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

Construcción de un CMI de la Seguridad: Selección de indicadores mediante un sistema experto probabilístico

Daniel Villafranca[1], Luis Enrique Sánchez[1], Eduardo Fernández-Medina[2], Mario Piattini[2]

[1]SICAMAN Nuevas Tecnologías. Departamento I+D, Juan José Rodrigo, 4. Tomelloso, Ciudad Real, España
{dvillafranca, lesanchez} @sicaman-nt.com
[2]ALARCOS Grupo de Investigación, Departamento de Tecnologías y Sistemas de Información Universidad Castilla-La Mancha 13.071 Ciudad Real, España
{Eduardo.FdezMedina, mario.piattini} @uclm.es

Resumen. La implantación práctica de Sistemas de Gestión de la Seguridad de la Información presenta una problemática añadida para el caso de las PYMES debido a la falta de herramientas y guías adaptadas a su estructura organizativa y procesos en el área de TI. Los criterios de evaluación de la seguridad deben corresponderse a los objetivos que se requieren y evolucionar conforme al nivel de madurez del sistema, de forma que las métricas se integren con los objetivos empresariales de Seguridad. El uso del cuadro de mando integral nos permitirá evaluar, de una forma rápida, el estado de la seguridad para una toma de decisiones coherente. De cara a su construcción, uno de los problemas principales a resolver será la selección de los indicadores apropiados que interpreten eficientemente la seguridad del sistema. En este artículo, analizaremos desde un enfoque práctico el proceso de recogida de estos indicadores, introduciendo un método para el diseño y construcción de cuadros de mando que mediante un sistema experto basado en redes bayesianas, facilitará esta tarea para su aplicación en entornos PYMES.

1. Introducción

El gobierno de la seguridad de la información ha empezado a considerarse un elemento clave en las actividades de la empresa, una consecuencia más de la creciente dependencia que la sociedad en general tiene de las TIC. Por ello, la necesidad de proteger la información está creciendo enormemente. Se demandan por lo tanto muchos productos, sistemas y servicios para gestionar y mantener esa información, y no es suficiente con realizar unos controles de seguridad superficiales [12]. Además es necesario aplicar un enfoque riguroso para evaluar y mejorar la seguridad de los productos y también de los procesos que se llevan a cabo en el contexto de las Tecnologías de la Información y las Comunicaciones.

Son numerosas las fuentes científicas que reclaman la necesidad de que la industria de la seguridad de la información y los profesionales de la misma establezcan sus métricas de seguridad, sus medidas y un marco para su gestión [1, 5, 9]. El **cuadro de**

mando de la seguridad nos permitirá gestionar la seguridad en base a información cuantitativa y objetiva, en base a los riesgos a los que se exponen los activos de una compañía, lo que facilita la toma de decisiones alineadas con los requisitos del negocio.

Las métricas de seguridad son necesarias para saber el estado de un sistema de información [8] y tienen por finalidad **conocer, evaluar y gestionar** la seguridad de los sistemas de información [7]. Si una organización no usa métricas de seguridad para la toma de decisiones, las elecciones serán motivadas por aspectos puramente subjetivos, presiones externas o por motivaciones puramente comerciales [17].

Un Sistema de Gestión de la Seguridad de la Información (SGSI) se puede definir como un sistema de Gestión usado para establecer y mantener un entorno seguro de la información [2]. Este SGSI debe tratar la puesta en práctica y el mantenimiento de procesos y de procedimientos para manejar la seguridad de la tecnología de la información. Por tanto la utilización de métricas en los SGSI es fundamental porque nos dará una información sobre la eficacia del mismo y permitirá una revisión posterior de su comportamiento [7].

Actualmente es muy complejo para una pequeña o mediana empresa abordar la implantación de un sistema de gestión de seguridad [11]. 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), para lo cual es preciso disponer de herramientas y metodologías adecuadas para este tipo de empresas [14].

El seguimiento estricto de estas fases en este tipo de empresas suele ser muy complicado debido a la falta de concienciación de la alta dirección y a la inexistencia del entorno inicial sobre unas bases mínimas en lo que a seguridad de la información se refiere. Para realizar esta tarea, hemos utilizado el concepto de Cuadro de Mando de Kaplan&Norton [6] aplicado a la Seguridad de la Información, diseñando nuevos mecanismos para la construcción del mismo y que se adaptan a la problemática de las PYMES.

En este artículo presentamos una solución práctica a la problemática que se ha generado en el uso seguro de las TIC, la necesidad de establecer un modelo de gestión de la seguridad en estos sistemas y de la complejidad que se presenta en la mayoría de los casos. Nuestra aportación plantea, desde una perspectiva práctica basada en el trabajo con nuestros clientes, un método para **definir y seleccionar las métricas de seguridad** necesarias para la construcción de un cuadro de mandos integral de la seguridad de la información. De forma novedosa, este método nos permite establecer soluciones de seguridad basadas en los niveles de madurez, estableciendo métricas acordes a las necesidades reales y siendo el resultado final un modelo de cuadro de mando acorde a los problemas reales de las PYMES. Esta metodología será aplicable a un gran número de casos adicionales y permitirá a las empresas construir modelos similares con un coste en tiempo y recursos muy razonable.

