Modelo de Sistemas Multi-Agentes para Percibir, Evaluar y Alertar Ex-Antes los Accesos no Autorizados a Repositorios de Base de Datos

Adrian Eusebio Quisbert Vilela
Postgrado en Informática
Universidad Mayor de San Andrés - UMSA
La Paz, Bolivia
aquisbertvilela@gmail.com

***Resumen*— En el presente trabajo de investigación se presenta la propuesta de un modelo de sistema multi-agente para percibir, evaluar y alertar ex-antes la detección de vulnerabilidades a los repositorios de bases de datos. Esta propuesta utiliza la tecnología de agentes inteligentes. Para esto, los agentes inteligentes hace uso de reglas de razonamiento que están almacenados en una base de conocimiento bajo un patrón de vulnerabilidad y así alertar de forma temprana la vulneración, para notificar a los administradores de base de datos y de sistemas para tomar las acciones correspondientes.**

Palabras clave*— *Multi-agente, Agentes inteligentes, Repositorios de base de datos, diseño de patrones, Vulnerabilidad.

I. INTRODUCCIÓN

Actualmente la informática y las redes de datos han evolucionado bastante donde se han desarrollado diferentes aplicaciones tanto en ambientes locales como en ambientes web, que emplean como mecanismo de transferencia de datos a la internet, estas aplicaciones acceden a repositorios de bases de datos las cuales proporcionar información a diferentes usuarios. Junto a estas aplicaciones se han introducido nuevas posibilidades de riesgos y vulnerabilidades a los repositorios de bases de datos, estos accesos no autorizados pueden realizarse de forma interna o externa.

Es así que las organizaciones, sean estas públicas o privadas y con el constante avance tecnológico cuenta con repositorios de bases de datos y aplicaciones que acceden a estas con fin mejorar los servicios a los usuarios o alcanzar los objetivos de la organización.

En este contexto las organizaciones que cuentan con repositorios de bases de datos, han tomado muy en cuenta el de proteger la información con la que cuenta, implementando mecanismos de seguridad, estableciendo normas y políticas de seguridad, con el objeto de prevenir los accesos no autorizados a estas bases de datos y así de esta manera mantener la integridad, la confidencialidad y la disponibilidad de la misma.

Para disminuir dicha problemática, en el presente trabajo se propone un modelo de sistema multi-agente para percibir, evaluar y alertar ex-antes la detección de vulnerabilidades a los repositorios de base de datos. En la Sección II, se establecerá la descripción del problemática sobre vulneración a los repositorios de bases de datos. En la Sección III, se muestra la pregunta de investigación. En la sección IV se plantea el objetivo y los objetivos, en la Sección V se plantea la Hipótesis en la Sección VI se plantea el esquema general del modelo del sistema multi-agente y como esta percibirá la vulneración a los repositorios de base de datos, y en la Sección VII se establece el marco teorico en el cual se basara el modelo y Finalmente en sección VII se concluye con las conclusiones del trabajo propuesto.

II. DESCRIPCIÓN DE LA PROBLEMÁTICA.

En la actualidad las computadoras se utilizan no solo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener y conseguir información, también como un nuevo medio de comunicación y condiciona su desarrollo de la informática; tecnología cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos. El progreso de la tecnología y sostenido por los sistemas computacionales permite hoy procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza, al alcance concreto de millones de interesados y usuarios. Las más diversas esferas del conocimiento humano, en lo científico, en lo técnico, en lo profesional y en lo personal están siendo incorporadas a sistemas informáticos que, en la práctica cotidiana de hecho sin limitaciones, entrega con facilidad a quien lo desee un conjunto de datos, las cuales están almacenadas en repositorios de base de datos[1]

.La seguridad de datos presenta un reto multidimensional donde los ambientes complejos incluyen una gran cantidad de sistemas para gestión de base de datos, aplicaciones

empresariales, plataformas de sistema operativo con múltiples rutas de acceso y niveles de permiso heterogéneos que han generado un conjunto aparentemente interminable de escenarios de amenazas y violaciones de seguridad.

Los tradicionales "enfoques tipo Fortaleza" como firewalls y políticas de seguridad ya no son suficiente protección contra los atacantes del siglo XXI que fácilmente traspasan las barreras perimetrales.[2]

La mayor parte de la información sensible del mundo se almacena en bases de datos como Oracle, Microsoft SQL Server, IBM DB2, Informix, Sybase, MySQL, Netezza y Teradata , Lo que hace de las bases de datos sean un blanco cada vez más buscado por los ciber-criminales y usuarios internos de la organizaciones[2].

