Patrocinadores

Ministerio de Educación y Ciencia · Zaragoza Ayuntamiento · Ministerio de Industria, Turismo y Comercio · Universidad de Zaragoza · Sun · Telefónica · Expo Zaragoza 2008 · Gobierno de Aragón, Departamento de Ciencia, Tecnología y Universidad

Entidades Organizadoras

- AdaSpain.
- Asociación de Enseñantes Universitarios de la Informática (AENUI).
- Asociación de Técnicos Informáticos (ATI).
- Asociación Española para la Inteligencia Artificial (AEPIA).
- Asociación para la Interacción Persona-Ordenador (AIPO).
- Asociación para el Desarrollo de la Informática Educativa (ADIE).
- Ayuntamiento de Zaragoza.
- Capítulo Español de la IEEE Computational Intelligence Society.
- Comité Español de Automática (CEA).
- Conferencia de Decanos y Directores de Informática (CODDI) de las Universidades Españolas.
- Departamento de Informática e Ingeniería de Sistemas de la Universidad de Zaragoza.
- European Society for Fuzzy Logia and Technology (EUSFLAT).
- Federación de Asociaciones de Ingenieros en Informática (AI2).
- W3C España (World Wide Web Consortium).
- Programa Nacional de Tecnologías Informáticas - Dirección General de Investigación. Ministerio de Educación y Ciencia.
- Red Española de Metaheurísticas.
- Red Española de Minería de Datos y Aprendizaje.
- Sección Española de la European Association for Computer Graphics (EUROGRAPHICS).
- Sociedad de Arquitectura y Tecnología de Computadores (SARTECO).
- Sociedad de Ingeniería del Software y Tecnologías de Desarrollo del Software (SISTEDES).
- Universidad de Zaragoza.

ISBN: 978-84-9732-607-0

CEDI 2007 II Simposio sobre Seguridad Informática | SSI'07 |

THOMSON

CEDI 2007

II CONGRESO ESPAÑOL DE INFORMÁTICA

ZARAGOZA SPAIN

AUDITORIO PALACIO DE CONGRESOS
11 AL 14 DE SEPTIEMBRE DE 2007

II Simposio sobre Seguridad Informática

| SSI'07 |

EDITORES
Benjamín Ramos Álvarez y Arturo Ribagorda Garnacho

ACTAS DEL
II SIMPOSIO SOBRE SEGURIDAD INFORMÁTICA [SSI'2007]

EDITORES

Benjamín Ramos Álvarez
Arturo Ribagorda Garnacho

SIMPOSIO ORGANIZADO POR

Grupo de Seguridad de las Tecnologías de la Información (SeTI)
Universidad Carlos III de Madrid

Grupo de Tecnologías de las Comunicaciones (GTC)
Universidad de Zaragoza

ENTIDADES COLABORADORAS

ACTAS DEL II SIMPOSIO SOBRE SEGURIDAD INFORMÁTICA (SSI'07)

Magallanes, 25; 28015 Madrid, ESPAÑA
Teléfono 91 4463350
Fax: 91 4456218
clientes@paraninfo.es

ISBN: 978-84-9732-607-0
Depósito legal: M-

Maquetación: Los Editores
Coordinación del proyecto: @LIBROTEX
Portada: Estudio Dixi
Impresión y encuademación: FER Fotocomposición, S. A.

