CIBSI 2009

16 al 18 de Noviembre
Montevideo, Uruguay

V Congreso Iberoamericano de Seguridad Informática

Actas del Congreso

Actas del V Congreso Iberoamericano de Seguridad Informática
CIBSI'09
Montevideo, Uruguay, 16 al 18 de Noviembre de 2009

Editores
Gustavo Betarte
Jorge Ramió Aguirre
Arturo Ribagorda Garnacho

ISBN: 978-9974-0-0593-8

Prefacio

Estimados colegas:

Este volumen contiene los trabajos presentados en el V Congreso Iberoamericano de Seguridad Informática (CIBSI'09) realizado en Noviembre en Montevideo, Uruguay.

Esta edición del Congreso Iberoamericano de Seguridad Informática, iniciativa de la Red Temática Iberoamericana de Criptografía y Seguridad de la información CriptoRed, ha convocado al igual que en sus anteriores ediciones a un gran número de investigadores y expertos de Latinoamérica, España y Portugal.

De 65 trabajos recibidos, el Comité de Programa Científico ha seleccionado 41 trabajos, 38 de los cuales se presentan en el evento. Los mismos proceden de investigadores de Argentina, Brasil, Chile, Colombia, España, EE.UU., Francia, México, Portugal, Uruguay y Venezuela.

El congreso cuenta asimismo con tres conferencistas que han sido invitados a presentar su trabajo de investigación en sesiones plenarias, el Dr. Gilles Barthe, de IMDEA Software de España, el Dr. Eduardo Giménez, de la Universidad de la República de Uruguay y el Dr. José Luis Piñar Mañas de la Universidad CEU San Pablo de España. Tendrá también lugar en el congreso un taller, titulado *Los retos de la protección de datos: la Ley 18331 de protección de datos personales*, a cargo del Dr. José Luis Piñar Mañas.

Desde estas páginas queremos hacer llegar nuestro profundo agradecimiento a los organizadores, autores, revisores, patrocinadores y asistentes, que son los que han hecho posible que una vez más tenga lugar este encuentro académico de expertos e investigadores en Seguridad Informática, esta vez en la ciudad de Montevideo.

Noviembre 2009

Gustavo Betarte
Jorge Ramió Aguirre
Arturo Ribagorda Garnacho
CIBSI'09

Organización de la Conferencia

CIBSI'09 es organizado por la Facultad de Ingeniería de la Universidad de la República en conjunto con la Universidad Politécnica de Madrid, a cuyos directivos asi como a todos y cada uno de los miembros del comité organizador queremos agradecer desde estas páginas.

Organización General

Gustavo Betarte, Universidad de la República, Uruguay
Jorge Ramió Aguirre, Universidad Politécnica de Madrid, España

Comité de Programa

Santiago Martín Acurio Del Pino, Pontificia Universidad Católica del Ecuador, Ecuador
Nicolás C.A. Antezana Abarca, Sociedad Peruana de Computación, Perú
Javier Areitio Bertolín, Universidad de Deusto, España
Walter Baluja García, Instituto Superior Politécnico José Antonio Echeverria, Cuba
Tomás Barros, NIC Labs, Chile
Gustavo Betarte (co-chair, Universidad de la República, Uruguay)
Joan Borrel Viader, Universidad Autónoma de Barcelona, España
Pino Caballero Gil, Universidad de La Laguna, España
Jeimy Cano Martínez, Universidad de los Andes, Colombia
Adriano Mauro Cansian, Universidade Estadual Paulista, Brasil
Hugo César Coyote Estrada, Instituto Politécnico Nacional, México
Enrique Daltabuit Godas, Universidad Nacional Autónoma de México, México
Jorge Dávila Muro, Universidad Politécnica de Madrid, España
Ángel Martín del Rey, Universidad de Salamanca, España
Josep Domingo-Ferrer, Universidad Rovira i Virgili, España
Josep Lluis Ferrer-Gomilla, Universidad de Las Islas Baleares, España
Amparo Fúster Sabater, Consejo Superior de Investigaciones Científicas CSIC, España
Luis Javier García Villalba, Universidad Complutense de Madrid, España
Roberto Gómez Cárdenas, ITESM Monterrey, México
Juan Pedro Hecht, Universidad de Buenos Aires, Argentina
Marco Aurelio Henriques, Universidade Estadual de Campinas, Brasil
Emilio Hernández, Universidad Simón Bolívar, Venezuela
Leobardo Hernández Audelo, Universidad Nacional Autónoma de México, México
Luis Hernández Encinas, Consejo Superior de Investigaciones Científicas CSIC, España
Alejandro Hevia, Universidad de Chile, Chile
Juan Guillermo Lalinde, Universidad EAFIT, Colombia
Javier López Muñoz, Universidad de Málaga, España
Julio César López, Universidade Estadual de Campinas, Brasil
Vincenzo Mendillo, Universidad Central de Venezuela, Venezuela
Carlos Mex Perera, ITESM Monterrey, México
Josep María Miret Biosca, Universidad de Lleida, España
Gaspar Modelo Howard, Universidad Tecnológica de Panamá, Panamá

