Utilización del Razonamiento Basado en Casos como apoyo a la toma de decisiones en Seguridad Informática

MSc. Mirta Julieta García García, Técnico B en Telemática, Departamento Planificación Estratégica, Vicepresidencia de Tecnología de la Información (VPTI), ETECSA
mirta.garcia@etecsa.cu

Introducción

Una de las formas más comunes en que los seres humanos resuelven cierto tipo de problemas, es utilizando una especie de razonamiento y aprendizaje basado en analogías. Es fácil darse cuenta de que la experiencia es una característica importante que todo buen profesional debe poseer. La mayoría de las personas que buscan la ayuda de un experto, eligen a uno con suficientes vivencias sobre las cuales base sus acciones.

Resulta interesante notar que este tipo de razonamiento existe en muchas situaciones cotidianas en las que se utilizan analogías y memoria como base del razonamiento y aprendizaje. Algunas de estas situaciones son por ejemplo: el aprendizaje de nuevas habilidades, la planeación diaria de nuestras actividades, jugar ajedrez, etc. Las nociones claves son experiencia, memoria y analogías.

En inteligencia artificial (IA), se le ha dado el nombre de Razonamiento Basado en Casos (RBC) a este tipo de razonamiento que se asume como un nuevo paradigma que provee, por un lado, un modelo cognoscitivo de la organización de la memoria, el razonamiento y el aprendizaje humano; y por otro, una nueva técnica para el desarrollo de sistemas computacionales [1].

En el presente trabajo se diseña e implementa una base de casos y se genera un experto en materia de seguridad informática con el propósito de apoyar y favorecer la toma de decisiones, a partir de la información relacionada con hechos violatorios de la seguridad en la Empresa de Telecomunicaciones de Cuba, S.A. (ETECSA). La base de conocimiento cuyo desarrollo se presentará es de casos, cuestión por la cual es necesario abordar, en primer lugar, algunos aspectos conceptuales del RBC.

Desarrollo

El Razonamiento Basado en Casos: fundamentos e implicaciones

Según Kolodner [2], el RBC es, por una parte, el modo en el que las personas utilizan casos para resolver problemas; y por otra, las formas con las que se puede hacer que las máquinas los utilicen. Difiere de otros enfoques y técnicas en que es capaz de emplear el conocimiento adquirido en situaciones previas y utilizarlo en la situación presente, si pertenecen al mismo contexto [3]. Para Riesbeck & Schank [4] no es más que un problema nuevo que se resuelve buscando en la memoria

un caso similar resuelto en el pasado. Al agregar nuevos casos para situaciones futuras, se enriquece aún más, lo cual le permite la actualización del dominio con el aumento del conocimiento almacenado.

Por consiguiente, el RBC es parte de la IA y tiene como objetivo esencial concentrar la experiencia en un sistema informático a través de un proceso de aprendizaje. De ese modo, el sistema se convierte en una memoria corporativa de los éxitos y errores previos, y se dota con la capacidad de autoaprendizaje [2]. El RBC no utiliza un modelo formal de conocimiento y con él se pretende recopilar en una base casos-experiencias que describen situaciones típicas, relevantes y representativas para razonar por analogías.

Esto implica que la adquisición del modelo formal se sustituya por la recopilación de casos típicos representativos del dominio para el que se construye el sistema y, además, que la implementación se centre únicamente en la determinación de los rasgos relevantes para cada uno de los casos.

La idea sobre la cual descansa esta nueva técnica es la siguiente: se le proporciona al sistema una especificación o problema de entrada y este busca en su memoria de casos uno ya existente que corresponda con la especificación de entrada suministrada. En la mejor de las situaciones, se hallará un caso que se ajuste perfectamente con el problema dado como entrada, y se obtiene la solución de modo directo. Pero si no es así, se encontrará uno o varios casos similares a la situación de entrada. Las posibilidades de hallar un caso que encaje perfectamente con la especificación de entrada, aumentan en la medida en que la memoria del sistema —es decir, la base de casos— sea mayor.

Si sólo se localizan casos similares, el usuario y el sistema entran en un proceso de adaptación. En este proceso se encuentran y modifican pequeñas porciones de los casos similares encontrados. Con esto se logra, por un lado, una solución completa al problema y, por otro, un nuevo caso que el sistema puede aprender, o sea, un nuevo caso que el sistema puede almacenar para su reutilización al enfrentar problemas similares en el futuro. En las figura 1 se representa un esquema general del RBC y, en la figura 2, un mapa conceptual del mismo.

