MEMORIAS

VIII CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMÁTICA

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

CIBSI ECUADOR 2015

10-12 NOV 2015

UNIVERSIDAD DE LAS FUERZAS ARMADAS DEL ECUADOR - ESPE

Sangolquí, ECUADOR

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Con la Organización de

ESPE-Innovativa EMPRESA PÚBLICA

CRIPTORED

fundación IN-NOVA Centro de Innovación

Memorias del VIII Congreso Iberoamericano de Seguridad Informática

CIBSI 2015

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

Compiladores

Luis Enrique Sánchez Crespo

Walter Marcelo Fuertes Díaz

Jorge Ramió Aguirre

ISBN: 978-9978-301-61-6

Universidad De Las Fuerzas Armadas Del Ecuador -ESPE

Quito, Ecuador

Patrocinadores

SEDE

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

ORGANIZACIÓN

ESPE-Innovativa
EMPRESA PÚBLICA

CRIPTORED

Fundación IN-N-VA
Centro de Innovación

PATROCINADORES Y EXPOSITORES

POLITÉCNICA
"Ingeniamos el futuro"
CAMPUS DE EXCELENCIA INTERNACIONAL

Ministerio de Telecomunicaciones y de la Sociedad de la Información

YACHAY
CIUDAD DEL CONOCIMIENTO

BLUEHAT consultores
EXPERTOS EN CIBERSEGURIDAD...

SNR Sicaman
Nuevas Tecnologías

GSyA
Grupo de Investigación en Seguridad y Auditoría

RACKLY
Grupo de Investigación de Sistemas Distribuidos. Ciberseeuridad v Contenido

COMITÉ DEL PROGRAMA

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

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

ORGANIZACIÓN

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

COMITÉ ORGANIZADOR LOGÍSTICO

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

COMITÉ DIFUSIÓN

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

COMITÉ TÉCNICO

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

EDITORES

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

CHAIR SESIONES

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

INDICE

PRESENTACIÓN

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

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

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

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

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

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

Luis Enrique Sánchez Crespo

Walter Marcelo Fuertes Díaz

Jorge Ramió Aguirre

Importancia de la Cultura de la Seguridad en las PYMES para la correcta Gestión de la Seguridad de sus Activos

A. Santos-Olmo, L. E. Sánchez, I. Caballero, D. Mellado, E. Fernandez-Medina

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

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

***Keyword* —Cybersecurity, Information Security Management Systems, ISMS, Safety Culture, SMEs, ISO27001, ISO27002.**

***Palabras clave* — Ciberseguridad, Sistemas de Gestión de Seguridad de la Información, SGSI, Cultura de la Seguridad, PYMES, ISO27001, ISO27002.**

I. Introducción

Un sistema de gestión de la seguridad de la información (SGSI) se puede definir como un sistema de gestión usado para establecer y mantener un entorno seguro de la información. El objetivo principal de los SGSIs es afrontar la puesta en práctica y el mantenimiento de los procesos y los procedimientos necesarios para gestionar la seguridad de las tecnologías de la información [1-5]. Dhillon [6] afirma que los SGSIs no se ocupan sólo de la seguridad de la información, sino que incluyen también la gestión de los aspectos formales e informales dentro de la misma [7]. Estas acciones incluyen la identificación de las necesidades de seguridad de la información y la puesta en práctica de las estrategias para satisfacer estas necesidades, medir los resultados y mejorar las estrategias de protección [8, 9].

Para ayudar a las empresas en la creación de una cultura de seguridad de la información los expertos han identificado diversos enfoques basados en políticas, sensibilización, formación y educación [10-13]. Sin embargo, las iniciativas de gestión por sí solas no influirán significativamente en el comportamiento de los empleados [14]. Según Schultz [15] es necesario prestar especial atención al factor humano.

Por otro lado, a la hora de implantar los SGSIs la mayor parte de los modelos se han centrado en aspectos técnicos y de gestión, dejando de lado un tercer aspecto que es el institucional, y que ha tomado una especial relevancia en los últimos años [1, 8, 16]. Así Von Solms [17] describe que la seguridad de la información no debe centrarse sólo en estas dos orientaciones (técnica y de gestión), sino que tiene que verse completada con una tercera orientación (institucional o de cultura de la seguridad). De esta forma, la función principal de cada una sería:

- *Orientación técnica:* Se ocupa de las direcciones técnicas de seguridad de la información mediante el uso de los sistemas informáticos, como autenticación y servicios de control de acceso.
- *Orientación a la gestión:* Comenzó cuando la alta dirección se involucró en la seguridad de la información con la evolución de Internet y las actividades de negocio electrónico, e incluye las tareas de preparación de seguridad de la información, políticas, procedimientos y métodos, así como la designación del responsable de seguridad.
- *Tendencia institucional:* De forma paralela a la primera y la segunda orientación, incluye la creación de una cultura corporativa de la seguridad, abarcando la normalización, certificación, medición y preocupación del aspecto humano en la seguridad de la información.

El objetivo de la institucionalización es construir una cultura de seguridad de la información, de tal manera que la ésta se convierta en un aspecto natural de las actividades cotidianas de todos los empleados de la organización [17, 18]. El desarrollo de la cultura de seguridad de la información pretende controlar el uso indebido de información por parte 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

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

D. Mellado, Agencia Tributaria, Spain, damefe@esdebian.org

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

los usuarios del sistema de información [19, 20]. En una cultura de la seguridad de la información el comportamiento del empleado contribuye a la protección de los datos, información y conocimientos [20], y la seguridad de la información se convierte en una parte natural de la actividad diaria del empleado [11]. El valor potencial de la adopción de una cultura de la gestión de la seguridad de la información también fue demostrado por Galletta y Polak [21], mostrando que entre el 20–50% de los empleados revelan información de la compañía o hacen un uso inadecuado del sistema de información [22-24]. Según Ernt&Young [25], en los últimos años se ha realizado un avance importante en el establecimiento de la cultura de la seguridad, pero todavía queda mucho trabajo por realizar.

Muchos gobiernos han realizado grandes esfuerzos para intentar mejorar el nivel de seguridad de sus compañías. Así, el grupo de políticas de seguridad de la información (DTI) [26] del Reino Unido tiene como fin ayudar a las empresas a gestionar eficazmente su seguridad de la información y proporcionar un conjunto de documentos que sirvan de punto de partida. "Las guías de la OCDE para la seguridad de los sistemas de información y las comunicaciones" [27] describen la necesidad de una mayor conciencia y comprensión de las cuestiones de seguridad y la necesidad de desarrollar una "cultura de seguridad".

El artículo continúa en la Sección 2, describiendo brevemente las metodologías y modelos para la gestión de la seguridad existentes que se han centrado en la importancia de la cultura de la seguridad para los SGSIs. En la Sección 3 se introduce brevemente nuestra propuesta de metodología para la gestión de la seguridad orientada hacia las PYMES denominada MARISMA. En la Sección 4 se analiza cómo se ha introducido el concepto de cultura de la seguridad en nuestra metodología. En la Sección 5, mostramos de forma práctica la aplicación del concepto de cultura de la seguridad. Finalmente, en la Sección 6 concluimos indicando cuál será el trabajo que desarrollaremos en el futuro.

II. Estado del Arte

La mayoría de las investigaciones sobre la cultura de la seguridad de la información [28-34] destacan que una cultura corporativa que incluya una cultura de seguridad de la información es un fenómeno colectivo transcendente y que puede ser diseñado por la propia dirección de una organización. Nosworthy [28] hace hincapié en que la cultura organizacional desempeña un papel importante en la seguridad de la información, ya que permite que la organización pueda resistir los cambios que sufre su sistema. Aunque la mayoría de las investigaciones coinciden en la importancia de la cultura de la seguridad para los SGSI [28], no se ha llegado a una definición clara del concepto de "cultura de la seguridad" [34], existiendo diferentes visiones:

- Siponen [35] describe que "la conciencia de seguridad de la información" es un estado donde los usuarios en una organización son conscientes de su misión en seguridad, dividiéndola en dos categorías: i) marco de aplicación (la normalización, certificación y medición de las actividades de la institucionalización); y ii) el contenido (el aspecto humano).
- Por otro lado Von Solms y Vroom [36, 37] sugieren el establecimiento de una cultura de formación y cooperación con los empleados, basada en una progresiva adaptación de la gestión de seguridad de la organización y los valores individuales y de comportamiento de los usuarios.
- Dhillon [6] tiene una visión amplia del término "cultura de seguridad", definiéndola como el comportamiento de los usuarios de una organización que contribuye a la protección de datos, información y conocimientos.
- Eloff [29] define la cultura de la seguridad de la información como un conjunto de características de seguridad de la información, tales como la integridad y la disponibilidad de la información.
- Para Chia [38] la cultura de la seguridad de la información es un aspecto fundamental, y define un conjunto de dimensiones que son importantes para medir la eficacia de la cultura de la seguridad de la información: i) la creencia en la importancia de la seguridad de la información; ii) equilibrio de largo y corto plazo, metas, políticas, procedimientos y procesos de mejora continua; iii) cooperación y colaboración; iv) atención a los objetivos de auditoría y cumplimiento. Sin embargo, esta lista ha sido recientemente criticada por Helokunnas [39], que hacen especial hincapié en los aspectos humanos de la seguridad de la información.
- Straub [40] sostiene que en los sistemas de información casi siempre se asume que una persona pertenece a una sola cultura, y por tanto proponen la teoría de identidad social para ser usada como base para la investigación de la cultura del sistema de información. La cultura de la identidad social sugiere que cada individuo está influido por multitud de culturas. Según [40], al aplicar la cultura de la seguridad los usuarios se verán influidos por aspectos éticos, de la legislación de cada país, y de organización de la seguridad. Esta cultura tiene un efecto sobre la forma en que el individuo interpreta el significado y la importancia de la seguridad de la información.
- Kuusisto [41] propone un sistema en que la cultura de la seguridad se crea a partir de la interacción del marco de referencia y los componentes (Figura 1).

