Actas
X Reunión Española sobre Criptología y Seguridad de la Información

Editores: Luis Hernández Encinas
Ángel Martín del Rey

Editores: Luis Hernández Encinas y Ángel Martín del Rey

Diseño de cubiertas: Yaiza Cortés Gómez

Imprime: SIGNE S.A. Impresores de Seguridad
Avda. de la Industria, 18 – 28760 Tres Cantos, (Madrid)
www.signe.es

Caminamos con paso firme hacia el pleno establecimiento de la que se ha dado en denominar Sociedad de la Información. No sólo los diferentes gobiernos y administraciones públicas sino también las empresas y organismos privados se han implicado en este desarrollo poniendo a disposición de los ciudadanos nuevos, potentes y eficaces servicios telemáticos: gobierno electrónico, comercio electrónico, voto electrónico, etc. En este sentido en el año 2006 se empezó a expedir el nuevo Documento Nacional de Identidad Electrónico (DNIe) que permite a su poseedor la firma digital de documentos electrónicos. Este fascinante nuevo escenario exige el desarrollo de algoritmos, medidas y políticas de seguridad que garanticen la confidencialidad, la integridad, la autenticidad y el no repudio de las gestiones realizadas.

Consecuentemente se ha dado lugar a un enorme esfuerzo de investigación en el campo de la protección de la información. Así, una de las líneas de investigación de la comunidad científica de mayor importancia y actualidad es el diseño, análisis e implantación de protocolos criptográficos que garanticen la seguridad de los datos transmitidos, almacenados o gestionados electrónicamente.

La *Reunión Española sobre Criptología y Seguridad de la Información* (RECSI) es el congreso científico referente español en el tema de la Seguridad en las Tecnologías de la Información. En él se dan cita periódicamente los principales investigadores españoles en el tema así como invitados extranjeros de reconocido prestigio. En el año 2008 se celebrará la décima edición de este congreso en el mes de septiembre y en la ciudad de Salamanca. Las pasadas ediciones se realizaron en Palma de Mallorca (1991), Madrid (1992), Barcelona (1994), Valladolid (1996), Torremolinos (1998), Santa Cruz de Tenerife (2000), Oviedo (2002), Leganés (2004) y Barcelona (2006).

La X RECSI se ha desarrollado entre el 2 y el 5 de septiembre de 2008. En ella se han llevado a cabo varias conferencias plenarias a cargo de investigadores de reconocido prestigio (Carlo Blundo, Ljupco Kocarev, Hugo Scolnik, Fausto Montoya) y de organismos y agencias tanto públicas como privadas (Centro Criptológico Nacional, Ministerio del Interior, Dirección General de Innovación y Modernización Administrativa de la Junta de Castilla y León, Signe, Realsec y Ericsson). También se han presentado 70 contribuciones científicas divididas en dos sesiones paralelas: Criptología y Seguridad de la Información.

Queremos dar las gracias a todos los patrocinadores y colaboradores por su apoyo moral y económico: CajaDuero, Realsec, Ericsson, IECISA, Junta de Castilla y León, Universidad de Salamanca, Centro Criptológico Nacional, Fábrica Nacional de Moneda y Timbre, Consejo Superior de Investigaciones Científicas, Ministerio de Ciencia e Innovación, Criptored, Red Temática de Matemáticas para la Sociedad de la Información y RENFE.

Finalmente queremos también mostrar nuestra más profunda gratitud a *Signe S.A. Impresores de Seguridad* por la elaboración de estas actas y por su incondicional apoyo.

Septiembre de 2008

Luis Hernández Encinas

Ángel Martín del Rey

Comités

Comité de Honor

S.A.R. El Príncipe de Asturias D. Felipe de Borbón
Excma. Sra. Ministra de Educación
Excma. Sra. Ministra de Defensa
Excmo. Sr. Ministro de Interior
Excmo. Sr. Secretario de Estado de Universidades e Investigación
Excmo. Sr. Consejero de Educación de la Junta de Castilla y León
Excma. Sra. Consejera de Administración Autonómica de la Junta de Castilla y León
Excmo. Sr. Alcalde de Salamanca
Excma. Sra. Presidenta de la Diputación de Salamanca
Excmo. y Magfco. Sr. Rector de la Universidad de Salamanca
Excmo. Sr. Vicerrector de Investigación de la Universidad de Salamanca

Comité Organizador

Presidente: Ángel Martín del Rey, Universidad de Salamanca
Vicepresidente: Luis Hernández Encinas, C.S.I.C.
Secretario: Gerardo Rodríguez Sánchez, Universidad de Salamanca
Tesorera: Ascensión Hernández Encinas, Universidad de Salamanca
Vocales: María Teresa de Bustos Muñoz, Universidad de Salamanca
María Araceli Queiruga Dios, Universidad de Salamanca
Yaiza Cortés Gómez, Universidad de Salamanca
Javier Espinosa García, C.S.I.C.

