Actas
X Reunión Española sobre Criptología y Seguridad de la Información

Editores: Luis Hernández Encinas
Ángel Martín del Rey

Editores: Luis Hernández Encinas y Ángel Martín del Rey

Diseño de cubiertas: Yaiza Cortés Gómez

Imprime: SIGNE S.A. Impresores de Seguridad
Avda. de la Industria, 18 – 28760 Tres Cantos, (Madrid)
www.signe.es

Caminamos con paso firme hacia el pleno establecimiento de la que se ha dado en denominar Sociedad de la Información. No sólo los diferentes gobiernos y administraciones públicas sino también las empresas y organismos privados se han implicado en este desarrollo poniendo a disposición de los ciudadanos nuevos, potentes y eficaces servicios telemáticos: gobierno electrónico, comercio electrónico, voto electrónico, etc. En este sentido en el año 2006 se empezó a expedir el nuevo Documento Nacional de Identidad Electrónico (DNIe) que permite a su poseedor la firma digital de documentos electrónicos. Este fascinante nuevo escenario exige el desarrollo de algoritmos, medidas y políticas de seguridad que garanticen la confidencialidad, la integridad, la autenticidad y el no repudio de las gestiones realizadas.

Consecuentemente se ha dado lugar a un enorme esfuerzo de investigación en el campo de la protección de la información. Así, una de las líneas de investigación de la comunidad científica de mayor importancia y actualidad es el diseño, análisis e implantación de protocolos criptográficos que garanticen la seguridad de los datos transmitidos, almacenados o gestionados electrónicamente.

La *Reunión Española sobre Criptología y Seguridad de la Información* (RECSI) es el congreso científico referente español en el tema de la Seguridad en las Tecnologías de la Información. En él se dan cita periódicamente los principales investigadores españoles en el tema así como invitados extranjeros de reconocido prestigio. En el año 2008 se celebrará la décima edición de este congreso en el mes de septiembre y en la ciudad de Salamanca. Las pasadas ediciones se realizaron en Palma de Mallorca (1991), Madrid (1992), Barcelona (1994), Valladolid (1996), Torremolinos (1998), Santa Cruz de Tenerife (2000), Oviedo (2002), Leganés (2004) y Barcelona (2006).

La X RECSI se ha desarrollado entre el 2 y el 5 de septiembre de 2008. En ella se han llevado a cabo varias conferencias plenarias a cargo de investigadores de reconocido prestigio (Carlo Blundo, Ljupco Kocarev, Hugo Scolnik, Fausto Montoya) y de organismos y agencias tanto públicas como privadas (Centro Criptológico Nacional, Ministerio del Interior, Dirección General de Innovación y Modernización Administrativa de la Junta de Castilla y León, Signe, Realsec y Ericsson). También se han presentado 70 contribuciones científicas divididas en dos sesiones paralelas: Criptología y Seguridad de la Información.

Queremos dar las gracias a todos los patrocinadores y colaboradores por su apoyo moral y económico: CajaDuero, Realsec, Ericsson, IECISA, Junta de Castilla y León, Universidad de Salamanca, Centro Criptológico Nacional, Fábrica Nacional de Moneda y Timbre, Consejo Superior de Investigaciones Científicas, Ministerio de Ciencia e Innovación, Criptored, Red Temática de Matemáticas para la Sociedad de la Información y RENFE.

Finalmente queremos también mostrar nuestra más profunda gratitud a *Signe S.A. Impresores de Seguridad* por la elaboración de estas actas y por su incondicional apoyo.

Septiembre de 2008

Luis Hernández Encinas

Ángel Martín del Rey

Comités

Comité de Honor

S.A.R. El Príncipe de Asturias D. Felipe de Borbón
Excma. Sra. Ministra de Educación
Excma. Sra. Ministra de Defensa
Excmo. Sr. Ministro de Interior
Excmo. Sr. Secretario de Estado de Universidades e Investigación
Excmo. Sr. Consejero de Educación de la Junta de Castilla y León
Excma. Sra. Consejera de Administración Autonómica de la Junta de Castilla y León
Excmo. Sr. Alcalde de Salamanca
Excma. Sra. Presidenta de la Diputación de Salamanca
Excmo. y Magfco. Sr. Rector de la Universidad de Salamanca
Excmo. Sr. Vicerrector de Investigación de la Universidad de Salamanca

Comité Organizador

Presidente: Ángel Martín del Rey, Universidad de Salamanca
Vicepresidente: Luis Hernández Encinas, C.S.I.C.
Secretario: Gerardo Rodríguez Sánchez, Universidad de Salamanca
Tesorera: Ascensión Hernández Encinas, Universidad de Salamanca
Vocales: María Teresa de Bustos Muñoz, Universidad de Salamanca
María Araceli Queiruga Dios, Universidad de Salamanca
Yaiza Cortés Gómez, Universidad de Salamanca
Javier Espinosa García, C.S.I.C.

COMITÉ CIENTÍFICO

Abascal Fuentes, Policarpo	Universidad de Oviedo
Álvarez Marañón, Gonzalo	C.S.I.C.
Amigó García, José María	Universidad Miguel Hernández
Areitio Bertolín, Javier	Universidad de Deusto
Borrell Viader, Joan	Universidad Autónoma de Barcelona
Caballero Gil, Pino	Universidad de La Laguna
Dávila Muro, Jorge	Universidad Politécnica de Madrid
Domingo Ferrer, Josep	Universidad Rovira i Virgili
Durán Díaz, Raúl	Universidad de Alcalá de Henares
Fernández-Medina Patón, Eduardo	Universidad de Castilla La Macha
Fúster Sabater, Amparo	C.S.I.C.
González Vasco, Mª Isabel	Universidad Rey Juan Carlos
Gutiérrez Gutiérrez, Jaime	Universidad de Cantabria
Hernández Encinas, Luis	C.S.I.C.
Hernández Goya, Candelaria	Universidad de La Laguna
Herrera Joancomartí, Jordi	Universitat Operta de Catalunya
Huguet Rotger, Llorenç	Universidad de las Islas Baleares
López Muñoz, Javier	Universidad de Málaga
Martín del Rey, Ángel	Universidad de Salamanca
Martínez López,Consuelo	Universidad de Oviedo
Miret Biosca, José María	Universidad de Lleida
Padró Laimon, Carles	Universidad Politécnica de Cataluña
Peinado Domínguez, Alberto	Universidad de Málaga
Ramió Aguirre, Jorge	Universidad Politécnica de Madrid
Ramos Álvarez, Benjamín	Universidad Carlos III de Madrid
Ribagorda Garnacho, Arturo	Universidad Carlos III de Madrid
Rifá Coma, Josep	Universidad Autónoma de Barcelona
Sáez Moreno, Germán	Universidad Politécnica de Cataluña
Salazar Riaño, José Luis	Universidad de Zaragoza
Sánchez Ávila, Carmen	Universidad Politécnica de Madrid
Sempere Luna, José María	Universidad Politécnica de Valencia
Soriano Ibáñez, Miguel	Universidad Politécnica de Cataluña
Tena Ayuso, Juan	Universidad de Valladolid
Villar Santos, Jorge	Universidad Politécnica de Cataluña

ÍNDICE

CONFERENCIAS INVITADAS

Certified information access 3
C. Blundo and C. Galdi

Nuevos algoritmos de factorización de enteros para atacar RSA 9
H. Scolnik

Cryptographic primitives based on quasigroups and quasigroup transformations 21
D. Gligoroski and L. Kocarev

Distribución cuántica de claves: luces y sombras 27
F. Montoya

CRIPTOLOGÍA

Private, but restricted, access to databases 37
J. Herranz

Un esquema de firma digital con curvas elípticas isógenas 43
F.J. Galán y J. Tena

Observaciones sobre la distribución de primos con representaciones binarias signadas cortas 47
J. Angel Angel y G. Morales-Luna

The SIP security enhanced by using pairing-assisted Massey-Omura signcryption 51
A. M. Deusajute and P.S.L.M. Barreto

Non-asymptotic performance evaluation of key distribution protocols based on noisy channels in presence of an active adversary 63
V. Yakovlev, V. Korzhik, and G. Morales-Luna

Shuttle: New compression function for iterated hash 69
Bo Yang, Zhimin Li, Lin Li, Shihui Zheng, Yixian Yang, and Zhihui Zhang

On the inadequacy of the logistic map for cryptographic applications 77
D. Arroyo, G. Alvarez, and V. Fernandez

On the use of genetic programming to develop cryptographic hashes 83
A. Torres-Vázquez, A. Ribagorda, and B. Ramos

Generación pseudoaleatoria basada en mapas caóticos: beneficios de sus simetrías y de sus propiedades geométricas 91
C. Pellicer-Lostao y R. López-Ruiz

Nuevos parámetros seguros para el criptosistema de Chor-Rivest e implementación con Magma 101
F. Hernández Álvarez, L. Hernández Encinas y A. Queiruga Dios

Related message attacks: A formal treatment 111
M. I. González Vasco and A. L. Pérez del Pozo

Designing self-synchronizing stream ciphers with flat dynamical systems 119
G. Millèrioux, P. Guillot, J.M. Amigó, and J. Daafouz

Creating an iris image from a given iris template 125
A. de Santos, C. Sánchez, and V. Jara

Caracterización y construcción de funciones bent de $n + 1$ variables a partir de funciones booleanas de n variables 133
J.J. Climent, F.J. García y V. Requena

Votación electrónica tolerante a fallos para escenarios móviles 141
V. Daza, J. Domingo-Ferrer y F. Sebé

Criptosistema basado en el esquema de McElice generado con códigos convolucionales 151
J.J. Climent, V. Herranz, V. Tomás y C. Perea

Experimental quantum key distribution at a wavelength of λ~850nm 157
V. Fernandez, D. Arroyo, M.J. Garcia, P.A. Hiskett, R.J. Collins, G.S. Buller, and A.B. Orue