IMPRESO EN ESPAÑA-PRINTED IN SPAIN

Presidente

Arturo Ribagorda Garnacho
Universidad Carlos III de Madrid

Vicepresidente

Benjamín Ramos Álvarez
Universidad Carlos III de Madrid

Secretario

José Luis Salazar Riaño
Universidad de Zaragoza

Comité de programa

Abascal Fuentes, Policarpo	Universidad de Oviedo
Álvarez Marañón, Gonzalo	CSIC
Areitio Bertolín, Javier	Universidad de Deusto
Borrell Viader, Joan	Universidad Autónoma de Barcelona
Caballero Gil, Pino	Universidad de La Laguna
Cabello, Adán	Universidad de Sevilla
Curty Alonso, Marcos	Universidad de Zaragoza
Dávila Muro, Jorge	Universidad Politécnica de Madrid
Domingo-Ferrer, Josep	Universidad Rovira i Virgili
Estévez Tapiador, Juan	Universidad Carlos III de Madrid
Fernández-Medina Patón, Eduardo	Universidad de Castilla La Mancha
Ferrer Gomila, Josep Lluis	Universidad Illes Balears
Fúster Sabater, Amparo	CSIC
García Teodoro, Pedro	Universidad de Granada
Gómez Eskarmeta, Antonio	Universidad de Murcia
González-Tablas Ferreres, Ana Isabel	Universidad Carlos III de Madrid
González Jiménez, Santos	Universidad de Oviedo
González Vasco, María Isabel	Universidad Rey Juan carlos
Gutiérrez Gutiérrez, Jaime	Universidad de Cantabria
Hernández Castro, Julio César	Universidad Carlos III de Madrid
Hernández Encinas, Luis	CSIC
Hernández Goya, Candelaria	Universidad de La Laguna

Herrera Joancomartí, Jordi	UOC
Huguet Rotger, Llorenç	Universidad Illes Balears
López Muñoz, Javier	Universidad de Málaga
Malagón Poyato, Chelo	CSIC-RedIris
Mañas Argemí, José Antonio	Universidad Politécnica de Madrid
Martín del Rey, Ángel	Universidad de Salamanca
Melús Moreno, José Luis	Universidad Politécnica de Cataluña
Miret Biosca, Josep María	Universidad de Lleida
Munuera Gómez, Carlos	Universidad de Valladolid
Orfila Díaz-Pabón, Agustín	Universidad Carlos III de Madrid
Ortega García, Javier	Universidad Autónoma de Madrid
Padró Laimon, Carles	Universidad Politécnica de Cataluña
Peinado Domínguez, Alberto	Universidad de Málaga
Pérez González, Fernando	Universidad de Vigo
Ramió Aguirre, Jorge	Universidad Politécnica de Madrid
Ramos Álvarez, Benjamín	Universidad Carlos III de Madrid
Ribagorda Garnacho, Arturo	Universidad Carlos III de Madrid
Rifá Coma, Josep	Universidad Autónoma de Barcelona
Robles Martínez, Sergi	Universidad Autónoma de Barcelona
Salazar Riaño, José Luis	Universidad de Zaragoza
Sánchez Reíllo, Raúl	Universidad Carlos III de Madrid
Sempere Luna, José María	Universidad Politécnica de Valencia
Soriano Ibáñez, Miquel	Universidad Politécnica de Cataluña
Tena Ayuso, Juan	Universidad de Valladolid
Villar Santos, Jorge	Universidad Politécnica de Cataluña

ÍNDICE

Criptografía

Autenticación y Biometría

Sistemas de detección y protección ante intrusos

Redes P2P y MANET

Gestión de la Seguridad

Protocolos y aplicaciones de seguridad

Modelo de Madurez para la Gestión de la Seguridad en las PYMES basado en Esquemas predeterminados

Luis Enrique Sánchez,
Daniel Villafranca,
Antonio Santos-Olmo
Departamento de I+D.
SICAMAN Nuevas Tecnologías.
13.700 Tomelloso
Lesanchez@sicaman-nt.com;
Dvillafranca@sicaman-nt.com;
Asolmo@sicaman-nt.com

Eduardo Fernández-Medina,
Mario Piattini
Grupo de Investigación Alarcos, Departamento
de Tecnologías y Sistemas de Información
Universidad Castilla-La Mancha
13.071 Palma de Mallorca
Eduardo.FdezMedina@uclm.es;
Mario.Piattini@uclm.es

Resumen

Para garantizar la subsistencia de las empresas y la evolución de sus modelos empresariales, éstas deben poder garantizar la seguridad de sus sistemas de información, pero ésto requiere que las empresas conozcan en todo momento el nivel de madurez de su seguridad y hasta qué punto debe evolucionar la seguridad de su sistema de información. En las pequeñas y medianas empresas, la aplicación de las normas de seguridad existentes se ha encontrado con el problema de no contar con el adecuado dimensionamiento y las características requeridas por este tipo de compañías. En este artículo mostramos nuestra propuesta de modelo de madurez para la gestión de la seguridad en las PYMES y analizamos de forma breve otros modelos que existen en el mercado. Este enfoque se está refinando de forma continua mediante su aplicación en casos reales.

