Modelo de Seguridad y protección en sistemas de información aplicando sistemas multi-agentes para las PYMES

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

***Resumen*—Se presenta la propuesta de un Modelo de Seguridad y protección en sistemas de información aplicando sistemas multi-agentes para PYMES. Donde los agentes inteligentes harán uso de reglas de razonamiento, que están almacenados en una base de conocimiento bajo un patrón de vulnerabilidades basados en el TOP 10 de OWASP. Dichos agentes se ejecutarán en un servidor proxy inverso, de esta manera evitar vulneraciones y al mismo tiempo alertar a los administradores de base de datos y de sistemas de información web oportunamente y así tomar las acciones correspondientes.**

Palabras clave—Multi-agente, agentes inteligentes, base de datos, sistemas web, diseño de patrones, vulnerabilidades, OWASP.

I. INTRODUCCIÓN

Actualmente la informática y las redes de datos han evolucionado y mejorado la productividad de muchas organizaciones, desarrollando e implementado diferentes aplicaciones informáticas, en ambientes locales y/o en entornos web, las mismas acceden a bases datos, donde almacenan información de procesos y de servicios de diferentes áreas de la organización, toda esta información se convierte en activos informáticos de mucho valor.

Al implementar los sistemas informáticos, los riesgos de vulneración han incrementado con accesos no autorizados a las bases de datos y a los sistemas informáticos; estos accesos pueden ser de manera interna y/o externa, realizados desde diferentes puntos de acceso, aspecto que facilita vulnerar, provocando un daño al patrimonio de la organización por la pérdida de información y/o equipos, además de afectar negativamente la eficiencia y la efectividad de los procesos de la organización.

Ante estos riesgos y vulneraciones se requieren que los mecanismos de seguridad sean cada vez más sofisticados, que eviten los accesos no autorizados a los sistemas de información y a la base de datos, manteniendo la integridad, la disponibilidad, la confidencialidad, la consistencia y el control de la información, elementos primordiales para mantener la seguridad de la información. Por lo que es necesario adoptar nuevos mecanismos de seguridad en los sistemas informáticos, que esté acorde a los avances tecnológicos y si fuese necesario aplicar otras áreas de investigación tal como es la Inteligencia Artificial, agentes inteligentes, las mismas son herramientas teóricas y experimentales de las ciencias de computación; para estudiar el fenómeno del comportamiento inteligente y el desarrollo de sistemas multi-agentes, área que ha producido un cuerpo de principios, representaciones, algoritmos y nuevas avances tecnológicas, el cual ha realizado importantes aportes en diferentes áreas como ser: la medicina, sistemas cooperativos, robótica, sistemas operativos, comercio electrónico, internet, inteligencia gestión del conocimiento, seguridad de la información entre otros.

Con el fin de mejorar la seguridad en las empresas PYMES, el presente trabajo de investigación propone un Modelo de seguridad y protección en sistemas de información aplicando sistemas multi-agentes, de esta forma dar mayor seguridad y confidencialidad a la información con la que cuentan.

Para definir la problemática, se parte de la siguiente premisa, que en la actualidad la información es el activo más valioso de muchas organizaciones, las cuales son almacenadas en bases de datos, dicha información es el resultado del proceso de las tareas cotidianas que efectúan los sistemas de información. Toda esta infraestructura tecnológica de hardware y software está a disposición de la sociedad con una cantidad creciente de información de toda naturaleza, almacenadas en grandes bases de datos a través de los sistemas de información; en las más diversas esferas del conocimiento humano, científico, técnico, profesional y personal que están siendo incorporadas a los sistemas informáticos a la práctica cotidiana. Este tipo de innovaciones tecnológicas proporcionan grandes beneficios al mundo empresarial, que están sujetos a amenazas y riesgos, ocasionando diversos tipos de daños y vulneraciones, entre otros; a los que se les conoce como ataques informáticos o vulnerabilidades tecnológicas.

Ante esta problemática latente es importante que se continúen realizando investigaciones proponiendo nuevas alternativas de solución para detectar y evitar las vulneraciones a las bases de datos que cada vez son más sofisticadas. Frente a este crecimiento, también las vulneraciones se han incrementado, por lo que la seguridad de datos presenta un reto multidimensional donde los ambientes complejos incluyen una gran cantidad de sistemas para gestión de base de datos, las aplicaciones empresariales, plataformas de sistema operativo

Para referenciar este artículo (IEEE):

[N] A. Quisbert, «Modelo de Seguridad y protección en sistemas de información aplicando sistemas multi-agentes para las PYMES», *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 8, pp. 11-17, 2020.

con múltiples rutas de acceso y niveles de permiso heterogéneos que han generado un conjunto aparentemente interminable de escenarios de amenazas y vulneraciones a la seguridad.

