Modelo de Sistema Basado en Conocimiento para el Análisis de la Seguridad de la Información en el Contexto de los Sistemas de Gestión

Bajarlía, María Victoria Soledad [(1)] , Eterovic Jorge [(1)] , Ierache Jorge [(1,2)]
Escuela de Posgrado Facultad Regional Buenos Aires - Universidad Tecnológica Nacional[(1)]
Castro Barros 91 (C1178AAA) C.A.B.A. Argentina . Tel: (54 11) 4983-8882
Instituto de sistemas inteligentes y enseñanza experimental de la robótica[(2)]
FICCTE-UM
victoriabajarlia@hotmail.com, jeterovic@hotmail.com, jierache@unimoron.edu.ar

Resumen. El objetivo del presente trabajo es proponer un modelo de un sistema basado en conocimiento (SBC) aplicado al análisis de seguridad de aplicaciones de gestión. El modelo a proponer se basa en un sistema basado en conocimiento (SBC) que cuenta con un componente cognitivo que le permite incorporar conocimiento. En virtud de que las amenazas y los ataques informáticos representan un problema constante y creciente se puede suponer que el SBC, a través del aprendizaje dinámico que lo mantendrá actualizado, podrá asistir a los especialistas en seguridad informática, en el área de competencia, a la elaboración de ERS.

1 Introducción

El aporte del presente trabajo es diseñar un sistema basado en conocimiento (SBC) aplicado al análisis de la seguridad de aplicaciones. La base de conocimiento será alimentada permanentemente por normas, estándares y mejores prácticas vigentes así como por aquellos informes de vulnerabilidades que tomen conocimiento público en la comunidad informática. El motor de inferencia, el cual trabajará sobre un universo abierto, tomará la información suministrada por la base de conocimiento para analizar la seguridad de una aplicación determinada. La solución del problema a través del método elegido comprenderá desde el análisis de seguridad de aplicaciones de gestión hasta el control de que las mismas cumplan con el marco regulatorio.

1.1 El problema

El avance tecnológico y el desarrollo de aplicaciones informáticas para soportar las necesidades del negocio de una organización hace imperioso cruzar fronteras, por ejemplo acceder desde la Web hasta llegar a una base de datos que está gestionada por un software que corre sobre un equipo Mainframe. De este modo la explotación de la

aplicación se realiza atravesando diversas capas e integrando diferentes plataformas existentes en la organización. Dado que las capas tienen distintas naturalezas de seguridad, es necesario implementar un mecanismo eficiente que permita que las aplicaciones sean realmente seguras cumpliendo con los estándares respectivos y permaneciendo altamente alineadas con la tecnología. [4] [7] [8] [9] [22] [23]. Para abordar esta problemática se propone un sistema basado en conocimientos (SBC) que asista a la elaboración de especificaciones de requerimientos de software (ERS) a fin de aportar con el desarrollo de aplicaciones que contribuyan eficientemente a reducir las potenciales vulnerabilidades de las aplicaciones y que permita evaluar si una aplicación dada pasa los niveles de seguridad establecidos. Esto a su vez contribuye con el mantenimiento y refinamiento del conocimiento.

1.2 Áreas involucradas en el dominio del problema de estudio

Las áreas que participan en el contexto del tema de estudio propuesto involucran: (a) Seguridad de la Información (SI). Engloba la investigación del área de la seguridad de aplicaciones de gestión. [24] [25] [26]. (b) Ingeniería de Requerimientos (IR). Se basa inicialmente en el estándar IEEE-830 de Especificación de Requisitos de Software (ERS), sobre el cual se realizarán aportes en función del modelo de conocimiento que se obtenga del trabajo con los expertos en el área de Seguridad de la Información, a partir de las consideraciones que surjan en relación a requerimientos funcionales y no funcionales.[13] [15]. (c) Ingeniería de Conocimiento (INCO). Incorpora el marco metodológico y las técnicas aplicadas al desarrollo de un Sistema Basado en Conocimiento (SBC) en el contexto dado de la INCO. Quedará comprendido en la extracción de conocimientos y la educción de conocimientos con los expertos del área de seguridad. [10] [14]. (d) Sistema basado en conocimiento (SBC). Comprende la implementación de un sistema que asista a la elaboración de los aspectos de seguridad de la aplicación en el marco de una ERS, a través de la incorporación de los aspectos de la materia de estudio en el modelo de conocimiento del experto de campo. Por último, y como conclusión, abarcará la implementación de un prototipo de SBC para el análisis y evaluación de ERS en los aspectos de seguridad, desde el punto de vista de la IR.