Las aplicaciones Web se han transformado y han mejorado la manera en que las empresas hacen negocios, pero también han hecho que las bases de datos estén más expuestas. La exposición existe porque la aplicación que utiliza los datos ahora sirve a un público mucho mayor y porque los usuarios no están limitados a empleados internos. Los atacantes tienen ahora una vía de entrada directa a través de la aplicación, pasando las defensas perimetrales al interior de la base de datos[2].

Si bien los repositorios de base de datos almacenan grandes volúmenes de información estas deben mantener los siguientes propiedades[3]:

- Confidencialidad, La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.
- Integridad, para la seguridad de la información, la integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.
- La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información.
- La Disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizado para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. Garantizar la disponibilidad implica también la prevención de ataque Denegación de servicio. La disponibilidad además de ser importante en el proceso de seguridad de la información.

Según el informe de Verizon (Data Breach)[4]. El 96% de los datos sustraídos durante 2012 provenían de bases de datos, estas amenazas frecuentes a base de datos se debe a lo siguiente:

Tabla 1.1 Amenazas de bases de datos

Privilegios excesivos e inutilizados.	Cuando a alguien se le otorgan privilegios de base de datos que exceden los requerimientos de su puesto de trabajo se crea un riesgo innecesario. Los mecanismos de control de privilegios de los roles de trabajo han de ser bien definidos o mantenidos
Abuso de Privilegios	Los usuarios pueden llegar a abusar de los privilegios legítimos de bases de datos para fines no autorizados, por ejemplo, sustraer información confidencial. Una vez que los registros de información alcanzan una máquina cliente, los datos se exponen a diversos escenarios de violación.
Inyección por SQL.	Un ataque de este tipo puede dar acceso a alguien y sin ningún tipo de restricción a una base de datos completa e incluso copiar o modificar la información.
Malware y spear phising.	Se trata de una técnica combinada que usan los cibercriminales, hackers patr ocinados por estados o espías para penetrar en las organizaciones y robar sus datos confidenciales.
Auditorías débiles.	No recopilar registros de auditoría detallados puede llegar a representar un riesgo muy serio para la organización en muchos niveles.
Exposición de los medios de almacenamie nto para backup.	Éstos están a menudo desprotegidos, por lo que numerosas violaciones de seguridad han conllevado el robo de discos y de cintas. Además, el no auditar y

	monitorizar las actividades de acceso de bajo nivel por parte de los administradores sobre la información confidencial puede poner en riesgo los datos.

[Fuente: http://www.ticbeat.com/tecnologias/10-grandes-amenazas-seguridad-bases-datos/]

Por otro lado el 70% son vulneraciones internas las cuales se debe a errores de desarrollo donde se deja puerta abiertas, que estas pueden ser intencionados o no, el 15% son descuidos de los usuarios donde se revela la clave de accesos de gestores de bases de datos o aplicaciones, el 15% son realizados por deshonestidad de los usuarios para favorecer a sus intereses.

Por otra parte los ataques externos son el 30% y de este porcentaje se establece que el 50% es porque la seguridad física, es decir no se ha establecido de manera correcta la configuración del hardware o del software, y el otro 50% son ataques remotos, que realizan los hackers, etc.

En sentido los ataques que sufren estos repositorios de base de datos se clasifican:

- Externos: Los que se realizan desde fuera del perímetro de seguridad.
- Internos: es decir dentro la red, los empleados descontentos, terceros dentro de la organización.

Que se resume en la siguiente tabla

Tabla 1.2 Porcentajes de intrusos en contra de las empresas

Tipos de Intrusos	Porcentaje
Internos	70%
Externos	30%

Fuente : [Julio Ardita, CYBSEC S.A]

También se muestra el análisis de la empresa Recovery Labs sobre fraudes los informáticos en el siguiente cuadro.

