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

Presentación

Hace dos años se celebró en Granada el primer CEDI (Congreso Español de Informática), lo que supuso un hito en nuestro país para las reuniones académicas de las numerosas materias que hoy en día engloba esta macrodisciplina que denominamos informática. Así pues, ésta fue la primera vez que gracias al esfuerzo coordinado de un gran número de profesores e investigadores –atinadamente dirigidos por los organizadores–, se logró reunir en un mismo escenario y en un breve lapso de tiempo a la práctica totalidad de los académicos que nos dedicamos a la informática.

Naturalmente, la seguridad de la información –una de las más pujantes disciplinas de la informática–, no podía estar ausente de este acontecimiento, y por ello celebramos en dicha ocasión el Simposio sobre Seguridad Informática. Esta participación fue una decisión fácil de tomar por parte de los que nos dedicamos a esta disciplina, pues aunque desde el ya lejano 1988 convocábamos una reunión bienal (de nombre Reunión Española de Criptología y Seguridad de la Información, más conocida como RECSI), no podíamos dejar pasar la oportunidad de acogernos al paraguas de CEDI y sumarnos a un Congreso que llamaba a todos nuestros compañeros y amigos de otras disciplinas hermanas.

Además, se da la circunstancia de que CEDI, aun siendo de periodicidad bienal, como RECSI, se reúne los años impares, mientras que la última lo hace los pares, por lo que aquél, aparte de su intrínseco interés, nos ofrecía a los dedicados a la seguridad la posibilidad de seguir manteniendo el contacto entre años impares.

Dado que la iniciativa fue un éxito, y en el 2005 el Simposio sobre Seguridad Informática congregó a un número importante de participantes, parecía indudable que se debía mantener la cita este año en Zaragoza, como así se hizo en su momento, con el resultado que este libro de actas muestra y que los lectores deben de juzgar.

Por lo que atañe a la seguridad de la información, cabe decir que es uno de los campos que ha experimentado en los últimos diez años un crecimiento más vertiginoso, principalmente en todo el llamado primer mundo.

En nuestro país, son tres las principales causas de este hecho. Por un lado, la rápida expansión de Internet, que en poco tiempo ha alcanzado todos los rincones de nuestra sociedad, convirtiéndose en una instrumento ineludible

para las empresas, sin el cual no ya su actividad, sino incluso su presencia entre sus clientes se veía seriamente comprometida. Igualmente, para las Administraciones Públicas Internet supone satisfacer los principios constitucionales de "eficacia, descentralización y coordinación", que, entre otros, deben guiar sus actuaciones, así como atender las demandas de los ciudadanos que requieren servicios públicos ágiles y accesibles.

En segundo lugar, la promulgación en el año 1992 de la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD) – derogada en 1999 por la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD)–, y sobre todo la publicación en 1999 del Real Decreto 994/1999 (Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal), supuso un revulsivo para empresas y Administraciones Públicas obligadas, so pena de ser sancionadas por la Agencia Española de Protección de Datos, a adoptar mecanismos y procedimientos de seguridad para proteger los datos personales que manejaban.

En tercer lugar, la presión de los usuarios informáticos, nada proclives a abandonar procedimientos ancestrales de relación con organismos públicos y privados, salvo que se les ofreciesen las mismas garantías de seguridad que se les supone (a menudo con más fe que raciocinio) a los procedimientos que se pretendían sustituir.

Por todo ello, lo que a finales de los ochenta era un pequeño grupo de académicos interesados casi en exclusiva por la criptología, ha devenido en un importante número de investigadores y docentes que, sin abandonar dicho campo, trabajan igualmente en los numerosos temas que figuran entre los de interés de este Simposio, y cuyas aportaciones se presentan en este libro.

Esperamos que estas actas y la reunión del próximo septiembre sirvan para potenciar aún más el interés y desarrollo de la seguridad, sin cuyo concurso difícilmente avanzaremos en la sociedad de la información que estamos conformando y de la que tanto esperamos para el progreso de la humanidad.

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

Hacia un método para la construcción de Cuadros de Mando de la Seguridad en TI para PYMES.