Es importante señalar el mecanismo de interacción de las áreas involucradas constituyendo el SBC: (a) IR-SI. Aporta la base metodológica para construir las Especificaciones de Requerimientos de Software de Seguridad en el aspecto específico de Seguridad de la Información (ERSSI) según el estándar IEEE-830. (b) IR-INCO. Aporta la metodología para el desarrollo del SBC en el contexto de la IR. (c) SI-INCO, aporta la conceptualización como producto de la extracción de conocimiento (marco regulatorio, mejores prácticas, etc.) y la educción de conocimiento (entrevistas con el experto y trabajo de campo), para la formalización e implementación del SBC. (d) ERSSI-SBC, como resultado de la interacción de las áreas involucradas se desarrollara un modelo que permita evaluar si una aplicación dada pasa los niveles de seguridad establecidos, luego el especialista en seguridad de aplicaciones alimentará a la ERSSI a partir de nuevas regulaciones de la industria, mejores prácticas, etc. lo que contribuirá con el crecimiento del sistema. Por último

dará lugar al mantenimiento del conocimiento y servirá de soporte la construcción y refinamiento/mejora continua de ERSSI sobre la base del SBC.

1.3 Estado del arte de seguridad de la información

La situación actual demuestra que, si bien existe un importante nivel de madurez en materia de seguridad informática respecto de la infraestructura tecnológica organizacional, no sucede lo mismo con los sistemas aplicativos que son soportados por dicha infraestructura. Esto conlleva a una falta de alineación entre los desarrolladores y los especialistas en el análisis de vulnerabilidades en el software de gestión. Finalmente esta falta de alineación puede poner en riesgo uno de los activos más importantes que tiene una organización: su información.

La infraestructura de capas del presente trabajo de investigación comprende: Autenticación, Servidor de Aplicaciones, Programas ejecutables y Repositorio de Datos. Como una evaluación preliminar del problema que origina este trabajo de investigación se hará una extracción y educción de expertos de conocimiento. Esto significa, en primer lugar, evaluar el tipo de seguridad que corresponde aplicar en cada una de las capas o layers que componen el desarrollo de un software. En segundo lugar se evaluará el trabajo de un experto en esta materia a fin de extraer el conocimiento necesario en relación a las posibles vulnerabilidades de software que pueden surgir con el crecimiento tecnológico. [12] [16] [17] [18] [19] [20] [21]

2 Metodología de desarrollo

Para la construcción del modelo se seleccionará una metodología adecuada del área de Ingeniería de Conocimiento (INCO): Metodología IDEAL. El desarrollo se articulara considerando fases I y II de la metodología IDEAL en virtud de que permiten alcanzar el estado de un prototipo para la explotación de los conocimientos basales del dominio en cuestión. Dando como resultado productos como el Diccionario de Conceptos, la Tabla Concepto-Atributo-Valor, el Modelo de Entidad y Relación, el Mapa de Conocimiento, la Formalización en Marcos, la Base de Hechos, la Base de Reglas y el Motor de Inferencias.

Dentro de la Fase I (Identificación de la tarea) se consideran los objetivos del proyecto del Sistema Experto (SE). Aplicado al problema a resolver, significará adquirir el conocimiento necesario en lo referente al marco regulatorio para la Seguridad de la Información, así como hacer educción de expertos en esta materia. Durante la Fase II (Desarrollo del prototipo) se continuará con la adquisición de conocimientos, se evaluará la viabilidad del sistema y se llegará a la conceptualización y formalización de los conocimientos e implementación del prototipo que permitirá validar con el experto el modelo de SBC. A continuación se

expondrá una síntesis de los ítems más significativos de la Fase II: Conceptualización, Formalización e Implementación.

