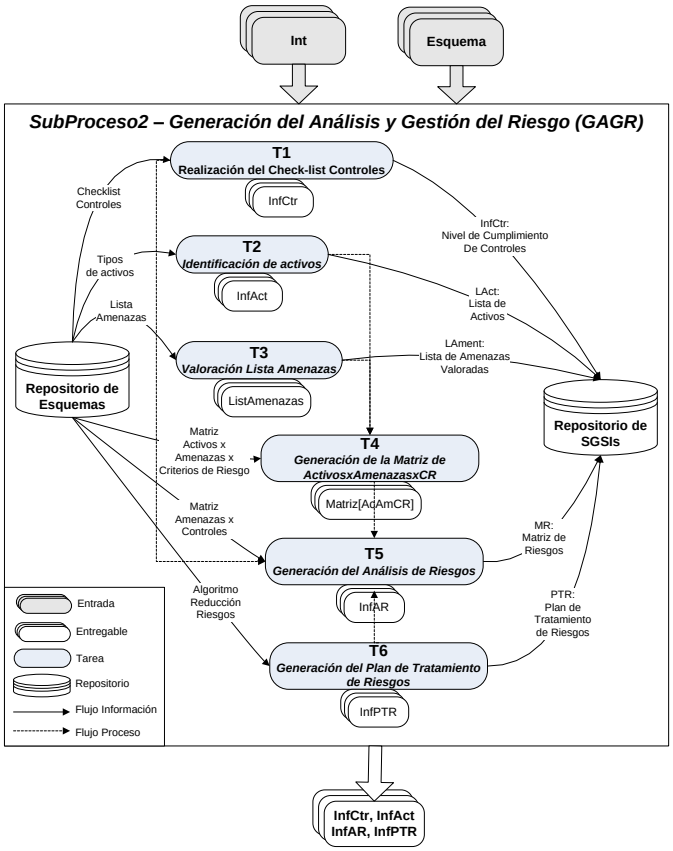

Figura 6. Esquema detallado a nivel de tarea del proceso GAGR.

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

El desarrollo de este proceso está basado en los propuestos por Stephenson, que se centran en la sinergia entre la prueba técnica y el análisis de riesgos tomando como referencia la ISO/IEC27002 [50] y en la metodología de análisis de riesgos Magerit v3.0 [45].

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 al proceso no son aceptados por las compañías. Por ello, la metodología MARISMA simplifica el proceso de evaluación del riesgo para adecuarlo a las PYMES, pero siempre manteniendo la calidad del proceso y haciendo que también sea válido para grandes compañías.

Las principales bases sobre las que se define este proceso son: flexibilidad, simplicidad y eficiencia en costes (humanos y temporales), así como la capacidad de que posteriormente el análisis de riesgos varíe de forma dinámica. Así pues, se trata de un proceso que pretende identificar con el menor coste posible los activos de la compañía y los riesgos asociados, usando para ello los resultados generados en los procesos anteriores y algunos algoritmos.

Para que este proceso 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 los procesos 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 [72].

Las tareas de este proceso se apoyarán en el esquema base generado durante el proceso GEAR.

A continuación mostramos las tareas que componen el proceso:

- *Tarea T1 – Realización del check-list de los controles:* El objetivo de esta tarea es facilitar un punto de partida respecto al nivel de gestión de seguridad actual de la compañía. Para ello la tarea toma como entrada un listado de unas 1.000 preguntas (sub-controles) extraídas en nuestro caso de la ISO/IEC27002:2013. Aunque el número de preguntas parece elevado, es necesario para obtener un resultado con un grado de error bajo, ya que durante la investigación se identificó que solo con 114 preguntas el grado de error era muy elevado. Aun así, tanto en la herramienta construida, como a nivel de la metodología se da la opción por comodidad de contestar solo las 114 preguntas, pero advirtiendo previamente del riesgo

que esto supone.

Como salida de esta tarea se obtiene un elaborado informe de la situación de la compañía, con recomendaciones sobre cómo mejorar y diagramas de kiviat con el nivel de cumplimiento de los literales de la norma ISO/IEC27001:2013 y el de los controles del Anexo A de la misma norma. En la Figura 7 se puede ver un ejemplo de una compañía que ha obtenido un nivel de cumplimiento de la parte de la norma del 78% (alto) y un nivel de cumplimiento de los controles del Anexo A del 41% (medio-bajo).

