NIHIL INTENTATUM

Universidad Católica de Salta

Papeles De Mar Del Plata

Anales del IV Congreso Iberoamericano de Seguridad Informática

Papeles De Mar Del Plata

Anales del IV Congreso Iberoamericano de Seguridad Informática

NIHIL INTENTATUM

Universidad Católica de Salta

PAPELES DE MAR DEL PLATA

ANALES DEL IV CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMÁTICA

COMPILADORES

Antonio Castro Lechtaler

Julio César Liporace

Jorge Ramió Aguirre

Universidad Católica de Salta

Salta

2007

Papeles de Mar del Plata: Actas del IV Congreso Iberoamericano de Seguridad Informática / Recopilado por Antonio Castro Lechtaler; Julio Cesar Liporace; Jorge Ramió Aguirre. - 1ª Ed. Salta: Universidad Católica de Salta - Eucasa, 2007.

606 p. ; 24 x 17 cm. (Anales Congreso)

ISBN 978-950-623-043-2

1. Seguridad Informática. I. Castro Lechtaler, Antonio, recop. II. Liporace, Julio Cesar, recop. III. Ramio Aguirre, Jorge, recop.

CDD 005.8

Campo Castañares, Salta, Provincia de Salta, (A4400EDD)
República Argentina
☎ + 54 - 387 – 426-8939 fax + 54 - 387 – 426-8800

ISBN: 978-950-623-043-2
Depósito legal: Argentina 2007

EDITOR: Sebastián Cañón, M.A.
PRODUCTOR: Cristian Cavaleiro
COMPOSICIÓN INTERIOR Y APOYO GRÁFICO: Señor Oscar Iturralde.

IMPRESO EN IMPRENTA DE DOCUPRINT S.A.
Rivadavia Nº 701, (C1002AAF).
Ciudad Autónoma de Buenos Aires, República Argentina.
☎ + 54 - 11 – 43 38 20 00 fax + 54 - 11 – 43 38 20 40

De esta edición se han impreso 300 ejemplares en el mes de noviembre de 2007.

PRINTED IN ARGENTINA - IMPRESO EN ARGENTINA

PAPELES DE MAR DEL PLATA

ANALES DEL IV CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMÁTICA

COMPILADORES

Antonio Castro Lechtaler
Julio César Liporace
Jorge Ramió Aguirre

Universidad Católica de Salta
Salta
2007

COMITÉ DE HONOR

PRESIDENTE: Dr. Néstor AUZA

Presidente de la Comisión de Investigaciones Científicas de la Provincia de Buenos Aires
y Rector de la Universidad Nacional del Centro de la Provincia de Buenos Aires.

MIEMBROS

Ing. Héctor Carlos BROTTO
Rector de la Universidad Tecnológica Nacional

Ing. Norberto CAMINOA
Rector de la Universidad Nacional de Chilecito

Dr. Alfredo Gustavo PUIG
Rector de la Universidad Católica de Salta

General Ingeniero Guillermo SEVILLA
Presidente de CITEFA (Instituto de Investigaciones Científicas y Técnicas de las Fuerzas Armadas)

Dr. Manuel Aguirre TELLEZ
Decano de la Facultad de Ciencias Exactas
Universidad Nacional del Centro de la Provincia de Buenos Aires

Coronel Ingeniero Gustavo LANDA
Director - Decano de la Escuela Superior Técnica/Facultad de Ingeniería
Universidad del Ejército

Lic. Jorge Luis CAJAL
Miembro del Directorio
Comisión de Investigaciones Científicas de la Provincia de Buenos Aires

Arq. Luis De MARCO
Decano de la Facultad Regional Buenos Aires
Universidad Tecnológica Nacional

Ing. Claudio MONDADA
Decano Facultad de Ingeniería
Universidad Católica de Salta

Dr. Hugo Daniel SCOLNIK
Universidad de Buenos Aires

COMITÉ ORGANIZADOR

Ing. Antonio Ricardo Castro Lechtaler, MSc
Presidente

Dr. Jorge Ramió Aguirre,
Vicepresidente y Presidente del Comité de Programa

Lic. Julio César Liporace, EspCyS
Vicepresidente Ejecutivo

Dr. Nelson Acosta,
Vicepresidente Coordinador Local

DIRECTORES DE ÁREAS

Lic. Jorge Zaccagnini,
Director de Comunicación Social y Prensa

Mag. Lic. Carlos Alberto López,
Director de Relaciones Institucionales

Lic. Carlos Tomassino,
Director de Relaciones con las Universidades

Ing. Hugo Ballesteros,
Director de Relaciones con los Institutos de Investigación

DIRECTORES LOCALES

Lic. Oscar Noguez
Director en Buenos Aires

Ing. Roberto Giordano Lerena,
Director en Mar del Plata

Dr. Carlos García Garino
Director en Mendoza

Lic. Javier Díaz,
Director en La Plata

Mag. Ing. Beatriz Parra de Gallo,
Directora en Salta

Ing. Fernanda Carmona,
Directora en La Rioja

COMITÉ DE PROGRAMA

Presidente
Dr. Jorge Ramió Aguirre,
Universidad Politécnica de Madrid, España

MSc. Nicolás César Alfonso Antezana Abarca
Universidad Católica San Pablo, Perú

Dr. Javier Areitio Bertolín
Universidad de Deusto, España

Dr. Walter Baluja García
Instituto Superior Politécnico José Antonio Echeverría, Cuba

Dr. Joan Borrel Viader
Universidad Autónoma de Barcelona, España

Dra. Pino Caballero Gil
Universidad de La Laguna, España

Dr. Josep Domingo i Ferrer
Universidad Rovira i Virgili, España

Dr. Jeimy José Cano Martínez
Universidad de los Andes, Colombia

Dr. Adriano Mauro Cansian
Universidade Estadual Paulista, Brasil

Dr. Hugo César Coyote Estrada
Instituto Politécnico Nacional, México

Dr. Ricardo Dahab
Universidade Estadual de Campinas, Brasil

Dr. Enrique Daltabuit Godas
Universidad Nacional Autónoma de México, México

Dr. Jorge Dávila Muro
Universidad Politécnica de Madrid, España

Dr. Jorge Estrada Sarlabous
Academia de Ciencias de Cuba, Cuba

Dr. Jose Luís Ferrer-Gomila
Universidad de Las Islas Baleares, España

COMITÉ CIENTÍFICO

Dr. Juan Pedro Hecht
Universidad de Buenos Aires, Argentina

Dr. Carlos Marcelo Sánchez
Universidad de Buenos Aires, Argentina

WORKSHOP EN TÉCNICAS DE HACKING Y FORENSIA INFORMÁTICA

Fecha: martes 27 de noviembre de 2007
Seminario práctico de 4 horas

Parte 1 (2 horas)

"Técnicas de Inyección en Hacking de Aplicaciones Web"

Ponente: Chema Alonso
Ingeniero y Dr. en Informática, a falta de la lectura de tesis en este año 2007. Es Microsoft MVP Windows Security desde Julio de 2004. Consultor de Seguridad Informática durante los últimos años. Ha participado en las últimas 7 giras de seguridad de Microsoft y los Security Days. Participa activamente con los cuerpos de seguridad del estado y realiza en Informática 64 test de intrusión para grandes compañías. Ponente en decenas de conferencias de seguridad al año.