2.1 Conceptualización del Conocimiento

La conceptualización comprende la identificación y adquisición de conocimientos Estratégicos, Fácticos y Tácticos, a fin de llegar a un mapa de conocimientos. Dicho mapa será la síntesis de la conceptualización de un Modelo Dinámico y de un Modelo Estático que constituirán el modelo conceptual del SBC.

Dentro del Modelo Estático se trabaja en primer lugar con los conocimientos fácticos (Diccionario de Conceptos, Glosario de Términos, Tabla Concepto-Atributo-Valor y Modelo de Entidad-Relación). Se definirán los conceptos, sus atributos y valores asociados, así como las relaciones entre ellos. Todo esto a partir de los conocimientos adquiridos y la educción de expertos en materia de seguridad de la Información. En segundo lugar se consideran los conocimientos estratégicos, a través de la identificación de funciones y actividades del proceso de resolución, análisis y juicio del experto y la efectiva aplicación de mejores prácticas y estándares de seguridad de la información. El análisis del conocimiento estratégico permitirá desarrollar una definición precisa de los cursos de acción modulares que sigue el experto al desempeñar sus tareas y el flujo de control que gobernará el funcionamiento y el dinamismo del sistema experto. De esta forma al efectuar la síntesis, en caso de ser necesario, se podrá realizar un reacomodamiento de etapas, pasos, tareas, etc.

A través del proceso de adquisición y extracción de conocimiento (fase I), el experto brinda conocimientos tácticos que especifican cómo el sistema puede utilizar escenarios o hechos conocidos así como hipótesis de los casos presentados a fin de obtener nuevas hipótesis, tanto en situaciones deterministas como en contextos de incertidumbre. La articulación de los conocimientos tácticos se realiza a través del empleo de seudorreglas que posteriormente se formalizarán a través de reglas en función de la herramienta de desarrollo del prototipo.

Dentro del Modelo Dinámico (o modelo de procesos) se debe definir una jerarquía de tareas, partiendo de la identificación de conocimientos estratégicos. El experto participa en la realización de este modelo comprobando las metas, submetas, decisiones, acciones, conceptos y atributos que se aplican. Para cada nivel en la jerarquía se definen metas (objetivo), entradas necesarias y salidas producidas.

El Mapa de Conocimiento (MC) es la síntesis del Modelo Dinámico y del Modelo Estático. Representa la parte estática y dinámica de los conocimientos del Experto. Permite ubicar una relación directa entre el Experto y el Ingeniero en Conocimiento al representar de manera entendible los conocimientos educidos a los usuarios finales. El enfoque a través de MC permite que los conocimientos educidos puedan ser empleados e implementados de una forma demostrable, documentable y auditable.

El experto identificó cuatro áreas esenciales para la construcción del MC a fin de arribar al diagnóstico final de situación de seguridad. Facilitando la evaluación de cada subproblema a resolver e instaurando un diagnóstico parcial por cada una de ellas, las áreas son: Nivel de Seguridad en Capa Autenticación, Nivel de Seguridad en Capa Servidor de Aplicaciones, Nivel de Seguridad en Capa Programas Ejecutables y Nivel de Seguridad en Capa Repositorio de Datos. A modo de ejemplo se ilustra en la figura 1 el MC para el nivel de Seguridad en Capa Servidor de Aplicaciones.