Daniel Villafranca, Luis Enrique Sánchez,
SICAMAN Nuevas Tecnologías.
Departamento I+D,
Juan José Rodrigo, 4. Tomelloso, Ciudad Real,
dvillafranca@sicaman-nt.com
lesanchez@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

La seguridad en los Sistemas de Información es algo de lo que las empresas están tomando conciencia. De la necesidad de mejorar la seguridad, nacen los Sistemas de Gestión de la Seguridad de la Información como solución general a este problema. La implantación práctica de estos sistemas presenta una problemática añadida para el caso de las PYMES, ya que es difícil valorar si el alcance de los objetivos que se definen se ajustan a las necesidades prácticas de las mismas. Los criterios de evaluación de la seguridad deben corresponderse a los objetivos que se requiere y evolucionar conforme al nivel de madurez del sistema, de forma que las métricas se integren con los objetivos empresariales. El cuadro de mando integral será la herramienta que nos permitirá evaluar de una forma rápida el estado de la seguridad para una toma de decisiones coherente. En este artículo, analizaremos desde un enfoque práctico el proceso de recogida de estos indicadores, la creación de métricas e introduciremos un método para el diseño y construcción de cuadros de mando que mejor se adaptan en las PYMES.

1. Introducción

Actualmente, el cambio social producido por Internet y la rapidez en el intercambio de información, ha producido que las empresas empiecen a tomar conciencia del valor que tiene la información para sus organizaciones y se preocupen de proteger sus datos. Con la creciente dependencia que la sociedad de la información tiene de las TIC, 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 [15]. 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 [3, 8, 12]. Este marco debe permitir que los directores de negocio dispongan de herramientas que les permitan identificar, medir y gestionar los riesgos existentes en sus activos de información y sus inversiones en seguridad, buscando el retorno de dichas inversiones y obtener una mejora en la seguridad de sus sistemas. El cuadro de mando de la seguridad nos permitirá gestionar la seguridad en base a información cuantitativa y objetiva, lo que facilita la toma de decisiones alineadas con los requisitos del negocio.

Como se indica en [8], lo que no puede ser medido, no puede ser gestionado. La necesidad de gestionar la seguridad de los sistemas de información obliga a la utilización de métricas e indicadores que permitan evaluar la situación real [21]. Las métricas de seguridad son necesarias para saber el estado de un sistema de información [11] y tienen por finalidad **conocer, evaluar y gestionar** la seguridad de los sistemas de información [10]. 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 [20].

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 [5]. 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 [10].

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 en el empleo de las métricas e indicadores en los diferentes estándares internacionales sobre la gestión de seguridad. En la Sección 3 se realiza un análisis de los problemas de seguridad en las PYMES y se presenta una propuesta de construcción de Cuadros de Mando Integrales (CMI) mediante los modelos de gestión de seguridad de la información, tratando su implantación práctica en la sección 3.1 y aportando una nueva propuesta de construcción del CMI para nuestro modelo de gestión de la seguridad en 3.2. Finalmente, aportamos las conclusiones e indicamos cuál será el trabajo que desarrollaremos en el futuro.

2. Las Métricas e Indicadores de Seguridad de la Información

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 [6]. 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 [20]:

- Las métricas no están siempre definidas en un contexto en donde 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 [22], algo necesario para abordar nuestro modelo. En la bibliografía se encuentran diferentes clasificaciones de métricas de seguridad. Por ejemplo, en [11] se propone una clasificación de métricas de seguridad para la gestión segura de los sistemas de información considerando los siguientes cuatro tipos de métricas: Métricas de gestión, métricas técnicas, métricas del entorno físico y métricas del personal. Otros autores [17] las clasifican en cuatro categorías, en base a lo que se quiere medir: Métricas de desarrollo, de soporte, de operaciones y de efectividad, incluyendo subcategorías dentro de cada una de ellas.

El modelo que define COBIT enlaza los requisitos del negocio de información de la dirección a los objetivos de las TI [24]. Se propone una estructura y una serie de indicadores para medir la tecnología de la información [7], basados en Indicadores Clave del Rendimiento (KPI), Indicadores clave de logros (KGI) y los Factores críticos del éxito (FCE). Ante la cuestión sobre lo que se debe medir, hay que establecer marcadores e indicadores clave de rendimiento (KPI) para las diferentes áreas funcionales de la seguridad [12]. 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, de la forma:

- 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.

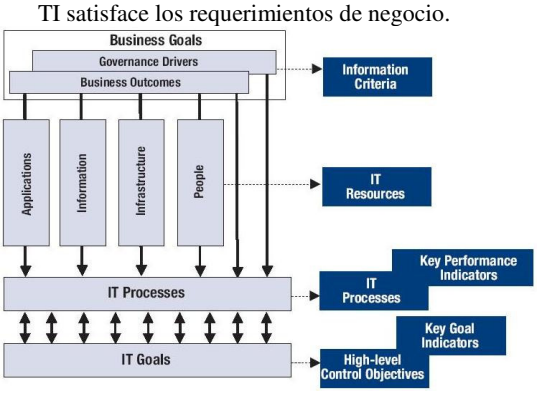

Figura 1. Gerencia, control, alineación y supervisión en COBIT (Fuente: IT Governance Institute)

Con un enfoque más práctico en la evaluación y selección de estos indicadores encontramos en NIST [13] 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 [25] 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 [26], 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.

