VI CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMÁTICA CIBSI 2011

Noviembre 2, 3 y 4

Bucaramanga, Colombia

CIBSI 2011

POLITÉCNICA

Universidad Pontificia Bolivariana
SECCIONAL BUCARAMANGA

20 años 1991 - 2011 UPB BUCARAMANGA

Actas del VI Congreso Iberoamericano de Seguridad Informática
CIBSI 2011
Bucaramanga, Colombia, 2 al 4 de Noviembre de 2011

Editores
Angélica Flórez Abril
Jorge Ramió Aguirre
Arturo Ribagorda Garnacho
Jeimy J. Cano Martínez

ISBN: 978-958-8506-18-0

Facultad de Ingeniería Informática, Universidad Pontificia Bolivariana, Seccional Bucaramanga, Colombia
Universidad Politécnica de Madrid, España

Prefacio

El Congreso Iberoamericano de Seguridad Informática (CIBSI) es una iniciativa de la Red Temática de Criptografía y Seguridad de la Información. Desde el año 2002 se ha venido desarrollando, tomando en cuenta durante los primeros años la realización con frecuencia anual y a partir del año 2003 se realiza cada dos años.

La primera versión del CIBSI fue desarrollada en el año 2002 en Morelia, México; en el año 2003 se celebra la segunda edición en Ciudad de México; en el año 2005 se realizó la tercera edición en Valparaíso, Chile; la cuarta edición tiene lugar en el año 2007 en Mar del Plata, Argentina; y en el año 2009 se celebra la quinta versión en Montevideo, Uruguay.

Éste año 2011, se desarrolla la sexta versión del congreso, teniendo como sede la Universidad Pontificia Bolivariana de Bucaramanga, Colombia, institución educativa que desde el año 2005 se encuentra ofreciendo programas de educación continua en seguridad de la información y a partir del año 2007 ofrece la Especialización en Seguridad Informática, convirtiéndose de ésta manera en una institución que apalanca el desarrollo docente e investigación en seguridad de la información en Colombia.

Para los investigadores del área de seguridad de la información en Colombia, es muy grato realizar por primera vez el CIBSI 2011, evento que facilita el intercambio de conocimiento y la formación de redes de colaboración en el ámbito de la investigación y el desarrollo en seguridad de la información.

Dentro de la agenda programada del evento se tienen definidos tres espacios: conferencias magistrales, ponencias de los trabajos presentados y el Primer Taller Iberoamericano de Enseñanza e Innovación Educativa en Seguridad de la Información (TIBETS).

Se realizarán tres conferencias magistrales por parte de reconocidos investigadores en el área, tales como el Dr. Sergio Rajsbaum de la Universidad Nacional Autónoma de México, el Dr. Justo Carracedo de la Universidad Politécnica de Madrid y el Dr. Jeimy Cano de la Universidad Pontificia Bolivariana de Bucaramanga.

Este documento contiene los trabajos a ser presentados como ponencias por investigadores de diversos países a nivel de Iberoamérica. Se recibieron 39 trabajos, de los cuales el Comité del Programa seleccionó 23 trabajos provenientes de los siguientes países: Argentina, Cuba, Colombia, España, Venezuela, Uruguay, México y Brasil.

Como nuevo aporte, en el marco del CIBSI se realizará el TIBETS, espacio que se dedicará a presentar las experiencias en enseñanza e innovación educativa en el área de seguridad de la información, nuevos rumbos docentes, análisis de proyectos de colaboración conjunta y programas de posgrados, que permita plantear estrategias de colaboración docente.

Se espera que estas actas y las reflexiones realizadas del 2 al 4 de noviembre en el Campus de la Universidad Pontificia Bolivariana de Bucaramanga sirvan para el fortalecimiento de la investigación en seguridad de la información, la generación de nuevos espacios de discusión y el estrechamiento de lazos interinstitucionales para el avance en programas de posgrados y rumbos docentes en el área.

Organización de la Conferencia

Comité Organizador General
Angélica Flórez Abril, Universidad Pontificia Bolivariana, Colombia
Jorge Ramió Aguirre, Universidad Politécnica de Madrid, España

Comité Organizador Logístico

Angélica Flórez Abril, Universidad Pontificia Bolivariana, Colombia
Jeimy Cano Martínez, Universidad Pontificia Bolivariana, Colombia
Reinaldo Mayol Arnao, Universidad Pontificia Bolivariana, Colombia

Comité Técnico

Reinaldo Mayol Arnao, Universidad Pontificia Bolivariana, Colombia
Con el apoyo de los estudiantes de Ingeniería Informática:
Miguel Gerardo Mateus Marín y Julián Eduardo Ramírez Rico

Comité del Programa

Jeimy Cano (Chair)	Universidad Pontificia Bolivariana
Arturo Ribagorda Garnacho (Chair)	Universidad Carlos III de Madrid
Marco Aurélio Amaral Henriques	State University of Campinas - Unicamp
Nicolás Antezana Abarca	Sociedad Peruana de Computación
Javier Areitio Bertolín	Universidad de Deusto
Gustavo Betarte	Universidad de la República
Joan Borrel Viader	Universidad Autónoma de Barcelona
Pino Caballero Gil	Universidad de La Laguna
Adriano Mauro Cansian	Universidad Estadual Paulista
Enrique Daltabuit Godas	Universidad Nacional Autónoma de México
Ángel Martín Delrey	Universidad de Salamanca
Josep Domingo-Ferrer	Universidad Rovera i Virgili
Josep Lluis Ferrer-Gomilla	Universidad de las Islas Baleares
Amparo Fúster-Sabater	Consejo Superior de Investigaciones Científicas
Juan Pedro Hecht	Universidad de Buenos Aires
Luis Hernandez Encinas	Consejo Superior de investigación
Emilio Hernández	Universidad Simón Bolívar
Leobardo Hernández Audelo	Universidad Nacional Autónoma de México
Julio César López	Universidad Estatal de Campinas
Vincenzo Mendillo	Universidad Central de Venezuela
Josep María Miret Biosca	Universidad de Lleida
Gaspar Modelo-Howard	Universidad Tecnológica de Panamá
Raul Monge	Universidad Técnica Federico Santa María
Guillermo Morales-Luna	Centro de Investigación y Estudios Avanzados

