FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA DE SISTEMAS COMPUTACIONALES

UNIVERSIDAD PRIVADA DEL NORTE

"ANÁLISIS Y TÉCNICAS DE SEGURIDAD EN REDES INFORMÁTICA BASADO EN OPEN SOURCE, UNA REVISIÓN DE LA LITERATURA CIENTÍFICA EN LOS ÚLTIMOS 5 AÑOS"

Trabajo de investigación para optar al grado de:

Bachiller en Ingeniería de Sistemas Computacionales

Autor:

Mario Jesús Farro Cachay

Asesor:

Ing. Neicer Campos Vásquez

Lima - Perú

2019

DEDICATORIA

A Dios por mantenerme con buena salud y por haberme guiado por el camino correcto.

A mis padres por ser fuente y motor para darme la fortaleza para continuar con mis objetivos profesionales.

A mis tías Martha y Gaby Capuñay, quienes desde niño me incentivaron a ser ingeniero. Sus palabras fueron inspiración para mi formación personal y profesional; por este motivo, siempre recordaré su afecto y cariño.

AGRADECIMIENTO

Agradecimiento especial a mi tío Jorge Cachay, quien despertó en mí el interés de la carrera de Ingeniería de Sistemas, y a mi madre, quien siempre confió en mis logros profesionales.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La seguridad informática es un tema de suma importancia para un administrador de redes, puesto que las licencias y demás herramientas de software de seguridad son de alto costo para una pequeña o mediana empresa. Como alternativa, surgen los sistemas de detección y prevención de intrusos (IDS/IPS) Open Source, los cuales proporcionan un alto nivel de seguridad con características eficientes; por lo tanto, poseen el mismo grado de efectividad que un software licenciado.

Suricata es un software de detección y prevención de intrusos (IDS/IPS) que analiza el tráfico con una amplia base de datos actualizada. Este presenta varias características resaltantes que lo posicionan como una excelente alternativa de código abierto basado en un conjunto de reglas y características que lo posicionan en ventaja frente al IDS/IPS SNORT.

En la presente investigación, se somete a prueba el software Suricata Open Source usando como base de distribución a Linux Ubuntu. Además, se mide su eficacia en el análisis del tráfico de red y de ataques de denegación de servicios.

PALABRAS CLAVES: Seguridad en redes informáticas, Sistema de detección y prevención de intrusos, Seguridad en redes Open Source, IDS Open Source, Network and Security.

CAPÍTULO I. INTRODUCCIÓN

La seguridad informática es uno de los temas más preocupantes en la actualidad. En efecto, toda entidad pública y privada debe proteger sus datos. Sin embargo, si bien las nuevas tecnologías avanzan a gran escala, los fraudes también lo hacen al mismo ritmo. El robo de información o sustracción de datos son el principal objetivo de los crackers, quienes buscan apoderarse y resquebrajar la seguridad del software o del hardware de las empresas. Generalmente, pueden lograrlo porque, a menudo, los sistemas de seguridad en redes informáticas están mal configurados.

Según Quiroz, S. y Macías, D (2017), la vulnerabilidad en la configuración de la seguridad informática es una puerta abierta y aprovechada por los posibles ataques que se apoderan del sistema. Asimismo, existen vulnerabilidades que tienen un alto grado de gravedad si no son identificadas a tiempo.

Por otra parte, de acuerdo con Diaz, G., Alzórriz, I., Sancristóbal, E. y Castro,M.(2014), la seguridad informática no se consigue comprando uno u otro producto, ni siquiera consiguiendo al mejor anti-hacker del mundo. Para los autores, el proceso de seguridad es complejo; por lo tanto, se debe hacer uso de herramientas actualizadas en seguridad y dicho proceso debe mantenerse siempre vigilado.

Conocer los nuevos y diferentes métodos de ataques que van apareciendo es la tarea de todo administrador de red que vela por la seguridad informática de su empresa. Por consiguiente, al estudiarlos con detalle, es posible contrarrestarlos con algunas de las siguientes técnicas aplicadas: sistemas de identificación, cortafuegos, sistemas

criptográficos, antivirus, análisis de vulnerabilidades y sistemas de detección de intrusos. Asimismo, Choque, A (2014), señala que, en la actualidad, las empresas tienen la responsabilidad y obligación de proteger su centro de control de datos ante peligrosos crackers, virus, malware, phishing y demás derivaciones de ataques digitales que generen o se conviertan en vulnerabilidades que perjudiquen a la compañía.

Según Vacca, J. (2014), muchas compañías invierten en hardware y software que dan respuesta a los ataques masivos de crackers. Estos no descansan en la búsqueda de aperturas o escaneos de sitios, desde donde se filtran para tomar posición y producir daños al sistema con fines de lucro. Es importante tener en cuenta que, desde el punto de vista de la seguridad informática, se puede explorar más de una solución realista con herramientas o técnicas administrables en Open Source, por ejemplo, OSSEC, Samhain, Tripwire, Qualys, nCircle, Verisys, AIDE.

A partir del análisis del contexto actual y de la revisión bibliográfica, surge la siguiente pregunta: ¿cuáles son las herramientas eficientes para la seguridad informática en Open Source en los últimos 5 años? De acuerdo con los estudios sobre seguridad informática, las herramientas de sistemas de detección de intrusos (IDS) y los sistemas de prevención de intrusos (IPS) en Open Source son los que se han propuesto recientemente. Estos detectan constantemente paquetes maliciosos y aplican medidas de acción en nuestra red si aparecen variantes sospechosas.