Cuadro 1.1 Estadísticas de Fraudes informáticos

-Un 46.71% son delitos informáticos como la falsificación o fraude informático mediante la introducción, borrado o supresión de datos informáticos, o la interferencia en sistemas informáticos. -Un 43.11% son delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos. Dentro de esta categoría las conductas que más se repiten son con un 63.89% delitos relacionados con el acceso ilícito a sistemas informáticos, y con un 36.11% todas aquellas conductas delictivas relativas a la interferencia en el funcionamiento de un sistema informático. -Un 10.18% son delitos relacionados con el contenido, como la producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

Fuente
[http://www.delitosinformaticos.info/peritaje_informatico/estadisticas.html, 2012]

Analizando estos porcentajes se observa que el 89.82%, se afecta a los datos, que son accedidos de manera ilegal produciendo vulneración a la base de datos haciendo que la información no sea confiable e integra.

Como consecuencia de estos accesos no autorizados ya sean internas o externas las cuales están motivados por diversos factores como ser:

- Robo de información por para la venta.
- Espionaje dirigido a la propiedad intelectual como diseño de nuevos productos, algoritmos, planes estratégicos,

Por lo expuesto anteriormente el problema de la presente investigación de accesos no autorizados a los repositorios de bases de datos son frecuentas que las mismas son vulneradas haciendo que la base de datos pierda la confidencialidad, integridad y la disponibilidad.

III. PREGUNTA DE INVESTIGACIÓN.

A partir del análisis de la problemática se llega a la siguiente pregunta de investigación.

¿Cómo percibir, evaluar y alertar ex-antes sucesos de vulneración en los repositorios de bases de datos de alerta temprana ante los hechos delictivos?

IV. OBJETIVO GENERAL Y OBJETIVOS ESPECIFICOS.

Todo trabajo de investigación cuenta con objetivos que se desea alcanzar ya sea un corto o largo plazo según las características del problema a resolver, es así que se plantea el siguiente objetivo general y objetivo específico, y para alcanzar dicho objetivos se tomara en cuenta diversas tecnologías entre las cuales podemos mencionar a los patrones de software, la inteligencia artificial, la ingeniería se software , los algoritmos de razonamiento el cual estará con estrecha relación con la base de conocimiento, la simbiosis de esta tecnología dará a lugar un producto que sirva a las organizaciones para mejorar y precautelar la seguridad de la información y así mantener la integridad, disponibilidad y la confidencialidad de los datos,

Plantear un modelo de sistema multi-agente para percibir, evaluar y alertar de forma temprana de accesos no autorizados a repositorios de base de datos, para mantener la integridad, confidencialidad y disponibilidad de la información y los datos

OBJETIVOS ESPECÍFICOS.

1. Utilizar algoritmos de razonamiento en los subsistemas de agentes inteligentes (agente que percibe, agente que evalúa, agente que alerta y agente coordinador), que permita alertar de forma temprana las vulneraciones a los repositorios de base de datos.
2. Establecer la base de conocimiento, basado en patrones de software para los sub-sistemas de agentes inteligentes.
3. Aplicar la metodología tropos para la formalización de la estructura del sistema multi-agente y los sub-sistemas de agentes de inteligentes.
4. Construir un prototipo del sistema multi-agente que sea una herramienta para percibir, evaluar y alertar en el acceso no autorizados a repositorios de bases de datos, para mantener la integridad, confidencialidad y disponibilidad de los datos.

V. HIPÓTESIS

Todo trabajo de investigación formal cuenta con una hipótesis el cual deber ser demostrada, en el caso particular de la presente investigación se desarrollara un prototipo de agentes inteligentes con el fin de verificar la validez de la investigación, se tomara como caso de estudio una base de datos académica, la cual se intentara vulnerar y los agentes deben responde de manera oportuna ante la vulneración.

Por lo que se establece la siguiente hipótesis.

El modelo de sistema multi-agente para percibir, evaluar y alertar accesos no autorizados en los repositorios de bases de datos, mejora la detección de forma temprana y oportuna ante las vulneraciones.

Variable Dependiente

Modelo de sistema multi-agente.

Variable Independiente

Vulneración a los repositorios de bases de datos.

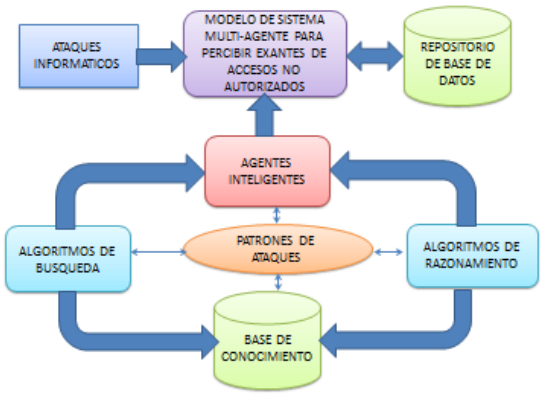
Variable Interviniente

Agentes Inteligentes y patrones.

