Características deseables para un SGSI orientado a PYMES

Luís Enrique Sánchez[1], Antonio Santos-Olmo[1], Eduardo Fernández-Medina[2] y Mario Piattini[3]

[1]SICAMAN Nuevas Tecnologías. Departamento de I+D,
Juan José Rodrigo, 4. Tomelloso, Ciudad Real, España.
{lesanchez, asolmo} @sicaman-nt.com
[2] Grupo de Investigación GSyA. Universidad de Castilla-La Mancha
Paseo de la Universidad, 4 – 13071 Ciudad Real, Spain
Eduardo.FdezMedina@uclm.es
[3] Grupo de Investigación ALARCOS. Universidad de Castilla-La Mancha
Paseo de la Universidad, 4 – 13071 Ciudad Real, Spain
Mario.Piattini@uclm.es

Resumen. La sociedad de la información cada vez depende más de los Sistemas de Gestión de la Seguridad de la Información (SGSI), y poder disponer de estos sistemas ha llegado a ser vital para la evolución de las PYMES. Sin embargo, este tipo de compañías requiere de SGSIs adaptados a sus especiales características, y que estén optimizados desde el punto de vista de los recursos necesarios para implantarlos y mantenerlos. En este artículo se presenta un análisis de las diferentes propuestas que están surgiendo orientadas a implantar los SGSIs en las PYMES, con el objetivo de determinar las características que debería tener una metodología de gestión de seguridad orientada a las PYMES.

Palabras clave: SGSI, PYMES, Gestión de la Seguridad, Niveles de Madurez

1 Introducción

Para las empresas, es muy importante implantar controles de seguridad que les permita conocer y controlar los riesgos a los que pueden estar sometidas [1, 2]. Pero la implantación de estos controles no es suficiente, siendo necesarios sistemas que gestionen la seguridad a lo largo del tiempo, de modo que les permita reaccionar ágilmente ante nuevos riesgos, vulnerabilidades, amenazas, etc. [3]. Sin embargo, es frecuente que las empresas no tengan sistemas de gestión de seguridad, o que si los tienen, éstos estén elaborados sin unas guías adecuadas, sin documentación y con recursos insuficientes [4].

Por lo tanto, a pesar de que la realidad ha 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 [5], el nivel de implantación con éxito de estos sistemas, realmente es muy bajo. Este problema 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].

De acuerdo a investigaciones recientes [6], el éxito de los SGSI, depende principalmente de los siguientes factores: i) enfocar la seguridad hacia el negocio; ii) implementar la seguridad en consonancia con la cultura de la empresa; iii) conseguir el apoyo indiscutible, visible y comprometido de la dirección de la empresa; iv) conseguir entender bien los requisitos de seguridad, de la evaluación y gestión de los riesgos; v) concienciar tanto a directivos como a empleados de la necesidad de la seguridad; vi) ofrecer formación y guías sobre políticas y normas a toda la organización; vii) definir un sistema de medición para evaluar el rendimiento de la gestión de la seguridad y sugerir mejoras. Para el caso de las PYMEs, estos factores son importantes, pero además, el SGSI debe estar optimizado en cuanto a recursos necesarios, y también debe tener un alcance suficiente, para no descuidar la seguridad, pero no excesivo, para controlar su coste. Por ese motivo, es muy importante poder contar con metodologías para la gestión de la seguridad de la información que estén especialmente diseñados para este tipo de empresas, y que además permitan reutilizar el conocimiento, de modo que su implantación sea más rápida, más certera y más económica.

Como mostraremos posteriormente en este artículo, existen ya algunas propuestas para la gestión de la seguridad de la información (ISO/IEC27001, ISO/IEC21827, ISM3, propuesta de Areiza, propuesta de Eloff, ASD, IS2ME, propuesta de Carey-Smith, propuesta de Tawileh, etc), casi todos elaborados por organizaciones internacionales de estandarización. Sin embargo, a pesar de que estas propuestas son muy completas e interesantes, están principalmente orientadas a grandes empresas. De hecho, hay numerosas fuentes de investigación ([3], [7]) que confirman que estas propuestas no son nada adecuadas para las PYMES, ofreciendo procesos excesivamente burocráticos y costosos para ellas.