Temario:

- Introducción a las técnicas de inyección.
- SQL injection, XPath injection, LDAP injection, HTML injection
- Análisis de exploits - Explotación mediante técnicas a ciegas
- Herramientas y caso práctico

Parte 2 (2 horas)

"Utilización de Patrones de Comportamiento en el Análisis Forense Informático"

Ponente: D. Julio César Ardita
Licenciado en Sistemas y Master en Gestión de las Telecomunicaciones. Es fundador del CISIar, Centro de Investigación en Seguridad Informática Argentina. Consultor de Seguridad Informática, es ponente invitado en decenas de congresos nacionales e internacionales. Desde Cybsec Security Systems S.A. es director de proyectos de investigación sobre sistemas de detección de intrusiones y penetration test, así como profesor en decenas de cursos de seguridad en Latinoamérica.

Temario:

- Características de los incidentes de seguridad internos
- Análisis forense informático
- Metodología de análisis de patrones de comportamiento del intruso
- Aplicación real y resultados obtenidos

PROGRAMA GENERAL ACADÉMICO

Lunes 26 de Noviembre (Sesiones Plenarias)	
10 hs - 11 hs	**11 hs - 12 hs**
Atacando RSA mediante un nuevo método de factorización de enteros	Seguridad y composición de protocolos criptográficos
Dr. Hugo Scolnik: Universidad de Buenos Aires, Argentina	**Dr. Alejandro Hevia; Universidad de Chile, Chile**

Martes 27 de Noviembre (Sesión Plenaria)
12:15 hs a 13:15 hs
Criptografía post-cuántica **Dr. Paulo Barreto; Universidad de Sao Paulo, Brasil**

Martes 27 de Noviembre (09:00 hs a 11:00 hs y 11:15 hs a 12:15 hs)	
Sala 1 (SESIÓN MM1)	**Sala 2 (SESIÓN MM2)**
Construcción de funciones Bent de n + 2 variables a partir de las funciones duales de funciones Bent de n variables. **Joan-Josep Climent, Francisco J. García, Verónica Requena (España)**	Medidas de Seguridad para ficheros no informatizados. **Javier Sempere Samaniego (España)**
Representation of Boolean maps through Hamiltonian paths. **Morales Luna, Rosaura Palma Orozco (México)**	Auditorias de Seguridad en Protección de Datos. **Ángel Igualada Menor (España)**
Performance Evaluation of Cryptographic Algorithms in JCOP41 Smart Card. **Matheus F. Oliveira, Marco A. A. Henriques (Brasil)**	Desarrollo y Mantenimiento Seguro de Software para Pymes: Moprosoft alineado a ISO/IEC 17799:2005. **Nancy Velásquez (Ecuador)**
Prediciendo secuencias producidas por un generador congruente lineal sobre curvas elípticas. **Jaime Gutiérrez, Álvar Ibeas (España)**	Hacia un Proceso sistemático para el desarrollo de sistemas Grid Seguros con Dispositivos Móviles **David G. Rosado, Javier López, Eduardo Fernández-Medina, Mario Piattini (España)**
Criptoanálisis del generador shrinking: una nueva propuesta basada en un time-memory trade-off. **M. E. Pazo-Robles, Amparo Fúster Sabater (Argentina)**	Construcción de un CMI de la Seguridad: Selección de indicadores mediante un sistema experto probabilística. **Daniel Villafranca, Luis Enrique Sánchez, Eduardo Fernández-Medina, Mario Piattini (España)**
StegSecret: una herramienta pública de estegoanálisis. **Alfonso Muñoz Muñoz, Justo Carracedo Gallardo (España)**	Concepción, Diseño e Implantación de un Laboratorio de Seguridad Informática **María Eugenia Corti, Marcelo Rodríguez, Gustavo Betarte (Uruguay)**

Martes 27 de Noviembre (14:30 hs a 16:30 hs y 16:45 hs a 17:45 hs)	
Sala 1 (SESIÓN MT1)	**Sala 2 (SESIÓN MT2)**
Autómatas celulares caóticos en la generación de funciones hash resistentes a los ataques de colisiones diferenciales. **Juan Pedro Hecht (Argentina)**	Buenas prácticas de elicitación de los requerimientos de seguridad. **Susana C. Romaniz (Argentina)**
A Signature Scheme based on Asymmetric Bilinear Pairing Functions. **Routo Terada, Denise H. Goya (Brasil)**	Evaluación de Riesgo en las Tecnologías de Información y Comunicaciones orientada a Organismos Públicos. **Pablo Andrés Pessolani (Argentina)**
A Class of Secret Sharing Schemes. **J.C. Ku, Horacio Tapia-Recillas (México)**	AUDISEG: Una metodología para la auditoría de la seguridad física del ambiente informático en el sector comercial. **Sandra Cristina Riascos, Juan Carlos Guerrero, Luís Byron Calvache, Jesús Eduardo Campaña (Colombia)**
Esquemas de reparto de secretos en términos de códigos producto. **Policarpo Abascal, Juan Tena (España)**	La Universidad Simón Bolivar a la luz de los controles de seguridad de las ISO - 17799/27001. **Vidalina De Freitas (Venezuela)**
Evitando el Replay attack en Protocolos de Intercambio Equitativo con Requisitos de Privacidad. **M. Magdalena Payeras-Capellà, Macià Mut-Puigserver, Llorenç Huguet-Rotger, Josep Lluís Ferrer-Gomila (España)**	Revisión sistemática y comparación de ontologías en el marco de la seguridad. **Carlos Blanco, Joaquín Lasheras, Rafael Valencia-García, Eduardo Fernández-Medina, Ambrosio Toval, Mario Piattini (España)**
Vulnerabilidad a un Ataque de Repetición en un Protocolo de Seguridad. **Macià Mut-Puigserver, Josep Lluís Ferrer-Gomila, Magdalena Payeras-Capellà, Llorenç Huguet-Rotger (España)**	

Miércoles 28 de Noviembre (09:00 hs a 11:00 hs y 11:15 hs a 13:15 hs)	
Sala 1 (SESIÓN XM1)	**Sala 2 (SESIÓN XM2)**
Análisis de las medidas de distancia entre sesiones para la clasificación de intrusos. **Sebastián García (Argentina)**	Análisis de la Seguridad en Ecosistemas de Ambiente Inteligente. **Juan J. Ortega, Antonio Maña, Antonio Muñoz, Alejandro Gómez(España)**
NCD Based Masquerader Detection Using Enriched Command Lines. **Maximiliano Bertacchini, Carlos E. Benitez (Argentina)**	Nuevas Tendencia en Fraude electrónico. Relación entre malware y criptografía. **Delgado, José María Cámara (España)**
Metodología para la Evaluación de la Seguridad de Aplicaciones Web frente a Ataques Blind SQL Injection. **Chema Alonso, Rodolfo Bordón, Marta Beltrán, Antonio Guzmán (España)**	Sistema de identificación biométrica mediante patrón de iris utilizando operadores morfológicos y representación multiescala. **Alberto de Santos Sierra, Carmen Sánchez Ávila, Raúl Sánchez Reíllo (España)**
w3af – Web Application Attack and Audit Framework. **Andrés Riancho (Argentina)**	Attacking the Giants: Exploiting SAP Internals. **Mariano Nuñez Di Croce (Argentina)**
Transacciones Seguras para Sistemas Móviles por medio de Relaciones de Confianza. **Chadwick Carreto Arellano, Rolando Menchaca Garcia, Rolando Menchaca Méndez (México)**	Implementación de una Interfaz de Administración para Java Cards. **Luis Adrián Lizama Pérez, Roberto León Oramas, Tirso Alejandro (México)**
Técnicas antiforenses: Ocultando información en HFS+. **Carlos Enrique Nieto Lara (Colombia)**	Message-embedding from a control-theoretical point of view. **Gilles Millérioux, José María Amigó, Jamal Daafouz (España)**
Servicio de No Repudio para Marketing y Comercio basados en Servicios de Localización. **Benjamín Ramos, Ana I. González-Tablas, Arturo Ribagorda, Daniel Garzón (España)**	