El artículo continúa en la sección 2, analizando los antecedentes de los estándares internacionales en el empleo de las métricas e indicadores con el fin de utilizarlos para la construcción de un Cuadro de Mando Integral (CMI, en ingles *BSC*) para la gestión de la seguridad en las TI en las PYMES. La sección 3 se divide en dos partes: en la primera se expone la metodología que hemos desarrollado y estamos utilizando para la construcción de CMI en nuestros clientes según el modelo de madurez que se ha presentado en anteriores artículos [15,16]. En la segunda parte se analiza de forma

detallada el proceso de selección de los indicadores como parte de esta metodología y realizado mediante un sistema experto realizado mediante una red bayesiana. Finalmente, aportamos las conclusiones e indicamos cuál será el trabajo que desarrollaremos en el futuro.

2. Las Métricas de Seguridad en la construcción del CMI

Las **métricas de seguridad** facilitan el cumplimiento de los objetivos, cuantificando la implantación de los controles de seguridad y la eficacia y eficiencia de los mismos, analizando la adecuación de los procesos de seguridad e identificando posibles acciones de mejora [3]. Las métricas deben proporcionar información cuantitativa (porcentajes, medias, números).

Los procesos de definición de métricas deben tener en cuenta la naturaleza del negocio y organización, para poder adecuarse a cada tipo de negocio. En la definición de métricas es habitual encontrarse con numerosos problemas, siendo los más relevantes los siguientes [17]:

- Las métricas no están siempre definidas en un contexto dónde el objetivo o interés industrial que se pretende alcanzar mediante su utilización es explícito.
- En ocasiones, aunque el objetivo sea explícito, las hipótesis experimentales a menudo no están hechas de forma explícita.
- Las definiciones de métricas no siempre tienen en cuenta el entorno o el contexto en el cual serán aplicadas.
- A menudo, no es posible realizar una adecuada validación teórica de las métricas porque el atributo que una métrica pretende cuantificar no está bien definido.
- Un gran número de métricas no han sido nunca objeto de validación empírica.

Las definiciones de métricas no siempre tienen en cuenta el entorno o el contexto en el cual serán aplicadas. Para analizar el propósito de las diferentes métricas es necesario usar una clasificación de las mismas [18], algo necesario para abordar nuestro modelo [14, 15].

Para responder a las necesidades de gestión de control en las TI, COBIT (*Control OBjectives for Information and related Technology*) es un conjunto de buenas prácticas y metodologías que provee una guía de gestión de activos y métricas para una organización en un entorno de 34 procesos de TI. El modelo que define COBIT enlaza los requisitos del negocio de información de la dirección a los objetivos de las TI [20]. Con este objetivo se propone una estructura y una serie de indicadores para medir la tecnología de la información [4], basados en Indicadores Clave del Rendimiento (*Key Performance Indicators, KPI*), Indicadores clave de logros (*Key Goal Indicators, KGI*) y los Factores críticos del éxito (*Critical Success Factors, CSF*). Ante la cuestión sobre lo que se debe medir, hay que establecer estos marcadores e indicadores para las diferentes áreas funcionales de la seguridad [9]. Según lo ilustrado en la figura 1, los recursos y las actividades relacionadas con los servicios de las TI se manejarán y controlarán mediante los objetivos del control:

- Indicadores clave del rendimiento (*KPI*): Definen las medidas del rendimiento de los procesos de TI en función de su funcionamiento y operación,

– Indicadores clave de logros (*KGI*): Definen las medidas que determinan si un proceso de TI satisface los requerimientos de negocio.

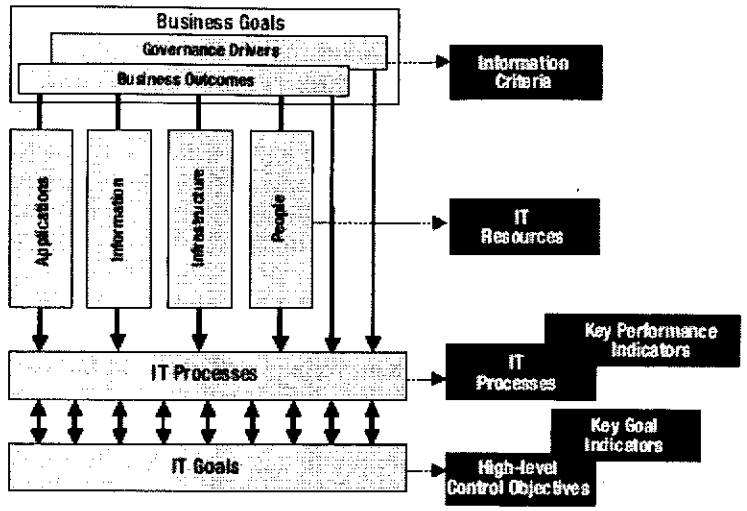

Fig. 1. Gerencia, control, alineación y supervisión en COBI (Fuente: IT Governance Institute)

Con un enfoque más práctico en la evaluación y selección de estos indicadores encontramos en NIST [10] una serie de parámetros que van a definir la métrica, tales como el tipo de control, propósito de medida, valores, etc., y que nos han servido de referencia en la construcción de nuestro modelo.

De cara a unificar esta situación, encontramos que la norma ISO/IEC 17799:2005 [21] nos relaciona los controles a aplicar según las áreas y políticas de seguridad que se establecen en la organización. De esta forma podemos adaptar los niveles de madurez y nuestras métricas en función de parámetros particulares de la empresa u organismo en cuestión. Con un enfoque más orientado a métricas [22], esta misma organización también nos define una guía detallada de las métricas e indicadores de seguridad, tratando de determinar la eficacia de un programa de seguridad de los sistemas de información en las organizaciones.