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 la gestión de seguridad 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 elaborado una metodología (MGSM-PYME) para la gestión de la seguridad y el establecimiento del nivel de madurez de los sistemas de información de las PYMES [8-11], y además hemos construido una herramienta que automatiza completamente la metodología [12], y lo hemos aplicado en casos reales [13], lo que nos ha permitido validar tanto la metodología como la herramienta. A través de esta metodología, uno de los artefactos que se obtienen son los Esquemas de SGSI, que son una plantilla completa que permite la implantación inmediata del SGSI en las empresas. Hay un Esquema para cada tipo de sector empresarial, obtenidos del Código Nacional de Actividades Económicas Español (CNAE), de modo que la experiencia de la aplicación de esta metodología se va acumulando en los esquemas, lo que ayuda a que la implantación de los SGSI (de cada sector empresarial), sean incrementalmente más precisos, más económicos y más rápidos. La aportación principal de este artículo se centra en presentar los esquemas que son construidos por la metodología MGSM-PYME.

El artículo continúa en la Sección 2, describiendo las metodologías y modelos para la gestión de la seguridad existentes y su tendencia actual para el caso de las PYMES. En la Sección 3 se analizan las características que debería tener la nueva metodología para adaptarse a las PYMES, obtenidas mediante la aplicación del método de investigación "investigación-acción" en casos reales. En la Sección 4 se introducen las actividades que conforman la nueva metodología y sus principales características. En la Sección 5 se analizan las relaciones existentes entre las diferentes propuestas analizadas y la MGSM-PYME. Finalmente, en la Sección 6 concluimos indicando cuál será el trabajo que desarrollaremos en el futuro.

2 Trabajo relacionado

Con el propósito de reducir las carencias mostradas en el apartado anterior y reducir las pérdidas que éstas ocasionan, ha aparecido un gran número de procesos, marcos de trabajo y métodos de la seguridad de la información cuya necesidad de implantación 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 los modelos de gestión de la seguridad han tomado como base el estándar internacional ISO/IEC17799 e ISO/IEC27002, y que los modelos de gestión de seguridad que están teniendo mayor éxito en las grandes compañías son ISO/IEC27001, COBIT e ISM3, pero que son muy difíciles de implementar y requieren una inversión demasiado alta que la mayoría de las PYMES no pueden asumir [14]. Aunque están surgiendo nuevas propuestas muy interesantes orientadas a este tipo de compañías, afrontan los problemas de una forma muy incompleta.

Entre los principales estándares de gestión de la seguridad se encuentran:

- ISO/IEC27001 [15]: Este estándar fue confeccionado para proveer un modelo para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI. La ISO/IEC27001, deja total libertad en los criterios para establecer el proceso global de seguridad y elegir el método para analizar, evaluar y gestionar los riesgos. En un proyecto de SGSI, esta libertad también puede convertirse en una deficiencia, pues en cierta forma está ligando estos proyectos a la propia experiencia de diseño de procesos de seguridad de los ejecutores del mismo.
- ISO/IEC20000 [16] e ITIL [17]: Son un extenso conjunto de procedimientos de gestión creados para facilitar a las organizaciones lograr la calidad y eficiencia en las operaciones de TI. Algunas de las críticas que se realizan son: i) carece de un modelo de madurez; ii) las métricas que tiene son muy pobres; iii) la gestión de los requerimientos es pobre; iv) carece de análisis y gestión de riesgos; v) carece de guías de implantación; vi) no suele tener éxito en las PYMES.
- COBIT [18]: COBIT es una metodología para el adecuado control de los proyectos de tecnología, los flujos de información y los riesgos que implican la falta de controles adecuados. La metodología COBIT se utiliza para planear, implementar, controlar y evaluar el gobierno de las TIC,

incorporando objetivos de control, directivas de auditoría, medidas de rendimiento y resultados, factores críticos de éxito y modelos de madurez. El principal problema que presenta es su complejidad para implantarse en compañías pequeñas.

- ISM3 [19]: Este modelo de gestión de la seguridad y su madurez está orientado a implementar un SGSI y a definir diferentes niveles de seguridad, donde cada uno de ellos puede ser el objetivo final de una organización. El principal problema de ISM3 es que, al igual que el resto de estándares, es demasiado generalista, intentando que la metodología sea útil para todos los tipos de compañías, lo que hace que su implantación sea costosa y difícil para el caso de las PYMES.

Fig. 1 Propuestas de SGSI orientadas a PYMES.