Miércoles 28 de Noviembre (14:30 hs a 16:30 hs)	
Sala 1 (SESIÓN XT1)	**Sala 2 (SESIÓN XT2)**
Analysis of security protocol MiniSec for Wireless Sensor Networks. **Llanos Tobarra, Diego Cazorla, Fernando Cuartero (España)**	Arquitectura Estándar para Identificación Digital. **Chadwick Carreto Arellano, Rolando Menchaca García, Jesús Martínez Castro (México)**
Análisis Forense de Equipos de Telefonía Celular. **Rubén Vázquez-Medina, Lucio Santes-Galván, Alberto Ramos Toxtle (México)**	Performance issues to consider when applying Digital Signature in XML documents. **Eduardo Esteban Casanovas, Marcelo da Cruz Pinto (Argentina)**
SCMM-TOOL: Desarrollando una herramienta para gestionar la seguridad de los sistemas de información en las PYMES basada en Esquemas predefinidos **Luís Enrique Sánchez, Daniel Villafranca, Antonio Santos-Olmo, Eduardo Fernández-Medina, Mario Piattini (España)**	VALI - Herramienta de correlación de mensajes de bitácoras basada en relojes vectoriales. **Roberto Gómez, Julio César Rojas, Erika Mata (México)**
OTPM: Utilización del teléfono móvil como token de autenticación en servicios de banca electrónica. **Jorge Munilla, Alberto Peinado, Bernardo Quintero, Javier Téllez (España)**	Una propuesta de Autenticación Unificada Basada en la Sincronización de LDAP con Microsoft Active Directory. **Federico Herman Lutz, Sebastián Azubel (Argentina)**

Señores Congresales del IV Congreso Iberoamericano de Seguridad Informática.

Para la Universidad Católica de Salta es un gran honor haber sido invitada a publicar, a través de su fondo editorial, estos Papeles de Mar del Plata – Actas del IV Congreso Iberoamericano de Seguridad Informática, resultado del Congreso Internacional que se realizará del 25 al 28 de noviembre de 2007 en nuestro país con ese nombre.

Los 48 trabajos que aquí se presentan, aprobados por un Comité de Expertos Internacional de muy alto nivel profesional que hoy se ponen a consideración de la comunidad de investigadores de Iberoamérica y del mundo entero, representan una importante contribución al desarrollo de la criptografía y la seguridad informática. Estamos por ello seguros, que serán sin duda de gran valor para aquellos que trabaja en estas temáticas.

Nuestra Universidad, a través de su Facultad de Ingeniería, ha dado una importante prioridad a la enseñanza e investigación en las áreas de la informática y las telecomunicaciones, carreras que se dictan en ella al más alto nivel, con destacados profesionales que participarán de este significativo evento.

Deseamos entonces, darles la bienvenida a las personalidades extranjeras que hoy nos visitan, como así también a los numerosos colegas de nuestro país. A todos ellos, nuestros más afectuosos saludos. Son bienvenidos en nuestra patria.

Salta, noviembre de 2007

Dr. ALFREDO GUSTAVO PUIG
Rector
Universidad Católica de Salta

PROLOGO DE LA COMISIÓN ORGANIZADORA

Estimados Colegas,

A fines del año 2006, cuando Jorge Ramió Aguirre concurría a dictar un curso de postgrado en la Especialización en Criptografía y Seguridad Teleinformática que se dicta todos los años en la Escuela Superior Técnica de la Universidad del Ejercito desde el año 2002, nos convocó y entusiasmó a los que en la República Argentina estamos de alguna manera vinculados a la Criptografía y a la Seguridad a organizar el IV Congreso Iberoamericano que se viene haciendo con singular éxito.

A partir de allí, hemos tratado de ir armando el Congreso del que a partir de hoy ustedes podrán participar en esta ciudad de Mar del Plata. Esperamos que ella, les resulte grata y acogedora.

Como ocurre en estos casos, no han sido pocos los problemas que hemos debido ir superando para llegar a esta fecha. Y son varias las Instituciones a las que les debemos nuestro agradeciendo por su colaboración recibida desde el primer momento que les planteamos la realización de este evento.

En primer lugar, a la Comisión de Investigaciones Cientificas de la Provincia de Buenos Aires como Institución, y en particular a su Presidente y Rector de la Universidad Nacional del Centro de la Provincia de Buenos Aires Dr. Néstor Auza quien fue el primero en brindarnos su sincero apoyo. También a todos aquellos que forman parte de la Comisión de Honor, que de alguna manera han colaborado a que este Congreso esté siendo inaugurado, en particular a las autoridades nacionales y universitarias a las que estamos muy agradecidos.

En ésta como en toda reunión científica, sus objetivos se enfocan para observar hacia donde se dirige el estado del arte de la actividad en particular, y para convocar a los expertos a un intercambio de reflexiones que permitan avizorar -en singular oportunidad- los nuevos desafíos.

No dudamos que el primero se ha cumplido. El numeroso conjunto de ponencias aprobadas con referato internacional así lo prueba. El segundo seguramente será también una realidad porque esta disciplina ya dejó de ser parte de otras disciplinas, para ocupar un lugar propio manejado por verdaderos profesionales en las temáticas.

Esperemos que estos Papeles de Mar del Plata sean una guia para aquellos que trabajan e investigan en estas ciencias con el objeto de correr cada día más las fronteras del conocimiento.

Mar del Plata, noviembre de 2007

Lic. JULIO CÉSAR LIPORACE, EspCySeg.
Vicepresidente Ejecutivo
Comité Organizador
IV Congreso Iberoamericano de Seguridad Informática

Prof. Ing. ANTONIO CASTRO LECHTALER, MSc
Presidente
Comité Organizador
IV Congreso Iberoamericano de Seguridad Informática

PRÓLOGO DEL COORDINADOR DE LA RED TEMÁTICA CRIPTORED

Estimados compañeros:

Por cuarta vez nos juntamos como cada dos años en este espacio académico y de investigación propuesto por la Red Temática CriptoRed, y que hemos denominado Congreso Iberoamericano de Seguridad Informática CIBSI, para hacer un repaso del estado del arte en las materias propias de la seguridad de la información, evento que dentro de Iberoamérica congrega al mayor número de representantes y expertos en seguridad informática de los países que la conforman: Latinoamérica, Portugal y España.

CIBSI 2007 cuenta con la especial acogida de la Universidad del Centro de la Provincia de Buenos Aires, quien organiza este congreso conjuntamente con la Universidad Politécnica de Madrid, a cuyos directivos así como a todos y cada uno de los miembros del Comité Organizador deseo agradecer desde estas páginas su buen hacer y la excelente hospitalidad que nos brindan a todos los asistentes.

De 69 trabajos recibidos, un selecto grupo de 43 expertos de 13 países (Argentina, Brasil, Chile, Colombia, Cuba, Ecuador, España, México, Panamá, Perú, Portugal, Venezuela y Uruguay) ha seleccionado 48 documentos, de los que al final se presentan en este evento 43, y que proceden de investigadores de Argentina, Brasil, Colombia, Ecuador, España, México, Uruguay y Venezuela.

Así mismo, el congreso cuenta con tres conferenciantes invitados a sesiones plenarias, el Dr. Paulo Barreto de Brasil, el Dr. Alejandro Hevia de Chile y el Dr. Hugo Scolnik de Argentina, y se impartirá de forma simultánea un Workshop sobre Técnicas de Hacking y Forensia Informática, a cargo de los expertos D. Julio César Ardita de Argentina y D. José María Alonso de España.

Ya van quedando para el histórico aquellos gratos recuerdos de las ediciones de Morelia en 2002 y en el DF en 2003, ambos en México, así como el de Valparaíso en Chile en 2005, observando que en cada edición aumenta la cantidad de los trabajos presentados, participan más países y más grupos de investigación, lo que permite augurar excelentes expectativas de crecimiento para las futuras ediciones de CIBSI en el año 2009 y siguientes.