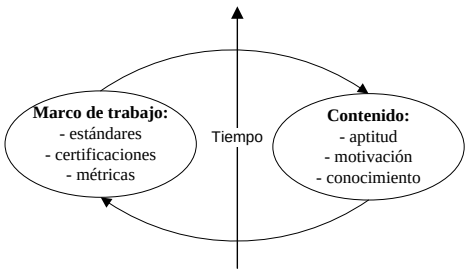

Figura 1. Marco de establecimiento de la cultura de seguridad.

- Por último, Detert [42] considera la cultura de la seguridad como un aspecto clave dentro de los SGSI y desarrolla un marco general para la seguridad de la información basado en ocho dimensiones. [34] aplicó esas ocho dimensiones a las zonas de seguridad de la información e identificó los principales factores de seguridad de la información de cada dimensión (Figura 2).

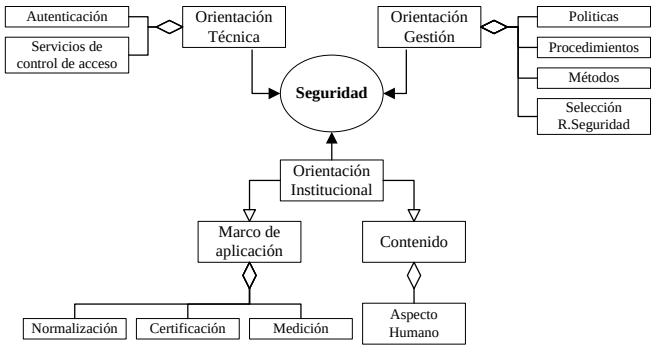

Figura 2. Orientaciones de seguridad [34].

Aunque estudios recientes demuestran la preocupación de las PYMES en relación con las dificultades de desarrollar una cultura de seguridad de la información [43], lo cierto es que la cultura de la seguridad tiene una serie de problemas adicionales a la hora de implantarse en las PYMES [44]. Según [45, 46], las PYMES se ven especialmente perjudicadas en comparación con las grandes organizaciones en la búsqueda de una cultura de seguridad de la información, por varios motivos:

- Las PYMES carecen de los fondos, tiempo y conocimientos necesarios para coordinar la seguridad de la información, o de forma eficaz imponer una cultura de seguridad de la información [10, 47].
- Las PYMES no suelen disponer de políticas y procedimientos, ni han definido las responsabilidades de los usuarios del sistema de información [48].
- Las PYMES son más susceptibles que las grandes compañías a influencias nacionales, como cambios en la legislación [49].

Como conclusión, podemos destacar que se han desarrollado diversos marcos de gestión de la seguridad orientados al desarrollo de una cultura de seguridad de la información [11, 17, 29, 31, 37, 39, 50-52], pero suelen estar orientados hacia las grandes organizaciones. En cambio, según Hutchinson y Dojkovski [45, 53] los marcos para las PYMES deberían estar basados en un estudio de las necesidades reales de éstas, identificando y desarrollando un marco específico para ellas.

Los expertos han propuesto diferentes marcos conceptuales para que la gestión de la seguridad de la información incluya la cultura de la seguridad de la información sobre la base de iniciativas de gestión de políticas, sensibilización, capacitación y educación [54, 55]. Sin embargo, esos marcos pueden ser más adecuados para medianas y grandes organizaciones debido a los recursos necesarios. En los últimos años han aparecidos varios marcos de trabajo para el establecimiento de la cultura de la seguridad sobre la base de: cultura organizacional y medición de la cultura de seguridad de la información [11, 30]; valores compartidos [48]: fases de seguridad de la información, niveles de madurez [17]; medidas relacionadas con el desarrollo del individuo, grupo y organización que permitan conocer sus deficiencias en materia de seguridad [29]; nivel socio–tecnológico sobre la seguridad de la información [56]; medidas basadas en la moral y ética de los usuarios [35]; métodos informales de concienciación [37]; conceptos clave de la cultura organizativa [31]; capacidades del personal [51]; aprendizaje organizativo [52]; y un enfoque multifacético [38]. Si bien esos marcos son claramente valiosos se centran en fragmentos del campo teórico, sin integrarse en un marco común y completo. Además, no abordan los requerimientos especiales de las PYMES.

Así, Kuusisto y Ilvonen [41] llegan a la conclusión de que no existe ninguna normativa adecuada para gestionar la seguridad en las PYMES, y que principalmente se necesita de modelos que sean válidos y que permitan aumentar la cultura de la seguridad en las PYMES.

En los siguientes subapartados se muestran dos propuestas que se centraron en el análisis de la necesidad de la cultura de la seguridad en las PYMES.

A. Propuesta de Dojkovski [45].

Dojkovski [45] planteo la construcción de un SGSI orientado a las PYMES tomando como punto central la cultura de la seguridad. Para ello analizó el estado de las PYMES de Australia, llegando a la conclusión que en los últimos quince años los riesgos de seguridad de la información para las PYMES de Australia han aumentado como resultado de un mayor acceso a Internet, pero el nivel de seguridad de la información y la sensibilización en las PYMES no se ha mantenido a buen ritmo y sigue siendo bajo.

Esta propuesta no entra en los mecanismos de implantación del SGSI, ni en aspectos como controles, métricas y gestión de riesgos que debe contener, centrándose solo en los elementos que debería contener un SGSI orientado a la cultura de la seguridad.

Las principales causas de los problemas de gestión de la seguridad detectadas en las PYMES fueron:

- Las PYMES ven el sistema de información como un sistema de apoyo a los departamentos de producción de la empresa y no como algo vital para su negocio. Esto hace que sean reactivas ante los fallos de seguridad en lugar de proactivas.
- Para las PYMES, el coste es fundamental y ven la seguridad como un gasto no justificado.
- Los gerentes no se preocupan de la seguridad, y por tanto el resto de empleados tampoco.
- Los usuarios ven muy difícil cumplir este marco de trabajo. Asimismo, es muy difícil hacer que cambien

los malos hábitos adquiridos, y ningún usuario quiere ser responsable de los activos del sistema de seguridad de la información.

- Se deben gestionar las iniciativas de forma adecuada, presentando las políticas y procedimientos a los usuarios a la hora de firmar el contrato. En el caso de la PYME esto puede ser más difícil al carecer de estructuras organizativas formales. Asimismo, es importante considerar el cumplimiento de la seguridad dentro de la valoración del trabajo de los empleados.
- Falta de formación adecuada en seguridad. Los encuestados consideraron el e–learning como herramienta de trabajo válida para mejorar el nivel de cultura de la seguridad de la información, así como la posibilidad de poder compartir experiencias con otras PYMES. Pero el problema es que normalmente en las PYMES no se puede hacer un curso para los trabajadores por cuestiones de tiempo y dinero, y que muchos trabajadores no realizarían estos cursos si no existiera algún tipo de motivación al respecto.

Para afrontar estos problemas Dojkovski [45] planteó la construcción de un SGSI orientado al desarrollo de la cultura de la seguridad de los sistemas de la información, que tendría que tener en cuenta cómo las personas piensan y se comportan, lo que sugiere la necesidad de un enfoque de investigación interpretativo. Siguiendo los principios de Lichtenstein [57] se validó el modelo en cuatro grupos diferentes. Se utilizaron diferentes marcos de trabajo y enfoques para desarrollar una teoría válida. Se realizó un análisis sobre un conjunto de PYMES intentando determinar su conciencia en seguridad, los desafíos que enfrentan las PYMES en el fomento de una cultura de seguridad de la información, así como la viabilidad del anteproyecto.