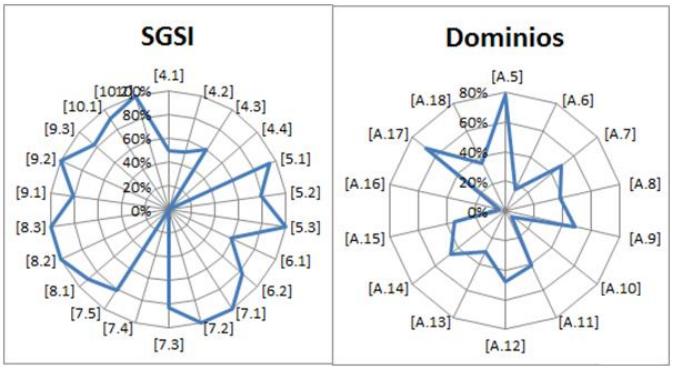

Figura 7. Diagrama de Kiviat del resultado obtenido por una compañía al evaluarse sobre los 1.000 sub-controles.

- *Tarea T2 – Identificación de activos:* El objetivo de la tarea 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 al suponer 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 [45] es que se busca que los activos sean lo más generales (grano grueso), mientras que Magerit intenta identificarlos de forma clara y precisa (grano fino).

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

  En esta tarea el consultor de seguridad (CoS) deberá ayudar el interlocutor (Int) a identificar el conjunto de activos de valor que componen el sistema de información de la compañía, y darles una valoración del 1 al 5, según el nivel de importancia estratégica para la compañía.

  Los resultados generados en esta tarea son fundamentales para poder realizar una evaluación del riesgo y un plan de mejora en las tareas 4, 5 y 6.

- *Tarea T3 – Valoración del listado de amenazas:* El objetivo de la tarea es obtener la valoración de dos variables (*probabilidad de la amenaza y el porcentaje de degradación del activo*) para cada una de las amenazas del esquema seleccionado.

  En este caso, el esquema seleccionado parte de la base de la lista de amenazas de Magerit v3.0 y se han tomado en cuenta 5 rangos de valoración para cada una de las variables en base a las tablas recomendadas en esa misma normativa. Para acelerar la revisión por parte del Responsable de Seguridad de la compañía el esquema precarga los valores que pueden ser más adecuados para la misma, en base a aspectos como: ubicación geográfica, sector empresarial, y tamaño de la compañía. Un extracto de este listado se puede ver en la Figura 8.

Codigo Tipo Amenaza	Tipo de Amenaza	Codigo Amenaza	Amenaza	Probabilidad Amenaza	Porcentaje Degradación Activo
[N]	Desastres naturales	[N.1]	Fuego	2	4
[N]	Desastres naturales	[N.2]	Daños por agua	2	2
[N]	Desastres naturales	[N.*]	Desastres naturales	2	3
[I]	De origen industrial	[I.1]	Fuego	2	3
[I]	De origen industrial	[I.2]	Daños por agua	2	3
[I]	De origen industrial	[I.*]	Desastres industriales	3	3
[I]	De origen industrial	[I.3]	Contaminación mecánica	4	3
[I]	De origen industrial	[I.4]	Contaminación electromagnética	4	4
[I]	De origen industrial	[I.5]	Avería de origen físico o lógico	2	4
[I]	De origen industrial	[I.6]	Corte del suministro eléctrico	2	2

Figura 8. Listado de amenazas para valorar

- *Tarea T4 – Generación de la matriz de [Activos] x [Amenazas] x [Criterios de Riesgo]:* El objetivo de esta tarea es identificar el porcentaje de degradación en que se vería afectado cada criterio de riesgo en el caso de que una amenaza impactase sobre un tipo activo de la compañía con el que está relacionado.

  En nuestro caso se carga la matriz a partir de la que se generó en la tarea 5 del proceso GEAR. Para agilizar el proceso, se eliminan automáticamente aquellos criterios de riesgo que no pueden verse afectados por esa amenaza, y se les identifica con "--". Para los que sí tienen relación se precarga el valor de la columna "*porcentaje de degradación del activo*" calculado en la tarea anterior, de tal forma que el Responsable de Seguridad solo tiene que validar los datos o aceptarlos directamente.