Los mecanismos tradicionales de seguridad informática como son los firewalls y políticas de seguridad (normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le afectan), ya no son suficiente para las nuevas formas de ataque que sufren los sistemas de información y las bases de datos. los ciber-delincuentes rompen las barreras perimetrales de forma fácil. Según estadísticas las vulneraciones pueden ser: internas y/o externas, los porcentajes indica que el 70% son ataques internos y el 30% son ataques externos. Por otra parte, según el análisis estadístico de la empresa Recovery Labs, (2015) [1] sobre las vulneraciones a los sistemas informáticos y a los repositorios de base de datos, los resultados se muestran en la tabla 1.

TABLA I. ESTADÍSTICAS DE VULNERACIONES INFORMÁTICOS

Porcentaje	Detalle
46.71%	Son delitos informáticos como la falsificación o fraude informático mediante la introducción, borrado o supresión de datos, o la interferencia en sistemas informáticos.
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
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: (Recovery Labs 2015)

Considerando los porcentajes 46.71% y 43.11% se tiene un total de 89.82%, según el porcentaje obtenido, las vulneraciones afectan las bases de datos, que son accedidos de manera ilegal produciendo vulneración y haciendo que la información no sea confiable e integra. Lo que implica que estos accesos no autorizados, están motivadas por diversos factores como ser:

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

En este sentido algunas empresas han invertido mucho presupuesto en infraestructura tecnológica para proteger la información, sin embargo, las PYMES no han corrido la misma suerte de poder implementar estos mecanismos de seguridad, porque las mismas cuentan con recursos limitados, esto hace que los sistemas informáticos sean más vulnerables, y sean un blanco fácil para los ciber-delincuentes, a razón de esto con el fin de reducir las vulneraciones y no pierdan la confidencialidad, integridad y disponibilidad, se propone una alternativa de desarrollar un modelo de seguridad aplicando los agentes inteligentes para las PYMES.

II. MÉTODO

Para dar solución esta problemática latente sobre la seguridad informática, y tomar las acciones correspondientes, en las empresas PYMES se plantea un modelo de seguridad con sistema multi-agente, cuyo esquema se muestra en la figura 1.

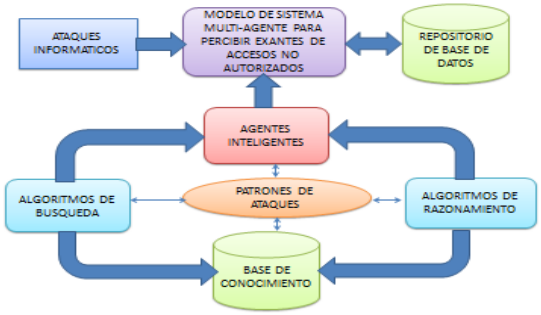

Fig. 1. Esquema del modelo de seguridad aplicando sistema multi-agente

El esquema consiste en alertar las diferentes vulnerabilidades OWASP, donde el modelo se compone de un conjunto de sub sistemas de agentes inteligentes, las cuales interactúan y realizan tareas enfocadas en percibir, evaluar y alertar ex-ante el hecho de vulneración y de esta manera conservar 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, un agente que proporcione alerta temprana para tomar acciones correspondientes, y un agente coordinador.

A. *Agente Coordinador*

Es el encargado de coordinar a los agentes que intervienen en el sistema. Determina el tipo de vulnerabilidad; para esto, el agente coordinador analiza la vulnerabilidad, ver figura 2.

Fig. 2. Sub sistemas de agentes inteligentes

B. *Agente que percibe la vulneración*

Este agente será el encargado de percibir la vulneración a los sistemas de informáticos y a la base de datos, el cual pasará información al agente evaluador.

C. *Agente evaluador*

Este agente se encargará de evaluar el nivel y tipo de vulneración que pretende realizar el intruso interno o externo.

D. *Agente que alerta la vulneración*

Está en función a la evaluación que realiza el agente evaluador, alertara de manera temprana a los administradores de bases de datos y de sistemas informáticos para puedan tomar acciones correspondientes sobre estas vulneraciones.

Todos estos agentes interactuaran de forma directa con una base de conocimiento que guarda información sobre las vulneraciones que se realizan a los repositorios bases de datos.

Los patrones. 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 [4].

La base de conocimiento. Donde almacenera información de las vulneraciones con todas las características de patrones establecidos y sobre esto los algoritmos de razonamiento conjuntamente con los agentes inteligentes podrán percibir y evaluar cuando se produzca una vulneración.

Agentes y Sistemas Multi-Agente [5]. La teoría de agentes surge como una evolución de la inteligencia artificial distribuida [6]. 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 [7].

Estos agentes inteligentes jugarán un papel importante en el modelo de seguridad, las mismas serán las encargadas directas de evitar las vulneraciones a los sistemas informáticos, los conjuntos de los agentes formarán el sistema Multi-Agente que estará organizado de forma sistemática, de esta forma, cada agente se enfoca en su propia conducta.

E. Vulneraciones según el TOP 10 de OWASP

Open Web Application Security Project, es un documento no oficial ni estándar donde se recopilan las vulnerabilidades más frecuentes y preocupantes por piratas informáticos, hay fallos de seguridad todos los años suponen una gran parte de los ataques informáticos a nivel mundial y, a pesar de ello, no se termina de desarrollar ninguna medida de seguridad que mitigue de forma definitiva. Estas vulnerabilidades que se repiten año tras año son los fallos de inyección de código y los problemas en las plataformas de autenticación [8].