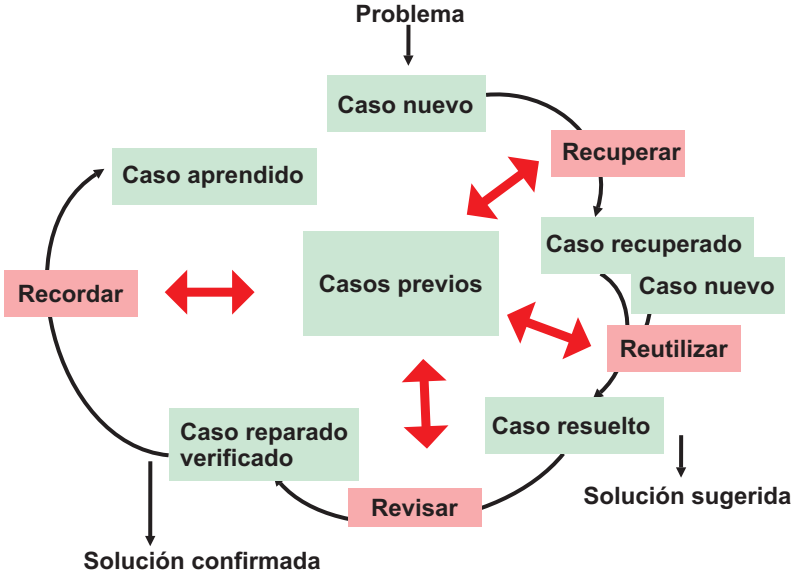

Figura 1 Esquema general del RBC [4]

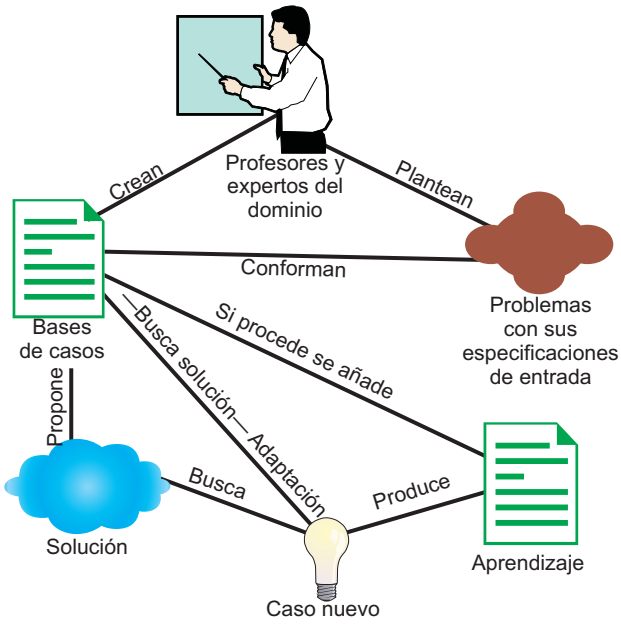

Figura 2 Mapa conceptual del Razonamiento Basado en Casos [4]

La intención es construir sistemas computacionales que permitan ayudar al hombre en diversas tareas cotidianas e importantes, donde normalmente sería necesario emplear a un experto.

La base de conocimientos

La adquisición del conocimiento y su modelización son las tareas que más tiempo requieren y más dificultades presentan al construir un sistema experto (SE). Puede ocurrir que no haya expertos, que las personas disponibles no sean tan versadas en ese campo de conocimiento, o que no quieran dar su conocimiento o no puedan —porque sea intuitivo—. Como resultado de la adquisición, se construye una base de conocimientos.

La base de casos es la encargada de mantener la representación y organización de los casos. Los casos son lecciones aprendidas a partir de un problema anteriormente resuelto, por lo tanto mantienen información del contexto y su solución [5]. Su propósito es facilitar la solución de problemas similares que eventualmente surgirán.

En el presente trabajo ha sido creada una base de casos sobre violaciones de la seguridad informática a partir de casos ocurridos y la decisión tomada en cada uno.

Existen diversas herramientas de software que posibilitan la aplicación del Razonamiento Basado en Casos, comúnmente utilizadas con fines académicos, entre ellas se encuentran: SISI —Sistema Inteligente de Selección de Información, desarrollado por investigadores cubanos de la Universidad Central de la Villas—, CASUEL —desarrollado en 1992, en el Proyecto INRECA fundado por la Unión Europea— y CASPIAN —desarrollado por el Departamento de Ciencias de la Universidad de Wales—.

En esta propuesta, específicamente, el intérprete de órdenes (*shells*) para el RBC que se utiliza para las pruebas y el uso de la base de conocimientos es el SISI, debido a que cuenta con una interfaz amigable y no requiere de una extensa capacitación para manipularlo. Su estilo de trabajo es de tipo interpretativo y utiliza ficheros de extensión .cbe que constituyen la base de casos.

La herramienta utilizada para la adquisición del conocimiento es el CBE, un editor de bases de conocimiento que fue construido por los mismos investigadores que crearon el intérprete de órdenes para el Razonamiento Basado en Casos SISI.

Para la realización del Sistema Basado en Casos, se plantearon de manera simplificada los requerimientos del sistema usuario/especialista de seguridad informática lo cual se muestra a continuación:

Usuario/especialista de seguridad informática	¿Qué necesita del sistema?
Usuario	Comete la violación informática
Especialista de seguridad informática	Registrar los análisis de la violación
	Registrar resultados de los análisis de la violación —solución o esclarecimiento—

Tabla 1 Necesidades del sistema de usuario/especialista de Seguridad Informática. (Fuente: elaboración propia)

A partir de la tabla anterior, se obtiene el Diagrama de Casos de Uso, que permite modelar el proceso simplificado que ocurre ante una violación considerando, además, como actores el contenido de la columna Usuario/ Especialista de Seguridad Informática.