En el estudio de la literatura existente se han hallado diferentes intentos (ver Figura 1) para resolver la problemática de aplicar los modelos SGSI tradicionales en la PYME centradas en algunos aspectos de los SGSIs. En las siguientes sub-secciones se muestran algunos de los modelos de madurez para la gestión de la seguridad que se están desarrollando orientados a PYMES y que, si bien no resuelven los problemas existentes, sí se ha considerado que tienen aportaciones interesantes que deben ser analizadas. Entre ellas podemos destacas:

- Propuesta de Eloff [20]: Este modelo define la implantación de un SGSI utilizando el ciclo PDCA, pero definiendo cuatro clases distintas de protección que permiten ir incrementando de forma progresiva los niveles de seguridad, basándose para ello en las secciones de la norma ISO/IEC17799 [21]. Más que un nuevo estándar, pretende aportar una mejora a la norma ISO/IEC17799 dividiendo sus dominios en niveles de madurez.
- Propuesta de Areiza [22]: Esta propuesta de modelo de madurez consiste 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. Este modelo tiene en cuenta que las organizaciones tienen estructuras internas diferentes, por lo

cual se considera que los controles definidos en cada nivel son los mínimos o más generales que deberían establecer las organizaciones, cualquiera que sea su estructura interna.

- Propuesta de Dojkovski [6] y Propuesta de Sneza [23]: Plantean la construcción de un SGSI orientado a las PYMES tomando como punto central la cultura de la seguridad. Las principales conclusiones obtenidas de la aplicación de estos marcos de trabajo son que aunque tiene valor de forma individual para identificar que elementos debería tener un SGSI, no es un modelo completo y utilizable.
- IS2ME [24]: Trata de cubrir el hueco existente entre el incumplimiento total y la implantación metodológica de la gestión de la seguridad mediante un estándar como ISO/IEC27001 [15]. Aunque intenta ser un método sencillo, su aplicación en la práctica requiere de gran inversión de tiempo por parte del consultor y del personal de la empresa.
- Propuesta de Wiander y Holapa [25]: Pretende ser un método de desarrollo de SGSIs tomando como base la ISO/IEC17799 y orientándola a PYMES. Aunque es un método sencillo para la implantación de SGSI, tiene grandes carencias ya que no entra en la gestión del riesgo y carece de métricas.
- Propuesta de Carey-Smith [26]: Aplica una serie de iteraciones de ciclos AR para desarrollar un SGSI, en la que cada final de fase sirve para obtener un aprendizaje que sirve de diagnostico para la siguiente fase. Al igual que otros modelos, el mayor problema que tiene es su excesiva simplicidad, no aportando un mecanismo real para implantar y mantener un SGSI.
- Propuesta de Tawileh [27]: Propone un sistema basado en una metodología para sistemas simples (SSM) con el objetivo de facilitar el desarrollo de sistemas de gestión de la seguridad dentro de las PYMES. Esta no entra realmente en cómo hacer las cosas, quedándose solo en la definición de los pasos del SGSI, dejando de lado los aspectos de gestión del riesgo, controles, activos o métricas, que son fundamentales para el SGSI.

En numerosas fuentes bibliográficas se detecta y resalta la dificultad que supone para las PYMES la utilización de las metodologías y modelos de madurez para la gestión de la seguridad tradicionales, que han sido concebidos para grandes empresas [28-31]. Se justifica en repetidas ocasiones que la aplicación de este tipo de metodologías y modelos de madurez 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 [32].

Por lo tanto, y como conclusión de este apartado, se puede decir que es pertinente y oportuno abordar el problema de desarrollar una nueva metodología para la gestión de la seguridad y su madurez para los sistemas de información en las PYMES con un modelo que valide su funcionamiento, así como una herramienta que soporte este modelo, tomando como base la problemática a que este tipo de compañías se enfrenta y que ha llevado a continuos fracasos en los intentos de implantación en este tipo de empresas.

3 Características de un SGSI orientado a PYMES

La metodología para la gestión de la seguridad y su madurez en las PYMES que se ha desarrollado, permite a cualquier organización gestionar, evaluar y medir la seguridad de sus sistemas de información, pero está orientado principalmente a las PYMES, ya que son las que tiene mayor tasa de fracaso en la implantación de las metodologías de gestión de la seguridad existentes.