En base al TOP 10 se realizarán los diferentes *Payloads* [9] que estarán almacenados en la base de conocimiento y así evitar los diferentes vectores de ataque [10] que realizan los piratas informáticos. Es importante reconocer que un vector de ataque podría estar conformado por más de una amenaza.

F. La metodología de desarrollo de la solución

Para la investigación de la propuesta del desarrollo del modelo de seguridad aplicando agentes inteligentes, se seguirá un conjunto de pasos de forma sistemática y metodológica, tal como se muestra en la figura 3.

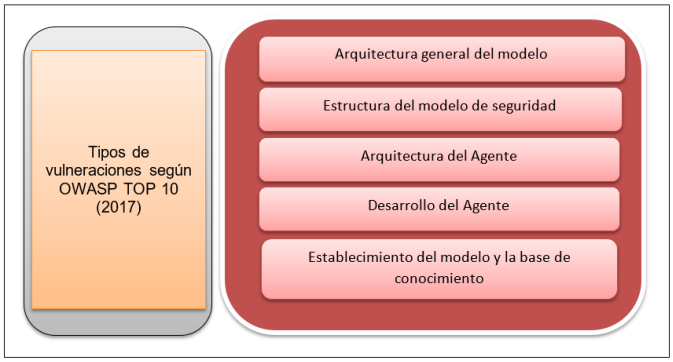

Fig. 3. Propuesta Metodológica de desarrollo

G. Tipos de Vulneraciones según OWASP TOP 10 (2017).

Las medianas y pequeñas empresas por los escasos recursos económicos con que cuentan no han logrado implementar estos mecanismos de seguridad para poder proteger la información con la que cuentan, que cada vez se vuelven más imperativos y necesarios para evitar las vulneraciones de los ataques informáticos, estas vulneraciones a las PYMES, han sufrido diferentes ataques tal como se muestra en la tabla 2.

TABLA II. PORCENTAJE DE ATAQUES Y APLICACIÓN DE SEGURIDAD

59%	Utilizo Seguridad web en 2014
48%	Utilizó seguridad web en 2015
43%	Ciberataques se concentran en las pymes en el año 2016

Fuente (Informe Anual de Cisco, 2016)

El modelo de seguridad se basa en el OWASP TOP 10 (2017), donde se considera las vulneraciones más frecuentes y comunes que sufre los sistemas de información y las bases de datos, esta lista de vulneraciones se muestra en la tabla 3.

TABLA III. TOP 10 RIESGOS DE SEGURIDAD EN LA WEB

Tipo	Descripción
A1	SQL Inyección
A2	Perdida de autenticación
A3	Exposición de datos sensibles
A4	XML Entidades externas
A5	Pérdida de control de acceso
A6	Configuración de seguridad incorrecta
A7	Referencia de sitios cruzados (XSS)
A8	Desacralización insegura
A9	Uso de componentes con vulnerabilidades conocidas
A10	Registro y monitoreo insuficiente.

Fuente: Owasp.org (2017)

H. Arquitectura general del modelo.

Para tener un mejor enfoque para el desarrollo del modelo de seguridad con agentes inteligentes se basará en la siguiente arquitectura que se muestra en la figura 4 que será el marco de trabajo que establece un conjunto de buenas prácticas para la elaboración del modelo.

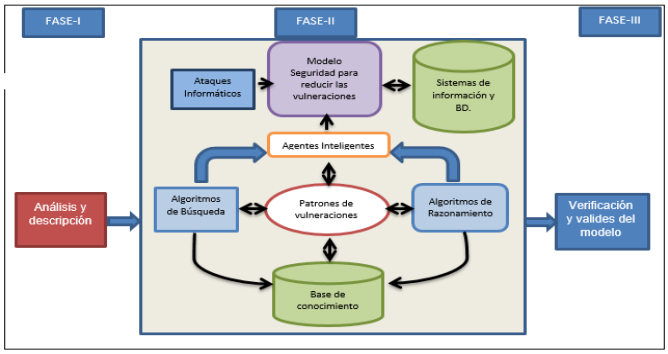

Fig. 4. Esquema general de la investigación

I. Descripción por fase.

Fase I: Análisis y descripción de las vulneraciones que sufre un sistema de información y las bases de datos, es decir, cuáles son las vulnerabilidades más frecuentes que existe en base al OWASP TOP10 (2017). Con toda esta información se desarrollará un modelo de seguridad para sistemas de información web, donde los agentes inteligentes juegan un papel importante para evitar las vulneraciones.

Fase II. Desarrollo del modelo: Una vez realizado todo el análisis y estudio pertinente sobre las vulneraciones, el siguiente

paso será el desarrollar el Modelo de Seguridad y Protección en Sistemas de información aplicando agentes inteligentes, estableciendo una base de conocimiento, los algoritmos razonamiento de los agentes y el motor de inferencia, el cual reducirá las vulneraciones, alertando de forma oportuna a los administradores de sistemas de información y bases de datos.