1. Introducción

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 diferenciador en la evolución de una compañía. Estos activos están sometidos a riesgos de una gran variedad, que pueden afectar de una forma crítica a las empresas. Existen multitud de fuentes que arrojan cifras que muestran la magnitud de los problemas ocasionados por la falta de unas medidas de seguridad adecuadas [2-7].

Actualmente es muy complejo para una pequeña o mediana empresa abordar la implantación de un sistema de gestión de seguridad [8, 9]. La tendencia en materia de seguridad de las empresas es ir migrando poco a poco su cultura hacia la creación de un sistema de gestión de seguridad (SGSI), aunque esta progresión es muy lenta. El mercado demanda actualmente a las empresas que sean capaces de garantizar que las tecnologías para los activos informáticos y de información sean seguras, rápidas y de fácil interacción [10].

En el presente articulo describimos una nueva propuesta de modelo de madurez y gestión de la seguridad orientado a las PYMES [11] que pretende solucionar los problemas detectados en los modelos clásicos, los cuales no se están mostrando eficientes a la hora de su implantación en las PYMES debido a su complejidad y otra serie de factores que serán analizados con detalle en las siguientes secciones del artículo. En anteriores trabajos hemos presentado las distintas versiones del modelo de madurez a medida que este ha ido evolucionando. En este artículo destacamos las diferentes etapas de que se compone la versión actual del modelo, centrándonos en el funcionamiento de su estructura de esquemas predefinidos.

El artículo continúa en la Sección 2, describiendo muy brevemente los modelos de madurez existentes, su tendencia actual y algunas de las nuevas propuestas que están surgiendo. En la Sección 3 se introduce nuestra propuesta de modelo de madurez orientado hacia las PYMES centrándonos en el uso de esquemas predefinidos. 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 [12-17] buscan establecer una valoración estandarizada, con la que se pueda determinar el estado de la seguridad de la información en una organización, y que nos permita poder planificar el camino que se tiene que recorrer para alcanzar las metas de seguridad deseadas.

Entre los modelos de madurez para seguridad de la información [18] que más se están aplicando en las empresas actualmente, destacan el SSE-CMM (Modelo de Capacidad y Madurez en la Ingeniería de Seguridad de Sistemas), COBIT [13] y el ISM3 [19], y aunque se han realizado investigaciones para desarrollar nuevo modelos, ninguna de ellas ha conseguido solucionar los problemas actuales que se producen a la hora de aplicar estos modelos en PYMES. Entre estas nuevas propuestas podemos destacar CC_SSE-CCM desarrollado por Jongsook Lee [17] que esta basado en el Common Criteria (CC) y SSE-CMM, el modelo de Eloff y Eloff [16] que define cuatro clases distintas de protección y que permiten ir incrementando de forma progresiva los niveles de seguridad.

Otras propuestas toman como punto central del SGSI el análisis de riesgos, entre ellas podemos destacar la propuesta de Karen & Barrientes [15] y UE CORAS (IST-2000-25031) [20]. La propuesta de Karen & Barrientes [15] esta basada 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. Por otro lado, UE CORAS (IST-2000-25031) [20] está desarrollando un marco para el análisis de riesgos de seguridad que utiliza UML2, AS/NZS 4360, ISO/IEC 17799, RM-ODP6, UP7 y XML8.

La mayoría de los modelos actuales basados en riesgos utilizan como metodología de análisis de riesgos Magerit v2 [21], el problema de esta metodología es que siendo la más completa y eficiente del mercado, no es útil para las PYMES ya que requiere de una enorme complejidad.

Frente a estos modelos que toman el Análisis de riesgos como el núcleo central del SGSI, en nuestro caso aunque es muy importante no deja de ser una pieza más del sistema. Siegel [22] señala que los modelos de seguridad informática que se centran exclusivamente en modelos de eliminación de riesgos no son suficientes y por otro lado Garigue [23] remarca que actualmente los gerentes no desean saber solo que se ha realizado para mitigar los riesgos, también se debe poder dar a conocerlo eficazmente que se ha realizado esta tarea y si se ha conseguido ahorrar dinero.

