Actas de la IX Reunión Española sobre Criptología y Seguridad de la Información

Casa de Convalescència, Hospital de la Santa Creu i Sant Pau

7, 8 y 9 de septiembre del 2006, Barcelona

Departament d'Enginyeria de la Informació i les Comunicacions,
Universitat Autònoma de Barcelona
Estudis d'Informàtica, Multimèdia i Telecomunicacions,
Universitat Oberta de Catalunya

Editores
Joan Borrell Viader
Jordi Herrera Joancomartí

Editores: Joan Borrell Viader y Jordi Herrera Joancomartí.
© de los autores.
Primera edición: julio 2006.
ISBN: 84-9788-502-3

Prólogo

Esta publicación recoge las actas de la Reunión Española sobre Criptología y Seguridad de la Información (RECSI), celebrada los días 7, 8 y 9 de septiembre del 2006 en Barcelona.

La RECSI llega en el año 2006 a su novena edición, organizada de forma conjunta por el Departamento de Ingeniería de la Información y de las Comunicaciones de la Universidad Autònoma de Barcelona y el Departamento de Informática y Multimedia de la Universidad Oberta de Catalunya. Esta IX RECSI quiere seguir siendo el lugar de encuentro y el foro en el que los criptólogos y, en general, todos aquellos que trabajan en el campo de la Seguridad de la Información expongan sus hallazgos y debatan sus ideas. Se trata de un congreso bienal que se celebra en universidades y centros de investigación de España. Las ediciones anteriores se llevaron a cabo en Palma de Mallorca (U. Illes Balears), Madrid (CSIC), Barcelona (U. Politècnica de Catalunya), Valladolid (U. de Valladolid), Torremolinos (U. de Málaga), Santa Cruz de Tenerife (U. de La Laguna), Oviedo (U. de Oviedo) y Leganés (U. Carlos III).

La expansión de Internet, el incremento exponencial del volumen de datos automatizados que se maneja, la creciente inquietud por la protección de la intimidad y, en general, la entrada en la era de la información hace que la seguridad de ésta se configure como un campo de singular importancia, y por ello concentre un especial interés por parte de las empresas, las administraciones, los profesionales y más ampliamente, la sociedad entera. Por otro lado, la Criptología, en su doble vertiente de diseño de algoritmos criptográficos y de análisis de sus posibles debilidades, se ha convertido en la disciplina vertebral de la seguridad, habiendo abandonado los círculos impenetrables en los que se desplegaba históricamente, para ser tratada en universidades, centros de investigación, empresas y organismos de todo tipo interesados en proteger las informaciones que manejan.

Conscientes de lo anterior, en la IX RECSI se tratan y profundizan los aspectos de estas materias que más despiertan la atención en estos días, así como otros, aún en investigación, pero que están llamados a ser de capital importancia en los sistemas y mecanismos de seguridad en un inmediato futuro. A lo largo de las tres jornadas que conforman la Reunión se presentan 63 comunicaciones en 18 sesiones paralelas. Queremos agradecer desde estas líneas el trabajo realizado por el Comité Científico y los revisores en el proceso de revisión.

La IX RECSI, buscando mantener un elevado nivel académico y también un adecuado nivel de contacto de la comunidad investigadora con las empresas y la sociedad, incluye también:

- Tres conferencias magistrales a cargo de investigadores de reconocido prestigio en el ámbito de la Criptología y la Seguridad de la Información, el Dr. Moni Naor, del Weizmann Institute of Science (Israel), el Dr. Frédéric Cuppens de la Escuela Normal Superior de Telecomunicaciones de Bretaña

(Francia) y el Dr. Gene Tsudik de la Universidad de California en Irvine (USA).

- Dos presentaciones de empresas, Safelayer Secure Communications, compañía líder en el mercado de seguridad y confianza para las TIC, desarrollando tecnología de identificación electrónica, firma electrónica y protección de datos basada en Infraestructura de Clave Pública (PKI), y Scytl Secure Electronic Voting, compañía líder en el desarrollo de plataformas de votación electrónica seguras y confiables, aplicables desde procesos electorales clásicos a juntas generales de accionistas.
- La presentación de la Unidad Central de Informática Forense de la Policía de la Generalitat de Catalunya - Mossos d'Esquadra.

Manifestar también nuestro agradecimiento por la ayuda financiera y de difusión recibida de los distintos patrocinadores, cuya relación aparece en la página de agradecimientos de estas actas.

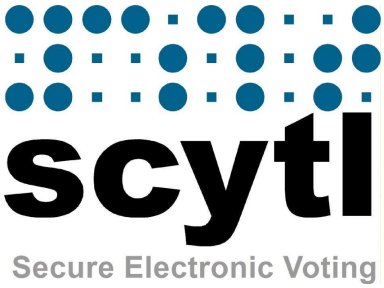
No quisieramos finalizar este prólogo sin recordar a nuestro amigo Andreu Riera Jorba, participante en varias Reuniones, tristemente fallecido en accidente de coche el 11 de marzo de 2006. Andreu, doctor por la UAB, era conocido tanto por su valiosa aportación en el campo de la criptografía aplicada al voto electrónico, como por su espíritu emprendedor que le llevó a fundar Scytl Secure Electronic Voting, empresa de la cual era Consejero Delegado.