En este apartado, se analizan las metodologías que sería deseable que tuviera un SGSI para su implantación y correcto funcionamiento dentro del entorno de las PYMES. Estas características han sido obtenidas mediante el análisis detallado del estándar ISO27001 y el método de investigación en acción. En la Figura 2 se pueden ver las once principales características que se ha determinado que debería tener una metodología de implantación de SGSIs orientada a las PYMES. Estas once características han sido obtenidas mediante la aplicación del método "*investigación en acción*", en casos reales.

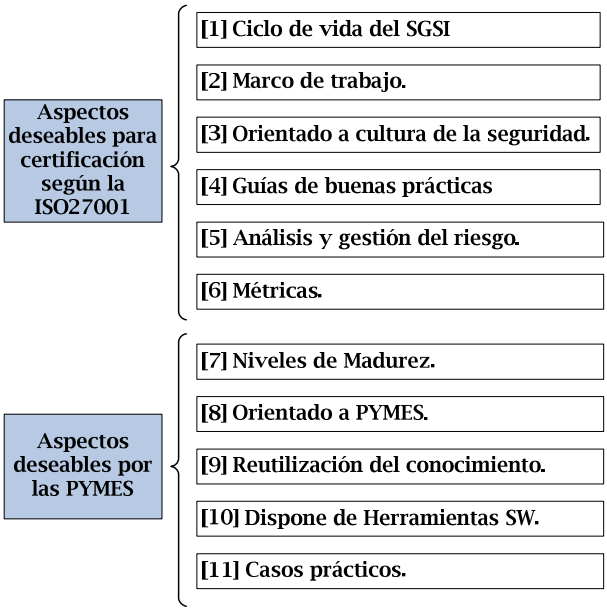

Fig. 2 Características deseables de un SGSI en las PYMES.

Partiendo de estas características, la metodología para la gestión de la seguridad y su madurez en las PYMES que se ha desarrollado, permite a cualquier organización gestionar, evaluar y medir la seguridad de sus sistemas de información, pero está orientado principalmente a las PYMES, ya que son las que tiene mayor tasa de fracaso en la implantación de las metodologías de gestión de la seguridad existentes.

Uno de los objetivos perseguidos en la metodología MGSM–PYME es que sea sencilla de aplicar, y que el modelo desarrollado sobre ella permita obtener el mayor nivel de automatización y reusabilidad posible con una información mínima, recogida

en un tiempo muy reducido. En la metodología se ha priorizado la rapidez y el ahorro de costes, sacrificando para ello la precisión que ofrecían otras metodologías, es decir, la metodología desarrollada busca generar una de las mejores configuraciones de seguridad pero no la óptima, priorizando los tiempos y el ahorro de costes frente a la precisión, aunque garantizando que los resultados obtenidos tengan la calidad suficiente.

	Ciclo de SGSI	**Marco de trabajo**	**Niveles de madurez**	**Cultura de .seguridad**	**Guía de buenas practicas**	**Análisis de riesgos**	**Métricas**	**Orientado a PYMES**	**Reutiliza el conocimiento**	**Dispone de herramienta Sw**	**Casos prácticos**
ISO/IEC27000	Si	Si	Si	Parc	Si	Si	Parc	No	No	Parc	Si
ISO/IEC15408/CC	No	No	Si	No	No	No	Parc	No	No	Parc	Si
ISO/IEC21827/SSE–CMM	Si	Si	Si	No	No	Parc	No	No	No	Parc	Si
ISO/IEC20000	Si	Si	No	No	Si	No	No	No	No	Parc	Si
ITIL	Si	Si	No	No	No	No	No	No	No	Parc	Si
COBIT	Si	Si	No	Parc	Si	Si	Si	No	No	Si	Si
ISM3	Si	Si	Si	No	Si	Parc	Si	Parc	No	Parc	Si
Propuesta de Eloff	No	No	Si	No	Si	No	Si	Si	No	No	No
Propuesta de Areiza	No	No	Si	No	Si	No	No	Si	No	No	No
Propuesta de Dojkovski	No	Si	No	Si	No	No	No	Parc	No	No	Parc
IS2ME	Si	No	No	No	Si	No	No	Si	No	Parc	Si
ASD	Parc	Parc	Si	No	Si	Parc	No	Si	No	No	Parc
Propuesta de Carey-Smith	Parc	No	No	No	Si	No	No	Si	Parc	No	No
Propuesta de Tawileh	Si	No	No	No	No	No	No	Si	No	No	Si
Propuesta de Sneza	No	Si	No	Si	No	No	No	Parc	No	No	Si
MGSM–PYME	**Si**	**Si**	**Si**	**Si**	**Si**	**Si**	**Si**	**Si**	**Si**	**Si**	**Si**

Tabla 1. Comparativa de metodologías de gestión de seguridad y características deseables para los SGSI en las PYMES.