Según Yauri, E. (2017), el sistema de detección de intrusos (IDS) Open Source contiene una amplia lista de registros de ataques que se va actualizando por Internet

frecuentemente. Su principal función es detectar o descubrir algún evento sospechoso en el sistema, así como mostrar un análisis en tiempo real, lo cual permite un monitoreo eficaz en la detección de intrusos. Del mismo modo, el sistema de prevención de intrusos (IPS) Open Source tiene la función de prevenir los ataques con la capacidad de bloquearlos. Las medidas que utiliza el IPS son técnicas que repelen los daños que podría ocasionar una posible amenaza.

Según Quintero, J. (2018), las recientes investigaciones demuestran que IDS/IPS son herramientas de seguridad con mayor madurez y son tan efectivos como los productos con licencias. Ambos sistemas existen en código abierto y cuentan con aplicaciones de libre distribución como Bro, Suricata, Snort y Ossec, los cuales pueden ser configurados y aplicados a la seguridad en redes informáticas para cualquier entidad pública.

La presente revisión sistemática tiene como objetivo de investigación demostrar cómo el IDS/IPS Open Source Suricata presenta similares cualidades que los productos con licencia y ha incorporado mejoras notables en tecnología para la seguridad de redes informáticas. Asimismo, se mostrará las eventualidades que pueden observarse en una interfaz gráfica con reportes de los eventos que ocurren en la red.

CAPÍTULO II. METODOLOGÍA

La siguiente revisión sistemática consistió en búsquedas detalladas de información actualizada y verídica, recolectando evidencias y experiencias de publicaciones científicas. Se ha utilizado una metodología cualitativa con respecto a la seguridad de redes informáticas, técnicas y herramientas en Open Source.

Estrategias de búsqueda:

En el proceso de búsqueda, se clasificó la información relevante seleccionada y exclusiva mediante bibliotecas virtuales y tesis encontradas desde Ebook Centra (27%), ProQuest (18%), Redalyc (18%), Biblioteca Virtual Scielo (10%) y Google Académico (27%). La búsqueda se realizó desde el día 29 de marzo del año 2019. Conforme avanzaba la investigación, la búsqueda se afinó aplicando filtros de búsqueda. Por ejemplo, respecto de la antigüedad de las publicaciones científicas se estableció un margen de 5 años, con lo cual se encontró información relevante y confiable en idioma español, portugués e inglés.

Las palabras claves fueron utilizadas para una mayor precisión en la búsqueda. Estos fueron las siguientes: Seguridad en redes informáticas, Sistema de detección y prevención de intrusos (IDS/IPS), Network and Security, Secure Network, Snort, Suricata.

Tabla 1

Publicaciones seleccionadas con relación a seguridad informática y en descarte a distintas bases de datos.

Raíz de búsqueda	**Google Academy**	**ProQuest**	**Ebook Central (Libros virtuales)**	**Redalyc**	**Biblioteca Virtual**	**Total**
Posibles encontrados	15	10	15	10	6	56
Búsquedas seleccionadas	8	3	10	5	4	30
Información excluida	7	8	7	7	4	33

Resultados de búsqueda seleccionadas. Elaboración propia.

Se filtró información digitando el uso de palabras claves relacionadas con el tema de seguridad informática en distintas bases de datos. Los resultados seleccionados se vinculan con el análisis y el contexto de la seguridad informática mediante Open Source. No se descartaron fuentes con información desarrollada en inglés. Por otra parte, la información excluida se relacionaba con temas referentes a la especialidad de electrónica y a fuentes escritas en diferentes paises.

La mayor parte de la información seleccionada se encontró tanto en español como en inglés. En relación con el tema buscado, se recopiló suficiente información para la revisión sistemática. Respecto de lo encontrado en revistas científicas, libros virtuales y tesis, se

utilizó la herramienta Mendeley Desktop para organizar la información recopilada. Las entradas temáticas se describen a continuación:

- Seguridad en informática
- Open Source Security Tools
- Sistema de prevención y detección de intrusos IDS / IPS
- System security networks

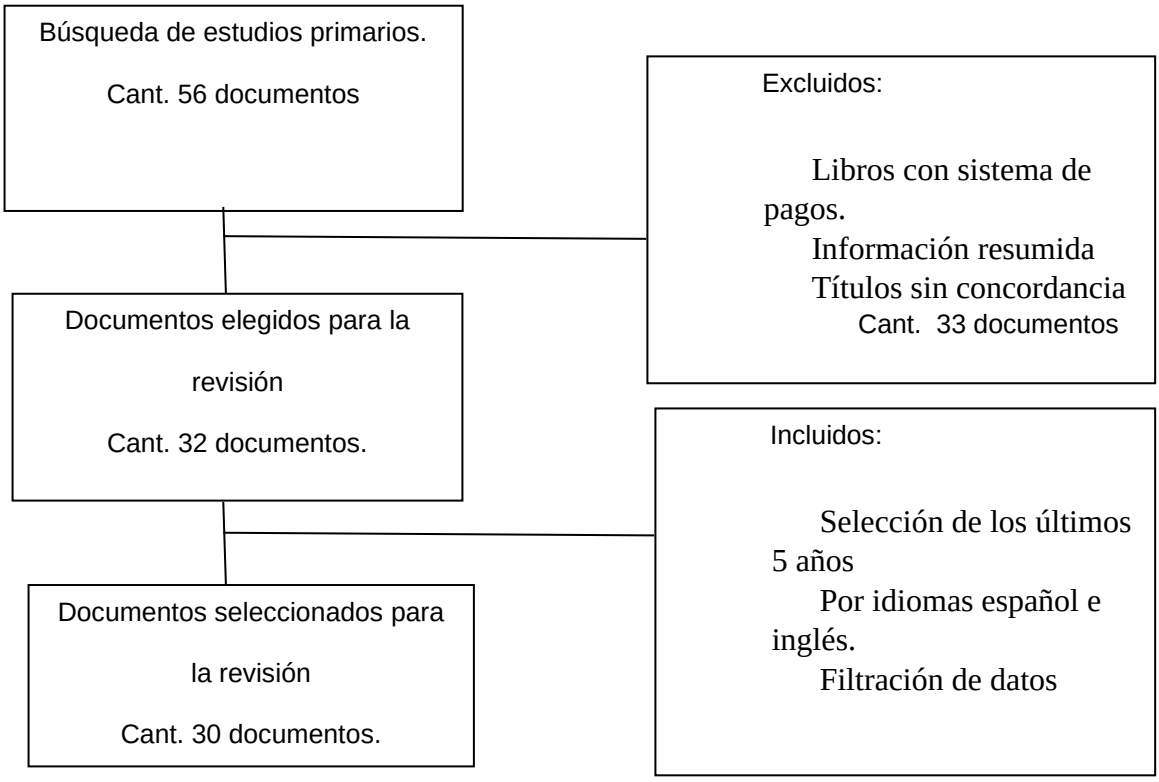
En el proceso de análisis de la información, se consideró los conceptos referidos a seguridad en redes informáticas para comprender lo importante que significa la seguridad informática en términos generales.