Este marco de trabajo está formado por los siguientes elementos (Figura 3):

- Aprendizaje organizativo e individual: La cultura de seguridad de la información debe ser difundida a todos los niveles de la organización, tanto a nivel individual como colectivo [29]. Según Van Niekerk [52] podría ser útil utilizar un enfoque de aprendizaje organizativo.
- E–Learning (la cooperación, la colaboración y el intercambio de conocimientos): las PYMES pueden realizar aprendizaje electrónico (e–learning) [58] y también pueden cooperar y colaborar electrónicamente en las comunidades y foros de seguridad de los sistemas de la información [39] con el objetivo de mejorar la cultura de la seguridad entre los usuarios del sistema de información.
- Gestión: Los programas de sensibilización (respaldo de la dirección, amenazas de medidas disciplinarias, cláusulas en los contratos de trabajo, etc), la formación, la educación o el valor del liderazgo [59] son iniciativas valiosas para el desarrollo de la cultura de la seguridad de la información [12, 51]. En las PYMES es probable que se generen diferentes niveles en la sensibilización, la formación y las necesidades de educación para los empleados individuales.
- Cultura de la seguridad: Procedimientos para responder a nuevos sucesos (como violaciones de seguridad) ayudarán a subrayar la importancia de la seguridad de la información a los trabajadores [27]. Los incentivos también pueden ser útiles para modificar el comportamiento de los empleados. Sin embargo, Rosanas y Velilla [14] advierten que los controles de la gestión debe estar basados en valores éticos.
- Comportamiento: Gestión de iniciativas destinadas a desarrollar los rasgos deseables de comportamiento respecto a la responsabilidad, integridad, confianza y ética del personal [20]. Sin embargo, valores fuertes son necesarios para apoyar las iniciativas de gestión [14]. Cuando los valores fuertes son difundidos entre entidades colaboradoras, empleados y otras partes interesadas, la seguridad de la información se fortalece [39]. El desarrollo de la motivación intrínseca es importante [35] y puede ser apoyada por la promoción al personal que cumpla las normativas de seguridad de forma adecuada [42].
- Ética nacional y cultura organizacional: Según Helokunnas [39], la creación de foros de seguridad dentro del ámbito nacional puede favorecer la creación de una cultura de la seguridad de la información.

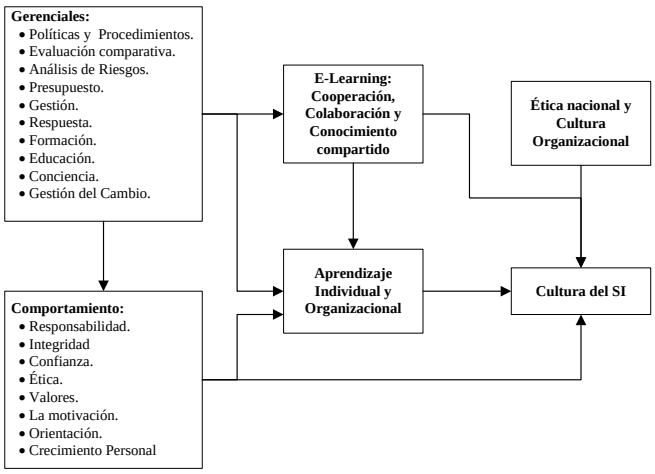

Figura 3. Marco para el desarrollo de la CS en la PYME [45].

Según las investigaciones realizadas por Dojkovski [45], los principales retos en el desarrollo de la cultura de seguridad de la información en las PYMES incluyen:

- Motivar a los propietarios para que asignen un presupuesto adecuado a la seguridad de la información.
- Convencer a los propietarios de realizar un análisis formal de los riesgos.
- Velar para que los propietarios desarrollen una política de seguridad de la información, desarrollen procedimientos y asignen responsabilidades.
- Desarrollar una postura proactiva hacia la seguridad

de la información.

- Identificar y establecer una serie de actividades de sensibilización para adaptarse a los entornos de las PYMES.

Las principales conclusiones obtenidas de la aplicación del marco de trabajo son que aunque tiene valor de forma individual para identificar qué elementos debería tener un SGSI orientado a las PYMES y a la cultura de la seguridad, no es un modelo completo y utilizable.

B. Propuesta de Sneza [60].

Plantea la construcción de un SGSI tomando como punto central el desarrollo de la cultura de seguridad de la información, y teniendo en cuenta cómo las personas piensan y se comportan. Por ello basaron su marco de trabajo en el establecimiento de la cultura de la seguridad en aspectos cualitativos en detrimento de los cuantitativos. Para definir su marco de trabajo, realizaron un estudio sobre PYMES Australianas de menos de 20 empleados [61].

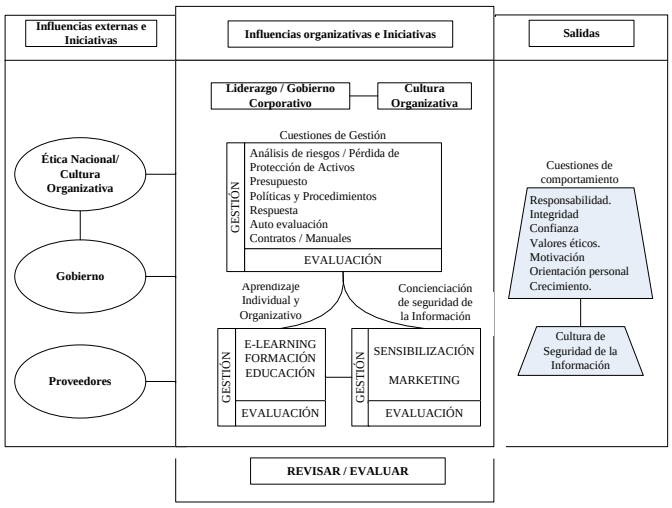

Figura 4. Marco para fomentar la CS en las PYMES [60]

En la Figura 4 se pueden ver los elementos que debería tener un SGSI basado en el fomento de la cultura de la seguridad de la información. En este marco se describen tres influencias externas:

- Ética nacional y cultura organizacional: las culturas nacionales pueden afectar a la organización de la seguridad de la información. La ética social también puede tener un impacto importante. Helokunnas [48] destaca la importancia de las redes sociales para compartir problemas de seguridad de la información y crear una conciencia sobre el tema.
- Las iniciativas del gobierno: Los gobiernos pueden jugar un papel fundamental para crear una cultura de seguridad de la información, aprobando legislaciones especiales y dando apoyos (cursos, subvenciones, etc).
- Proveedores: Los proveedores pueden proporcionar fiabilidad a las PYMES, como garantías adicionales de seguridad de los productos que les venden.

Este marco de trabajo está formado por los siguientes elementos:

- Liderazgo y gobierno corporativo: Los propietarios de las PYMES deben demostrar que apoyan la gestión de la seguridad de la información. Según Dutta [59], el apoyo de la dirección se valoró mucho en las grandes organizaciones, pero no en el caso de las PYMES.
- Cultura organizativa: La cultura de la organización y del entorno influye directamente en el cumplimiento de la gestión de la seguridad.
- Gestión: Las PYMES consideran los resultados del análisis de riesgos como clave para garantizar que las políticas y procedimientos son realmente necesarios. Además, las PYMES deben guiarse por el riesgo de pérdidas de activos, derivado del análisis de riesgos. Martins había identificado esta necesidad en las grandes organizaciones. En tercer lugar, se debe asignar un presupuesto para la gestión de la seguridad, que incluirá las iniciativas para establecer una cultura de gestión de seguridad en los recursos. Martins sugirió anteriormente que el presupuesto tiene una gran influencia en las organizaciones. En cuarto lugar, los procedimientos que responden a incidentes de seguridad de la información ayudarán a subrayar la importancia de la seguridad de la información a los empleados, lo que también ha sido sugerido por OCDE [27] en general. En quinto lugar, las PYMES se verán favorecidas por evaluar periódicamente la cultura de la seguridad de la información. En sexto lugar, el contrato de trabajo debe incluir sanciones o incentivos a los empleados para influir en su motivación. Todos los procesos de gestión deben ser evaluados de forma periódica.
- Aprendizaje individual y organizativo: El e–learning, la formación y la educación son iniciativas potencialmente valiosas para el desarrollo de la cultura de seguridad de la información para las PYMES, como también lo son para las grandes empresas [35, 51, 58]. El intercambio de conocimientos, la cooperación y la colaboración son importantes para el aprendizaje en los distintos niveles de la organización y con el fin de desarrollar la cultura de seguridad de la información. Los procesos de aprendizaje deben ser evaluados periódicamente.
- Concienciación de seguridad de la organización: [58] ha sugerido medidas de sensibilización formales e informales para las PYMES. [35] propone incluir medidas de sensibilización que además tengan aspectos de persuasión.
- Revisión y evaluación: Las PYMES deberían examinar y evaluar periódicamente las medidas adoptadas con el fin de mejorar continuamente [12].
- Comportamiento: Una serie de iniciativas externas e internas pueden desarrollar comportamientos de responsabilidad, integridad, confianza y ética. Según Dhillon [20], en las grandes organizaciones esta transformación parte de iniciativas de gestión interna,

mientras que en el marco propuesto [60] se reparte esta responsabilidad entre agentes internos y externos. Siponen [35] señala la importancia de la motivación intrínseca. Una medida eficaz para la organización es ofrecer beneficios a los usuarios que cumplan con el reglamento de seguridad del sistema de información [42].

Las principales conclusiones obtenidas de la aplicación de este marco de trabajo fueron:

- Los propietarios de las PYMES de Australia carecen de una adecuada comprensión de la importancia de la seguridad de la información para su negocio [23, 47, 48, 62].
- 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 [23].
    - Los propietarios de las PYMES de Australia no entienden el valor estratégico de las TI en su negocio. Otros estudios demuestran que esto no es un caso aislado, así un estudio de O'Halloran [63] determinó que las PYMES del Reino Unido no entienden cómo la seguridad les ofrece valores añadidos a sus negocios.
- Un requisito previo para el desarrollo de la cultura de seguridad de la información en las PYMES es el desarrollo y la comunicación de las políticas, procedimientos y responsabilidades. Como muchos expertos y estudios han señalado, la mayoría de las PYMES en los países desarrollados carecen de tales políticas [23, 47, 62].
- La cooperación, colaboración, intercambio de conocimientos y aprendizaje electrónico para los empleados de las PYMES de Australia eran actividades valiosas. Este hallazgo coincide con el estudio realizado por ISBS [23].