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 [3]. 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.

3. Cuadro de Mandos de Seguridad en TI para PYMES

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 y que está

especialmente diseñado para ser implantado en PYMES [18,19] y debido a sus características particulares, resulta difícil adecuar los estándares y modelos sobre métricas y seguridad de la información presentados en el apartado anterior, principalmente las siguientes razones:

- Falta de madurez de las empresas en lo relativo a seguridad, ya que no existe una conciencia real del problema hasta que no ocurren los incidentes.
- Los estándares son demasiado generales y han sido elaborados para empresas con un cierto tamaño, siendo su implantación demasiado costosa en tiempo y recursos para PYMES.
- Las PYMES requieren de normas ajustadas a su dimensión y de herramientas que permitan la viabilidad en la implantación de los SGSI, mediante la reducción de los recursos para implantar y mantener los sistemas.
- Es importante enfocar la implantación de un SGSI de acuerdo a ciertos factores particulares de la compañía, ya que el ámbito de la misma y su tamaño así lo exigen.

En el panorama actual de los SGSI, y dentro de los objetivos que nos plantean nuestros clientes, con la idea de aplicar los programas de gestión de la seguridad en los SI, hemos llevado a cabo dos actividades:

- Desarrollo de una metodología de gestión de la seguridad orientada a las PYMES [16] 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.

En esta sección en primer lugar introduciremos el modelo de madurez para la seguridad y a continuación se presentará cómo se han definido los indicadores y seleccionado las métricas para el desarrollo de un modelo de cuadro de mandos en el gobierno de la seguridad.

3.1. Modelo de Madurez de la seguridad para PYMES

Los Modelos de Madurez de Seguridad [1,5,18] buscan establecer una valoración estándar 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.

En anteriores trabajos [18, 19] hemos partido de un enfoque sistemático para abordar la implantación de SGSI, se ha analizando el nivel de madurez y establecidos los niveles de protección y controles para una organización, siguiendo el enfoque de la figura 2.

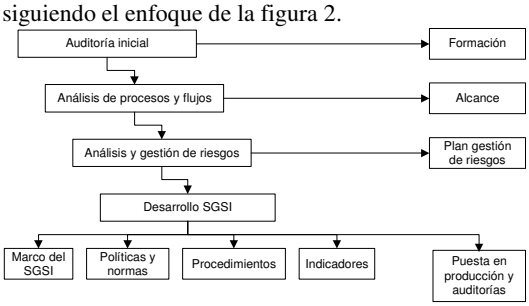

Figura 2. Fases en la implantación de un SGSI

Ello nos motivó a elaborar nuestro modelo propio, cuya principal ventaja es la implantación progresiva de la seguridad (v. figura 3) dependiendo de dos parámetros básicos:

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.

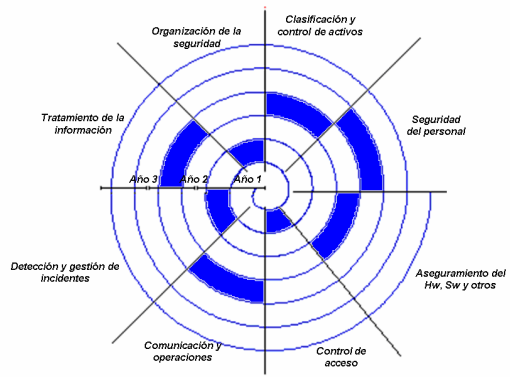

Figura 3. Modelo en espiral para madurez de los SGSI.

El panorama para una PYME es complejo a la hora de abordar la implantación de un sistema de gestión de seguridad. Es por ello, que desde nuestra experiencia en la aplicación de los SGSI, hemos desarrollado este modelo más práctico que, mediante la definición de unos indicadores

particulares, permite una aplicación más sencilla en las PYMES. El modelo está basado en tres niveles de seguridad, que aplicamos según el nivel de madurez de la empresa y su tamaño.

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, 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.

Dentro de este modelo, toma vital importancia encontrar los indicadores clave que sirvan para definir una herramienta que nos va a permitir asegurar el cumplimiento de los objetivos marcados en nuestro programa de seguridad [16]. 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.

3.2. Proceso de definición de Cuadros de Mandos de Seguridad para PYMES

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 [7]. Este planteamiento ha sido trasladado a las tecnologías de la información y de forma más específica a la seguridad en las TIC.