Criptoanálisis de un cifrador caótico realizado con redes neuronales celulares 163
A.B. Orue, V. Fernandez, G. Pastor, M. Romera, G. Alvarez y F. Montoya

Curvas isógenas para evitar ataques ZVP 173
J. Miret, D. Sadornil, J. Tena, R. Tomàs y M. Valls

Sobre la probabilidad de éxito de dos preguntas relacionadas 181
P. Morillo y C. Ràfols

Modelización del generador auto-shrinking mediante autómatas celulares 187
A. Fúster-Sabater, M.E. Pazo-Robles y P. Caballero-Gil

Curvas de género 2 sobre cuerpos binarios: un filtro para usos criptográficos 195
J. Miret, R. Moreno, J. Pujolàs y A. Rio

On the optimization of bipartite secret sharing schemes 201
A. Cheraghi, O. Farràs, C. Padró, and L. Vázquez

Esquemas de firma digital con verificación distribuida 209
J. Herranz, A. Ruiz y G. Sáez

Sistema electrónico de votación basado en firmas a ciegas con emparejamientos 217
L. López-García, F. Rodríguez-Henríquez y M.A. León-Chávez

Conditions on the *C*-TA property in linear codes 227
M. Fernandez, J. Cotrina, M. Soriano, and N. Domingo

An evaluation of the energy cost of authenticated key agreement in wireless sensor networks 231
D. Galindo, R. Roman, and J. Lopez

Protección de la privacidad mediante microagregación multivariante basada en algoritmos genéticos: selección por ruleta vs. selección uniforme 237
U. González-Nicolas y A. Solanas

SEGURIDAD DE LA INFORMACIÓN

La lucha contra el ciberterrorismo y los ataques informáticos 251
A. Gómez Vieites

A fast indexless digital forensic search procedure 263
S. Petrovic and K. Franke

Modelo de detección de intrusos basado en sistemas multi-agente, inteligencia computacional y representaciones ontológicas 271
G.A. Isaza, A.G. Castillo y A.A. Segura

Un sistema de marca de agua de espectro expandido tolerante a ataques de transposición y supresión 283
F. Sebé y J. Domingo-Ferrer

Componentes ejecutables, un paso más allá en los patrones de seguridad 287
D. Serrano, B. Gallego-Nicasio Crespo, A. Muñoz y A. Maña

El DNI electrónico: aproximación a su regulación jurídica 295
A. Martínez Nadal y J.L. Ferrer Gomila

Computación segura de sistemas multiagentes aplicada en ambientes inteligentes 307
A. Muñoz, A. Maña y D. Serrano

Un framework genérico para el soporte de pagos por clic 315
A. Ruiz-Martínez, Ó. Cánovas y A.F. Gómez-Skarmeta

Clasificación de canales encubiertos. Un nuevo canal: Covert_DHCP 325
R. Ríos y J. A. Onieva

Analysis of new threats to online banking authentication schemes 337
O. Delgado, A. Fúster-Sabater, and J.M. Sierra

Herramienta DCST. Automatización de estegoanálisis en redes sociales 345
A. Muñoz Muñoz y J. Carracedo Gallardo

Sistema impreciso de control de acceso basado en la conversión cuantificada de atributos para escenarios de interoperabilidad 357
C. Martínez-García, G. Navarro-Arribas, J. Borrell y A. Martín-Campillo

Prevención de ataques de *Cross-Site Scripting* en aplicaciones Web 369
J. Garcia-Alfaro y G. Navarro-Arribas

Billetes electrónicos seguros 379
J. Castellà-Roca y A. Vives-Guasch

Componente de tolerancia a fallos para un sistema de agentes móviles sobre plataformas ligeras 389
J. Borrell, J. Cucurull, M.C. de Toro, C. Martínez-García, X. Piñol y S. Robles

Consideración sobre la integración de módulos criptográficos basados en hardware vs. módulos criptográficos software 399
J.M. Delgado Barroso y J.A. Gordo Bravo

JXTA security in basic peer operations 405
J. Arnedo-Moreno and J. Herrera-Joancomartí

An order independent consistency-based diagnosis for firewall rule sets 415
S. Pozo, R. Ceballos, R.M. Gasca, and A.J. Varela-Vaca

El diseño del proceso contractual en la contratación a través de dispositivos móviles 425
A. Paniza y M. Payeras

Ataque a la seguridad de un protocolo utilizando *Strand Spaces* 433
M. Mut Puigserver, M.M. Payeras Capellà, J.Ll. Ferrer Gomila y Ll. Huguet Rotger

Análisis de vulnerabilidad de un parámetro frente a ataques LDAP Injection & Blind LDAP Injection 441
J.M. Alonso, A. Guzmán, R. Bordón y M. Beltrán

Estableciendo el nivel de gestión de la seguridad utilizando un modelo basado en esquemas predefinidos 449
L.E. Sánchez, D. Villafranca, A. Santos-Olmo, E. Fernández-Medina y M. Piattini

Usando la técnica MPR para la certificación de claves en MANETs 461
C. Hernández Goya, P. Caballero Gil y O. Delgado Mohatar

Despliegue de mecanismos de autorización para servicios federados en eduroam 471
M. Sánchez, O. Cánovas, G. López y A.F. Gómez-Skarmeta

Mejora del *clustering* de ataques realizado en una red distribuida de sistemas trampa 483
M. Fernández, R. Uribetxeberria, U. Zurutuza e I. Vélez de Mendizabal

Caracterización estadística de archivos de texto cifrados con AES para fines del cómputo forense 493
M. Donado, J. Lopez y J. Cano

Historial clínico distribuido y seguro para situaciones de emergencias 503
A. Martín-Campillo, S. Robles, R. Martí y C. Garrigues

IMPRESS, desarrollo de aplicaciones seguras basado en MDA 513
D. Serrano y A. Maña

Protocolos para la verificación de la proximidad en RFID 523
J. Munilla y A. Peinado

Hacia un sistema preventivo del exceso de velocidad 533
J.M. de Fuentes, A.I. González-Tablas y A. Ribagorda

Análisis de seguridad de un sistema de archivos distribuido 543
J. Vera del Campo, J. Hernández Serrano y J. Pegueroles

Prevención de ataques de desincronización en esquemas de watermarking de audio 551
X. Domènech, J. Herrera-Joancomartí y D. Megías

Propuesta GKM *cross-layer* distribuida para redes inalámbricas de sensores 557
J. Hernández Serrano, J. Pegueroles, J. Vera del Campo y M. Soriano

Postprocesado para microagregación multivariante: un estudio con datos reales 569
G. Pujol, A. Solanas, A. Martínez-Ballesté y J.M. Mateo-Sanz

Modelo para la formalización abstracta e intuitiva de las propiedades de seguridad 577
A. Maña y G. Pujol

Diseño de patrón de selección de métricas para la construcción de CMI de la seguridad 585
D. Villafranca, L.E. Sánchez, E. Fernández-Medina y M. Piattini

Repudio de firmas electrónicas en infraestructuras de clave pública 595
J.L. Hernández-Ardieta, A.I. González-Tablas y B. Ramos

Un marco inteligente para el análisis de tráfico generado por gusanos en Internet 607
U. Zurutuza, R. Uribeetxeberria, M. Fernández, I. Vélez de Mendizabal y D. Zamboni

Resolución de consultas anónimas sobre DNS 619
J. García-Alfaro y S. Castillo-Pérez

Gestión de recursos de un navegador Web para prevenir ataques contra la privacidad en Tor 629
G. Navarro-Arribas, J. Garcia-Alfaro, O. Mula-Valls y J. Herrera-Joancomartí

Análisis de seguridad y privacidad para sistemas EPC-RFID en el sector postal 639
J. Melià-Seguí, J. Herrera-Joancomartí y J. García-Alfaro

Construcción de redes sociales anónimas 647
A. Silva, L.J. García-Villalba y C. Díaz

CHARLAS INVITADAS

El Documento Nacional de Identidad Electrónico: DNIe 655
Dirección General de la Policía y de la Guardia Civil

Integración de metodologías de evaluación para la seguridad TIC 665
Centro Criptológico Nacional

Estableciendo el nivel de gestión de la seguridad utilizando un modelo basado en esquemas predefinidos

L.E. Sánchez[1], D. Villafranca[1], A. Santos-Olmo[1], E. Fernández-Medina[2] y M. Piattini[2]

***Resumen*—Para garantizar la subsistencia de las empresas y la evolución de sus modelos empresariales, éstas deben poder garantizar la seguridad de sus sistemas de información, pero esto requiere que las empresas conozcan en todo momento el nivel de madurez de su seguridad y hasta qué punto esta debe evolucionar para ser adecuada. Actualmente las empresas requieren de auditorias periódicas para tener este conocimiento, lo que hace que muchas veces las medidas de seguridad se implanten tarde y tengan un coste que la empresa no pueda asumir. En este artículo mostramos los puntos principales del nuestra propuesta de modelo de madurez para la gestión de la seguridad en las PYMES, centrándonos en la fase que determina el estado de la compañía y en algunos de los mecanismos que permiten mantener actualizado el nivel de seguridad sin tener que realizar auditorias continuas. Este enfoque se está refinando de forma continua mediante su aplicación en casos reales, cuyos resultados mostramos en el artículo.**

***Palabras clave*—SGSI, modelo de madurez, gestión de la seguridad, análisis de riesgos.**

I. Introducción

DISPONER de un sistema de gestión de la información, es fundamental para la estabilidad de las compañías [1], y supone el principal factor diferenciador en la evolución de una compañía. Estos activos están sometidos a riesgos de una gran variedad, que pueden afectar de una forma crítica a las empresas, pero el principal riesgo al que se enfrenta la empresa es la incapacidad de gestionarlos. Existen multitud de fuentes que arrojan cifras que muestran la magnitud de los problemas ocasionados por la falta de unas medidas de seguridad adecuadas [2-7].