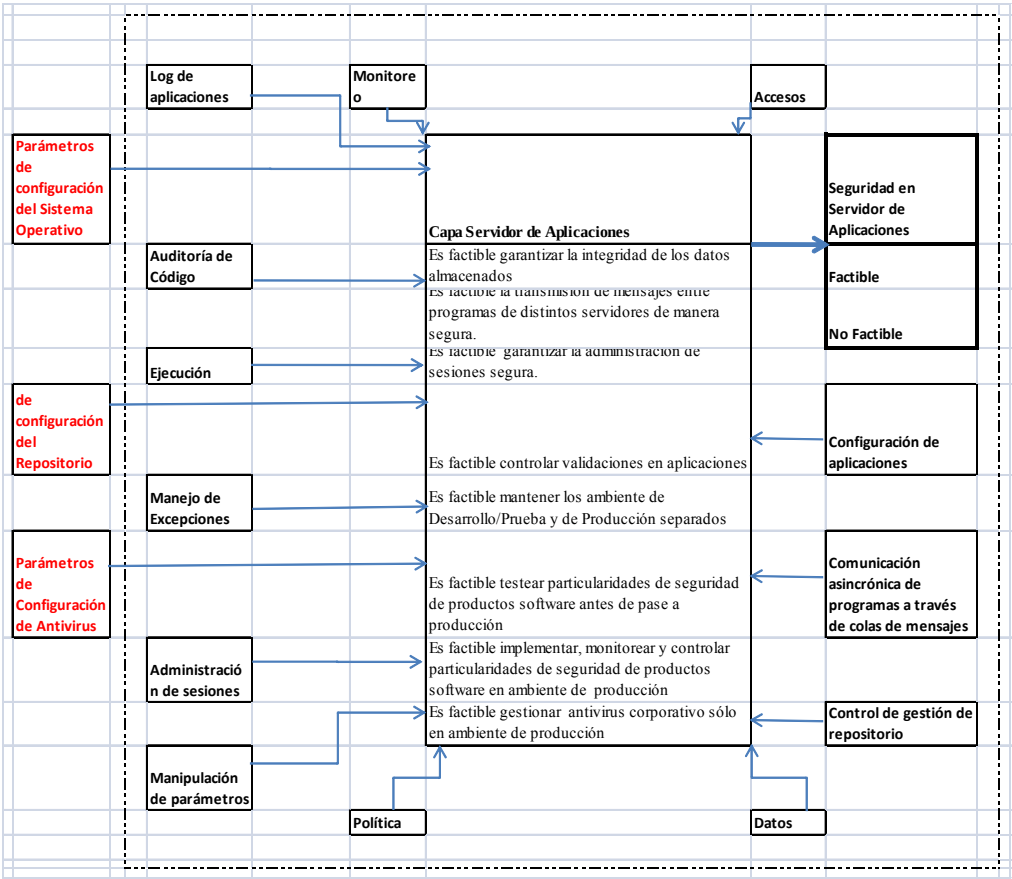

Fig. 1. Mapa de conocimiento - Nivel de Seguridad en Capa Servidor de Aplicaciones

El experto validó el Modelo Estático y el Modelo Dinámico y comprobó el MC a través de distintos juegos de ensayo.

2.2 Formalización del conocimiento

La formalización del conocimiento es el resultado obtenido a partir de la conceptualización de conocimientos representada a través del conocimiento fáctico (Tabla Concepto-Atributo-Valor), táctico (seudorreglas) y estratégico (Árbol de descomposición funcional). Establece modelos formales que brindan una representación semi-interna o semi-computable de los conocimientos y conducta del experto que puedan ser utilizadas por una computadora.

El formalismo de Marcos es una de las técnicas más utilizadas cuando el conocimiento del dominio se organiza en base a conceptos. Los Marcos agregan una tercera dimensión al permitir que los nodos tengan estructuras, que pueden ser valores simples u otros marcos [2] [3]. A través de formalismos de Marcos se representan los conceptos y sus atributos determinados en la fase conceptualización a través del conocimiento fáctico, los conceptos de la tabla concepto- atributo- valor se formalizan en Marcos clase, los atributos del concepto representan las propiedades del Marco. Los valores de cada atributo correspondiente a las propiedades del Marco se detallan a través de las facetas que formulan los valores con los que se puede completar cada propiedad. Los Marcos Clase representados son: diagnóstico general nivel de seguridad, diagnóstico capa autenticación, diagnóstico capa servidor de aplicaciones, diagnóstico capa programas ejecutables, diagnóstico capa repositorio de datos, Entorno de Testeo, Entorno de Producción, Gestión de Liberaciones de aplicaciones, Separación de ambientes operativos, Vulnerabilidades de las aplicaciones Web, Resguardo y Recupero de Programas fuente, Resguardo y Recupero de Datos, entre otros.

