Modelo de Sistema Basado en Conocimiento en el Dominio de la Seguridad de Aplicaciones

María Victoria Bajarlía[1], Jorge Ierache[2,3], Jorge Eterovic[4]
1. Maestría en Ingeniería de Sistemas de Información. Universidad Tecnológica Nacional (FRBA)
2. Laboratorio de Sistemas Avanzados de Información Facultad de Ingeniería. Universidad de Buenos Aires
3. Instituto de Sistemas Inteligentes y Enseñanza Experimental de la Robótica FICCTE-Universidad de Morón
4. Universidad de Morón - Morón, Argentina
mvbajarlia@gmail.com, jierache@yahoo.com, jeterovic@unimoron.edu.ar

***Resumen*—El objetivo es proponer un modelo de un sistema basado en conocimiento (SBC) aplicado al análisis de seguridad de aplicaciones de gestión. El modelo se fundamenta 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 de la Información, en el área de competencia, a la elaboración de Especificación de Requerimientos.**

***Palabras Clave* —Seguridad de aplicaciones, sistemas basados en conocimiento.**

I. INTRODUCCIÓN

Se propone la aplicación de 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 de la industria informática así como por aquellos informes de vulnerabilidades y ataques que tomen conocimiento público en la comunidad informática. El motor de inferencia, que 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 abarcará desde el análisis de seguridad de aplicaciones de gestión hasta el control de que las mismas cumplan con el marco regulatorio.

El presente trabajo es el producto resultante de un trabajo de investigación realizado en el marco de la tesis de la Maestría en Ingeniería en Sistemas de Información y pretende ser una contribución con la Seguridad de la Información.

A. El problema

El avance tecnológico y el desarrollo de aplicaciones informáticas para soportar las necesidades del negocio de una organización hace necesario traspasar fronteras en un contexto de infraestructura tecnológica, por ejemplo acceder desde la Web hasta llegar a una base de datos que está gestionada por un software que se ejecuta 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 imperioso implementar un mecanismo eficiente que permita que las aplicaciones sean realmente seguras cumpliendo con los estándares respectivos en materia de Seguridad de la Información y permaneciendo altamente alineadas con la tecnología. [4] [8] [13] [16] [17] [18]

Por este motivo para abordar esta problemática se plantea un SBC que asista a la elaboración de especificaciones de requerimientos de software (ERS) a fin de colaborar con el desarrollo de aplicaciones seguras que contribuyan eficientemente a reducir las potenciales vulnerabilidades de las mismas. A su vez que permita evaluar si una aplicación dada se ajusta satisfactoriamente a los niveles de seguridad establecidos, contribuyendo con el mantenimiento y el refinamiento del conocimiento.

B. Áreas involucradas en el dominio del problema de estudio

Las áreas que participan en el contexto del tema propuesto involucran:

a) Seguridad de la Información (SI). Engloba la investigación del área de la seguridad de aplicaciones de gestión. [23] [26] [27]

b) Ingeniería de Requerimientos (IR). Se basa inicialmente en el estándar IEEE-830 de Especificación de Requisitos de Software (ERS), sobre el cual se realizan 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. [24] [28]

c) Ingeniería de Conocimiento (INCO). Incorpora el marco metodológico y las técnicas aplicadas al desarrollo de un SBC en el contexto dado de la INCO. Quedará comprendido por la extracción y educción de conocimientos con los Expertos del área de seguridad. [19] [25]

d) Sistema basado en conocimiento (SBC). Comprende la implementación de un sistema que asista a la elaboración de especificaciones en materia 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. [2] [3] [4]

Es importante señalar el mecanismo de interacción de las áreas involucradas constituyendo el SBC:

- 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.

- IR-INCO. Aporta la metodología para el desarrollo del SBC en el contexto de la IR.
- 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.
- ERSSI-SBC. Como resultado de la interacción de las áreas involucradas se desarrolla un modelo que permita evaluar si una aplicación dada se ajusta a 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 para la construcción y refinamiento/mejora continua de ERSSI sobre la base del SBC. La Figura 1 sintetiza el mecanismo de interacción.

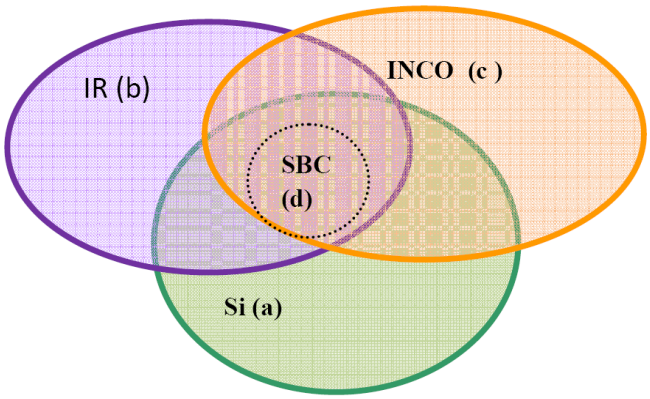


Fig. 1. Representación conceptual de las áreas involucradas

C. 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 analistas, constructores, arquitectos de software y 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 propuesta comprende: Autenticación, Servidor de Aplicaciones, Programas ejecutables y Repositorio de Datos. Como una evaluación preliminar del problema se realizo 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 que componen el desarrollo de un software. En segundo lugar evaluar 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. [1] [9] [10] [11] [14] [19] [22] [29]

A continuación se enumeran resumidamente, para cada capa, los distintos aspectos investigados y que sirvieron como piedra fundamental para el desarrollo de la solución.

- Autenticación

-Mecanismo de autenticación (Mecanismos de autenticación estándares, etc.)

-Protección de la red interna (firewall y sus distintos tipos, etc.)

- Servidor de aplicaciones

- S.O.A (Arquitectura orientada a servicios).

-Servicios Web (protocolos estándares, transmisión de datos seguros de extremo a extremo, etc.)

- Programas ejecutables

-Aplicaciones Web y sus vulnerabilidades (mejores prácticas de la industria, ataques más comunes como ingeniería social y phishing entre otros)

-Seguridad de Programas Ejecutables (Auditoría de Código, Log de aplicaciones, Validaciones de datos de Entrada y de Salida, tratamiento de datos dentro del programa, etc.)

-Calidad de los datos (procedimientos de corrección, validación y normalización de datos, etc,)

-Gestión de liberación y reguardo de versiones fuente de programas

- Repositorio de datos

-Procedimientos asociados (Resguardo y recupero, Clasificación, etc.)

-Seguridad de Bases de datos (mejores prácticas recomendadas en la industria)

-Tecnologías para almacenamiento seguro (cifrado de datos, etc.)

II. Metodología de Desarrollo

Para la construcción del modelo se seleccionó una metodología adecuada del área de Ingeniería de Conocimiento (INCO): Metodología IDEAL. El desarrollo se articuló considerando las 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 principales para la construcción del Sistema Experto (SE), aplicado al problema a resolver, significa en primer lugar adquirir el conocimiento necesario en lo referente al marco regulatorio y mejores prácticas de la industria informática para la Seguridad de la Información. En segundo lugar hacer educción de los conocimientos de los especialistas en esta materia evaluando el trabajo de un Experto en Seguridad de la Información. Durante la Fase II (Desarrollo del prototipo) se continuó con las actividades de adquisición del conocimiento, se realizó la viabilidad del sistema, la conceptualización y la formalización de los conocimientos e implementación del prototipo que permitió validar con el Experto el modelo de SBC propuesto. A continuación se expone una síntesis de los ítems más significativos de la Fase II: Conceptualización, Formalización e Implementación.