En este articulo seguimos profundizando en nuestra propuesta de modelo de madurez y gestión de la seguridad orientado a las PYMES [8-13] que pretende solucionar los problemas detectados en los modelos clásicos, los 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 han sido analizados en anteriores artículos [14, 15]. En anteriores trabajos hemos presentado la situación actual de sistemas de gestión de la seguridad para los sistemas de información [14, 15], distintas versiones de nuestro modelo de madurez a medida que este ha ido evolucionando, así como de la herramienta que se ha desarrollado para darle soporte automatizado [16] y las métricas que ayudan a mejorar su eficacia y reducir sus costes [17, 18]. En este artículo hemos profundizado más en la fase del modelo encargada de establecer la situación actual de la compañía, analizando los resultados obtenidos sobre 11 casos de estudio reales al aplicarles esta fase de nuestro modelo. También mostramos las diferencias que aparecen en estos modelos al actualizar su esquema que tomaba como base la ISO17799:2000 [19] a un nuevo esquema que toma como base la ISO27001 (anterior ISO27001) [20, 21]. Por último mostramos el funcionamiento de uno de los procedimientos principales del sistema que permite evolucionar el nivel del sistema de seguridad obtenido inicialmente, alterando los datos del cuadro de mando de forma instantánea, permitiendo a la dirección de la compañía ser consciente de la situación actual y tomar decisiones en tiempos razonables.

El artículo continúa en la Sección 2, describiendo muy brevemente los modelos de madurez existentes, su tendencia actual y algunas de las nuevas propuestas que están surgiendo. En la Sección 3 se introduce de forma muy breve nuestra propuesta de modelo de madurez orientado hacia las PYMES centrándonos en los resultados obtenidos hasta el momento en la fase que permite establecer la situación actual de la compañía con respecto a su nivel de gestión de seguridad y en el funcionamiento del *Procedimiento de Denuncia* que permite ajustar de forma dinámica el nivel de cumplimiento de los controles que forman parte del sistema. Finalmente, en la Sección 4 mostramos nuestras conclusiones e indicamos cuál será el trabajo que desarrollaremos en el futuro.

II. Trabajo relacionado

Existen ocho errores clásicos que se producen en la mayoría de las empresas, a la hora de gestionar su seguridad: i) *Inexistencia de un análisis previo de riesgos* para evaluar

Esta investigación es parte del proyecto MISTICO, parcialmente financiado por el FEDER y por la Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha y el proyecto SCMM-PYME financiado por el PROFIT y concedido por Ministerio de Industria, Turismo y Comercio.

[1]Departamento de I+D, SICAMAN Nuevas Tecnologías, 13.700 Tomelloso. {Lesanchez, Dvillafranca, Asolmo}@sicaman-nt.com.

[2]Grupo de Investigación Alarcos, Departamento de Tecnologías y Sistemas de Información, Universidad Castilla-La Mancha, 13.071 Ciudad Real. {Eduardo.FdezMedina, Mario.Piattini}@uclm.es.

las posibles amenazas que, aprovechando una vulnerabilidad en los activos de la organización, ocasionen un impacto económico en la misma; ii) *Asignar una cantidad insuficiente de personal* para la definición, desarrollo y mantenimiento de la seguridad; iii) *Falta de entendimiento de la estrecha relación entre la seguridad de la información y el crecimiento del negocio*: las organizaciones suelen entender la necesidad de una adecuada seguridad física pero son incapaces de ver las consecuencias de una pobre seguridad de la información, cuando cada vez más dependen en mayor medida de sus activos lógicos; iv) *Incapacidad para gestionar los aspectos operativos de la seguridad*. En muchos casos, se procede a la implantación de medidas correctoras y/o preventivas pero no se establecen mecanismos de control y actualización de dichas medidas; v) *Centrar la responsabilidad de la seguridad de la información únicamente en mecanismos tecnológicos de seguridad*: muchas organizaciones creen que por el solo hecho de tener instalado un firewall están protegiendo su negocio contra cualquier tipo de ataque, ignorando por ejemplo la posibilidad de una sanción legal por cesión indebida de datos personales; vi) *Incapacidad para darse cuenta de la influencia del valor de su información y su reputación en el aspecto económico del negocio*; vii) *Respuestas reactivas y correctivas a los problemas de seguridad e implantación de soluciones a corto plazo*. No se adopta una estrategia pro-activa que prevenga los incidentes de seguridad ni se minimizan los riesgos, sólo se buscan soluciones rápidas según se detectan; viii) *Pretender que los riesgos desaparecerán si son ignorados* (la gestión de la seguridad es un aspecto de baja prioridad para la organización). Esta visión miope es muy habitual en aquellos sectores donde la seguridad no se percibe como un componente crítico para el negocio.

Todos estos problemas se resumen en una falta de concienciación en materia de gestión de la seguridad, por una falsa sensación de seguridad en la dirección de la empresa, al carecer esta de herramientas que permitan ejercer una adecuada gestión y medición del SGSI (Sistema de Gestión de Seguridad de la Información) de la compañía. El mercado demanda actualmente a las empresas que sean capaces de garantizar que las tecnologías para los activos informáticos y de información sean seguras, rápidas y de fácil interacción [22].

Los Modelos de Madurez de Seguridad [23-28] buscan establecer una valoración estandarizada, con la que se pueda determinar el estado de la seguridad de la información en una organización, y que nos permita poder planificar el camino que se tiene que recorrer para alcanzar las metas de seguridad deseadas.

Entre los modelos de madurez para seguridad de la información [29] que más se están aplicando en las empresas actualmente, destacan el SSE-CMM (Modelo de Capacidad y Madurez en la Ingeniería de Seguridad de Sistemas), COBIT [24] y el ISM3 [30], y aunque se han realizado investigaciones para desarrollar nuevo modelos [27, 28, 31], ninguna de ellas ha conseguido solucionar los problemas actuales que se producen a la hora de aplicar estos modelos en PYMES.

Otras propuestas toman como punto central del SGSI el análisis de riesgos. La mayoría de los modelos actuales basados en riesgos utilizan como metodología de análisis de riesgos Magerit v2 [32], el problema de esta metodología es que siendo la más completa y eficiente del mercado, no es útil para las PYMES ya que requiere de mucho esfuerzo y recursos por parte de la compañía.

Frente a estos modelos que toman el Análisis de riesgos como el núcleo central del SGSI, en nuestro caso, aunque es muy importante no deja de ser una pieza más del sistema. Siegel [33] señala que los modelos de seguridad informática que se centran exclusivamente en modelos de eliminación de riesgos no son suficientes y por otro lado Garigue [34] remarca qué actualmente los gerentes no desean saber solo que se ha realizado para mitigar los riesgos, también se debe poder dar a conocerlo eficazmente que se ha realizado esta tarea y si se ha conseguido ahorrar dinero.

El problema principal de la mayoría de los modelos de madurez mencionados es que no están teniendo éxito a la hora de implantarse en PYMES, debido principalmente a que fueron desarrollados pensando en organizaciones grandes y en las estructuras organizativas asociadas a estas, sus estructuras son rígidas, complejas y costosas de implementar, lo que las hace inadecuadas para el entorno de una PYME.

La visión de cómo afrontar estos niveles de madurez, difiere según los autores que se tomen como referencia. De esta forma algunos autores, insisten en utilizar la norma internacional ISO/IEC17799 en modelos de gestión de seguridad, pero siempre haciéndolo de manera incremental, considerando las necesidades particulares de seguridad [26, 27, 30, 35].

La propuesta que nosotros hemos desarrollado también esta basada en la norma internacional ISO/IEC17799 pero se ha orientado su aplicación hacia las PYMES, evitando los problemas detectados en los modelos actuales, los cuales requieren de más recursos de los que la compañía puede aportar.

III. Modelo de Madurez Basado en Esquemas Predeterminados

En artículos anteriores [8-13] se han presentado versiones previas del modelo, por lo que aquí se presenta de forma detalla la fase encargada de establecer y cuantificar la situación actual de la compañía, aportando mejoras obtenidas por la aplicación práctica del mismo a casos reales que consisten en la definición de esquemas predefinidos que posibilitan el desarrollo del plan director de seguridad en un periodo de tiempo muy reducido y con pocos recursos. Mostramos también los resultados obtenidos de su aplicación en 11 casos reales, aunque por motivos de confidencialidad y debido a que dichos resultados muestran puntos débiles en sus sistemas de gestión seguridad, se ha mantenido en el anonimato el nombre de algunos de ellos.

El Modelo de Madurez para la Seguridad de la Información que proponemos permite a cualquier organización evaluar el estado de su seguridad, pero está orientado principalmente a

las PYMES desarrollando modelos de gestión de seguridad sencillos, económicos, rápidos, automatizados y progresivos y sostenibles que son los principales requerimientos que tienen este tipo de compañías a la hora de implantar estos modelos.

Uno de los objetivos perseguidos en todo el proceso que hemos desarrollado es obtener el mayor nivel de automatización posible con una información mínima, recogida en un tiempo muy reducido. En nuestro sistema hemos priorizado la velocidad y el ahorro de costes, sacrificando para ello la precisión que ofrecen otros modelos, es decir, nuestro modelo buscará una de las mejores configuraciones de seguridad pero no la óptima y siempre priorizando los tiempos y el ahorro de costes.

Otra de las principales aportaciones que presenta el modelo que hemos desarrollado es un conjunto de matrices que permite relacionar los diferentes componentes del SGSI y que el sistema utiliza 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, aunque debido a la limitada extensión del articulo, no podremos analizar los resultados de estas matrices.