En el proceso de posibles encontrados en distintas bases de datos se prosiguió a elegir los temas de mayor interés y relacionados a la seguridad informática, sin embargo, la información excluida pertenecía a los años 2006, 2010 y 2012, así también se excluyeron libros fuera de contextos al tema de seguridad informática. Por tanto, fueron seleccionados d libros, tesis y artículos; de diferentes países internacionales sumando un total de 30 documentos que demostraron relación al contexto general de seguridad informática Open Source, sistemas prevención o detección de intrusos Open Source.

CAPÍTULO III. RESULTADOS

En la presente revisión sistemática, fueron incluidos y seleccionados 40 documentos encontrados en distintas bases de datos. Dichos documentos permitieron conseguir y analizar información precisa para el desarrollo del tema de interés.

Diagrama de Flujo - Proceso de selección de datos.



En el proceso de selección, fueron consultadas diferentes bases de datos, como Redalyc, Alicia, Google Académico, Elseiver, Scielo, entre otras. Los documentos

examinados y seleccionados fueron agregados usando la herramienta Zotero, la cual permite tener un mejor orden y control para la revisión sistemática.

Asimismo; la información relevante fue seleccionada de diferentes fuentes académicas como libros digitales, tesis, artículos escritos en los últimos 5 años. La siguiente imagen nos muestra la cantidad de publicaciones obtenidas en los últimos años.

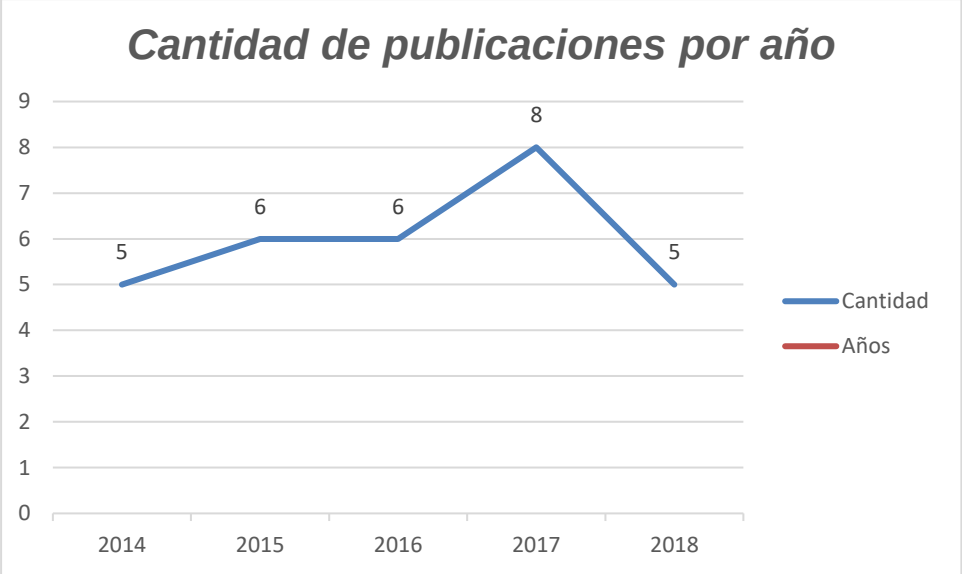


Figura 1. Publicaciones seleccionadas en distintas bases de datos (2014-2018). Elaboración propia

En el intervalo de los últimos cinco años (2014 al 2018), el año 2017 cuenta con mayor cantidad de documentos publicados en diferentes bibliotecas. No obstante, toda la información relevante de los últimos años será considerada para el análisis de los documentos recopilados. De esta manera, se contará con nuevas herramientas e información actualizada.

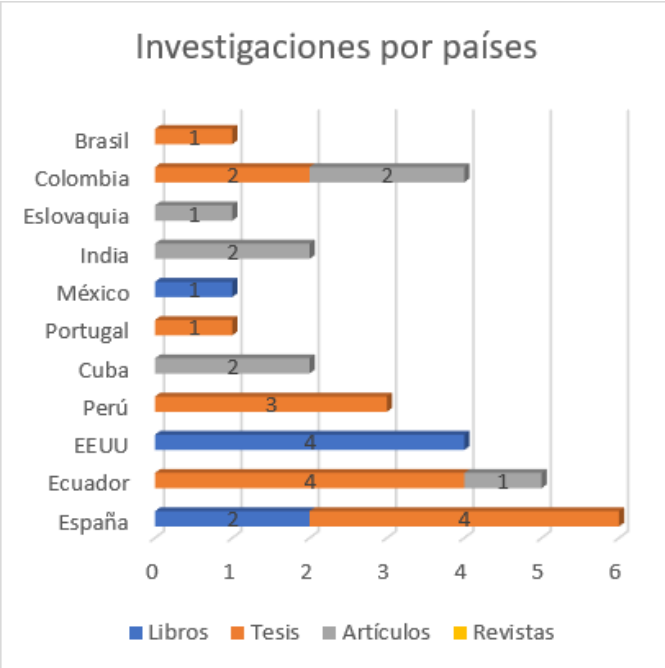


Figura 2. Resultados sobre seguridad en redes informáticas por países. Elaboración propia.