Septiembre 2006

Joan Borrell Viader
Jordi Herrera Joancomartí

Agradecimientos

Los organizadores de la RECSI quieren agradecer a los patrocinadores de la Reunión su apoyo logístico y económico.



Organización

La IX RECSI ha sido organizada conjuntamente por el Departament d'Enginyeria de la Informació i les Comunicacions de la Universitat Autònoma de Barcelona y los Estudis d'Informàtica, Multimèdia i Telecomunicacions de la Universitat Oberta de Catalunya.

Comité ejecutivo

Joan Borrell Viader
Jordi Herrera Joancomartí
Josep Rifà Coma

Comité científico

Abascal Fuentes, Policarpo (U. de Oviedo)
Arranz Chacón, Maria Luisa (Alcatel)
Areitio Bertolín, Javier (U. de Deusto)
Borrell Viader, Joan (U.Autònoma de Barcelona)
Caballero Gil, Pino (U. de La Laguna)
Dávila Muro, Jorge (U. Politécnica de Madrid)
Domingo-Ferrer, Josep (U. Rovira i Virgili)
Fernández-Medina Patón, Eduardo (U. de Castilla La Mancha)
Ferrer Gomila, Josep Lluis (U. de les Illes Balears)
Fúster Sabater, Amparo (CSIC)
Gómez Skarmeta, Antonio (U. de Múrcia)
González Jiménez, Santos (U. de Oviedo)
Guía Martínez, Dolores de la (CSIC)
Gutiérrez Gutiérrez, Jaime (U. de Cantabria)
Herrera Joancomartí, Jordi (U. Oberta de Catalunya)
Huguet Rotger, Llorenç (U. de les Illes Balears)
López Muñoz, Javier (U. de Málaga)
Martín del Rey, Angel (U. de Salamanca)
Mañas Argemí, José Antonio (U. Politécnica de Madrid)
Miret Biosca, Josep Maria (U. de Lleida)
Padró Laimon, Carles (U. Politècnica de Catalunya)
Peinado Domínguez, Alberto (U. de Málaga)
Ramió Aguirre, Jorge (U. Politécnica de Madrid)
Ramos Álvarez, Benjamín (U. Carlos III de Madrid)
Ribagorda Garnacho, Arturo (U. Carlos III de Madrid)
Rifà Coma, Josep (U. Autónoma de Barcelona)
Robles Martínez, Sergi (U. Autónoma de Barcelona)

Salazar Riaño, Jose Luís (U. de Zaragoza)
Sempere Luna, José Maria (U. Politécnica de Valencia)
Soriano Ibáñez, Miquel (U. Politècnica de Catalunya)
Rifà Coma, Josep (U. Autònoma de Barcelona)
Tena Ayuso, Juan (U. de Valladolid)
Villar Santos, Jorge (U. Politècnica de Catalunya)

Comité Organizador

Joan Arnedo (Universitat Oberta de Catalunya)
Carles Garrigues (Universitat Autònoma de Barcelona)
David Megías (Universitat Oberta de Catalunya)
Alvaro Moratalla (Universitat Autònoma de Barcelona)
Guillermo Navarro (Universitat Autònoma de Barcelona)
Josep Prieto (Universitat Oberta de Catalunya)
Segi Robles (Universitat Autònoma de Barcelona)
Jordi Serra (Universitat Oberta de Catalunya)
Pere Urbón (Universitat Autònoma de Barcelona)

Revisores

Guillermo Azuara Guillén
Óscar Cánovas Reverte
Jordi Castellà Roca
Sergio Castillo Pérez
Vanesa Daza Fernández
Oscar Esparza Martín
Juan M. Estévez Tapiador
Joaquín García Alfaro
Félix J. García Clemente
Maria Isabel González Vasco
Julio César Hernández Castro
Gabriel López Millán
Consuelo Martínez López
Antoni Martínez Ballesté
Gregorio Martinez Perez
José Luis Muñoz-Tapia
Josep Pegueroles
Joan Josep Piles Contreras
Helena Rifà Pous
Francesc Sebé Feixas
Agusti Solanas Gómez

Índice general

Sesión C1

Sesión S1

Sesión C2

Sesión S2

Sesión C3

Sesión S3

Sesión C4

Sesión S4

Sesión C5

Sesión S5

Sesión S6

Sesión S7

Sesión C6

Sesión S8

Sesión S12

Desarrollando un Modelo de Madurez para la Gestión de la Seguridad de los Sistemas de Información en las PYMES

