

# Madrid News

ISACA® MADRID, Paseo de la Castellana nº 91 3ª-I. Madrid 28046  
<http://www.isacamadrid.es> [administracion@isacamadrid.es](mailto:administracion@isacamadrid.es) 91.636.29.60



## Este número

**Julio San José Sánchez**  
 Vocal Relaciones con Asociados

### Contenido

Este número	1
Firma invitada	2
Noticias de la Asociación	5
Noticias del trimestre	6
La asociación en cifras	8

Desde Madrid News, os deseamos



Feliz 2010

## Firma Invitada

Luís Enrique Sánchez , Antonio Santos-Olmo Parra

# Metodología para Gestionar la Seguridad en las PYMES

### Introducción

En un entorno empresarial globalizado y competitivo como el existente en la actualidad, las compañías dependen cada vez más de sus sistemas de información, pues se ha demostrado que tienen una enorme influencia para aumentar su nivel de competitividad. Pero sin una adecuada gestión de la seguridad estos sistemas de información carecen de valor real, ya que no pueden aportar las suficientes garantías de continuidad a las empresas. Por ello, las compañías empiezan a tener conciencia de la enorme importancia que tiene el poseer unos sistemas de seguridad de la información adecuados, así como una correcta gestión de los mismos. De esta forma, pese a que muchas empresas todavía asumen el riesgo de prescindir de las medidas de protección adecuadas, otras muchas han comprendido que los sistemas de información no son útiles sin los sistemas de gestión de seguridad y las medidas de protección asociados a ellos.

Gran parte de este cambio de mentalidad en las empresas tiene su origen en el cambio social producido por Internet y la rapidez en el intercambio de información, que ha dado lugar a que las empresas empiecen a tomar conciencia del valor que tiene la información para sus organizaciones y se preocupen de proteger sus datos. De esta forma, las empresas ya han tomado conciencia de que la información y los procesos que apoyan los sistemas y las redes son sus activos más importantes (Dhillon and Backhouse 2000) Estos activos están sometidos a riesgos de una gran variedad, que pueden afectar de forma crítica a la empresa. Así, la importancia de la seguridad en los sistemas de información viene

avalada por numerosos trabajos (Masacci, Prest et al. 2005; Walker 2005), por citar sólo algunos.

Anteriormente, las compañías que habían decidido proteger sus sistemas de información habían afrontado proyectos desde la perspectiva de que la seguridad era algo individual que afectaba a un objeto pero no al conjunto al que pertenecía el objeto, es decir, se basaban en la implantación de medidas de seguridad, pero sin llevar a cabo una adecuada gestión de dichas medidas (Humphrey 2008). Con el tiempo, al no disponer de una gestión adecuada, los controles implantados dejaban de mantenerse y se convertían en controles pasivos, que en lugar de ayudar a mejorar la seguridad contribuían a desinformar, ofreciendo información errónea en muchos casos. Así, en (Tsuji 2004) se destaca que para la construcción de un sistema de seguridad no bastan los aspectos tecnológicos, sino que también son necesarios los aspectos de gestión, así como los aspectos legales y éticos.

El problema de la seguridad de la información se caracteriza por la complejidad y la interdependencia. La gestión de la seguridad contiene un número importante de factores y elementos que se interrelacionan entre sí. Las PYMES en los países desarrollados suelen tener una débil comprensión de la seguridad de la información, tecnologías de seguridad y medidas de control, y suelen dejar el análisis de riesgos o el desarrollo de las políticas de seguridad olvidados (Gupta and Hammond 2005). Esto puede deberse a que las PYMES carecen de los recursos, tiempo y conocimientos especializados para coordinar la seguridad de la información u ofrecer información adecuada sobre la seguridad, la formación y la educación (Gupta and Hammond 2005).

Sin embargo, la literatura sugiere una explicación muy diferente. (Johnson and Koch 2006) dicen que las PYMES no quieren pagar por la seguridad, y que prefieren mantener una seguridad física con la que están familiarizados. (Gupta and Hammond 2005) señalan que, al carecer de un conocimiento especializado de tecnologías de seguridad, las PYMES suelen mantener la seguridad con las tecnologías con las que ya están familiarizados. Así mismo, las PYMES no ven la seguridad vinculada a la estrategia empresarial, lo que impacta directamente en el cumplimiento de la misma (O'Halloran 2003). De hecho, una investigación reciente pone de manifiesto la necesidad de vincular la seguridad de la información con los sistemas de información de planificación estratégica y, por tanto, con los objetivos de la empresa (Doherty and Fulford 2006).