VI. ESQUEMA DE SOLUCIÓN

Una vez establecido la problemática, los objetivos y la respectiva hipótesis, se muestra el esquema de modelo para percibir, evaluar y alertar ex-antes la detección de vulnerabilidades a los repositorios de base de datos, y con esto alertar de forma temprana a los administradores de bases de datos y de sistemas que puedan tomar las acciones correspondientes, en este contexto se presenta el esquema general del modelo sistema multi-agente que se muestra en la siguiente figura 1.1

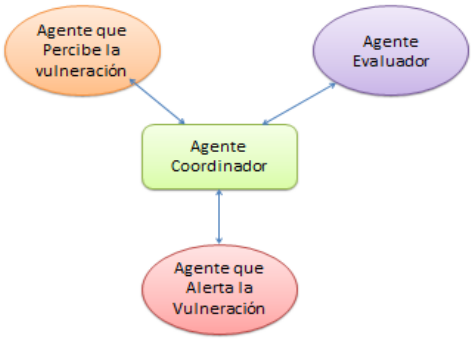
Fig. 1.1 Esquema del modelo sistema multi-agente



El esquema consiste en que el modelo sistema multi-agente en alertar las vulnerabilidades a los repositorios de base de datos, el sistema se compone de un conjunto de sub sistemas de agentes inteligentes, las cuales interactúan y realizan tareas enfocadas en percibir, evaluar y alertar ex-antes ante un hecho de vulneración y de esta manera conserva la confidencialidad, integridad y disponibilidad. Para esto, se cuenta con un agente encargado de percibir las vulnerabilidades, otro agente de evaluar qué tipo de acceso no autorizado si es interno o externo y por último, un agente que proporcione una alerta temprana para tomar las acciones correspondientes, en esto habrá un agente coordinador el cual estará relacionado con tres agentes. A continuación se describe a detalle cada uno de estos agentes:

Agente Coordinador. Es el agente encargado de coordinar a los agentes que intervienen en el sistema. Además determina el tipo de vulnerabilidad para esto, el agente coordinador analiza la vulnerabilidad y como se muestra en la figura 1.2.

Figura 1.2. Sub sistemas de agentes inteligentes



Agente que percibe la vulneración. Este agente será el encargado de percibir la vulneración a los repositorios de base de datos, el cual pasara información al agente evaluador.

Agente evaluador, este agente se encargara de evaluador el nivel de vulneración, el tipo de vulneración que se pretende realizar por el tipo de intruso interno o externo.

Agente de alerta. Este agente en función a la evaluación que realizo el agente evaluador, esta alertara de manera temprana a los administradores de bases de datos y de sistemas para puedan tomar acciones correspondientes sobre estas vulneraciones.

Todos estos agentes interactuaran de forma directa con una base de conocimiento donde en esta base, toda la información sobre las diferentes vulneraciones que se realiza a los repositorios de bases de datos.

Los patrones[5]. Un patrón de diseño es una descripción para resolver un problema de diseño general en un contexto particular. En nuestro caso se aplica estos patrones porque existen características comunes de vulneración a los repositorios de bases de datos, de tal forma que estos que estos elementos comunes se establezcan como patrones que simplifique la base de conocimiento y la búsqueda de solución sea efectiva.

La base de conocimiento. Para realizar la representación de conocimiento se empleara los Frames, donde se establecerá las características de vulneración y se definirán los patrones más frecuentes de vulneración y sobre los algoritmos de razonamiento con la cuentan los agentes inteligentes podrán percibir y evaluar cuando se produzca una vulneración.

VII. MARCO TEÓRICO.

Para comprender mejor el trabajo se establecerá la teoría base para la elaboración del modelo multi-agente.

La Tecnología de Agentes y Sistemas Multi-Agente[6]. La teoría de agentes surge como una evolución de la inteligencia artificial distribuida (Russel y Norvig, 1995). La evolución del software, y más concretamente del software que incorpora elementos de la inteligencia artificial, tiende a la creación de entidades con comportamientos y conductas similares a las de los humanos. En definitiva, los agentes son capaces de tomar decisiones, reaccionar ante estímulos externos, cambiar su propio comportamiento y adaptarse a las necesidades del entorno. Por otra parte, un sistema multi-agente se define como cualquier sistema compuesto de múltiples agentes autónomos con capacidades incompletas para resolver un problema global, en donde no existe un sistema de control global, los datos son descentralizados y la computación es asíncrona[8] (Wooldridge, 2002), (Mas, 2005)

Concepto de Agente Se define un agente como un sistema computacional que se sitúa en algún entorno y es capaz de actuar de forma autónoma en dicho entorno para alcanzar sus objetivos de diseño (Wooldridge, 2002).