El modelo de gestión de seguridad está formado por tres fases y los resultados de cada una de las fases anteriores son necesarios para la fase siguiente. En este artículo nos centraremos en realizar un análisis detallado de la Fase I, así como de uno de los procedimientos que sirve de retroalimentación a los resultados obtenidos en esta fase, denominado "*Procedimiento de Denuncia*", analizando los resultados obtenidos de la aplicación del modelo a casos reales de estudio.

A. Fase I: Establecimiento del nivel de madurez

El principal objetivo de esta fase como puede verse en la Fig. 1, es conocer el nivel de seguridad actual y deseable para la compañía, mediante dos subfases que pueden realizarse de forma paralela. Además, se conseguirá información vital para las Fase II y III. Esta fase se compone de dos subfases, que pueden definirse de forma separada, pero cuyos resultados se complementan. En la primera subfase podremos determinar hasta dónde es aconsejable que llegue la compañía, mientras que en la segunda subfase determinaremos cual es el punto actual en que se encuentra el nivel de gestión de la seguridad de la compañía. Para la primera hemos tomados como base información del INE (Instituto Nacional de Estadística) relativa al estado actual de las PYMES Españolas con respecto a indicadores tecnológicos y empresariales, mientras que la base de la segunda es la normativa ISO27001.

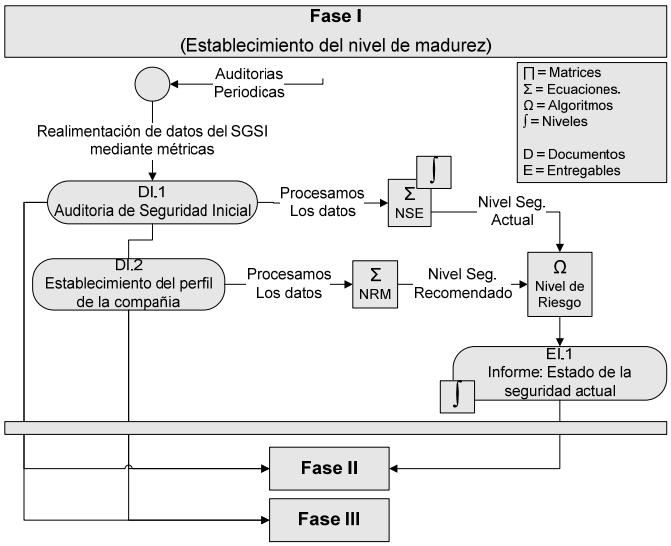

Fig. 1. Esquema de la Fase I del Modelo en Espiral.

El modelo que hemos desarrollado, se esta validando mediante su aplicación en 11 casos reales (compañías del Grupo Sicaman y clientes de la misma), cuyos datos principales podemos ver en la Tabla I.

TABLA I
DATOS DE LOS CLIENTES QUE HAN SERVIDOR DE CASOS DE PRUEBA.

Nombre	Localización	Sector
SNT	Ciudad Real	Actividades informáticas
Cliente2	Madrid	Investigación y desarrollo
Cliente3	Madrid	Investigación y desarrollo
Cliente4	Argamasilla de Alba	Industria de productos alimenticios y bebidas
Cliente5	Tomelloso	Fabricación de productos metálicos, excepto maquinaría y equipo
Cliente6	Madrid	Otras actividades empresariales
IMP	Madrid	Otras actividades empresariales
ComerciaRed	Ciudad Real	Construcción
Pronatec	Tomelloso	Actividades inmobiliarias
Cliente10	Madrid	Actividades informáticas
Cliente11	Madrid	Fabricación de material electrónico.

A continuación, se describe los principales detalles y la aplicación en casos reales de las dos subfases que componen la fase de establecimiento del nivel de madurez.

1) Auditoria de seguridad inicial:

Esta subfase dentro de la Fase I consiste en realizar un detallado check-list que nos ayude a posicionar el estado actual de la compañía con respecto a su nivel de seguridad.

Inicialmente el estudio se empezó a realizar sobre la ISO17799:2000 [19], habiéndose realizado posteriormente una actualización del esquema y de todos los datos a la ISO27001 [20], lo que permite comparar la variaciones que sufre el modelo en ambos al evolucionar desde la versión 2000 de la norma a la 2005.

En la Tabla II, se puede ver la diferencia obtenida en los resultados del checklist según el esquema aplicado. En el primer caso se ha aplicado un checklist obtenido a partir de la ISO17799:2000 sobre 735 subcontroles, y el segundo de los casos se ha tomando como base la ISO27001 sobre 896 subcontroles. Entre los resultados obtenidos, es interesante destacar que en general los resultados obtenidos sufren pequeñas variaciones (entre 1-2%) aunque existen clientes con desfases mayores (5-10%) al estar afectados de forma directa por algunos de los cambios. Aún así, ateniéndonos a la media la desviación obtenida es de un 2% aproximadamente.

TABLA II
NIVEL DE SEGURIDAD ACTUAL DE LOS CASOS DE PRUEBA OBTENIDOS A PARTIR DEL CHECKLIST DE LA ISO17799:2000 Y LA ISO27001.

		ISO17799	
SGSI	**Nombre**	**2000**	**2005**
SGSI-01	SGSI Sicaman 2007	59	59
SGSI-02	SGSI Cliente2 2006	28	37
SGSI-03	SGSI Cliente3 2007	67	62
SGSI-04	SGSI Cliente4 2007	18	23
SGSI-05	SGSI Cliente5 2007	19	24
SGSI-06	SGSI Cliente6 2007	50	51
SGSI-07	SGSI IMP 2007	33	38
SGSI-08	SGSI ComerciaRed 2007	40	41
SGSI-09	SGSI Pronatec 2007	34	38
SGSI-10	SGSI Cliente10 2007	14	14
SGSI-11	SGSI Cliente11 2007	22	23
	TOTAL:	**35**	**37**

En nuestra versión actual del modelo, el nivel de los subcontroles, solo se utiliza para obtener un valor lo más aproximado posible del nivel de seguridad actual por control. Una vez obtenido estos valores, las métricas obvian este nivel y actualizan de forma automática el nivel de seguridad, partiendo de los valores obtenidos en esta fase. Las auditorias periódicas que se realicen sobre el sistema de gestión de seguridad de la compañía, recalcularán el checklist utilizando nuevamente el nivel más bajo que son los subcontroles.

Estas auditorias funcionarán como un sistema de reajuste del cuadro de mandos para actualizar los niveles de seguridad, como si se tratara de un reloj que deseamos poner en hora. El desfase producido para cada control entre dos auditorias nos servirá para ir ajustando el modelo y hacerlo más eficiente, requiriendo cada vez menos esfuerzo y dedicación de auditores externos.

En la Tabla III podemos ver los resultados obtenidos por dominio sobre la norma ISO17799:2000. Se puede ver como algunas compañías han obviado totalmente aspectos como la Continuidad del Negocio, considerándolo superfluo para su compañía.

TABLA III
RESULTADOS OBTENIDOS PARA LOS CASOS DE PRUEBAS A PARTIR DEL CHECKLIST DE LA ISO17799:2000.

Dominio	**Cli2**	**SNT**	**Cli3**	**Cli4**	**Cli5**	**Cli6**	**IMP**	**CMR**	**PRO**	**Cli10**	**Cli11**
3	50	88	88	25	25	50	13	63	25	13	0
4	16	59	75	9	14	43	32	43	32	6	31
5	22	31	51	0	0	17	8	13	8	0	28
6	25	89	87	7	7	34	33	33	34	8	17
7	43	60	45	26	29	62	57	57	61	47	64
8	30	63	72	26	26	68	51	51	50	20	21
9	44	63	65	25	24	76	54	54	54	19	20
10	29	56	63	18	18	45	35	35	35	12	12
11	2	32	68	5	4	50	5	5	5	0	1
12	15	52	56	40	39	61	44	44	38	18	29
	28	**59**	**67**	**18**	**19**	**50**	**33**	**40**	**34**	**14**	**22**

En la Fig.2 podemos ver el resultado medio por dominio de los 11 casos analizados en la tabla anterior. Es destacable ver como ninguno de los dominios supera el 50% de cumplimiento y existen dos casos “Clasificación de Activos” y “Continuidad del Negocio” en que las compañías suspenden de forma clara.

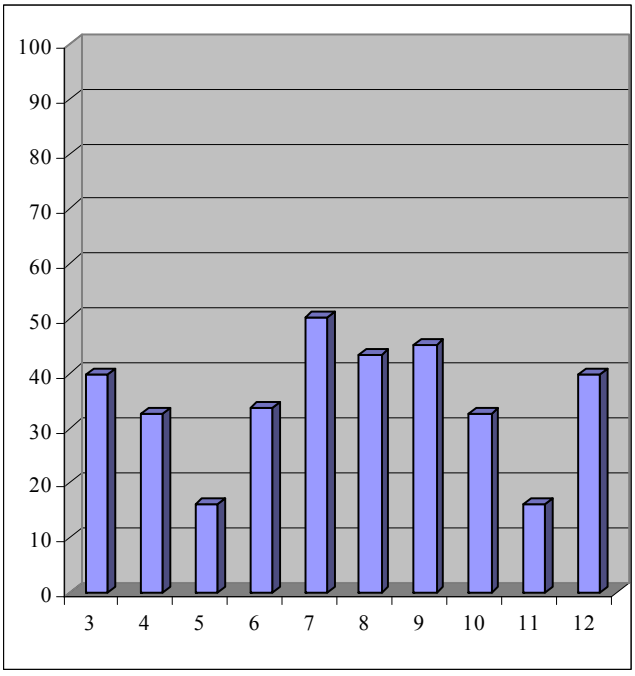

Fig. 2. Nivel de cumplimiento medio de los dominios de la ISO17799:2000

TABLA IV
RESULTADOS OBTENIDOS PARA LOS CASOS DE PRUEBAS A PARTIR DEL CHECKLIST DE LA ISO27001.