En la imagen referida a las investigaciones por países, se muestra a España como uno de los países con mayor índice de investigaciones durante los últimos 5 años, seguido del país EE. UU. con el mayor índice en publicaciones de libros digitales realizadas sobre seguridad en redes informáticas. Estos estudios describen las técnicas que destacan en Open Source. Aplicando la regla de Pareto a los datos recolectado, se obtiene la siguiente información:

Tabla 2
Porcentaje de investigaciones realizadas por países sobre seguridad informática

Resumen de porcentaje en investigación

Países	Cantidad	Porcentaje	Porcentaje Acumulado
España	6	20%	32%
Ecuador	5	17%	49%
EEUU	4	13%	62%
Perú	3	10%	72%
Cuba	2	7%	79%
Portugal	1	3%	72%
México	1	3%	75%
India	2	7%	82%
Eslovaquia	1	3%	88%
Colombia	4	13%	101%
Brasil	1	3%	105%
Total	30	100%	

Fuente: Elaboración propia

En la siguiente figura, se muestra los resultados de investigación en porcentaje por países, mediante el diagrama Pareto en función de la revisión sistemática.

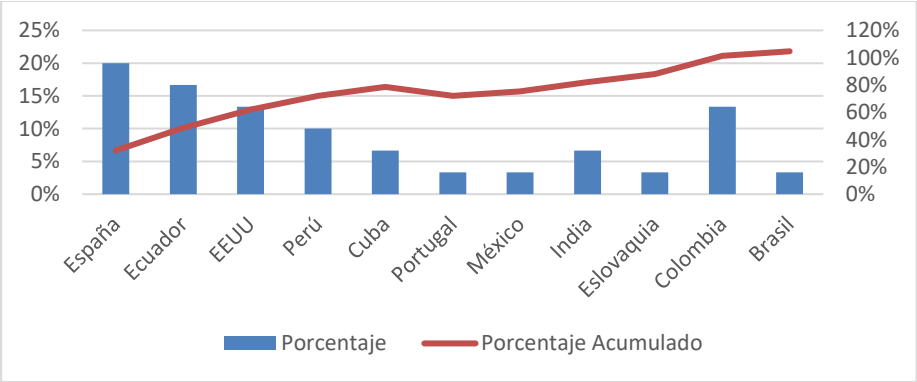


Figura 3. Diagrama Pareto aplicado en porcentajes de investigación. Elaboración propia

De acuerdo con los resultados mostrados por el diagrama Pareto en el periodo 2014-2018, los países con mayor porcentaje de investigaciones encontradas en tesis, libros digitales y artículos que describen las herramientas y técnicas vigentes, tanto en idioma español como inglés, serán incluidos para la revisión y elaboración del tema de sistema de detección y prevención de intrusos (IDS / IPS) en Open Source.

Esta recolección de datos forma parte de nuestra investigación y está incluida en los hallazgos que conducen a analizar y explicar la seguridad de redes informáticas. Esta temática incluye los principios que la rigen, las problemáticas, las instalaciones de *software*, los casos de estudios y los casos de éxitos documentados en los países ya mencionados.

Se muestra la siguiente tabla en la cual se clasifica la información encontrada en distintas bases de datos de los países mencionados. Se detalla la cantidad de libros, tesis, artículos y documentos. Su elección se constituye como la base para nuestra investigación sistemática.

Tabla 3

Información encontrada en la revisión sistemática

	Libros	Tesis	Artículos	Total
España	2	4		6
Ecuador		4	1	5
EE. UU.	4			4
Perú		3		3
Cuba			2	2
Portugal		1		1
México	1			1
India			2	2
Eslovaquia			1	1

Colombia		2	2	4
Brasil		1		5

Fuente: Elaboración propia

En cuanto a los resultados de tesis vinculadas con el tema de nuestra revisión sistemática, destaca la siguiente: Diseño y despliegue de un sistema de detección de intrusos en redes por software, elaborada por Orbegozo Aldalur (2018) en España. En esta tesis, se enfatiza la importancia de un sistema de detección de intrusos (IDS) y de un sistema de prevención de intrusos (IPS) que tengan la capacidad de cerrar conexiones que constituyan un problema o riesgo.

Otra tesis relevante es la titulada Sistema de detección de intrusos mediante SNORT y comparación con otras aplicaciones, elaborada por Janeth Sánchez Restrepo (2017) en Ecuador. En esta, se menciona a SNORT como la herramienta y la técnica más utilizada en el mundo. Este sistema IDS/IPS se encuentra disponible bajo licencia GPL, además de ser multiplataforma para sistemas operativos Windows y Linux.

También se ha encontrado la investigación Implementación de un sistema de detección de intrusos en la red interna, elaborada por Jayner Quintero Herrera (2018) en Colombia. Este estudio menciona otra nueva y eficiente herramienta para el sistema de detección y prevención de intrusos (IDS/ IPS): SURICATA. Dicha herramienta tiene el respaldo de Open Information Security Foundation (OISF), organización comprometida con el desarrollo y soporte de SURICATA, como parte de un proyecto de código abierto para la detección y prevención de amenazas complejas.