AMENAZAS			ACTIVOS			% DEGRADACIÓN C.R				
ID	TIPO	NOMBRE	ID	TIPO	NOMBRE	C	I	D	A	T
155	[A.10]	Alteración de secuencia	128	[COM]	Equipos de red	--	4	--	--	--
155	[A.10]	Alteración de secuencia	138	[COM]	Sistema de alarma	--	4	--	--	--
155	[A.10]	Alteración de secuencia	127	[SW]	Código fuente	--	5	--	--	--
155	[A.10]	Alteración de secuencia	124	[SW]	Software	--	5	--	--	--
155	[A.10]	Alteración de secuencia	123	[SW]	Software de Servicios	--	5	--	--	--
155	[A.10]	Alteración de secuencia	116	[S]	Dominios	--	5	--	--	--
155	[A.10]	Alteración de secuencia	118	[S]	Servicios Proveedores	--	5	--	--	--
156	[A.11]	Acceso no autorizado	128	[COM]	Equipos de red	5	5	--	--	--

Figura 9. Listado de amenas por activos para valor el porcentaje de degradación de sus criterios de riesgo

- *Tarea T5 – Generación del análisis de riesgos:* Una vez que ya se cuenta con todos los elementos necesarios, esta tarea se ocupa de generar la matriz de riesgos para la compañía utilizando toda la información obtenida en las diferentes tareas y la del esquema seleccionado.

  El resultado que contiene la matriz engloba los siguientes datos:

  - *Bloque Activos:* Tipo, Descripción y Nombre del activo.
  - *Bloque Amenazas:* Código y Nombre de la Amenaza.
  - *Valor - Valor del Activo:* Valor estratégico del activo para la compañía, según los datos introducidos por el Responsable de Seguridad en la tarea T2 del proceso GAGR.
  - *FR – Frecuencia de la Amenaza:* Corresponde al valor introducido en la columna "*probabilidad de la amenaza*" en la tarea T3 del proceso GAGR.
  - *V – Vulnerabilidad:* Esta columna es de gran valor en nuestra metodología, ya que calcula el nivel de la vulnerabilidad de un par [Activo] x [Amenaza] a partir de las respuestas del checklist de la tarea T1 del proceso GAGR, que nos determinan el nivel de cumplimiento de los controles (NCC), por lo que podemos considerar que las vulnerabilidades de un control son (1-NCC). A partir de ese valor, se calcula la media de las vulnerabilidades de todos los controles que intentan proteger ese activo de la amenaza, utilizando para ello la matriz generada en la T6 del proceso GEAR.
  - *Bloque Dimensiones:* Se muestran los valores para cada una de las dimensiones definidas, en base a los valores aprobados en la T4 del proceso GAGR.
  - *IT – Impacto Técnico:* Se calcula como el máximo valor de los criterios de riesgo.
  - *IMP - Impacto:* Se calcula como el [Valor Activo] x [IT – Impacto Técnico].
  - *Nivel Riesgo:* Es el nivel de riesgo en ausencia de controles, es decir, partiendo de que las vulnerabilidades de los controles son el 100%. Y se calcula como el [Impacto] * [Probabilidad de ocurrencia], y sobre una escala que va del [1 al 500], siendo 500 el riesgo máximo que se puede alcanzar.
  - *Nivel Riesgo Actual:* Es el nivel de riesgo teniendo en cuenta el nivel de implantación y activación de los controles actuales. Se calcula como [Nivel de Riesgo] * [Vulnerabilidad], y se mueve en un rango de [1-500].
  - *ER – Escala de Riesgo:* Está columna no permite dividir los valores de riesgo en 10 niveles, en base a una escala logarítmica, que se calcula aplicando la formula indicada en la Ecuación 1.

$$y = a^x$$
$$500 = a^{10}$$
$$log\ 500 = 10\ log\ a$$
$$log\ a = \frac{log 500}{10} = 0{,}26989700$$
$$a = 10^{0{,}26989} = 1{,}8616455$$
$$y = a^x \rightarrow x = \frac{\log y}{\log 1{,}86164}$$

Ecuación 1. Calculo niveles para riesgo.

Los resultados de aplicar la Ecuación 1 sobre una escala de riesgo máximo de 500 se puede ver de forma numérica y grafica en la Figura 10.