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

[1] SICAMAN Nuevas Tecnologías. Departamento de I+D
Juan José Rodrigo, 4. Tomelloso, Ciudad Real, España Universidad
lesanchez, dvillafranca@sicaman-nt.com
[2] Castilla-La Mancha, Grupo de Investigación Alarcos,
Departamento de Tecnologías y Sistemas de Información
Paseo de la Universidad 4 - 13071, Ciudad Real, España.
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 la seguridad adecuado, pero esto requiere que las empresas conozcan en todo momento su nivel de madurez de seguridad actual y hasta qué punto debe evolucionar su seguridad. Los modelos de madurez actuales se están mostrando ineficientes en las pequeñas y medianas empresas, las cuales cuentan con una serie de problemas adicionales a la hora de implantar sistemas de gestión de la seguridad. En este artículo realizamos un análisis de los modelos de madurez orientados a la seguridad que existen en el mercado, analizando sus principales inconvenientes en las PYMES y mostramos nuestra propuesta, un nuevo mode-lo orientado a las PYMES utilizando como marco de referencia la norma ISO/IEC 17799. Este enfoque está siendo aplicado directamente a casos reales, consiguiendo así una constante mejora en su aplicación.

1. Introduction

La información y los procesos que apoyan los sistemas y las redes son los activos más importantes para cualquier organización [1], y suponen el principal factor dife-renciador 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 [2]. De esta forma, el CGI/FBI Computer Crime and Security Survey [3] estima que el total de perdidas en los EEUU en el 2004 como resultado de las brechas de seguridad fue de 141.496.560$. Pero la mayor parte de las pérdidas no se conocen, ya que la falta de controles adecuados para realizar el seguimiento de la información imposibilita a las empresas el conocer la existencia de fugas de información, y por tanto poder cuantificuantificar el coste de las mismas.

Las organizaciones, sin importar su tamaño o actividad, se ven en la necesidad de implementar un Sistema de Gestión de la Seguridad de la Información (SGSI) para proteger sus activos más sensibles [4][5], pero para desarrollar estos SGSI no basta con afrontar solo aspectos tecnológicos [6], sino que también es necesario desarrollar aspectos de gestión, así como los aspectos legales y éticos.

De cualquier forma aunque están surgiendo muchas normas nuevas, la tendencia actual [7] para afrontar un SGSI es conseguir homogeneizar algunos de sus aspectos básicos, como son los modelos de madurez y las guías de buenas prácticas, en un conjunto estable que permita poder afrontar cada caso con el modelo de SGSI que mejor se adapte.

Como núcleo de la nueva orientación de la seguridad como sistema de gestión, se han creado políticas de seguridad que contienen conjuntos de reglas y regulaciones para determinar cómo debe protegerse una organización [8]. Así Cabrera Martin [9] plantea que la forma para acometer la planificación de la seguridad en una organización debe partir siempre de la definición de una Política de Seguridad que determine lo que se quiere hacer en materia de seguridad en la organización para a partir de ello decidir mediante un adecuado plan de implementación cómo se alcanzarán los objetivos fijados.

Antes de iniciar un proyecto de implantación de un sistema de gestión de seguridad de la información en una compañía, es necesario determinar el nivel en que se encuentra el Gobierno de Seguridad de la Información de la compañía, ya que la ausencia de éste garantiza el fracaso de la gestión de la seguridad. No es viable comenzar la implantación de un sistema de gestión de seguridad de la información en ausencia de un gobierno de seguridad de la información estable y definido [10]. El siguiente paso para la implantación de un SGSI es establecer el nivel de madurez de seguridad de la compañía y hacia donde debe evolucionar, aunque estos niveles de madurez pueden ser establecidos de diferentes formas. Así Von Solms [11] ve la seguridad como una disciplina de múltiples dimensiones que deben ser cubiertas para obtener un plan de seguridad, mediante una certificación incremental de la seguridad, para Von Solms la fase más importante del plan es determinar el nivel de madurez del SGSI de la empresa y comparar ese nivel con las perdidas que puede ocasionar en el negocio. Nuestra propuesta de modelo de madurez plantea una evolución de los niveles de madurez parecida en algunos aspectos a la planteada por Von Solms, de tal forma que las empresas podrán certificarse en los diferentes niveles de madurez del modelo, lo que les supondrá afrontar proyectos con una visión temporal más corta y poder analizar antes los resultados del plan.

Actualmente es muy complejo para una pequeña o mediana empresa abordar la implantación de un sistema de gestión de seguridad. La tendencia en materia de seguridad de las empresas es ir migrando poco a poco su cultura hacia la creación de un SGSI, aunque esta progresión es muy lenta, de tal forma que René Sant-Germain [3] estima que con los modelos actuales en el 2009 tan solo 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.

La mayor parte de las compañías han encontrado muchos problemas a la hora de implantar sistemas como la certificación BS7799 y las UNE71502, ya que son certificaciones totales, lo que impide a la compañía tener puntos intermedios en los que centrar el alcance de sus objetivos, y a los departamentos de sistemas obtener éxitos

intermedios que les permitan obtener el apoyo de la dirección. El modelo de madurez que planteamos permite la obtención de certificaciones intermedias, pudiendo afrontar cada nivel de madurez en periodos de 1 a 2 años en lugar de los 3 a 6 años que se necesitan actualmente en una empresa mediana. La auditoría, certificación y acreditación del sistema de gestión es importante para proporcionar credibilidad al entorno de seguridad, a los clientes y a los proveedores. Por eso nuestra propuesta de modelo de madurez está basada en la certificación por niveles y no en una sola certificación total. Nuestro modelo de madurez propone dividir la certificación UNE71502 y la ISO27001 en tres niveles de certificación [1 a 3], cada uno de los cuales cuenta con un subconjunto de controles sacados de los ISO/IEC 17799.