COMITÉ CIENTÍFICO

Abascal Fuentes, Policarpo	Universidad de Oviedo
Álvarez Marañón, Gonzalo	C.S.I.C.
Amigó García, José María	Universidad Miguel Hernández
Areitio Bertolín, Javier	Universidad de Deusto
Borrell Viader, Joan	Universidad Autónoma de Barcelona
Caballero Gil, Pino	Universidad de La Laguna
Dávila Muro, Jorge	Universidad Politécnica de Madrid
Domingo Ferrer, Josep	Universidad Rovira i Virgili
Durán Díaz, Raúl	Universidad de Alcalá de Henares
Fernández-Medina Patón, Eduardo	Universidad de Castilla La Macha
Fúster Sabater, Amparo	C.S.I.C.
González Vasco, Mª Isabel	Universidad Rey Juan Carlos
Gutiérrez Gutiérrez, Jaime	Universidad de Cantabria
Hernández Encinas, Luis	C.S.I.C.
Hernández Goya, Candelaria	Universidad de La Laguna
Herrera Joancomartí, Jordi	Universitat Operta de Catalunya
Huguet Rotger, Llorenç	Universidad de las Islas Baleares
López Muñoz, Javier	Universidad de Málaga
Martín del Rey, Ángel	Universidad de Salamanca
Martínez López,Consuelo	Universidad de Oviedo
Miret Biosca, José María	Universidad de Lleida
Padró Laimon, Carles	Universidad Politécnica de Cataluña
Peinado Domínguez, Alberto	Universidad de Málaga
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
Sáez Moreno, Germán	Universidad Politécnica de Cataluña
Salazar Riaño, José Luis	Universidad de Zaragoza
Sánchez Ávila, Carmen	Universidad Politécnica de Madrid
Sempere Luna, José María	Universidad Politécnica de Valencia
Soriano Ibáñez, Miguel	Universidad Politécnica de Cataluña
Tena Ayuso, Juan	Universidad de Valladolid
Villar Santos, Jorge	Universidad Politécnica de Cataluña

ÍNDICE

CONFERENCIAS INVITADAS

CRIPTOLOGÍA

Diseño de patrón de selección de métricas para la construcción de CMI de la seguridad

D. Villafranca[1], L. E. Sánchez[1], E. Fernández-Medina[2] y M. Piattini[2]

***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. El uso de patrones y su aplicación para resolver problemas de seguridad en las TI ha ido creciendo cada vez más y en diferentes aspectos de este campo. Este artículo presenta una solución al problema de selección de métricas de seguridad mediante la definición y uso de un patrón de selección específico, para así facilitar la construcción del CMI de seguridad específico en entornos de PYMES.**

***Palabras clave*—Métricas de seguridad, indicadores, cuadro de mandos de la seguridad de la información (CMSI), sistema experto probabilístico, patrones de seguridad.**

I. 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 [30], 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 vulnerabilidades en los momentos más tempranos que se produzcan.

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 [7] 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. 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

Esta investigación es parte de los proyectos DIMENSIONS (PBC-05-012-1) y MISTICO (PBC-06-0082), parcialmente financiado por el FEDER y por la Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha y el proyecto SCMMPYME (FIT-360000-2006-73) financiado por el PROFIT y concedido por Ministerio de Industria, Turismo y Comercio.

[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, Departamento de Tecnologías y Sistemas de Información Universidad Castilla-La Mancha 13.071 Ciudad Real, España. {Eduardo.FdezMedina, mario.piattini}@uclm.es.