Raúl Monge, Universidad Técnica Federico Santa María, Chile
Edmundo Monteiro, Universidad de Coimbra, Portugal
Guillermo Morales Luna, Centro de Investigación y Estudios Avanzados del IPN, México
Alberto Peinado Domínguez, Universidad de Málaga, España
Yoan Pinzón, Universidad Nacional de Colombia, Colombia
Tamara Rezk, INRIA Sophia Antipolis, Francia
Arturo Ribagorda Garnacho, (co-chair) Universidad Carlos III de Madrid, España
Josep Rifà Coma, Universidad Autónoma de Barcelona, España
Miguel Soriano Ibáñez, Universidad Politécnica de Cataluña, España
Horacio Tapia Recillas, Universidad Autónoma Metropolitana, México
Routo Terada, Universidade de São Paulo, Brasil
Alfredo Viola, Universidad de la República, Uruguay
Horst von Brand, Universidad Técnica Federico Santa María, Chile

Organización Local

Alejandro Blanco, Universidad de la República, Uruguay
Eduardo Carozo, ANTEL, Uruguay
Carlos Luna, Universidad de la República, Uruguay
Marcelo Rodríguez, Universidad de la República, Uruguay
Leonardo Vidal, Universidad de la República, Uruguay
Felipe Zipitría, Universidad de la República, Uruguay

Revisores Externos

Joao Afonso Abrunhosa, Universidade de Lisboa, Portugal
Almudena Alcaide, Universidad Carlos III de Madrid, España
Jorge Blasco Alis, Universidad Carlos III de Madrid, España
Philippe Camacho, Universidad de Chile, Chile
Eduardo Carozo, ANTEL, Uruguay
Eduardo Cota, Universidad de la República, Uruguay
Tiago Cruz, Universidade de Coimbra, Portugal
Eduardo Giménez, Universidad de la República, Uruguay
Jorge Granjal, Universidade de Coimbra, Portugal
Daniel Hedin, Chalmers University of Technology, Suecia
Julio César Hernandez-Castro, University of Southampton, Inglaterra
Jesús Manjón, Universitat Rovira i Virgili, España
Mireya Morales, Universidad Simón Bolivar, Venezuela
Gloria Pujol, Universitat Rovira i Virgili, España
Alejandro Russo, Chalmers University of Technology, Suecia
Miguel Torrealba, Universidad Simón Bolivar, Venezuela
Rolando Trujillo, Universitat Rovira i Virgili, España
Alexandre Viejo, Universitat Rovira i Virgili, España
Arnau Vives, Universitat Rovira i Virgili, España

Tabla de Contenidos

Metodología para la selección de métricas en la construcción de un Cuadro de Mando Integral

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

[1]SICAMAN Nuevas Tecnologías. Departamento I+D,
Juan José Rodrigo, 4. Tomelloso, Ciudad Real, España
{dvillafranca, lesanchez} @sicaman-nt.com
[2]Grupo de Investigación ALARCOS, Universidad Castilla-La Mancha
Paseo de la Universidad, 4 – 13071 Ciudad Real, Spain
{Eduardo.FdezMedina, mario.piattini} @uclm.es

Resumen. La implantación práctica de Sistemas de Gestión de la Seguridad de la Información presenta una problemática añadida para el caso de las PYMES debido a la falta de herramientas y guías adaptadas a su estructura organizativa y procesos en el área de las Tecnologías de la Información (TI). La selección de indicadores adecuados y la definición de métricas acordes para la construcción de un Cuadro de Mando Integral (CMI) de la Seguridad de la Información es un problema que las guías y métodos estándar no resuelven completamente. Es por ello que hemos desarrollado un nuevo método, orientado a PYMES y desde un punto de vista empírico, para la selección de indicadores y construcción de las métricas que van a proveer la información para nuestro CMI. En este artículo exponemos en detalle dicho método.

Palabras clave: Métricas, Selección de indicadores, Cuadros de Mando Integral (CMI), SGSI.

1. Introducción

En la última década, el mundo empresarial ha experimentado una transformación radical de sus procesos de trabajo con una dependencia cada vez mayor de las TI. Una de las consecuencias de este hecho es que las organizaciones necesitan aplicaciones cada vez más seguras. Las cifras manejadas por EITO (Observatorio Europeo de las Tecnologías de la Información) son una prueba de que la seguridad es una de las principales preocupaciones de las empresas [18], aunque en un reciente informe del Small Business Technology Institute [31] se ha descubierto que el 20% de ellas no poseen protección antivirus adecuada. Para mejorar la seguridad de las tecnologías de información para las empresas es necesario definir controles de seguridad, y que su cumplimiento sea monitorizado continuamente [10]. Esto permitiría mejorar la eficiencia de esos controles y conocer las vulnerabilidades al principio.

Asociados a estos controles de seguridad, se deberían usar métricas o indicadores de seguridad que nos permitan tener datos objetivos del cumplimiento de estos

controles. Para ello es preciso contar con un marco adecuado para la selección e implementación de métricas [6]. Por lo tanto, las métricas de seguridad son necesarias para saber el estado de un sistema de información [9] y tienen por finalidad conocer, evaluar y gestionar la seguridad de los sistemas de información.

Las métricas de seguridad son por lo tanto especialmente importantes para gestionar la seguridad de las empresas. Esta gestión se hace mediante los sistemas conocidos como Sistemas de Gestión de Seguridad (SGSI) [20], que requieren herramientas y metodologías adecuadas para su implantación. Actualmente, la mayoría de las grandes empresas han abordado la implementación de SGSI, con base en modelos de madurez, para la gestión de su seguridad [1], pero desafortunadamente la implantación de este tipo de sistemas en pequeñas y medianas empresas es muy complejo debido fundamentalmente que no disponen de herramientas y metodologías adecuadas para este tipo de empresas [14].