Características de los agentes

Las características que un programa debe poseer para ser considerado un agente inteligente son:

Inteligencia: Rodearse de conocimiento (creencias, deseos, intenciones y metas). Aprendizaje.

Habilidad de adaptarse progresivamente a cambios en entornos dinámicos, mediante técnicas de aprendizaje.

Reactividad. Percibir su entorno y actuar sobre éste con la capacidad de adaptarse a sus necesidades.

Pro-Actividad o Racionalidad. Tomar la iniciativa para definir metas y planes que les permitan alcanzar sus objetivos.

Movilidad: Capacidad para moverse de un sitio a otro.

Situación. Situarse dentro de un entorno, ya sea real o virtual.

Habilidad social. Interactuar con otros agentes, incluso con humanos.

Sistemas Multi-Agente. Una vez descritos los principales requisitos que debe cumplir un agente y las características de agentes, es necesario definir lo que es un sistema multi-agente (MAS, Multi-Agent System). Se considera un sistema multi-agente cuando dos o más agentes son capaces de trabajar de forma conjunta con el objetivo de resolver un problema (Mas, 2005). Dentro de la terminología de este campo es importante aclarar la diferencia entre un sistema basado en agentes y un sistema multi-agente . Un sistema basado en agentes, puede contener uno o más agentes (Corchado y Molina, 2002), pero solo utiliza el concepto de agente como mecanismo de abstracción, ya que a la hora de implementarlo no existe alguna estructura de software correspondiente a éstos. Contrario a un sistema multi-agente que debe cumplir una serie de condiciones (Wooldridge, 2002):

Al menos uno de los agentes debe de ser autónomo y debe existir al menos una relación entre dos agentes en la que se cumpla que uno de los agentes satisface el objetivos del otro. Esto quiere decir que al menos uno de los agentes dispone de información incompleta o de capacidades limitadas para resolver el problema.

Los sistemas multi-agente se caracterizan porque no existe un sistema control global y porque cada agente se centra en su conducta individual.

Por otro lado, los datos se encuentran organizados de forma distribuida (descentralizado), lo que favorece su computación asíncrona.

Cada agente puede decidir con libertad, dinámicamente, que tareas debe efectuar y a quien asigna estas tareas

En un sistema multi-agente, los datos se encuentran organizados de forma distribuida y no existe un sistema de control global. De esta forma, cada agente se enfoca en su propia conducta, tomando la iniciativa guiado por sus objetivos y decidiendo dinámicamente las tareas que debe realizar o asignar a otros agentes. Por tal motivo, es necesario que los agentes trabajen de forma coordinada, principalmente a través de mecanismos de negociación, para alcanzar sus objetivos (Ossowski y García-Serrano, 1998).

Metodología Tropos Es una metodología de desarrollo orientada a agentes con larga trayectoria. La principal característica que le identifica respecto de otras alternativas, consiste en un mayor énfasis dirigido a la identificación y análisis de requisitos.

El desarrollo siguiendo Tropos se compone de cinco fases: análisis de requisitos iniciales, análisis de requisitos tardíos, diseño arquitectónico, diseño detallado, y finalmente la fase de implementación. Respecto a la fase de implementación, Tropos inicialmente no la contemplaba como una fase de su desarrollo.

Durante el análisis requisitos iniciales, se busca identificar el ámbito en el cual el sistema debe funcionar, en términos de qué interesados relevantes se consideran dentro del dominio y qué relaciones existen entre ellos. Para hacer esto, Tropos considera dos diagramas: de actores y de justificación. El diagrama de actores, plasma a los interesados identificados (que serán los actores) con sus relaciones (que se muestran en términos de dependencias). La representación utilizada consiste en un grafo dirigido donde los nodos son actores, considerando el nodo origen como el actor dependiente y el nodo destino como el dependiente. La arista toma el papel de la dependencia concreta que existe entre ellos, y según su tipo (objetivos, tareas, recursos), modifica la arista con un icono intermedio.