A. Conceptualización del Conocimiento

La conceptualización comprende la identificación y adquisición de conocimientos Fácticos, Estratégicos 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, este último también denominado DER). Para ello se definieron los conceptos, sus atributos y valores asociados, así como las relaciones entre ellos, 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.

1) Conocimientos Fácticos

La propuesta inicial para la conceptualización incorpora la interacción del paradigma del conocimiento para ser instrumentado por el SBC, sobre las bases del paradigma funcional, considerando dentro de este último los requerimientos funcionales (RF) y los requerimientos no funcionales (RNF) desarrollados en la ERSSI. En la misma se presentan los requerimientos de Seguridad de la Información relacionados específicamente con la seguridad de las aplicaciones informáticas, en el dominio de las aplicaciones de gestión. Los requerimientos no funcionales quedan representados por características vinculadas con la configuración, la administración y el mantenimiento de un entorno seguro para las aplicaciones, dentro y fuera de la organización.

Dentro de la ERSSI también se definen niveles de aceptación a los que debe ajustarse una aplicación. Para la definición de los mismos se tomó como base la probabilidad de ocurrencia de amenazas y vulnerabilidades que puedan sufrir las aplicaciones así como el impacto que el riesgo asociado a las mismas puede causar en la organización. A modo de recomendación se clasifican en:

- Mandatario. Por considerar que su cumplimiento está fuertemente ligado al nivel de seguridad que requieren las aplicaciones en relación al dominio de la misma dentro de los objetivos de negocio de la organización.
- Sugerido. Por considerar que el no cumplimiento se relaciona con riesgos de mediana probabilidad de ocurrencia en el uso de las aplicaciones, desde el punto de vista de la seguridad de la información.
- Deseable. Por considerar que el no cumplimiento se relaciona con riesgos de baja probabilidad de ocurrencia en el uso de las aplicaciones.

El análisis inicial dentro del proceso de conceptualización es la evaluación del tipo de seguridad que corresponde aplicar en cada una de las capas que componen el desarrollo de un software y que forman parte de un contexto donde se desarrollarán las aplicaciones. En segundo lugar evaluar el trabajo de un Experto en Seguridad de la Información considerando todos los aportes que un especialista puede incorporar en dicha materia, completando así los puntos que nacen de la extracción de conocimiento. Posteriormente, la educción de conocimiento, producto de las heurísticas de los especialistas, permitió a través de distintas entrevistas ampliar el horizonte para luego mejorar cada aspecto con los aportes de los Expertos, la alineación a estándares relacionados a la Seguridad de la Información, la implementación de buenas prácticas, etc.

Es importante destacar que el contexto de aplicación está dado por una infraestructura de capas, de ella se desprenden los conceptos necesarios a fin de llegar al proceso de conceptualización.

Los conceptos se encuentran altamente vinculados con los requerimientos funcionales y no funcionales detallados en la ERSSI. La infraestructura de capas propuesta, comprende:

- Autenticación.
- Servidor de Aplicaciones
- Programas ejecutables
- Repositorio de Datos.

El segundo paso en el marco del proceso consiste en identificar las relaciones entre los conceptos definidos. Se trabaja con conocimientos fácticos y se busca simbolizar el modelo mental que el Experto tiene de la vista estática del problema a resolver a través de la observación y de las distintas entrevistas que se mantiene con el Experto a lo largo del trabajo, El modelo mental quedará reflejado a través del Modelo de Entidad-Relación (DER). Bajo la óptica de este modelo, el contexto de aplicación está conformado por las cuatro capas mencionadas anteriormente, para cada una de ellas se establecerá un subdiagnóstico que posteriormente aportará a la construcción del diagnóstico final que brindará el SBC. La relación entre los conceptos y los requerimientos de tipo funcional y no funcional quedará determinada por las contribuciones de la ERSSI y por los resultados logrados en función del diagnóstico que brindará el Experto y los aportes en materia de Seguridad de la Información que realicen los especialistas.

El modelo plantea como entidad principal el Diagnostico Final de Situación de Seguridad - DFSS que se relaciona con 4 entidades representadas por Subdiagnósticos (Capa Autenticación, Capa Servidor Aplicaciones, Capa Programas Ejecutables y Capa Repositorio de Datos). Cada subdiagnóstico tendrá relaciones de tipo “muchos a muchos” con entidades de tipo Conceptos según su propio contexto, por ejemplo Conceptos Capa Autenticación, Conceptos Capa Servidor Aplicaciones, Conceptos Capa Programas Ejecutables y Conceptos Capa Repositorio de Datos. Los distintos Requerimientos Funcionales (RF) y los Requerimientos No Funcionales (RNF) definidos para cada subdiagnóstico serán las entidades vinculantes entre el Contexto de Infraestructura Tecnológica - CIT, el Diagnóstico Final de Situación de Seguridad - DFSS y los distintos subdiagnósticos. El propósito es que queden representados los conceptos y sus relaciones, en virtud de cómo se plasman en el ámbito de la Seguridad de la Información, la Ingeniería de Requerimientos, y finalmente en el diagnóstico que brindará el SBC.

2) Conocimientos Estratégico

El análisis del conocimiento estratégico permite 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. El conocimiento estratégico se resume a través del Árbol de descomposición funcional, Figura 2. En trazos resaltados en color azul se encuentran los pasos analizados en este primer alcance del prototipo al que se pretende arribar , dejando sin explotar los pasos concernientes

al diagnóstico del nivel de seguridad en la capa de autenticación asumiendo vínculos seguros y procesos de autenticación sólidos y estandarizados.

De acuerdo al trabajo de educción de conocimiento para el diagnóstico y los subdiagnósticos correspondientes se establece el nivel de aceptación que puede presentar una aplicación en materia de Seguridad de la Información. El nivel de aceptación queda expresado como resultado parcial o final ya sea si corresponde al diagnóstico general o a los subdiagnósticos y queda constituido de acuerdo a los niveles de aceptación propuestos en la ERSSI.

Los niveles de aceptación propuestos se describen a continuación, dejando abierta la posibilidad de agregar otros en futuros trabajos, permitiendo que el SBC instaure más diagnósticos. Los niveles propuestos son:

- OPTIMO (no se puede vulnerar por el nivel de protección definido)
- SEGURO (se recomienda monitoreo a fin de detectar vulnerabilidades, fallas y/o ataques a la seguridad)
- INSEGURO (no se garantiza la integridad, disponibilidad y confidencialidad de los datos)

3) Conocimientos Tácticos

Mediante el 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.

4) Mapa de conocimiento

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 tales los conocimientos puedan ser empleados e implementados de una forma demostrable, documentable y auditable.

En este contexto el Experto identificó cuatro áreas esenciales para la construcción del MC a fin de arribar al diagnóstico final de situación de seguridad.

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, como se exhibe en la Figura 3.