Como coordinador de CriptoRed, comunidad virtual de expertos en seguridad de la información con más de 650 miembros de 185 universidades y 240 empresas, que son el verdadero motor de este congreso, sólo puedo reiterar mis agradecimientos a todos, organizadores, autores, revisores, patrocinadores y asistentes, por permitir que este gran esfuerzo que todos hemos realizado se convierta nuevamente en una realidad, esta vez ante el marco excepcional de la hermosa ciudad de Mar del Plata y en un bello país de paisajes y gentes, Argentina.

A todos, un caluroso abrazo con todo mi afecto.

Mar del Plata, noviembre de 2007

Dr. JORGE RAMIÓ AGUIRRE
Coordinador de CriptoRed

Presidente
Comité de Programa
IV Congreso Iberoamericano de Seguridad Informática

INDICE

SCMM-TOOL: Desarrollando una herramienta para gestionar la seguridad de los sistemas de información en las PYMES basada en Esquemas predefinidos

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

[1]SICAMAN Nuevas Tecnologías. Departamento de I+D,
Juan José Rodrigo, 4. Tomelloso, Ciudad Real, España.
{lesanchez, dvillafranca, asolmo} @sicaman-nt.com
[2] ALARCOS Research Group Information Systems and Technologies Department
and Development Institute University of Castilla-La Mancha
Paseo de la Universidad, 4 – 13071 Ciudad Real, Spain
{Eduardo.FdezMedina, Mario.Piattini}@uclm.es

Resumen. Para que las empresas puedan utilizar las tecnologías de la información y las comunicaciones con garantías, es necesario disponer de un sistema de gestión de seguridad adecuado y herramientas que permitan gestionarlo. En las pequeñas y medianas empresas, la aplicación de normativas de seguridad cuenta con el problema adicional de no tener recursos suficientes para realizar una adecuada gestión. En este artículo mostramos las últimas normativas y modelos surgidos para la gestión de los sistemas de seguridad, así como los últimos avances realizados sobre nuestro modelo de gestión de seguridad orientado a las PYMES y sobre la herramienta que lo sustenta, la cual permite el desarrollo, implantación y mantenimiento de un sistema de gestión de seguridad adaptado a las necesidades y recursos de los que dispone una PYME. Así mismo mostramos cómo esta herramienta permite obtener razonables reducciones de costes y recursos con respecto a otros modelos, lo que permite que compañías con recursos limitados puedan gestionar de forma muy eficaz su sistema de seguridad utilizando nuestro modelo. Este enfoque está siendo aplicado directamente a casos reales, consiguiendo así una constante mejora en su aplicación.

1 Introducción

La información y los procesos que apoyan los sistemas y las redes son los activos más importantes para cualquier organización, y suponen 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. Existen multitud de fuentes que arrojan cifras que muestran la magnitud de los problemas ocasionados por la falta de unas medidas de seguridad adecuadas [1-4].

Actualmente es muy complejo para una pequeña o mediana empresa abordar la implantación de un sistema de gestión de seguridad [5, 6]. La tendencia en materia de

seguridad de las empresas es ir migrando poco a poco su cultura hacia la creación de un sistema de gestión de seguridad (SGSI), aunque esta progresión es muy lenta. Así, estudios como el de René Sant-Germain [7] estiman que con los modelos actuales en el 2009 tan sólo un 35% de las compañías del mundo de más de 2000 trabajadores tendrá implantado un SGSI y las cifras en las PYMES serán mucho peores. Por otra parte, en diferentes congresos se ha puesto de relevacia que las normativas existentes no son validas para las PYMES [8, 9].

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 [10]. Pero para cumplir estos objetivos, los gerentes de sistemas se han encontrado con dos problemas para los que no existe una solución satisfactoria: la falta de herramientas que permitan afrontar la gestión de la seguridad de los sistemas de información de una forma centralizada, sencilla y dimensionada al tamaño de las compañías, y la falta de guías de seguridad de la información, que permitan responder a las preguntas de ¿dónde tengo que buscar?, ¿qué tengo que controlar? y ¿cómo tengo que controlarlo?.

El primer problema sigue sin resolverse, pero creemos que podrá ser resuelto cuando se dé solución al segundo. Con respecto al segundo problema, las organizaciones tanto nacionales como internacionales se han preocupado por elaborar un conjunto de normas y especificaciones relativas a la seguridad en las tecnologías de la información y las comunicaciones. Éstas se centran sobre todo en la definición de controles de seguridad mediante códigos de buenas prácticas, normas que definen sistemas de gestión de seguridad, y normas con criterios para certificar la seguridad. No obstante, el panorama es complejo y, para una pequeña o mediana empresa, abordar la implantación de un sistema de gestión de seguridad, con la posibilidad de tener varios niveles de exigencia y con unos recursos limitados [5, 6], se convierte en una tarea muy compleja.

En trabajos anteriores [11-13] se han mostrado versiones iniciales del modelo que presentamos de forma más detallada en este artículo. La principal aportación de este artículo con respecto a los anteriores es que aquí describimos una propuesta refinada [14, 15] del modelo de madurez y gestión de la seguridad orientado a las PYMES que hemos desarrollado para solucionar los problemas de los modelos clásicos y la herramienta que lo hace viable tomando como nucleo esquemas predefinidos. El modelo desarrollado se está probando en clientes de la empresa tecnológica SICAMAN.

El artículo continúa en la Sección 2, describiendo muy brevemente los modelos de madurez existentes y su tendencia actual y algunas de las nuevas propuestas que están surgiendo. En la Sección 3 se introduce nuestra propuesta de modelo de madurez orientado hacia las PYMES. En la Sección 4 se introduce la herramienta sobre la que se está implementando este modelo de madurez. Finalmente, en la Sección 5 concluimos indicando cuál será el trabajo que desarrollaremos en el futuro.

2 Trabajo relacionado

Los Modelos de Madurez de Seguridad [16-20] 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 [21] que más se están aplicando en las empresas actualmente, destacan el SSE-CMM [22], COBIT 4.0 [23] y el ISM3 [24], y aunque se han realizado investigaciones para desarrollar nuevos modelos, ninguno de ellos ha conseguido solucionar los problemas que actualmente se producen a la hora de aplicar estos modelos en las PYMES. Entre estas nuevas propuestas podemos destacar CC_SSE-CCM desarrollado por Jongsook Lee [20] que está basado en el Common Criteria (CC) y SSE-CMM, o el modelo de Eloff y Eloff [19] que define cuatro clases distintas de protección y que permiten ir incrementando de forma progresiva los niveles de seguridad.

Casi todos los modelos de madurez definidos, tienen dominios en común y se han desarrollados matrices [19, 25] que permiten interconectar y relacionar unos modelos de madurez con otros.

Otras propuestas toman como punto central del SGSI el análisis de riesgos. Entre ellas podemos destacar la propuesta de Karen & Barrientes [18] y UE CORAS [26]. La mayoría de los modelos actuales basados en riesgos utilizan como metodología de análisis de riesgos Magerit v2 [27]. El problema es que siendo la más completa y eficiente del mercado, no suele mostrarse eficiente en las PYMES ya que requiere de una enorme complejidad en la toma de datos y la involucración directa del usuario.

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 [28] remarca que los modelos de seguridad informática que se centran exclusivamente en modelos de eliminación de riesgos no son suficientes, y por otro lado Garigue [29] remarca que actualmente los gerentes no desean saber sólo qué se ha realizado para mitigar los riesgos, también se debe poder dar a conocer eficazmente que se ha realizado esta tarea y si se ha conseguido ahorrar dinero.