Fase III. En esta fase se realizará la respectiva validación del modelo de seguridad, tomando como punto de partida el prototipo, el mismo que se implementará en un servidor NginX, con todo esto, se tomará una muestra simple seleccionando 10 empresas con sitios web, que será configurado en el servidor, por otra parte, se utilizará la aplicación DVWA (Damn Vulnerable Web Application), con esto verificaremos que los agentes inteligentes realizan el trabajo de evitar y reducir las vulneraciones más frecuentes.

J. Modelo de arquitectura de los agentes

La arquitectura de los agentes que se plantea para el modelo de seguridad, está asociado a un conjunto de agentes inteligentes que interactúan entre sí, con miras a conseguir el objetivo, la misma que se muestra en la Figura 5, donde se especifican los diferentes componentes que interactúan en el sistema para conseguir el fin, todo esto alimentado con una base de conocimiento, el cual evitará vulneraciones de los ataques.

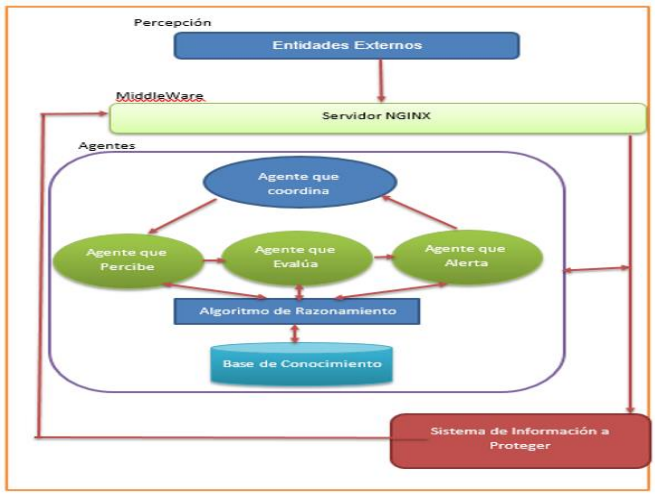

Fig. 5. Modelo de arquitectura de los agentes

La arquitectura de agentes será deliberativo, que se inicia con una percepción, que en este caso serán los entes externos que intentan vulnerar los sistemas de información web y las bases de datos, dentro de la arquitectura existe una parte intermedia (middleware), que será el servidor NginX, donde se instalaran los agentes inteligentes y actuaran para evitar las vulneraciones de acuerdo al OWASP TOP 10 (2017), y la acción inmediata será el de proteger el sistema de información y las bases de datos. A partir de este esta arquitectura se tiene la siguiente función general matemática que se detalla a continuación.

$$\text{Modelo de seguridad} = G(\ F(TV),\ FA(PR,BC,AR))$$

Donde:
- F,FA : son funciones
- G : Middleware (servidor NginX)
- TV : Tipos de vulneraciones
- PR : Programas
- BC : Base de Conocimiento
- AR : Algoritmos de Razonamiento.

La base de conocimiento que se convirtió en una lista de Payloads se detalla en la tabla 4.