Para la definición de un Cuadro de Mando para la seguridad de la información, en consonancia con la guía de COBIT [6], se nos definen cuatro perspectivas tal y como se muestra en la tabla 1:

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 ven los usuarios en TI a la seguridad en la tecnología de la información

Tabla 1. Cuadro de mando para la Seguridad en IT según COBIT

En nuestro caso, el trabajo con nuestros clientes, se requiere de diferentes aspectos a salvaguardar en la seguridad de 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. Es por ello que los parámetros que hemos tenido en cuenta para definir, seleccionar y evaluar las métricas han sido:

- **Política de la organización:** Es la relación de la métrica con la estructura de análisis en 12 secciones o áreas que la organización debe vigilar para garantizar la seguridad que define el estándar ISO 17799.
- **Objetivo de Control:** Se define para cada uno de los dominios establecidos en la norma, ya que mediante las métricas podremos medir el cumplimiento y calidad del proceso de la organización.
- **Proceso o método de recogida:** Especifica el tipo de prueba realizada para la obtención del valor: automática, checklist,… Será de vital importancia poder realizar una medida automática que evite valores subjetivos en el proceso. Además, uno de los principales objetivos perseguidos con este esquema es realizar un SGSI automatizable que permita a las compañías mantener su sistema de seguridad con el mínimo esfuerzo.
- **Niveles de Madurez**: En nuestra herramienta SSE-PYME, según el nivel de madurez que se desea alcanzar hemos segmentado las métricas**,** dando más peso en función objetivo.
- **Tipo de Empresa:** En función del sector económico y la naturaleza de la empresa, tendrá más repercusión el garantizar la aplicación de un tipo de métricas y unos objetivos de control específicos.

- **Valores:** Determina el rango de valores que definen la métrica. Se tiene en cuenta para reducir la complejidad en la definición de nuestros niveles de madurez (reducido a 3).
- **Escalas:** Nuestra herramienta determina un conjunto de escalas que se reajustan en función de la realimentación conseguida mediante la aplicación práctica en clientes.
- **Validez**: Es un punto clave en la aplicación de la métrica, ya que según se va avanzando en el nivel de madurez y en la consecución de los objetivos, las métricas dejan de ser efectivas.
- **Automatización de la métrica**. Este factor nos va a permitir eliminar la subjetividad de los resultados y dar un rigor a los resultados.
- **Nivel de Madurez**. Nos permite variar la escala de medición del valor de la métrica en función del nivel de madurez en el que se ha encajado a la empresa.
- **Frecuencia de medición**: Durante el proceso de evaluación en ciclos, se podrá requerir la repetición de las mediciones para establecer un promedio en la revisión final del indicador.
- **Relación de costes:** Asociado a la obtención de los valores medidos, será preciso definir los criterios económicos y tiempos de obtención, ya que no se podrán realizar en algunos casos.

Existen principalmente dos metodologías para la construcción de un Cuadro de Mando: top-down y down-top [15]. Alternativamente, también se han propuesto otras técnicas en cascada [29]. Por considerar algo rígidos estos métodos [27], la idea de nuestro enfoque es un planteamiento mixto entre un enfoque en cascada y que además se realimenta con experiencias de implantaciones anteriores, recogiendo los objetivos que se definen desde la gerencia y el estado previo de los sistemas con los que cuenta la organización.

Este método es un procedimiento incremental que viene dado por el modelo de madurez desarrollado en espiral (v. figura 2), que conjuga varias fases en su definición. Partiendo de una clasificación práctica de las mediciones para agruparlas en un CMI, las hemos agrupado en internas y externas, realizado una clasificación global en cinco categorías, en contraposición al enfoque clásico del CMI (v. tabla 1) y que 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 que tipo de aplicaciones, así como la infraestructura de comunicaciones será fundamental controlar
- **Los clientes y el negocio**: será vital determinar qué activos son los más importantes y 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**: 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 que hemos definido en nuestro modelo en espiral.

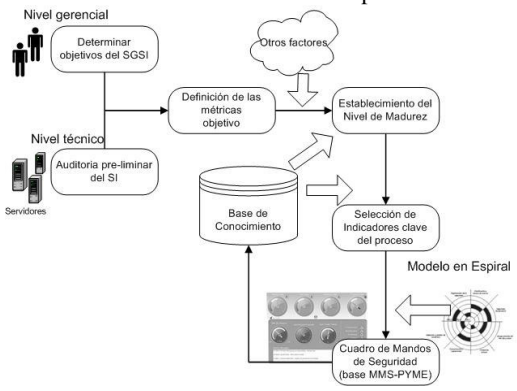

Figura 4. Esquema de nuestro CMI de Seguridad

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 [27]:

- **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 gran parte de las métricas utilizadas en la norma ISO 17799 y NIST como guía para desarrollar las áreas de control que está tratando de medir. 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 al 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 previos, incluso antes de haber decidido la implantación del SGSI.
- **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" en dos aspectos: la selección de las métricas y 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.