En la Tabla 1 se puede ver una comparativa de los diferentes modelos, metodologías y guías analizadas en la sección anterior para gestionar la seguridad, incluyendo la metodología que hemos desarrollado, con las características deseables para las PYMES. Se considera que los aspectos valorados se pueden cumplir de forma total, parcialmente o no haber sido abordados en el modelo. A continuación, se describe cada uno de los aspectos analizados:

- Ciclo de SGSI: El modelo describe de forma clara las fases de desarrollo, implantación y mantenimiento del SGSI. Normalmente los modelos utilizan el ciclo PDCA.
- Marco de trabajo: El modelo describe de forma clara todos los elementos que forman el SGSI una vez que ha sido implantado.
- Niveles de madurez: El modelo está orientado a la implantación de una seguridad progresiva basada en niveles.
- Cultura de seguridad: El modelo ha tenido en cuenta la orientación hacia la cultura de la seguridad y no sólo la orientación técnica y de gestión de los modelos clásicos.
- Guía de buenas prácticas: El modelo incluye o contempla la integración de un guía de buenas prácticas o controles de seguridad dentro del SGSI.
- Análisis y gestión del riesgo: El modelo incluye mecanismos de valoración y gestión de los riesgos a los que están sometidos los activos del sistema de información.
- Métricas: El modelo incluye mecanismos de medición del cumplimiento de los controles de seguridad.
- Orientado a PYMES: El modelo ha sido desarrollado pensando en la casuística especial de las PYMES.
- Reutiliza el conocimiento: El modelo adquiere conocimiento de las implantaciones, de forma que este conocimiento pueda ser reutilizado para facilitar posteriores implantaciones.
- Dispone de herramienta software: El modelo dispone de una herramienta que lo soporte.
- Casos prácticos: El modelo ha sido desarrollado y refinado a partir de casos prácticos.

4 La Metodología MGSM-PYME.

En esta sección se ofrece una visión global del conjunto de subprocesos y actividades que componen la metodología MGSM–PYME [33] y los estándares y propuestas utilizados para su creación.

La metodología MGSM–PYME incluye todos los aspectos que se han considerado deseables para las PYMES, incluyendo la automatización de modelos de gestión de seguridad para reducir los costes de generación del sistema y un desarrollo totalmente orientado hacia las PYMES, evitando la generalización de los otros modelos.

Por otro lado, frente a metodologías como la IS2ME que se han centrado sólo en la generación de un SGSI a partir de una información básica, pero dejando de lado aspectos como el análisis de riesgos o la construcción propiamente dicha del SGSI, la metodología MGSM–PYME sí se ocupa de todos esos aspectos, utilizando el conocimiento adquirido para desarrollar SGSIs mucho más completos sin que ello suponga un coste mayor, gracias a la utilización de esquemas predefinidos que almacenan las características y el conocimiento de grupos de compañías.

Otra de las ventajas que aporta MGSM–PYME frente a los modelos analizados es que utiliza el conocimiento adquirido durante diferentes implantaciones para reducir

los costes de generación del SGSI en compañías de similares características, utilizando para ello el concepto de "esquemas". Esto es de especial relevancia, ya que permite entender las relaciones entre la información de la empresa con el objetivo de poder gestionar su seguridad [33].

4.1 Subproceso P1: GEGS – Generación de esquemas.

El principal objetivo de este subproceso es permitir la generación de un esquema (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.

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.

Actualmente el repositorio de esquemas se compone de un solo esquema 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. Este subproceso está formado por cuatro actividades:

- 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.
- 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.
- Actividad A1.3 - Generación de tablas del análisis de riesgos: 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. Aunque el análisis de riesgos es una de las partes fundamentales en la norma ISO/IEC27001 [15] y se encuentra descrita en detalle en el estándar ISO/IEC27005 [34], el principal objetivo del análisis de riesgos incluido en la metodología desarrollada es que sea lo menos costoso posible, aunque obteniendo un resultado con la suficiente calidad.

- 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.