2.3 Implementación del Sistema Experto

Como herramientas para desarrollo se utilizará Kappa-PC que es una herramienta que facilita la implementación de sistemas que hayan sido formalizados en base a marcos. Brinda un entorno de desarrollo que facilita la construcción rápida, permitiendo un ciclo de vida en donde en cada iteración se incrementen los conocimientos y así lograr un desarrollo basado en prototipado incremental congruente con las bases propuestas en la Metodología IDEAL [1] [2] [3] [5] [6]. Para la implementación del Sistema Experto se realizaron los pasos que se detallan a continuación:

1) Declaración de la base de conocimientos formalizada en Marcos, a través de la herramienta para la representación de Marcos Clase y Marcos Instancias (explotados a través de los casos de pruebas del experto).
2) Incorporación de reglas para cada una de las áreas que forman el dominio del Problema hasta llegar a las correspondientes reglas del Diagnóstico General de Seguridad (en concordancia con las seudorreglas definidas a través de la conceptualización).
3) Correspondencia del sistema con la estructura de razonamiento de encadenamiento hacia atrás. Se desarrollan los objetivos de acuerdo al siguiente orden: Subdiagnóstico Capa Autenticación, Subdiagnóstico Capa Servidor de Aplicaciones, Subdiagnóstico

Capa Programas Ejecutables, Subdiagnóstico Capa Repositorio de Datos y Diagnóstico General de Seguridad.

4) Desarrollo de pantallas gráficas correspondientes a menús de ingreso/selección de datos por parte del usuario así como visualización de resultados correspondiente a los distintos subdiagnósticos. A modo de ejemplo se exhibe,la pantalla correspondiente al Subdiagnóstico Capa Servidor de Aplicaciones- Gestión de ambientes operativos, figura 2 y la pantalla correspondiente al Subdiagnóstico Capa Programas Ejecutables - Diferencial, figura 3.

5) Realización de diversas sesiones de pruebas con el Experto a fin de evaluar la facilidad de navegación de las Interfaces de usuario. A su vez se efectuaron pruebas funcionales del sistema experto en lo relacionado a la base de reglas, dando un resultado ampliamente satisfactorio en relación a los requerimientos del usuario. Los resultados se condensan en la tabla 1.