En el presente articulo se propone un modelo de madurez orientado a las PYMES que pretende solucionar los problemas detectados en los modelos clásicos de madurez, los cuales no se están mostrando eficientes a la hora de su implantación en las PYMES debido a su complejidad y otras serie de factores que serán analizados con detalle en la siguientes secciones del artículo.

El artículo continúa en la Sección 2, describiendo 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. Finalmente, en la Sección 4 concluimos indicando cuál será el trabajo que desarrollaremos en el futuro.

2 Trabajo relacionado.

Los Modelos de Madurez de Seguridad 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. Estos niveles de madurez serán progresivos, de tal forma que la seguridad de la información implementada aumente conforme se incrementan los niveles de madurez. Estos niveles son el mecanismo ideal para conocer la seguridad de las compañías que se quieren analizar, y de terceras compañías con las que esta tenga que interactuar. El problema, es que aunque existen modelos de madurez en el mercado, tan solo existen certificaciones de seguridad totales, lo que impide a muchas compañías poder tener una valoración de su nivel de madurez actual. Por eso nuestro modelo sugiere la certificación por niveles de madurez, en lugar de la certificación única que existe en la actualidad, esta certificación será revisada periódicamente y la compañía podrá subir o bajar su nivel de madurez. Este modelo coincide con las apreciaciones de Eloff y Eloff [5], el cual sugiere ir realizando una implantación progresiva de controles que permita que la empresa pueda irse adaptando a la evolución de la seguridad de una forma no traumática.

La visión de cómo afrontar estos niveles de madurez, difiere según los autores que se tomen como referencia. De esta forma algunos autores, insisten en utilizar la 17799 en modelos de gestión de seguridad, pero siempre haciéndolo de manera incremental, considerando las necesidades particulares de seguridad [11], usando para ello los modelos de madurez. Otros modelos como el Information Security Institute of South Africa (ISIZA) [11] plantea también un incremento progresivo de la seguridad. El

Nivel 1 de ISIZA consiste en la selección de un nivel básico de un pequeño subconjunto de controles de la ISO7799 relacionados con la política de seguridad, control de virus y seguridad del personal. Siguiendo el modelo propuesto por ISIZA se han conseguido reducciones de tiempo a la hora de certificar a las compañías con la norma BS7799 [11].

Para nuestro modelo de madurez se ha utilizado el estándar ISO17799 como punto de partida, coincidiendo con las investigaciones que la universidad de Pittsburgh está emprendiendo para el desarrollo y la puesta en práctica de un estándar comprensivo de la seguridad basada en las guías proporcionadas por la ISO/IEC 17799 [12]. Otros estudios consideran importante la norma, pero la complementan de alguna forma con otros aspectos [13], como es el caso de Endorf [14], que incorpora los requisitos de la HIPAA norteamericana a un programa de seguridad complementando la ISO/IEC 17799; Von Solms [15], que considera una aplicación conjunta y complementaria de los COBIT y la norma; o incluso Masacci [16], que además de la norma considera controles relativos al cumplimiento de la legislación italiana en materia de protección de datos y privacidad.

Otros de los aspectos que se están estudiando para su aplicación a los modelos de madurez es la gestión de los costes asociados a la gestión de la seguridad, ya que estos pueden influir en el dimensionamiento del modelo. De esta forma Rebecca Mercuri [17] propone asociar como parte fundamental del desarrollo de los SGSI los análisis de coste-beneficio (CBA) en la fase del análisis de riesgos; Kim&Choi [18] analiza una metodología orientada a modelos de procesos y criterios de análisis de factores de coste y beneficio que soporten la justificación económica de la inversión en seguridad y que puede ser aplicada a estimar el nivel máximo de madurez que debe afrontar la empresa; y Peltier [13] plantea que los controles deben ser seleccionados en base al coste-efectividad en relación con el riesgo que reducen y las perdidas potenciales que las brechas de seguridad pueden ocasionar.

2.1. Otros Modelos de Madurez de Seguridad

Entre los modelos de madurez para seguridad de la información [19] que más se están aplicando en las empresas actualmente, destacan el SSE-CMM, COBIT y el ISM3 [20], aunque actualmente se están desarrollando nuevos modelos de madurez que intentan solucionar los problemas detectados en estos modelos. A continuación se muestra una descripción breve de los principales modelos de madurez existentes en la actualidad y algunas de las propuestas más prometedoras:

- **ISO 21827/SSE-CMM:** El Modelo de Capacidad y Madurez en la Ingeniería de Seguridad de Sistemas es un modelo derivado del modelo de madurez del software CMM y orientado hacia la seguridad, que describe las características esenciales de los procesos que deben existir en una organización para asegurar una buena seguridad en los sistemas. En Lobree 2002 [21] se comparan las guías de buenas prácticas más importantes con el modelo de madurez SSE-CMM, llegando a la conclusión de que todas consideran básicamente los mismos aspectos de seguridad, pero con diferente nivel de profundidad.