TABLA IV. BASE DE CONOCIMIENTO

/*	mysql comment (/*)	BODY|URL | ARGS | $ HEADERS_VAR:Cookie	$SQL:8
***/**	msg:mysql comment (*/)	BODY|URL| ARGS | $ HEADERS_ VAR: Cookie	$SQL:8
|	mysql keyword (|)	BODY|URL |ARGS |$ HEADERS_VAR: Cookie	$SQL :8"
&&	mysql keyword (&&)	BODY|URL |ARGS |$ HEADERS_VAR:Cookie	$SQL :8"
--	mysql comment (--)	BODY|URL| ARGS |$ HEADERS_VAR:Cookie	$SQL :4
	Semicolon	BODY|URL |ARGS	$SQL :4, $XSS: 8
=	equal sign in var	probable sql/ xss ARGS|BODY	$SQL :2
(	open parenthesis	probable sql/xss ARGS|URL | BODY |$ HEADERS_VAR:Cookie	$SQL: 4$ XSS:8
)	close parenthesis	probable sql/xss ARGS|URL| BODY |$ HEADERS_VAR:Cookie	$SQL :4$ XSS:8
'	simple quote	ARGS|BODY |URL|$ HEADERS_VAR:Cookie	$SQL :4,$ XSS:8
,	double arobase (@@)	BODY|URL | ARGS|$ HEADERS_VAR:Cookie	$SQL:4"
#	mysql comment (#)	BODY|URL | ARGS|$ HEADERS_VAR:Cookie	$SQL:4
@@	double arobase (@@)	BODY|URL| ARGS|$ HEADERS_VAR:Cookie	$SQL:4
http://	http:// scheme	ARGS|BODY |$ HEADERS_VAR:Cookie	$RFI:8
https://	https:// scheme	ARGS|BODY|$ HEADERS_VAR:Cookie	$RFI:8
ftp://	ftp:// scheme	ARGS| BODY |$ HEADERS_VAR:Cookie	$RFI:8
php://	php:// scheme	ARGS|BODY| $ HEADERS_VAR:Cookie	$RFI:8
sftp://	sftp:// scheme	ARGS|BODY| $ HEADERS_VAR:Cookie	$RFI:8
zlib://	zlib:// scheme	ARGS|BODY |$ HEADERS_VAR:Cookie	$RFI:8
data://	data:// scheme	ARGS|BODY |$ HEADERS_VAR:Cookie	$RFI:8
glob://	glob:// scheme	ARGS|BODY |$ HEADERS_VAR:Cookie	$RFI:8
phar://	phar:// scheme	ARGS|BODY |$ HEADERS_VAR:Cookie	$RFI:8
file://	file:// scheme	ARGS|BODY |$ HEADERS_VAR:Cookie	$RFI:8
gopher://	gopher:// scheme	ARGS|BODY |$ HEADERS_VAR:Cookie	$RFI:8
..	double dot	ARGS|URL| BODY |$ HEADERS_VAR:Cookie	$TRAV ERSAL : 4
/etc/ passwd	obvious probe	ARGS|URL| BODY |$ HEADERS_VAR:Cookie	$TRAV ERSAL : 4
c:	obvious windows path	ARGS|URL| BODY |$ HEADERS_VAR:Cookie	$TRAV ERSAL : 4
cmd.exe	obvious probe	ARGS|URL| BODY |$ HEADERS_VAR:Cookie	$TRAV ERSAL : 4
****	Backslash	ARGS|URL |BODY |$ HEADERS_VAR:Cookie	$TRAV ERSAL : 4
<	html open tag	ARGS|URL |BODY |$ HEADERS_VAR:Cookie	$XSS:8
>	html close tag	ARGS|URL |BODY |$ HEADERS_VAR:Cookie	$XSS:8
[	open square backet ([)	possible js BODY| URL |ARGS|$ HEADERS_VAR:Cookie	$XSS:4
]	close square bracket (])	possible js BODY | URL |ARGS|$ HEADERS_VAR:Cookie	$XSS:4
~	tilde (~) character	BODY|URL | ARGS|$ HEADERS_VAR:Cookie	$XSS:4
`	grave accent (`)	ARGS|URL | BODY|$ HEADERS_VAR:Cookie	$XSS:8
&#	utf7/8 encoding	ARGS|BODY | URL|$ HEADERS_VAR:Cookie	$EVADE: 4
%U	M$ encoding	ARGS|BODY |URL|$ HEADERS_VAR:Cookie	$EVADE: 4

III. RESULTADOS

En función de la Figura 6 Esquema del modelo sistema multi-agente, se ha desarrollado un prototipo para comprobar el modelo, con las respectivas pruebas, el desarrollo se ha efectuado en dos fases: primero el desarrollo de agentes inteligentes que interactuaran con la base de conocimiento, la

segunda fase es la implementación y configuración del servidor NginX, ver Figura 6.

Fig. 6. Contenido del prototipo de Modelo de seguridad

A partir del anterior esquema se implementó el modelo de seguridad, bajo una arquitectura, que se muestra en la Figura 7; es decir, cualquier usuario que quiera acceder al sistema de información y a las bases de datos, deberán de pasar por el servidor NginX, el cual será una pasarela, donde se encuentra los programas desarrollados sobre los agentes inteligentes, las mismas que detectaran las diferentes vulneraciones de acuerdo al top 10 de OWASP.

Fig. 7. Arquitectura del modelo de seguridad

A partir de esta arquitectura, se configuró el servidor NGINX, el cual es un servidor HTTP libre, de código abierto, con un proxy inverso, así como un servidor proxy IMAP / POP3. NGINX es mejor conocido por su alto rendimiento, estabilidad, conjunto de características ricas, configuración sencilla y bajo consumo de recursos, NGINX maneja eficientemente las tareas que podrían ralentizar su servidor web. Los sitios dinámicos, construidos utilizando desde Node.js a PHP, suelen utilizar NGINX como caché de contenido y proxy inverso para reducir la carga en los servidores de aplicaciones, toda esta arquitectura se muestra en la Figura 8.