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 17799 [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 [12], y sobre todo, hemos adaptado la idea de patrones de diseño de seguridad [4] [17] a la construcción de nuestro CMI de seguridad. 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], 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 y por último se revisará la utilización de patrones de diseño en el ámbito de la seguridad. En el apartado 3 presentaremos el proceso de construcción del CMI de seguridad basado en un patrón de selección de métricas de seguridad. Revisaremos un caso de estudio de aplicación de este patrón (apartado 4) y finalmente expondremos las conclusiones y marcaremos los hitos para futuros trabajos.

II. BACKGROUND

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 los principales conceptos del uso de los patrones de seguridad, describiendo la plantilla general que lo define.

A. 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 [11]. Los indicadores son generados mediante a partir de una medición, mientras que las métricas son generadas a partir de un análisis [6]. En otras palabras, los indicadores 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 [7].

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 [27], que actualmente está en fase de desarrollo (está prevista su publicación en noviembre de este año), 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 [11] 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 [28] 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 la empresa 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 y desde el primer momento. 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 [5] 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 (según COBIT [25])

Esta figura representa un enfoque para el gobierno de TI describiendo los tópicos en los que la gerencia requiere poner atención para gobernar la TI 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 [14] [20], en las que debido a sus características particulares, resulta difícil adecuar los estándares y modelos sobre métricas y seguridad de la información.

B. 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 [7]. De esta forma, el CMI como herramienta, debe monitorizar los procesos de seguridad en TI y facilitar la toma de decisiones a las organizaciones, que en el caso de las PYMES, que suelen carecer de estructura y departamentos especializados en TI, requieren presentar la información de forma muy precisa y simplificada a la dirección.

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 [12]. El primero

es más formal y completo, permitiendo a los distintos grupos de interés definir sus necesidades y objetivos. 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 [11]:

TABLA I
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 II
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 [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:

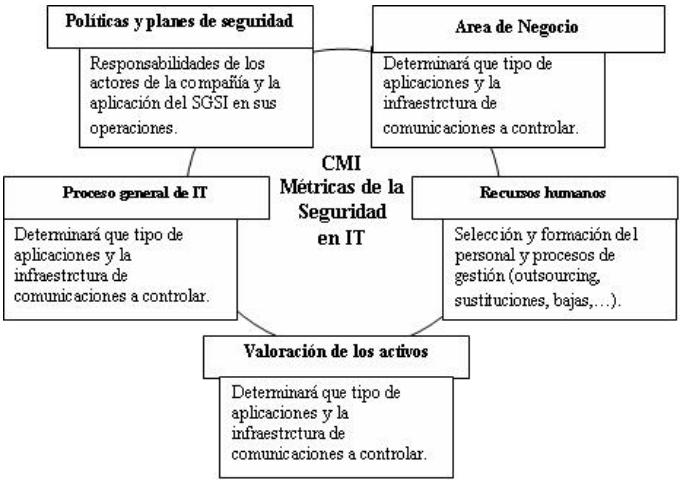

Fig. 2. Perspectivas de nuestro CMI de Seguridad

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:

- **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.

C. Patrones de diseño para la seguridad

La idea del uso de patrones en la ingeniería tuvo su origen en el campo de la arquitectura. A finales de la década de los años 70, Christopher Alexander, escribió varios libros que describían patrones en arquitectura de construcción y planificación urbana. Las ideas presentadas en estos libros son aplicables a varios campos además de la arquitectura, incluyendo el software [17]. Los patrones se han aplicado también en campo de las TI y fueron usados inicialmente en la definición de arquitecturas software, proponiendo diseños para interfaces de usuario.

Abstrayendo el concepto original, un **Patrón** es una solución a un problema dado dentro de un contexto definido. Los patrones permiten capturar el conocimiento experto en el área de la seguridad, ya que modelan soluciones para escenarios que se han analizado en múltiples ocasiones. Los patrones son independientes del dominio particular donde son aplicados, pudiendo ser reutilizados en otros escenarios. También hay que considerar que se pueden presentar en diferentes niveles de abstracción [24].

En el ámbito del desarrollo de aplicaciones, los Patrones de Seguridad fueron propuestos como un medio de superar la brecha existente entre los desarrolladores y los expertos en seguridad. Fueron planteados para captura experiencia en seguridad para problemas recurrentes, de forma que fueran usados y comprendidos por desarrolladores que no eran expertos en seguridad [13].