Lo que tienen en común estas metodologías que propugnan la creación de un sistema de gestión es que éste debe basarse en los procesos que la organización ejecuta. En este panorama, dentro de los objetivos de los SGSI y los que nos plantean los clientes de SICAMAN, con la idea de aplicar los programas de gestión de la seguridad en los SI, hemos llevado a cabo varias actividades:

– Desarrollo de una metodología de gestión de la seguridad orientada a las PYMES [13] con base en la norma ISO 17799.
– Desarrollo de una herramienta de gestión global de la seguridad, que incluya un cuadro de mandos orientado a la gerencia.
– Definición de un proceso específico para la construcción de un cuadro de mando orientado a la seguridad que realice la selección adecuada de las métricas y defina el nivel deseable de éstas en función de las características de la empresa.

La construcción de un SGSI es más complejo para una PYME, por lo que hemos desarrollado un modelo más práctico basado en tres niveles de seguridad que aplicamos según el nivel de madurez inicial y las características particulares de la empresa.. En la construcción de nuestro modelo, hemos considerado principalmente el núcleo de la norma ISO/IEC 17799, complementada con otras guías de seguridad, ya que por sí sola no nos proporciona un SGSI completo, sino un conjunto de controles que nos sirven de referencia. Complementariamente se han obtenido referencias de diferentes métricas a partir del Instituto Nacional de Normas y Tecnología (NIST).

Las características más destacadas de nuestro modelo son las siguientes: i) tiene tres niveles de seguridad [1 a 3] en lugar de los 5-6 niveles que proponen los modelos clásicos (v. Figura 2), ii) se propone que cada nivel sea certificable, en lugar de la certificación total existente hasta el momento, por último, iii) se asocia el nivel de madurez a las características de la empresa.

- **Nivel 1 – Protección mínima.**
  - Seguridad Personal.
  - Planificación de la continuidad de negocio.
  - Cumplimiento.
- **Nivel 2 - Protección razonable.**
  - Organización de la seguridad.
  - Clasificación y Control de Activos.
  - Control de Acceso.
- **Nivel 3 – Protección conveniente.**
  - Seguridad Personal.
  - Seguridad Física.
  - Comunicaciones y Operaciones.
  - Desarrollo y mantenimiento de sistemas.

Fig. 2. Niveles de seguridad del modelo MMISS-SME

Dentro de este modelo, toma vital importancia encontrar los indicadores clave que sirvan para definir una herramienta que nos va a permita asegurar el cumplimiento de los objetivos marcados en nuestro programa de seguridad [13]. Esta propuesta de selección y evaluación de estos indicadores, nos permitirá solucionar el problema de la falta de herramientas, realizando una evolución progresiva en todos los niveles hasta alcanzar metas parciales, sin sobredimensionar el sistema de seguridad en la empresa.

Desde su introducción en 1992, el entorno de gestión basado en un CMI ha sido usado por cientos de organizaciones en todo el mundo para describir la estrategia empresarial y como una estrategia para medir su rendimiento.

Los **cuadros de mando** son muy útiles para controlar procesos regulares con un flujo de información continuo (y este es el caso de la gestión de la seguridad de la información), ya que permiten agrupar la información más relevante (es decir, útil para la toma de decisiones) necesaria para tener un conocimiento permanente de la

situación de la gestión y su evolución en el tiempo [7]. Es una herramienta que nos va a permitir en nuestro caso sintetizar los procesos de control de seguridad para ofrecer una información sencilla, resumida y eficaz para la toma de decisiones en el caso de las PYMES. El marco genérico de un CMI puede ser traducido a las necesidades más específicas de las funciones de TI, sus proyectos y sus procesos específicos [19], con el fin de definir y gestionar sus requerimientos. Este marco se debe particularizar además según la organización y adecuar así sus objetivos de control a los activos más críticos de sus procesos.

De esta forma, para introducir el proceso general para la construcción de nuestro CMI orientado a PYMES, hay que revisar cómo se han definido los indicadores y seleccionado las métricas. La selección de estos indicadores es una de las claves de nuestro proceso de desarrollo de un modelo de cuadro de mandos orientado al gobierno de la seguridad. El trabajo con nuestros clientes requiere tener en cuenta los diferentes aspectos de la seguridad con objeto de salvaguardar la información, desde la seguridad física con controles biométricos, pasando por la seguridad en los desarrollos software y hasta la seguridad de la externalización de servicios y recursos IT.

Este trabajo nos ha aportado diferentes experiencias que nos han ayudado a definir las variables que se debe contemplar para la selección de los indicadores en el proceso de construcción de un CMI en una PYME y que según sus procesos pueden ser recomendable su aplicación con mayor o menor peso. Entre otras variables que debemos tener en cuenta señalamos las siguientes:

- Política de la organización
- Objetivo de Control
- Proceso o método de recogida
- Niveles de Madurez.
- Tipo de Empresa
- Valores/Pesos
- Validez
- Automatización de la métrica.
- Frecuencia de medición
- Relación de costes

Con el objetivo principal de presentar sólo la información en materia de seguridad necesaria para cada organización, el método de construcción de cuadro de mandos que presentamos en este artículo se enmarca dentro de un modelo de madurez de la seguridad que hemos elaborado. Está especialmente diseñado para ser implantado en PYMES [15,16] debido a las características particulares de éstas, en las que resulta difícil adecuar los estándares y modelos sobre métricas y seguridad de la información presentados al inicio. En el siguiente apartado revisaremos con detalle el planteamiento anterior y cómo nos sirve de base para el desarrollo de un sistema experto para la selección de los indicadores más apropiados para nuestro CMI

3. Proceso de construcción de un CMI y selección de métricas

Un cuadro de mandos integral podría definirse como una herramienta de gestión que ofrece información clave, entre otras cosas que permite a la gerencia manejar el negocio, consiguiendo resultados satisfactorios y adaptando la organización a las tendencias del entorno, ofreciendo un conjunto de perspectivas de diferentes aspectos de una organización [4]. Este planteamiento ha sido trasladado a las tecnologías de la información y de forma más específica a la seguridad en las TIC.