Una de las herramientas más importantes para los SGSI son los CMI de la seguridad. Desde su aparición en 1992 [8] los CMI han sido usados por centenares de organizaciones como un medio para describir su estrategia y medir su rendimiento. Los CMI son muy útiles para controlar procesos regulares con un flujo de información continuo (como es el caso de la gestión de la seguridad en las empresas), ya que obtener y agrupar la información más relevante y útil para la toma de decisiones, y que resulte crucial para tener un conocimiento permanente de la situación que se gestiona y de su evolución en el tiempo [5]. Junto a los modelos de madurez, los CMI nos ayudarán a conocer la situación de la seguridad conseguida mediante la implantación del SGSI, así como su evolución.

Las métricas de seguridad han sido siempre difíciles de evaluar [1]. Cada vez se utilizan en los procesos de auditoría de TI herramientas automatizadas para el desarrollo de sus revisiones, lo que ha contribuido enormemente a que se pueda suplir la falta de conocimiento en determinados campos específicos durante el desarrollo de una auditoría de TI. Por otro lado, para solucionar estos problemas, algunas propuestas abogan por incorporar nuevas tecnologías que permitan captar la experiencia humana en la auditoría de TI, mediante los Sistemas Expertos (SE) [10]. En este sentido, los SE permiten fundamentalmente obtener respuestas inmediatas y fiables, extender el conocimiento de un experto en una materia concreta.

Como hemos expuesto en trabajos anteriores [15] [16], en las pequeñas y medianas empresas, la aplicación de normativas de seguridad cuenta con el problema adicional de no tener recursos humanos y económicos suficientes para realizar una adecuada gestión. Los modelos de madurez generales no han sabido dar respuesta práctica en este caso, lo que nos ha llevado a desarrollar un modelo propio, tomando como marco de referencia la norma ISO/IEC 27002 [14]. También se ha visto la necesidad de complementarlo con un proceso particular de selección de métricas para la construcción de CMIs adecuados al contexto de este tipo de empresas [20].

Por lo tanto, el objetivo de esta investigación es la definición de un método sistemático basado en ingeniería que nos permita seleccionar y segmentar las métricas de seguridad para la construcción de cuadros de mando de seguridad optimizados para cada caso. Para la construcción de este método nos hemos basado en los planteamientos de construcción de cuadros de mando clásicos top-down y bottom-up [13]. La idea es ofrecer soluciones consolidadas y que pueden ser reutilizadas en el contexto del diseño del CMI de la seguridad.

Asimismo, este proceso de construcción del CMI de Seguridad encaja con nuestro modelo de madurez desarrollado para PYMES [14] [17], ya que se realiza de forma incremental partiendo del nivel que la organización tiene según nuestro modelo de madurez en espiral [15] y conjuga otros elementos adicionales (*know-how* previo, sistemas expertos probabilísticos, herramientas para la selección automática de indicadores,…) conformando de esta forma un procedimiento recurrente para la selección de métricas.

El resto del artículo se organizará así: en el apartado siguiente se revisarán los indicadores y métricas de seguridad, los estándares que los definen y su planteamiento para su utilización en la construcción del CMI de la seguridad. En el apartado 3 presentaremos nuestra metodología para la construcción del CMI de seguridad, expondremos los detalles y mecanismos de selección en el apartado 4 y finalmente presentaremos las conclusiones y marcaremos los hitos para futuros trabajos.

2. Antecedentes

El Cuadro de Mando de Seguridad de la Información es una herramienta de control de gestión que traduce la estrategia de seguridad en un conjunto de objetivos relacionados, medidos a través de indicadores, con unas metas fijadas y ligados a unos objetivos que facilite la toma de decisiones.

A continuación describiremos cómo se fijan las métricas de seguridad (los objetivos), para la construcción de nuestro CMI de seguridad que será la herramienta para la gestión de la seguridad, para finalmente describir la metodología que hemos desarrollado.

2.1 Indicadores y Métricas de seguridad en la construcción del CMI de la Seguridad

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

En cambio, los indicadores proporcionan un solo punto en el tiempo, son puntos de vista específicos, factores discretos, mientras que las métricas son derivadas de la comparación de varios indicadores sobre una referencia [12]. Los indicadores son generados a partir de una medición, mientras que las métricas son generadas a partir de un análisis [6]. En otras palabras, los indicadores son datos objetivos en bruto, mientras que las métricas son interpretación de esos datos. Sin embargo en COBIT 4.0 [25] existen algunos matices sobre lo anteriormente expuesto, ya que algunos de los términos que se refieren como indicadores serían lo que se denominan métricas en el NIST 800-55 [8].

En un intento de especificar las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados, es interesante destacar la normativa ISO 27004 [26], que actualmente está en fase de desarrollo (se

ha retrasado su publicación), y que nos va a aportar una visión en el área de las métricas de seguridad.

Una vez revisados los conceptos sobre las métricas, la dificultad siguiente se encuentra en definir cómo deben generarse para construir un programa de métricas de seguridad. En [12] se presentan una serie de pasos principales, que puede utilizarse como referencia en procesos parecidos, y que es una guía para establecer este programa de seguridad:

- Definir el programa de métricas objetivo(s) y los objetivos del mismo.
- Decidir los indicadores que van a conformar las métricas a generar.
- Desarrollar estrategias para la generación de las métricas.
- Establecer puntos de referencia y *benchmarks*.
- Determinar la forma la que las métricas serán reportadas.
- Crear un plan de acción y llevarlo a cabo, y
- Establecer un programa formal de revisión y refinamiento del ciclo.