Una lista actualizada de los patrones relativos a la seguridad se puede encontrar en [17], [18]. Estos patrones son expuestos en orden cronológico con el fin de reflejar la evolución de los mismos, agrupándose de la siguiente forma:

- **Aplicaciones de Seguridad**: Encontramos ejemplos de patrones básicos como: check point, single access point, human computer interface, etc…
- **Software criptográfico**: que modelan aspectos para mantener la confidencialidad, integridad, autenticidad y no repudio.
- **Patrón de autenticación**: Referencia trabajos de autenticación de procesos para acceso a objetos distribuidos.
- **Patrones de autorización**: En este conjunto se incluyen patrones de filtrado de datos, clientes RPC, autenticación y guardas de seguridad.

Como ejemplo de aplicación de patrones de Seguridad, en [13] se recoge de forma específica buena cuenta de ellos, haciendo un análisis comparativo de sus características principales.

Por último mencionamos entre las principales referencias sobre patrones orientados a la construcción e implementación de sistemas seguros, las propuestas de Eduardo B. Fernández [4]. En múltiples trabajos se analizan y diseñan patrones básicos en varios niveles y que son implementados en diferentes fases del ciclo de desarrollo.

La diversidad de usos y aplicación del concepto de patrón, más específicamente en el ámbito de la seguridad, nos ha servido de base para definir el proceso de selección de métricas que estamos implementando, dentro de un ámbito específico y que da soporte a este proceso clave en la construcción de nuestro cuadro de mando de la seguridad.

III. PROCESO PARA CONTRUCCIÓN DE UN CMI DE LA SEGURIDAD BASADO EN PATRONES DE SELECCIÓN

En todo el escenario descrito, nuestra principal preocupación ha sido la selección de las métricas adecuadas que deben definir nuestro CMI de la seguridad. 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.

Pasamos a describir las características del mismo.

A. Plantilla para la definición del patrón

Uno de los principales problemas a la hora de realizar un patrón encontramos el problema de cómo identificarlo dentro del escenario donde se va a aplicar. Algunos autores [8] apuntan un conjunto de checklist para escribir un buen patrón. Entre estos criterios encontramos que el patrón debe describir un problema sencillo, dentro de un contexto, con una serie de reglas para construir la solución y que ésta se resuelve de forma óptima.

Existe también el problema de cómo definir o estructurar el patrón con el fin de qué sea más sencillo identificar su propósito. Los patrones se organizan en varias secciones conformando una plantilla que describe las principales características del mismo y su aplicación. Cada sección de la plantilla de patrón contribuye a entender el patrón particular.

Existen varios formatos de plantilla con diferentes secciones [8], [13], [17], estando en casi todas ellas presentes las siguientes:

- Nombre: Descripción que además sirve para identificarlo en la comunidad que lo utiliza.
- Contexto: Conjunto de entornos bajo los cuales existe el patrón.
- Problema: Describe los problemas de seguridad que se han encontrado y que justifica su creación.
- Solución: Describe la solución y sus elementos en más detalle.

También podemos encontrar otras características opcionales, tales como consecuencias o resultados que ofrece, patrones relacionados y conocidos, etc... que se utilizan de forma opcional en función del campo de donde se define el patrón.

Esta plantilla nos va a servir como referencian en la explicación de nuestro patrón de selección de métricas. En el apartado siguiente exponemos los motivos que nos han llevado a definir un patrón para dar solución al problema que hemos expuesto anteriormente.

B. Proceso de construcción del CMI de seguridad mediante un sistema experto probabilístico

El uso de patrones en el campo de la seguridad es muy diverso tal y como analizábamos en la sección 2.3. Los patrones han sido utilizados en otros entornos de las TI como las bases de datos, sistemas operativos, etc. [4], lo que nos da una idea de la amplitud y uso de este tipo de herramienta.

Actualmente, los patrones son un gran campo de investigación sobre la seguridad en las TI, planificando su aplicación en nuevos escenarios que permitan implantar mecanismos de seguridad ya conocidos ante las amenazas que surgen a diario.

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]. Los patrones de seguridad pueden ayudar a salvar esta brecha, facilitando la selección e integración de indicadores y permitiendo la agregación de las métricas de alto nivel en un CMI de seguridad.