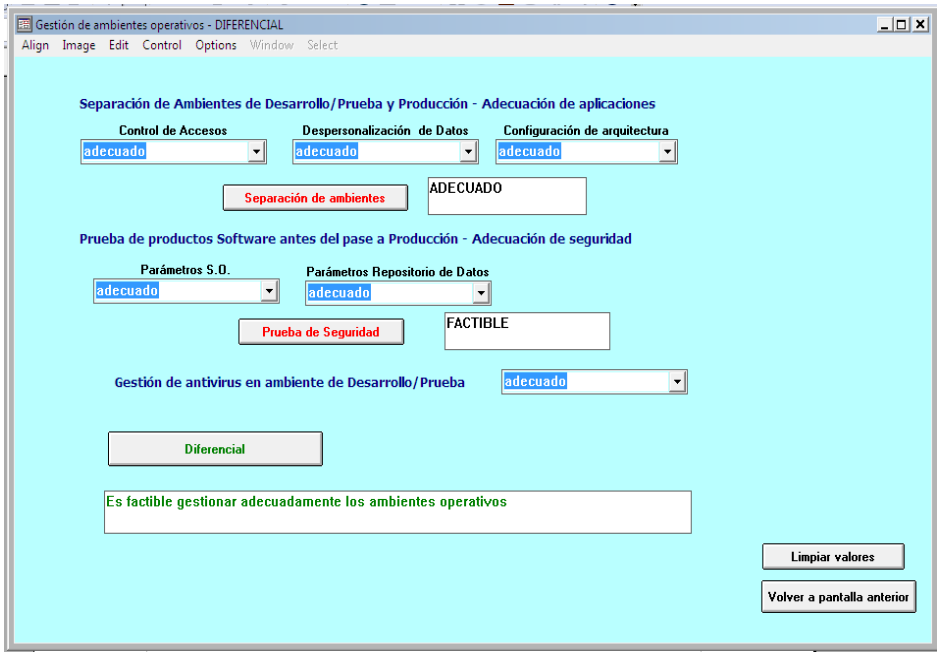

Fig. 2. Interface de Usuario- Gestión de ambientes operativos

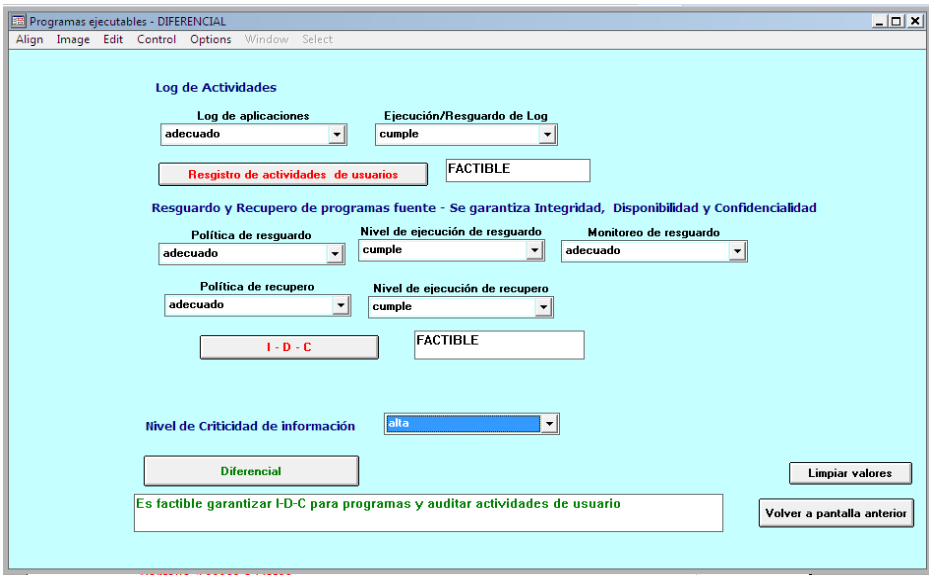

Fig. 3. Interface de Usuario- Programas Ejecutables

Caso de prueba	Resultado Obtenido (Diagnóstico del Sistema)	Resultado Esperado (Experto)
1 - Gestión de Turnos	Nivel de seguridad: ÓPTIMO La aplicación cumple con todos los parámetros de seguridad requeridos	**OPTIMO. La aplicación pasa satisfactoriamente requerimientos mandatorios y opcionales de seguridad.**
2 - FTP Seguro	Nivel de seguridad: ÓPTIMO La aplicación cumple con todos los parámetros de seguridad requeridos	**OPTIMO. La aplicación pasa satisfactoriamente requerimientos mandatorios y opcionales de seguridad.**
3 - Sistema Integral de Delegaciones	Nivel de seguridad: SEGURO. La aplicación cumple con los parámetros de seguridad. No se garantiza gestión adecuada de datos sensibles.	**SEGURO. La aplicación pasa los requerimientos mandatorios de seguridad. No verifica niveles apropiados de IDC ni datos sensibles.**
4 - Base Unificada de Administración de Prestaciones	Nivel de seguridad: SEGURO. La aplicación cumple con los parámetros de seguridad. No se garantiza gestión adecuada de datos sensibles.	**SEGURO. La aplicación pasa los requerimientos mandatorios de seguridad. No verifica niveles apropiados de IDC ni datos sensibles.**
5 - Gestión de usuarios por Web	Nivel de seguridad: INSEGURO. Recomendación: volver a evaluar la aplicación, los datos y el entorno.	**INSEGURO. La aplicación no pasa los requerimientos mandatorios y diferenciales de seguridad.**
6 - Compra Electrónica Web	Nivel de seguridad: INSEGURO. Recomendación: volver a evaluar la aplicación, los datos y el entorno.	**INSEGURO. La aplicación no pasa los requerimientos mandatorios y diferenciales de seguridad.**

Tabla 1. Resumen de pruebas funcionales

3 Conclusiones y trabajo futuro

Se detallan los aportes que el presente trabajo ofrece a la problemática específica de la seguridad de las aplicaciones de gestión:

- Propone un modelo de un Sistema Basado en Conocimiento (SBC), capaz de dar respuesta al análisis de los niveles de seguridad de aplicaciones de gestión.
- Sistematiza y documenta, con metodología de Sistemas Expertos, el conocimiento requerido para el área de la seguridad de aplicaciones de gestión.
- Fija las bases para la realización de un Sistema Experto que asiste en el análisis y evaluación de ERS, que incorpora como propuesta los aspectos de seguridad, desde el punto de vista de la Ingeniería de Requerimientos (IR).
- Aplica, para el área de Ingeniería en Conocimiento, un marco metodológico a través de la metodología IDEAL, asegurando el desarrollo y posterior crecimiento del Sistema Experto, en los aspectos relativos al mantenimiento del conocimiento.