En el presente artículo describimos la metodología que hemos desarrollado para la gestión de la seguridad en las PYMES, que pretende solucionar los problemas detectados en las metodologías clásicas, las cuales no se están mostrando eficientes a la hora de su implantación en las PYMES debido a su complejidad y otra serie de factores que serán analizados con detalle en las siguientes secciones del artículo.

### **MGSM-PYME: METODOLOGÍA PARA LOS SGSI EN LAS 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 tienen 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 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 pretende 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.

“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. 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.

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 1).



Figura 1: Subprocesos de la metodología.

Esta 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. 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.

La generación de esquemas es una labor que será realizada por los expertos en seguridad y aunque su elaboración es un proceso costoso, se ve compensado por las enormes reducciones de costes que produce en los otros subprocesos al poder ser reutilizado por compañías con características parecidas (mismo sector y mismo tamaño)

## Referencias

- Batista, J. and A. Figueiredo (2000). "SPI in very small team: a case with CMM." Software Process Improvement and Practice 5(4): 243-250.
- Calvo-Manzano, J. A. (2000) Método de Mejora del Proceso de desarrollo de sistemas de información en la pequeña y mediana empresa (Tesis Doctoral) Universidad de Vigo.
- COBITv4.0 (2006). Cobit Guidelines, Information Security Audit and Control Association.
- Dhillon, G. and J. Backhouse (2000). "Information System Security Management in the New Millennium." Communications of the ACM 43(7): 125-128.
- Doherty, N. F. and H. Fulford (2006). "Aligning the Information Security Policy with the Strategic Information Systems Plan." Computers & Security 25(2): 55-63.
- Gupta, A. and R. Hammond (2005). "Information systems security issues and decisions for small businesses." Information Management & Computer Security 13(4): 297-310.
- Hareton, L. and Y. Terence (2001). "A Process Framework for Small Projects." Software Process Improvement and Practice 6: 67-83.
- Humphrey, E. (2008). Information security management standards: Compliance, governance and risk management. Information Security Tech. Report.
- ISO/IEC17799 (2005). ISO/IEC 17799. Information Technology - Security techniques - Code of practice for information security management.
- Johnson, D. W. and H. Koch (2006). Computer Security Risks in the Internet Era: Are Small Business Owners Aware and Proactive? 39th Annual Hawaii International Conference on System Sciences (HICSS'06).
- MageritV2 (2005) Metodología de Análisis y Gestión de Riesgos para las Tecnologías de la Información, V2, Ministerio de Administraciones Públicas.
- Maturity Model (SSE-CMM), Version 3.0. Department of Defense. Arlington VA. 326.
- Tsujii, S. (2004) Paradigm of Information Security as Interdisciplinary Comprehensive Science. International Conference on Cyberworlds (CW'04), IEEE Computer Society.
- Tuffley, A., B. Grove, et al. (2004). "SPICE For Small Organisations." Software Process Improvement and Practice 9: 23-31.
- Walker, E. (2005). "Software Development Security: A Risk Management Perspective." The DoD Software Tech. Secure Software Engineering 8(2): 15-18.

**Luis Enrique Sánchez**

**Antonio Santos-Olmo Parra**

SICAMAN NT. Departamento de I+D+i,  
Juan José Rodrigo, 4. Tomelloso,  
Ciudad Real, España

Pueden ser localizados en

{lesanchez, asolmo} @sicaman-nt.com

## Noticias de la Asociación

EL pasado día 26 de Noviembre tuvimos la ocasión de volver a reunirnos en el *Hotel Holliday In* de Madrid para celebrar la Asamblea General 2009.

Algunos de los puntos tratados fueron:

- Evolución de los asociados
- Órganos de gobierno
- Relaciones con capítulos ISACA® España
- Formación
- Certificaciones CISA®, CISM® y CGEIT®
- Charlas Técnicas
- Comisiones de trabajo
- Publicaciones
- Web
- Bolsa de empleo
- Estado de cuentas
- Presupuesto



Posteriormente fue presentado por la Junta, la propuesta de gestión para el 2010 que resumimos brevemente

- Ajustes al Plan de Formación
- Consolidación del Boletín ISACA® MadridNews
- Desarrollo de indicadores, para medir la satisfacción del asociado
- Acciones de Marketing dirigido
- Jornadas de Auditoría 2010
- Implantación nuevo modelo de Patrocinios
- Comisión de Gobierno
- Actividades Comisión Gobierno Corporativo de las TI

## Noticias del trimestre

Coincidiendo con la celebración de la Asamblea General de la Asociación, el pasado 26 de Noviembre, se procedió a la entrega de los certificados que acreditan a sus poseedores como los TOP CISM®, CISA® y CGEIT®

A continuación unas instantáneas de los momentos de la entrega,



## ISACA® invitada a exponer en las Jornadas del IAI

Durante los meses de Noviembre y Diciembre, Auditoría Interna tuvo la oportunidad de disertar en distintos foros donde expresó su visión sobre el desarrollo de la profesión de la Auditoría en Tecnología de la Información.