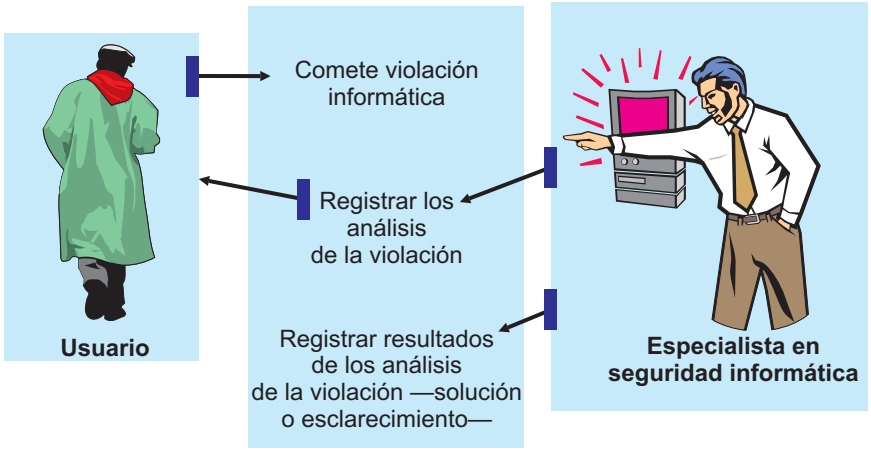

Figura 3 Diagrama de casos de uso para las violaciones informáticas. (Fuente: elaboración propia)

Para definir el contenido del sistema, la organización y el análisis de la información de la base de casos, se requirió la consulta de especialistas y expertos, así como la correspondiente revisión bibliográfica sobre el tema.

Propuesta de la base de conocimientos —base de casos—

De manera general, el análisis comprende la descripción y preparación de los datos indispensables para valorar las relaciones entre las variables y los resultados obtenidos. La Base de casos relativa a la investigación está formada por 8 rasgos predictores y un rasgo objetivo, la actuación (Tabla 2).

Rasgos	Variables	Valores	Fuente de obtención
Alcance	x1	- Parcial -Total	Violación informática
Referencia a documentos legales	x2	- No refiere - Referencia en documento normativo Empresa - Referencia en documento normativo MIC - Referencia en documento normativo país	Violación informática
Impacto de la afectación	x3	- No - A la Empresa - Al usuario - Paraliza servicios Web - Paraliza servicios correo - Paraliza el negocio - No refiere	Violación informática
Tipo de violación	x4	- No refiere - Ataques informáticos - Violación del trabajo con la información clasificada - Difusión de virus informáticos - Publicación de material subversivo y/o ofensivo - Denegación del servicio - Intento de acceso no autorizado a sistemas informáticos y servicios de Internet y otros - Recopilación y/o divulgación no autorizada de información - Violaciones en la transmisión de la información clasificada - Difusión de material pornográfico - Propaganda no acorde con los valores éticos, culturales, sociales y políticos de nuestra sociedad - Calumnias, injurias contra cualquier persona de la Empresa - Daños al sistema informático - Difusión de software con fines fraudulentos - No adopción de la Política antivirus establecida - Spam comercial - Spam de contenidos banales del tipo Hoax	Violación informática
Conocimiento del plan de seguridad informática y de contingencias	x5	- Sí - No - No refiere	Violación informática
Conocimiento del plan de contingencias	x6	- Sí - No - No refiere	Violación informática
Cargo	x7	- No - Funcionario - Dirigente - Especialista - Administrador de red - Especialista seguridad informática	Violación informática
Actuación	y1	-Conciente - Inconsciente	Violación informática
Acción a realizar por el especialista de seguridad informática	y2	- Plan recursos capacitación - Plan seminarios - Separación definitiva - Separación del cargo - Afectación salarial - Traslado temporal a otra plaza de menor cuantía - Amonestación pública - Amonestación privada	Violación informática

Tabla 2 Estructura de la base de conocimientos. (Fuente: elaboración propia)

La base de casos guardará toda la información sobre las violaciones ocurridas y las medidas tomadas, lo que constituye un excelente material de consulta y estudio.

Con esta base, el sistema realiza el diagnóstico de las situaciones de violaciones de la seguridad informática y la propuesta de medida a tomar a partir de las similitudes que pueda tener con otros casos ya existentes en la base.

La presentación de casos y su posterior discusión diagnóstica es un tipo de educación en el trabajo que tiene como objetivo que los usuarios desarrollen los raciocinios necesarios para integrar y evaluar los datos encontrados en las nuevas situaciones que se presenten, a la luz de los conocimientos teóricos y de la información pertinente para llegar a un juicio de tipo diagnóstico, que permita establecer juicios pronósticos o retroactivos correspondientes. Con la presentación de casos se entrena al directivo y especialista en seguridad informática en las operaciones de identificación, modificación o rechazo de la hipótesis planteada y el establecimiento de una propuesta a analizar y ejecutar.