Del trabajo efectuado, así como de la experiencia adquirida, surgen las siguientes propuestas para futuros trabajo:

- Ampliar el modelo de conocimientos del SBC optimizando la taxonomía de requerimientos funcionales y no funcionales con la incorporación de temas vinculados con la gestión de activos, la seguridad del personal, la seguridad física y ambiental, la gestión de la comunicación y las operaciones ente otros aspectos de la seguridad de la información.
- Ampliar el alcance del SBC incorporando nuevos conceptos relacionados con la seguridad en las capas analizadas, así como otros que puedan agregar valor a partir de la explotación de la taxonomía de requerimientos funcionales y no funcionales.
- Investigar sobre herramientas de soporte para la gestión de datos que puedan incorporarse al sistema incrementando de esta manera su robustez y permitiendo efectuar trazabilidad de los resultados.
- Extender las funcionalidades de explotación del SBC por parte de los usuarios y expertos remotos a través de una capa de interfase de usuario vía WEB.

4 Referencias bibliográficas

1. Fernández Galán, S., González Boticario, J., Mira Mira, J., Problemas resueltos de Inteligencia Artificial Aplicada. Búsqueda y representación (Addison-Wesley, 1998).
2. García Martinez R., Britos P., Ingeniería de sistema Expertos (Nueva Librería ,2004)
3. Giarratano, J., Riley, G., Sistemas Expertos Principios y Programación (Thomson International, 2000).
4. Harrison, R., ASP/MTS/ADSI Web Security (Longman, 1999).
5. Intellicorp, Kappa PC Quick Start (Intellicorp Inc., 1992)
6. Intellicorp, Kappa PC User Guide (Intellicorp Inc., 1992)
7. Jaworski, J., Perrone, P.J., Seguridad en Java (Prentice Hall, 2000).
8. Kaeo, M., Diseño de Seguridad en Redes (Pearson Educación, 2003).
9. Maiwald, E., Fundamentos de la seguridad de redes. Conocimientos esenciales a tu alcance (McGraw-Hill, 2005).
10. Maté Hernández, J.L., Pazos Sierra J., Ingeniería del Conocimiento. Diseño y construcción de sistemas expertos (Sepa S.A.,1988).
11. MinsKy M. A framework for representing Knowledge (McGraw Hill,1975)
12. Piattini Velthuis, M., Del Peso Navarro, E., Auditoría informática un enfoque práctico (Alfaomega Grupo Editor Argentino S.A., 2001).
13. Pressman R., Ingeniería del Software, un enfoque práctico (McGraw Hill,2006)
14. Rusell, S.J., Norvig, P., Inteligencia Artificial (Pearson Educación, 2004).
15. Sommerville , I., Ingeniería de Software (Addison Wesley, 2002).
16. ISO/IEC 27001, 2006. Gestión de la Seguridad de la Información.
17. Stallings, W., Fundamentos de la seguridad en redes. Aplicaciones y estándares (Pearson Educación, 2004).
18. ArCERT (Coordinación de Emergencias en Redes Teleinformáticas de la Administración Pública), Subsecretaría de Gestión Pública) www.arcert.gov.ar.
19. HISPASEC SISTEMAS. www.hispasec.com .
20. IEEE (Institute of Electrical and Electronics Engineers), www.ieee.org.
21. ISO (International Organization for Standardization), www.iso.org.
22. ISECOM (Institute for security and open methodologies) www.isecom.org.
23. NIST (National Institute of Standards and Technology, Technology Administration U.S. Department of Commerce), www.nist.gov .
24. PKI (Public Key Infraestructure), Subsecretaría de Gestión Pública www.pki.gov.ar
25. Seguridad en Windows www.microsoft.com/security
26. Seguridad en Java www.java.sun.com/products/jaas.