Si bien los expertos han señalado la importancia de los valores de los usuarios hacia la gestión de la seguridad en las organizaciones sin importar su tamaño [11, 29, 48, 64], el estudio realizado por Sneza [60] demostró que es muy complejo inculcar estos valores a los usuarios de las PYMES.

Algunas de las limitaciones que se desprendieron del estudio fueron: i) el análisis es interpretativo y las conclusiones están basadas en el estudio de un pequeño conjunto de PYMES australianas; ii) el marco carece de elementos aplicables sólo a las PYMES; iii) el marco de proceso carece de directrices detalladas para permitir su aplicación; iv) el estudio se centró en la investigación de PYMES de perfil técnico, cuyo personal ya tenía conocimientos técnicos; v) se desarrolló el marco centrándose sólo en el contexto Australiano, y por tanto puede no ser válido para otros países; vi) el marco no ofrece pro–actividad a la empresa y deja en ella la responsabilidad de ser dinámica.

III. Framework Marisma

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 [65, 66].

Uno de los objetivos perseguidos en la metodología MARISMA 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 [67]. 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 [68], apoyándose en otras normativas [69, 70].

Otra de las principales aportaciones que presenta la metodología que se ha desarrollado es un conjunto de matrices que permiten relacionar los diferentes componentes del SGSI (controles, activos, amenazas, vulnerabilidades, criterios de riesgo, procedimientos, registros, plantillas, instrucciones técnicas, reglamentos y métricas) y que el modelo utilizará, para generar de forma automática gran parte de la información necesaria, reduciendo de forma muy notable los tiempos necesarios para el desarrollo e implantación del SGSI [71]. Este conjunto de interrelaciones entre todos los componentes del SGSI, permite que el cambio de cualquiera de esos objetos altere el valor de medición del resto de objetos de los que se compone el modelo, de forma que se pueda tener en todo momento una valoración actualizada de cómo evoluciona el sistema de seguridad de la compañía.

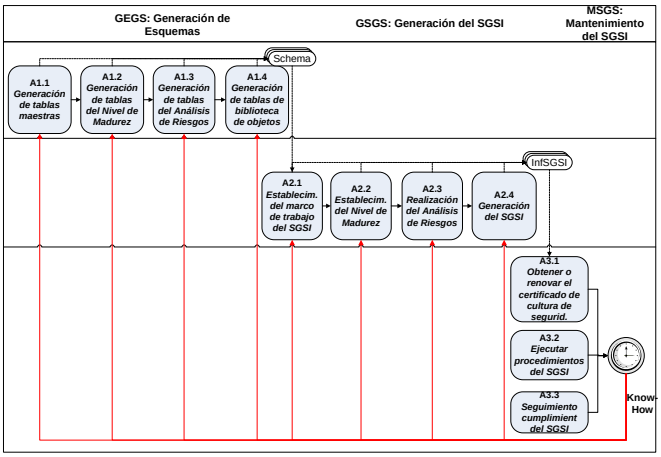

Figura 5. Subprocesos de la metodología.

De esta forma y a partir de la información obtenida mediante la implantación en diferentes empresas, se ha desarrollado una metodología de gestión y madurez de la seguridad de los sistemas de información y un modelo asociado a la misma (ver Figura 5).

Está metodología consta de tres subprocesos principales:

- GEGS – Generación de Esquemas de Gestión de Seguridad: El principal objetivo de este subproceso está orientado a la construcción de "esquemas", que son estructuras necesarias para la construcción de SGSIs, creadas para un conjunto de posibles compañías de la misma categoría. Estos esquemas son reutilizables y permiten reducir el tiempo de creación del SGSI, así como sus costes de mantenimiento hasta hacerlos adecuados para la dimensión de una PYME [65]. El uso de esquemas es de especial interés en el caso de las PYMES ya que por sus especiales características, éstas suelen tener sistemas de información sencillos y muy parecidos entre sí.
- GSGS – Generación de Sistemas de Gestión de Seguridad: El objetivo principal de este subproceso es la creación de un SGSI adecuado para una compañía, utilizando para ello un esquema existente.
- MSGS – Mantenimiento del Sistema de Gestión de Seguridad: El objetivo principal de este subproceso es el mantener y gestionar la seguridad del sistema de información de la compañía, aportando información actualizada en el tiempo de un SGSI generado.

Las principales actividades que se ocupan de ir creando una cultura de la seguridad progresiva, se centran en el proceso de mantenimiento del SGSI.

IV. GCCS-PYME: Gestión de los certificados de cultura de la seguridad

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, y sin la que no podrán acceder al mismo [72].

Durante el desarrollo de la investigación 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.

La idea principal es requerir un "certificado de nivel cultural" con respecto al sistema de la información a los usuarios del mismo, certificado que puede ser retirado y que debe ser renovado periódicamente para garantizar que se sigue manteniendo el nivel necesario de cultura de seguridad.

La actividad ha demostrado que, por su sencillez y el poco tiempo que requiere, va creando de forma progresiva una cultura de la seguridad en los usuarios. La automatización de la misma evita costes adicionales de mantenimiento y planificación, y hace que la cultura de seguridad se mantenga como algo inherente al propio sistema de información.

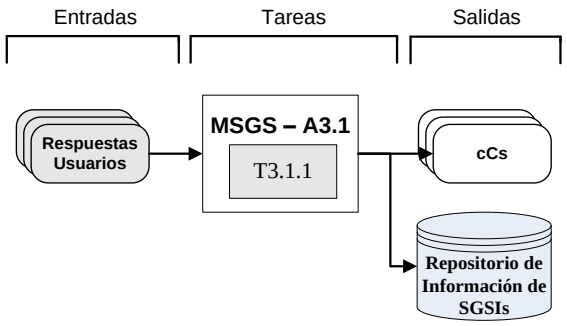

Figura 6. Esquema simplificado a nivel de tarea de la actividad A3.1.

En la Figura 6 se puede ver el esquema básico de entradas, tareas y salidas que componen esta actividad:

- Entradas: Como entradas se recibirán las respuestas de los usuarios al cuestionario de preguntas sobre el reglamento generado por el sistema.
- Tareas: El subproceso estará formado por una sola tarea que se ocupará de la emisión de los certificados de seguridad.
- Salidas: La salida producida por este subproceso consistirá en el certificado de cultura de seguridad en el caso de que la nota obtenida en el cuestionario sea superior a cinco o la denegación del certificado en caso contrario. Si se suspende el examen, se recomendará al usuario el estudio del manual de seguridad incluido en el SGSI o bien la asistencia a un curso de gestión de seguridad para aumentar los conocimientos en la materia.

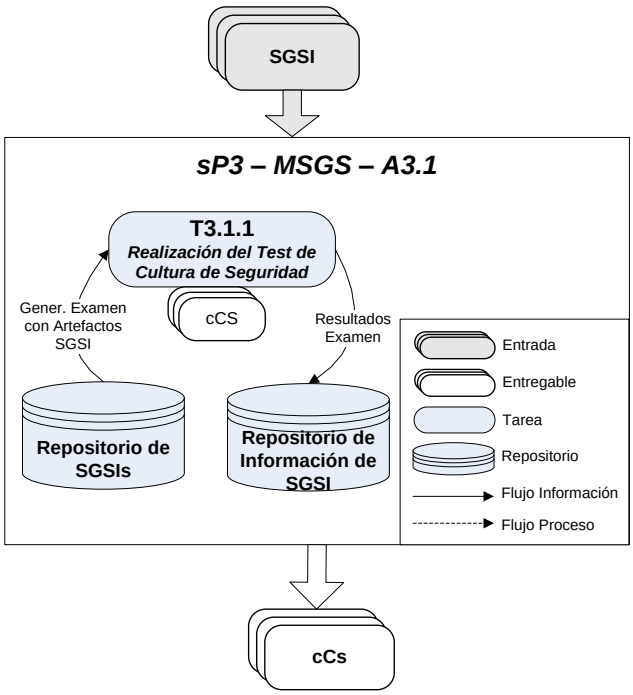

Figura 7. Esquema detallado a nivel de tarea de la actividad A3.1.

En la Figura 7 muestra la tarea de la actividad de forma mucho más detallada, viendo cómo interactúa ésta con el repositorio de información de SGSIs encargado de contener los certificados de seguridad concedidos y la nota obtenida.

El objetivo de la tarea T.3.1.1 es realizar una evaluación de los conocimiento que un usuario que desea acceder al sistema de información de la compañía tiene con respecto al reglamento que compone el SGSI, determinando si está preparado o no para acceder al mismo.

El limitar el acceso al sistema de información a los usuarios, hasta que consigan demostrar que tienen unos conocimientos básicos de cómo deben actuar con él es un control que ayuda a mitigar los riesgos a los que está sometido el sistema, obligando a los usuarios a incrementar su cultura de seguridad de forma progresiva y con un bajo coste.