Dominio	Cli2	SNT	Cli3	Cli4	Cli5	Cli6	IMP	CMR	PRO	Cli10	Cli11
5	30	55	55	25	25	30	14	39	14	0	0
6	49	64	55	23	28	41	40	48	40	3	23
7	52	57	68	28	28	48	43	46	43	18	45
8	48	77	64	11	11	38	42	40	43	5	15
9	47	61	48	30	33	66	59	58	61	48	68
10	46	46	49	28	29	56	42	44	42	18	20
11	51	68	71	28	29	86	65	65	68	25	26
12	41	66	74	21	21	49	42	42	39	11	11
13	29	64	68	14	14	36	21	21	22	2	15
14	2	32	68	5	4	50	5	5	5	0	1
15	16	54	58	41	41	63	46	47	39	20	32
	37	**59**	**62**	**23**	**24**	**51**	**38**	**41**	**38**	**14**	**23**

En la Tabla IV podemos ver los resultados obtenidos por dominio sobre la norma ISO17799:2000. Como podemos ver casi todas las compañías han considerado la "Continuidad del Negocio" como un punto superfluo en su modelo de negocio, lo que demuestra que la raíz del problema es cultural y no puntual en algunas compañías.

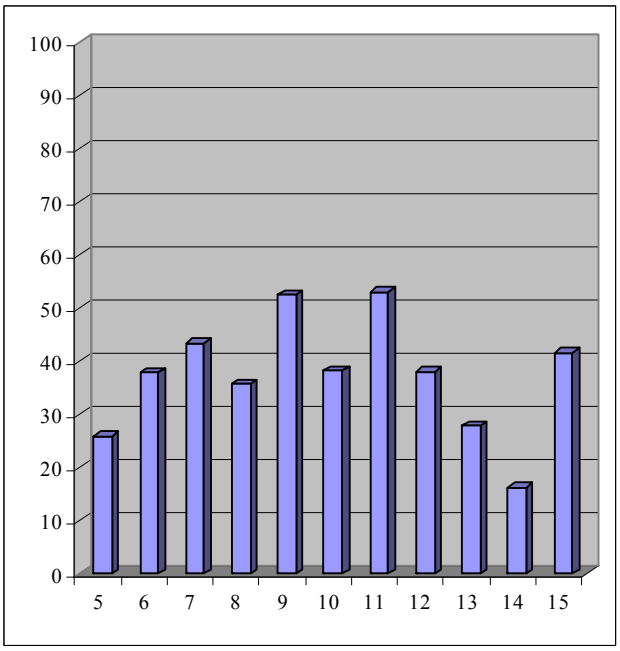

Fig. 3. Nivel de cumplimiento medio de los dominios de la ISO27001

En la Fig. 3 podemos ver que aunque la "Continuidad del Negocio" sigue siendo una de las asignaturas pendientes, la "Clasificación de Activos" sufre una mejora al medirlo con la nueva normativa, ya que algunos controles se han movido a otros dominios y se han tenido en cuenta factores que antes no se evaluaban. En general el análisis de los resultados obtenidos con la ISO27001 se han mostrado mucho más precios que los de la ISO17799:2000. Por último algunas de las distorsiones que se producen entre los resultados de los modelos se deben a que la ISO27001 tenía en cuenta factores actualizados que la ISO17799:2000 estaba obviando.

Por último y a modo de resumen, en la Fig. 4, podemos ver una comparativa del nivel de seguridad global para cada caso de prueba, aplicando la ISO17799:2000 frente a la ISO27001.

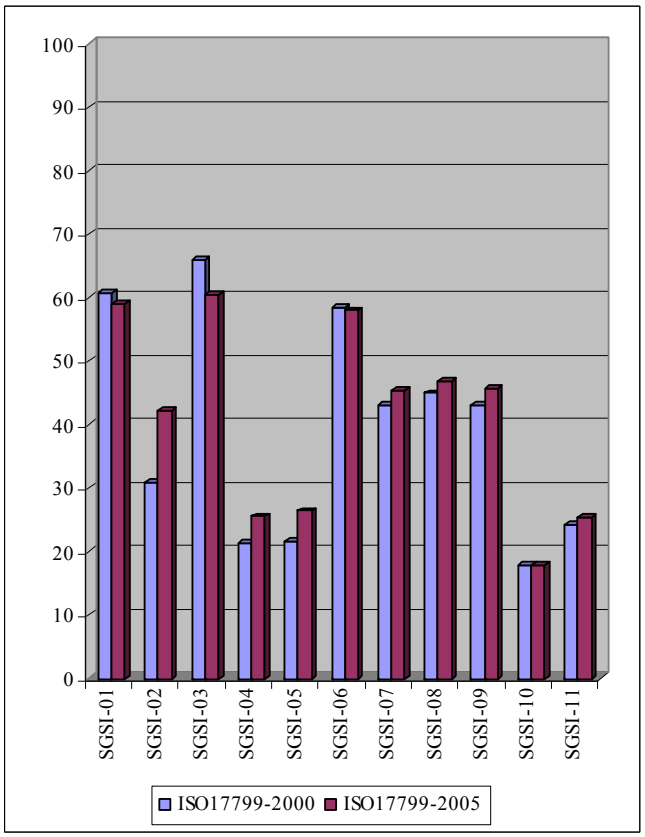

Fig. 4. Comparativa de los niveles de cumplimiento de 11 casos reales entre la ISO27001 y la ISO27001

2) Establecimiento del perfil de la compañía

El modelo que nosotros proponemos utiliza un conjunto de características intrínsecas a la compañía para definir el nivel de madurez máximo al que la compañía debe evolucionar en la situación actual.

La solución planteada para esta subfase, es sencilla, ya que en todo momento se ha buscado que el modelo sea ágil, barato y rápido. No obstante, este modelo, aunque es sencillo, nuestra experiencia nos ha demostrado que es efectivo, y nos proporciona un resultado muy acertado. En la versión actual solo hemos considerado como parámetros un conjunto reducido de las características que hemos considerado más destacables en las compañías como se puede ver en la Tabla V: i) Número de empleados, ii) Facturación anual, iii) Departamento de I+D, iv) Número de empleados que utilizan el Sistema de Información, v) Número de personas asociadas directamente al Departamento de Sistemas, vi) Nivel de dependencia de la compañía del outsourcing del S.I.

TABLA V
REGLAS PARA DETERMINAR EL NIVEL DE MADUREZ DE LA PYME.

Nº Factor	Descripción	Regla	Valoración
1	Número de empleados.	0 - 25 Empleados	0
		25 - 250 Empleados	1
		> 250 Empleados	2
2	Facturación anual.	0 - 1 Millones €	0
		1 - 100 Millones €	1
		> 100 Millones €	2
3	Departamento I+D: Alta, Bajo, Medio, Nulo.	Nulo	0
		Bajo	1
		Medio	2
		Alta	3
4	Número de empleados que utilizan el Sistema de Información.	0 - 10% total empleados	0
		10% - 40% total empleados	1
		>50% total empleados	2
5	Número de personas asociadas directamente al Departamento de Sistemas.	0 empleados	0
		1 - 5 empleados	1
		> 5 empleados	2
6	Nivel de dependencia de la compañía del outsourcing del S.I	Nulo	0
		Bajo	1
		Medio	2
		Alta	3

Cada uno de estos parámetros se traduce en un valor y la suma normalizada de estos valores determina el nivel de madurez máximo que el sistema considera apropiado para la compañía.

A su vez el sector de la compañía determina una matriz de pesos para cada uno de estos factores.

El control del peso en los factores es fundamental para evitar que las casuísticas de ciertos sectores determine un nivel de seguridad superior al que realmente puede soportar la infraestructura de la compañía. En condiciones normales el peso será de 0.50, si queremos restar peso a un valor lo reduciremos a 0.25 y si queremos eliminarlo lo pondremos a 0. En caso de que queremos darle mayor importancia lo subiremos a 0.75 y si es fundamental a 1. Por ejemplo en el caso de una compañía de Energías el valor de su Departamento de I+D es fundamental para su evolución, por lo que el peso de este factor debe ser el máximo, mientras que en una empresa perteneciente al sector de la Construcción el peso del factor de I+D es mucho menor, mientras que el de Outsourcing suele tener mayor relevancia.

En (1) mostramos la ecuación que permite calcular NMD (Nivel de Madurez Deseable) de la compañía, este nivel puede cambiar, según cambia el perfil de la misma:

$$NMD = \Sigma(PesoFactor*(ValoraciónFactor/ValorMaximoFactor))/NumFactores \quad (1)$$

Según la expresión de (1) y la experiencia práctica obtenida del estudio sobre clientes del Grupo Sicaman, hemos considerado 3 niveles de madurez que podemos ver en la Fig. 5:

- Nivel1 si el resultado esta entre 0–0.25
- Nivel2 si esta entre 0.25–0.75
- Nivel3 si esta entre 0.75–1

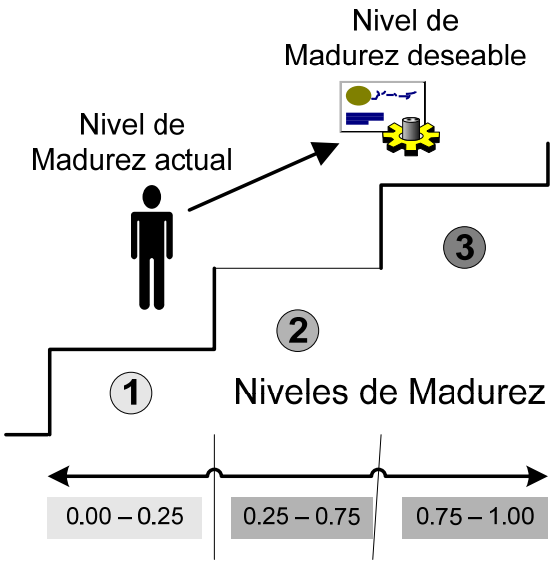

Fig. 5. Fase I – Niveles de Madurez.