Debemos tener en cuenta que el análisis de riesgos es un proceso costoso, que no se puede repetir cada vez que se realiza una modificación. Por eso es importante desarrollar metodologías específicas que permitan mantener los resultados del análisis de riesgos. El proyecto de la UE Coras [20] hace de este mantenimiento del análisis de riesgo el punto principal de su modelo.

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

La visión de cómo afrontar estos niveles de madurez, difiere según los autores que se tomen como referencia. De esta forma algunos autores, insisten en utilizar la norma internacional ISO/IEC17799 en modelos de gestión de seguridad, pero siempre haciéndolo de manera incremental, considerando las necesidades particulares de seguridad [15, 16, 19, 24].

La propuesta presentada en este articulo también esta basada en la norma internacional ISO/IEC17799 pero se ha orientado su aplicación hacia las PYMES y evitando los problemas detectados en los modelos actuales.

3. Modelo de Madurez basado en Esquemas predeterminados

En [11] se han presentado versiones previas del modelo, aquí se presenta la evolución del modelo, aportando mejoras obtenidas por la aplicación práctica del mismo a casos reales que consisten en la definición de esquemas predefinidos que posibilitan el desarrollo del plan director de seguridad en un periodo de tiempo muy reducido y con pocos recursos.

El Modelo de Madurez para la Seguridad de la Información que proponemos permite a cualquier organización evaluar el estado de su seguridad, pero está orientado principalmente a las PYMES desarrollando modelos de gestión de seguridad sencillos, económicos, rápidos, automatizados y progresivos y sostenibles que son los principales requerimientos que tienen este tipo de compañías a la hora de implantar estos modelos.

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

Otra de las principales aportaciones que presenta el modelo que hemos desarrollado es un conjunto de matrices que permite relacionar los diferentes componentes del SGSI (controles, activos, amenazas, vulnerabilidades, riesgo, procedimientos, registros, plantillas, instrucciones técnicas, reglamentos y métricas) y que el sistema utiliza para generar de forma automática gran parte de la información necesaria, reduciendo de forma muy notable los tiempos necesarios para el desarrollo e implantación del SGSI. Este conjunto de inter-relaciones entre todos los componentes del SGSI, permite que el cambio de éstos en cualquiera de esos objetos altere el valor de medición del resto de objetos del sistema, de forma que podemos tener en todo momento una valoración actualizada de cómo evoluciona el sistema de seguridad de la compañía.

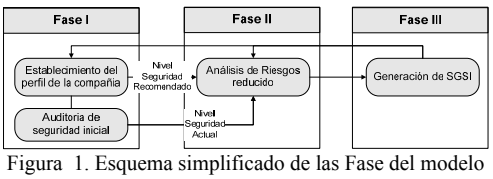

Figura 1. Esquema simplificado de las Fase del modelo espiral

El modelo de gestión de seguridad está formado por tres fases y los resultados de cada una de las fases anteriores son necesarios para la fase siguiente (ver Figura 1). A su vez, existe una retroalimentación de información desde la Fase III a las Fases I y II que permite al sistema ir modificando su parámetros y adecuándose a las nuevas circunstancias.

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

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

El principal objetivo de esta fase (ver Figura 2) es conocer el nivel de seguridad más adecuado para la compañía, y posteriormente por medio de una auditoria obtener su nivel actual de seguridad. Además, se conseguirá información vital para las Fase II y III. Esta fase se compone de dos subfases.

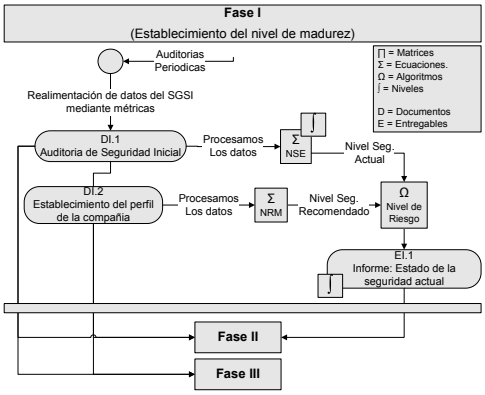

Figura 2. Esquema de la Fase I del Modelo en Espiral.