4.2 Subproceso P2: GSGS – Generación del SGSI.

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

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

El generador de SGSIs se puede considerar una importante aportación de la metodología desarrollada, ya que permite generar los elementos que componen el SGSI con un coste muy reducido. Este subproceso está formado por cuatro actividades:

- Actividad A2.1: Establecimiento del marco de trabajo del SGSI: El principal objetivo de esta actividad es crear un marco de trabajo inicial entre el consultor de seguridad (CoS) encargado de la generación del SGSI y el cliente (Cl).
- Actividad A2.2: Establecimiento del nivel de madurez: El principal objetivo de esta actividad es establecer el punto inicial en que se encuentra la compañía con respecto a la gestión de la seguridad (nivel de madurez actual) y el punto que sería deseable que la compañía alcanzara (nivel de madurez deseable). En [35] se demostraron las ventajas de realizar entrevistas mediante cuestionarios que tienen pre–establecida una serie de preguntas con un número limitado de categorías de respuesta.

- Actividad A2.3: Realización del análisis de riesgos: El principal objetivo de esta actividad es establecer una evaluación de los riesgos a los que se encuentran sometidos los principales activos del sistema de información de la compañía sobre la que se quiere implantar el SGSI, así como proponer un plan al responsable de seguridad (Cl/RS) para gestionar los riesgos de la forma más eficiente posible.
- Actividad A2.4: Generación del SGSI: El principal objetivo de esta actividad es generar los elementos que compondrán el SGSI para la compañía y obtener la aprobación del interlocutor (Int) designado por la compañía del resultado obtenido, o en caso contrario tomar las medidas pertinentes para subsanar las deficiencias (mediante la alteración del esquema seleccionado, la selección de otro esquema más adecuado, o corrigiendo las entradas del subproceso).

4.3 Subproceso P3: MSGS – Mantenimiento del SGSI.

El principal objetivo de este subproceso es permitir y dar soporte a la compañía para que pueda gestionar la seguridad del sistema de información, utilizando para ello los entregables generados en el subproceso GSGS y los elementos que componen el SGSI seleccionados durante la actividad A2.4.

Este subproceso ha sido desarrollado para que sea muy fácil y cómodo para los usuarios del sistema de información su cumplimiento, simplificando las tareas que lo componen. Este subproceso está formado por tres actividades:

- Actividad A3.1 - Obtener o renovar el certificado de CS: El principal objetivo de esta actividad es establecer una cultura de seguridad básica en los usuarios que tendrán que trabajar con el sistema de información de la compañía, sin la cual no podrán acceder al mismo. Durante el desarrollo de la metodología se han probado diversos métodos para establecer una cultura de la seguridad en la compañía. Finalmente, el procedimiento que se ha determinado implantar consiste en la realización de una serie de cuestionarios de seguridad asociados al reglamento del SGSI, con el objetivo de mantener y mejorar la cultura de la seguridad de la compañía sin que tenga un coste alto de mantenimiento.
- Actividad A3.2 - Ejecutar procedimientos del SGSI: Esta actividad tiene como principal objetivo permitir a los usuarios del sistema de información la ejecución de los procedimientos que contienen los procesos necesarios para mantener el SGSI de la compañía. La ejecución de uno de los procedimientos pertenecientes al SGSI producirá una instancia del procedimiento, que será el conjunto de datos únicos introducidos durante la ejecución de ese procedimiento.
- Actividad A3.3 - Seguimiento del cumplimiento del SGSI: Esta actividad tiene como principal objetivo mantener actualizado el nivel de madurez del SGSI y conocer en todo momento el nivel de cumplimiento de los controles de seguridad que forman parte del SGSI de la compañía.

5 Relación entre las actividades de MGSM-PYME y otros estándares

En esta sub-sección podemos ver como cada una de las propuestas analizadas en el apartado 2, han servido de base para desarrollar las diferentes actividades que componen la metodología MGSM-PYME.

En la Tabla 2 se puede ver cómo se asocian las diferentes actividades de los subprocesos de la metodología MGSM–PYME con las diferentes metodologías analizadas y que han sido utilizadas como base para la propuesta. La asociación no es total, ya que en muchos casos las actividades planteadas en MGSM–PYME presentan un mayor potencial que la guía o metodología con la que se encuentra asociada. El objetivo de esta tabla es ofrecer una guía para conocer qué estándares, modelos y metodologías han servido de base para el desarrollo de cada actividad.