X	Y
0	1,000
1	1,861
2	3,465
3	6,451
4	12,011
5	22,360
6	41,627
7	77,496
8	144,269
9	268,579
10	499,994

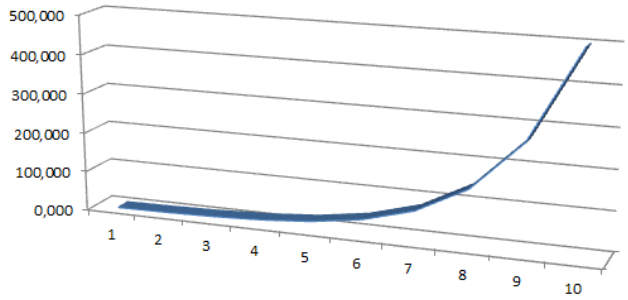

Figura 10. Escala logarítmica para el cálculo de los niveles de riesgo

Para la metodología actual se ha considerado que las compañías deben tratan los riesgos que quedan por encima de 6.

ACTIVOS		AMENAZAS				DIMENSIONES							RIESGOS		
Tipo	Activo	AMENAZAS	Valor	FR	V	C	I	D	A	T	IT	IMP	Nivel Riesgo	Nivel R. Actual	ER
[D]	Contratos	[E.1]	5	100%	44%	80	80	80	--	--	80	400	400	177	8
[Keys]	Llaves criptográficas	[E.1]	5	100%	44%	80	80	80	--	--	80	400	400	177	8
[SW]	Código fuente	[A.8]	5	60%	50%	100	100	100	--	--	100	500	300	151	8
[P]	Empleados	[E.28]	3	80%	75%	--	--	60	--	--	60	180	144	108	7
[D]	Acuerdos de Servicio	[E.1]	3	100%	44%	80	80	80	--	--	80	240	240	106	7
[D]	Información financiera	[E.1]	3	100%	44%	80	80	80	--	--	80	240	240	106	7
[D]	Passwords	[E.1]	3	100%	44%	80	80	80	--	--	80	240	240	106	7
[D]	Pólisas de Seguro	[E.1]	3	100%	44%	80	80	80	--	--	80	240	240	106	7
[D]	Registros	[E.1]	3	100%	44%	80	80	80	--	--	80	240	240	106	7
[Keys]	Certificados SSL/TLS	[E.1]	3	100%	44%	80	80	80	--	--	80	240	240	106	7
[SW]	Software	[E.1]	3	100%	44%	80	80	80	--	--	80	240	240	106	7
[SW]	Software de Servicios	[E.1]	3	100%	44%	80	80	80	--	--	80	240	240	106	7
[S]	Dominios	[E.1]	3	100%	44%	80	80	80	--	--	80	240	240	106	7
[SW]	Código fuente	[E.8]	5	40%	51%	100	100	100	--	--	100	500	200	103	7
[D]	Información de respaldo	[A.18]	5	40%	36%	--	--	100	--	--	100	500	200	73	6
[D]	Información empleados	[A.18]	5	40%	36%	--	--	100	--	--	100	500	200	73	6
[SW]	Código fuente	[A.18]	5	40%	36%	--	--	100	--	--	100	500	200	73	6
[D]	Contratos	[A.19]	5	40%	35%	100	--	--	--	--	100	500	200	70	6

Figura 11. Matriz de Riesgos

Para finalizar esta tarea se aplica un algoritmo que combina todos los elementos anteriores, generando un resultado como el que se puede ver en la Figura 11, aunque en este caso se ha mostrado de forma resumida por motivos de espacio.

- *Tarea T6 – Generación del plan de tratamiento de riesgos:* Una vez que en la tarea anterior hemos generado la matriz de riesgos, el objetivo de esta tarea es la de ejecutar un algoritmo recursivo que permita ir calculando cuáles deben ser los controles que la compañía debe aplicar en orden para ir minimizando sus riesgos hasta alcanzar un nivel aceptable (ER<=6).

  Para ello, el algoritmo elige el registro con el mayor "*nivel de riesgo actual*" y extrae los controles relacionados, seleccionando el que supone una mayor vulnerabilidad, generando un paso de recomendación para aplicarlo, y recalculando toda la matriz de riesgo de nuevo para determinar si sigue existiendo un riesgo superior al aceptable, y en caso afirmativo, cuál es el nuevo control que deberíamos acometer.