1. Establecimiento del perfil de la compañía: El modelo que nosotros proponemos utiliza un conjunto de características intrínsecas a la compañía para definir el nivel de madurez máximo al que la compañía debe evolucionar en la situación actual. Cada uno de estos parámetros se traduce a un valor y la suma normalizada de estos valores determina el nivel de madurez máximo que el sistema considera apropiado para la compañía.

La ecuación para calcular el nivel de madurez asociado a la compañía es:

$$\Sigma(\text{PesoFactor}*(\text{ValoraciónFactor}/\text{ValorMaximoFactor}))/\text{NumFactores} \quad (1)$$

Según esa expresión (ver Ecuación 1) y nuestra experiencia práctica con nuestros clientes hemos considerado 3 niveles de madurez (ver Figura 3): Nivel1 si el resultado esta entre 0–0.25, Nivel2 si esta entre 0.25–0.75 y Nivel3 si esta entre 0.75–1.

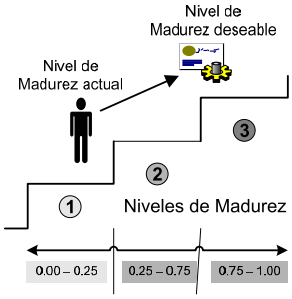

Figura 3. Fase I – Niveles de Madurez.

Los distintos elementos de esta expresión son los siguientes:

- *Factores:* Los factores representan un conjunto de parámetros que hemos seleccionado y que afectan a la hora de determinar el dimensionamiento de seguridad adecuado para la compañía. Estos factores tienen asociados rangos de valores que se determinan según las características de la compañía.
- *PesoFactor:* Es un parámetro corrector que se extrae de una matriz que asigna valores para el par factor-sector. Este parámetro de la ecuación nos permite controlar las desviaciones que pueden producir las características especiales de compañías pertenecientes a ciertos sectores.

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

3.2. Fase II: Análisis de Riesgos.

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

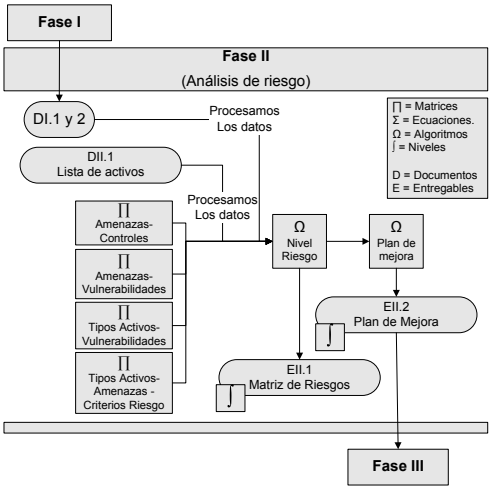

Figura 4. Esquema de la Fase II del Modelo en Espiral.

Esta Fase (ver Figura 4) es enormemente delicada por los importantes costes que puede llegar a suponer y por la importancia de los resultados para el éxito del SGSI.

El modelo de Análisis de Riesgos que hemos desarrollado, esta basado en los modelos propuestos por Stephenson [25] que se centran en la sinergia entre la prueba técnica y el análisis de riesgos tomando como referencia la ISO17799 y en la metodología de análisis de riesgos Magerit v2 [21]. Estos modelos no se muestran adecuados para las PYMES debido a su enorme complejidad, a que requieren un enorme esfuerzo de involucración por parte de los miembros de la compañía y a que los costes asociados a los mismos no son aceptables para este tipo de compañías.

Por ello, en nuestro modelo hemos buscando en todo momento simplificar los modelos anteriores para adecuarlos a las PYMES. Las principales bases sobre las que se define nuestra metodología son: Flexibilidad, Simplicidad y Eficiencia en costes (humanos y temporales). Se trata pues de una metodología que pretende identificar con el menor coste posible los activos de la compañía y los riesgos asociados, usando para ello los resultados generados en la fase I y unos sencillos algoritmos.