Los parámetros que se han tomado en consideración inicialmente han sido obtenidos del análisis de miles de datos estadísticos de carácter económico y tecnológico procedentes del INE (Instituto Nacional de Estadística Español) y representan un pequeño conjunto inicial.

Para la elección y refinado de los datos estadísticos se han tenido especial consideración con los siguientes factores:

- Datos Económicos del tejido empresarial.
- Datos Tecnológicos del tejido empresarial.
- Informes estadísticos que tuvieran segregación de los factores anteriores por CNAE.
- Informes estadísticos que tuvieran segregación de los factores anteriores por número de empleados.

En la Tabla III, se pueden ver los resultados obtenidos en los casos de estudio, para establecer el nivel actual de madurez de la seguridad de la compañía (NMD), que al aplicar la ecuación (1) y los rangos mostrados en la Fig. 2, nos permite obtener los valores del Nivel de Madurez Deseable (NMD) para la compañía. Las columnas del nivel de madurez actual para la versión de la ISO17799:2000 e ISO27001 se obtiene de la primera parte de la Fase I (Auditoria de Seguridad Inicial). Por último en la tabla se puede ver el desfase que se produce entre los niveles de madurez actual y deseable.

TABLA VI
NIVELES DE MADUREZ ACTUALES Y DESEADOS DE LOS CASOS DE PRUEBA.

		Nivel Madurez				
SGSI	**NMD**	**Actual-2000**	**Actual-2005**	**Deseable**	**Desfase 2000**	**Desfase 2005**
SNT	0.67	2	2	2	0	0
Cli2	0.78	2	2	3	1	1
Cli3	0.78	2	2	3	1	1
Cli4	0.47	**1**	**2**	2	1	0
Cli5	0.47	**1**	**2**	2	1	0
Cli6	0.75	2	2	3	1	1
IMP	0.28	2	2	2	0	0
CMR	0.50	2	2	2	0	0
PRO	0.25	2	2	3	1	1
Cli10	0.56	1	1	2	1	1
Cli11	0.50	**1**	**2**	2	1	0

En el caso de que el resultado de aplicar la ecuación (1), devuelva un valor que coincida entre el limite de dos niveles, siempre tenderemos a normalizar dicho valor, al nivel superior de madurez.

En la Tabla VI podemos ver, como valores que estaban cerca del límite entre dos niveles, han pasado al nivel superior al cambiar la versión del Esquema desde la ISO17799:2000 a la ISO27001.

Aún cuando esta formula nos da una indicación del nivel actual, esto no quiere decir que la seguridad sea correcta, por ejemplo en el caso de SNT el nivel de seguridad actual coincide con el deseable, pero puede que el reparto de la carga de los dominios no sea el adecuado y por tanto requerimos del plan que se generara en otras fases. Esta previsto un avance del prototipo para solucionar este problema, refinando los resultados obtenidos.

Es interesante comprobar como actualmente ninguna de las compañías tiene más de 1 nivel de desfase e incluso varias están en el nivel correcto de seguridad, aunque como hemos comentando anteriormente, esto no significa que la seguridad este siendo aplicada de forma adecuada. La razón de esto es que estas compañías en mayor o menor medida han aplicado ya algunos procesos de seguridad, aunque de forma limitada, ya que también se puede comprobar que no existe sobre-dimensionamiento del nivel en ninguno de los casos estudiados, aunque si puede existir en dominios particulares.

Posteriores versiones del modelo pretenden crear una nueva matriz que asocie características extraídas de estos informes con los controles de la normativa ISO27001, de tal forma que conociendo el sector al que pertenece la compañía y el número de empleados, seamos capaces de establecer el nivel deseable y actual de la compañía no solo a nivel global como realizamos actualmente, sino directamente a nivel de controles.

B. Fase II: Análisis de riesgos.

Una vez que hemos realizado la primera fase para posicionar a la empresa en un Nivel de Madurez y decidir hasta dónde debe llegar en la implantación del SGSI, debemos proceder a realizar un análisis de riesgos de los activos de la misma.

El modelo de Análisis de Riesgos que hemos desarrollado, esta basado en los modelos propuestos por Stephenson [36] que se centran en la sinergia entre la prueba técnica y el análisis de riesgos tomando como referencia la ISO27001 y en la metodología de análisis de riesgos Magerit v2 [32].

Para nuestro modelo hemos buscando en todo momento simplificar otras propuestas anteriores para adecuarlos a la dimensión y recursos [37, 38] de los que pueden disponer las PYMES. Las principales bases sobre las que se define nuestra metodología son: Flexibilidad, Simplicidad y Eficiencia en costes (humanos y temporales).

Dentro del análisis de riesgos que hemos desarrollado uno de los aspectos más importantes son las Matrices de asociación que permiten minimizar el coste del análisis de riesgo y producir el máximo resultado e información para la compañía con el menor esfuerzo. Se ha realizado una serie de matrices que permiten asociar los diferentes componentes del análisis de riesgo (activos-amenazas-vulnerabilidades) y a su vez estos con los resultados producidos en la fase I (controles). Estas matrices son de gran importancia ya que ayudan a simplificar el análisis de riesgos y ayudan a obtener una valoración del nivel de cobertura de un activo con respecto a los controles de la ISO27001.

C. Fase III: Generación del SGSI.

En esta Fase se ha buscado que el SGSI sea manejable, enfocado en los dominios de la norma de mayor interés para la organización y con un número de métricas reducido, obteniendo rápidos resultados y realimentando el proceso en cada ciclo, hasta obtener el nivel de madurez marcado inicialmente.

En las fases anteriores hemos obtenido el perfil de la compañía, su nivel actual de madurez, su nivel máximo recomendable de madurez, el estado de sus controles, sus activos, los riesgos asociados a ello y el plan de mejora. Con toda esta información el sistema está en situación de preparar de forma automática un plan de gestión del sistema de información para la compañía.

Este conjunto de matrices que junto con las mostradas en la Fase I y II son una de las principales aportaciones de nuestro modelo, son las que utilizará internamente el sistema para la compañía.

Dentro de esta fase de generación del SGSI uno de los aspectos más importantes son las Matrices de asociación que permiten asociar todos los objetos de estas librerías. Estas matrices las utiliza internamente el sistema para recomendar un plan inicial de SGSI para la PYME en función de la información obtenida en las fases anteriores.

Las matrices asociadas a las ISO27001 son de vital importancia en el diseño de nuestro sistema, ya que son las que utiliza el algoritmo para la selección de los documentos y procedimientos que se considerarán de vital importancia tanto para el diseño del SGSI como para su posterior seguimiento.

El resultado final de esta fase será un conjunto de

reglamentos y procedimientos que deberán cumplirse para mejorar el nivel de seguridad de la compañía, los cuales tendrán asignados un código de colores para indicar de una forma visual y rápida al usuario donde deben aplicar un mayor esfuerzo. El SGSI será dinámico, adaptándose a los cambios en los niveles de cobertura de los controles y en los niveles de seguridad según evolucione el sistema. La evolución del sistema se medirá mediante un conjunto de métricas definidas sobre el conjunto de objetos del SGSI.

D. Procedimientos: Procedimiento de denuncia.

En este sub-apartado, se muestra de forma muy resumida el proceso general de trabajo con el SGSI de nuestro modelo, centrándonos en el Procedimiento de Denuncia que nos permite mantener actualizado nuestro scoreboard.

Una vez que hemos generado el SGSI comienza el verdadero trabajo de la compañía. Hasta el momento y gracias al uso de esquemas, el consultor ha sido capaz de definir el sistema de gestión adecuado para la compañía con unos costes asequibles. Ahora la compañía debe comenzar a trabajar con el sistema.

Nuestro modelo de SGSI se ha diseñado para que evolucione de forma dinámica sin que sea obligatoria, aunque si aconsejable la intervención de auditores externos. De esta forma nuestro modelo no tiene que esperar a la llegada de auditores externos para conocer como evoluciona el sistema, sino que el sistema evoluciona constantemente cambiando el nivel de seguridad de los controles y reajustando todas las fases del sistema.

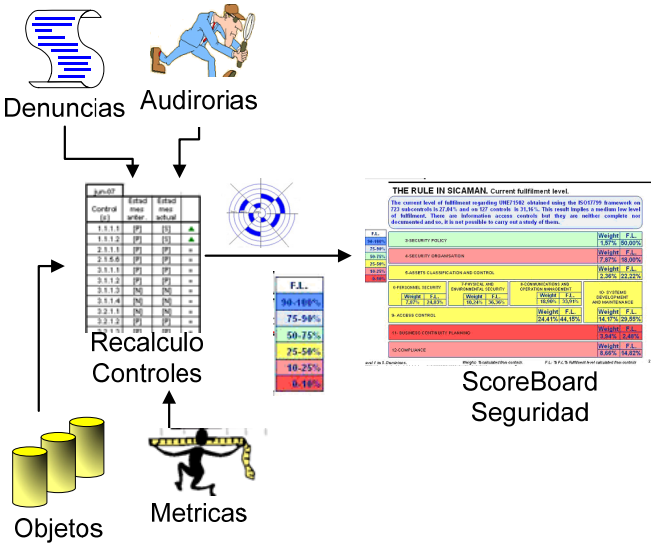

Fig. 6. Factores de actualización del SGSI.

La versión actual de la aplicación, evoluciona teniendo en cuenta cuatro aspectos que podemos ver en la Fig. 6: i) la periodicidad de los objetos, ii) las denuncias, iii) el conjunto de métricas y iv) las auditorias externas. En base a estos factores el sistema recalcula los controles y adapta el cuadro de mandos de seguridad de la compañía.