- **ISM3 [12]:** Está orientado a definir diferentes niveles de seguridad donde cada uno de ellos puede ser el objetivo final de una organización. En otras palabras, no es un modelo que se pueda utilizar para mejorar, sino que sirve para clasificar el nivel de seguridad que requiere una empresa. ISM3 define cinco niveles de madurez de la seguridad de una empresa [0 a 4]. Estos niveles irán asociados a procesos de tal forma que, dependiendo del nivel de madurez, la empresa estará obligada a cumplir con una serie de procesos. De esta forma, un nivel 0 implicará no cumplir con ningún proceso.
- **COBIT:** El modelo de madurez de COBIT [19] ofrece las bases para el entendimiento y la evaluación de las condiciones actuales de seguridad y control de los procesos del ambiente de TI de una organización. Este modelo provee las bases para la evaluación de las principales funciones del área de TI, a través de la consideración de cada uno de sus procesos clave, a los cuales se les asignará un valor entre [0-5], indicando así el nivel de esfuerzo ("madurez") que se sugiere invertir en la actividad de control de dicho proceso, de forma de garantizar una buena relación costo beneficio al asegurar el nivel de seguridad estrictamente requerido. El modelo de madurez de COBIT está basado en el modelo de madurez de desarrollo de software CMM-SW, lo que hace que éste no sea un modelo actualizado, ya que hoy en día lo que se está manejando es el modelo CMMI. Von Solms [13] [15] ha investigado la coexistencia y uso complementario de COBIT y la ISO 17799 desarrollando un mapa para la sincronización de ambos marcos de referencia y analizando las razones por las que ambos son complementarios. Algunos de los detractores de la ISO17799 presentan como desventaja que es una guía de soporte, pero que no alcanza todo el marco necesario para el gobierno de las tecnologías de la información. Su principal ventaja frente a COBIT es que es más detallada y tiene más guías orientadas a como deben hacerse las cosas. Un reciente informe del IT Governance Institute soluciona el problema de sincronización desarrollando el mapa entre COBIT´s DCO´s e ISO/IEC17799:2000. Existen multitud de escenarios [11] en que se pueden usar ISO 17799, Common Criteria y COBIT.
- **CC_SSE-CMM:** El Common Criteria (CC) provee sólo de estándares para evaluar la información de productos o sistemas de seguridad. Por otra parte SSE-CMM provee de estándares de seguridad para la evaluación de la ingeniería de procesos. Jongsook Lee [7] propone integrar CC y SSE-CMM para crear CC-SSE-CMM, que es un modelo de madurez con las ventajas de ambos modelos. Este nuevo modelo se divide en procesos, productos y ambiente. Las ventajas de este modelo son que es útil cuando una organización que fue desarrollada con el CC desea ser evaluada con SSE-CMM para mejorar su nivel con respecto al proceso de seguridad, y viceversa. CC_SSE-CMM consiste en 23 áreas de procesos con 5 niveles de madurez. Cada área de proceso (PA) tiene BP (prácticas base) y los niveles de capacidad tienen GP (prácticas genéricas).
- **Eloff y Eloff [5]:** Se decanta por definir cuatro clases distintas de protección, que permiten ir incrementando de forma progresiva los niveles de seguridad, basándose para ello en las secciones de la norma ISO17799.
- **Karen & Barrientes [22]:** Esta propuesta de Modelo de Madurez consiste en llevar a cabo un análisis relativo a la seguridad informática para identificar el

grado de vulnerabilidad y determinar los aspectos de mejora a ser llevados a cabo en la organización con el objeto de reducir el riesgo. Este modelo apoya la evaluación de la seguridad de la información de una organización, y permite determinar en qué nivel se encuentra la misma con respecto a la seguridad, y así poder establecer cuáles son sus fortalezas y debilidades a la hora de proteger su información. El modelo propuesto cuenta con los 5 niveles planteados por el CMMI, con su debida adaptación para que esté acorde con la seguridad de la información. Cada nivel cuenta con una definición y con una descripción general en la cual se indica el comportamiento que tiene una organización con respecto a la seguridad de la información. Dicho comportamiento determina el nivel de madurez en el que se encuentra la seguridad de la información. Las prácticas de cada nivel corresponden a los controles que están definidos en el estándar internacional ISO/IEC 17799-2000 [23]. Este modelo tiene en cuenta que las organizaciones tienen estructuras internas diferentes, por lo cual se considera que los controles definidos en cada nivel son los mínimos o más generales que deberían establecer las organizaciones, cualquiera que fuera su estructura interna.