El modelo de funcionamiento básico sobre el que se sostiene el cuadro de mando es la fijación de unos objetivos en la organización, que son realizados mediante unas actuaciones que tienen reflejo en unas variables clave y que se controlan a través de indicadores [7]. De esta forma, el CMI como herramienta, debe monitorizar los procesos de seguridad en TI y facilitar la toma de decisiones a las organizaciones, que en el caso de las PYMES, que suelen carecer de estructura y departamentos especializados en TI, requieren presentar la información de forma muy precisa y simplificada a la dirección.

Para la definición de un Cuadro de Mando para la seguridad de la información, en consonancia con la guía de COBIT [3], se nos definen cuatro perspectivas tal y como se muestra en la Figura 3:

Contribución corporativa	**Orientación al usuario**
Cómo ve la organización el valor creado por la seguridad en TI	Cómo ven los usuarios en TI a la seguridad en la tecnología de la información
Excelencia Operacional	**Orientación Futura**
Cuán eficientes y efectivos son los procesos de administración de la seguridad en TI	Cómo están posicionadas las TI para satisfacer las necesidades futuras

Fig. 3. Cuadro de mando para la Seguridad en IT según COBIT

3.1 Proceso de definición de Cuadros de Mandos de Seguridad para PYMES

Por nuestra experiencia hemos comprobado que cada compañía tiene intereses distintos en materia de seguridad, y las métricas se establecen de acuerdo a lo que se esté tratando de proteger y medir, así como de la situación de la empresa [6]. Las compañías se imponen como objetivo gestionar la seguridad en base a información cuantitativa que facilite la toma de decisiones y el análisis de inversiones y de confianza a accionistas, dirección y usuarios [1]. Por tanto se trata de determinar qué factores son los más importantes según la actividad de la misma

Las características que se deberían cumplir en los indicadores y métricas de seguridad, se resumen en los siguientes puntos:

- Establecer los objetivos de las métricas automatizables para desarrollar una herramienta eficaz y óptima en su aplicación.
- Filtrar la selección de los indicadores a aplicar de acuerdo a su nivel en el ciclo de nuestro modelo en espiral, reflejando el nivel a partir del que se puede aplicar la métrica.
- Evaluación del impacto del proceso de obtención del valor del indicador en la organización, analizando las áreas funcionales de la organización y evaluando la aplicación de las métricas adecuadas en cada una.
- Optimización de costes temporales y económicos de los procesos de aplicación de nuestro modelo de madurez.
- La aplicación de la experiencia recogida en nuestro trabajo de prevención y corrección de incidentes de seguridad en el día a día con las empresas, a través de los informes periódicos que se presentan a la gerencia.

Existen principalmente dos metodologías para la construcción de un Cuadro de Mando: *top-down* y *down-top* [12]. Alternativamente, también se han propuesto otras técnicas en cascada [29]. Por considerar algo rígidos estos métodos [23], la idea de nuestro enfoque es un planteamiento mixto entre un enfoque en cascada con realimentación de las experiencias de implantaciones anteriores, y los modelos de construcción *top-down* y *down-top*, pues se recogen los objetivos que se definen desde la gerencia y el estado previo de los sistemas con los que cuenta la organización.

El modelo *top-down* es más formal y completo, que en nuestro caso permite ala dirección definir sus necesidades y objetivos. Por el contrario el método *down-top* es algo menos formal, aunque permite acelerar el desarrollo de construcción del CMI [7]. Por ello, nuestro método es básicamente un procedimiento incremental que viene dado por el modelo de madurez desarrollado en espiral, que conjuga varias fases en su definición.

En este contexto definimos las etapas del proceso de construcción del CMI de la seguridad, según se define en la Figura 4. Este modelo presenta un desarrollo inspirado en el método en cascada de Van der Zee [23]:

- **Determinar los objetivos del SGSI:** Para aplicar nuestra metodología en la práctica hemos de empezar por determinar los componentes funcionales que quiere medir. Para ello hemos aplicado diferentes guías generales, como la norma ISO 17799, COBIT y NIST como base para desarrollar las métricas en las áreas de que se está tratando de controlar. No sólo se han adaptado sus dominios funcionales, sino que se han establecido nuevos indicadores que encajan dentro de nuestro objetivo final. Se ha dado especial prioridad a los componentes que desea medir en función del ciclo de implantación de SGSI.
- **Auditoria preliminar**. Se establecerá una evaluación a priori de la infraestructura del SI a partir de las experiencias que se hayan recogido en los trabajos de auditoría de la seguridad previos, incluso antes de que la dirección decida la implantación del SGSI.
- **Selección de las métricas mediante le modelo en Espiral:** Se define en 3 etapas:
  - ***Definición de las métricas objetivo***. En función de los dos procesos anteriores y de acuerdo al conocimiento adquirido en experiencias anteriores se definirán las