	Actividades de MGSM-PYME										
Propuestas SGSIs	**A1.1**	**A1.2**	**A1.3**	**A1.4**	**A2.1**	**A2.2**	**A2.3**	**A2.4**	**A3.1**	**A3.2**	**A3.3**
ISO/IEC27000		X	X	X		X	X	X		X	X
ISO/IEC15408		X				X					
ISO/IEC21827		X		X		X					
ISO/IEC20000				X							
ITIL				X							
COBIT			X	X			X				
ISM3		X	X	X		X	X				
Propuesta de Eloff		X				X					
Propuesta Areiza		X				X					
Prop. Dojkovski									X	X	
IS2ME					X	X		X			
ASD		X				X					
Prop. Carey-Smith								X			
Prop. Tawileh								X			
Prop. Sneza									X	X	

Tabla 2. Asociación de metodologías con las actividades de MGSM–PYME.

6 Conclusiones y futuros trabajos.

En este artículo se ha realizado una revisión de las diferentes guías y metodologías de gestión de la seguridad y madurez de los sistemas de información, y de los procesos asociados a la implantación de los sistemas de gestión de la seguridad clásicos.

Como resultado de esta revisión se ha podido establecer la importancia que tiene la gestión de los sistemas de seguridad en el desempeño y evolución sostenible de las empresas, ya que constituye un requisito básico para alcanzar la misión y los objetivos organizacionales en un entorno altamente competitivo.

En relación con los estándares más destacados se ha podido constatar que la mayor parte de los modelos de gestión de la seguridad han tomado como base el estándar internacional ISO/IEC17799 e ISO/IEC27002, y que los modelos de gestión de seguridad que están teniendo mayor éxito en las grandes compañías son ISO/IEC27001, COBIT e ISM3, pero que son muy difíciles de implementar y requieren una inversión demasiado alta que la mayoría de las PYMES no pueden asumir [14]. Aunque están surgiendo nuevas propuestas muy interesantes orientadas a este tipo de compañías, afrontan los problemas de una forma muy incompleta.

En numerosas fuentes bibliográficas se detecta y resalta la dificultad que supone para las PYMES la utilización de las metodologías y modelos de madurez para la gestión de la seguridad tradicionales, que han sido concebidos para grandes empresas [28-31]. Se justifica en repetidas ocasiones que la aplicación de este tipo de metodologías y modelos de madurez 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 [32].

El problema principal de todos los modelos de gestión de la seguridad y su madurez presentados es que no están teniendo éxito a la hora de implantarse en PYMES, debido principalmente a que:

- Unos fueron desarrollados pensando en organizaciones grandes (ISO/IEC27001, ISO/IEC21827, Common Criteria, ISO/IEC20000, ITIL, COBIT) y en las estructuras organizativas asociadas a éstas.

- Otros (ISM3, propuesta de Areiza, propuesta de Eloff, ASD, IS2ME, propuesta de Carey-Smith, propuesta de Tawileh) han intentando centrarse en los problemas de las PYMES, pero son modelos incompletos que sólo afrontan parte del problema, o intentan aportar unas guías básicas de los pasos a realizar, pero sin entrar en cómo gestionar realmente el SGSI. Además, la mayoría son modelos teóricos y están todavía en desarrollo.

Todos estos estándares y propuestas para la gestión de la seguridad, son muy importantes, y sus aportaciones han sido tenidas en cuenta para el desarrollo de la metodología planteada.

Fruto de esta investigación, se han podido obtener el conjunto de características que sería deseable que tuviera un SGSI orientado a PYMES y como se puede abordar cada una de estas características utilizando diferentes componentes de los estándares e investigaciones más relevantes existentes en la actualidad.

Agradecimientos

Esta investigación es parte de los proyectos: MEDUSAS (IDI-20090557), financiado por el Centro para el Desarrollo Tecnológico Industrial, BUSINESS (PET2008-0136) concedido por el Ministerio de Ciencia e Innovación de España y SEGMENT (HITO-09-138) y SISTEMAS (PII2I09-0150-3135) financiados por la Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha.