El problema principal de todos los modelos de madurez mencionados es que no están teniendo éxito a la hora de implantarse en PYMES, debido principalmente a que fueron desarrollados sin tener en cuenta las estructuras específicas de las PYMES y los limitados recursos con los que este tipo de sociedades podía contar para un proyecto de estas características.

La visión de cómo afrontar estos sistemas de gestión de información 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 [18, 19].

La propuesta presentada en este artículo también está basada en la norma internacional ISO/IEC 17799, pero se ha orientado su aplicación hacia las PYMES evitando los problemas detectados en los modelos actuales.

3 SCMM-PYME: Modelo de Madurez y Gestión de la Seguridad para PYMEs

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, progresivos y sostenibles, que son los principales requerimientos que tienen este tipo de compañías a la hora de implantar estos modelos. Esas características se obtienen gracias al uso de un soporte automatizado y al uso de *Esquemas* predefinidos para compañías pertenecientes a un mismo sector.

Los *Esquemas* están formados por un conjunto de matrices que al interrelacionarse definen las propiedades principales que deben formar el SGSI de una compañía perteneciente a un sector específico. Este conjunto de matrices que permite relacionar los diferentes componentes del SGSI es utilizado por el sistema para generar de forma automática gran parte de la información necesaria, reduciendo los tiempos necesarios para el desarrollo e implantación del SGSI.

De esta forma y a partir de la información obtenida mediante la implantación en clientes de la compañía tecnologica SICAMAN, se ha desarrollado un modelo de madurez siguiendo una estructura en espiral. Este modelo persigue facilitar la realización de ciclos rápidos y económicos que permitan crear una cultura de seguridad en la organización, de forma constante y progresiva. Nuestro modelo propone realizar inicialmente una estimación del nivel de madurez de la empresa, de tal forma que con un bajo coste, y en poco tiempo, se puede determinar un plan de proyecto que presentar a la dirección de la empresa.

Uno de los objetivos perseguidos en todo el proceso es obtener el mayor nivel de automatización posible con una información mínima. En nuestro sistema hemos priorizado la velocidad y el ahorro de costes, sacrificando para ello la precisión que ofrecen otros modelos.

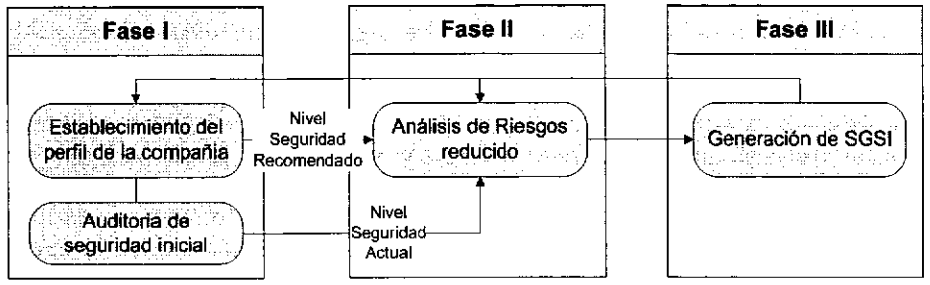

Fig. 1. Esquema simplificado de las Fase del modelo espiral

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 siguiente (ver Fig. 1). A su vez, existe una retroalimentación de información desde la Fase III a las otras que permite al sistema ir modificando sus parámetros y adecuándose a las nuevas circunstancias.

A continuación analizaremos de forma resumida el funcionamiento de cada una de las fases del modelo, revisando y analizando los algoritmos que el sistema utiliza para generar información adecuada para la compañía con el menor esfuerzo.

3.1 Fase I: Establecimiento del Nivel de Madurez Actual y Deseado.

El principal objetivo perseguido en esta fase (ver Fig. 2) es obtener un punto inical del estado de seguridad actual de la compañía. Este punto de partida servirá al sistema para ir recalculando posteriormente y por medio de las métricas su nivel de seguridad según éste vaya cambiando. En esta fase también se obtendrá el nivel de seguridad deseable para la compañía según su perfil actual. Además, se conseguirá información vital para las Fase II y III.

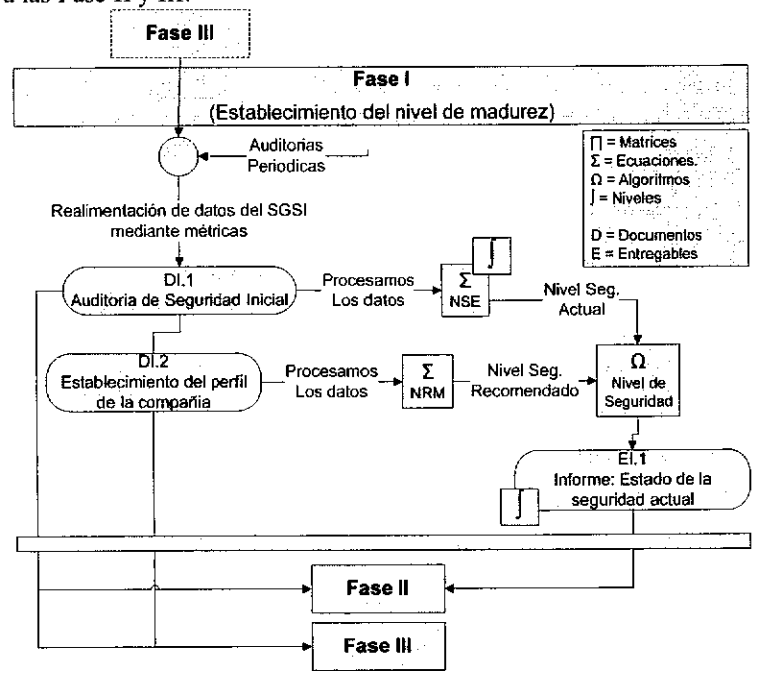

Fig. 2. Componentes de la Fase I de la Generación de Esquemas.

Está fase se compone de dos subfases.

- ***Auditoria de seguridad inicial:*** Esta subfase dentro de la Fase I consiste en realizar un detallado check-list de 735 sub-controles, que nos ayude a establecer un punto de control inicial del estado actual de la compañía con respecto a su nivel de seguridad y que servirá para establecer unos valores de inicialización de las métricas del sistema.
- ***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. Cada uno de estos parámetros se traduce a un valor y la suma normalizada de estos valores determina el nivel de madurez máximo que el sistema considera apropiado para la compañía.

3.2 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 (ver Fig. 3).

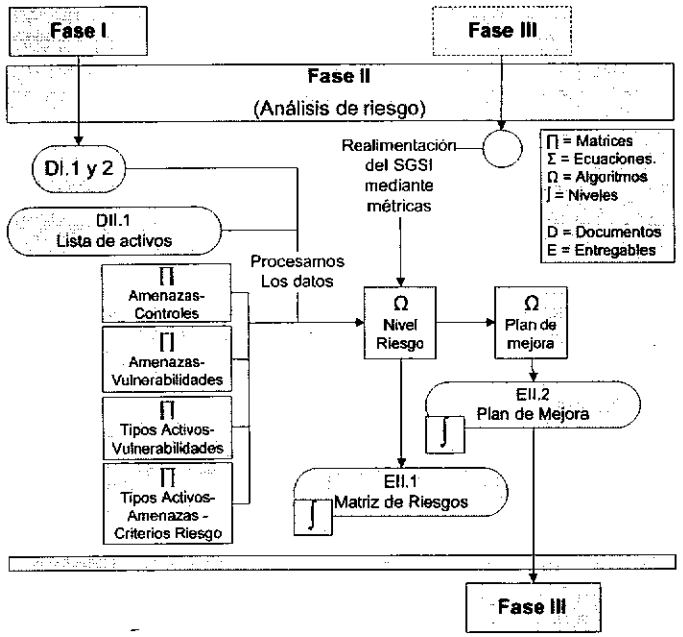

Fig. 3. Componentes de la Fase II de la Generación de Esquemas.