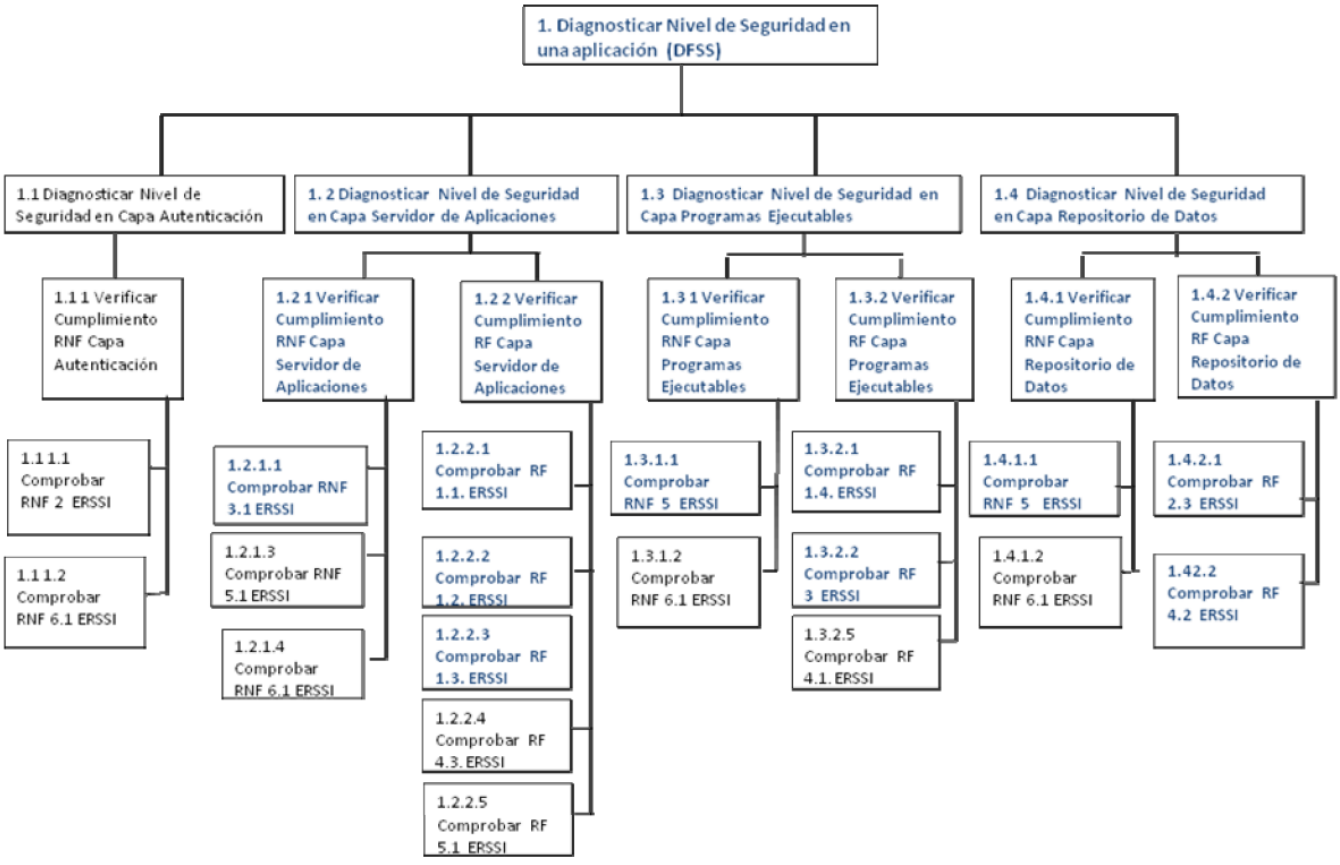


Fig. 2. Árbol de descomposición funcional

Fig. 3. Mapa de conocimiento diagnóstico DFSS

Los MC que se desarrollan a fin de representar el problema de estudio se exhiben a en las siguientes figuras. El Experto identificó tres áreas esenciales para la construcción del MC, facilitando la evaluación de cada subproblema a resolver, las áreas son: Nivel de Seguridad en Capa Servidor de Aplicaciones, Figura 4; Nivel de Seguridad en Capa Programas Ejecutables, Figura 5; Nivel de Seguridad en Capa Repositorio de Datos, Figura 6.

Para finalizar el proceso de conceptualización del conocimiento, el Experto validó el Modelo Estático y el Modelo Dinámico y comprobó el MC a través de distintos juegos de ensayo.

B. 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 [6] [7]. 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.

1) Marcos Clase y Marcos Instancia

Los Marcos Clase se utilizan para representar conceptos de la tabla Concepto-atributo-valor así como situaciones genéricas proporcionadas por un conjunto de características, unas con valores determinados y otras sin valores asignados que son comunes al concepto. Los Marcos Clase representados son: DIAGNIVELSEG (diagnóstico general nivel de seguridad), DIAGCSAP (diagnóstico capa servidor de aplicaciones), DIAGCPE (diagnóstico capa programas ejecutables), DIAGCRD (diagnóstico capa repositorio de datos), Entorno de Testeo, Entorno de Producción, Gestión de Liberaciones, Separación de ambientes, Control de Programas Ejecutables, Vulnerabilidades de las aplicaciones Web, Control de Programas fuente, Resguardo de Programas fuente, Recupero de Programas fuente, Capa de Seguridad, Resguardo de Datos, Recupero de Datos, Acceso a Datos.

Los Marcos Instanciados se utilizan para representar conceptos particulares al momento de efectuar la tarea de diagnóstico, es decir cuando se está evaluando un escenario particular.