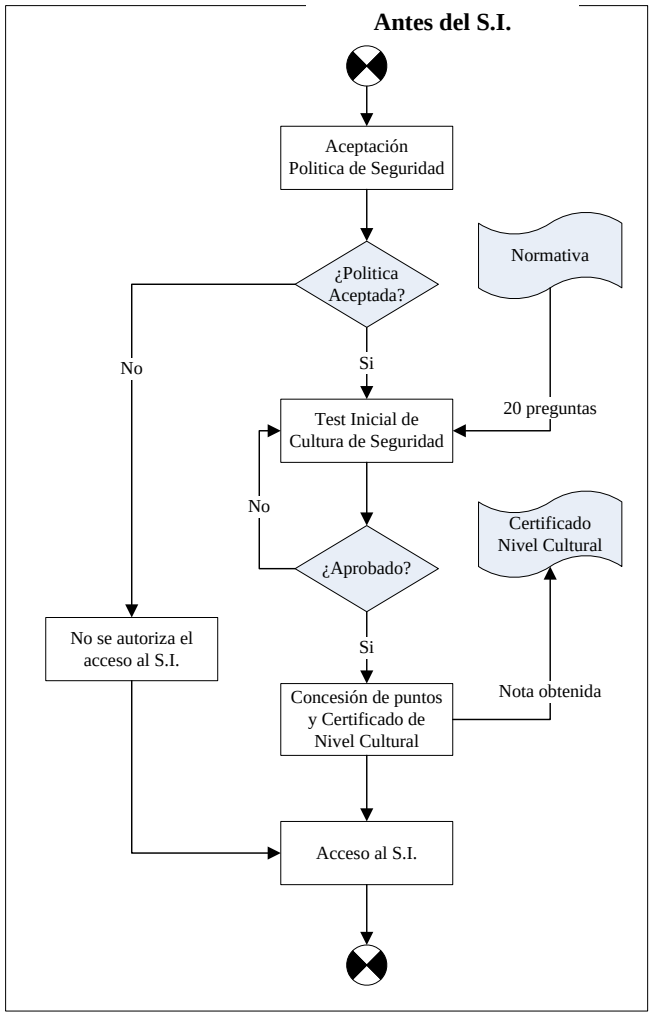

Figura 8. Obtención inicial de un certificado de "cultura de seguridad".

En el caso de que un usuario suspenda un examen, deberá volver a estudiar la información del SGSI o asistir a un curso de gestión de seguridad para adquirir el nivel de conocimiento adecuado para acceder al sistema.

Dentro de esta tarea existen dos procesos diferenciados: i) Obtención del certificado de cultura de la seguridad.; ii) Renovación del certificado de cultura de la seguridad.

En la Figura 8 se puede ver en detalle el diagrama de flujo de los diferentes pasos que conforman el primero de estos procesos (obtención del certificado de cultura de la seguridad). La primera vez que el usuario accede al sistema de información, deberá aceptar la política de seguridad de la empresa. De esta forma se garantiza que el usuario lea, aunque sea de forma rápida, la política de la empresa (mejorando la cultura de seguridad). Después, el usuario deberá pasar un test inicial compuesto por unas veinte preguntas extraídas al azar a partir del SGSI de la compañía.

Mientras el usuario no consiga obtener más del 50% de respuestas correctas en el test se considera que su "cultura de seguridad" para el sistema de información de la compañía no es adecuada y deberá realizar otro examen hasta conseguir una calificación superior o igual a cinco. El usuario no podrá acceder al sistema de información de la compañía hasta que no alcance un nivel adecuado de "cultura de seguridad". De esta forma se garantiza implantar la cultura de una forma eficiente.

Una vez que el usuario consiga el aprobado su nota se guardará en un registro, se le concederá un certificado de "cultura de seguridad" y se le dará acceso al sistema de información. La nota obtenida será importante para poder mantener el certificado obtenido en el tiempo, ya que ésta se verá modificada por otras tareas del sistema.

El segundo de los procesos que componen la tarea de "realización del test de cultura de seguridad" es la renovación del certificado de cultura de la seguridad (CS), ya sea por la caducidad del mismo o por la pérdida de puntos de la calificación. Los pasos de este proceso se pueden ver en detalle en el diagrama de flujo de la Figura 9.

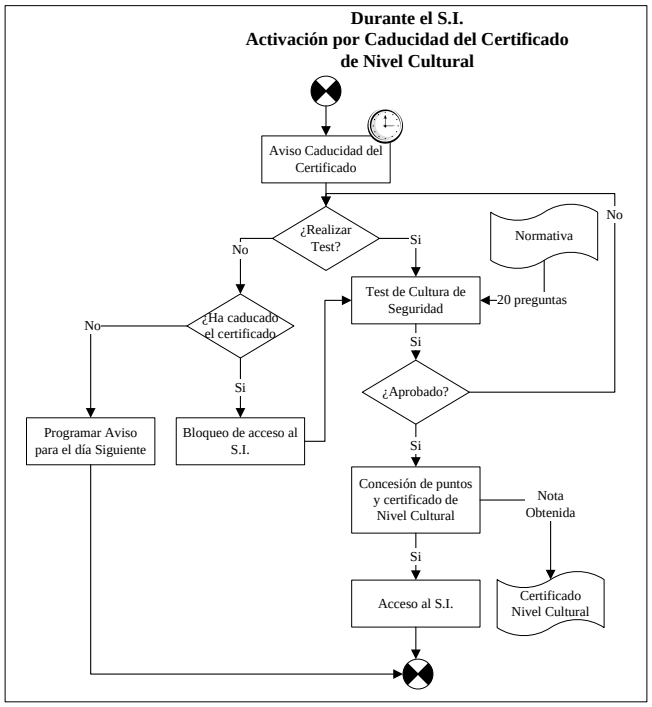

Figura 9. Esquema de renovación de un certificado de la CS.

Se ha establecido un periodo de renovación del certificado de cultura de la seguridad de 1 año, aunque esta cifra podría reducirse a 6 meses para acelerar el establecimiento de la cultura de la seguridad de la información. Debido a la sencillez del procedimiento no es aconsejable relajar más el tiempo de la renovación de los certificados, porque podría degradarse la cultura de seguridad (ej.: se considera que un tiempo de 2 años sería contraproducente), ni forzarlo demasiado porque podría producir rechazo entre los usuarios (Ej.: se considera que un tiempo inferior a 6 meses crearía rechazo entre los usuarios). En la Figura 10 se puede ver cómo, según los resultados de las investigaciones realizadas durante la elaboración de la investigación, si el periodo de renovación se mueve entre los 6 y los 18 meses el nivel de la cultura de la seguridad (NCS), medido como la calificación media obtenida en los exámenes al obtener el certificado de cultura de la seguridad, es más alto, lo que hace recomendable la renovación del certificado cada 12 meses.

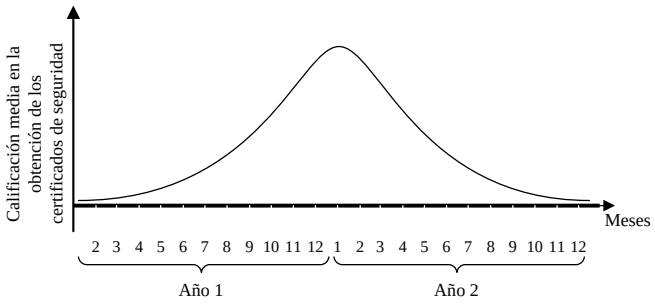

Figura 10. Asociación del NCS con el periodo de renovación de los certificados.

Para evitar interferir en el trabajo diario de los usuarios, la notificación de caducidad del certificado se produce desde 1 mes antes de ser efectiva, de forma que el usuario puede postergar la realización de los test al momento que desee dentro de ese periodo. El sistema diariamente le irá recordando el tiempo que resta para que caduque su certificado. Llegada la fecha de caducidad, si el usuario no ha realizado y aprobado el test se bloqueará su acceso al sistema de información hasta que consiga renovar el certificado.

Dado que el tiempo consumido por recurso (TcR) es uno de los factores principales de éxito para la metodología (en particular en el caso de las PYMES), se han realizado estimaciones del tiempo que podría costar la implantación de la cultura de seguridad, llegando a la conclusión de que la sencillez del proceso lo hace totalmente aceptable para las PYMES (se ha estimado que la obtención inicial del certificado podría llevar entre 1 y 2 horas, en torno a 90 minutos para la lectura de la política de seguridad y el entendimiento de los elementos del SGSI, y unos 30 minutos para la realización y aprobación de test). Esta inversión de tiempo se realizaría sólo inicialmente ya que, aunque el certificado se debe renovar de forma periódica, la política de seguridad sólo se debe leer y aprobar inicialmente. La experiencia obtenida a partir de los casos de prueba demuestra que los usuarios del sistema de información consideran esta inversión de tiempo razonable.

Por último, merece la pena destacar que los usuarios que intentaron saltarse la lectura de la política de seguridad para ahorrar tiempo tuvieron que repetir varias veces los test, invirtiendo finalmente el mismo tiempo que si hubieran leído la política. Cualquiera de los dos caminos se puede considerar correcto, ya que ambos conducen al objetivo de introducir en los usuarios la semilla inicial de la "cultura de seguridad".

Con esta sencilla tarea los usuarios nunca pierden conciencia de la importancia de mantener actualizado su nivel de cultura de la seguridad. Asimismo, dado que los test se realizan al azar mediante combinación de preguntas de los reglamentos de seguridad activados en la compañía, los usuarios van tomando conciencia cada vez mayor de estos reglamentos, de una forma intuitiva y con un coste mínimo.