El problema principal de todos los modelos de madurez presentados, es que no están teniendo éxito a la hora de implantarse en PYMES, debido principalmente a que fueron desarrollados pensando en organizaciones grandes y en las estructuras organizativas asociadas a estas.

3 SSE-PYME: Modelo de Madurez de la Seguridad Orientado a 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, ya que son las que mayor tasa de fracaso en la implantación de los SGSI están teniendo y con las que menos éxito están teniendo los modelos de madurez existentes. Además, las PYMES representan más del 95% de las empresas Españolas, lo que supone que hasta que no se consiga un adecuado nivel de seguridad en ese tipos de empresas, el tejido empresarial Español no podrá considerarse maduro desde el punto de vista tecnológico. Las características más destacadas de nuestro modelo son que tiene tres niveles de seguridad [1 a 3] en lugar de los 5-6 niveles que proponen los modelos clásicos y que se propone que cada nivel sea certificable, en lugar de la certificación total existente hasta el momento, por último, se asocia el nivel de madurez a las características de la empresa, no siendo obligatorio (ni aconsejable en algunos casos), que todas las compañías lleguen al nivel 3.

De esta forma y a partir de la información obtenida mediante la implantación en clientes de SICAMAN, se ha desarrollado un modelo de madurez siguiendo la estructura en espiral que podemos ver en la Fig.1. 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 pueden determinar un plan de proyecto que pre-

sentar a la dirección de la empresa. Otra de las características del modelo que proponemos, es que el modelo busca que los planes propuestos sean a corto plazo, en lugar de los planes derivados de los modelos actuales que tienen una duración elevada, lo cual hace que sean totalmente inadecuados para la estructura cambiante presente en las PYMES.

Mediante este modelo, podemos estimar en un plazo mínimo de tiempo el nivel de madurez del SGSI de la empresa e identificar el conjunto de normas que más se adapta a ella, trazando hitos realistas a corto plazo de la evolución esperada en la empresa para cada ciclo de la espiral. Una vez que hayamos identificado el nivel de madurez actual de la empresa, se elaborara un plan de mejora que será presentado a la dirección y cuyo principal objetivo, será complementar el nivel de madurez actual para llegar al siguiente nivel de madurez.

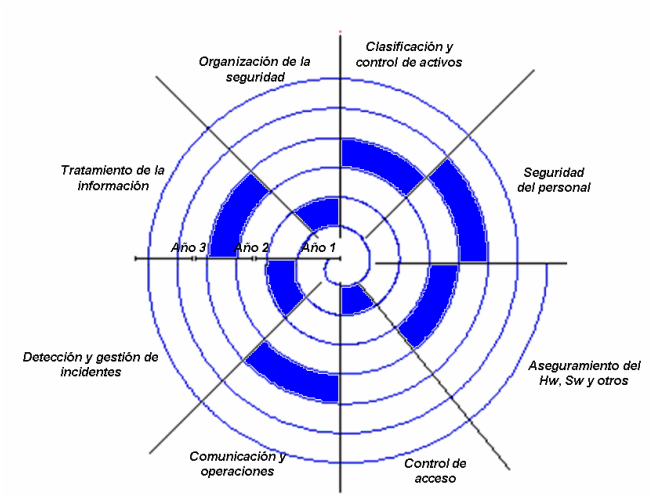


Fig. 1. Modelo en espiral para madurez de los SGSI.

Aunque en la Fig.1 el modelo de madurez presenta solo ocho secciones de la norma ISO17799, el modelo de madurez final se está desarrollando sobre las diez secciones presentes en esta norma. Actualmente se están analizando las posibilidades de migrar los resultados obtenidos mediante el método investigación-en-acción a la nueva versión de la norma ISO17799:2005. Además, aun cuando el núcleo principal del modelo que hemos desarrollado, está basado en la ISO/IEC 17799, no hemos renunciado a complementarlo con otro tipo de estándares y recomendaciones en materia de seguridad y de gestión de seguridad, que puedan solucionar carencias detectadas en la ISO17799 y que han sido analizadas en la Sección 2 del presente articulo.

Nuestro modelo define tres niveles de madurez para valorar el estado de la seguridad del sistema de información de la empresa. De esta forma, una empresa que según los parámetros de empleados y facturación se considere pequeña sólo debería aplicar el nivel de madurez ISO17799-1 que es un subconjunto de los controles recomendados por la ISO17799 (Tabla 1). Cualquiera de las otras dos versiones de la norma supondría sobredimensionar la seguridad de la empresa. Esto conllevaría un aumento

del nivel de riesgo de que los controles implantados no sean sostenibles y produciría una degradación continua de los controles y del nivel de madurez. Otro factor a tener en cuenta, es que aún cuando las diferentes secciones podrían avanzar de forma independiente, lo lógico es que planifiquemos mejorar aquellos aspectos que necesitan una menor seguridad.