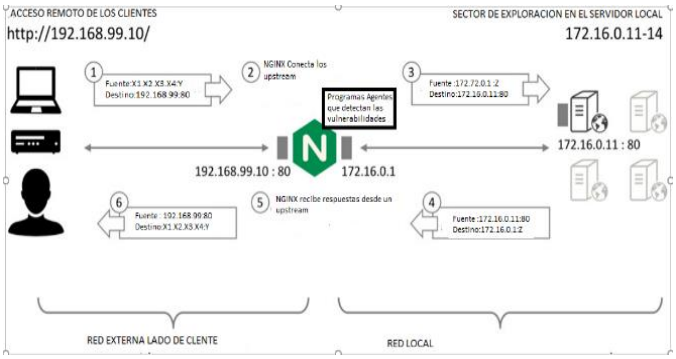

Fig. 8. Arquitectura del servidor NGINX

Una vez implementado los agentes en servidor NGINX, se implementó el prototipo que se muestra en la Figura Nro. 9

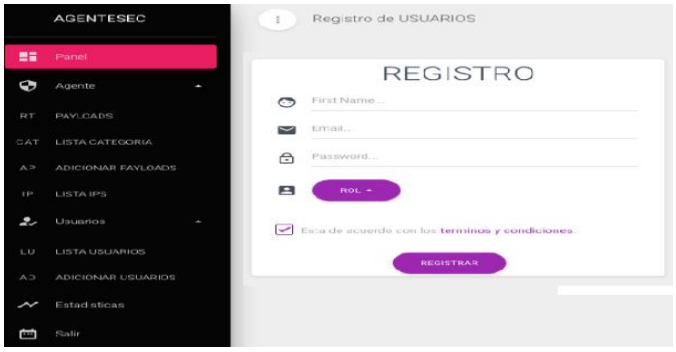

Fig. 9. Pantalla del prototipo

Con el fin de validar el modelo de seguridad se implementó un prototipo que funciona con una base de conocimiento que esta descrito en la tabla 3 a partir de esto se realizó pruebas y se diseñó los instrumentos necesarios que permiten medir el impacto del modelo y del prototipo elaborado, siendo los siguientes elementos que se consideran a continuación:

- La infraestructura del servidor NginX es adecuada.
- Base de conocimiento actualizado.
- Mejoramiento de la seguridad en las PYMES.
- efectividad de la herramienta
- Uso y utilidad: desempeño, variedad de reportes, facilidad toma de decisiones.

Para realizar validación mediante el prototipo se realizó pruebas de vulneración a los siguientes sitios web, ver tabla 5.

TABLA V. LISTA DE SITIOS WEB

Nro.	Descripción del sitio web
Emp.1	www.zaraeli.com
Emp.2	www.itrational.com
Emp.3	www.insdustrailmurillo.edu.bo
Emp.4	www.itso.es
Emp.5	www.industria.gnb.com.bo
Emp.6	www.cense.edu.bo
Emp.7	www.feyalegria.org
Emp.8	190.129.72.239
Emp.9	www.adrianquisbertvilela.com

Se elabora un cuestionario, el cual permite obtener información sobre la percepción del modelo de seguridad que se aplica a las empresas de la tabla 5; las preguntas del cuestionario de acuerdo a la funcionalidad y considerando el impacto que tiene en la protección de la información ante diferentes vulneraciones se ven en la tabla 6.

TABLA VI. PREGUNTAS DEL CUESTIONARIO

Variable	Descripción de la pregunta
A1	Alguna vez ha sufrido una vulneración a su sistema de información web
A2	La herramienta de seguridad es útil
A3	La herramienta de seguridad es eficiente
A4	La herramienta es accesible respecto al costo
A5	La herramienta satisface necesidades respecto a la seguridad del sistema de información
A6	Que tipos de ataque sufrió
A7	En cuanto aumento el nivel de confianza con aplicación de la herramienta
A8	Con la herramienta ha sufrido alguna vulneración.
A9	La herramienta detecta oportunamente las vulneraciones
A10	La herramienta redujo las vulneraciones

El resultado de la encuesta se despliega a continuación.

Pregunta 1. Alguna vez ha sufrido una vulneración a su sistema de información web.

Si	No	Total
6	4	10

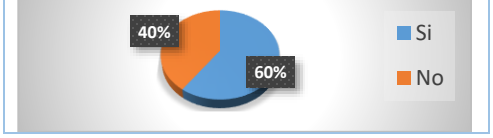

Fig. 10. Pregunta 1

Pregunta 2. Con la herramienta ha sufrido alguna vulneración.

Si	No	Total
2	8	10

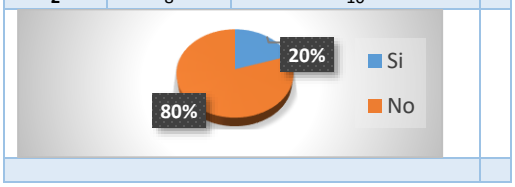

Fig. 11. Pregunta 2

Pregunta 3. Que tipos de ataque sufrió.

a	b	C	D	E
Sql Inyection	XSS	RFI	Trasnversal	Evade
6	2	1	0	0

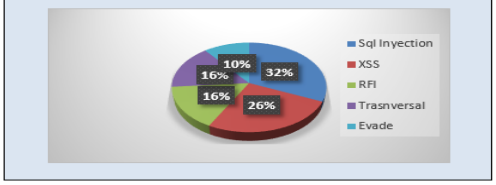

Fig. 12. Pregunta 3

Pregunta 4. La herramienta detecta oportunamente las vulneraciones.