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:

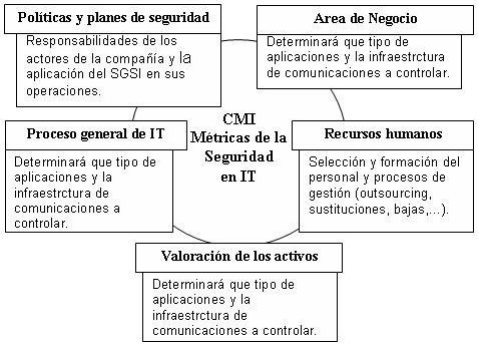

Figura 5. Perspectivas de nuestro CMI de Seguridad

Para cada uno de ellos 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 una 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).

4. Conclusiones y Trabajos Futuros

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.

Después de haber revisado y aplicado in situ alguna de las guías de control para la seguridad en los SI, hemos comprobado además que es muy complejo para una pequeña o mediana empresa abordar la implantación de un sistema de gestión de seguridad.

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 presentamos, 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 en nuestros clientes, dejamos pendiente profundizar más en las características de las métricas con las que estamos trabajado y la

información que nos han aportado para mejorar la gestión de la seguridad de sus SI.

En base a estas métricas, hemos desarrollado un nuevo modelo que nos permite construir un CMI orientado a PYMES, que estamos aplicando y obteniendo unos resultados satisfactorios que permiten optimizar el coste de implantación de los SGSI.

Referencias

[1] Aceituno Canal, V. ISM3 1.0. ISM3: easier Information Security Management (Jun 2005)

[2] Briand, L., Arisholm, S., Counsell, F., Houdek, F., & Thévenod-Fosse, P. (1999). Empirical Studies of Object-Oriented Artifacts, Methods, and Processes. Empirical Software Engineering.

[3] Carrillo Verdún, J. La Gestión de la Seguridad: Métricas e Indicadores. AEMES (Nov.2003)

[4] Chapin, David A. How can security be measured?. Information Systems Control Journal, Volume 5, 2005. 43-49.

[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

[6] Erro, G. Seguridad TICs, ¿qué hay que medir?. Aplicabilidad de las Métricas en Seguridad. Jornada Técnica Seguridad Informática.

[7] Fernández-Medina, E., Moya, R., Piattini, M. Seguridad de las Tecnologías de la Información. Ediciones AENOR, (2003).

[8] Guenther, M. Evaluation, Metrics and Measurement for Security Awareness (2003)

[9] Heschl, J. COBIT in Relation to Other International Standars. Information Systems Control Journal, Volume 4, 2004. 37-40.

[10] Llaneza, P., Las Métricas de Seguridad de la Información.

[11] Mañas, José A. Security Metrics and Measurements for IT. UPGRADE. August-05.

[12] McCarthy,L. La importancia de las métricas de seguridad. Artículos de Seguridad. Symantec Corporation (Dic.2004).

[13] NIST Special Publication. Initial Public Draft. Guide to Performance Metrics for Information Security. April 2006.

[14] Peltier, T.R. (2003). Preparing for ISO 17799. Security Management Practices.

[15] Opacki, D. Security Metrics: Building Business Unit Scorecards. Dic 2005. 4-8

[16] 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).

[17] Vaughn, R., Henning, R., Siraj, A. Information Assurance Measures and Metrics – State of Practice and Proposed Taxonomy. 36th Hawaii International Conference on System Sciences (2003)

[18] 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)

[19] 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.

[20] 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.

[21] Villarrubia, C., Fernández-Medina, E. y Piattini, M. Métricas e indicadores de política de gestión de contraseñas.

[22] Van Grembergen, W., De Haes, S. COBIT's Management Guidelines Revisited: The KGIs/KPIs Cascade. Information Systems Control Journal, Volume 6, 2005.

[23] Warkentin, M., Vaughn R. Enterprise Information Systems Assurance and Systems Security. IDEA Group Publishing (2000).

[24] ITGI, CobiT Control Objetives, 2005.

[25] ISO/IEC. International standard iso/iec 17799 (2000). Information technology, 2000.

[26] ISO TC JTC1/SC 27 N4188. Information Security Management Metrics and Measurement, 2004.

[27] 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, pp