Una vez concluidos los primeros casos, se efectuaron pruebas iniciales con la participación de especialistas en seguridad informática para verificar el funcionamiento de la base de casos al diagnosticar cualquier posible acción a tomar.

En las figuras 4 y 5 se muestran ejemplos de la base de casos con sus atributos y valores, editados con el Case Base Editor (CBE).

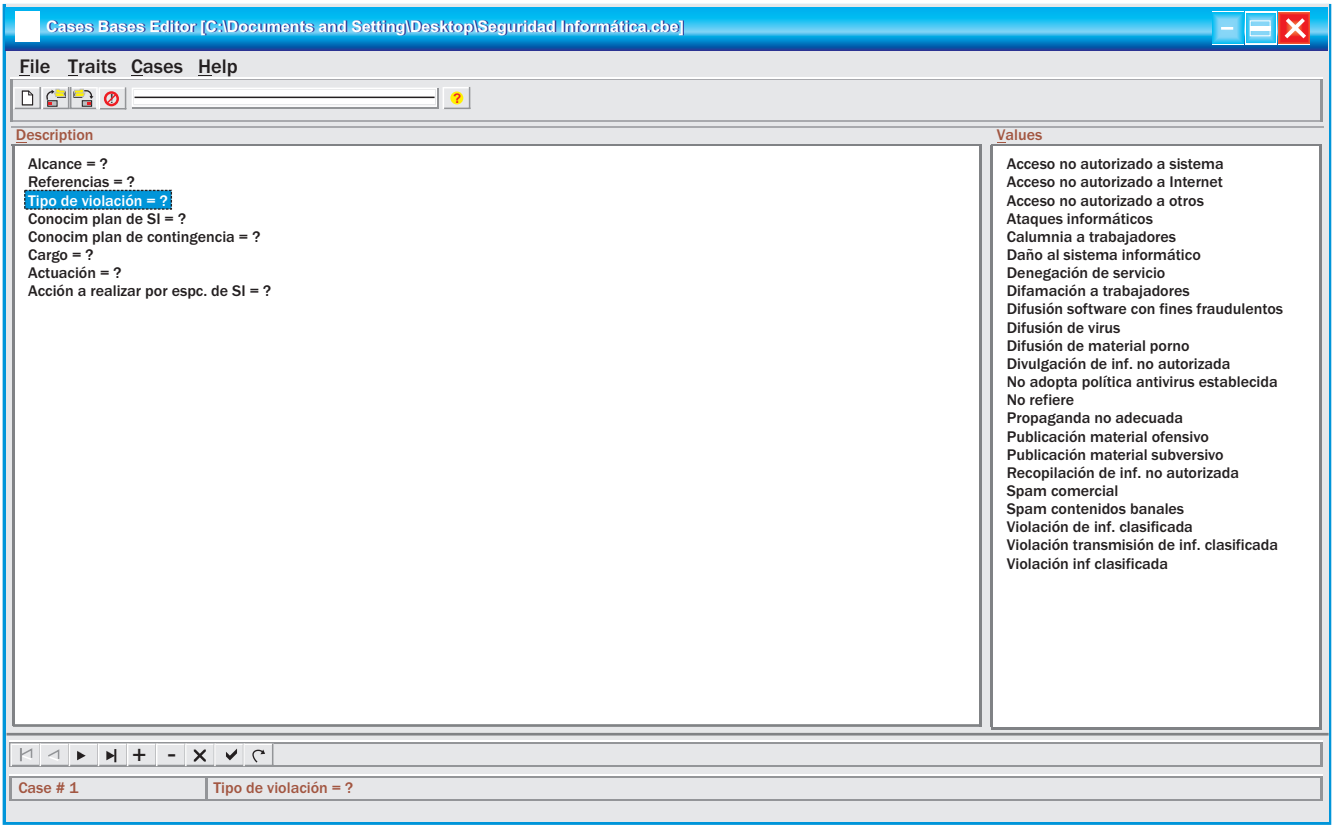

Figura 4 Ejemplo de los valores definidos según el tipo de violación en la base de casos. (Fuente: elaboración propia)