Como primer paso para poner en marcha nuestro modelo en una compañía, determinaremos qué nivel de normas deberemos aplicar en base a las características de la empresa. Una vez identificado el nivel apropiado realizaremos un análisis de controles para determinar el plan que nos permita complementar ese nivel de madurez. En nuestro modelo el nivel de seguridad de la compañía, evolucionará en un rango del 0-100% para cada uno de los tres niveles de madurez propuestos, a su vez cada nivel de madurez ha sido dividido en seis subniveles para ayudar a la dirección en el seguimiento del proyecto.

Nivel de madurez (Según pre-auditoria realizada sobre la norma ISO17799)		**Tipo de Empresa (según nº de empleados y facturación)**		
Valoración	**Nivel de madurez**	**Pequeña**	**Mediana**	**Grande**
		0 – 25 Empleados	25 – 250 Empleados	>250 Empleados
		0 – 1 Millones €	1 – 100 Millones €	>100 Millones €
0 – 100%	Bajo	ISO17799-1 (100)	ISO17799-1 (100)	ISO17799-1 (100)
100% - 200%	Medio	ISO17799-1 (100)	ISO17799-2 (300)	ISO17799-2 (300)
200 - 300%	Alto	ISO17799-1 (100)	ISO17799-2 (300)	ISO17799-3 (500)

Tabla 1. Modelos propuestos según el tipo de empresa y su nivel de madurez**.**

Algunas de las principales y más valiosas conclusiones obtenidas de la realimentación de los clientes de SICAMAN en los que se han analizado estos modelos son las siguientes:

- El sobredimensionamiento del nivel de seguridad de una empresa con respecto a su tamaño termina produciendo una degradación de los controles sobredimensionados, hasta que éstos alcanzan su equilibrio natural. La consecuencia final de esto es que la empresa invierte un mayor número de recursos de los estrictamente necesarios, que no aportarán valor alguno. En la Fig. 2, podemos ver una simulación de cómo, según el tamaño de la empresa, existe una tendencia natural de los sistemas de seguridad a encontrar su equilibrio, es decir, como el sobre-dimensionamiento de las medidas de seguridad aplicadas en una empresa, supone una perdida económica para la misma, ya que la propia estructura de la empresa termina rechazando ese sobre-esfuerzo en la seguridad, del cual no se obtiene retorno de inversión.

  En la Fig.2 el porcentaje de 0-100% (también se puede denominar 0-100% Nivel1) representa el nivel de madurez 1, el porcentaje 100-200% representa el nivel de madurez 2 (también se puede denominar 0-100% Nivel2) y el porcentaje de 200-300% (también se puede denominar 0-100% Nivel3) representa el nivel de madurez 3. Existen excepciones en algunos sectores y tipos de

empresas en las que no se cumple esta tendencia, por lo que se esta realizando mejoras en el modelo añadiendo variables al mismo.

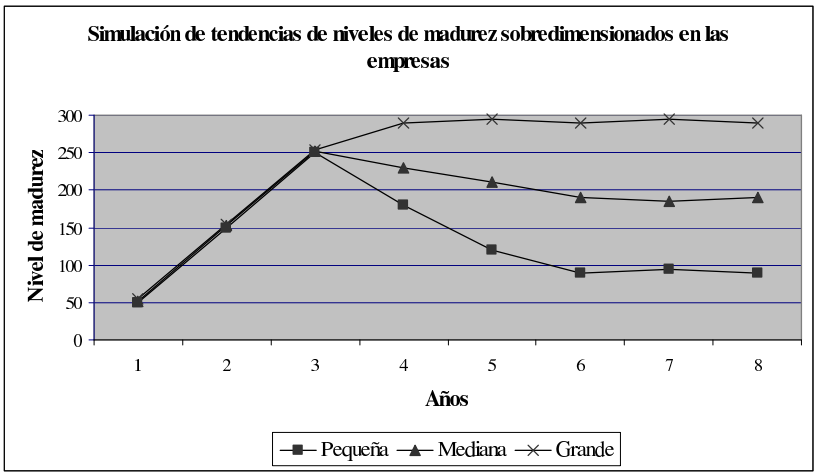


Fig. 2. Simulación de tendencia de niveles de madurez sobredimensionados.

- Las empresas se muestran más receptivas ante planes de implantación de corto plazo (1 a 2 años) que ante planes a largo plazo (4 a 6 años). La certificación por niveles ofrece una garantía para la valoración de la evolución del proyecto a corto plazo.

Otros modelos en los que actualmente estamos trabajando incluyen nuevos factores que pueden afectar a la hora de decidir sobre el nivel de cumplimiento que se debe aplicar: el tipo de actividad de la empresa, la dependencia de departamentos (como el de I+D), etc.

4 Conclusiones y Trabajos Futuros

A pesar de los enormes esfuerzos que se están realizando para crear modelos de madurez adecuados para mediar y gestionar la seguridad en las PYMES, éstos no terminan de encajar con el entorno en que deben ser implantadas. La causa más probable es la falta de madurez de las empresas y 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 empleando 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, aunque supone un punto de partida muy bueno para el desarrollo de nuevos modelos de madurez.