Dentro del análisis de riesgos que hemos desarrollado uno de los aspectos más importantes son las Matrices de asociación que permiten minimizar el coste del análisis de riesgo y producir el máximo resultado e información para la compañía con el menor esfuerzo. Se ha realizado una serie de matrices que permiten asociar los diferentes componentes del análisis de riesgo (activos-amenazas-vulnerabilidades) y a su vez estos con los resultados producidos en la fase I (controles). Estas matrices son de gran importancia ya que ayudan a simplificar el análisis de riesgos y ayudan a obtener una valoración del nivel de cobertura de un activo con respecto a los controles de la ISO/IEC 17999. Estas matrices son estáticas, aunque el consultor puede decidir modificarlas para adecuarlas a la compañía:

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

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

El nivel de cobertura actual de un control sobre un activo y para una amenaza dada se calcula como (ver Ecuación 2):

$$NCAA = \Sigma(VACAM)/NCAM \quad (2)$$

Siendo:

- **VACAM:** Valor actual del control afectado por la amenaza medido en la fase I para cada uno de los niveles de madurez.
- **NCAM:** Número de controles afectados por la amenaza para ese nivel de madurez.
- **NCCAA:** Nivel de Cobertura que ofrecen los controles actuales ubicados en el sistema para un activo X frente a una amenaza Y con respecto al nivel de madurez Z.

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

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

3.3. Fase III: Generación del SGSI.

En esta Fase (ver Figura 5) se ha buscado que el SGSI sea manejable, enfocado en los dominios de la norma de mayor interés para la organización y con un número de métricas reducido, obteniendo rápidos resultados y realimentando el proceso en

cada ciclo, hasta obtener el nivel de madurez marcado inicialmente.

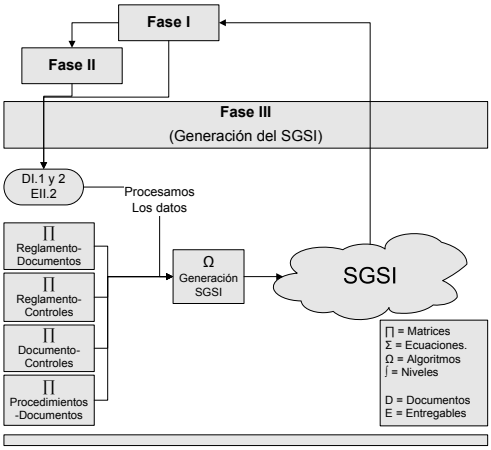

Figura 5. Esquema de la Fase III del Modelo en Espiral.

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

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

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

- *Relación entre el reglamento y los documentos:* El reglamento define normativas que deben cumplirse en una temática concreta del SGSI. La violación de una regla de esta normativa va normalmente asociada al incumplimiento de otros objetos (procedimientos, plantillas, registros, etc).
- *Relación entre el reglamento y la ISO17779:* Esta matriz nos permite asociar las reglas de la normativa con controles de la ISO17799 de tal forma que podamos medir incumplimientos en controles de la ISO17799.
- *Relación entre los documentos y los controles de la ISO17799:* Es la matriz más importante ya que permite asociar los documentos que componen nuestro modelo con los controles de la ISO17799.
- *Relación entre los procedimientos y sus documentos asociados:* Esta matriz actualmente se utiliza a modo de referencia para determinar los documentos que son de E/S y los que solo son solo de Entrada o Salida.

Las matrices asociadas a las ISO17799 son de vital importancia en el diseño de nuestro sistema, ya que son las que utiliza el algoritmo para la selección de los documentos y procedimientos que se considerarán de vital importancia tanto para el diseño del SGSI como para su posterior seguimiento.

Para finalizar esta fase, se utiliza un Algoritmo de generación del SGSI. Dado el enorme alcance de la investigación, el algoritmo de generación del SGSI se ha desarrollado buscando el principio de sencillez. Este algoritmo se compone de los siguientes pasos: i) Selección de objetos del SGSI, ii) Aplicación códigos de colores.

Cuando un procedimiento tenga que cumplirse solo parcialmente implicara que tan solo las partes afectadas por los controles de la ISO17799 serán de obligado cumplimiento para el Nivel de Madurez actual. En posteriores versiones se irán atomizando más los objetos de tal forma que los procedimientos cambien de forma dinámica en base a la selección inicial de controles y a los niveles de madurez.