Orden	Código	Control	N.C	Riesgo	R.Actual	ER
0	[A.14.2.3]	Revisión técnica de las aplicaciones ...	0	400	177	8
1	[A.14.2.7]	Externalización del desarrollo de software	0	400	170	8
2	[A.18.1.2]	Derechos de propiedad intelectual (DPI)	0	400	165	8
3	[A.5.1.2]	Revisión de la política de seguridad de la información	0	400	164	8
4	[A.7.2.3]	Proceso disciplinario	0	400	150	8
5	[A.8.1.3]	Uso aceptable de los activos	0	300	145	8
6	[A.18.1.5]	Regulación de los controles criptográficos.	0	400	142	7
7	[A.18.2.2]	Cumplimiento de las políticas y normas de seguridad.	0	400	138	7
8	[A.18.2.3]	Comprobación del cumplimiento técnico.	0	400	130	7
9	[A.16.1.2]	Notificación de los eventos de ...	0	192	124	7
10	[A.15.1.3]	Cadena de suministro de tecnología ...	0,04	400	120	7
11	[A.16.1.4]	Evaluación y decisión sobre los eventos	0,12	300	116	7
12	[A.16.1.5]	Respuesta a incidentes de seguridad de la ...	0,11	300	110	7
13	[A.9.1.1]	Política de control de acceso	0,07	300	106	7
14	[A.16.1.6]	Aprendizaje de los incidentes de	0,23	300	105	7
15	[A.17.1.3]	Verificación, revisión y evaluación de la ...	0,04	300	100	7
16	[A.8.1.2]	Propiedad de los activos	0	300	90	7
17	[A.16.1.3]	Notificación de puntos débiles de la seguridad	0,1	300	88	7
18	[A.17.1.2]	Implementar la continuidad de la seguridad de la	0,13	300	83	7
19	[A.8.2.1]	Clasificación de la información	0,53	300	81	7
20	[A.6.1.2]	Segregación de tareas	0	192	79	7

Figura 12. Controles del plan de tratamiento de riesgos.

De la ejecución del algoritmo se obtienen dos resultados de gran interés para la compañía.

- *Listado de controles* que debe acometer para reducir el riesgo a un nivel aceptable (ver Figura 12): Dentro de este listado se mostrará el orden de prioridad de los controles en que se recomienda que sean acometidos, el nivel de cobertura (N.C) actual de cada uno de ellos en base a las respuesta que se dio en el checklist, así como el nivel de riesgo actual y la escala de riesgo.

  En el ejemplo que se muestra en la Figura 12, se puede ver cómo a una compañía sólo le recomienda acometer 20 controles de los 114 del esquema utilizado. El resto se considera que tienen un nivel de cobertura adecuado o que el nivel de vulnerabilidad no hace que el riesgo de los activos que protege suba por encima del nivel adecuado.

Paso 0:

El *riesgo máximo actual* de la compañía (una vez acometidos los pasos anteriores) es 176 sobre un rango de [0-500], con un riesgo aceptable por debajo de [77 – Nivel 6].

El *Activo más afectado* por este riesgo es: "Llaves criptográficas de acceso a terminales, llaves criptográficas de cifrado/descifrado de información (Llaves criptográficas)", cuya pérdida tendría un coste para la organización de 125.000€, y cuyo valor estratégico para la compañía es Alto, siendo el tipo del activo "[Keys]", el cual tiene una Probabilidad de Ocurrencia [Muy Alta, 5.0] y una Degradación (daño causado por un incidente en el supuesto de que ocurra) [Alto, 4.0].

Los *principales criterios de riesgos* que se verán afectados son ["Disponibilidad - Integridad - Confidencialidad"].

Para este la terna *[Activo x Amenaza x Control]* = ["Errores de los usuarios", "[A.14.2.3] - Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo."] se han calculado los siguientes valores:

a) Impacto sobre el activo, calculado como ([Valor Activo]*[Degradación del valor]) = 80;

b) Riesgo sobre el activo, calculado como ([Impacto]*[Probabilidad de Ocurrencia]) = 400.0;

c) El Nivel de Cobertura del Control calculado como el Sumatorio del nivel de cumplimiento de los subcontroles es 0.0;

d) El Riesgo final sobre el activo, calculado como ([Riesgo]*[1-Nivel de cobertura del Control]) = 176.576.