	del IPN
Alberto Peinado Domínguez	Universidad de Malaga
Josep Rifà Coma	Universidad Autónoma de Barcelona
Jorge Blasco Alis	Universidad Carlos III de Madrid
Hugo Francisco González Robledo	Universidad Politécnica de San Luis de Potosí
José María de Fuentes García-Romero de Tejada	Universidad Carlos III de Madrid

Tabla de contenido

Definición de un modelo automatizado para la evaluación y mantenimiento de un SGSI

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

[1]DELTANET Sistemas de Información. Departamento I+D,
C/Juan II, 1-1ºE, - 13001 Ciudad Real, España
dvillafranca@deltanet.es
[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. Uno de los activos más importantes dentro de cualquier empresa es la información que sustenta todos sus procesos. Con el objetivo de garantizar que los riesgos de la seguridad de la información son conocidos, asumidos, minimizados y gestionados por la organización se han desarrollado los Sistemas de Gestión de la Seguridad de la Información (SGSI). Asociados a los controles que definirá el SGSI, se usan métricas o indicadores de seguridad que nos permiten tener datos objetivos del cumplimiento de estos controles y la evolución futura del SGSI. Sin embargo, la implantación de un SGSI es un proceso largo y complejo, que si no es gestionado correctamente desde el inicio, puede conllevar unos gastos incrementados y la posibilidad de fracaso del proyecto. Para garantizar su desarrollo y mantenimiento, se requiere seleccionar las métricas adecuadas y el uso de herramientas que permita su gestión y evolución. En este artículo exponemos una propuesta práctica que se traduce en una herramienta para permitir optimizar y asegurar el éxito en este tipo de proyectos.

1. Introducción

En los últimos años se ha experimentado un creciente interés de las empresas por la seguridad de la información. Este hecho se ve impulsado por diferentes factores con distinto origen. Por una parte está el interés de la organización para garantizar la confidencialidad, integridad y disponibilidad de la información que gestiona [15]. Por otra parte están los aspectos legales y la regulación cada vez más exigentes que favorecen esta tendencia. Pero el argumento que probablemente cobra más fuerza es lo que realmente está en juego: garantizar la continuidad del negocio y proteger uno de los activos más vitales, la información [1]

Para mejorar la seguridad de las tecnologías de información de las empresas es necesario definir controles de seguridad, y que su cumplimiento sea monitorizado

continuamente [10]. Esto permitiría mejorar la eficiencia de dichos controles y conocer vulnerabilidades en los momentos más tempranos que se produzcan.

Una de las herramientas más importantes para los SGSI es el Cuadro de Mando Integral (CMI) de la Seguridad. Desde su aparición en 1992 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 porque permiten obtener y agrupar la información más relevante y útil para la toma de decisiones, y resulta 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.

La implantación de Cuadros de Mando para la Gestión de Seguridad es, por tanto, un proceso complejo. Cerca del 70% de los proyectos dedicado a plantear Cuadros de Mando fracasan o son abandonados tras su implantación [2]. Esta cifra pone de manifiesto la complejidad del proceso, algo que se puede mitigar si se define un número razonable de indicadores (20-25 máximo), adecuadamente escogidos y útiles, no sólo podremos entender el presente de nuestra gestión de Seguridad TI y como ésta se adapta a lo planificado, sino también prever los incidentes de seguridad antes de que sucedan [3].

Debemos tener en cuenta que la seguridad de la información es un proceso dinámico en constante evolución que debe ser evaluado y monitoreado, con métricas establecidas que permitan, comparar de manera consciente y objetiva escenarios diferentes y tomar decisiones con respecto a los riesgos que se afrontan y los recursos que se invierten [4]. Es necesario encontrar una metodología que conduzca a una solución eficaz y eficiente, desde el punto de vista técnico y económico. Esta metodología deberá considerar aspectos como las necesidades de los procesos del negocio con respecto a la información, aplicaciones y servicios, así como el uso eficiente de los recursos tecnológicos como soporte de estos procesos [5, 6].

La cuestión del establecimiento de métricas en seguridad de la información está en pleno debate en todos los foros. Hay quien propone recomendaciones sobre cómo definir los indicadores, y otros proponen complejos sistemas de medida [7]. Las diferentes normativas, indicadores y métricas de seguridad no ayudan en este escenario cada vez más complejo. La implantación de los SGSI requiere la realización de un análisis complejo 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 [8]. No es posible que un SGSI vaya madurando correctamente si no existe un sistema que mida los niveles de eficiencia de todos sus componentes (todo aquello que no se puede medir, no se puede mejorar) [9]. Las métricas irán madurando y cambiando en función del nivel de madurez que vaya adquiriendo la compañía.

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. Del análisis de los principales estándares anteriores se concluye que es posible plantear una metodología para la construcción de métricas específicas de seguridad de la información [6, 8], aunque esta

metodología se hace complicada de implementar en entornos PYMES [10]. Para facilitar este proceso [6] es preciso contar con un marco adecuado para la selección e implementación de métricas.