La siguiente figura ilustra los resultados de tesis encontrados en distintos países, contando con un mayor número en España y Ecuador.

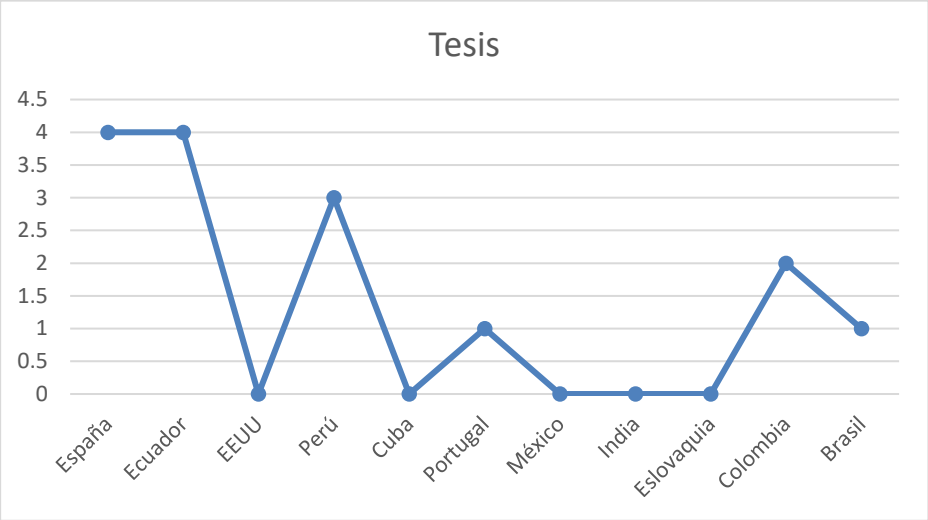


Figura 4. Resultado de tesis encontradas en diferentes bases de datos. Elaboración propia

La arquitectura de IDS/IPS debe generar una alerta al administrador de red para su revisión y acción ante un posible evento sospechoso, se representa en la siguiente figura.

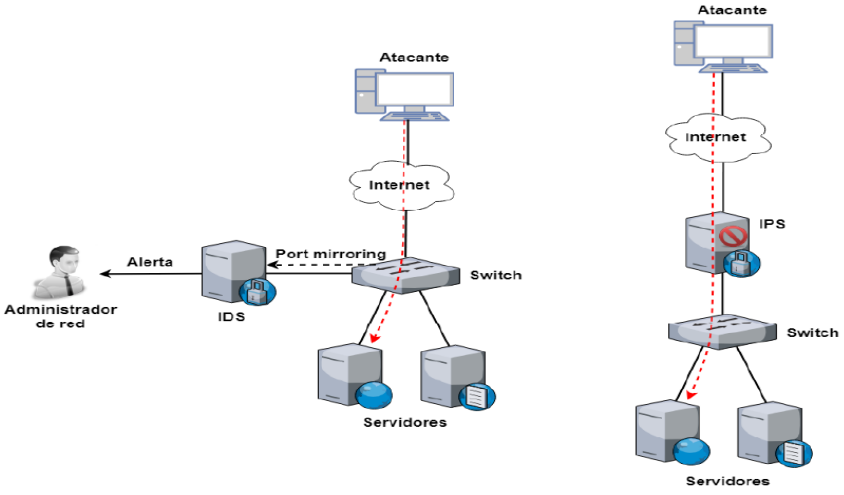


Figura 5. Sistema de detección y prevención de intrusos definidas por *software* (Orbegozo Aldalur, 2018)

Tabla 4
Descripción comparativa de IDS / IPS

Características	Bro	Snort	Suricata
Procesamiento multihilo	No	No	Sí
Soporte completo IPv6	Sí	Sí	Sí
Detección Automática de Protocolos	Sí	No	Sí
Aceleración con GPU	No	No	Sí
Variables Globales/Flowbits	Sí	No	Sí
GeoIP	Sí	No	Sí
Análisis Avanzado de HTTP	Sí	No	Sí
HTTP Access Logging	Sí	No	Sí
SMB Access Logging	Sí	No	Sí

La comparación de las características de cada IDS/IPS nos revela que Suricata se centra en la seguridad, la usabilidad, eficiencia y otras funciones que sobrepasan lo ofrecido por Snort y Bro.

Otra característica que destaca en Suricata, y que no se encuentra en Snort, es su cualidad *multithreading* (multihilos); es decir, se encarga de distribuir la carga de trabajo en varios procesos al mismo tiempo (Sánchez, 2017).

Tabla 5
Comparativo de Suricata con IDS/IPS propietarias

Características	Soluciones Comerciales IDS/IPS	Suricata
Procesamiento multihilo	No	Sí
Soporte completo IPv6	Cisco, IBM, Stonesoft	Sí
IP Reputación	Cisco	Sí
Detección Automática de Protocolos	No	Sí
Aceleración con GPU	No	Sí
Variables Globales/Flowbits	No	Sí
GeoIP	No	Sí

Análisis Avanzado de HTTP	No	Sí
HTTP Access Logging	No	Sí
SMB Access Logging	No	Sí
Anomaly Detection	Sí	No
Alta Disponibilidad	Sí	No
GUI de Administración	Sí	No
Software Libre	No	Sí

Los libros digitales, en forma general, fueron encontrados en distintas bases de datos que representan a EE. UU. Sin embargo, cuenta con un sistema de compra de libros *on line*; asimismo, existen libros de libre acceso a lectura en idioma español e ingles. El libro Open Source Security (511 páginas) desarrolla con detalle la eficiencia de las herramientas de código abierto aplicadas en la protección de los recursos de red.