El resultado final de esta fase será un conjunto de reglamentos y procedimientos que deberán cumplirse para mejorar el nivel de seguridad de la compañía, los cuales tendrán asignados un código de colores para indicar de una forma visual y rápida al usuario donde deben aplicar un mayor esfuerzo. El SGSI será dinámico, adaptándose a los cambios en los niveles de cobertura de los controles y en los niveles de seguridad según

evolucione el sistema. La evolución del sistema se medirá mediante un conjunto de métricas definidas sobre el conjunto de objetos del SGSI.

4. Conclusión

A pesar de los enormes esfuerzos que se están realizando para crear modelos de madurez adecuados para gestionar la seguridad en las PYMES, éstos no terminan de encajar con el entorno en que deben ser implantadas. La causa más probable es la falta de madurez de las empresas y 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.

En este artículo se ha presentado la propuesta de un nuevo modelo de madurez y gestión de seguridad orientada a las PYMES que permite reconfigurar y adaptarse para garantizar la seguridad de la misma y la estabilidad de su sistema de gestión con respecto a la dimensión de la compañía. Para ello se ha definido la metodología y una herramienta que permita soportar los resultados que se han ido generando durante la investigación (en este articulo por motivos de espacio no se ha descrito esta herramienta). Se ha definido como se debe utilizar este nuevo modelo de madurez y las mejoras que ofrece con respecto a los sistemas clásicos.

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

- La mayor parte de las PYMES tienen estructuras de seguridad muy parecidas. Esta característica permite desarrollar sistemas de seguridad automatizables mediante la definición esquemas.
- Si sobredimensionamos el nivel de seguridad de una empresa con respecto a su tamaño, se produce una degradación de los controles que hemos sobredimensionado, hasta que éstos alcanzan su punto de equilibrio natural.
- Las empresas se muestran más receptivas ante planes de implantación de muy corto plazo que ante planes a largo. La certificación por niveles ofrece una garantía para la valoración de la evolución del proyecto a corto plazo.

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

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

Entre las líneas de trabajo que serán abordadas como trabajo futuro, destacan las siguientes:

- Mejorar el algoritmo de establecimiento del nivel de madurez deseable para una compañía.
- Refinar el generador de Esquemas sobre el que se soporta el modelo.
- Aumentar los mecanismos de medición y auto-evaluación de la seguridad.

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.

Agradecimientos

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

Referencias

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

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

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

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

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

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

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

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

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

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

[11] Sánchez, L.E., D. Villafranca, E. Fernández-Medina, y M. Piattini. *Security Management in corporative IT systems using maturity models, taking as base ISO/IEC 17799.* in *International Symposium on Frontiers in Availability, Reliability and Security (FARES'06) in conjunction with ARES.* 2006. Viena (Austria).

[12] Areiza, K.A., A.M. Barrientos, R. Rincón, y J.G. Lalinde-Pulido, *Hacia un modelo de madurez para la seguridad de la información.* IV Congreso Internacional de Auditoría y Seguridad de la Información, 2005b. **Dic (2005)**.

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

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

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

[16] Eloff, J. y M. Eloff, *Information Security Management - A New Paradigm.* Annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology SAICSIT´03, 2003: p. 130-136.

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

[18] Areiza, K.A., A.M. Barrientos, R. Rincón, y J.G. Lalinde-Pulido, *Hacia un modelo de madurez para la seguridad de la información.* 3er Congreso Iberoamericano de seguridad Informática, 2005a. **Nov, (2005)**: p. 429 - 442.

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

[20] Lund, M.S., F.d. Braber, y K. Stolen, *Proceedings of the Seventh European Conference On Software Maintenance And Reengineering (CSMR'03)*. IEEE, 2003.