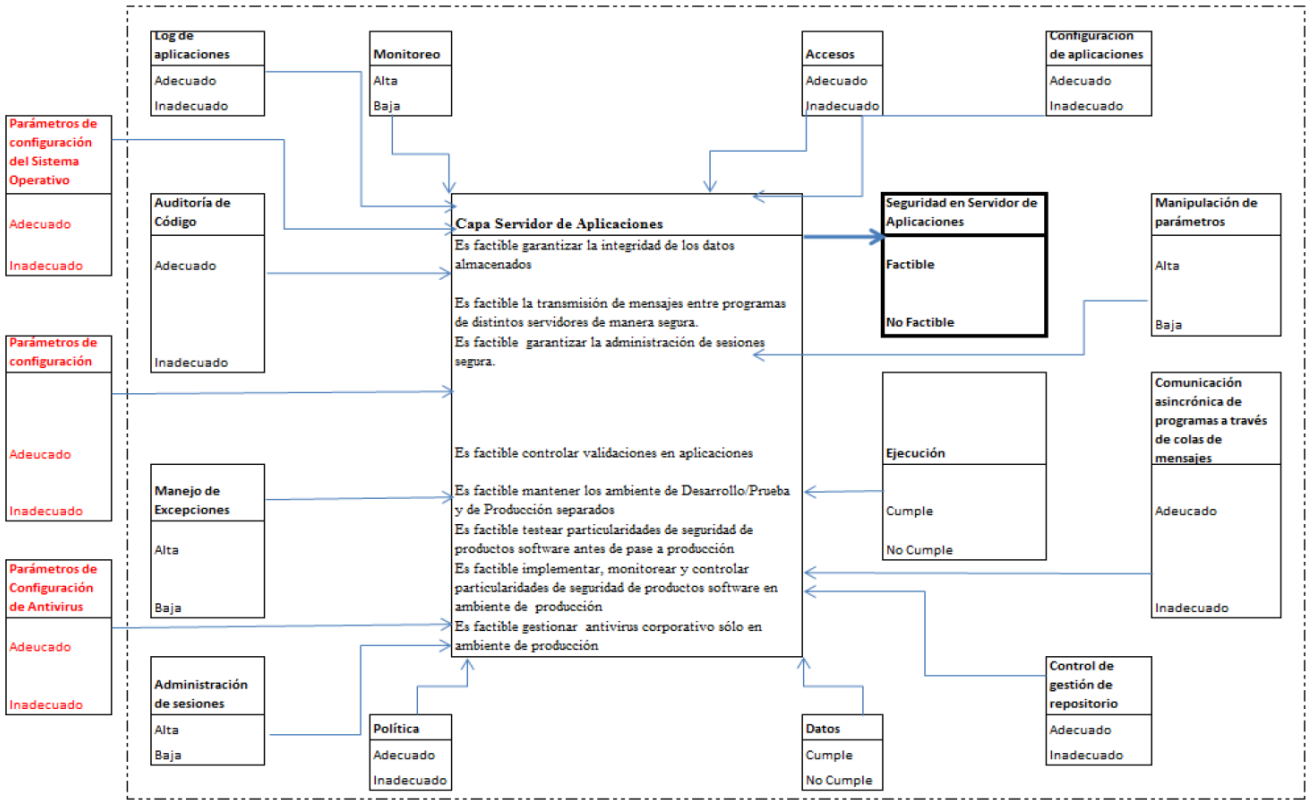


Fig. 4. Nivel de Seguridad en Capa Servidor de Aplicaciones

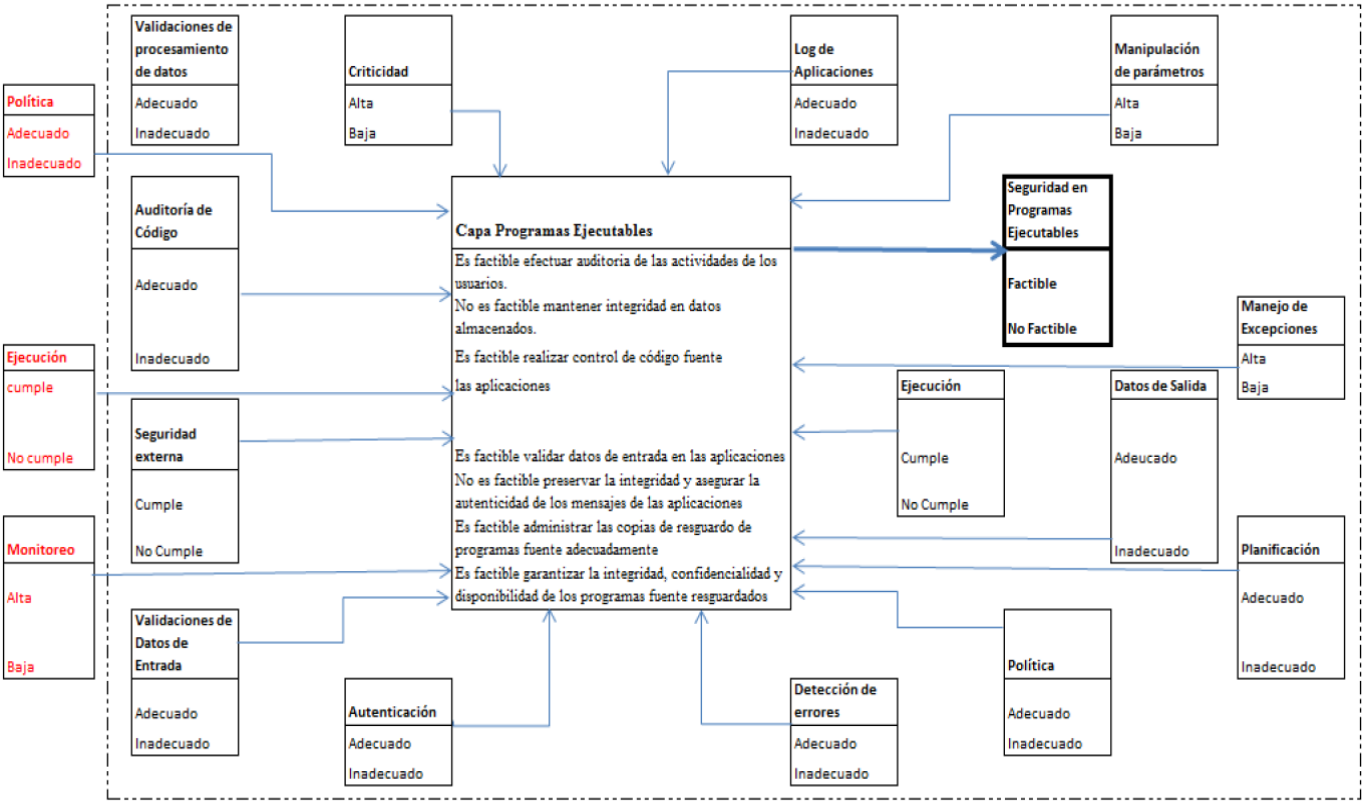


Fig. 5. Nivel de Seguridad en Capa Programas Ejecutables

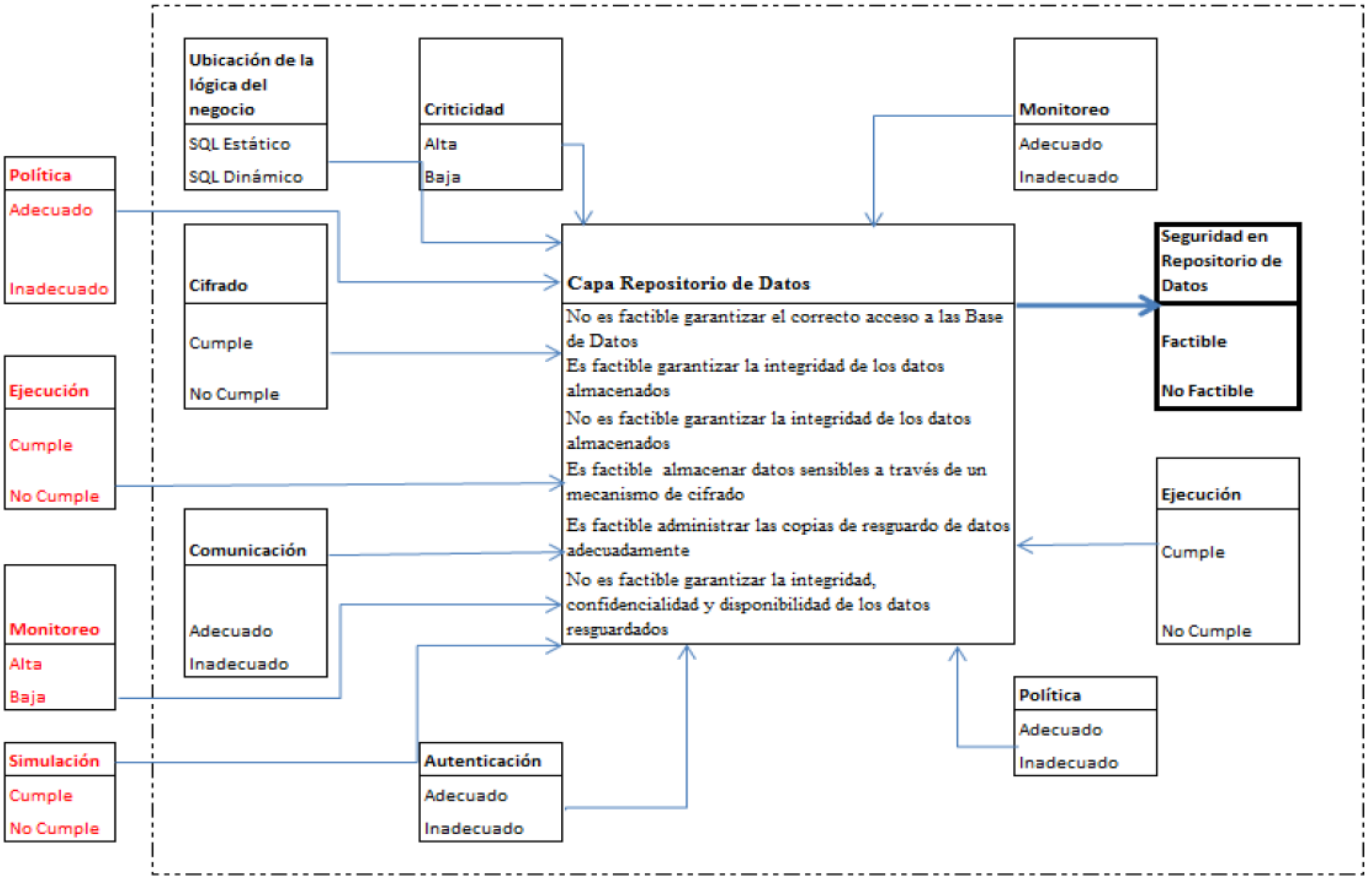


Fig. 6. Nivel de Seguridad en Capa Repositorio de Datos

Los Marcos instanciados representados son: DIAGNIVELSEG Presente (diagnóstico general nivel de seguridad), DIAGCSAP Presente (diagnóstico capa servidor de aplicaciones), DIAGCPE Presente (diagnóstico capa programas ejecutables), DIAGCRD Presente (diagnóstico capa repositorio de datos), Entorno de Testeo Presente, Entorno de Producción Presente, Gestión de Liberaciones Presente, Separación de ambientes Presente, Control de Programas Ejecutables Presente, Vulnerabilidades de las aplicaciones Web Presente, Control de Programas fuente Presente, Resguardo de Programas fuente Presente, Recupero de Programas fuente Presente, Capa de Seguridad Presente, Resguardo de Datos Presente, Recupero de Datos Presente, Acceso a Datos Presente. En esta ocasión los Marcos Instanciados fueron utilizados en el momento de implementación y explotados para los casos de prueba. Esto considerando que el Experto, a través de las entrevistas, brindó los valores por defecto para completar dichos marcos, así como valores para conformar los casos basales para efectuar las pruebas y validar el resultado arrojado por el sistema.

2) Relaciones entre conceptos

El formalismo de marcos permite representar las relaciones del dominio, con relaciones entre marcos clase, entre marcos instancias y entre marcos clase y marcos instancias, estableciendo de esta manera un sistema basado en marcos (SBM). El significado de las relaciones es el siguiente:

- La relación "Se basa en": representa el diagnóstico parcial de cada uno de los dominios a evaluar y que contribuirá a obtener el Diagnostico Final de Situación de Seguridad (DFSS) de una aplicación.
- La relación "Se comprueba": representa el nivel de cumplimiento de cada uno de los requerimientos funcionales (RF) y los requerimientos no funcionales (RNF) desarrollados en la ERSSI.