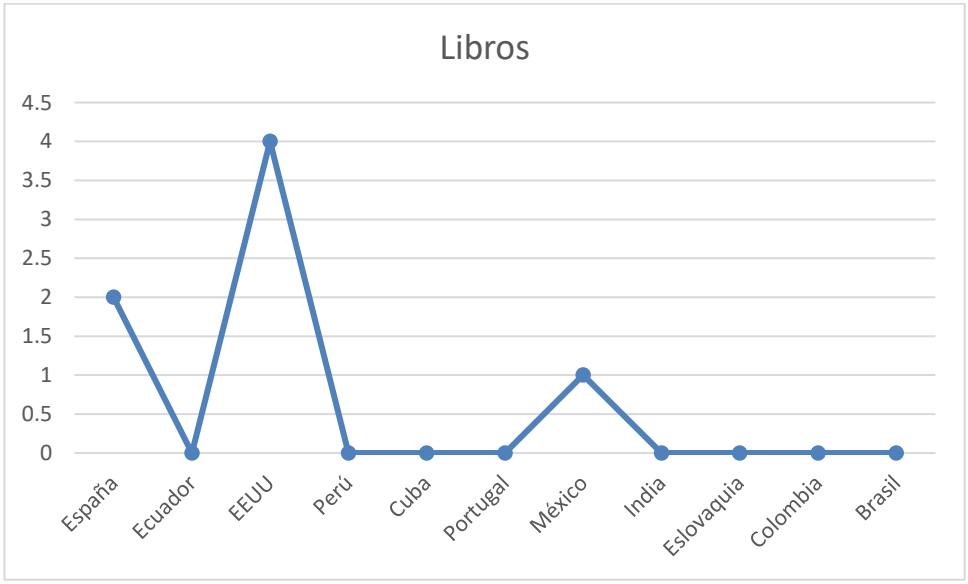


Figura 6. Resultados de libros digitales encontrados en diferentes bases de datos. Elaboración propia

Otra manera de representar el sistema de detección de intrusos es contar con un firewall detrás del IDS, esto permite un mejor resguardo de los equipos conectado a internet.

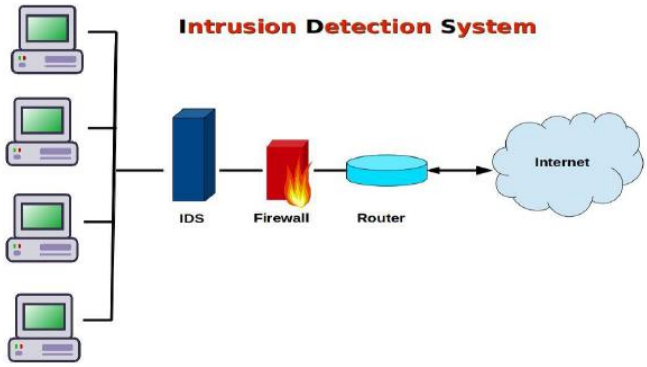


Figura 7. Diseño e implementación del sistema de prevención y detección de intrusos (Ortiz y Barrionuevo, 2018)

No obstante, se contó con artículos referidos a IDS / IPS de los siguientes países que se muestra en la figura 8.

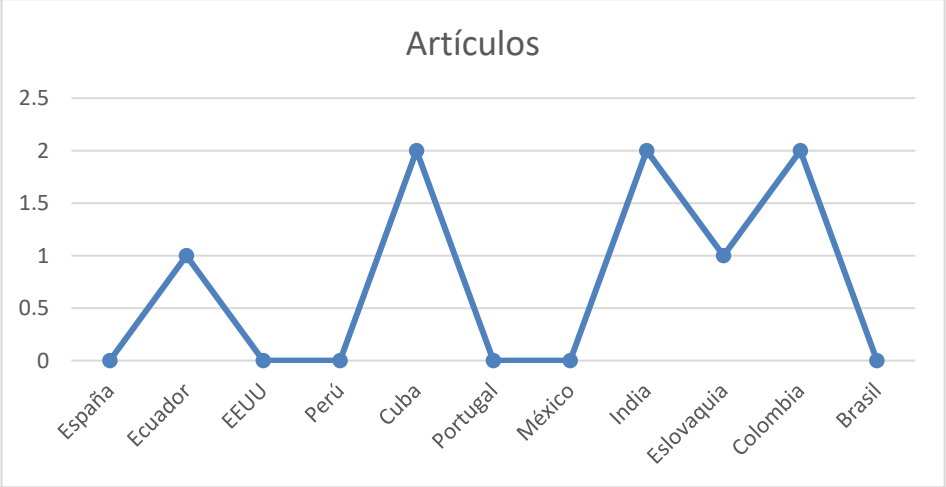


Figura 8. Resultados de artículos encontrados en diferentes bases de datos. Elaboración propia.

Los artículos recopilados nos indican también la clasificación de los IDS basados en red (NIDS) y los IDS basados en hosts (HIDS).

En el caso del sistema de detección de intrusiones basado en redes (NIDS), este monitorea un segmento de red. Su función es la captura de paquetes que pasan por la red para su análisis o la toma de una acción pertinente.

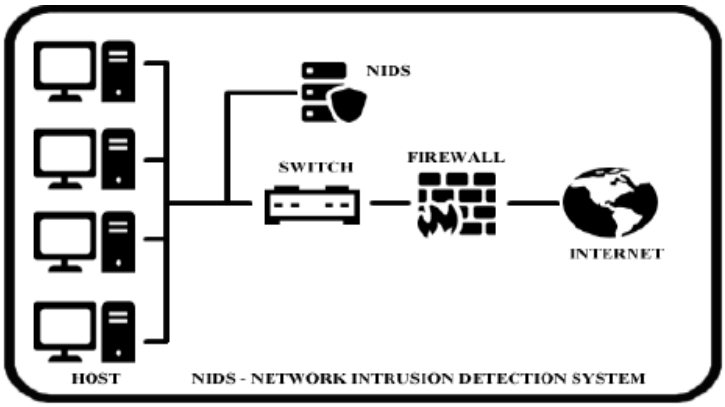


Figura 9. Imagen representativa de NIDS (Vieira, 2016)

En cambio, el sistema de detección de intrusiones por *host* (HIDS) se encarga de las anomalías o ficheros dentro del sistema operativo, como programas en ejecución, procesos del sistema u otros perteneciente a los equipos de los usuarios finales.