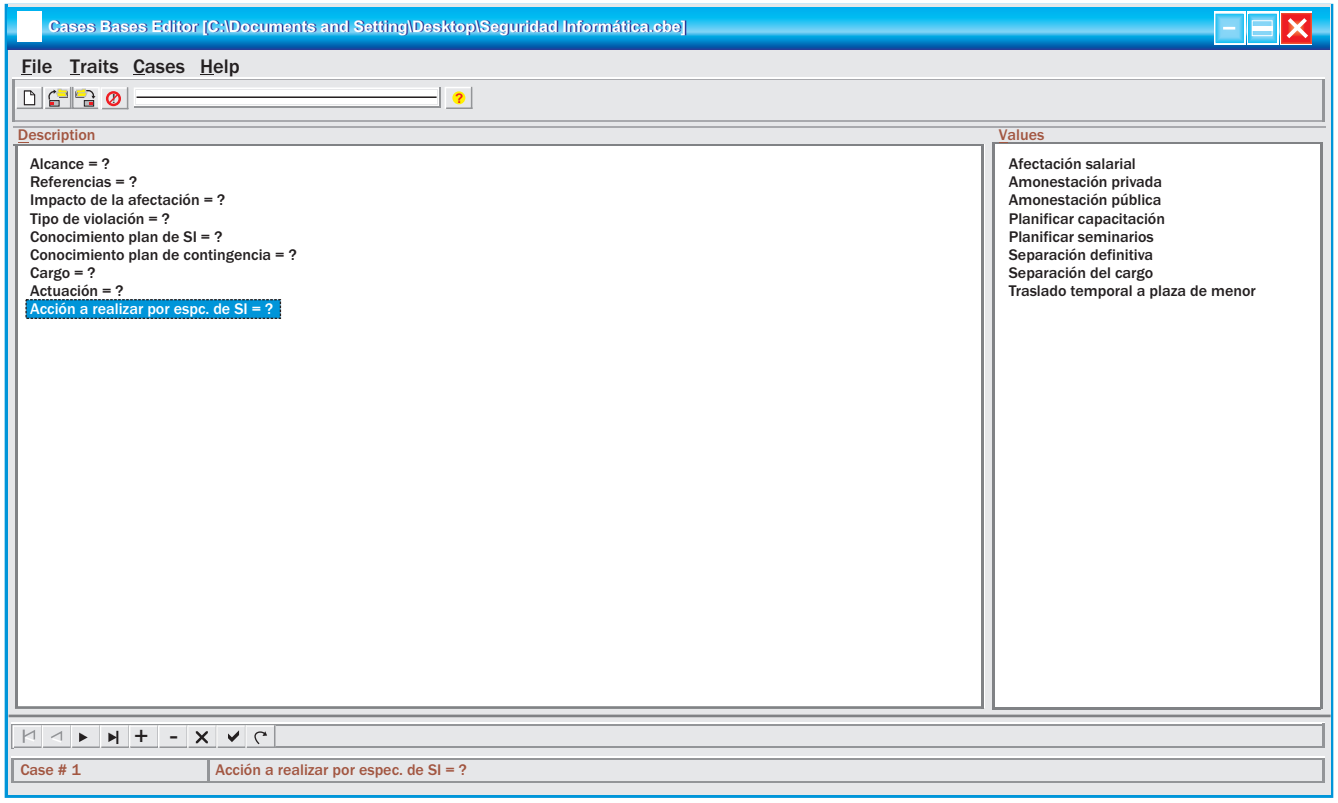

Figura 5 Ejemplo de los valores definidos según la acción a realizar por el especialista de Seguridad Informática en la Base de Casos. (Fuente: elaboración propia)

El experto creado con el diagnóstico de un caso resuelto aparece en la figura 6.