Si	No	Total
9	1	10

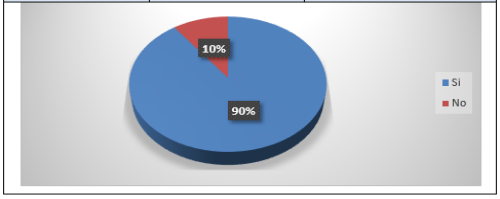

Fig. 13. Pregunta 4

Pregunta 5. En cuanto aumento el nivel de confianza con aplicación de la herramienta.

0%-20%	21%-40%	41%-60%	61%-80%	81%-100%
Muy bajo	Bajo	Medio	Alto	Muy Alto
1	1	2	6	0

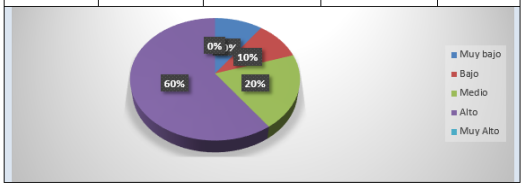

Fig. 14. Pregunta 5

Pregunta 6. La herramienta de seguridad es eficiente.

1	2	3	4	5
Malo	regular	Bueno	Muy bueno	optimo
0	0	40%	60%	0

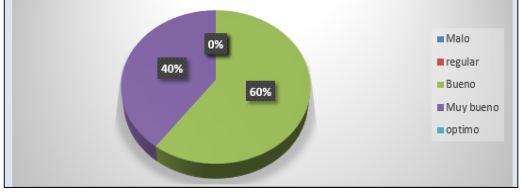

Fig. 15. Pregunta 6

Pregunta 7. La herramienta de seguridad es útil.

1	2	3	4	5
Malo	regular	Bueno	Muy bueno	optimo
0	0	2	8	0

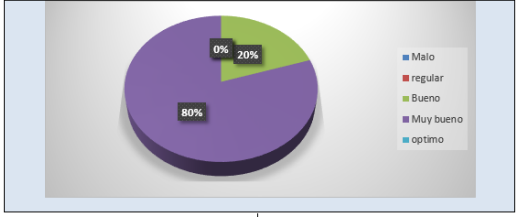

Fig. 16. Pregunta 7

Pregunta 8. La herramienta redujo las vulneraciones.

Si	No	Total
9	1	10

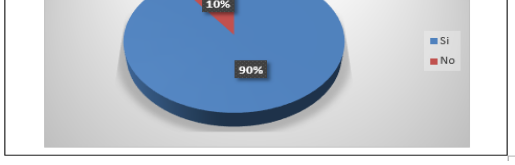

Fig. 17. Pregunta 8

Pregunta 9 La herramienta satisface necesidades respecto a la seguridad del sistema de información.

1	2	3	4	5
Malo	regular	Bueno	Muy bueno	optimo
0	1	6	3	0

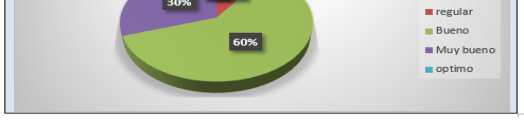

Fig. 18. Pregunta 9

Pregunta 10 La herramienta es accesible respecto al costo.

Si	No	Total
8	2	10

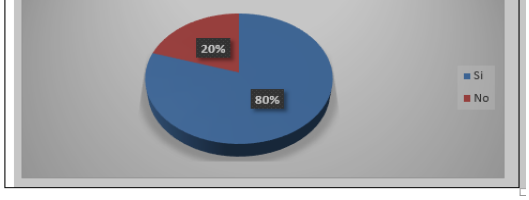

Fig. 19. Pregunta 10

A. Análisis de resultados

El análisis del modelo de seguridad, se efectúa mediante los resultados del cuestionario, en la siguiente tabla 7.