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], [27]. Estos datos son importantes a la hora de construir una buena métrica, pero también se expusieron ciertos problemas que hacen difícil cubrir estas características. Como respuesta a estas dificultades se han tenido en cuenta estos detalles en el proceso de selección de métricas y que son contempladas dentro del patrón que se presenta.

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. El esquema del mismo lo vemos en la siguiente figura:

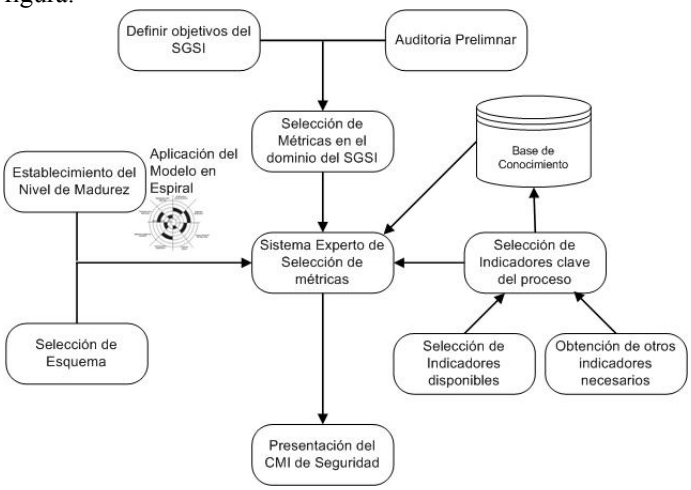

Fig. 3. Esquema del patrón para la selección de métricas de seguridad

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. Este proceso de selección es el patrón que proponemos y que forma parte del proceso de construcción de cuadros de mando antes presentado (figura 3).

En la siguiente sección comentamos los detalles del patrón propuesto.

C. Descripción detallada del patrón 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 patrón de seguridad específico para la selección de indicadores y construcción de las métricas que conformarán el CMSI. Dicho patrón tiene por objeto principal su aplicación en la construcción de SGSI a partir de los objetivos de estas organizaciones y con la experiencia recogida previamente en las mismas.

Para exponer el patrón de selección que hemos desarrollado, utilizaremos la plantilla que analizamos en la sección 3.1, con algunas características adicionales que nos servirán para explicarlo mejor:

1) *Motivación:*

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.

Nuestra propuesta de patrón de selección 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 ahora agrupamos en un esquema general.

2) *Contexto:*

La implementación de un SGSI que se reflejará en un CMI a medida de las PYMES y a partir de los objetivos que define la gerencia, enlazados con indicadores obtenidos previamente a partir de herramientas automatizadas.

En relación al marco que justifica las características particulares que componen el proceso de selección, se debe

tener en cuenta:

- Es un proceso repetitivo a lo largo del ciclo de vida del SGSI, lo que justifica la confección de patrón de seguridad particular para este proceso.
- Dicho esquema de selección precisa aplicar un algoritmo de selección específico que emula el conocimiento experto en el ámbito de la seguridad.
- La razón para la selección de este tipo de sistema experto probabilístico, es que utilizando las redes bayesianas podemos introducir conocimiento del experto en los nodos del árbol de decisión para la selección, utilizando las dependencias entre variables (características de los indicadores y del SGSI).

3) *Problema:*

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 preliminares 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.

4) *Solución:*

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.

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 realimentar el modelo de selección de métricas (el patrón y su aplicación en futuros escenarios de empresas u organizaciones similares.

Los principales componentes de la solución del sistema experto que se ha diseñado no difiere de los que componen un sistema experto típico: memoria de trabajo, base de conocimiento y motor de inferencias. Los componentes complementarios, tales como el subsistema de aprendizaje y el subsistema de explicación, no se han implementado completamente.