Una vez definido el proceso, el paso siguiente es desarrollar un formato estándar que garantice el análisis y la evaluación para la selección de estos indicadores de forma repetida. Con esta idea, en NIST [11] podemos encontrar un formato o plantilla que nos provee detalles de sobre 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.

Aún estando claro su propósito, no es sencilla la construcción de una buena métrica. En la definición de métricas es habitual encontrarse con numerosos problemas, siendo los más relevantes los siguientes [21]:

- 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

De acuerdo a nuestra experiencia en SICAMAN, con el uso de métricas de seguridad en nuestros clientes, hemos observado que en la implantación de un SGSI es fundamental tener pocos indicadores al principio pero bien definidos, teniendo claro lo que se está midiendo, porqué y para qué. Se debe de poder hacer comparativas (históricas o benchmarking), hay que medir las cosas de la misma manera. Para ello se deben de buscar procedimientos sencillos y de fácil implementación.

Por otro lado, encontramos el concepto del gobierno de las TI que surge como respuesta a la brecha existente entre las expectativas y los resultados obtenidos en el uso de las TI en las organizaciones. En [4] se propone que entre las medidas a realizar para lograrlo deben realizarse una mejora en las operaciones con un enfoque integrado de seguridad, disponibilidad e integridad de proceso.

También encontramos en COBIT [25] una respuesta para dar soporte al gobierno de TI al brindar un marco de trabajo que garantiza que (figura 1):

- TI está alineada con el negocio
- TI capacita el negocio y maximiza los beneficios
- Los recursos de TI se usen de manera responsable
- Los riesgos de TI se administren apropiadamente

Fig. 1. Áreas principales del Gobierno de TI (COBIT [25])

Esta figura representa un enfoque para el gobierno de TI describiendo los tópicos en los que la gerencia requiere poner atención en sus empresas. La dirección operacional usa procesos para organizar y administrar las actividades cotidianas de TI. Se establecen equivalencias entre los modelos de procesos COBIT y las áreas principales del gobierno de TI, ofreciendo así un puente entre lo que los responsables de seguridad y operaciones deben realizar y lo que la gerencia desea controlar.

Aunque no existe un consenso en cómo realizar el alineamiento estratégico de una organización, en las próximas secciones veremos como el cuadro de mando de la seguridad es una respuesta a estos problemas [32] y va a contribuir a establecer el Gobierno de las TSI. Como más adelante expondremos, el enfoque anterior nos ha servido de base para definir las principales áreas que vamos a contemplar en la construcción de nuestro CMI.

Tal y como hemos expuesto, las conclusiones sobre el marco de Gobierno de TI, las diferentes normativas, indicadores y métricas de seguridad representan una escenario complejo. La implantación de los SGSI requiere la realización de un análisis inaccesible para pequeñas organizaciones en las que es difícil alinear objetivos de gobierno (demasiado abstractos) con las necesidades de seguridad que se tienen en la operativa diaria [16]. Esto nos ha llevado a la elaboración de un modelo de madurez de la seguridad que está especialmente diseñado para ser implantado en las PYMES [17] [20], en las que debido a sus características particulares, resulta difícil adecuar los estándares y modelos sobre métricas y seguridad de la información.

2.2 Proceso de construcción del CMI de Seguridad

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 dé confianza a accionistas, dirección y usuarios.

El Cuadro de Mando de Seguridad de la Información es una herramienta de control de gestión que traduce la estrategia de seguridad en un conjunto de objetivos relacionados, medidos a través de indicadores, con unas metas fijadas y ligados a unas iniciativas. Esta es una herramienta que nos va a permitir en nuestro caso sintetizar los procesos de control de seguridad para ofrecer una información sencilla, resumida y eficaz para observar la evolución de los indicadores y métricas de seguridad.

El modelo de funcionamiento básico sobre el que se sostiene el cuadro de mando es la fijación de unos objetivos en la organización, que son realizados mediante unas actuaciones que tienen reflejo en unas variables clave y que se controlan a través de indicadores [8]. De esta forma, el CMI como herramienta, debe monitorizar los procesos de seguridad en TI y facilitar la toma de decisiones a las organizaciones [5], que en el caso de las PYMES, que suelen carecer de estructura y departamentos especializados en TI, requieren presentar la información de forma muy precisa y simplificada a la dirección.

El aspecto fundamental que determina la elección de la metodología o aproximación que escojamos para el cuadro de mando es la finalidad del mismo. De esta forma, en el proceso general para la construcción de nuestro CMI orientado a PYMES, hay que revisar cómo se han definido los indicadores y seleccionado las métricas. [20].

Existen principalmente dos metodologías para la construcción de un Cuadro de Mando: top-down y bottom-up [13]. El primero es más formal y completo, permitiendo a los distintos grupos de interés definir sus necesidades y objetivos [5]. Por el contrario el efecto abajo-arriba, es menos formal y permite a las organizaciones inmaduras en cuanto a la seguridad, acelerar el desarrollo de sus CMIs. Alternativamente, también se han propuesto otras técnicas en cascada [20]. Estos dos enfoques se exponen de forma práctica en las siguientes tablas [12]:

Tabla 1. Enfoques de construcción del CMI: *top-down*

ENFOQUE *TOP-DOWN*	
a. Definir/lista de objetivos del programa general de la seguridad.	Ejemplo de objetivo: *Reducir el número de infecciones por virus dentro de la compañía en un 30% sobre el año anterior.*
b. Identificar métricas que puedan indicar el progreso hacia cada objetivo.	Ejemplo de métrica: *Ratio de alertas de virus por infecciones en comparación a la referencia del año anterior.*
c. Determinar indicadores necesarios para cada métrica	Ejemplo de indicadores: *Número de alertas de virus en la organización por meses Número de infecciones de virus reportadas*