En este artículo nosotros presentamos, desde nuestra experiencia práctica, una primera aproximación al desarrollo de un nuevo modelo de madurez orientado a las PYMES, que toma como base o marco de referencia la norma tan mencionada en este artículo, adaptándola para ajustarla al tamaño de la empresa en que se desee implantar y a su nivel de madurez. Este modelo esta siendo desarrollado tomando como base los modelos de madurez existentes en la actualidad, analizando sus principales desventajas y probándolos en nuestros clientes para determinar los factores de éxito y fracaso del modelo.

El modelo de madurez presentado reduce los costes de implantación de los sistemas y mejora el porcentaje de éxito de las implantaciones.

Puesto que esta propuesta es muy preliminar, nuestro objetivo a medio y largo plazo es profundizar en los modelos de madurez para acometer el desarrollo completo de un nuevo modelo de madurez que suponga un mayor porcentaje de éxito en las PYMES. Mediante el método de investigación "investigación en acción", con la ayuda de la retroalimentación obtenida directamente de nuestros clientes, esperamos conseguir una mejora continua de estas implantaciones.

Este modelo de madurez, y la metodología de la que forma parte, se verán complementados con una herramienta de gestión de sistemas de seguridad, orientada principalmente a la gerencia, para facilitar la toma de decisiones a la hora de realizar las planificaciones de los sistemas de seguridad.

Agradecimientos.

Esta investigación es parte de los proyectos DIMENSIONS, parcialmente financiado por el FEDER y por la Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha (PBC-05-012-1), CALIPO (TIC2003-07804-C05-03) y RETISTIC (TIC2002-12487-E) concedidos por la "Dirección General de Investigación del Ministerio de Ciencia y Tecnología" (España).

Referencias

1. Dhillon, G. y Backhouse, J. Information System Security Management in the New Millennium, Communications of the ACM, (2000) 43(7).
2. Computer Security Institute – CSI. Computer Crime and Security Survey. (2002)
3. René Sant-Germain. Information Security Management Best Practice Based on ISO/IEC 17799. Setting Standars, The information Management Journal – July/August 2005.
4. María Eugenia Corti, Gustavo Betarte, and Reynaldo de la Fuente. Hacia una implementación Exitosa de un SGSI. 3er Congreso Iberoamericano de seguridad Informática, Nov, (2005).
5. 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) 130-136.

6. Tsujii, S. Paradigm of Information Security as Interdisciplinary Comprehensive Science. Proc. of the 2004 International Conference on Cyberworlds (CW'04), IEEE Computer Society, (2004) 1-12.
7. Jongsook Lee, Jieun Lee, Seunghee Lee and Byoungju Choi. A CC-based Security Engineering Process Evaluation Model. Proceedings of the 27th Annual International Computer Software and Applications Conference (COMPSAC`03)
8. Rodriguez, Luis Ángel. Seguridad de la Información en Sistemas de Computo. Ventura Ediciones, México, (1995).
9. Cabrera Martin, Álvaro. Políticas de Seguridad. Boletín del Criptonomicón #71.Madrid, (2000).
10. Isg, Information Security Governance a call to action, Abril 2004.
11. Von Solms, B. y Von Solms, R. Incremental Information Security Certification. Computers & Security 20, (2001) 308-310.
12. Walton, J.P. Developing an Enterprise Information Security Policy. Proc. of the 30th annual ACM SIGUCCS conference on User services, (2002) 153-156.
13. Peltier, T.R. Preparing for ISO 17799. Security Management Practices, jan/feb, (2003) 21-28.
14. Endorf, C. Outsourcing Security: The Nedd, the Risks, the Providers, and the Process. Information Security Management, (2004) 17-23.
15. Von Solms, B. Information Security governance: COBIT or ISO 17799 or both? Computers & Security 24, (2005) 99-104.
16. Masacci, F., Prest, M., Zannone, N. Using a security requirements engineering methodology in practice: The compílanse with the Italian data protection legislation. Computer Standards & Interfaces 27, (2005) 445-455.
17. Rebecca T. Mercuri. Analyzing Security Costs. Communications of the ACM, June 2003/vol.46, nº 6.
18. S. Kim and I.Choi. Cost-Benefit Análisis of Security Investments: Methodology and Case Study. P. Gervasi et al. (Eds.): ICCSA 2005, LNCS 3482, pp. 1239 – 1248, 2005.
19. Karen A. Areiza, Andrea M. Barrientos, Rafael Rincón, and Juan G. Lalinde-Pulido. Hacia un modelo de madurez para la seguridad de la información. 3er Congreso Iberoamericano de seguridad Informática, Nov, (2005).
20. Vicente Aceituno. Ism3 1.0: Information security management matury model, 2005. 12 Karen A. Areiza et al.
21. Bruce A. Lobree, CISSP. Impact of legislation and information security management. Security Management Practices, November/December 2002
22. Andrea M. Barrientos Karen A. Areiza. Integración de un sistema de gestión de seguridad de la información conun sistema de gestión de calidad. Master's thesis, Universidad EAFIT, 2005.
23. ISO/IEC. International standard iso/iec 17799 (2000). information technology - code of practice for information security management, 2000.