- La relación "Considera el": representa el peso que tiene el nivel de cumplimento de aquellos RF y RNF que son considerados "de soporte" para la evaluación del DIAGCSAP, dentro del alcance planteado. Para este caso los valores usados son valores por defecto o aquellos valores indicados por el Experto en los casos de prueba.

C. Implementación del Sistema Experto

Como herramienta para desarrollo se utilizó 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 [5] [6] [7] [11] [12]. 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. Se declararon los objetos clase correspondientes a: diagnóstico general nivel de seguridad, diagnóstico capa servidor de aplicaciones, diagnóstico capa programas ejecutables, diagnóstico capa repositorio de datos, Entorno de Testeo, Entorno de Producción, Gestión de Liberaciones, Separación de ambientes, Control de Programas Ejecutables, Vulnerabilidades de las aplicaciones Web, Control de Programas fuente, Resguardo de Programas fuente, Recupero de Programas fuente, Capa de Seguridad, Resguardo de Datos, Recupero de Datos y Acceso a Datos.

2- Definición de las propiedades de clase de los diferentes marcos, utilizando los slots que se pueden definir en cada objeto. Para cada slot se define cardinalidad, valor tipo y valor permitido.

3- 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 construidas en el marco de la Conceptualización del Conocimiento.

4- Correspondencia del sistema con la estructura de razonamiento de encadenamiento hacia atrás. Se desarrollan los objetivos de acuerdo al siguiente orden:

- Subdiagnóstico Capa Servidor de Aplicaciones.
- Subdiagnóstico Capa Programas Ejecutables.
- Subdiagnóstico Capa Repositorio de Datos.
- Diagnóstico General de Seguridad.

5- 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.

6- Adecuación de las distintas interfaces, conforme a las sugerencias del usuario. La forma de navegar el sistema se muestra en la Figura 7.

7- 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.

1) Mapa de pantallas

A continuación se exhibe la manera en que el usuario puede navegar por las distintas pantallas que tiene el sistema.

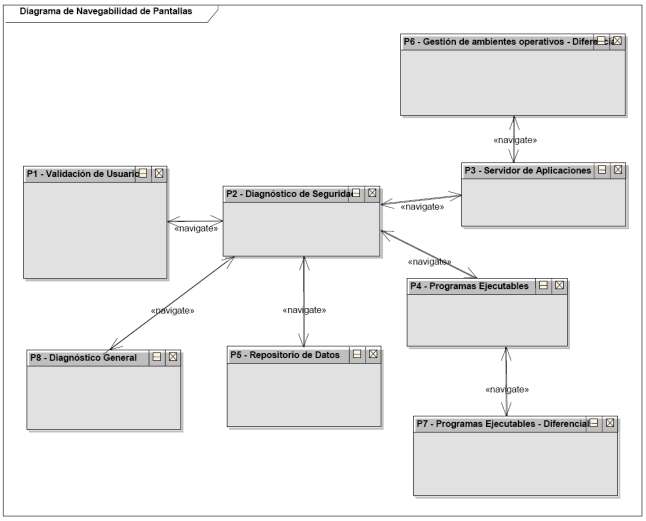


Fig. 7. Navegabilidad de interfaces de usuario

2) Interfaces de Usuario

A modo ilustrativo se exhiben algunas pantallas que forman parte del prototipo construido con la herramienta Kappa-PC.