Por otro lado, la puntuación de los certificados de cultura de seguridad cambia cuando se producen ciertas acciones: i) violaciones del reglamento de seguridad; y ii) pérdida del certificado de cultura de la seguridad por tener menos puntos de los requeridos.

A lo largo de la investigación se ha determinado que cuanto mayor es la cultura de seguridad de la compañía, mayor es el número de denuncias que llegan de parte de los usuarios, máxime cuando dichas denuncias no implican actualmente sanciones graves contra los denunciados.

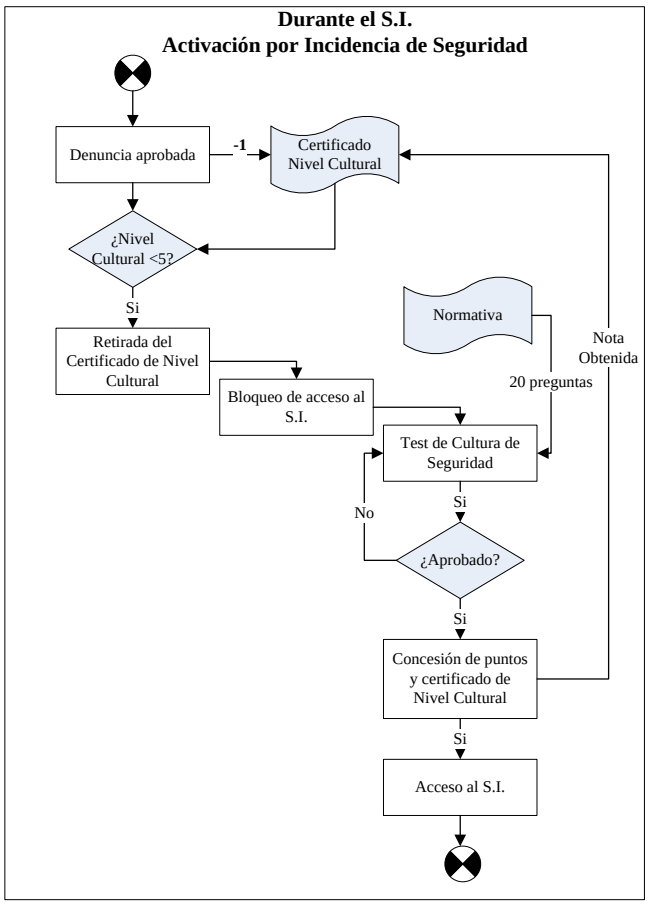

Figura 11. Alteración del NCS por una violación de la normativa.

Cuando se realiza una denuncia de un incidente de seguridad y el responsable de seguridad considera que está justificada y por lo tanto la aprueba, además de verse afectado el nivel de seguridad global de la compañía se ve afectada la puntuación del certificado de cultura de la seguridad del usuario que cometió la violación de seguridad. Cada violación implica la pérdida de un 1 punto del certificado de cultura de la seguridad (NCS) que el usuario tenía hasta el momento, y que era el resultado de la nota obtenida en el test de cultura de seguridad, menos los puntos que ya hubiera perdido durante el periodo de validez de ese certificado por violaciones de la normativa activa en la compañía. Si la pérdida de puntos debida a violaciones de seguridad hace que la puntuación del certificado de cultura de la seguridad baje de los 5 puntos, se le quitará al usuario el certificado, y con ello el acceso al sistema de información de la compañía, hasta que vuelva a aprobar el examen y así obtenga un nuevo certificado de seguridad. Todo este proceso se puede ver en la Figura 11.

Este proceso sirve como control preventivo para que los usuarios del sistema de información sean conscientes de que las violaciones de las normativas tienen un coste. Asimismo, la medida no es excesivamente grave y por tanto los usuarios no la ven con rechazo. Este control no tiene un coste de gestión representativo, ni en tiempo ni en recursos para la compañía, pero supone un importante refuerzo para establecer una correcta cultura de seguridad en la compañía.

En la Figura 12 se puede ver cómo se relacionan las puntuaciones del examen de cultura de la seguridad con la matriz de reglamentos–controles, de forma que cuando un certificado de seguridad se obtiene con una nota baja afecta a los controles asociados a las normativas de las que se han obtenido las cuestiones, ya que al fallar una pregunta del examen se reduce en un porcentaje el nivel de los controles asociados a dicha pregunta (–0.1%). De igual manera, si se acierta la pregunta aumenta el nivel de los controles (+0.1%).

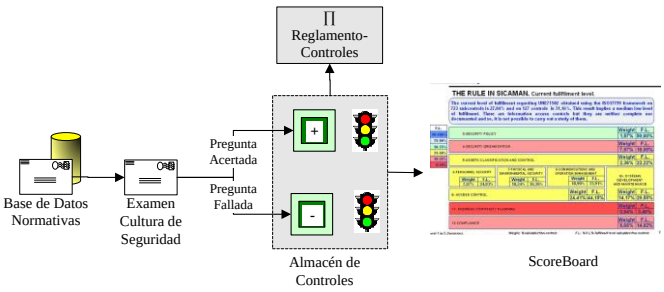

Figura 12. Gestionar los certificados de cultura de la seguridad.

Por lo tanto, podemos concluir en que esta actividad permite de una forma sencilla obtener un certificado de cultura de la seguridad a los usuarios, aumentando el conocimiento de los mismos con respecto al SGSI de una forma sencilla y valorando su nivel de conocimientos con respecto al SGSI, y a la vez este certificado de cultura de la seguridad se irá actualizando de forma dinámica, mediante la aplicación de las sanciones por violaciones de seguridad, que permiten actualizar de forma dinámica y sin coste este certificado de cultura de la seguridad.

V. Aplicación práctica de GCCS-PYME

A nivel de aplicación, el aspecto principal de la cultura de la seguridad será realizar pequeños cuestionarios con el objetivo de determinar si los usuarios del sistema de información de la compañía tienen un conocimiento que les permita cumplir y respetar las normas del mismo. El resultado será una calificación respecto a la cultura de la seguridad de los usuarios, obtenida mediante la realización de un test generado de forma automática por el sistema de cultura de seguridad (Figura 13) asociado al SGSI. Esta zona se corresponde con la actividad A3.1 del subproceso MSGS de la metodología.

	Nombre	Asociar
N/SI-01	Responsabilidades de los encargados de seguridad de la informacion	☐
N/SI-02	Responsabilidades de la dirección.	☐
N/SI-03	Uso correcto de la información.	☐
N/SI-04	Validez de la política cuando no esta activa.	☐

Figura 13. A3.1 – Pantalla de test de cultura de seguridad.

Cuando el certificado de cultura de seguridad es revocado por reiteradas violaciones de seguridad, o caduca, deberá ser renovado siguiendo las mismas premisas enunciadas en la sección anterior.

En la Tabla I se puede ver la simulación de un examen realizado por un usuario del sistema para obtener el acceso al mismo.

Tabla I. Examen de obtención del certificado de cultura de la seguridad

Realización de test para obtención del certificado de cultura de seguridad			
Usuario:	José Antonio Parra	**Fecha:**	12/08/2014

Parte 1ª: Responda V/F a la pregunta ¿El reglamento es de obligado cumplimiento para el SGSI de su compañía?

Código	Reglamento	Descripción	Respt. Usuario	Respt. Correct	Nota
N/AS–03	Control de acceso	Todos los accesos al perímetro de seguridad deben ser supervisados …	F	V	0
N/AS–06	Registro de accesos físicos	La organización debe guardar un “registro de visitas” …	V	V	1
N/SE–09	Registro de mantenimiento	Se debe mantener un registro de todos los fallos detectados …	V	F	0
N/CS–01	Copias de seguridad	Las copias de seguridad del sistema de información …	V	V	1
N/CS–03	Premisas para almacenar copias de seguridad	Las copias de seguridad se deben mantener en una localización …	V	V	1
N/ISI–08	Revisión independiente de la política de seguridad	La política de seguridad debe ser revisada periódicamente …	V	V	1

N/AT–01	Tipo de acceso	Cuando un tercero debe acceder a las instalaciones, …	F	V	0
N/OE–03	Cláusulas de los contratos de servicios	Todos los contratos de servicios asociados al sistema de información, debe …	V	F	0
N/ISFI–05	Tipos de incidentes de seguridad	Cualquier empleado o contratado ha de conocer …	V	V	1
N/ISFI–15	Incumplimiento de las políticas	La organización aplicara medidas disciplinarias …	V	V	1
N/CI–03	Inventario de activos	Se debe realizar una revisión anual del inventario …	V	V	1
N/CI–04	Clasificación de activos de información	Toda la información debe ser considerada confidencial …	V	V	1
N/DPT–07	Cláusula de seguridad	Los empleados contratados deberán firmar las cláusulas de confidencialidad, propiedad …	F	V	0
N/DPT–08	Despido	Cuando se despide a un empleado, se debe comunicar …	V	V	1
N/AS–02	Zonas críticas	Sólo estará permitido el acceso a zonas críticas …	F	V	0

Parte 2ª: Responda V/F a la pregunta ¿El procedimiento forma parte del SGSI de su compañía?