Durante el mes de Noviembre y durante el desarrollo de las XIV Jornadas de Auditoría Interna de España, ISACA® Madrid presentó una ponencia denominada “La Auditoría Informática como Garante del Control Interno”.

Seguida por más de 300 personas, se destacó la importancia y el crecimiento que ha tenido esta actividad dentro de las organizaciones modernas, marcando entre otros temas que “.. Ya no puede ser aceptado un sistema de control interno que no base fuertemente el mismo en la Tecnología instaurada en cada empresa”.

Tras la exposición se arribó a la conclusión que la Auditoría en TI garantiza el control interno porque, da seguridad sobre la gestión de los recursos tecnológicos y su alineación con el negocio, ayuda a alcanzar los objetivos estratégicos, da visión integrada y completa de la situación de la organización y de sus riesgos, no es eficaz ni eficiente auditar los riesgos operativos sin considerar los tecnológicos por otro y finalmente no podemos considerar madura a una organización de control interno que no disponga de la función de auditoría en TI o que ésta no esté integrada y alineada a la estrategia y objetivos del negocio.



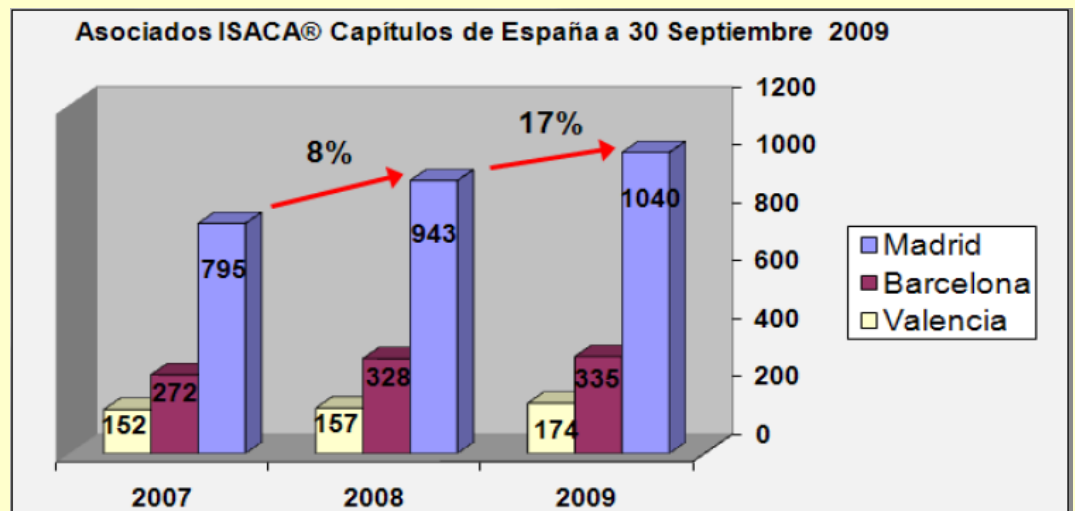
Foto de la presentación en las Jornadas de Auditoría Interna España 2009

## Cifras ISACA® Madrid

A lo largo de 2009, hemos superado la cifra del millar de asociados



Lo que nos sitúa como el **cuarto capítulo de Europa** y el **25º a nivel mundial**



Consulta la web para ver el contenido de los cursos

*Amplio catálogo con cursos*

*“La formación es el valor fundamental en la ecuación de la seguridad”.*



# Únete

# al

# líder

ISACA®, Capítulo de Madrid (183)  
Pº Castellana, 91 - 3º Izda. 28046  
Madrid

Teléfono  
91.636.29.60

Fax  
91.634.42.44

Correo electrónico  
[administracion@isacamadrid.es](mailto:administracion@isacamadrid.es)



---

*ISACA® Madrid, no comparte necesariamente las opiniones vertidas, siendo estas expresadas por los autores a título personal*

---