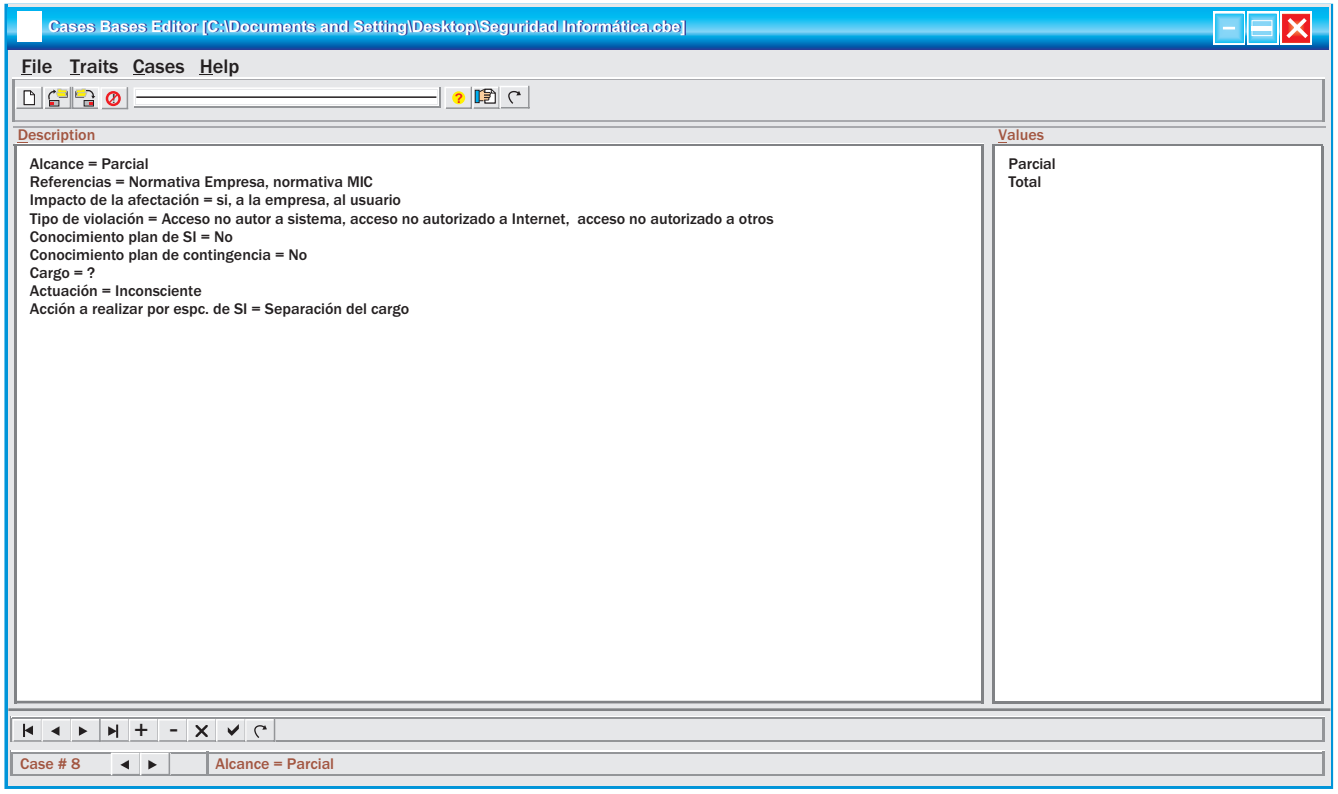

Figura 6 Ejemplo de un caso resuelto según SISI. (Fuente: elaboración propia)

Biblioteca de casos resueltos

La biblioteca de casos contiene los problemas resueltos que se le han dado al sistema, cuyo número aumentará conforme se enriquezca con un mantenimiento constante o por aportación del mismo sistema.

La base de casos sobre diferentes situaciones de violaciones de la seguridad informática y las medidas tomadas, es la encargada de mantener la representación y organización de los casos. Para extraer el conocimiento, se empleó una fuente de conocimiento documentado (explícito). También se gestionó conocimiento tácito, aspecto de mucha importancia para el desarrollo de este trabajo. Se realizaron entrevistas a expertos y se aplicaron cuestionarios a especialistas de seguridad informática cuyo perfil está directamente relacionado con la gestión de la seguridad informática. Otra de las técnicas utilizadas para la evaluación del conocimiento tácito extraído de los expertos y plasmado en la base de casos fue el grupo focal —focus group—.

Análisis de la información de la base de casos con el software SISI

Para la creación del experto se siguieron los siguientes pasos.

A) Crear la estructura de la Base de casos con el editor CBE

1.Activar el menú *File* y elegir *New* para una base de casos nueva. Seleccionar el menú *Trait* y, luego, elegir *Add*, esperar por el cuadro de diálogo *New trait.*

2.Escribir el nombre de rasgo, el tipo de datos y el ancho para los valores, a continuación, presionar el botón *Domain* y esperar por el cuadro de diálogo *Domain edition.*

3.Proceder a editar y agregar cada uno de los valores del rasgo; al terminar, presionar el botón OK.

4.Realizar el mismo procedimiento para cada rasgo a partir del paso 2 hasta que se termine la estructura con sus rasgos y valores

5.Guardar la estructura de la base de casos eligiendo la opción *Save* del menú *File*.

La siguiente figura muestra la pantalla principal del editor de casos CBE.