En consecuencia, en este artículo se revisa la definición de una metodología que apoyándose en los estándares de seguridad internacionales más importantes (como ISO/IEC 27000, CobIT o NIST), va a permitir evaluar el éxito del desarrollo y la implantación de un SGSI en una organización (principalmente PYMES). Dicho método será la base que utilizaremos en el diseño de una herramienta que le dará soporte al proceso de construcción del SGSI y su mantenimiento posterior, con el objeto de aportar una perspectiva que permita de forma óptima la construcción de un CMI específico para realizar el mantenimiento y mejora continua del programa de seguridad de la información.

El resto del artículo se organizará así: en el apartado siguiente se revisan algunos de los estándares y la problemática que plantea su aplicación práctica. En la sección 3 revisamos nuestra metodología para la selección de indicadores y métricas de seguridad y exponemos algunos resultados obtenidos de su aplicación práctica. Finalmente en la sección 4 presentamos un diseño de la herramienta que estamos desarrollando que permitirá realizar este proceso de forma automática y para concluir extraemos algunas conclusiones y marcamos los hitos de futuros trabajos.

2. Antecedentes

Existen diversos trabajos, metodologías y herramientas que abordan la temática de la implementación y gestión de SGSI. Algunas de ellas como CRAMM [11] son antecedentes incluso para la norma BS7799-3 y por consecuencia para la ISO/IEC 27005 [4]. Algunas declaran además de ser compatibles y cumplir los requerimientos de la norma ISO/IEC 27001[13], otras definen objetivos diferentes a los de la norma pero igualmente ser compatibles con ésta, especialmente en la fase de Planificación, y en las otras fases, tener importantes aportes para los procesos de gestión y documentos requeridos.

A continuación se introducen algunas de las iniciativas más destacables por parte de los cuerpos de estandarización y de la industria en el contexto de la seguridad de la información:

- **ISO/IEC 15408 Common Criteria Framework (CCF),** estándar que propone un marco de trabajo para la evaluación de la seguridad y que fue elaborado en enero de 1996 en un esfuerzo común entre Canadá, Francia, Alemania, Holanda, Reino Unido y los Estados Unidos [12].
- **ISO/IEC 17799:2005**, es la adopción por parte de la ISO de la primera parte de la norma BS7799 del BSI (British Standards Institute), dedicada a definir un código de buenas prácticas para la gestión de la seguridad por las organizaciones [13].
- **Familia ISO/IEC 27000**, que es el grupo de estándares, dedicado a la definición de los SGSI (Sistemas de Gestión de Seguridad de la Información). Esta familia, formada por 5 estándares internacionales, abarca los requisitos de los sistemas de gestión de la seguridad, la gestión del riesgo, métricas y medidas, guías de

implantación, glosario de términos y mejora continua. Actualmente, el único componente liberado es el ISO 27001, equivalente a la segunda parte de la norma BS7799, especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información según el "Círculo de Deming": PDCA - acrónimo de Plan, Do, Check, Act. Además, la norma ISO/IEC 17799:2005 mencionada anteriormente quedará enmarcada en esta familia bajo el ISO 27002 [14].

- **ISO/IEC 21827:2002 SSE-CMM.** SSE-CMM (Systems Security Engineering Capability Maturity Model) es un modelo de proceso cuyo propósito es mejorar y evaluar la capacidad de la ingeniería de la seguridad de una organización. SSE-CMM ha sido adoptado por el estándar ISO/IEC 21827 [15].
- **COBIT** (Control Objectives for Information and related Technology) es un conjunto de mejores prácticas para el manejo de información creado por la Information Systems Audit and Control Association (ISACA), y el IT Governance Institute (ITGI) en 1992. Incluye un marco de trabajo para la gestión, los usuarios, auditores de sistemas de información y profesionales de la seguridad [16].
- **TSP-Secure** (Team Software Process for Secure Software Development) del SEI, extiende el proceso TSP [17] centrándose en la seguridad de las aplicaciones software. El proyecto TSP-Secure es un esfuerzo conjunto entre la iniciativa TSP del SEI y el programa CERT, y su principal objetivo es desarrollar un método basado en TSP que puede producir software seguro de manera predecible [18].
- **MAGERIT versión 2** (Método de Análisis y GEstión del RIesgo del MinisTerio de Administraciones Públicas), es el método de análisis y gestión del riesgo definido por la Administración Pública Española [19].

Uno de los aspectos que tienen en común estas metodologías es que propugnan la creación de un sistema de gestión y que éste debe basarse en los procesos que la organización ejecuta, aunque no quedan claramente personalizados en los indicadores y métricas que propugnan [20]. Además, otra de las críticas que se les puede hacer a los estándares y normas anteriormente analizadas es que aunque en algunos de ellos se definen qué indicadores y cómo se deben usar, no se cubre adecuadamente los motivos para los que se utilizan, obviando además otras fuentes de información y medidas más personales y valiosas dentro de cada organización (como los empleados, otros datos de la industria y los numerosos estudios sobre amenazas, vulnerabilidades e incidentes etc.).

Según se analiza en la figura 1, la complejidad de estos estándares crece en función del nivel de detalle requerido, algo que en la práctica será un hándicap para su uso en organizaciones que requieren la elaboración de un SGSI muy específico y no generalista como en el caso que nos ocupa: las PYMES.