métricas necesarias para cada caso. Es en esta parte donde se realiza un aprovechamiento de nuestro "know-how" para la selección de las indicadores para la determinación de las métricas según el Nivel de Madurez.
  - ***Establecimiento del Nivel de Madurez***. Dentro de nuestro modelo en espiral y a partir del análisis de riesgos que se realiza, se definen unas métricas acordes al nivel del modelo de madurez que se aplica en el SGSI.
  - ***Selección de los indicadores clave del proceso***. En la implantación de cada una de las métricas para cada uno de los modelos de madurez de nuestro sistema, se ha tenido en cuenta la integración con los objetivos Empresariales y que en los diferentes niveles de la empresa, han podido comprender y colaborar en el éxito del programa.
- **Construcción del CMI de seguridad**. Finalmente se realiza el cálculo de los indicadores de forma global para presentarlos a la dirección un CMI para el gobierno de la seguridad de la información adaptado a sus procesos y basado en el modelo de negocio. Adicionalmente se realiza un registro de estos valores en un histórico.

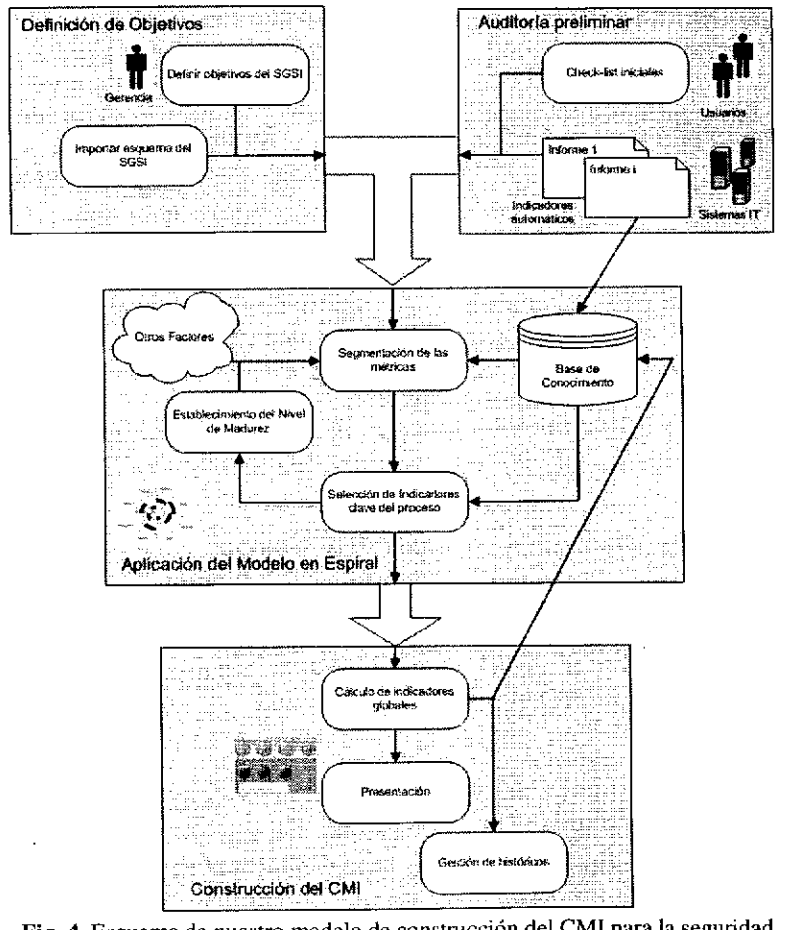

Fig. 4. Esquema de nuestro modelo de construcción del CMI para la seguridad

Finalmente, para la construcción de un buen CMI se requiere que las métricas estén equilibradas [7] de acuerdo a:

- En el tiempo: Pasadas (resultados) vs. Futuras (mejora y crecimiento).
- En el alcance: Externas (accionistas y clientes) vs. Internas (empleados y procesos).
- En las perspectivas: Que en los modelos generales no orientados a la seguridad serían Indicadores de resultados (financiera y clientes) vs. Inductores de resultados (procesos internos y empleados).

En el caso del CMI orientado a la seguridad, una vez obtenidos los valores de las métricas totales para cada uno de los dominios, la presentación de la información en el CMI se agrupará en las áreas, según refleja la Figura 5:

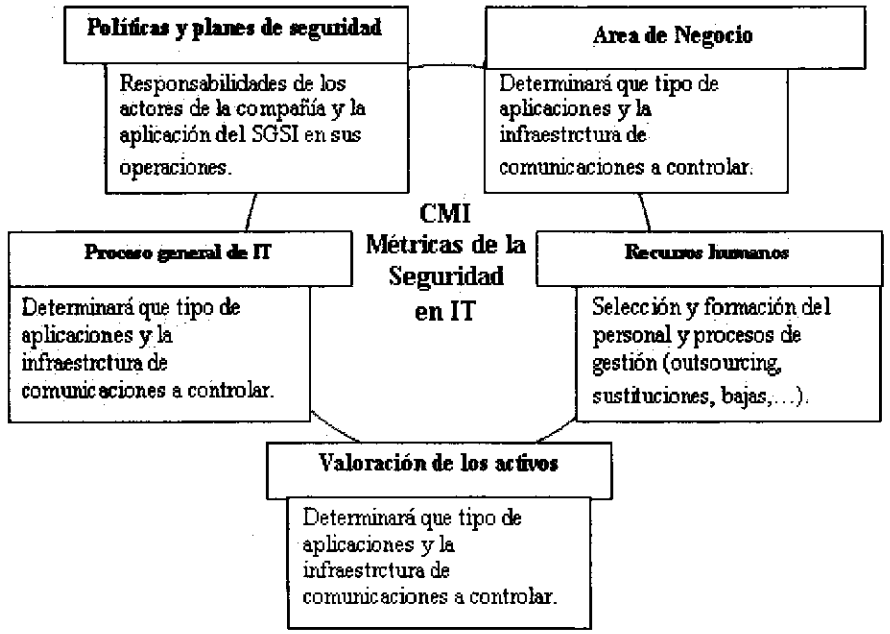

Fig. 5. Perspectivas de nuestro CMI de Seguridad

Para cada uno de estos dominios se contemplará un rango porcentual indicando el valor medido entre 0-100%. Este CMI irá variando sus indicadores en cada uno de los dominios y ciclos del modelo en espiral, según el nivel de madurez y los objetivos del plan de SGSI que se hayan definido al inicio del desarrollo.

Por último, también se realizará una gestión de los totales históricos. Para ello, se realizará un registro de la evolución de los valores de cada uno de las áreas del proceso del SGSI. Para una mejor percepción de los avances se mostrará el último valor anterior y el actual (según el diseño que se seleccione).

3.2 Proceso de selección de los indicadores mediante una Red Bayesiana

Un punto fundamental en la construcción del CMI es la selección de los indicadores que vamos a reflejar en él. Para ello la selección de una buena métrica, sin criterios subjetivos, de bajo costo de obtención y con valores cuantitativos (no cualitativos) y acorde con las características de la empresa es fundamental.

Ello nos motivó a elaborar nuestro modelo propio, cuya principal ventaja es la implantación progresiva de la seguridad (ver Figura 4) dependiendo de dos parámetros principales:

- La *dimensión de la empresa*, medido con parámetros tales como su actividad, nº de trabajadores y facturación.
- El *nivel de madurez de la seguridad* en la misma, relativo a los objetivos y metas establecidos previamente en la organización.

En relación a nuestro modelo, con base a los dos puntos anteriores y partiendo de una clasificación práctica basada en nuestra experiencia de las mediciones realizadas en las empresas, hemos realizado una clasificación global en cinco categorías, en contraposición al enfoque clásico del CMI (ver Figura 3) y con el objeto de construir un CMI a medida de las necesidades de cada organización. Estas categorías son:

- **Los recursos humanos**: relacionada con la selección y formación del personal, así como los procesos de gestión del mismo.
- **El proceso**: en función de la actividad de la empresa y la tecnología utilizada en el mismo, determinará qué tipo de aplicaciones, así como la infraestructura de comunicaciones que será fundamental controlar.
- **Los clientes y el negocio**: será vital determinar qué activos son los más importantes que se deben proteger de acuerdo a preservar la imagen de la compañía.
- **Valoración de los activos**, la relación coste/resultado que se obtiene de la implantación de un control para mitigar un riego va a constituir un factor clave, ya que muchos riesgos se asumen porque el esfuerzo es mayor que el beneficio que se obtiene.
- **Política operativa y planes de seguridad**: Nos permitirá determinar las responsabilidades de los actores de la compañía y la aplicación práctica de nuestro sistema de gestión de la seguridad en función de sus operaciones, definiendo las métricas dentro de los dominios de nuestro modelo en espiral.

Para ello, hemos diseñado un algoritmo para la selección de indicadores a medida de cada empresa y que está basado en sistemas expertos probabilísticos. Para la construcción de este sistema experto hemos diseñado una red bayesiana que tiene en cuenta variables directamente relacionadas con cada caso. Entre los motivos principales para la selección de este tipo de redes enumeramos los siguientes:

- El marco para trabajar con la incertidumbre está bien estudiado, comprendido y asentado dentro de los métodos de inferencia con base en el Teorema de Bayes.
- La necesidad de usar incertidumbre es algo aplicable en el mundo real y más en el campo de la seguridad en los sistemas de información, por lo que el uso de un método probabilístico nos permite manejarla de forma apropiada.

- La teoría de probabilidad es un mecanismo claro para la toma de decisiones muy cercano al razonamiento humano, en nuestro caso el auditor de SI.
- En una red bayesiana la probabilidad de los nodos está condicionada a priori por los nodos relacionados, lo que en nuestro caso son las variables que condicionan la selección de las métricas, y que empíricamente hemos venido observando que están relacionados en nuestro modelo.
- Este mecanismo nos va a permitir realizar un aprendizaje automático mediante la propagación de la probabilidad.

Dado un indicador, la probabilidad de utilización de la misma y su contribución en la construcción de nuestro CMI viene dada por una serie de variables con valores definidos de forma escalar y que hemos seleccionado en contraposición a otras variables con menor probabilidad de ocurrencia (ej. relación con políticas de seguridad) o que no tienen relación con el resto de variables que definen nuestro problema (ej. facturación o número de empleados). Las variables (valores) que por consiguiente hemos seleccionado son las siguientes:

- **TE**: Tipo de Empresa (pequeña, mediana, grande)
- **TA**: Tipo de Activo, (23 en el esquema que define nuestro modelo)
- **A**: Obtención Automática (S/N)
- **NM**: Nivel de madurez (1,2,3)
- **NI**: Número medio de Incidencias por año (%)
- **C**: Coste de obtención (bajo/medio/alto)
- **FM**: Frecuencia de medición (bajo/medio/alto).
- **P**: Peso del indicador en el CMI (1-5)