Referencias

1. Kluge, D. Formal Information Security Standards in German Medium Enterprises. in CONISAR: The Conference on Information Systems Applied Research. 2008.
2. Dhillon, G. and J. Backhouse, Information System Security Management in the New Millennium. Communications of the ACM, 2000. 43(7): p. 125-128.
3. Barlette, Y. and V. Vladislav. Exploring the Suitability of IS Security Management Standards for SMEs. in Hawaii International Conference on System Sciences, Proceedings of the 41st Annual. 2008. Waikoloa, HI, USA.
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. 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.
6. Dojkovski, S., S. Lichtenstein, and M.J. Warren. Challenges in Fostering an Information Security Culture in Australian Small and Medium Sized Enterprises. in 5th European Conference on Information Warfare and Security. 2006. Helsinki, Finland: 1-2 June.
7. Coles-Kemp, E. and R.E. Overill. The Design of Information Security Management Systems for Small-to-Medium Size Enterprises. in ECIW - The 6th European Conference on Information Warfare and Security. 2007. Shrivenham, UK: Defence College of Management and Technology.
8. 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).
9. 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.
10. 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.
11. Sánchez, L.E., et al. Developing a maturity model for information system security management within small and medium size enterprises. in 8th International Conference on Enterprise Information Systems (WOSIS'06). 2006. Paphos (Chipre). March.
12. 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.
13. 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.

14. Velásquez, N. and M. Estayno. Desarrollo y Mantenimiento Seguro de Software para Pyme: MoProSoft alienado a ISO/IEC 17799:2005. in IV Congreso Iberoamericano de Seguridad Informática (CIBSI'07). 2007. Mar de Plata. Argentina.: Noviembre.
15. ISO/IEC27001, ISO/IEC 27001, Information Technology - Security Techniques Information security management systemys - Requirements. 2005.
16. ISO/IEC20000, ISO/IEC20000, Service Management IT. 2005.
17. ITILv3.0, ITIL, Information Technology Infrastructure Library., C.C.a.T.A. (CCTA). Editor. 2007.
18. COBITv4.0, Cobit Guidelines, Information Security Audit and Control Association. 2006.
19. ISM3, Information security management matury model (ISM3 v.2.0). 2007, ISM3 Consortium.
20. 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.
21. ISO/IEC17799, ISO/IEC 17799, Information Technology - Security Techniques - Code of practice for information security management. 2005.
22. Areiza, K.A., et al., Hacia un modelo de madurez para la seguridad de la información. 3er Congreso Iberoamericano de seguridad Informática, 2005a. Nov, (2005): p. 429 - 442.
23. Sneza, D., L. Sharman, and W. Matthew John. Fostering information security culture in small and medium size enterprises: An interpretive study in australia. in the Fifteenth European Conference on Information Systems. 2007. University of St. Gallen, St. Gallen.
24. Linares, S. and I. Paredes (2007) IS2ME: Information Security to the Medium Enterprise. Volume,
25. Wiander, T. and J. Holappa, Managing Information Security in Small and Medium-sized Organization, in Handbook of Research on Information Security and Assurancence. 2007.
26. Carey-Smith, M.T., K.J. Nelson, and L.J. May. Improving Information Security Management in Nonprofit Organisations with Action Research. in Proceedings of The 5th Australian Information Security Management Conference. 2007. Perth, Western Australia: School of Computer and Information Science. Edith Cowan University.
27. Tawileh, A., J. Hilton, and S. McIntosh, Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach, in ISSE/SECURE 2007 Securing Electronic Business Processes, Vieweg, Editor. 2007. p. 331-339.
28. 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.
29. Hareton, L. and Y. Terence, A Process Framework for Small Projects. Software Process Improvement and Practice, 2001. 6: p. 67-83.
30. Tuffley, A., B. Grove, and M. G, SPICE For Small Organisations. Software Process Improvement and Practice, 2004. 9: p. 23-31.
31. Calvo-Manzano, J.A., Método de Mejora del Proceso de desarrollo de sistemas de información en la pequeña y mediana empresa (Tesis Doctoral). Universidad de Vigo. 2000.
32. Mekelburg, D., Sustaining Best Practices: How Real-World Software Organizations Improve Quality Processes. Software Quality Professional, 2005. 7(3): p. 4-13.
33. Sánchez, L.E., et al., MGSM-PYME: Metodología para la gestión de la seguridad y su madurez en las PYMES., in V Congreso Iberoamericano de Seguridad Informática. 2009: Montevideo, Uruguay.
34. ISO/IEC27005, ISO/IEC 27005, Information Technology - Security Techniques - Information Security Risk Management Standard (under development). 2008.
35. Fontana, A. and J. Frey, The Interview, in The SAGE Handbook of Qualitative Research. 3rd edition, N.L. Denzin, Y, Editor. 2005: Thousand Oaks, SAGE Publication. p. 695-727.