Por ello, se recomienda acometer la activación del control: ***[A.14.2.3] (Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.).***

Figura 13. Pasos para el plan de tratamiento de riesgo.

- *Listado de pasos* detallados describiendo todos los elementos involucrados (ver Figura 13): Se puede ver cómo para cada uno de los pasos que ha considerado el algoritmo, el sistema va a describir todos los elementos que se ven afectados intentando justificar por qué recomienda que se mejore ese control de forma específica. El objetivo es que el Responsable de Seguridad tenga una justificación clara ante la dirección de la empresa de por qué debe acometer esa inversión.

Con esta última tarea, se finalizaría el proceso de generación del Análisis de Riesgos y del Plan de mejora. Aunque inicialmente el proceso puede parecer complejo, la herramienta que se ha creado y que lo soporta incluye facilidades que permiten que en un solo día una compañía pueda realizar su análisis de riesgos, obteniendo resultados de gran valor para ella.

D. Proceso 3: Mantenimiento Dinámico del Análisis de Riesgos (MDAR).

Una vez que hemos conseguido que el sistema sea capaz de generar un análisis de riesgos de bajo coste y con un elevado nivel de detalle y valor para la compañía, desde la

metodología se ha buscado solucionar otro de los grandes problemas que tienen actualmente este tipo de sistemas para las empresas, y es el coste del mantenimiento de este tipo de procesos y el poco valor que aporta una imagen estática a medio plazo. Es decir, las empresas requieren de un análisis de riesgos que tenga la capacidad de ir cambiando con el tiempo mientras suceden eventos de seguridad dentro de la compañía.

Por ello, el principal objetivo de este proceso es establecer mecanismos que nos permitan ir actualizando de forma dinámica el análisis de riesgos, con el objetivo de maximizar el valor que este sistema puede aportar a la compañía.

En la Figura 14 se puede ver el esquema básico de entradas, tareas y salidas que componen este proceso:

- *Entradas:* Como entrada se recibirán los datos de la compañía y el SGSI implementado por la misma, así como el estado actual de las métricas e indicadores que permitirán al sistema funcionar.

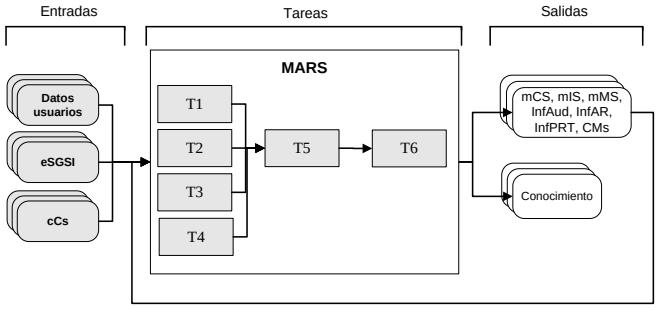

Figura 14. Esquema simplificado a nivel de tarea del proceso MDAR.

- *Tareas:* El proceso estará formado por seis tareas. Las tareas 1-4 pueden ejecutarse de forma independiente, e irán alimentado las entradas de la matriz de riesgo que se irá recalculando según la información que reciba de éstas. La tarea 6 irá mostrando de forma gráfica mediante un dashboard el nivel de cobertura de los controles de seguridad en cada momento.
- *Salidas:* La salida producida por este sub-proceso consistirá en una serie de entregables (mCS – Informe del nivel de cultura de la seguridad; mIS - Informe de incidentes de seguridad; mMS – Informe de las métricas de seguridad; InfAud – Informe de las Auditorías Anuales; InfAR – Matriz de Riesgos dinámica; InfPTR – Plan de Tratamiento de Riesgos Dinámico; CMs – Dashboard representando en tiempo real el nivel de gestión de la seguridad de la compañía.

En la Figura 15 se pueden ver las tareas del proceso de forma mucho más detallada, mostrando cómo interactúan con el repositorio de Esquemas y de SGSIs encargado de contener los elementos que conforman la parte del Análisis de Riesgos del SGSI. Cada tarea generará un entregable para su análisis por parte del consultor de seguridad (CoS) y almacenará la información para que sea utilizada por las tareas T5 y T6 del proceso MDAR (Mantenimiento Dinámico del Análisis de Riesgos).