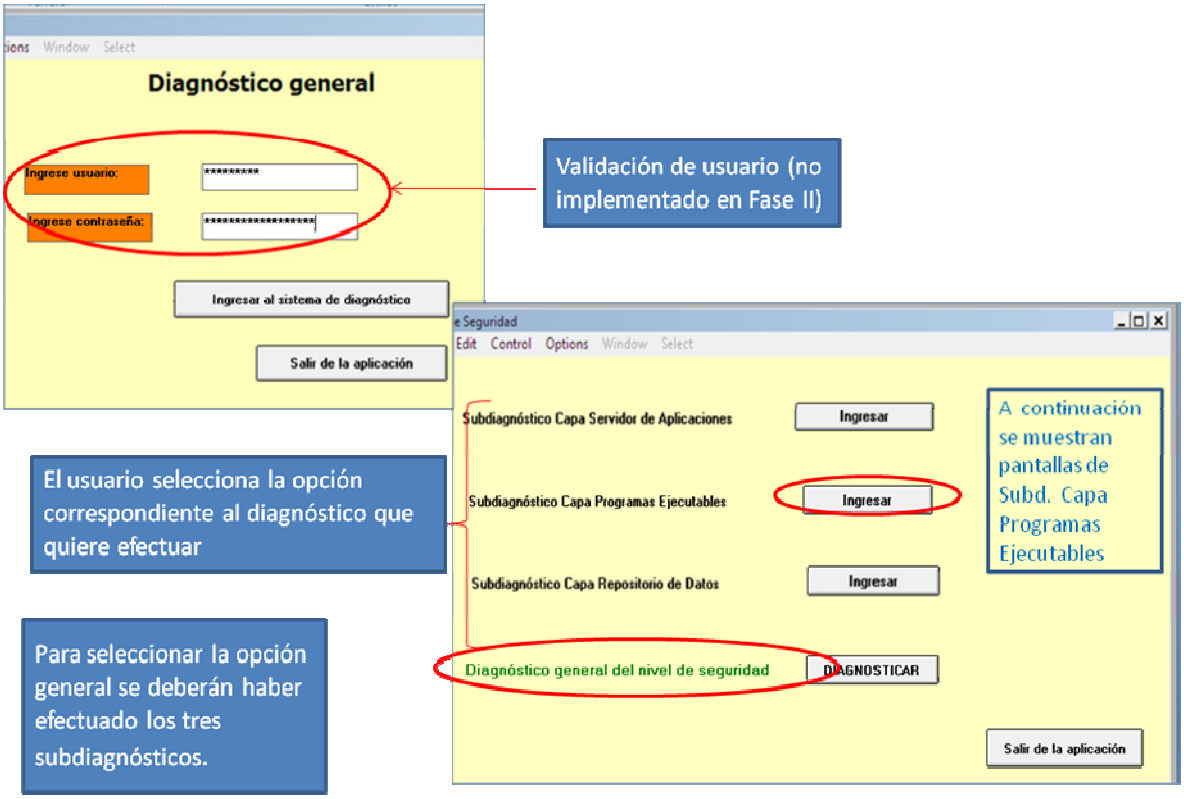


Fig. 8. Interfaces: Ingreso y validación de Usuario (a) – Menú de selección de subdiagnósticos (b)