TABLA VII. ANÁLISIS DE RESULTADOS

Indicadores	Preguntas	Escala de valoración
Tipos de vulneraciones a los sistemas de información	Alguna vez ha sufrido una vulneración a su sistema de información web	Los resultados de la encuesta indican que el 55% si han sufrido por lo menos una vulneración al sistema de información con la que cuenta, esto se puede contrastar con los datos obtenidos que 43% han sufrido algún tipo de ataque (ver tabla 4.1 pág. 62), y un 45% no han sufrido ningún tipo de ataques, eso nos indica que el modelo propuesto es necesario para poder proteger la información.
Vulneraciones Frecuentes	Con la herramienta ha sufrido alguna vulneración.	Para poder verificar esta pregunta se hizo pruebas donde se configura las páginas de las empresas, para luego vulnerar, se utilizó la herramienta DWVA que se configuro también el servidor de NginX, resultado de esto, se tuvo que un 80%, no ha sufrido vulneraciones, por lo tanto, se pude concluir que el modelo es eficiente, también esto se puede contrastar que un 53%, que si utiliza mecanismos de seguridad, en contraparte el 20% si ha sufrido vulneraciones, esto sirvió también para mejorar el modelo para hacerlo más efectivo.
El modelo que tipos de vulneraciones detecta	Que tipos de ataque sufrió	El modelo considera 5 tipos de ataques que se tomó del top 10 2017 como referencia de vulneraciones, el resultado la vulneración más frecuentes es el sql Injection con 67%, el resultado es alto por que los sistemas de información web la mayoría cuentan con una base de datos, la segunda vulneración es el XSS, con un 22%, esto se debe a que las páginas web utilizan en front-end java scripts, en la vulneración RFI es el 11%, para obtener, estos resultados se realizó las vulneraciones con la herramienta DWVA
En cuanto incrementa la seguridad con el modelo	La herramienta detecta oportunamente las vulneraciones	Tras realizar las pruebas con la herramienta DWVA, si hicieron varias vulneraciones, el resultado de esta pregunta nos muestra que en un 90% el modelo es aceptable y cumple el objetivo, en un 10% no detecta oportunamente, esto se debe a que existen nuevos payloads para realizar vulneraciones.
	En cuanto aumento el nivel de confianza con aplicación de la herramienta	Antes de implementar el modelo el nivel de confianza era bajo, luego de aplicar el modelo tiene un nivel de confianza del 60% como muy bueno y 20% como bueno. Esto nos indica que el modelo tiene un grado de aceptabilidad.
En cuanto reduce las vulneraciones de las empresas	la herramienta de seguridad es eficiente.	La herramienta es eficiente y tiene una aceptación como muy bueno con un 60% de eficiencia, lo que implica si se la herramienta se empieza a utilizar tendría una aceptación muy buena. El 40% lo cataloga como bueno, pero sumando los dos se tendría una aceptación del 100%.
	La herramienta de seguridad es útil	Referente sobre la utilidad de la herramienta, como resultado se tuvo que en un 80% es muy bueno y 20% como bueno, sin embargo, se considera que en un 100% la herramienta es útil
	La herramienta redujo las vulneraciones	Con el uso de la herramienta se redujo las vulneraciones en un 90% lo que significa que la herramienta, permite reducir.
El modelo reduce los costos de seguridad	La herramienta satisface necesidades respecto a la seguridad del sistema de información	En este punto se tiene un resultado de satisfacción del 30% como muy buena y un 60% como buena, sin la suma de ambos resultados no da un 90% de satisfacción.
	La herramienta es accesible respecto al costo	Como la herramienta está dirigida para aquellas empresas cuya economía es baja, la aceptación es alta con un 90% de aceptación de uso de la herramienta.

IV. CONCLUSIONES

Al finalizar el presente trabajo y tras la realización de la misma se ha llegado a las siguientes conclusiones.

1. El desarrollo de un prototipo permitió determinar que es posible mejorar la seguridad de los sistemas de información de las PYMES conjuntamente con la aplicación de los agentes inteligentes.
2. Los sistemas multi-agentes como una rama de la inteligencia artificial, se ha convertido en una de las áreas de investigación y aplicación en el campo de las ciencias de la computación, el cual permitió la implementación del prototipo.
3. La metodología a diseñar los agentes de una manera más estructurada y objetiva, y como resultado es el desarrollo del prototipo de los agentes.
4. El concepto de agente/sistema multi-agente es el área de la inteligencia artificial tuvo éxito en la elaboración de prototipo y su implementación en el servidor NginX
5. Las herramientas para el desarrollo en lado *back-end (bash*, *nodejs y Python*) y en *front-end (html 5*, bootstrap 4.0, css3), hicieron posible todo el desarrollo de la aplicación.
6. El *servidor* NginX fue de gran ayuda para llevar a cabo la implementación y hacer realidad que si se puede mejorar la seguridad en las empresas PYMES. Así mismo es necesario continuar buscando nuevos mecanismos de seguridad informática que reduzca los costos y su efectividad en diferentes empresas y haciendo que los agentes inteligentes sean más autónomos.

REFERENCIAS

[1] Ardita, J CYBSEC S.A, http://www.cybsec.com/upload/ataque.pdf Recuperado el 10 de septiembre de 2018

[2] Estadísticas, Recuperado 20 oct 2018 http://www.delitosinformaticos.info/peritaje_informatico/estadisticas.html

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

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

[5] Russell S & Norvig P,2008, Inteligencia Artificial Un Enfoque Moderno, Segunda Edición, Pearson Educaction España

[6] Wooldridge, M. (2009). An Introduction to MultiAgent Systems. Wiley Publishing, 2nd edition

[7] open software security, https://mega.nz/#!qdJiza4Z!DFD2QMrV1M7nTL1R539S 4jNj3vrgvgU1Bor126ftEM20

[8] https://openwebinars.net/blog/que-es-payload/

https://tecnofor.es/que-es-un-vector-ataque-ciberseguridad

Breve CV del autor

Adrian Eusebio Quisbert Vilela es Licenciado en Informática.
Su actividad laboral consiste en el desarrollo de software, soporte en seguridad informática y docencia universitaria.
Su interés investigativo abarca temas de seguridad de la información y la inteligencia artificial. Email: aquisbertvilela@gmail.com.