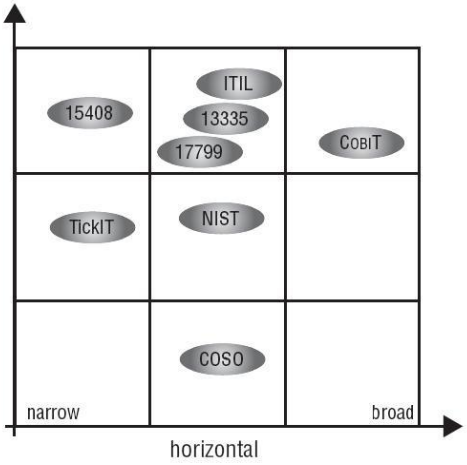

Figura 1. Comparación del nivel de detalle de los estándares analizados

De acuerdo a nuestra experiencia en el uso de métricas de seguridad con nuestros clientes, hemos observado que para la implantación de un SGSI es fundamental tener pocos indicadores al principio pero bien definidos, exponiendo de una forma clara lo que está midiendo, porqué y para qué. Otro punto importante es 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. Además, cada compañía tiene intereses distintos en materia de seguridad, y las métricas se deben establecen de acuerdo a lo que se esté tratando de proteger y medir, así como de la situación de la empresa [3].

En el punto siguiente exponemos nuestro proceso de selección de métricas y los resultados obtenidos en la aplicación del mismo.

3. Revisión de la metodología para la selección de métricas para la construcción del CMI de la Seguridad

Los objetivos que nos hemos marcado en nuestra investigación previa han perseguido 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. En dicho proceso se partía de unos indicadores de seguridad predefinidos que según la naturaleza de la organización en la que se planteaba implantar el SGSI [5, 21], 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 [6].

3.1 Descripción del proceso de selección de métricas

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) [3]. Como comentábamos en trabajos anteriores [5, 21], las métricas e indicadores de cara a su identificación e implementación práctica son seleccionadas en base a unas características (tipo de control, forma de obtención,…). Estos datos son importantes a la hora de construir una buena métrica, pero también se expusieron ciertos problemas que hacen difícil cubrir estas características.

Todos los elementos anteriores se recogen en el siguiente esquema, que se ha ido refinando y conformando según se presenta en la siguiente figura:

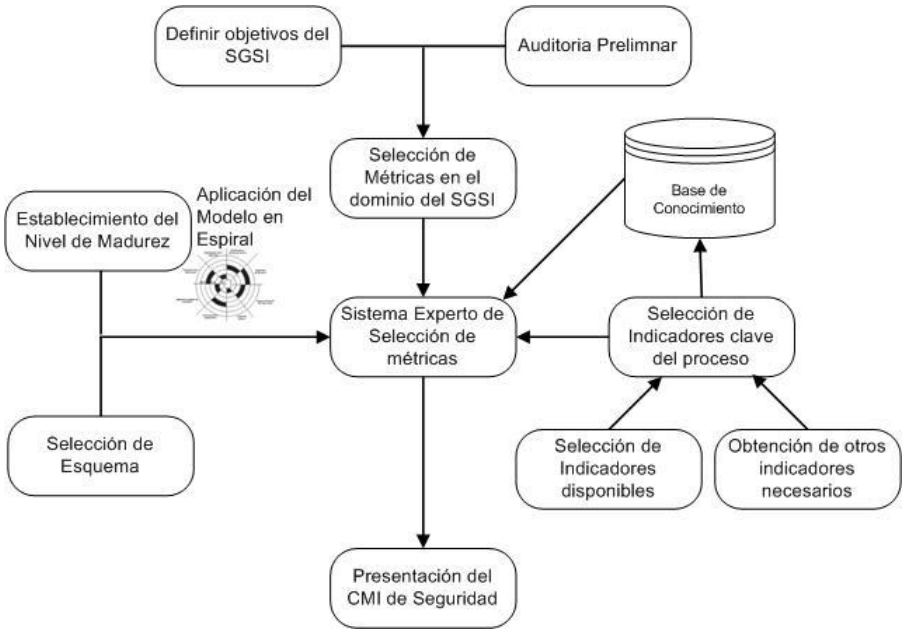

Figura 2. Esquema de la metodología para la selección de métricas de seguridad

En este esquema (figura 2) 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 [21]. 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.

Toda métrica debe tener asignado un responsable que se encargue de recoger, procesar y comunicar los resultados obtenidos al Cuadro de Mando. Esto implica que hay que formar y concienciar al personal que participa en el proyecto en los procesos

a evaluar, ya que el hecho de implantar métricas de seguridad implica un trabajo adicional para los afectados y la inversión de recursos adicionales.

El grado de desarrollo del cuadro de mando, y por consecuencia, de las métricas y de los indicadores, irá reflejando el nivel de madurez de la compañía. De hecho, la calidad de las decisiones que tome la Dirección está estrechamente ligada a la información utilizada. La revisión de los datos obtenidos, se realiza una vez que se han implantado los indicadores. Lo que se pretende comprobar es que los indicadores sean útiles y rentables.

Con todas estas variables, el elemento central de nuestro proceso es el sistema experto que nos va a permitir seleccionar los mejores indicadores justificado en el trabajo que realizaría un auditor experto. El detalle del proceso de selección basado en redes bayesianas mismo se describe en [6].

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 va a aportar:

- 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.

3.2 Breve resumen de los resultados obtenidos con la metodología

Los resultados obtenidos de la aplicación de nuestro proceso permiten asegurar la evaluación eficaz del estado del SGSI en un primer nivel. Se han utilizado diferentes herramientas para la obtención de indicadores automáticos en los entornos de la red y de las bases de datos. Estos datos se han complementado con pruebas manuales (con base en los indicadores definidos en la ISO 27000) realizados con nuestro equipo de auditores y que han ayudado a ir revisando y complementado los resultados que nuestro sistema ha ido ofreciendo.