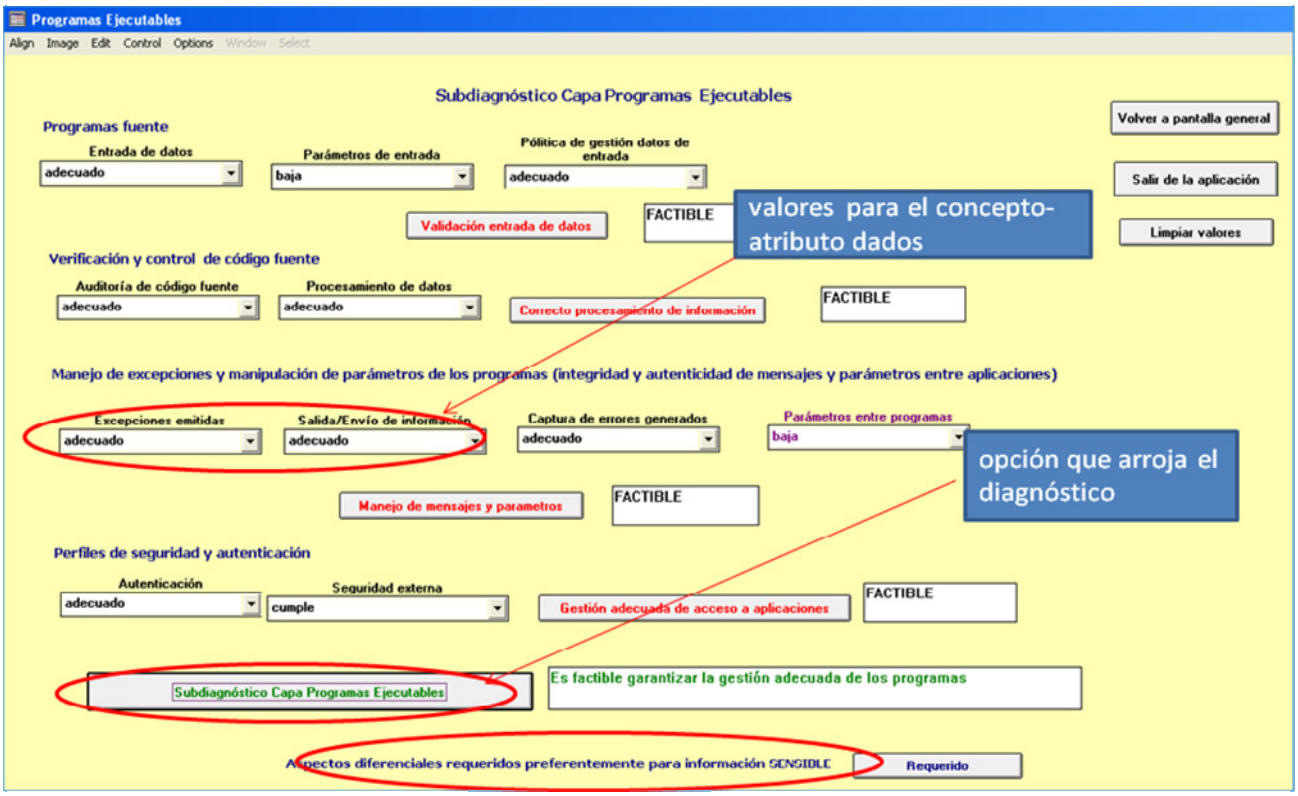


Fig. 9. Interfaz: Subdiagnóstico de Programas Ejecutables

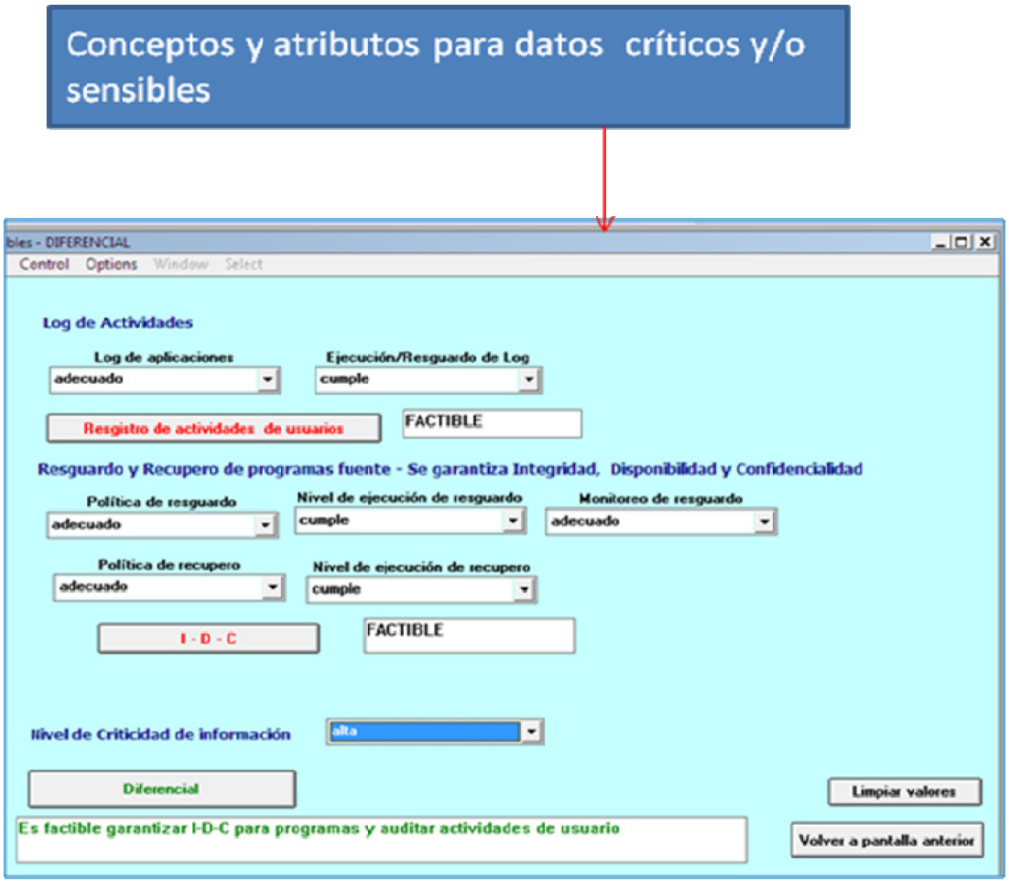


Fig. 10. Interfaz: Subdiagnóstico de Programas Ejecutables - Diferencial

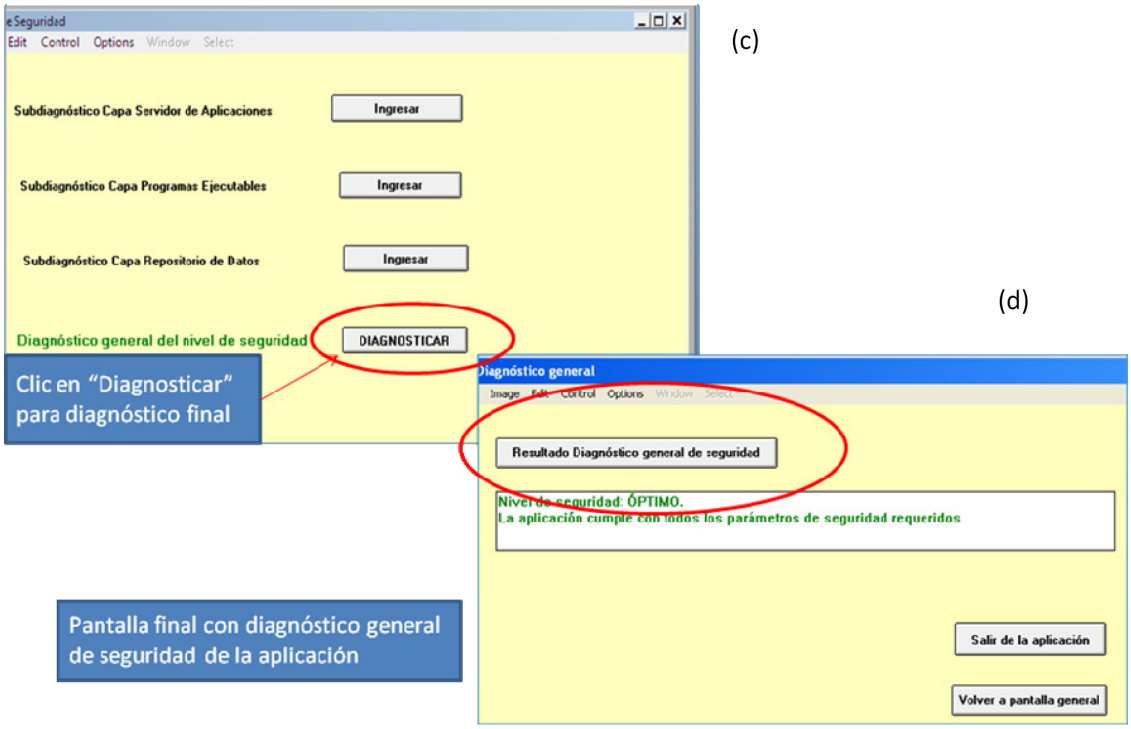


Fig. 11. Interfaces Diagnóstico Final (c) - Resultado obtenido de la evaluación (d)

3) Resumen de casos de prueba para validar el modelo propuesto

La siguiente tabla condensa la prueba funcional que efectuó el Experto. Es el resultado de diez (10) casos de prueba, instancias de casos base, que se aplicaron para la evaluación funcional del Sistema. Los mismos fueron presentados y evaluados por el experto y se basan en sus actividades cotidianas sobre su conocimiento basal.

TABLA I. RESUMEN DE PRUEBAS FUNCIONALES

Caso de prueba	Resultado Obtenido (Diagnóstico del Sistema)	Resultado Esperado (Diagnóstico del 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 - SATCS – SAT Control Stage	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.
4 - Gestión de Accesos automáticos	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 adecuación de ambiente de desarrollo/prueba.
5 - 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.
6 - Emulador Web	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.
7 - 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.
8 - 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.
9 - Cambio de Delegación por e-mail	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.
10 - 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.

III. CONCLUSIONES

Se detallan los aportes que el presente trabajo ofrece a la problemática específica de la seguridad de las aplicaciones de gestión, teniendo en cuenta los siguientes aspectos:

- 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 Especificación de Requisitos de Software (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.
- Documenta y modela la educción y extracción de conocimiento. Se apoya en técnicas de adquisición de conocimiento, la elaboración de una taxonomía de los requisitos funcionales y no funcionales, la conceptualización de los conocimientos estratégicos, facticos y tácticos para el domino de seguridad de las aplicaciones, la formalización y la posterior implementación de un prototipo del SBC, validado a través de casos de pruebas determinados por el experto en Seguridad de la Información.
- Sostiene la aplicación de la solución a través de un SBC, sobre la base de un Test de Viabilidad que permite, desde una etapa temprana, establecer un umbral de éxito que vale como incentivo para continuar con el desarrollo del Sistema Experto.