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 una 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 $P(x|\Pi x)$ 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, lo que ha conformado el siguiente GDA propuesto:

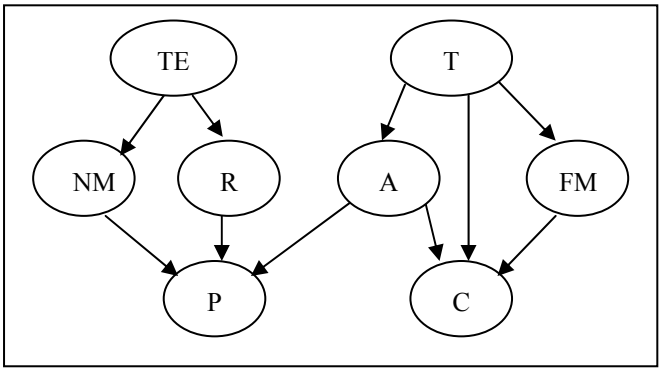

Fig. 4. Red causal para la selección de métricas de seguridad

Para la parte de la distribución condicional, hemos realizado un algoritmo de agrupamiento para obtener los grupos maximales y obtener el cálculo de probabilidades queda reflejado en la siguiente tabla:

TABLA III.
OBTENCIÓN DE LAS PROBABILIDADES DE CADA NODO

Variable	Grupo	Probabilidad
A	G1	$P(TE) = _{TA,\ FM} P(A,TA,FM)$
TA	G1	$P(TA) = _{A,\ FM} P(A,TA,FM)$
FM	G1	$P(F) = _{A,\ TA} P(A,TA,FM)$
C	G2	$P(C) = _{TE,\ FM} P(A, FM, C)$
P	G3	$P(P) = _{NM,R,TE} P(NM, R, P ,A)$
TE	G4	$P(TE) = _{NM,\ R} P(TE, NM, R)$
NM	G4	$P(NM) = _{TE,\ R} P(TE,NM,R)$
R	G4	$P(R) = _{TE,\ NM} P(TE,NM,R)$

Mediante la tabla anterior se realiza el cálculo de la propagación de la probabilidad. Dicho dato es utilizado para analizar cada uno de los indicadores seleccionados, definiendo su contribución en la métrica si supera un umbral definido.

5) *Consecuencias:*

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.

La principal ventaja de este patrón la 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.

Mediante el uso de este patrón obtenemos un procedimiento repetible en múltiples organizaciones que, de una forma óptima, pueden implementar CMI de seguridad a partir de indicadores y métricas que son de fácil obtención y que han sido probadas con éxito en otras organizaciones similares.

Por último, señalar que el aprovechamiento del know-how a partir de la realimentación de métricas de seguridad anteriormente utilizadas con éxito y mediante esquemas de seguridad [14]-[16], conforman 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.

6) *Implementación:*

El 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.

```
Algorithm Selecting metric

/* 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
```

Fig. 5. Algoritmo se selección de indicadores de nuestro mediante uso de red bayesiana

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.

Otro de los procesos claves es la utilización de un modelo de madurez adaptado a este tipo de organizaciones (mediante el modelo en espiral).

7) *Usos conocidos:*

La implementación de este patrón 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 la sección 3.2 e incorpora el patrón de selección como el núcleo del proceso de construcción del CMI de la seguridad (Figura 6).

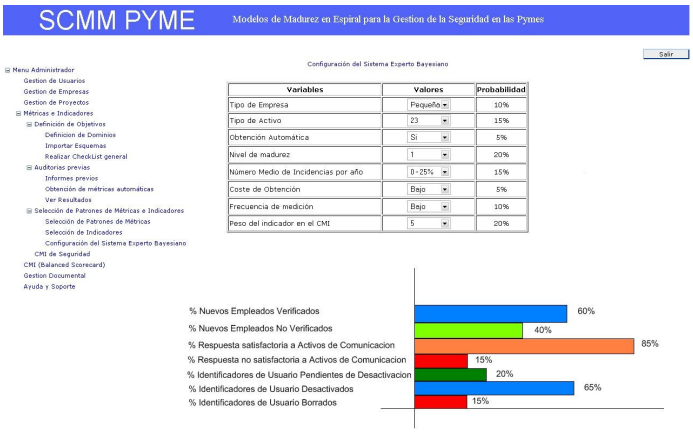

Fig. 6. Imagen de nuestra herramienta con la configuración del SE y el CMI de la Seguridad

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, la evolución del patrón es continua para el caso de la obtención de indicadores automáticos, ya que son múltiples las herramientas que cada día aparecen y que sirven para obtener los indicadores automáticos, por lo que es posible que este patrón evolucione con la incorporación de nuevos indicadores y con los datos recogidos en su utilización.

8) *Patrones relacionados:*

Los patrones relacionados nos los encontramos en niveles inferiores para la obtención de indicadores y definición de métricas claves en los procesos de seguridad: autenticación, autorización, single access point y otras características para la implementación de seguridad en aplicaciones.