Tabla 2. Enfoques de construcción del CMI: *bottom-up*

ENFOQUE *BOTTOM-UP*	
a. Identificar indicadores que están o pueden ser recogidos en este proceso	Ejemplo de indicador: *Número medio de vulnerabilidades de Nivel 1 detectadas por servidor en cada departamento utilizando la herramienta de escaneo xyz*
b. Determinar las métricas que pueden ser generadas a partir de los indicadores	Ejemplo de métrica: *Cambio en el número de vulnerabilidades críticas detectadas en los servidores por departamento desde el último informe*
c. Determinar las asociaciones entre las métricas derivadas y los objetivos establecidas en el programa general de la seguridad	Ejemplo de objetivo: *Reducir el nivel de vulnerabilidades detectables en servidores por cada departamento dentro de la compañía*

Por considerar algo rígidos estos métodos [19] debido a que están más orientados a modelos de negocio específicos en lugar de la integración de las TI, la idea de nuestro enfoque para la construcción de un CMI de seguridad 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 [20]. Es importante señalar que en el enfoque bottom-up deben asociarse los datos derivados de las métricas con los objetivos establecidos en el programa del SGSI.

Finalmente, de cara a resolver nuestro problema con un enfoque más orientado a las PYMES, para la construcción de un buen CMI se requerirá que las métricas estén equilibradas [5] [23] de acuerdo a:

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

En el caso del CMI que hemos diseñado, 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 2:

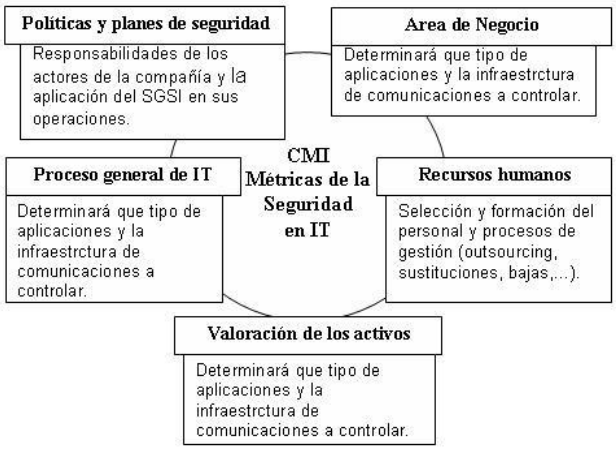

Fig. 2. Perspectivas de nuestro CMI de Seguridad

En relación a nuestro modelo, con base a los dos puntos anteriores y partiendo de una clasificación práctica basada en nuestra experiencia de las mediciones realizadas en las empresas, hemos realizado una clasificación global en cinco categorías, en contraste con el enfoque clásico del CMI de las TI: orientación al cliente, a la organización, a la operativa actual y futura. El objeto de construir un CMI a medida de las necesidades de cada organización nos ha hecho definir las siguientes categorías que están relacionadas con el modelo tradicional [19] y los dominios de COBIT [25]:

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

El principal problema que se encuentra en la construcción de los CMI de seguridad, particularmente en el caso de proyectos orientados a PYMES, es seleccionar las métricas adecuadas que a partir de la utilización de indicadores que

tengan un menor coste, preferentemente obtenidas de forma automática, y que produzcan un menor impacto en el sistema para cumplir los objetivos del SGSI.

Este proceso de decisión no está definido en ninguna guía o estándar de forma óptima para su aplicación en las organizaciones que nos ocupan, ni se tampoco se ha planeado la incorporación en herramientas de procesamiento automático. Así mismo, al ser uno de los procesos claves y más costosos en tiempo para la evaluación de nuestro SGSI debe ser optimizado y este ha sido la principal motivación en nuestro trabajo.

3. Metodología para la construcción de un CMI de la Seguridad

El objetivo de nuestra investigación ha sido automatizar y optimizar el proceso de selección de indicadores y definición de las métricas de seguridad para la construcción de un Cuadro de Mandos Integral para la Seguridad, partiendo de unos indicadores de seguridad predefinidos que nos da el Esquema del SGSI, otros que disponemos previamente y otros que serán necesarios obtener, para ir construyendo las métricas que conformarán el CMI para los objetivos que son definidos por la gerencia. Es por ello, que al ser un proceso clave y de evolución continuo en la medición de nuestro SGSI, que hemos buscado la definición de un proceso sencillo, repetible y fácilmente automatizable.

En el problema que nos ocupa, existe una disparidad entre los requisitos de seguridad de alto nivel (lo qué quieren los gerentes de las organizaciones) y los indicadores que se recogen a bajo nivel (lo que sucede realmente en los sistemas de TI) [6].

Como comentábamos en la sección 2.1, las métricas e indicadores de cara a su identificación e implementación práctica son definidas en base a unas características (tipo de control, forma de obtención,…), [10], [26]. Estos datos son importantes a la hora de construir una buena métrica, pero también se expusieron ciertos problemas que hacen difícil cubrir estas características.

Asimismo, anteriormente hemos relatado la importancia del proceso de selección de los indicadores y de las métricas para la correcta definición de un CMI de seguridad, que garantice el éxito del SGSI y así mantener la confianza de los interesados (stakeholders) en su inversión [10]. Por ello es fundamental que el proceso defina también los objetivos de la gerencia para la evaluación de la seguridad con nuestro CMI.