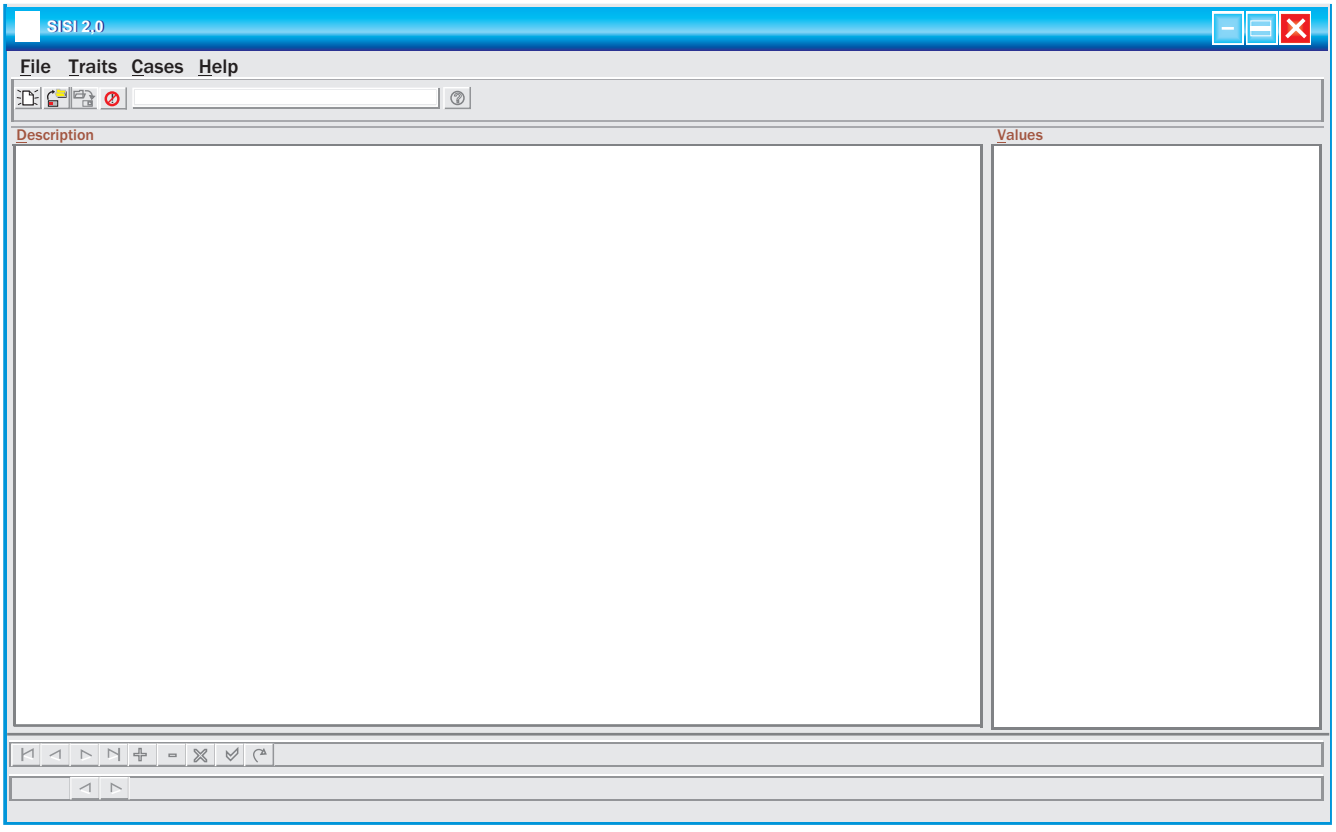

Figura 7 Pantalla principal del editor CBE [4]

B) Introducir los casos

1.Activar el menú *File* y elegir *Open*, posteriormente señalar la base de conocimiento.

2.Elegir con doble clic el valor de entrada para cada rasgo.

3.Una vez señaladas la entradas (valores), activar el menú *Cases* y elegir *Add*.

4.Realizar el mismo procedimiento a partir del paso 2 tantas veces como casos se agreguen.