La siguiente fase (análisis de requisitos tardíos) repite lo visto anteriormente, considerando al sistema que se pretende construir como un nuevo actor, y utilizando los mismos diagramas. De esta forma se identifican los requisitos funcionales y no funcionales del sistema, describiendo al sistema dentro del entorno donde se pretende desplegar.

El diseño arquitectónico, configura la estructura de la organización del sistema a través de su descomposición en subsistemas relacionados mediante dependencias. Esta fase se desarrolla en tres etapas: definición de la estructura general del sistema, especificación de las capacidades disponibles para cada autor y la definición de tipos de agentes, a quienes se les asignan las capacidades identificadas.

Para definir la estructura general del sistema, se considera el uso de diferentes estilos, que se utilizan a modo de patrones. Estos estilos se definen mediante una meta clase que, a partir de unos parámetros de diseño, presenta su asignación de objetivos y procesos. la fase de diseño detallado consiste en aumentar el nivel de detalle respecto a los componentes que se han identificado en la fase anterior. Esto incluye definir los protocolos que guiarán las comunicaciones que se han encontrado durante el diseño. Para dar soporte en esta fase, Tropos propone diferentes patrones sociales, que presentan situaciones comunes de interacción. Los patrones sociales se dividen en dos categorías, según la naturaleza de la interacción: pareja o mediación. Los patrones de pareja representan interacciones donde un actor se comunica con uno o más actores adicionales en una comunicación de par a par. Un patrón de pareja que considera más de dos actores, tendrá un actor que tiene una misma interacción con más de un actor (como puede ser una subasta). Los patrones de mediación representan situaciones donde es necesario un intermediario, siendo el propósito de la interacción satisfacer las necesidades de los otros actores.

Durante la fase de implementación, se consideran actividades para guiar el traslado del diseño al código de la manera más natural posible, haciendo corresponder las propiedades de la plataforma de agentes objetivo con la semántica del diseño.

VIII. CONCLUSIONES

Presentamos un modelo de un sistema multi-agente que permite integrar cuatro sub-sistemas de agentes inteligentes con diferentes funcionalidades asociadas a percibir, evaluar y alertar de forma temprana ante las vulneraciones a los repositorios de bases de datos y que a la vez variara de forma dinámica según los tipos de vulneraciones ya sean internos o externos.

Los agentes inteligentes utilizaran algoritmos de razonamiento con patrones de software las cuales acceden a una base de conocimiento, dicho modelo percibirá las vulneraciones desde los diferentes puntos de acceso.

La unión de diferentes tecnologías como ser los sistemas multi-agentes, los agentes inteligentes, los patrones de software, ingeniería de software, la base de conocimiento permite obtener un producto que une los mejor de cada uno. Estos beneficios serán reflejados en la alerta temprana de las vulneraciones a los repositorios de base de datos y así de esta forma podrán tomar las acciones necesarias los administradores de bases de datos y de sistemas.

REFERENCIAS

[1] Se entiende por repositorio: Un deposito o archivo es un sitio centralizado donde se almacena y mantiene información digital, habitualmente base de datos, o archivos informática: Fuente [http://es.slideshare.net/YOSMAR0508/repositorio-de-datos]

[2]http://www.ais.com.mx/alianzas/guardium/3_Proteccion_contra_ataques.pdf]

[3]: [Fuente: https://docs.google.com/presentation/d/1qD6-m8E2C4UEsILmE9tZBbxBYq4L7kBY-GMoZ1OfNFI/edit#slide=id.i29].

[4]. [Fuente: http://www.ticbeat.com/ tecnologias/ 10-grandes-amenazas-seguridad-bases-datos].

[5]Desing Patterns. E. Gamma, R. Helm, R. Johnson, and J. Vlissides. Design Patterns. Addison Wesley, 1995.

[6] J. Gómez-Sanz, 2002, Metodología de Desarrollo de Sistemas Multiagente (Ph.D. Tesis). Universidad Complutense de Madrid.

[7]. Lucero, 2013, Modelo de seguridad multi-agente para la detección de fraudes en correos electrónicos, Tesis de licenciatura,Universidad de Sonora.

[8]Wooldridge, 2002, Wooldridge, M. (2002). Introduction to MultiAgent Systems: John Wiley & Sons.

[9] Wooldridge y Jennings, 1995) Wooldridge, M., Jennings, N. R. (1995). Intelligent Agents: Theory and Practice. Knowledge Engineering Review.