A partir de la aplicación de la experiencia en nuestros trabajos y la revisión conjunta de nuestro equipo de auditoría, hemos encontrado las siguientes relaciones entre las variables anteriormente descritas:

- $TE \rightarrow NM \rightarrow P$
- $TE \rightarrow NI \rightarrow P$
- $TA \rightarrow A \rightarrow C$
- $TA \rightarrow A \rightarrow P$
- $TA \rightarrow C$
- $TA \rightarrow FM \rightarrow C$

Estas relaciones las hemos reflejado en un grafo que nos va a servir para formar la red de cálculo probabilístico. Dicha red queda representada de forma gráfica en la Figura 6 que se muestra a continuación:

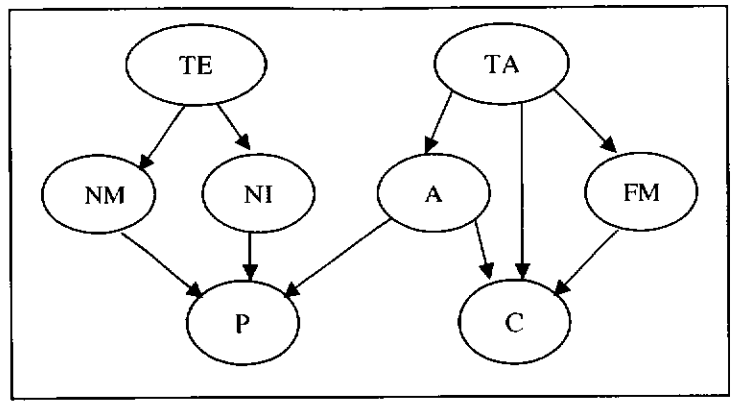

Fig. 6. Red causal para la selección de métricas de seguridad

Inicialmente, para solucionar el problema expuesto decidimos utilizar algoritmos de propagación con métodos exactos mediante agrupamiento, ya que son los que más éxito han tenido en los sistemas expertos de este tipo, y que básicamente consisten en transformar la red en otra estructura gráfica acíclica y no dirigida, cuyos nodos están formados por conjuntos de variables.

Sin entrar en mucho detalle del desarrollo para estos métodos, señalamos que estos algoritmos de agrupamiento se desarrollan en dos fases que con base en la teoría de grafos, tienden a simplificar el cálculo de probabilidades. De esta forma resumida, exponemos las etapas del algoritmo que vamos a emplear:

- **FASE I. Obtención de un árbol de grupos maximales**
  1. Obtención del grafo moral (GM), que es un grafo no dirigido que posee las independencias presentes en el grafo dirigido original
  2. Obtención del grafo triangulado (GT), que se usará para obtener una descomposición en los grupos maximales.
  3. Construcción del árbol de grupos maximales a partir de GT y de la lista de grupos maximales asociada. Con este conjunto C de grupos maximales efectuaremos los cálculos de las propagaciones.
- **FASE II. Cálculo de las probabilidades**
  4. Cálculo de las funciones potenciales, que permitan obtener una factorización de la distribución de probabilidad conjunta a partir del árbol de grupos maximales.
  5. Construcción de una factorización de la distribución de probabilidad conjunta, que se definirá como un producto de las funciones potenciales
  6. Fase de absorción de evidencias, donde se actualizan los potenciales de acuerdo a ellas.
  7. Fase de propagación de la evidencia, que utiliza el árbol de grupos maximales junto a los potenciales asociados a cada uno de ellos.

El objetivo de las fases anteriores es reducir el grafo mediante estructuras intermedias a un árbol de forma que nos facilite el cómputo de probabilidades. De esta forma, una vez que tenemos las distribuciones conjuntas de todos los grupos de la

red podemos calcular la distribución de probabilidad de cada variable eligiendo el grupo de menor tamaño que la contiene y marginalizando la distribución, según vemos en la tabla siguiente:

Variable	*Grupo*	*Probabilidad*
TE	*G1*	*P(TE) = TA, FM P(TE,TA,FM)*
TA	*G1*	*P(TA) = TE, FM P(TE,TA,FM)*
FM	*G1*	*P(FM) = TE, TA P(TE,TA,FM)*
C	*G2*	*P(C) = TE, FM P(TE,FM,C)*
P	*G3*	*P(P) = NM,NI,TE P(NM,NI,P,TE)*
TE	*G4*	*P(TE) = NM,NI P(TE,NM,NI)*
NM	*G4*	*P(NM) = TE, NI P(TE,NM,NI)*
NI	*G4*	*P(NI) = TE,,NM P(TE,NM,NI)*

Tabla 1. Obtención de las probabilidades de cada nodo

A partir de esta red y mediante un cálculo basado en métodos exactos mediante agrupamiento, hay que desarrollar una estructura acíclica que realice la propagación de la evidencia y nos permita realizar el cálculo de probabilidades.

Las variables anteriores están directamente relacionadas con las cinco categorías de nuestro CMI, así como con la aplicación de nuestro modelo de madurez en la empresa, y en el proceso de construcción final que expondremos en detalle en próximos artículos, también tendrá en cuenta:

- Información de las guías y estándares de seguridad
- Ratios *Benchmarck* sobre valores de métricas en otras empresas.
- Información de nuestros clientes acerca de incidencias de seguridad anteriores.
- Información de trabajos de auditoría de seguridad.