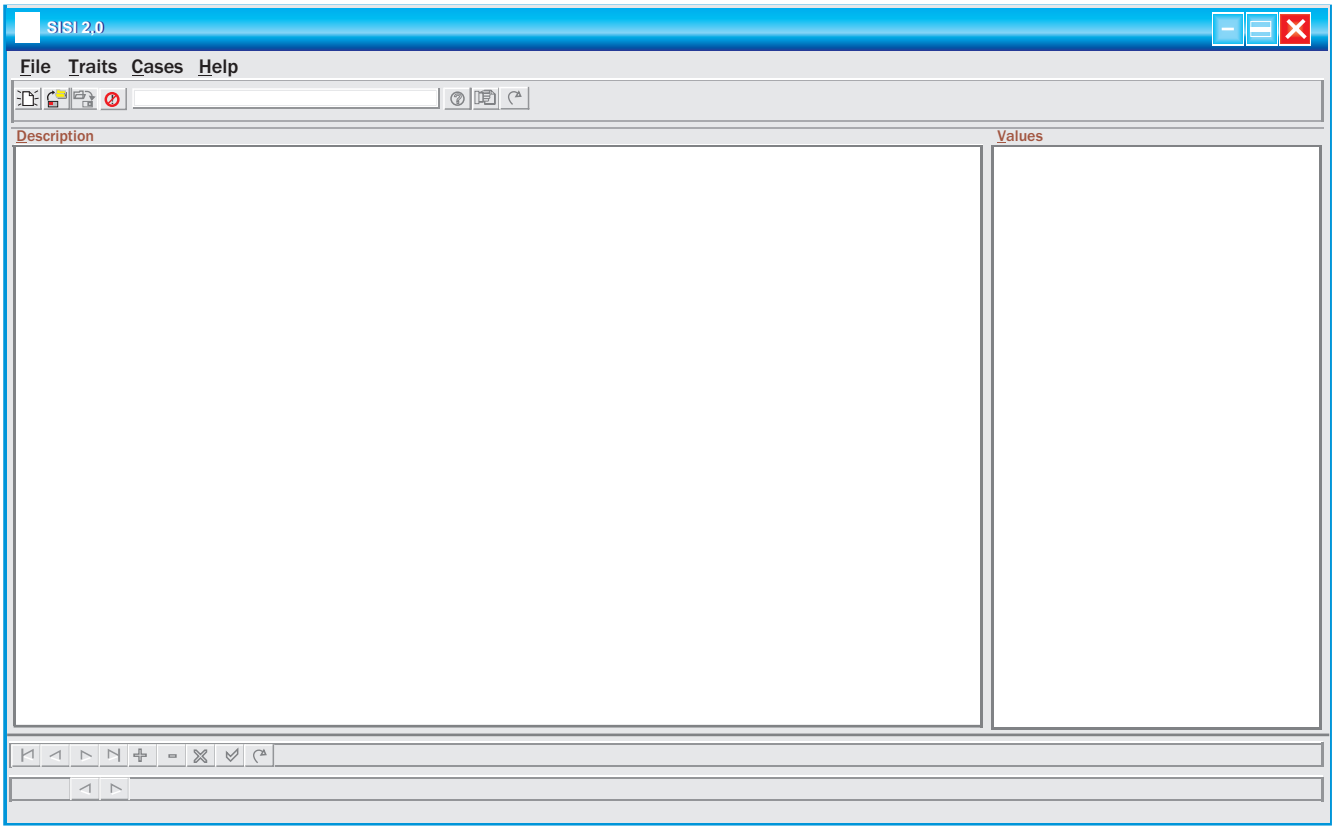

Figura 8 Pantalla principal del software SISI v 2.0 [4]

C)Procedimiento general para consultar los casos usando el SISI

1.Activar el menú *File* y Seleccionar la opción *New*.

2.Presionar el botón *Browse* y señalar base de conocimiento a consultar.

3.Al presionar el botón OK, se presentarán los rasgos y los valores.

4.Seleccionar con un clic cada rasgo e introducir el valor correspondiente presionando doble clic sobre el valor de entrada.

5.Una vez introducidos los valores según cada rasgo, activar el menú *Expert* y elegir la opción *Infer Case*.

Principales beneficios obtenidos con la construcción de una base de conocimientos —base de casos—:

- Soluciones a partir de casos resueltos lo que simplifica la toma de decisiones y reduce el tiempo de respuesta en el análisis de nuevas violaciones a la seguridad.
- Soluciones más confiables debido a que se generan basadas en casos reales, es decir, los casos reflejan lo que realmente sucede.
- Aprender a partir de un conocimiento existente el cual puede crecer reflejando la experiencia acumulada.

Conclusiones

A partir de los resultados alcanzados pueden plantearse las siguientes conclusiones:

1- La utilización de un sistema de Razonamiento Basado en Casos es un punto de partida en la introducción de las técnicas de inteligencia artificial en materia de seguridad informática.

2- La base de casos desarrollada juega un papel muy importante al poner a disposición de directivos y especialistas de seguridad informática un conocimiento sobre los principales hechos ocurridos en cuanto a las violaciones de la seguridad informática.

3- Esta base de casos servirá de referencia en la toma de decisiones en el momento de ocurrir algún hecho violatorio.

4- Los resultados de los métodos de investigación aplicados evidenciaron que disponer de una base de conocimientos de casos constituye una herramienta para fomentar la cultura sobre el tema entre directivos, especialistas y usuarios en general y, en consecuencia, crear las condiciones para disminuir los incidentes de seguridad y mejorar su gestión.

5- Esta base de conocimientos permite disponer de un conocimiento almacenado para la solución de los casos, que influye en la manera de tomar una adecuada decisión ante un hecho violatorio y, además, disminuye el período de respuesta del análisis de estos hechos que infringen la seguridad informática en los entornos laborales.

Referencias bibliográficas

[1] Almeida Campos, Santiago. "Metodología para la gestión del conocimiento en ciencias básicas biomédicas con el empleo de las tecnologías de la información y las comunicaciones". Tesis presentada en opción al grado científico de Doctor en Ciencias de la Educación, Universidad de Matanzas "Camilo Cienfuegos", Matanzas, 2007. Ciudad de La Habana: Ministerio de Educación Superior, Editorial Universitaria, 2008. Disponible: http://revistas.mes.edu.cu/elibro/tesis/ciencias-de-la-educacion/9789591607676.pdf/at_download/file. (acceso febrero 27, 2008).

[2] Citado por Estrada Sentí, Vivian. "Razonamiento Basado en Casos (RBC)". Módulo Inteligencia Artificial, 9na Edición Maestría Gestión de Información en las Organizaciones, La Habana, 2007.

[3] Medina Pagola, Mercedes y Febles Rodríguez, Juan Pedro. "Utilización del Aprendizaje basado en Problemas Bajo la Óptica de la Inteligencia Artificial". Revista Cubana de Informática Médica, año 2, no. 1 (2002). Disponible: http://www.rcim.sld.cu/revista_2/articulos_html/febles.htm. (acceso enero 15, 2008).

[4] Citado por Estrada Sentí, Vivian. "Inteligencia Artificial". Módulo Inteligencia Artificial, 9na Edición Maestría Gestión de Información en las Organizaciones, 2007

[5] Watson, Ian and Marir, Farhi. "Case, -Based Reasoning: A Review". Disponible http://www.ai-cbr.org/classroom/cbr-review.html. (acceso febrero 27, 2008)