Las empresas analizadas han sido clasificadas en función al número de equipos fijos, servidores y portátiles que disponían en el momento del análisis. El estudio fue realizado sobre 35 empresas. Hemos realizado una clasificación en un rango que nos permitiera definir la importancia de la misma, dando una idea clara de la infraestructura que contaban.

Nº Puestos	Nº Empresas	% Empresas
>20	2	5,71 %
Entre 11-20	10	28,57 %

Entre 3-10	15	42,86 %
Entre 1-2	8	22,86 %
TOTAL	**35**	**100,00** %

Tabla 1. Grupo de empresas analizadas

Además de las pruebas automáticas, sobre un rango de 0-10 una realizó una serie de cuestionarios para poder evaluar un nivel de cumplimiento en función de la los indicadores seleccionados:

TIPO MÉTRICAS	Nº Métricas
I.- Inversiones en seguridad y Recursos Humanos	9
II.- Software de protección	12
III.- Incidencias de seguridad de la información	4
IV. Seguridad en los accesos	10
V.- Planes de seguridad	4
VI.- Operaciones de Back-up	3

Tabla 2. Categorías de las métricas empleadas

En la siguiente tabla mostramos el resultado de los datos sobre las empresas analizadas:

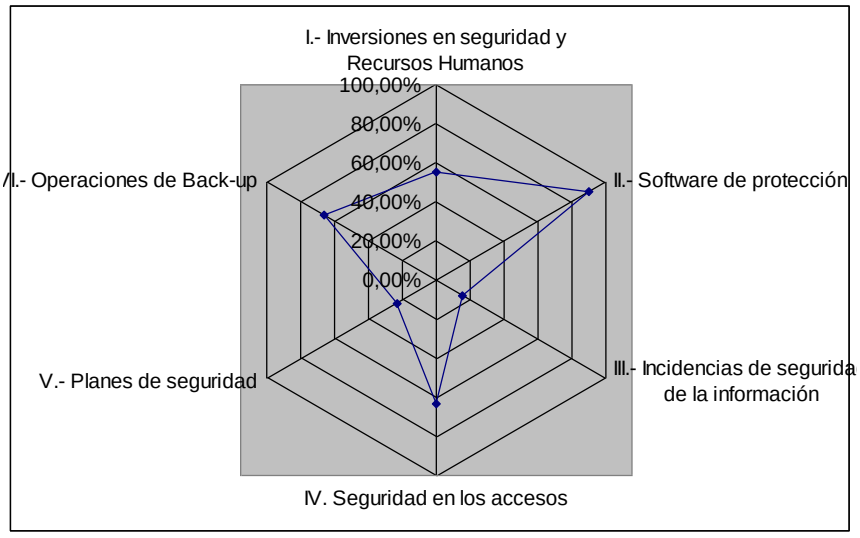

Figura 3. Análisis de métricas de seguridad previas

Un análisis inicial de los resultados, refleja un optimismo en cuanto al bajo número de incidencias en materia de seguridad y una creencia de uso de software de

protección eficaz. También se nota una inversión media en seguridad y recursos, así como una concienciación de la seguridad de los datos (Back-up). Por último, podemos extraer conclusiones sobre la baja concienciación en cuanto a planes de seguridad efectivos.

Estos datos e indicadores no han servido de base para el desarrollo de las diferentes métricas de seguridad que se tomarán de referencia en la implementaremos en nuestra herramienta y que pasamos a describir en el siguiente punto.

4. Definición de la herramienta para la evaluación y el mantenimiento del SGSI.

En la implantación del SGSI, un aspecto clave es la elección de una aplicación que soporte el SGSI y que cumpla con los siguientes requisitos: flexibilidad y adaptabilidad para la definición, implantación y administración del modelo de gestión de la seguridad de la información (procesos, roles, etc.); dotada de herramientas para la realización del análisis de riesgos y capacidades para el control documental (control de versiones, control de accesos, tanto para el sistema en sí como las evidencias del mismo) [7].

Además de aplicar la experiencia propia, hemos analizado diferentes propuestas [4, 22-24] para definir las características funcionales que son deseables en un software de gestión y mejora de un SGSI, entre ellas seleccionamos como claves las siguientes:

- **Flexibilidad y adaptabilidad** para la definición, implantación y administración del modelo de gestión de la seguridad de la información (procesos, roles, etc.).
- Identificar y **clasificar los procesos y sus activos asociados**, valorizando los mismos en función de la escala establecida en cuanto a su necesidad de: confidencialidad, integridad y disponibilidad. De esta forma se identificarán activos críticos y se podrán revisar los controles y salvaguardas atendiendo a las dependencias entre procesos y activos.
- Permitir la **clasificación de activos y riesgos** realizada por la organización y que alcancen a activos y procesos dentro del dominio del SGSI. Estas clasificaciones podrán ser ponderadas en función de la jerarquía establecida y la criticidad o podrán tratarse como un mínimo aceptable (límite inferior) en el caso que las clasificaciones heredadas sean obligatorias. El software debería ser configurable, y tratar esto mediante coeficientes de ponderación, roles y permisos para cambiar ciertos valores asignados.
- Herramientas para la realización del **análisis de riesgos** (ejecución de metodologías de análisis de riesgos)
- **Gestión de los procedimientos y políticas** aplicables, ya sean de la ISO/IEC como de los marcos reglamentarios a los que se deba ajustar la organización.
- **Cumplimiento de los aspectos legales** y de regulación, requerimientos que se han percibido cada vez más exigentes en este proceso.
- **Funcionalidades de workflow** donde se puedan identificar roles, etapas de

cambios de personal, definición, comunicación y delegación, supervisión, escalamiento, etc., que comprenda la naturaleza jerárquica de las organizaciones.