Esta Fase es enormemente delicada por los importantes costes que puede llegar a suponer y por la importancia de los resultados para el éxito del SGSI.

El modelo de Análisis de riesgos que hemos desarrollado está basado en los modelos propuestos por Stephenson [30], que se centran en la sinergia entre la prueba técnica y el análisis de riesgos tomando como referencia la ISO17799 y en la metodología de análisis de riesgos Magerit v2 [27]. Estos modelos no se muestran adecuados para las PYMES debido a su enorme complejidad, a que requieren un enorme esfuerzo de involucración por parte de los miembros de la compañía y a que los costes asociados a los mismos no son aceptables para este tipo de compañías.

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 riesgos y producir el máximo resultado e información para la compañía con el menor esfuerzo. Se han realizado una serie de matrices que permiten asociar

los diferentes componentes del análisis de riesgos 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 ISO/IEC 17999. Estas matrices son *estáticas,* aunque el consultor puede decidir modificarlas para adecuarlas a la compañía:

- ***Matriz de tipo de activos vs vulnerabilidades:*** nos permite asociar a los activos las vulnerabilidades que pueden afectarle.
- ***Matriz de amenazas vs vulnerabilidades:*** nos permite asociar las vulnerabilidades a cada tipo de amenaza. Con esta matriz también podemos asociar las amenazas y los activos por medio de la matriz de activos-vulnerabilidades.
- ***Matriz de amenazas vs controles de la ISO17799:*** nos permite asociar las amenazas con los controles de la ISO17799 que le afectan, y gracias a las matrices anteriores también permite llegar a establecer un nivel de seguridad sobre un activo a partir de los controles asociados al mismo.
- ***Tipos de Activos-Vulnerabilidades vs Criterios de riesgo:*** Esta matriz nos permite asociar los tipos de activos y vulnerabilidades de una compañía con respecto a los criterios de riesgo que hemos definido.

Otro de los aspectos que aportamos en nuestro modelo de riesgos es el *Nivel de cumplimiento de un control sometido a un riesgo inaceptable.* El nivel de cumplimiento de un control tiene una importancia vital a la hora de priorizar el plan de mejora del sistema, ya que nos permite determinar el nivel de cobertura actual de un activo en particular. En el caso de un activo cuyo riesgo sea alto por el impacto que podría tener un fallo de seguridad en la organización y que a su vez tenga una cobertura de control baja, deberemos priorizar aumentar dicha cobertura para aumentar el nivel de protección del mismo.

Por último, nuestro análisis de riesgos estará basado en dos algoritmos:

- ***Algoritmo de Nivel de Riesgo:*** La definición del nivel de riesgo (NR) nos la da la combinación de la probabilidad (P) de ocurrencia (vulnerabilidades) con el nivel de la amenaza (NA).
- ***Algoritmo de generación de plan de Mejora:*** Este algoritmo se genera tomando como referencia los activos que han obtenido un riesgo alto y ordenándolos por la cobertura de control de mayor a menor. Con los resultados obtenidos el sistema obtiene los controles y emite un informe indicando el control que debe mejorarse y los factores que mejorarán.

3.3 Fase III: Generación del SGSI.

En esta Fase se ha buscado que el SGSI sea manejable, enfocado a 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, utilizando para ello una serie de matrices asociadas a los resultados anteriores (ver Fig. 4).

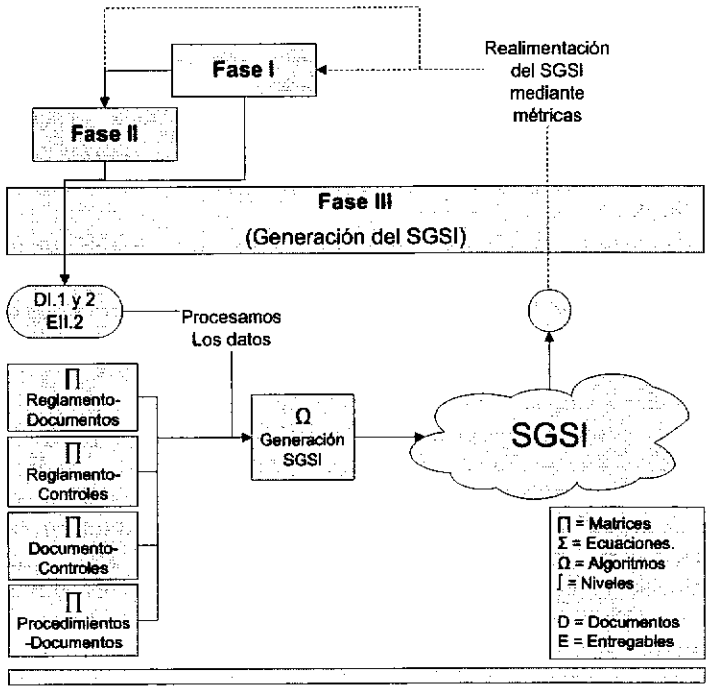

Fig. 4. Componentes de la Fase III de la Generación de Esquemas.

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 determinar que procedimientos, instrucciones técnicas, registros, etc, debe activar para la compañía.

La librería de objetos que compone el SGSI de la aplicación ira creciendo con el tiempo, por lo que se ha preferido generar la primera versión del modelo con una librería sencilla.

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. Existen cuatro tipos de matrices:

- ***Relación entre el reglamento y los documentos:*** El reglamento define normativas que deben cumplirse en una temática concreta del SGSI. La violación de una regla de esta normativa va normalmente asociada al incumplimiento de otros objetos (procedimientos, plantillas, registros, etc). Cuando se identifica una violación de una regla de la normativa, se debe incrementar en uno el incumplimiento de los documentos asociados a la

misma de forma que las métricas posteriores demuestren que el control no se está cumpliendo de forma eficiente.

- ***Relación entre el reglamento y la ISO17779:*** Esta matriz nos permite asociar las reglas de la normativa con controles de la ISO17799 de tal forma que podamos medir incumplimientos en controles de la ISO17799. La importancia de esta matriz es que nos permite realimentar el informe inicial y en el futuro nos permitirá evolucionar de forma dinámica el Nivel de seguridad mostrándolo en un Scoreboard. Dado que una normativa está asociada a un procedimiento, esta matriz también define el conjunto de procedimientos que deben o no activarse según los datos recogidos en las fases previas.
- ***Relación entre los documentos y los controles de la ISO17799:*** Es la matriz más importante ya que permite asociar los documentos que componen nuestro modelo con los controles de la ISO17799. Esta matriz es utilizada por el algoritmo de generación del SGSI para, a partir de la información generada en las Fase I y II, generar el SGSI para la compañía.
- ***Relación entre los procedimientos y sus documentos asociados:*** Esta matriz actualmente se utiliza a modo de referencia para determinar los documentos que son de E/S y los que sólo son de Entrada o Salida.

Las matrices asociadas a las ISO17799 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.

Para finalizar esta fase, se utiliza un *Algoritmo de generación del SGSI,* que genera un conjunto de reglamentos y procedimientos que deberán cumplirse para mejorar el nivel de seguridad de la compañía. 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.

4 SCMM-TOOL: Herramienta para los SGSIs en las PYMEs

La aplicación sobre la que sustentar 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, progresivos y sostenibles que son los principales requerimientos que tienen este tipo de compañías a la hora de implantar estos modelos.