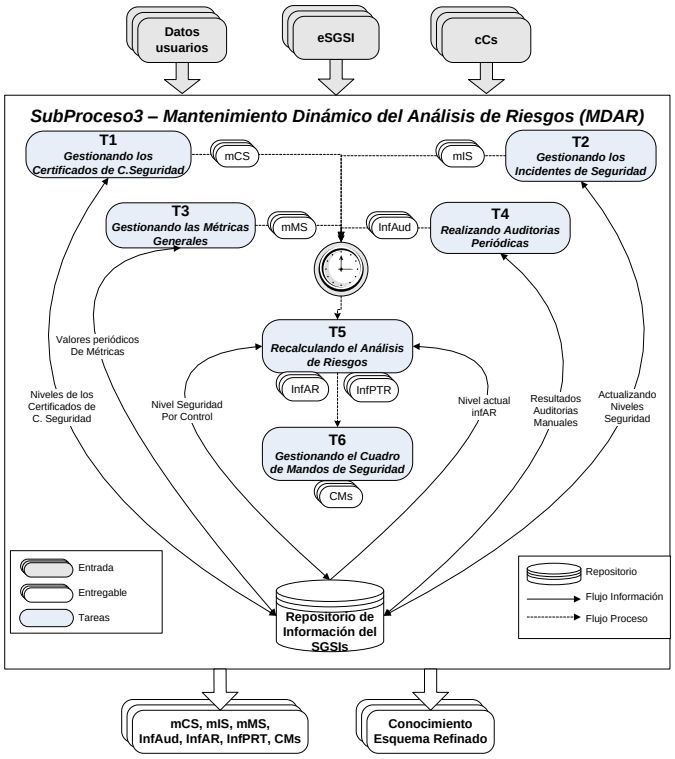

Figura 15. Esquema detallado a nivel de tarea del proceso MDAR.

Las principales bases sobre las que se define este proceso son: simplicidad, eficiencia en costes (humanos y temporales), y usabilidad (capacidad de que la compañía tenga información actualizada de los riesgos).

Las tareas de este proceso se apoyarán en el esquema base generado durante el proceso GEAR y en el análisis de riesgos generado en el proceso GAGR.

A continuación mostramos las tareas que componen el proceso:

- *Tarea T1 – Gestión de los certificados de Cultura de la Seguridad:* El objetivo de esta tarea es auto-evaluar al personal periódicamente con preguntas extraídas de la política de seguridad y del documento de aplicabilidad de la compañía (SOA). Cada una de estas preguntas se encuentra vinculada a uno o varios controles del esquema. Cuando un usuario responde correctamente una pregunta, se refuerza en un porcentaje (Ej: 1%) el nivel de cobertura de los controles asociados, y cuando la falla el nivel de cobertura baja en un porcentaje similar. El porcentaje es configurable porque depende del número de empleados de la compañía y la periodicidad de la prueba.

  Está métrica está basada en el concepto de Cultura de la Seguridad (CS) y el factor humano, cuanto mayor sea el nivel de CS de una compañía, menor es la vulnerabilidad de los controles.
- *Tarea T2 – Gestión de los incidentes de seguridad:* El objetivo de esta tarea es que cada vez que se produzca un incidente de seguridad, éste se asocie con la

amenaza que lo ha producido, y por medio de la matriz de [Amenazas] x [Controles] podamos penalizar el nivel de cumplimiento de los controles asociados con dicha amenaza. El porcentaje es configurable, dependiendo del número de empleados de la compañía y la periodicidad de la prueba.

Está métrica está basada en que la ocurrencia de un incidente de seguridad es la transformación de una amenaza que ha conseguido aprovechar un fallo en un control y por lo tanto implica que esos controles no son tan seguros como la compañía piensa y deben ser revisados y reforzados.