Sin embargo, a pesar de la próxima aparición del estándar ISO 27004 tratado previamente, tal y como ya expusimos en anteriores trabajos [14], [20], debido a las características particulares, nos sigue resultando complicado adecuar los estándares y modelos sobre métricas y seguridad de la información a las PYMES. Por ello, para adaptar a las necesidades básicas de este tipo de organizaciones, nos dio pie a desarrollar una metodología propia para la evaluación de nuestro SGSI, con base en el modelo de madurez desarrollado [15], y que trata específicamente la problemática en este tipo de empresas.

Este esquema se ha ido refinando y conformando según se presenta en la siguiente figura:

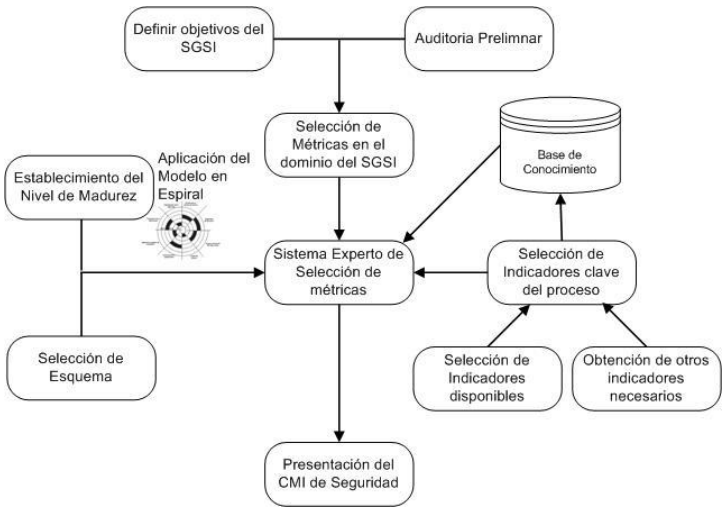

Fig. 3. Esquema de la metodología para la selección de métricas de seguridad

En este esquema se describe el proceso de obtención del CMI de seguridad, a partir de los objetivos definidos para el SGSI, la auditoría preliminar realizada y los indicadores clave recogidos. Otra dato importante que se tiene en cuenta es el nivel de madurez que tiene la empresa en ese momento y el esquema seleccionado para la empresa [14]. Finalmente se hace uso de la experiencia anterior y de los valores de referencia (benchmarks) que se obtienen a partir de las empresas u organizaciones que se dedican a la misma actividad.

Con todas estas variables, el proceso central del proceso es el sistema experto que nos va a permitir seleccionar los mejores indicadores justificado en el trabajo que realizaría un auditor experto (figura 3).

Nuestro método forma parte de un proceso general con diferentes procesos que fueron descritos de forma parcial en anteriores trabajos [14] y [20]. En ellos se exponían algunos aspectos clave a la hora de seleccionar los indicadores y métricas que iban a conformar el CMI de seguridad y que a continuación presentamos.

4. Descripción detallada del proceso de Selección de métricas de seguridad

Debido a la diversidad de criterios encontrados, la problemática suscitada y la importancia que el proceso de definición de las métricas de seguridad tiene para la construcción del CMI, hemos considerado plantear un proceso para la selección de indicadores y construcción de las métricas que conformarán el CMSI.

Como propuesta para resolver el problema, hemos diseñado un algoritmo para la selección de indicadores a medida de cada empresa y que está basado en un sistema

experto probabilístico [20]. En su conjunto el proceso global hace uso de nuestro modelo en espiral aplicado a la implantación de SGSI, procesos de selección de Esquemas, sistemas de selección de métricas basados en redes bayesianas y una realimentación de las métricas seleccionadas para nuestro el proceso de selección.

El motor de inferencia implementa un modelo probabilístico basado en una red bayesiana. El proceso de construcción de este modelo tiene varias fases: en primer lugar es preciso definir las variables, a continuación obtener la estructura de la red y finalmente obtener las distribuciones de probabilidad locales.

Las variables que se han utilizado para construir la red de razonamiento bayesiano son las siguientes:

- **TE**: Tipo de Empresa (pequeña, mediana, grande)
- **TA**: Tipo de Activo, (son 23 en el esquema que define nuestro modelo)
- **A**: Obtención Automática (S/N)
- **NM**: Nivel de madurez (1,2,3)
- **R**: Ratio (*benchmark*) de incidencias (en rango %).
- **C**: Coste de obtención (bajo/medio/alto)
- **F**: Frecuencia de medición (bajo/medio/alto).
- **P**: Peso del indicador en el CMI según el tipo de dominio (1-5)

La red bayesiana (RB) se compone de dos partes. Por un lado, la estructura, el modelo o parte cualitativa: un grafo dirigido acíclico (GDA) donde cada nodo representa la variable aleatoria y los arcos representan dependencias probabilísticas entre las variables. Por otra parte, de una distribución condicional de probabilidades de la forma P(x|Πx) para cada nodo x dado su conjunto de padres Πx.