- Permitir realizar ajustes en los valores de los activos y sus amenazas para **reevaluar los riesgos** de una forma periódica.
- Capacidades para la **gestión documental** (control de versiones, control de accesos, tanto para el sistema en sí como las evidencias del mismo). La Gestión de Documentos con definición de roles, gestión de permisos de consulta y modificación, de forma que la documentación sea tratada como un activo más, preservando sus requerimientos de Confidencialidad, Integridad y Disponibilidad.

De nuestra experiencia en el uso de aplicaciones para gestión de procesos e incidentes de seguridad, una situación frecuente que encontramos se produce cuando diferentes componentes por separado y con características complementarias, cada uno de ellos viene equipado con su propia consola de administración. Esta ha sido otra de las motivaciones que nos ha llevado al diseño de una herramienta que agrupara el trabajo de gestión con el SGSI y permitiera la posibilidad de gestionar de forma conjunta en una única consola diferentes herramientas, y de esta forma elaborar y monitorizar en un mismo CMI toda la información del SGSI.

Al igual que es vital que los incidentes o problemas para la seguridad sean detectados gestionados de una forma rápida, se precisa analizar y gestionar nuevos riesgos de forma eficaz mediante el CMI [22]. Por ello el modelo que describimos integra los requerimientos funcionales anteriormente definidos para dar solución a muchas de las situaciones que son clave durante el ciclo de vida del SGSI.

En la siguiente imagen recogemos de forma gráfica los diferentes módulos que componen nuestra herramienta:

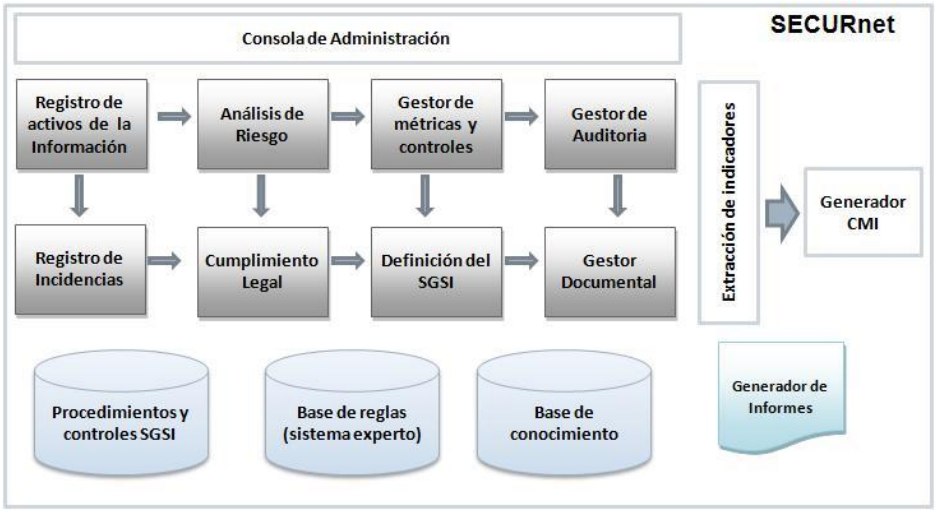

Figura 4. Esquema general de la herramienta SECURnet

La descripción general y origen de cada uno de ellos se expone a continuación:

- **Registro y clasificación de activos**: El objetivo fundamental del SGSI es garantizar la continuidad del negocio, el enfoque por procesos se impone sobre el posible enfoque tecnológico, y su punto de partida se debe centrar en el análisis en el valor relativo de un activo de información para un determinado proceso de negocio. Mediante un inventariado automático y un proceso de clasificación ponderado se considera el punto de partida en el proceso.
- **Análisis de riesgos:** Basada en la metodología de MAGERIT [25] se integra un módulo que permite realizar el análisis de riesgos a partir de la clasificación anterior, identificando amenazas y vulnerabilidades, calculando de esta forma el riesgo y evaluando el nivel de seguridad del sistema en el inicio. Revisando los pesos de los diferentes elementos del análisis se podrá ir reevaluando durante la implantación y posterior mantenimiento del SGSI.
- **Registro de Incidencias:** Mediante una herramienta externa se provee un control que va desde la alerta o petición, la asignación del ticket, la gestión de la solución y, si procede, el seguimiento de las acciones correctivas. Los indicadores obtenidos a partir de la información recogida en este módulo serán claves en la construcción de las métricas que conformarán el CMI.
- **Cumplimiento legal:** Una de las exigencias de la ISO27001 es el cumplimiento legal, lo que en España incluye a la Ley Orgánica 15/1999, de 13 de diciembre, que lleva a cabo la transposición al ordenamiento jurídico español de la Directiva Comunitaria 95/46/CEE establece como su objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales [26]. Para resolver este punto contamos con una herramienta específica en este campo (LOPDnet) que permite el cumplimiento de las obligaciones impuestas revisa las medidas técnicas adoptadas y permite agilizar el cumplimiento de las mismas.
- **Gestión de Métricas y controles**: Este módulo permitirá la gestión de las métricas, según el proceso de extracción que se define más abajo.
- **Definición del SGSI:** Gestionará el establecimiento y la implantación del SGSI conforme a la norma ISO 27001 de una forma integral, con la definición del alcance, declaración de aplicabilidad y el plan de tratamiento de los riesgos, además de la monitorización y mantenimiento posterior.
- **Gestor de Auditoría:** Facilitará el proceso de evaluación de la eficacia del Sistema de Gestión de la Seguridad de la Información (SGSI), según las normas ISO/IEC 27006 e ISO 19011, de forma que la evolución y mejora continua del SGSI que agregue valor a la implementación y a la organización en general.
- **Gestor Documental:** Los documentos que exige el SGSI deben estar protegidos y controlados, registrando entro otros datos: autor, fecha de creación o modificación, título, versión, estado, etc. Adicionalmente nos posibilitará la plataforma para gestionar otra documentación complementaria como la del módulo de auditoría y otros registros.