- *Tarea T3 – Gestión de métricas generales:* El objetivo de esta tarea es establecer métricas sobre los controles. Cada métrica activada sobre un control y que se incumpla penalizará a los controles asociados. El porcentaje de la penalización es configurable al depender del número de empleados de la compañía y la periodicidad de la prueba.
- *Tarea T4 – Realización de auditorías periódicas:* El objetivo de este control es que cada vez que se realice una auditoría interna o externa que detecte no conformidades en controles, altere el valor de dichos controles de forma manual.
- *Tarea T5 – Recalculo Dinámico del Análisis de Riesgos:* Cada vez que una de las cuatro primeras tareas produzca un evento sobre el nivel de cobertura de los controles, el sistema recalculará de nuevo el análisis de riesgos de la compañía y el plan de mejora recomendado, de forma que siempre estará actualizado con respecto al estado real de la compañía.
- *Tarea T6 – Gestionando el cuadro de mandos de Seguridad:* Toda la información del nivel de cobertura de los controles se irá mostrando de forma dinámica en un cuadro de mando (Dashboard) de forma que tanto el Responsable de Seguridad como la Dirección de la compañía podrán ver de forma visual el estado de la gestión de seguridad de la misma.

De esta forma, se ha desarrollado un proceso de muy bajo coste de mantenimiento para la compañía y que le permite tener un sistema de análisis de riesgos completamente dinámico y con la capacidad de informar en todo momento de la situación real de la compañía, lo que es de enorme valor para ella.

IV. Conclusiones.

En este artículo se ha presentado la propuesta de una metodología innovadora para realizar el análisis y gestión del riesgo denominado MARISMA-ARG, que 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 el caso de las PYMES.

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

El proceso MARISMA-AGR cumple con los objetivos propuestos, así como con los principios que según la OCDE [73] debe seguir todo proceso de evaluación del riesgo, según el cual el sistema debe tener la capacidad de autoevaluar su riesgo de forma continuada en el tiempo, proponiendo medidas.

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

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

AGRADECIMIENTOS

Esta investigación ha sido co-financiada es parte por los proyectos ERABAC (1315ITA227) y ESACC (1315ITA225) financiados por la “D.G. de Empresas, Competitividad e Internacionalización de la Consejería de Economía, Empresas y Empleo de la JCCM”, los proyectos SIGMA-CC (TIN2012-36904) y GEODAS (TIN2012-37493-C03-01) financiados por el “Ministerio de Economía y Competitividad y Fondo Europeo de Desarrollo Regional FEDER” (España), del proyecto SERENIDAD (PEII14-2014-045-P) financiados por la “Consejería de Educación, Ciencia y Cultura de la Junta de Comunidades de Castilla-la Mancha y el Fondo Europeo de Desarrollo Regional FEDER” (España), del proyecto “Plataformas Computacionales de Entrenamiento, Experimentación, Gestión y Mitigación de Ataques a la Ciberseguridad - Código: ESPE-2015-PIC-019” financiado por la ESPE y CEDIA (Ecuador), y del proyecto PROMETEO financiado por la Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT) del Gobierno de Ecuador.

Referencias

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

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

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

[30] 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.

[31] 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.

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

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

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

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

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

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

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

[39] 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).

[40] 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.

[41] 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.

[42] 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.

[43] 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.

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

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

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

Antonio Santos-Olmo is MsC in in Computer Science and is an Assistant Professor at the Escuela Superior de Informática of the Universidad de Castilla- La Mancha in Ciudad Real (Spain) (Computer Science Department, University of Castilla La Mancha, Ciudad Real, Spain), MSc in Information Systems Audit from the Polytechnic University of Madrid, and Certified Information System Auditor by ISACA. He is the Director of Software Factory departments of the company Sicaman Nuevas Tecnologías S.L. His research activities are management security system, security metrics, data mining, data cleaning, and business intelligence. He participates in the GSyA research group of the Department of Computer Science at the University of Castilla- LaMancha, in Ciudad Real (Spain).

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

Esther Álvarez President of Private Foundation In-nova and Research of the UPM. Consultant in strategic communications programs radio, mobile and wireless both public and private sectors and in civil and military. Currently a member of the board of the Delegation of COIT (Association of Telecommunications Engineers) CLM, representative of Castilla La Mancha in the groups of the free and COIT New Technologies of the National Coordinator of the Treatment Research Chair in Digital Image at the Madrid Polytechnic University of Madrid. PhD in Information Systems specializing in Business ETSI Industriales (UPM) and the Specialty Program Communications Signals, Systems and Radiocommunications Department SSR ETSI Telecomunicaciones (UPM).

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

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