Para la primera parte, hay distintos enfoques para obtener la estructura de la red, aunque sin entrar en el detalle del razonamiento apuntamos que hemos ajustado las dependencias de las variables según nuestra experiencia [15][16], lo que ha conformado el siguiente GDA propuesto [20]:

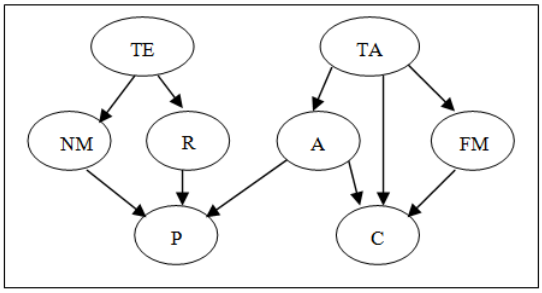

Fig. 4. Red causal para la selección de métricas de seguridad

Para la parte de la distribución condicional, hemos realizado un algoritmo de agrupamiento para obtener los grupos maximales y obtener el cálculo de probabilidades de cada nodo a partir de la red anterior. Con este valor se realiza el cálculo de la propagación de la probabilidad para así analizar cada uno de los

indicadores seleccionados, definiendo su contribución en la métrica si supera un umbral definido [20].

La idea esencial consiste en aprovechar las relaciones de dependencia (y por tanto también las de independencia) existentes entre las características del indicador y del problema para ayudar a definir la contribución del mismo en la formulación de la métrica. De esta forma se logra una implantación progresiva de la seguridad dependiendo de dos parámetros principales:

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

De esta forma y a partir del aprovechamiento del know-how con la realimentación de métricas de seguridad anteriormente utilizadas con éxito y mediante esquemas de seguridad [14]-[16], se conforma un proceso repetible en las organizaciones que tienen varios elementos en común y que se reflejan en las características de las métricas utilizadas y en algunas de las variables del sistema experto.

Este proceso de **formulación de las métricas** que conforman nuestro cuadro de mando, lo que es el núcleo repetible del proceso, se muestra en el siguiente algoritmo:

Algoritmo se selección de indicadores de nuestro mediante uso de red bayesiana

```
/* Create list of indicators */
FOR Each Control object in the schema
     IF Exist Indicator
            (Automatic or Knowledgebase) THEN
            I_i.Value = V_i
     ELSE
            Calulate V_i.Value
     ENDIF
     Insert into IndicatorList (I_i,V_i)
END FOR
/* Calculate metric value */
FOR Each element M_i of MeasurementsList
     Calculate P(M_i) (Bayesian Net)
     IF P(M_i)>Umbral THEN
            M_i = P(I_i)*V_i
     ENDIF
     Metric.Value = ∑(M_i)/∏(P(I_i))
     Insert into MetricList(M_i)
END FOR
Return MetricList
```

Se parte de una selección inicial de indicadores, que agrupados en su dominio, utilizan el sistema experto para definir su aplicación. Dentro del sistema experto se calcula la probabilidad de la contribución del indicador según sus características.

La implementación de este algoritmo es una parte del proyecto global que conforma nuestra herramienta de gestión de seguridad: SCMM-PYME. El proceso de evaluación de dicho SGSI implementa el proceso descrito en punto 3 e incorpora el proceso de selección como el núcleo nuestro método de construcción del CMI de la seguridad (Figura 5):

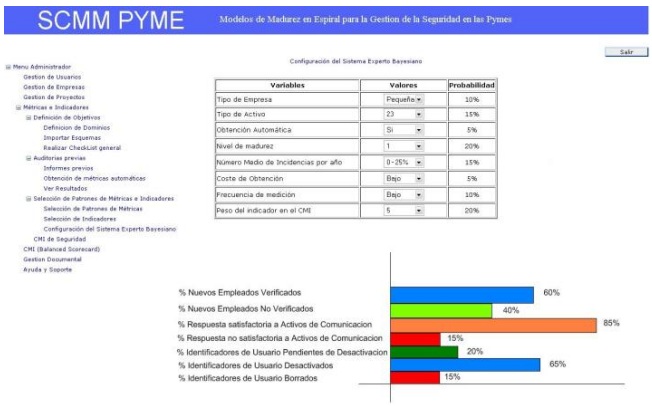

Fig. 5. Imagen de nuestra herramienta con la configuración del SE y para conformar el CMI de la Seguridad

La utilización de esta herramienta en nuestros clientes, como ya fue comentado, arroja datos satisfactorios sobre su aplicación y el cumplimiento de los objetivos propuestos. En cualquier caso, será preciso una evolución de este proceso para la obtención de nuevos indicadores, ya que son múltiples las herramientas que cada día aparecen y que sirven para obtener los indicadores automáticos y a partir de los datos recogidos en su utilización.

5. Conclusiones y próximos trabajos

Para lograr un gobierno efectivo, la seguridad de la información es fundamental, siendo necesario poder evaluar y medir la capacidad de los procesos. Para ello se deben alinear las necesidades de seguridad con las de negocio, con lo que es preciso disponer de indicadores adecuados que nos ofrezcan unas métricas eficaces para medir si nuestro SGSI responde a la inversión realizada en él.

Las métricas de seguridad son la clave que van a permitir cuantificar la implantación de los controles y evaluar la eficacia de los mismos, identificando posibles acciones de mejora. Por ello, en estos procesos de definición de métricas es vital tener en cuenta la naturaleza del negocio y organización, para poder adecuarse a cada tipo de actividad.