Desde el punto de vista del usuario, la aplicación que sustenta nuestro modelo presenta dos ventajas claras:

- ***Simplicidad:*** Todas las fases del SGSI se han orientado a reducir la complejidad del proceso de gestión del mismo, pensando en organizaciones cuyas estructuras organizativas son muy sencillas.
- ***Automatización:*** Todo el sistema utiliza los *esquemas* para poder automatizar los procesos necesarios para el SGSI.

La aplicación se compone de dos partes claramente diferenciadas:

- ***BackOffice:*** Cuyo núcleo central es el *Generador de Esquemas* para SGSIs. Mediante esta herramienta se pueden generar esquemas completos que permiten automatizar las partes más complejas y costosas del SGSI.
- ***FrontOffice:*** Que permite a los usuarios la generación del SGSI con el mayor nivel de automatización y sencillez a partir de un esquema generado previamente.

En el BackOffice administrado por el consultor se definen esquemas de tres fases que se almacenan en la biblioteca de esquemas. A su vez los usuarios definen en el FrontOffice el SGSI para su compañía mediante un ciclo de tres fases retroalimentado que toma como base para su generación un esquema de la biblioteca de esquemas.

En cada una de las fases del BackOffice se define el esquema que utilizará posteriormente esa fase del FrontOffice para generar los datos de una instancia del SGSI.

Los *Esquemas* son el núcleo sobre el que se desarrolla nuestro modelo, ya que permiten la automatización de los SGSIs. Estos *Esquemas* están formados por un conjunto de objetos y matrices definidos a partir de la experiencia y la práctica en clientes.

4.1. Generador de Esquemas.

El generador de esquemas es una de las principales aportaciones de nuestro modelo y se puede considerar como el núcleo principal de la aplicación. La herramienta permite definir esquemas para realizar el proceso de investigación sobre las compañías, lo que permitirá ir realizando pequeños ajustes sobre estos esquemas hasta conseguir el esquema que mejor se ajuste a cada tipo de compañía.

Actualmente la herramienta se compone de un sólo esquema, al que se ha llegado mediante el refinamiento sucesivo por medio de la aplicación del modelo en diversos clientes de SICAMAN y el análisis posterior de los resultados.

Los esquemas se definen en tres fases:

- ***Fase I*** *(de definición de Esquema):* Esta fase nos permitirá definir el conjunto de niveles, factores y controles necesarios para establecer el nivel de madurez actual y el deseable.
- ***Fase II*** *(de definición de Esquema):* Esta fase nos permitirá definir el conjunto de objetos necesarios para poder realizar un análisis de riesgos básico de los activos de la compañía en un plazo mínimo de tiempo. El modelo obtenido permite que a partir de la lista de activos el sistema sea capaz de realizar un análisis y control del riesgo.
- ***Fase III*** *(de definición de Esquema):* Esta fase define la librería de objetos de los que se compone el SGSI y sus propiedades. Cada uno de los objetos definidos tiene asociado un conjunto de propiedades adicionales que servirán para recalcular dinámicamente el nivel de cumplimiento de los controles. El esquema actual está formado por una librería de objetos compuesta por el siguiente conjunto: 50 procedimientos, 4 instrucciones técnicas, 25 ficheros de reglamentos, 67 plantillas y 36 registros.

4.2. Generación del SGSI.

Cuando un consultor desee generar un SGSI para una compañía, con la aplicación y metodología que hemos desarrollado lo podrá realizar en un tiempo y coste mínimo. Para ello sólo tendrá que realizar tres fases, en las que tendrá que introducir un mínimo de información necesaria para que el sistema, a partir del esquema seleccionado y de los algoritmos definidos en la aplicación, genere un SGSI adecuado para la compañía.

- ***Fase I*** *(de Generación del SGSI) - Establecimiento del Nivel de Madurez:* Esta es la fase inicial y la que más información requerirá del sistema, ya que tendremos que definir el perfil de la compañía y el nivel de seguridad actual de la misma. Como resultado de esta fase obtendremos un porcentaje de cumplimiento de cada control para cada nivel de madurez del modelo seleccionado y un nivel al que sería deseable llegar.
- ***Fase II*** *(de Generación del SGSI) - Establecimiento del nivel de riesgo:* En esta fase y gracias a la creación previa del esquema, sólo se tendrá que definir el conjunto de activos de la compañía. Una vez que hayamos definido el conjunto de activos el sistema aplicará dos algoritmos para generar los resultados de esta fase.
- ***Fase III*** *(de Generación del SGSI) - Generación del SGSI:* En esta fase el sistema no requiere de información adicional, generando de forma totalmente automática el SGSI adecuado para la compañía mediante el *algoritmo de generación de SGSIs.*

4.3. Trabajando con el SGSI.

Una vez que hemos generado el SGSI la compañía debe comenzar a trabajar con el sistema. 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 la aplicación y obtendrá una lista de los procedimientos que él puede activar. Una vez seleccionado el procedimiento deseado, el sistema irá de forma automática activando las fases y solicitando las operaciones necesarias para pasar a la siguiente fase a cada uno de los usuarios involucrados (ver Fig. 5). De esta forma, hasta que el usuario responsable de una fase no da la aprobación de la misma, el procedimiento quedará pendiente y el sistema almacenará los retrasos ocasionados para un posterior análisis.

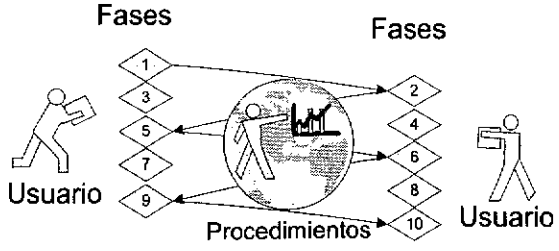

Fig. 5. Flujo de acciones de un procedimiento

Cuando un usuario entre en el sistema, podrá ver en todo momento el estado de los procedimientos en que está involucrado y aquellos que se encuentran retenidos por él.

Existe un tipo de procedimiento especial en el sistema denominado *"Procedimiento de Denuncia"*. Este procedimiento (ver Fig. 6) gestiona las denuncias por parte de un usuario del sistema sobre el incumplimiento de una normativa. El responsable de seguridad determinará si la denuncia está justificada o no, y en el caso de considerarla justificada el sistema decrementará de forma automática el nivel de seguridad de los controles asociados a esa norma.

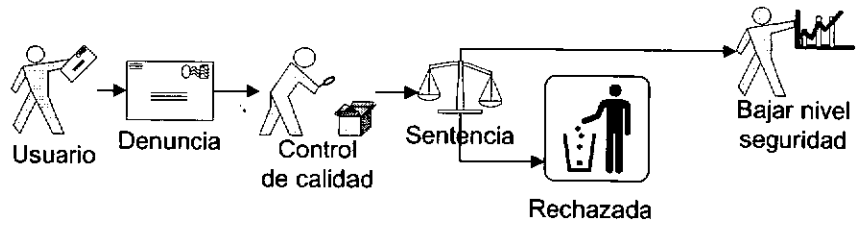

Fig. 6. Esquema del procedimiento de denuncia.

4.4. Evolución del SGSI.

Nuestro modelo de SGSI se ha diseñado para que evolucione de forma dinámica (ver Fig. 7) sin que sea obligatoria, aunque sí aconsejable, la intervención de auditores externos. De esta forma, nuestro modelo no tiene que esperar a la llegada de auditores externos para conocer cómo evoluciona el sistema, sino que el sistema evoluciona constantemente cambiando el nivel de seguridad de los controles y reajustando todas las fases del sistema.

La versión actual de la aplicación evoluciona teniendo en cuenta cuatro aspectos: 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.