El trabajo con el sistema de gestión de seguridad propuesto se ha desarrollado pensando en la sencillez, por eso los usuarios deberán conocer un máximo de 50 procedimientos y unas 250 normas. No todos los usuarios deben conocer esos 50 procedimientos, ya que la mayoría solo pueden ser utilizados por el responsable de seguridad o miembros del departamento de sistemas. En general los usuarios deberán conocer tan solo la existencia de un pequeño conjunto de ellos.

Cuando un usuario requiere el uso de un activo o realizar una operación que pueda afectar a la seguridad del sistema de información de la compañía entrará en MMGS-TOOL (Herramienta del Modelo de Madurez de Gestión de la Seguridad) y obtendrá una lista de los procedimientos que el puede activar. Una vez seleccionado el procedimiento deseado, el sistema ira de forma automática activando las fases y solicitando las operaciones necesarias para pasar a la siguiente fase a cada uno de los usuarios involucrados se pueden ver en la Fig. 7. De esta forma, hasta que el usuario responsable de una fase no de la aprobación de la misma el procedimiento quedará pendiente y el sistema almacenara los retrasos ocasionados, para un posterior análisis.

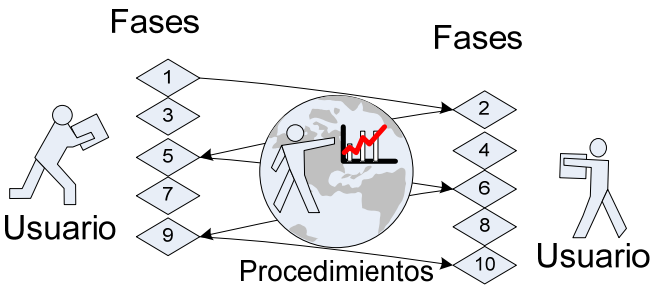

Fig. 7. Flujo de actividad en procedimientos.

Cuando un usuario entre en el sistema, podrá ver en todo momento el estado de los procedimientos que le afectan y el estado en que se encuentran.

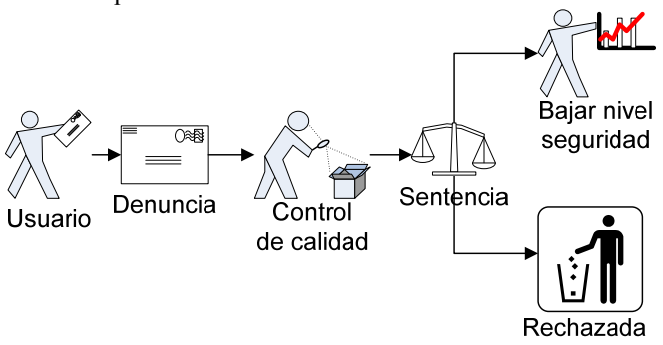

Fig. 8. Esquema del procedimiento de denuncia.

Existe un tipo de procedimiento especial en el sistema denominado *Procedimiento de Denuncia*, que es de vital importancia para mantener actualizado el nivel de seguridad. El esquema general de este procedimiento se puede ver en la Fig. 8 y es el encargado de gestionar las denuncias por parte de un usuario del sistema sobre el incumplimiento de una

normativa. El responsable de seguridad determinara si la denuncia esta justificada o no, y en el caso de considerarla justificada el sistema disminuirá de forma automática el nivel de seguridad de los controles asociados a esa norma.

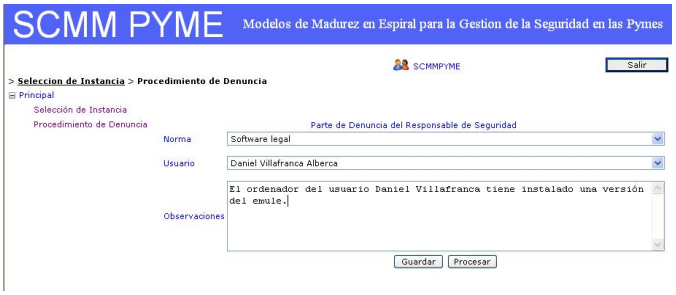

Fig. 9. Pantalla para la introducción de una violación de una norma por un usuario del sistema de información.

A continuación mostramos un ejemplo de funcionamiento del procedimiento de denuncia: un Usuario con acceso al sistema de Información de Sicaman Nuevas Tecnologías (SNT), detecta una violación de la normativa N/PSM-01 que regula el "Uso de software legal" y cuya definición detallada es "Esta terminantemente prohibido el uso de software sin licencia dentro de las instalaciones del sistema de información de la compañía. La instalación del software en los terminales será realizada por el personal del departamento de sistemas una vez se haya verificado que se cumplen con todos los requerimientos necesarios". Se introduce en la herramienta de gestión de seguridad MMGS-TOOL e inserta la denuncia en una pantalla como la de la Fig. 9.

El responsable de Seguridad recibe la denuncia y analiza si existen evidencias suficientes para tenerlas en cuenta. En caso de encontrar la evidencia requerida “localizar software ilegal en el equipo denunciado”, aprobara la denuncia al tener base sólida. Se introduce en la herramienta de gestión de seguridad MMGS-TOOL y aprueba la denuncia en una pantalla como la de la Fig. 10.

Fig. 10. Pantalla para la validación y aprobación de una violación del sistema de información por parte del responsable de seguridad.

Al aprobar la denuncia automáticamente el sistema busca en la matriz que asocia la normativa y los controles descubriendo que la normativa N/PSM-01 esta directamente vinculada a un control (podrían estarlo con varios controles) el 8.3.1 en la ISO17799:2000 ó 10.4.1 en la ISO27001 denominado "Controles contra software malicioso", que tiene un nivel de cumplimiento actual del 45,45% y lo sanciona con un -1% de cumplimiento y un periodo de sanción de 1 año.

Es decir, desde ese momento el nivel de cumplimiento pasará del 45,45% al 44,45% y la sanción se mantendrá 1 año siempre y cuando no exista una nueva violación de seguridad sobre ese control, en cuyo caso el contador se inicializaría de nuevo. El esquema de funcionamiento de este proceso se puede ver en la Fig. 11.

Con este proceso, las violaciones de la normativa de seguridad afectan de forma directa e inmediata al cuadro de mando, sin necesidad de esperar que un auditor venga a revisar el sistema. Así mismo se ven afectados todos los niveles del cuadro de mandos, alertando a la gerencia de forma sencilla cuando algo va mal, sin necesidad de esperar a la auditoria anual o bi-anual que realiza un auditor externo para poder tomar decisiones. Al poder tomarse decisiones cuando los problemas aparecen, sin necesidad de esperar un periodo largo de tiempo, evitamos el efecto domino que se produce al empezar a degradarse controles de seguridad y carecer de la información necesaria para aplicar las medidas correctivas, antes de que afecten a otros controles. Por último evitamos el efecto de desorientación que produce al responsable de seguridad, conocer la existencia de fallos en el sistema, pero no su origen.

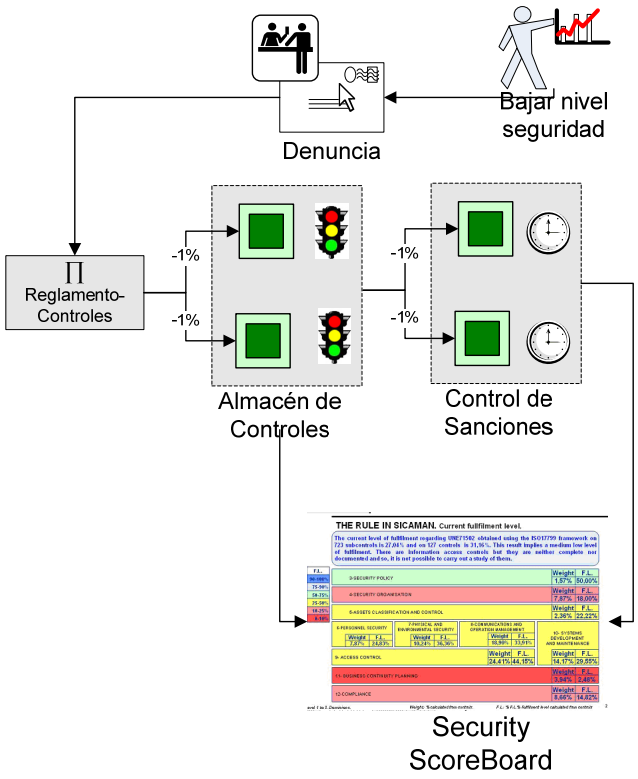

Fig. 11. Esquema de activación de un procedimiento de denuncia.

IV. Conclusión

A pesar de los enormes esfuerzos que se están realizando para crear modelos y herramientas de madurez adecuados para gestionar la seguridad en las PYMEs, éstos no terminan de

encajar con el entorno en que deben ser implantadas. La causa más probable es la falta de madurez de las empresas y la falta de herramientas especializadas en ese tipo de compañías. Aun cuando existen herramientas en el mercado, estás no ofrecen una solución total y tienen que ser completadas con otras herramientas y guías, convirtiendo la seguridad de los sistemas de información de las compañías en un conjunto de aplicaciones heterogéneas y no integrables que obligan a la compañía a invertir grandes cantidades de recursos para su mantenimiento.

En este artículo se ha presentado la propuesta de nuestro modelo y la herramienta que soporta el modelo de madurez y gestión de seguridad para las PYMEs, desarrollado durante la investigación. Esta herramienta permite a las compañías adaptarse al cambio con un mínimo coste, garantizando la seguridad y estabilidad de su sistema de información. Se ha definido de forma clara como la aplicación utiliza el modelo desarrollado para alcanzar los objetos y las mejoras que ofrece con respecto a los sistemas clásicos.

También hemos presentado algunos de los resultados obtenidos durante el proceso de investigación, centrándonos por motivos de espacio en los resultados obtenidos en la primera fase y en la evolución sufrida por el esquema del prototipo que ha pasado de utilizar la normativa ISO17799:2000 como base a utilizar la ISO27001.