Del resto de los diferentes patrones de seguridad revisados, no se ha encontrado un enfoque o aplicación similar en este tipo de escenarios, lo que conforma la novedad principal de nuestro trabajo.

IV. Conclusiones

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 permitirán evaluar la eficacia de los mismos, permitiendo identificar posibles acciones de mejora. Por ello, en estos procesos de definición de métricas es vital deben 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. Para ello, hemos definido enfoque novedoso para definir un patrón para la selección y transformación de los indicadores en métricas, que hace uso de Sistemas Expertos (SE) basados en redes bayesianas. Auque 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 a un patrón que realizará el procedimiento completo de selección, aprovechamiento del know-how, automatización e implementación con un sistema experto que permite construir el CMSI de forma óptima y buscando el rápidamente el ROI en las organizaciones en las que estamos trabajando.

Tanto nuestro patrón, como nuestro modelo general, 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 patrón de selección. Para ello se estudia incorporar nuevos patrones de seguridad, mejorar los algoritmos actuales e incorporar nuevos algoritmos de aprendizaje.

En próximos trabajos iremos describiendo más en profundidad los detalles de este patrón, presentando nuevos datos de su ejecución práctica y refinando su funcionamiento y exponiendo nuevos modelos asociados a la resolución de problemas de seguridad.

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] E. B. Fernandez, R. Pan A pattern language for security models PLoP 2001 conference.

[5] 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.

[6] Heyman, T., Scandariato, R, Huygens, C. From security objectives to security metrics: a round trip.. SecSE Barcelona 2008

[7] Kaplan, R.S. y Norton, D.S. (1992): "The Balanced Scorecard-Measures That Drive Performance", Harvard Business Review, septiembre-octubre.

[8] Lea, D. "Checklist on how to write good pattern". Hillside Group (ww.hillside.net/patterns/writing/writingpatterns.htm)

[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] Payne, S.C. A Guide to Security Metrics. (SANS Security Essentials GSEC Practical Assignment) SANS Institute. June 2006.

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

[13] Rosado, D., Fernández-Medina, E., Piattini, M. Comparison of Security Patterns. IJCSNS International Journal of Computer Science and Network Security, Vol.6 No 2B, February 2006.

[14] Sánchez, L.E., Villafranca, D., Fernández-Medina, E. y Piattini, M Developing a model and a tool to manage the information security in Small and Medium Enterprises. SECRYPT (2007).

[15] 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] Schumacher, M., Roeding, U. Security Engineering with Patterns. PLoP 2001 conference.

[18] Schumacher, M. Security Pattern Homepage. http://www.security-patterns.de, 2001. 6

[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. International standard iso/iec 17799 (2000). Information technology, 2000.

[27] ISO/IEC WD 27004. Information technology — Security techniques — Information security management — Measurements
[28] NIST Special Publication 800-80. Initial Public Draft. Guide to Performance Metrics for Information Security. April 2006.
[29] NIST Special Publication 800-55. Security Metrics Guide for Information Technology. Systems. July 2003.
[30] The European Information Technology Observatory : www.eito.com
[31] Small Business Technology Institute (SBTI): www.sbtechnologyinstitute.org
[32] ITGI (2005). IT Alignment: Who Is in Charge?. IT Governance Domain Practices and Competencies, IT Governance Institute.

La Reunión Española sobre Criptología y Seguridad de la Información (RECSI) celebró su décima edición en la ciudad de Salamanca del 2 al 5 de septiembre de 2008. Se trata del congreso científico nacional referente en el tema de la Seguridad en las Tecnologías de la Información. En él se dan cita periódicamente los principales investigadores españoles en el tema, así como invitados extranjeros de reconocido prestigio.

En esta edición se ha contado con la presencia invitada de los investigadores Carlo Blundo, Ljupco Kocarev, Hugo Scolnik y Fausto Montoya. Además, han colaborado representantes del Centro Criptológico Nacional, la Dirección General de la Policía y de la Guardia Civil, la Junta de Castilla y León y las empresas Signe, Realsec y Ericsson España.

En este libro de actas se recogen todas las contribuciones presentadas en la reunión así como las conferencias invitadas.

ISBN: 978-84-691-5158-7