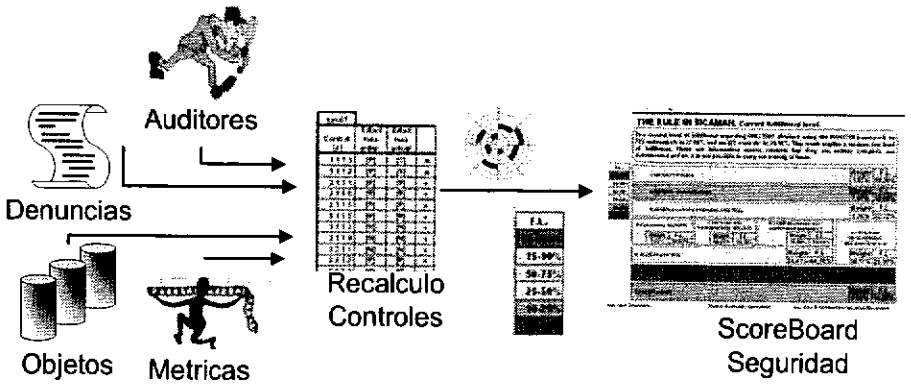

Fig. 7. Factores de actualización del SGSI

5 Conclusiones y futuros trabajos.

A pesar de los enormes esfuerzos que se están realizando para crear modelos de madurez adecuados para gestionar la seguridad en las PYMES, estos no terminan de encajar con el entorno en que deben ser implantados. La causa más probable es la falta de madurez de las empresas y el haber intentado realizar modelos demasiado generales y ambiciosos. Esto hace que muchas veces las empresas no sepan cuál es el alcance que deben cumplir, o por dónde deben empezar a acometer la reestructuración de sus sistemas, o que las metas planteadas estén demasiado lejanas y terminen desanimando a la dirección de las empresas. Uno de los documentos generados por grupos internacionales de estandarización que mayor proyección ha tenido en el ámbito internacional es el código de buenas prácticas ISO/IEC 17799, que define un conjunto muy amplio de controles de seguridad y que está siendo empleado en algunos de los modelos de madurez más innovadores del mercado. No obstante, este código de buenas prácticas no ofrece una solución global y debe ser complementado con otras normas y mecanismos de gestión adecuados.

En este artículo se ha presentado un nuevo refinamiento del modelo de madurez y gestión de seguridad orientada a las PYMES mostrado en anteriores artículos, el cual permite desarrollar y mantener sistemas de gestión de seguridad utilizando un conjunto mínimo de recursos, lo que hace que sea aplicable en el caso de las PYMES. Para ello se ha definido la metodología y una herramienta que permita soportar los resultados que se han ido generando durante la investigación.

Algunas de las principales y más valiosas conclusiones obtenidas de la realimentación de las empresas participantes en las que se han analizado varios modelos son las siguientes:

- La mayor parte de las PYMES tienen estructuras de seguridad muy parecidas. Esta característica permite desarrollar sistemas de seguridad automatizables mediante la definición de *esquemas* formados por matrices estáticas, reconfigurables a posteriori.
- Si sobredimensionamos el nivel de seguridad de una empresa con respecto a su tamaño, se produce una degradación de los controles que hemos sobredimensionado, hasta que estos alcanzan su punto de equilibrio natural.

El modelo de madurez presentado 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.

Puesto que esta propuesta está en constante desarrollo, nuestro objetivo a medio y largo plazo es profundizar en los modelos de madurez para refinar nuestro modelo, así como la herramienta que se está desarrollando de forma paralela al modelo.

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

- Mejorar los algoritmos que componen el sistema para aumentar su eficacia en la toma de decisiones.

- Incluir un planificador de tiempos y recursos que la compañía quiere invertir en el proyecto, para que el sistema sea capaz de estimar en el plan de mejora hitos temporales.
- 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.

Mediante el método de investigación "investigación en acción", con la ayuda de la retroalimentación obtenida directamente de nuestros clientes, esperamos conseguir una mejora contínua de estas implantaciones.

Agradecimientos

Esta investigación es parte de los proyectos DIMENSIONS (PBC-05-012-1) y MISTICO (PBC-06-0082), parcialmente financiado por el FEDER y por la Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha, RETISTRUST (TIN2006-26885-E) concedidos por el Ministerio de Educación y Ciencia, y el proyecto SCMM-PYME (FIT-360000-2006-73) financiado por el PROFIT y concedido por Ministerio de Industria, Turismo y Comercio.

Referencias

1. Biever, C., *Revealed: the true cost of computer crime*, in *Computer Crime Research Center*. 2005.
2. Goldfarb, A., *The medium-term effects of unavailability* Journal Quantitative Marketing and Economics 2006. 4(2): p. 143-171
3. 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.
4. 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.
5. Kim, S. and I. Choi. *Cost-Benefit Análisis of Security Investments: Methodology and Case Study.* in *ICCSA 2005, LNCS 3482*. 2005.
6. Pertier, T.R., *Preparing for ISO 17799.* Security Management Practices, 2003. jan/feb: p. 21-28.
7. Sant-Germain, R., *Information Security Management Best Practice Based on ISO/IEC 17799.* Setting Standars, The information Management JournaL, 2005. 39(4): p. 60-62, 64-66.
8. Laporte, C.Y., A. April, and A. Renault. *Applying ISO/IEC Software Engineering Standars in Small Setting: Historical Perspectives and Initial Achievements.* in *SPICE*. 2006. Luxembourg.
9. Laporte, C.Y. and A. April. *Applying Software Engineering Standards in Small Settings: Recent historical perspectives and initial achievements.* in *International Research Workshop for Process Improvement in Small Settings*. 2005. Pittsburgh.
10. 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.

11. Sánchez, L.E., *La gestión de la seguridad de los sistemas de información: pasado, presente y futuro.*, in *Revista Base Informática*. 2006. p. 54-62.
12. Sánchez, L.E., et al., *Towards a Model of Information Security Management for Small and Medium-Size Enterprises with ISO/IEC 17799.* International Journal of Computer Science and Network Security (IJCSNS), 2005. 5(11): p. 111-117.
13. Sánchez, L.E., et al. *Gestión de la seguridad de los sistemas de información en las empresas desde la perspectiva de su tamaño y nivel de madurez, tomando como base la ISO/IEC 17799. IV Congreso Internacional de Auditoría y Seguridad de la Información (CIASI'05)*. 2005. Madrid (España). Diciembre.
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. 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.
16. 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).
17. Aceituno, V., *Ism3 1.0: Information security management matury model.* 2005.
18. 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.
19. 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.
20. 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.
21. 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.
22. SSE-CMM, *Systems Security Engineering Capability Maturity Model (SSE-CMM), Version 3.0. Department of Defense. Arlington VA. 326.* 2003.
23. COBITv4.0, *Cobit Guidelines, Information Security Audit and Control Association.* 2006.
24. ISM3, *Information security management matury model (ISM3 v.2.0).* 2007, ISM3 Consortium.
25. Jimmy Heschl, C., CISM. *COBIT Mapping: Mapping of ISO/IEC 17799:2005 with COBIT.* IT Governance Institute 2006 [cited; Available from: http://www.itgi.org.
26. Lund, M.S., F.d. Braber, and K. Stolen, *Proceedings of the Seventh European Conference On Software Maintenance And Reengineering (CSMR'03).* IEEE, 2003.
27. MageritV2, *Metodología de Análisis y Gestión de Riesgos para las Tecnologías de la Información, V2.* 2005, Ministerio de Administraciones Públicas.
28. 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.
29. Garigue, R. and M. Stefaniu, *Information Security Governance Reporting.* Information Systems Security, 2003. sept/oct: p. 36-40.
30. Stephenson, P., *Forensic Análisis of Risks in Enterprise Systems.* Law, Investigation and Ethics, 2004. sep/oct: p. 20-21.