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

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

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

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

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

[15] Giorgini, P., H. Mouratidis, y N. Zannone, Modelling Security and Trust with Secure Tropos, in Integrating Security and Software Engineering: Advances and Future Visions. 2006, Idea Group Publishing.
[16] Gruber, T., Towards Principles for the Design of Ontologies used for Knowledge Sharing. International Journal of Human-Computer Studies, 1995. 43(5/6): p. 907-928.
[17] Gruninger, M. y J. Lee, Ontology Applications and Design. Communications of the ACM, 2002. 45(2): p. 39-41.
[18] Guarino, N. y C. Welty, Evaluating ontological decisions with ONTOCLEAN. Communications of the ACM, 2002. 45(2): p. 61-65.
[19] Kagal, L. y T. Finin, Modeling conversation policies using permissions and obligations. AAMAS workshop on Agent communication, LNCS. Springer-Verlag, 2005.
[20] Karyda, M., et al., An ontology for secure e-government applications. First International Conference on Availability, Reliability and Security (ARES'06). IEEE Computer Society, 2006: p. 1033-1037.
[21] Kim, A., J. Luo, y M. Kang. Security Ontology for Annotating Resources. in 4th International Conference on Ontologies, Databases, and Applications of Semantics (ODBASE'05). 2005. Agia Napa, Cyprus.
[22] Kitchenham, B., Procedures for performing systematic reviews (Joint Technical Report), in TR/SE-0401. 2004, Keele University, Sortware Engineering Group. Department of Computer Science. p. 33.
[23] Kwon, J. y C.-J. Moon, Visual modeling and formal specification of constraints of RBAC using semantic web technology. Knowledge-Based Systems, 2006. In Press, Corrected Proof.
[24] Lozano-Tello, A. y A. Gómez-Pérez, ONTOMETRIC: A Method to Choose the Appropriate Ontology. Journal of Database Management. Special Issue on Ontological analysis, Evaluation, and Engineering of Business Systems Analysis Methods, 2004. 15(2).
[25] Maamar, Z., N.C. Narendra, y S. Sattanathan, Towards an ontology-based approach for specifying and securing Web services. Information and Software Technology, 2006. 48(7): p. 441-455.
[26] McGibney, J., N. Schmidt, y A. Patel, A service-centric model for intrusion detection in next-generation networks. Computer Standards & Interfaces, 2005. 27(5): p. 513-520.
[27] Mouratidis, H. y P. Giorgini, An Introduction, in Integrating Security and Software Engineering: Advances and Future Visions. 2006, Idea Group Publishing.
[28] Mouratidis, H., P. Giorgini, y G. Manson, An Ontology for Modelling Security: The Tropos Approach, in Knowledge-Based Intelligent Information and Engineering Systems. 2003, Springer Berlin / Heidelberg. p. 1387-1394.
[29] Raskin, V., et al., Ontology in information security: a userful theoretical foundation. Proceedings of the 2001 workshop on New security paradigms NSPW'01. ACM Press, 2001.
[30] Ruíz, F., El Meta-Meta, las Ontologías y la Investigación en Ingeniería del Software. II Workshop en Métodos de Investigación y Fundamentos Filosóficos en Ingeniería del Software y Sistemas de Información, 2004.
[31] Tan, J.J. y S. Poslad, Dynamic security reconfiguration for the semantic web. Engineering Applications of Artificial Intelligence, 2004. 17(7): p. 783-797.
[32] Thuraisingham, B., Security standards for the semantic web. Computer Standards & Interfaces, 2005. 27(3): p. 257-268.
[33] Tsoumas, B. y D. Gritzalis, Towards an Ontology-based Security Management. Proceedings of the 20th International Conference on Advanced Information Networking and Applications. IEEE Computer Society, 2006. Volume 1 (AINA'06) - Volume 01 AINA '06.
[34] Undercoffer, J., A. Joshi, y J. Pinkston. Modeling Computer Attacks: An Ontology for Intrusion Detection. in The Sixth International Symposium on Recent Advances in Intrusion Detection. 2003: Springer.
[35] Vorobiev, A. y J. Han, Security Attack Ontology for Web Services. Proccedings of the Second International Conference on Semantics, Knowledge, and Grid SKG '06. IEEE Computer Society, 2006: p. 42.
[36] Yu, E., L. Liu, y Mylopoulos, A Social Ontology for Integrating Security and Software Engineering, in Integrating Security and Software Engineering: Advances and Future Visions. 2006, Idea Group Publishing.