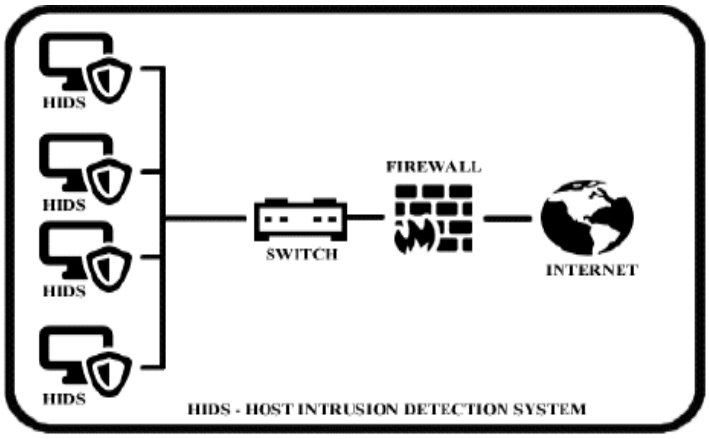


Figura 10. Imagen representativa de HIDS (Vieira, 2016)

En las investigaciones recopiladas, se describe a Snort como una de las herramientas IDS/IPS vigentes que se utiliza en todo el mundo. Sin embargo, algunos de los estudios reconocen que Suricata va ganando terreno con sus características adicionales y su fácil manejo. Ambos sistemas contienen reglas para contrarrestar ataques conocidos, asimismo; se encuentran en constantes actualizaciones su base de datos ante las últimas amenazas.

Cabe precisar que conocer ataques tradicionales en la actualidad es de suma importancia para su identificación en contrarrestar su operación, las nuevas formas o variantes que infringen la seguridad informática forman parte en los sistemas que son vulnerables, por lo tanto, se debe contar con actualizaciones constantes y de nuevas herramientas configurables para conseguir una mejor protección en una red perimetral.

CAPÍTULO IV. CONCLUSIONES

Discusiones

En el proceso de recopilar información en distintas bibliotecas y bases de datos, lo cual forma parte de la revisión sistemática, se discute distintos puntos de vista acerca de los sistemas de seguridad en redes informáticas y la importancia de administrar un sistema de detección y prevención de intrusos (IDS/IPS) eficiente. Distintas fuentes recomiendan emplear técnicas y herramientas de seguridad IDS/IPS Open Source como Snort, el cual cuenta con el mayor número de descargas y presenta una mayor usabilidad a nivel mundial. No obstante, en los últimos años, Suricata, otra IDS/IPS propuesta por las fuentes recopiladas, ha demostrado que ofrece mayores funciones y un fácil manejo, además de contar con la ventaja de generar menor consumo de recursos en un sistema operativo.

Otro aspecto muy importante para la implementación del sistema de detección de intrusos (IDS) es la elección del sistema operativo, la base de datos, la interfaz gráfica para la administración y, por último, el software para la recolección de datos. Todo ello deberá ser instalado e implementado para una óptima funcionalidad y operatividad con el objetivo de mantener gran parte del control en la seguridad de redes informáticas.

Por otra parte, en un escenario de implementación de sistemas de detección y prevención de intrusos (IPS/ IDS), siempre surge la interrogante acerca de dónde instalar el IDS: delante o detrás de un *firewall*. Las recomendaciones de diferentes fuentes proponen que debe ser instalado detrás del *firewall*. Con esta ubicación, se convertirá en otro filtro que

garantice la seguridad con los demás componentes en red. De este modo, su función principal será la de escanear puertos, o analizar los paquetes entrantes y salientes en el tráfico de la red.

Respecto de la investigación, se obtuvo distintos enfoques sobre un mismo concepto y sobre la descripción de las herramientas que se utilizan en distintos países (Agra Monte, 2017; Clavero, 2015; Bermejo, 2015; Sanna, 2018; Ortiz y Santana, 2018; Quintero, 2018; Ocampo, Castro y Solarte, 2017; Sánchez, 2017).

Conclusiones

La presente investigación tuvo como tema de interés estudiar la literatura elaborada durante los últimos 5 años sobre el análisis de las técnicas de seguridad para redes informáticas basadas en Open Source. En el desarrollo del estudio, se determinó, con un análisis y clasificación de distintas bases de datos, que el sistema de detección y prevención de intrusos IDS/IP es la herramienta de seguridad en Open Source más conocida y usada en distintos países para la administración de una red aplicada en distintos escenarios.

Una de las múltiples ventajas de un IDS/IP implementado en una red es estar un paso adelante de los intrusos o tener la capacidad de una reacción rápida ante una vulnerabilidad que afecta a los componentes que integran una red. Otra ventaja es que el soporte y las continuas mejoras de sus funciones generan que esta herramienta siga creciendo con constantes actualizaciones, utilidades y nuevas reglas. Así, al tratarse de una herramienta de

código libre, una gran cantidad de usuarios puede beneficiarse de los distintos aportes de los programadores al sistema.