A partir de estas métricas se construye el CMI de seguridad como una herramienta que nos proveerá una información muy útil para la gestión y poder revisar los objetivos del SGSI. En base a las métricas e indicadores seleccionados y organizados, el CMI nos aportará:

- Control de la gestión de la seguridad relacionando los objetivos de la organización con el SGSI.
- Perspectiva histórica sobre las mejoras y evolución del SGSI

- Una referencia o comparación (benchmarking) interno y externo de nuestras métricas con las de otras organizaciones.
- Una herramienta de información a la Dirección para soporte a la toma de decisiones.
- Relacionar la seguridad con los objetivos de la empresa o del departamento

Asimismo, los equipos de auditoría en TI deben buscar y reevaluar las herramientas automatizadas que emplean para considerar nuevas y mejores formas en la manera de realizar sus trabajos.

La propuesta presentada ha tenido en cuenta los parámetros anteriores y propone un nuevo método de construcción de CMI de seguridad, mediante la selección y transformación de los indicadores en métricas, que hace uso de Sistemas Expertos (SE) basados en redes bayesianas. Aunque está claro que este tipo de sistemas no son la solución a todas nuestras necesidades, sino a una parte importante de ellas, también está claro que debemos tenerlas en cuenta cuando se logra obtener un mejor rendimiento.

En el presente artículo hemos conjugado todos los puntos anteriores para dar lugar al procedimiento completo de selección, aprovechamiento del *know-how*, automatización e implementación con un sistema experto que permite construir el SGSI de forma óptima y buscando rápidamente el ROI en las organizaciones.

Nuestro proceso forma parte de una herramienta de reciente creación que incorpora nuestro proceso de construcción del SGSI en base al modelo de madurez definido. Aunque los resultados que hemos obtenido en las primeras pruebas, hacen presagiar un buen futuro, se debe seguir trabajando en un refinamiento general y del proceso de selección. Para ello se estudia incorporar nuevos indicadores automáticos, mejorar los algoritmos actuales e incorporar nuevos algoritmos de aprendizaje.

Agradecimientos

Esta investigación es parte de los proyectos ESFINGE (TIN2006-15175-C05-05), concedido por el Ministerio de Educación y Ciencia y QUASIMODO (PAC08-0157-0668) financiado por la Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha.

Referencias

1. Chapin, D., Akridge, S. "How can security be measured?". Information Systems Control Journal, Volume 2, 2005.
2. Corletti, A. ISO-27001 e ISO-27004. http://www.kriptopolis.org/iso-27001-e-iso-27004
3. Erro, G. Seguridad TICs, ¿qué hay que medir?. Aplicabilidad de las Métricas en Seguridad. Jornada Técnica Seguridad Informática.
4. Hardy, G. (2006). Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. Information Security Technical Report 11 , 55-61.

5. Hervada F. y Piattini, M. Gobierno de las Tecnologías y Seguridad de la Información. RAMA (2007).
6. Heyman, T., Scandariato, R, Huygens, C. From security objectives to security metrics: a round trip.. SecSE Barcelona 2008
7. ITGI (2005). IT Alignment: Who Is in Charge?. IT Governance Domain Practices and Competencies, IT Governance Institute.
8. Kaplan, R.S. y Norton, D.S. (1992): "The Balanced Scorecard-Measures That Drive Performance", Harvard Business Review, septiembre-octubre.
9. Mañas, José A. Security Metrics and Measurements for IT. UPGRADE. Vol. VI, issue no. 4, August 2005.
10. Martín Soria, D. Nuevas Tecnologías Desplegadas con Inteligencia, ¿Serán las Aliadas de los Profesionales de Auditoría de TI en las Grandes Corporaciones? Information Systems Control Journal, Volume 1, 2008.
11. NIST Special Publication 800-80. Initial Public Draft. Guide to Performance Metrics for Information Security. April 2006.
12. Payne, S.C. A Guide to Security Metrics. (SANS Security Essentials GSEC Practical Assignment) SANS Institute. June 2006.
13. Opacki, D. Security Metrics: Building Business Unit Scorecards. Dic 2005. 4-8
14. Sánchez, L.E., Villafranca, D., Fernández-Medina, E. y Piattini, M Developing a model and a tool to manage the information security in Small and Medium Enterprises. SECRYPT (2007).
15. Sánchez, L.E , Villafranca, D.., Fernández-Medina, E. y Piattini, M. Practical Approach of a Secure Management System based on ISO/IEC 17799. Ares (2005)
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. WOSIS 2006.
17. Sánchez, L.E., Villafranca, D., Fernández-Medina, E. y Piattini, M Developing a model and a tool to manage the information security in Small and Medium Enterprises. SECRYPT (2007).
18. The European Information Technology Observatory : www.eito.com
19. 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
20. Villafranca, D., Sánchez, L.E., Fernández-Medina, E. y Piattini, M. Construcción de un CMI de la Seguridad: Selección de indicadores mediante un sistema experto probabilístico. CIBSI'07. Mar de Plata, Nov.2007
21. 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.
22. Van Grembergen, W., De Haes, S. COBIT's Management Guidelines Revisited: The KGIs/KPIs Cascade. Information Systems Control Journal, Volume 6, 2005.
23. Van Grembergen, W., De Haes, S. Using COBIT and the Balanced Scorecard as Instruments for Service Level Management. Information Systems Control Journal, Volume 4, 2003.
24. Washizaki, H., Kubo, A., Fukazawa, Y.."Measuring Abstraction Levels of Security Patterns" Proceedings of the 1st International Workshop on Software Patterns and Quality (SPAQu'07)", pp.59-60 (2007)
25. COBIT® 4.0. 2005. IT Governance Institute (ITGI) (www.itgi.org)
26. ISO/IEC WD 27004. Information technology — Security techniques — Information security management — Measurements