Desde una aplicación práctica, hemos comprobado con este método de selección experto y con la supervisión del auditor, que se han conseguido reducir los tiempos de aplicación de nuestro modelo de madurez para la construcción de nuestro CMI para la gestión de la seguridad, logrando ajustar la selección de los indicadores a las características de la empresa y nuestra experiencia anterior.

4. Conclusiones y próximos trabajos

La seguridad no es un producto, sino un proceso continuo que debe ser controlado, gestionado y monitorizado. Como tal la seguridad tiene un objetivo que es garantizar el buen funcionamiento de los procesos de negocio.

La necesidad de medir la Seguridad de los Sistemas de Información de una compañía, nos lleva a la selección de los indicadores adecuados para cada organización y a la construcción de un cuadro de mando comprensible que le permita conocer el estado de la seguridad de la información de la organización.

Los beneficios obtenidos en la utilización de métricas de seguridad en las organizaciones, son evidentes. Los datos recogidos proporcionan una línea base para

valorar fuentes de problemas y riesgos, permitiendo la toma de decisiones para la gestión de riesgos.

En este artículo hemos presentado, desde nuestra experiencia práctica, una primera aproximación a la definición de los indicadores que estamos introduciendo para la implantación de sistemas de gestión de seguridad en PYMES. Hemos revisado los criterios que han influido en la selección de estos indicadores en función de la experiencia práctica con nuestros clientes, y dejamos pendiente profundizar más en las características de las métricas con las que estamos trabajando y la información que nos han aportado para mejorar la gestión de la seguridad de sus SI.

También se ha descrito la posibilidad del uso de Sistema Expertos en la construcción de un CMI totalmente enfocado en PYMES, definiendo un método novedoso con el uso de Redes Bayesianas. Este método que estamos aplicando en nuestros clientes y del que estamos obteniendo unos resultados satisfactorios que permiten optimizar el coste de implantación de los SGSI.

En próximos trabajos iremos refinando estos mecanismos de selección de métricas en base a la experiencia que estamos acumulando y a las nuevas amenazas que surgen cada día en esta área. Expondremos también más detalles de nuestro modelo para la construcción de un CMI adecuado a la seguridad de las TI que las PYMES están demandando.

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. Carrillo Verdún, J. La Gestión de la Seguridad: Métricas e Indicadores. AEMES (Nov.2003)
2. Eloff, J. y Eloff, M. Information Security Management – A New Paradigm. Proc. of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology SAICSIT'03, (2003
3. Erro, G. Seguridad TICs, ¿qué hay que medir?. Aplicabilidad de las Métricas en Seguridad. Jornada Técnica Seguridad Informática.
4. Fernández-Medina, E., Moya, R., Piattini, M. Seguridad de las Tecnologías de la Información. Ediciones AENOR, (2003).
5. Guenther, M. Evaluation, Metrics and Measurement for Security Awareness (2003)
6. Kaplan, R and D. Norton, The balanced scorecard: translating vision into action, Harvard Business School Press, Boston, 1996

7. Hervada F. y Piattini, M. Gobierno de las Tecnologías y Seguridad de la Información. RAMA (2007).
8. Mañas, José A. Security Metrics and Measurements for IT. UPGRADE. August-05.
9. McCarthy,L. La importancia de las métricas de seguridad. Artículos de Seguridad. Symantec Corporation (Dic.2004).
10. NIST Special Publication. Initial Public Draft. Guide to Performance Metrics for Information Security. April 2006.
11. Peltier, T.R. (2003). Preparing for ISO 17799. Security Management Practices.
12. Opacki, D. Security Metrics: Building Business Unit Scorecards. Dic 2005. 4-8
13. Sánchez, L.E., Villafranca, D., Fernández-Medina, E. y Piattini, M. Gestión de la seguridad de los sistemas de información en las empresas desde la perspectiva de su tamaño y nivel de madurez, tomado como base la ISO/IEC 17799. CIASI (2006).
14. Sánchez, L.E., Villafranca, D., Fernández-Medina, E. y Piattini, M Developing a model and a tool to manage the information security in Small and Medium Enterprises. SECRYPT (2007).
15. Villafranca, D., Sánchez, L.E., Fernández-Medina, E. y Piattini, M. Practical Approach of a Secure Management System based on ISO/IEC 17799. Ares (2005)
16. Villafranca, D., Sánchez, L.E., Fernández-Medina, E. y Piattini, M. Gestión de la seguridad de los sistemas de información en las empresas desde la perspectiva de su tamaño y nivel de madurez, tomado como base la ISO/IEC 17799. WOSIS 2006.
17. Villarrubia, C., Fernández-Medina, E. y Piattini, M. Towards a Classification of Security Metrics. Workshop on Security in Information Systems. WOSIS 2004, Oporto, Portugal., pp. 342-350.
18. Van Grembergen, W., De Haes, S. COBIT's Management Guidelines Revisited: The KGIs/KPIs Cascade. Information Systems Control Journal, Volume 6, 2005.
19. Van Grembergen, W., De Haes, S. Using COBIT and the Balanced Scorecard as Instruments for Service Level Management. Information Systems Control Journal, Volume 4, 2003.
20. ITGI, CobiT Control Objetives, 2005.
21. ISO/IEC. International standard iso/iec 17799 (2000). Information technology, 2000.
22. ISO TC JTC1/SC 27 N4188. Information Security Management Metrics and Measurement, 2004.
23. Van der Zee, J. "Alignment is not enough: integrating business and IT management with the balanced scorecard", Proceedings of the 1st Conference on the IT Balanced Scorecard, Antwerp, March 1999.