Código	Procedimiento	Respt. Usuario	Respt. Correct	Calificac
OS/SI–PR01	Procedimiento de revisión y evaluación periódica de la política de seguridad	V	V	1
OS/ISI–PR02	Procedimiento para autorización de acceso al sistema de información desde instalaciones personales.	F	F	1
SP/DPT–PR01	Procedimiento previo a la contratación	F	V	0
SF/AS–PR01	Control de acceso físico.	V	V	1
CO/GR–PR01	Procedimiento de revisión periódica de controles de red.	F	F	1

Una vez finalizado el examen, el sistema analizará el resultado obtenido para determinar si debe o no repetirse. En caso de aprobar, el usuario obtiene su certificado por un periodo de tiempo dado, y con dicho certificado obtiene el acceso al sistema de información (Tabla II).

TABLA II. RESULTADO DEL EXAMEN DE CERTIFICADO DE SEGURIDAD

La calificación obtenida por el usuario "***José Antonio Parra***" el día 12/08/2014 ha sido de **6.5** puntos (13/20), lo que le autoriza la concesión del certificado de cultura de la seguridad y con ello el acceso al sistema de información de la compañía. La validez de dicho certificado será hasta el **12/08/2015**, salvo que sea retirado antes por violaciones de seguridad.

Por otro lado, al producirse una violación de seguridad de una de las normativas que forma parte del SGSI, se ve afectado el certificado de cultura de seguridad, retirando 1 punto por sanción. Por lo tanto, siguiendo el caso del ejemplo, el siguiente paso del proceso de sanción es retirar un punto de sanción del certificado de cultura de seguridad del usuario denunciado, que actualmente está con 6.5, dejándolo en 5.5 puntos. En el caso de que el usuario hubiera bajado de 5 puntos, el sistema revocaría sus permisos de acceso al sistema de información de la empresa y le obligaría a obtener un nuevo certificado de cultura de seguridad.

Por último, cuando el usuario realiza el examen, las preguntas contestadas correctamente sirven para incrementar (+0.1%) y las incorrectas para disminuir (–0.1%) en una pequeña proporción los controles asociados a los reglamentos y procedimientos que formaron parte de las preguntas del examen (Tabla III).

TABLA III. EJEMPLO DE PENALIZACIÓN DE CONTROLES PARA EXAMEN DE CULTURA DE LA SEGURIDAD

Reglamento	Controles asociados	Cambio nivel
N/AS–03	8.3.3, 9.1.2	–0.1
N/AS–06	8.3.3, 9.1.2	+0.1
N/SE–09	9.2.4	–0.1
N/CS–01	10.5.1	+0.1
N/CS–03	10.5.1	+0.1
N/ISI–08	6.1.8	+0.1
N/AT–01	6.2.1	–0.1
N/OE–03	6.2.2, 10.2.2	–0.1
N/ISFI–05	13.1.1, 13.1.2, 13.2.1	+0.1
N/ISFI–15	8.2.3	+0.1
N/CI–03	7.1.1, 7.1.2	+0.1
N/CI–04	7.2.1	+0.1
N/DPT–07	6.1.5	–0.1
N/DPT–08	8.1.3, 8.3.1, 8.3.2	+0.1
N/AS–02	8.3.3, 9.1.2	–0.1
Reglamento	**Controles asociados**	**Cambio nivel**
OS/SI–PR01	5.1.2	+0.1
OS/ISI–PR02	6.1.4	+0.1
SP/DPT–PR01	6.1.5, 8.1.1	–0.1
SF/AS–PR01	8.3.3, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5	+0.1
CO/GR–PR01	10.6.1, 10.6.2, 11.4.4, 11.4.6, 11.4.7, 12.5.4	+0.1

Con la introducción de este sencillo sistema, se ha conseguido que reducir la tasas de fracaso de mantenimiento del sistema del 35% al 25%.

VI. CONCLUSIONES

En este artículo se ha mostrado la importancia que tiene la cultura de la seguridad dentro de los SGSIs en las PYMES, cómo se ha incorporado ese elemento dentro de la metodología MARISMA y las ventajas que se han obtenido.

La metodología MARISMA cumple con los principios que según la OCDE [27] debe seguir toda metodología de implantación y mantenimiento de un SGSI para que cuente con una correcta cultura de la seguridad de la información, garantizando el éxito del SGSI en la compañía. A continuación se muestran estos principios y cómo la metodología MARISMA los cumple en su totalidad, lo que es otra muestra de la validez de la misma:

- Concienciación, responsabilidad, respuesta, ética: Mediante un sistema de cursos basados en sencillas preguntas de tipo test y un sistema de premios y sanciones, se va creando de forma progresiva la conciencia de cultura de la seguridad entre los usuarios del sistema de información. La actividad A3.1 está basada en sencillos cuestionarios.
- Democracia: El sistema debe proteger los puestos de trabajo de los usuarios y a la compañía, a la vez que no les suponga impedimento alguno para realizar su trabajo con eficiencia. El principal objetivo de la actividad A3.1 es permitir el acceso sólo de aquellos usuarios que tengan constancia de la importancia de la seguridad en el sistema de información.
- Evaluación del riesgo: El sistema debe tener la capacidad de autoevaluar su riesgo de forma continuada en el tiempo, proponiendo medidas. Gracias a la nota obtenida en la actividad A3.1 (Obtención del certificado de cultura de la seguridad) se tiene una constancia del nivel de conocimiento con respecto al reglamento de los usuarios, y esta medida se ve completada con la evaluación de riesgos y el plan de mejora de la actividad A2.3 (Realización del análisis de riesgos).
- Diseño y realización de la seguridad: La metodología está pensada para integrarse dentro del marco de trabajo como una pieza más, orientando a organizar la forma de trabajo con respecto a la seguridad sin ser una carga para los trabajadores. La actividad A3.1 está totalmente integrada dentro del trabajo diario con el SGSI como una actividad más.
- Gestión de la seguridad: La metodología debe permitir gestionar la seguridad de una forma cómoda para que la cultura de la seguridad asociada a ella vaya introduciéndose de forma natural en los usuarios del sistema de información. Toda la metodología MARISMA ha sido enfocada pensando en la sencillez a la hora de trabajar con ella.
- Reevaluación: La metodología debe contar con métricas que permitan que el sistema pueda reevaluarse de forma periódica con bajo coste y recomendar las medidas adecuadas. La metodología MARISMA cuenta con métricas de carácter general y otras de carácter específico que permiten mantener, con un coste muy bajo, actualizado en todo momento el cuadro de mandos de seguridad, lo que posibilita conocer el nivel de cumplimiento de los controles de seguridad en todo momento. Ejemplo de estas métricas es la nota del certificado de cultura de la seguridad de cada usuario, que define un nivel mínimo de cultura de la seguridad para los usuarios del sistema.

Las características ofrecidas por la nueva metodología y su orientación a las PYMES ha sido muy bien recibida, y su aplicación está resultando muy positiva ya que permite acceder a este tipo de empresas al uso de sistemas de gestión de seguridad de la información, algo que hasta ahora había estado reservado a grandes compañías. Además, con esta metodología se obtienen resultados a corto plazo y se reducen los costes que supone el uso de otras metodologías, consiguiendo un mayor grado de satisfacción de la empresa.

Todas las mejoras futuras de la cultura de la seguridad se están orientando a reducir los incumplimientos en materia de gestión de la seguridad por parte de los usuarios del sistema de información, pero siempre respetando el principio de coste de recursos y orientada a la cultura de la seguridad.

AGRADECIMIENTOS

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

Referencias

[1] 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.

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

[3] Disterer, G., *Iso/iec 27000, 27001 and 27002 for information security management.* 2013.

[4] 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.

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

[6] Dhillon, G., *Managing Information System Security*, ed. M.P. Ltd1997, Great Britain. 210.

[7] 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.

[8] Whitman, M. and H. Mattord, *Management of information security*2013: Cengage Learning.

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

[10] Furnell, S.M., M. Gennatou, and P.S. Dowland. *Promoting Security Awareness and Training within Small Organisations*. in *1st Australian Information Security Management Workshop*. 2000. Deakin University, Geelong, Australia.

[11] Schlienger, T. and S. Teufel. *Information Security Culture - From Analysis to Change.* in *3rd Annual IS South Africa Conference*. 2003. Johannesburg, South Africa.

[12] Lichtenstein, S. and P.M.C. Swatman. *Effective Management and Policy in E-business Security*. in *Fourteenth Bled Electronic Commerce Conference*. 2001b. Bled, Slovenia.

[13] Cole, K.S., S.M. Stevens-Adams, and C.A. Wenner, *A Literature Review of Safety Culture*. Sandia National Laboratories, 2013.

[14] Rosanas, J.M. and M. Velilla, *The Ethics of Management Control Systems: Developing Technical and Moral Values.* Business Ethics, 2005. **53**: p. 87-96.

[15] Schultz, E., *The Human Factor in Security*. Computers & Security, 2005. **24**: p. 425-426.

[16] Bugdol, M. and P. Jedynak, *Integrated Management Systems*2015: Springer.

[17] Von Solms, B., *Information Security - The Third Wave?* Computers and Security, 2000. **19**(7): p. 615-620.

[18] Bozic, G. *The role of a stress model in the development of information security culture*. in *MIPRO, 2012 Proceedings of the 35th International Convention*. 2012.

[19] Magklaras, G. and S. Furnell. *The Insider Misuse Threat Survey: Investigating IT misuse from legitimate users*. in *International Information Warfare Conference*. 2004. Perth, Australia.