IV. Trabajo Futuro

Se exponen las futuras líneas de investigación que se pueden tomar en cuenta con el objetivo de continuar con el presente trabajo incrementando las funcionalidades del Sistema Experto y ampliando el conocimiento del sistema a través de la incorporación de módulos para el manejo de situaciones específicas. Del trabajo efectuado, así como de la experiencia adquirida, surgen las siguientes propuestas:

- 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 conceptos relacionados con la seguridad en la Capa Autenticación, ampliando conceptos relacionados con la seguridad de la Capa Servidor Aplicaciones, Capa Programas Ejecutables y Capa Repositorio de Datos, 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 interfaz de usuario vía WEB.
- Investigar la viabilidad de la aplicación de reglas difusas en el domino de estudio.

Agradecimientos

A la Escuela de Posgrado de la Universidad Tecnológica Nacional y al Instituto de Sistemas Inteligentes de la Universidad de Morón. Por último, y muy especialmente, al Experto en Seguridad de la Información por todo el trabajo de campo realizado, por sus grandes aportes al trabajo y por el tiempo brindado desinteresadamente.

Referencias bibliográficas

[1] ArCERT (Coordinación de Emergencias en Redes Teleinformáticas de la Administración Pública), Subsecretaría de Gestión Pública) www.arcert.gov.ar.

[2] Bajarlía, M.V. 2010."Modelo del conocimiento en Seguridad de aplicaciones".Tesis de Magister en Ingeniería en Sistemas de Información, UTN, Escuela de Posgrados, publicado.

[3] Bajarlía, M.V., Ierache, J., Eterovic, J. 2010. "Modelo de Sistema Basado en Conocimiento para el Análisis de la Seguridad de la Información en el Contexto de los Sistemas de Gestión". XVI Congreso argentino de ciencias de la computación- V Workshop Arquitectura, Redes y Sistemas Operativos (WARSO), CACIC 2010. Universidad de Moron, 18 al 22 de Octubre, 2010. ISBN 78-950-9474-49-9, publicado.

[4] Bajarlía, M.V., Ierache, J., Eterovic, J. 2008. "Elaboración de Especificación de Requerimientos de Seguridad en el desarrollo de Sistemas de Información basado en la Modelización de Conocimientos". X Workshop de Investigadores en Ciencias de la Computación - WICC 2008, Universidad Nacional de La Pampa, 5 y 6 de Mayo, 2008. ISBN 978-950-863-101-5, publicado.

[5] Fernández Galán, S., González Boticario, J., Mira Mira, J.1998. Problemas resueltos de Inteligencia Artificial Aplicada. Búsqueda y representación. Addison-Wesley.

[6] García Martinez R., Britos P.2004. Ingeniería de Sistemas Expertos. Nueva Librería.

[7] Giarratano, J., Riley, G.2000. Sistemas Expertos Principios y Programación. Thomson International.

[8] Harrison, R. 1999. ASP/MTS/ADSI Web Security. Longman.

[9] HISPASEC SISTEMAS. www.hispasec.com .

[10] IEEE (Institute of Electrical and Electronics Engineers), www.ieee.org.

[11] Intellicorp. 1992. Kappa PC Quick Start. Intellicorp Inc.

[12] Intellicorp. 1992. Kappa PC User Guide Intellicorp Inc.

[13] ISECOM (Institute for security and open methodologies) www.isecom.org.

[14] ISO (International Organization for Standardization), www.iso.org.

[15] ISO/IEC 27001, 2006. Gestión de la Seguridad de la Información.

[16] Jaworski, J., Perrone, P.J. 2000. Seguridad en Java. Prentice Hall.

[17] Kaeo, M. 2000. Diseño de Seguridad en Redes. Pearson Educación.

[18] Maiwald, E.2005. Fundamentos de la seguridad de redes. Conocimientos esenciales a tu alcance. McGraw-Hill.

[19] Maté Hernández, J.L., Pazos Sierra J. 1988. Ingeniería del Conocimiento. Diseño y construcción de sistemas expertos. Sepa S.A.

[20] MinsKy M. 1975. A framework for representing Knowledge.McGraw Hill.

[21] NIST (National Institute of Standards and Technology, Technology Administration U.S. Department of Commerce), www.nist.gov .

[22] Piattini Velthuis, M., Del Peso Navarro, E.2001. Auditoría informática un enfoque práctico. Alfaomega Grupo Editor Argentino S.A.

[23] PKI (Public Key Infraestructure), Subsecretaría de Gestión Pública www.pki.gov.ar

[24] Pressman R.2006. Ingeniería del Software, un enfoque práctico. McGraw Hill.

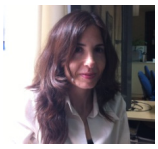
[25] Rusell, S.J., Norvig, P. 2004. Inteligencia Artificial. Pearson Educación.

[26] Seguridad en Java www.java.sun.com/products/jaas.

[27] Seguridad en Windows www.microsoft.com/security

[28] Sommerville, I. 2002. Ingeniería de Software. Addison Wesley.

[29] Stallings, W. 2004. Fundamentos de la seguridad en redes. Aplicaciones y estándares. Pearson Educación.



María Victoria Bajarlía Magister en Ingeniería en Sistemas de Información, Universidad Tecnológica Nacional en 2010. Especialista en Ingeniaría en Sistemas de Información, Universidad Tecnológica Nacional en 2009. Actualmente es Analista de Calidad en Proyectos de T.I. en el sector público. Docente adjunta en Universidad de Ciencias Empresariales y So-ciales en el área de Programación, docente auxiliar en Universidad Tecnológica Nacional en el área de Sistemas. En el campo de la educación cuenta con intereses en po-sicionamiento en actividades de I+D, gestión académica de grado y pos grado, transferencia de tecnología, publi-caciones y artículos técnicos, proyectos de investigación, etc. En el ámbito laboral la expectativa es continuar con el liderazgo funcional, en el marco de la gestión de la calidad aplicada a proyectos de TI.

Jorge Eterovic. Magister en Dirección de Sistemas de Información por la Universidad del Salvador, Especialista en Criptografía y Seguridad Teleinformática por la Escuela Superior Técnica - Universidad del Ejército. Director de la carrera de Ingeniería en Informática y Profesor titular de la materia Auditoria y Seguridad Informática en la Universidad de Morón. Profesor Asociado de las materias Proyecto y Auditoria y Seguridad Informática en la Universidad Nacional de La Matanza. Docente de posgrado en las Universidades Austral, del Salvador y Nacional de La Matanza. Categorizado como Investigador Principal en el régimen del CONICET.

Jorge Ierache Doctor en Ciencias Informáticas por la Universidad Nacional de la Plata, Magíster en Ingeniería del Conocimiento por la Universidad Politécnica de Madrid. Profesor Adjunto regular del área Ingeniera de Software Facultad de Ingeniería Universidad Nacional de Buenos Aires, Director del Laboratorio de Sistemas Avanzados de Información de FIUBA y del Instituto de Sistemas Inteligentes y Enseñanza Experimental de la Robótica (ISIER) de la Universidad de Morón.