Aunque alguna de las herramientas y módulos anteriormente descritos son propietarios y otra se ha desarrollado previamente, la característica principal que nos lleva a su selección es que sean de código abierto, lo que permite su análisis, integración y mantenimiento sin las restricciones que un fabricante impone sobre un producto cerrado.

Asimismo, en cada uno de los diferentes módulos funcionales se deberá extraer la información que permita elaborar indicadores clave del proceso para confeccionar posteriormente la métrica. Combinando el enfoque de los procesos basados en sistemas experto para la toma de decisiones [27, 28] junto con nuestro procesos de selección de métricas [6] y otros procesos de selección complementarios [6, 20, 29, 30], hemos definido un método que permite construir de forma automática nuestro Cuadro de Mando de la Seguridad para ofrecer la información requerida en los diferentes niveles:

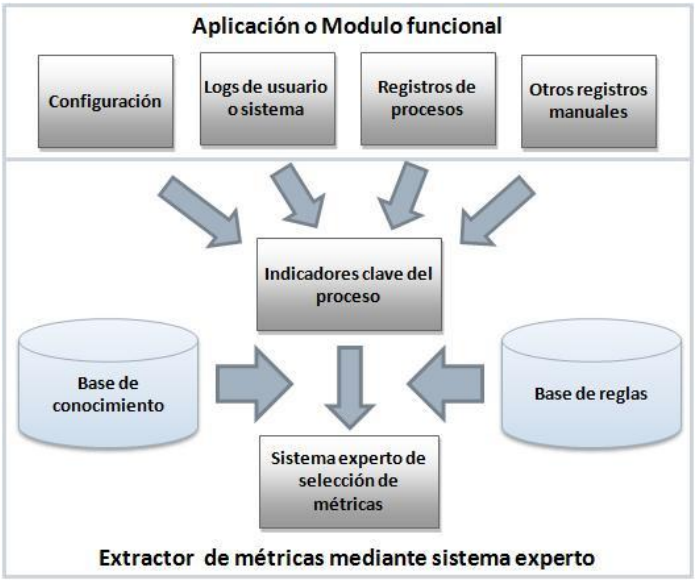

Figura 5. Proceso de extracción de métricas

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), en nuestro caso 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.

A pesar de que 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 En la aplicación práctica de la herramienta con nuevos clientes revisaremos los resultados obtenidos y depuraremos el proceso general.

5. Conclusiones y próximos trabajos

El objetivo de construir un Cuadro de Mandos de la Seguridad óptimo es prioritario a la hora de implantar un SGSI, ya que ofrece un modelo de referencia en el que las medidas e indicadores se ordenan y relacionan, de manera que en conjunto nos dan más información que de forma independiente y que nos aporta información adecuada y útil para la gestión de la seguridad a distintos niveles.

En el presente artículo hemos revisado los problemas que las guías estándar ofrecen y se han expuesto los resultados que hemos logrado con la implementación de un proceso de selección de métricas basado en un sistema experto, a partir del *know-how* obtenido a partir de nuestra experiencia y buscando rápidamente el ROI en las organizaciones en las que hemos planificado SGSI.

Adicionalmente se han expuesto las diferentes características que una herramienta debe cumplir para poder realizar un proceso de construcción y evaluación continua de un SGSI mediante la selección de métricas. Mediante el uso de un proceso automatizado, el análisis de riesgos que se ofrece permite realizar variaciones ajustando de forma dinámica los pesos y valores de la evaluación.

Con esta herramienta se gestionará de forma global implantación y evaluación de un SGSI, comprendiendo cada una de las actividades en todas las fases de implantación del sistema. De esta forma, el control y coordinación de la implantación se simplifica y permitirá gestionar con un único interfaz toda la organización y asegurar la implantación eficaz y su mantenimiento evolutivo.

Adicionalmente nuestra propuesta se engloba dentro de una solución *cloud computing* que se aprovecha de las características y potencial que esta nueva forma de ofrecer servicios ofrece, reduciendo el coste de grandes plataformas en pequeñas empresas, sin necesidad de adquirir una infraestructura que le supondría un coste muy alto en hardware, licencias y mantenimiento. De esta forma se ofrece una solución escalable, con menor mantenimiento por parte del departamento de IT y con un menor coste en infraestructuras y licencias.

En posteriores trabajos expondremos los avances y las mejoras graduales del proceso de implementación y uso de la herramienta, los resultados obtenidos con ella, así como otras mejoras que se planifiquen, orientadas a otras necesidades:

- Aplicación de nuevos procesos de extracción de indicadores y definición de métricas de seguridad.
- Análisis de nuevos módulos que permitan avanzar en la mejora continua del proceso (BCP, Formación,…)
- Integración con nuevas plataformas para poder realizar una monitorización en tiempo real de la seguridad y realizar un sistema que permita complementar la extracción de conocimiento a partir de otros registros, logs y correlación de eventos.

Agradecimientos

Esta investigación es parte del proyecto SERENIDAD (PEII11-0327-7035) financiado por la Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha.