[20] Dhillon, G. and J. Backhouse, *Current Directions in Information Systems Security Research: Toward Socio-Organizational Perspectives.* Information Systems Journal, 2001b. **11**(2): p. 127-153.

[21] Galletta, D.F. and P. Polak. *An Empirical Investigation of Antecedents of Internet Abuse in the Workplace*. in *AIS SIG-HCI Workshop*. 2003. Seattle: December, 2003.

[22] CSI/FBI, *Tenth Annual CSI/FBI Computer Crime and Security Survey*. Computer Security Institute2005, USA.

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

[24] AusCERT, *Australian Computer Crime and Security Survey*. AusCERT, 2005.

[25] Ernst&Young, *2006 Global Information Security Survey*. Ernst & Young, 2006.

[26] DTI. *The_Empirical_Economics_of_Standards*. 2005 www.dti.gov.uk/iese/ The_Empirical_Economics_of_Standards.pdf.

[27] 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.

[28] Nosworthy, J., *Implementing Information Security in the 21st Century - Do You Have the Balancing Factors.* Computers and Security, 2000. **19**(4): p. 337-347.

[29] Martins, A. and J.H.P. Eloff. *Information Security Culture*. in *IFIP TC11 17th International Conference on Information Security (SEC2002)*. 2003. Cairo, Egipt.

[30] Schlienger, T. and S. Teufel. *Information Security Culture: The Socio-cultural Dimension in Information Security Management*. in *IFIP TC11 17th International Conference on Information Security (SEC2002)*. 2002. Kluwer Academic Publishers, USA.

[31] Zakaria, O. and A. Gani. *A Conceptual Checklist of Information Security Culture*. in *2nd European Conference on Information Warfare and Security*. 2003. University of Reading, UK: 30 June – 1 July.

[32] Zakaria, O., P. Jarupunphol, and A. Gani. *Paradigm Mapping for Information Security Culture Approach*. in *4th Australian Conference on Information Warfare and IT Security*. 2003b. Adelaide, Australia.

[33] Schein, E.H., *Organizational Culture and Leadership 2nd*, ed. Jossey-Bass1992, San Francisco, USA.

[34] Chia, P.A., A.B. Ruighaver, and S.B. Maynard. *Understanding Organizational Security Culture.* in *Security Culture. Proc. of PACIS2002*. 2002b. Japan.

[35] Siponen, M.T., *A conceptual foundation for organizational information security awareness.* Information Management & Computer Security, 2000. **8**(1): p. 31-41.

[36] Von Solms, B. and R. Von Solms, *Incremental Information Security Certification*. Computers & Security, 2001. **20**: p. 308-310.

[37] Vroom, C. and R. Von Solms, *Towards information security behavioural compliance.* Computers & Security, 2004. **23**(3): p. 191-198.

[38] Chia, P.A., S.B. Maynard, and A.B. Ruighaver. *Exploring Organisational Security Culture: Developing A Comprehensive Research Model*. in *IS ONE World Conference*. 2002. Las Vegas, USA.

[39] Helokunnas, T. and R. Kuusisto. *Information security culture in a value net.* in *2003 IEEE International Engineering Management Conference (IEMC 2003)*. 2003b. Albany, New York, USA: 2-4 November 2003.

[40] Straub, D., et al., *Toward a Theory-Based Measurement of Culture.* Global Information Management, 2002. **10**(1): p. 13-23.

[41] Kuusisto, T. and I. Ilvonen. *Information security culture in small and medium size enterprises*. in *Frontiers of e-business research 2003.* 2003.

[42] Detert, J., R. Schroeder, and A. J. Mauriel, *A Framework For Linking Culture and Improvement Initiatives in Organisations.* The Academy of Management Review, 2000. **25**(4): p. 850-863.

[43] Taylor, M. and A. Murphy, *SMEs and eBusiness.* Small Business and Enterprise Development, 2004. **11**(3): p. 280-289.

[44] Hutchinson, D., C. Armitt, and D. Edwards-Lear, *The application of an agile approach to it security risk management for SMES.* 2014.

[45] 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.

[46] Hutchinson, D. and M. Warren. *e-Business Security Management for Australian Small SMEs - A Case Study*. in *e-Business: how far have we come? Proceedings of the 7th International We-B (Working for E-Business) Conference*. 2006c. Electronic Commerce Research Unit ECRU, Australia.

[47] 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.

[48] Helokunnas, T. and L. Iivonen. *Information Security Culture in Small and Medium Size Enterprises*. in *e-Business Research Forum – eBRF 2003*. 2003. Tampere, Finland: Tampere University of Technology.

[49] Warren, M.J. *Australia's Agenda for E-Security Education and Research*. in *TC11/WG11.8 Third Annual World Conference on Information Security Education (WISE3)*. 2003. Naval Post Graduate School, Monterey, California, USA.

[50] Von Solms, R. and B. Von Solms, *From policies to culture.* Computers & Security, 2004. **23**(4).

[51] Furnell, S.M. and N.L. Clarke. *Organisational Security Culture: Embedding Security Awareness, Education and Training*. in *4th World Conference on Information Security Education (WISE 2005)*. 2005. Moscow, URSS.

[52] Van Niekerk, J.C. and R. Von Solms. *Establishing an Information Security Culture in Organisations: an Outcomes-based Education Approach*. in *ISSA 2003:3rd Annual IS South Africa Conference*. 2003. , Johannesburg, South Africa: 9-11 July 2003.

[53] Hutchinson, D. and M. Warren. *Australian SMES and e-Security Guides on Trusting the Internet*. in *Fourth Annual Global Information Technology Management World Conference*. 2003. Global Information Technology Management Association (GITMA), USA

[54] Knapp, K.J., et al., *Information Security: Management's effect on culture and policy.* Information Management & Computer Security, 2006. **14**(1): p. 24-36.

[55] Lichtenstein, S., *Internet security policy for organisations*. Unpublished thesis (PhD) (public version), ed. S.o.I.M.S. Monash University2001, Melbourne, Australia.

[56] Stanton, J.M., et al., *Analysis of end-user security behaviors.* Computers & Security, 2004. **24**: p. 124-133.

[57] Lichtenstein, S. and P.M.C. Swatman. *The Potentialities of Focus Groups in e-Business Research: Theory Validation, in Seeking Success in e-Business: a Multi-disciplinary Approach*. in *IFIP TC8/WG 8.4 Second Working Conference on E-business: Multidisciplinary Research and Practice*. 2003. Copenhagen, Denmark: Kluwer Academic Publishers.

[58] Furnell, S., A. Warren, and P.S. Dowland. *Improving security awareness and training through computer-based training*. in *3rd World Conference on Information Security Education (WISE 2004)*. 2004. Monterey, California.
[59] Dutta, A. and K. McCrohan, *Management's Role in Information Security in a Cyber Economy*. California Management Review, 2002. **45**(1): p. 67-87.
[60] 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.
[61] ABS, *1321.0 - Small Business in Australia.* Australian Bureau of Statistics, 2001.
[62] Gupta, A. and R. Hammond, *Information systems security issues and decisions for small businesses.* Information Management & Computer Security, 2005. **13**(4): p. 297-310.
[63] O'Halloran, J., *ICT business management for SMEs.* Computer Weekly, 2003. **December 11**.
[64] Dhillon, G., *Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns.* Computers & Security, 2001b. **20**(2): p. 165-172.
[65] 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.
[66] Sánchez, L.E., et al., *Managing Security and its Maturity in Small and Medium-sized Enterprises.* J. UCS, 2009. **15**(15): p. 3038-3058.
[67] 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.
[68] 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.
[69] ISO/IEC27001, *ISO/IEC 27001:2013, Information Technology - Security Techniques Information security management systemys - Requirements.*, 2013.
[70] ISO/IEC27002, *ISO/IEC 27002:2013, the international standard Code of Practice for Information Security Management (en desarrollo).* 2013.
[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] Sánchez, L.E., et al., *Security Culture in Small and Medium-Size Enterprise*, in *ENTERprise Information Systems*2010, Springer Berlin Heidelberg. p. 315-324.

ntonio 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). He belongs to various professional and research associations (COIICLM, ATI, ASIA, ISACA, eSEC, INTECO, etc).

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). He belongs to various professional and research associations (COIICLM, ATI, ASIA, ISACA, eSEC, INTECO, etc).

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

Daniel Mellado holds a PhD and MSc in Computer Science from the Castilla- La Mancha University (Spain) and holds a degree in Computer Science from the Autonomous University of Madrid (Spain), and he is Certified Information System Auditor by ISACA (Information System Audit and Control Association). He is Assistant Professor of the Department of Information Technologies and Systems at the Rey Juan Carlos University (Spain). He participates at the GSyA research group of the Department of Information Technologies and Systems at the Castilla- La Mancha University. He is civil servant at the Spanish Tax Agency (in Madrid, Spain), where he works as IT Auditor Manager. His research activities are security governance, security requirements engineering, security in cloud computing, security in information systems, secure software process improvement and auditory, quality and product lines. He has several dozens of papers in national and international conferences, journals and magazines on these subjects and co-author of several chapter books. He belongs to various professional and research associations (ASIA, ISACA, ASTIC, ACTICA, etc).

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. He belongs to various professional and research associations (ATI, AEC, ISO, IFIP WG11.3 etc.).