La aplicación desarrollada reduce los costes de implantación de los sistemas y mejora el porcentaje de éxito de las implantaciones en las PYMEs. Por estas razones, ya que la mayoría de nuestros clientes son PYMEs, nuestra propuesta ha sido bien recibida y su aplicación está resultando muy positiva ya que permite acceder a este tipo de empresas al uso de modelos de madurez de la seguridad, algo que hasta ahora había estado reservado a grandes compañías. Además, con este modelo se permite obtener resultados a corto plazo y reducir los costes que supone el uso de otros modelos, consiguiendo un mayor grado de satisfacción de la empresa.

Puesto que esta propuesta esta en constante desarrollo, nuestro objetivo a medio y largo plazo es profundizar en los modelos de madurez para refinar nuestro modelo, mejorando el nivel de automatización de la herramienta.

Entre las mejoras del modelo sobre las que se esta trabajando de cara al futuro destacan:

- Incluir una nueva matriz que permita obtener el nivel de madurez deseable a nivel de control, para poder compararlos con los niveles de seguridad actual de cada control.
- Mejorar los algoritmos del sistema para maximizar su eficacia en la toma de decisiones.
- Incluir un planificador de los recursos que la compañía está dispuesta a invertir en un periodo de tiempo, para que el sistema sea capaz aplicarlos en el plan de mejora.
- Incluir en la Fase III una librería con los subproyectos que se deben afrontar para mejorar de formar global el sistema de gestión de seguridad.
- Incluir en la Fase III nuevos objetos que permita seguir ajustando el modelo a la nueva versión del esquema base la ISO27001.
- Incluir sistemas de métricas avanzados basados en técnicas informáticas avanzadas (redes bayesianas, sistemas difusos).
- Obtención de nuevos informes estadísticos de los desfases producidos entre dos auditorias utilizando el modelo, para sincronizar los mecanismos de recalibración de los cuadros de mando.
- Incluir en el modelo nuevas normativas de seguridad que ayuden a mejorar la gestión de la seguridad, como la LOPD Española o la HIPPA Americana.

Mediante el método de investigación "investigación en acción", con la ayuda de la retroalimentación obtenida directamente de nuestros clientes, estamos consiguiendo una mejora continua de estas implantaciones.

REFERENCIAS

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

[2] CSI, *Computer Security Institute*. 2002: Computer Crime and Security Survey.

[3] Wood, C.C. *Researchers Must Disclose All Sponsors And Potential Conflicts*. in *Computer Security Alert*. 2000. San Francisco, CA: Computer Security Institute.

[4] Biever, C., *Revealed: the true cost of computer crime*, in *Computer Crime Research Center*. 2005.

[5] Goldfarb, A., *The medium-term effects of unavailability* Journal Quantitative Marketing and Economics 2006. **4**(2): p. 143-171

[6] Telang, R. and S. Wattal. *Impact of Vulnerability Disclosure on Market Value of Software Vendors: An Empirical Analysis.* in *4h Workshop on Economics and Information Security*. 2005. Boston.

[7] Hyder, E.B., K.M. Heston, and P. M.C., *The eSCM-SP v2: The eSourcing Capability Model For Service Providers (eSCM-SP) v2*. 2004: Pittsburh, Pennsylvania, USA.

[8] Sánchez, L.E., et al. *SCMM-TOOL: Desarrollando una herramienta para gestionar la seguridad de los sistemas de información en las PYMES basada en Esquemas predefinidos*. in *IV Congreso Iberoamericano de Seguridad Informática (CIBSI'07)*. 2007. Mar de Plata. Argentina.: Noviembre.

[9] Sánchez, L.E., et al. *Developing a model and a tool to manage the information security in Small and Medium Enterprises*. in *International Conference on Security and Cryptography (SECRYPT'07)*. 2007. Barcelona. Spain.: Junio.

[10] Sánchez, L.E., et al. *Modelo de Madurez para la Gestión de la Seguridad en las PYMES basado en Esquemas predeterminados*. in *Simposio de Seguridad Informática, dentro del congreso Español de Informática (CEDI'07)*. 2007. Zaragoza. España.

[11] Sánchez, L.E., et al. *Building a Maturity Security Model Based on ISO 17799.* in *The 2006 International Conference on Computational Science and its Applications (ICCSA 2006)*. 2006. Glasgow (Reino Unido). Mayo.

[12] Sánchez, L.E., et al. *Developing a maturity model for information system security management within small and medium size enterprises.* in *8th International Conference on Enterprise Information Systems (WOSIS'06)*. 2006. Paphos (Chipre). March.

[13] Sánchez, L.E., et al. *Security Management in corporative IT systems using maturity models, taking as base ISO/IEC 17799.* in *International Symposium on Frontiers in Availability, Reliability and Security (FARES'06) in conjunction with ARES*. 2006. Viena (Austria).

[14] Sánchez, L.E., D. Villafranca, and E. Fernández-Medina, *Capitulo 9. Modelo de Madurez para SGSI desde un enfoque práctico.*, in *Gobierno de las Tecnologías y los Sistemas de Información.*, RA-MA, Editor. 2006: Madrid (España). p. 175-209.

[15] Villafranca, D., et al. *La Norma ISO/IEC 17799 como base para Gestionar la Seguridad de la Información.* in *Tercer Taller de*

Seguridad en Ingeniería del Software y Bases de Datos (JISBD'05). 2005. Granada (España).

[16] Sánchez, L.E., et al. *SCMM-TOOL: Tool for computer automation of the Information Security Management Systems*. in *2nd International conference on Software and Data Technologies (ICSOFT'07).* . 2007. Barcelona-España Septiembre.

[17] Villafranca, D., et al. *Construcción de un CMI de la Seguridad: Selección de indicadores mediante un sistema experto probabilístico*. in *IV Congreso Iberoamericano de Seguridad Informática (CIBSI'07).* 2007. Mar de Plata. Argentina.: Noviembre.

[18] Villafranca, D., et al. *Hacia un método para la construcción de Cuadros de Mando de la Seguridad en TI para PYMES.* in *Simposio de Seguridad Informática, dentro del congreso Español de Informática (CEDI'07)*. 2007. Zaragoza. España.

[19] ISO/IEC17799, *ISO/IEC 17799. Information Technology - Security techniques - Code of practice for information security management*. 2000.

[20] ISO/IEC17799, *ISO/IEC 17799. Information Technology - Security techniques - Code of practice for information security management*. 2005.

[21] ISO/IEC27002, *ISO/IEC 27002:2005, the international standard Code of Practice for Information Security Management (en desarrollo).* 2007.

[22] Corti, M.E., G. Betarte, and R. De la Fuente, *Hacia una implementación Exitosa de un SGSI.* IV Congreso Internacional de Auditoría y Seguridad de la Información, 2005.

[23] Areiza, K.A., et al., *Hacia un modelo de madurez para la seguridad de la información.* IV Congreso Internacional de Auditoría y Seguridad de la Información, 2005b. Dic (2005).

[24] COBITv2.0, *Cobit Guidelines, Information Security Audit and Control Association*. 2000.

[25] Aceituno, V., *Ism3 1.0: Information security management matury model.* 2005.

[26] Barrientos, A.M. and K.A. Areiza, *Integración de un sistema de gestión de seguridad de la información conun sistema de gestión de calidad.*, in *Master's thesis*. 2005, Universidad EAFIT.

[27] 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.

[28] Lee, J., et al. *A CC-based Security Engineering Process Evaluation Model*. in *Proceedings of the 27th Annual International Computer Software and Applications Conference (COMPSAC)*. 2003.

[29] Areiza, K.A., et al., *Hacia un modelo de madurez para la seguridad de la información.* 3er Congreso Iberoamericano de seguridad Informática, 2005a. Nov, (2005): p. 429 - 442.

[30] Walton, J.P. *Developing an Enterprise Information Security Policy*. in *30th annual ACM SIGUCCS conference on User services*. 2002.

[31] Velásquez., N. and M. Estayno. *Desarrollo y Mantenimiento Seguro de Software para Pyme: MoProSoft alienado a ISO/IEC 17799:2005*. in *IV Congreso Iberoamericano de Seguridad Informática (CIBSI'07).* 2007. Mar de Plata. Argentina.: Noviembre.

[32] MageritV2, *Metodología de Análisis y Gestión de Riesgos para las Tecnologías de la Información, V2*. 2005, Ministerio de Administraciones Públicas.

[33] Siegel, C.A., T.R. Sagalow, and P. Serritella, *Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security.* Security Management Practices, 2002. sept/oct: p. 33-49.

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

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

[36] Stephenson, P., *Forensic Análisis of Risks in Enterprise Systems.* Law, Investigation and Ethics, 2004. sep/oct: p. 20-21.

[37] Kim, S. and I. Choi. *Cost-Benefit Análisis of Security Investments: Methodology and Case Study.* in *ICCSA 2005, LNCS 3482*. 2005.

[38] Pertier, T.R., *Preparing for ISO 17799.* Security Management Practices, 2003. jan/feb: p. 21-28.

La Reunión Española sobre Criptología y Seguridad de la Información (RECSI) celebró su décima edición en la ciudad de Salamanca del 2 al 5 de septiembre de 2008. Se trata del congreso científico nacional referente en el tema de la Seguridad en las Tecnologías de la Información. En él se dan cita periódicamente los principales investigadores españoles en el tema, así como invitados extranjeros de reconocido prestigio.

En esta edición se ha contado con la presencia invitada de los investigadores Carlo Blundo, Ljupco Kocarev, Hugo Scolnik y Fausto Montoya. Además, han colaborado representantes del Centro Criptológico Nacional, la Dirección General de la Policía y de la Guardia Civil, la Junta de Castilla y León y las empresas Signe, Realsec y Ericsson España.

En este libro de actas se recogen todas las contribuciones presentadas en la reunión así como las conferencias invitadas.

ISBN: 978-84-691-5158-7