Referencias

1. Sánchez Luengo, N., *Implantación de un SGSI: Factores críticos que garantizan el buen gobierno y la seguridad corporativa*, in *Auditoría y Seguridad*. 2008. p. 72-74.
2. Megias Terol, J. *Una introducción a los Indicadores y Cuadros de Mando de Seguridad para el apoyo a la Dirección estratégica de TI*. 2007 [cited; Available from: www.criptored.upm.es/guiateoria/gt_m531b.htm.
3. Heyman, T., et al. *Using security patterns to combine security metrics*. in *Proceedings of the 2008 Third International Conference on Availability, Reliability and Security (ARES-2008)*. 2008. Barcelona: IEEE Computer Society
4. Pallas, G. and M.E. Corti. *Metodología de Implantación de un SGSI en grupos empresariales de relación jerárquica*. in *V Congreso Iberoamericano de Seguridad Informática (CIBSI'09)*. 2009. Montevideo (Uruguay).
5. Villafranca, D., et al. *Hacia un método para la construcción de Cuadros de Mando de la Seguridad en TI para PYMES.* in *Simposio de Seguridad Informática, dentro del congreso Español de Informática (CEDI'07).* 2007. Zaragoza. España.
6. Villafranca, D., et al. *Metodología para la selección de métricas en la construcción de un Cuadro de Mando Integral*. in *CIBSI*. 2009. Montevideo (Uruguay).
7. Prats Abadía, L., *Las métricas y la gestión de objetivos en la empresa*, in *Red Seguridad*. 2006.
8. Sánchez, L.E., et al. *Security Management in corporative IT systems using maturity models, taking as base ISO/IEC 17799.* in *International Symposium on Frontiers in Availability, Reliability and Security (FARES'06) in conjunction with ARES.* 2006. Viena (Austria).
9. Corletti, A. and C. De Alba-Muñoz, *Métricas de Seguridad, Indicadores y Cuadro de Mando*, in *Auditoría y Seguridad*. 2008.
10. Sánchez, L.E., et al. *Practical Application of a Security Management Maturity Model for SMEs Based on Predefined Schemas.* in *International Conference on Security and Cryptography (SECRYPT'08).* 2008. Porto–Portugal.
11. CRAMMv5.4, *CRAMM v5.4, CCTA Risk Analysis and Management Method.* 2009.
12. ISO/IEC, *ISO/IEC 15408:2005 Information technology - Security techniques - Evaluation criteria for IT security, (Common Criteria v3.0)*. 2005.
13. ISO/IEC, *ISO/IEC 17799:2005 Code of Practice for Information Security Management*. 2005.

14. ISO/IEC, *ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements*. 2005. p. 34.
15. ISO/IEC, *ISO/IEC 21827:2002 Information technology -- Systems Security Engineering -- Capability Maturity Model (SSE-CMM)*. 2002, ISO/IEC. p. 123.
16. IT_Governance_Institute, *Control Objectives for Information and related Technology (COBIT 4.0)*. 2005.
17. Humphrey, W.S., *TSP(SM)—Coaching Development Teams*. The SEI Series in Software Engineering. 2006: Addison Wesley Professional. 448.
18. Davis, N. and J. Mullaney, *The Team Software Process (TSP) in Practice: A Summary of Recent Results*. 2003, Software Engineering Institute, Carnegie Mellon University: Pittsburgh, PA, USA.
19. Lopez, J., et al., *Specification and design of advanced authentication and authorization services.*, in *Computer Standars and Interfaces*. 2005. p. 467-478.
20. Mellado, D., E. Fernández-Medina, and M. Piattini. *A Comparison of Software Design Security Metrics*. in *MeSSa 2010 - 1st International Workshop on Measurability of Security in Software Architectures* 2010. Copenhagen, Denmark.
21. Sánchez, L.E., et al. *SCMM-TOOL: Tool for computer automation of the Information Security Management Systems*. in *2nd International conference on Software and Data Technologies (ICSOFT'07).* . 2007c. Barcelona-España Septiembre.
22. Kapur, R., *Use of the Balanced Scorecard for IT Risk Management*, in *Information Systems Control Journal*. 2010.
23. Jansen, W., *Directions in Security Metrics Research*, in *Draft Special Publication*, N. 7564, Editor. 2009, NIST.
24. Corti, M.E., *Metodologías para la implantación de SGSI*, in *CERTuy - Ciclo de Charlas 2010* 2010: Montevideo, Uruguay.
25. MageritV2, *Metodología de Análisis y Gestión de Riesgos para las Tecnologías de la Información, V2*. 2005, Ministerio de Administraciones Públicas.
26. Igualada Menor, A., *La Protección de Datos y el diseño de Tratamientos de datos personales. Especificaciones funcionales necesarias.*, in *V Congreso Iberoamericano de Seguridad Informática (CIBSI'09).* 2009, Noviembre: Montevideo (Uruguay).
27. Cooper, *Computational complexity of probabilistic inference using bayesian belief networks.* Artificial Intelligence, 1992. 42: p. 393-405.
28. Russel, S. and P. Norvig, *Artificial Intelligence: A Modern Approach*. 2002: Prentice Hall.
29. Lim, Y., et al. *An Enterprise Security Management System as a Web- Based Application Service for Small/Medium Businesses*. in *Inscrypt 2006*. 2006. Beijing, China: Springer-Verlag Berlin Heidelberg.
30. Krautsevich, L., F. Martinelli, and A. Yautsiukhin. *Formal approach to security metrics. What does "more secure" mean for you?* in *MeSSa 2010 - 1st International Workshop on Measurability of Security in Software Architectures* 2010. Copenhagen, Denmark.