A partir de lo investigado, queda clara la importancia de que, con el pasar del tiempo, un IDS/IPS siga evolucionando ante las nuevas amenazas. Para ello, los *softwares* que se integran a una implementación son de gran utilidad para su administración en modo gráfico. También es pertinente asociarlo con un router Mikrotik o Raspberry que albergue un IDS/IPS. Esto despierta el interés de aplicar nuevos conceptos de solución para distintos escenarios.

Finalmente, después de revisar y analizar distintos casos de éxitos en la implementación y solución de un sistema IDS/IPS, se recomienda que todo administrador de red debe conocer cómo administrar o aplicar estos conceptos de seguridad. Con ello, se logrará una óptima funcionalidad y operatividad de servidores y demás equipos que se integran a la red. Actualmente, aplicar un *firewall* o un antivirus no es suficiente. Por ello, la integración de nuevos software o herramientas son soluciones que se emplean para evitar alguna incidencia.

REFERENCIAS

Agra Monte, A. (2017). *Diseño e implementación de infraestructura NIDS (Network Intrussion Detection System) para PIMES*. (Tesis de bachillerato. Universitat Politécnica de Valencia, Valencia, España). Recuperado de http://hdl.handle.net/10251/88856

Badillo Bernal, D. (2015). *Estudio comparativo de las distribuciones Linux orientado a la seguridad de redes de comunicación*. (Tesis de maestría. Pontificia Universidad Católica del Ecuador, Quito, Ecuador). Recuperado de http://repositorio.puce.edu.ec/handle/22000/10002?show=full

Chapman, C. (2016). *Network Performance and Security: Testing and Analyzing Using Open Source and Low-CostTools*. Cambridge, USA: Syngress. Recuperado de https://books.google.com.pe/books?id=XFrBBwAAQBAJ

Clavero Almirón, J. M. (2015). *Detección de intrusos con Snort*. (Tesis de bachillerato. Universitat Oberta de Catalunya, Barcelona, España). Recuperado de http://openaccess.uoc.edu/webapps/o2/handle/10609/43087

Choque, T. (2014*). Buenas prácticas en la administración de seguridad perimetral de un firewall en empresa del sector de telecomunicaciones*. (Tesis de bachillerato. Universidad Nacional de Ingeniería, Lima, Perú). Recuperado de https://alicia.concytec.gob.pe/vufind/Record/UUNI_656cefb9df2c231d62185059871f90b6

Castro, M., Díaz, G., Alzórriz, I. y Sancristóbal, E. (2014). Procesos y herramientas para la seguridad de redes. Madrid, España: Editorial UNED. Recuperado de https://books.google.com.pe/books?id=dG4lAwAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Da Costa Calado, J. P. (2018*). Open Source IDS/IPS in a production environment: comparing, assessing and implementing*. (Tesis de maestría. Universidade de Lisboa, Lisboa, Portugal). Recuperado de http://repositorio.ul.pt/bitstream/10451/35418/1/ulfc121871_tm_Jo%C3%A3o_Paulo_Calado.pdf

De Haro Bermejo, F. (2015). *Detección de intrusiones con Snort.* (Tesis de posgrado. Universitat Oberta de Catalunya, Barcelona, España). Recuperado de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/43100/5/fdeharobTFM0615memoria.pdf

Eldow, O., Chauhan, P., Lalwani, P. y Potdar, M.B. (2016). Computer Network Security Ids Tools And Techniques (Snort/Suricata). *International Journal of Scientific and*

Research Publications, *6*(1), 593-597. Recuperado de http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.735.1457

Ennert, M., Madoš, B. y Dudláková, Z. (2014). Data Visualization Of Network Security Systems. *Acta Electrotechnica et Informatica*, *14*(4), 13–16, Recuperado de https://www.researchgate.net/profile/Branislav_Mados/publication/275241255_DATA_VISUALIZATION_OF_NETWORK_SECURITY_SYSTEMS/links/562759b908aed3d3f13a2d1b/DATA-VISUALIZATION-OF-NETWORK-SECURITY-SYSTEMS.pdf

Gil Vera, V. D. y Gil Vera, J. C. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. *Scientia Et Technica*, *22*(2), 193-197. Recuperado de http://www.redalyc.org/articulo.oa?id=84953103011

Gregg, M. (2015). *The network security test lab: A step-by-step guide*. Recuperado de https://ebookcentral.proquest.com/lib/upnpe/detail.action?docID=4040350&query=The+network+security+test+lab%3A+A+step-by-step+guide

Hernández Ortíz, D. y Santana Barrionuevo, A. (2018). Diseño e implementación del sistema de prevención y detección de intrusiones en la empresa Proauto C.A. (Tesis de bachillerato. Universidad de las Américas, Quito, Ecuador). Recuperado de http://dspace.udla.edu.ec/handle/33000/10325

Gómez Vieites, A. (2014). Gestión de incidentes de seguridad informática. Recuperado de https://ebookcentral.proquest.com/lib/upnortesp/reader.action?docID=3229340

Miranda Cairo, M., Valdés Puga, O., Pérez Mallea, I., Portelles Cobas, R. y Sánchez Zequeira, R. (2016). Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática. *Revista Cubana de Ciencias Informáticas*, *10*(2), 14-26. Recuperado de https://www.redalyc.org/pdf/3783/378345292002.pdf

Nathans, D. (2015). *Designing and building security operations center*. Recuperado de https://ebookcentral.proquest.com/lib/upnpe/detail.action?docID=1834659&query=Designing+and+building+security+operations+center

Ocampo, C. A., Castro Bermúdez, Y. V. y Solarte Martínez, G. R. (2017). Sistema de detección de intrusos en redes corporativas. *Scientia Et Technica*, *22*(1), 60-68. Recuperado de http://www.redalyc.org/articulo.oa?id=84953102008

Orbegozo Aldalur, I. (2018). Diseño de despliegue de un sistema de detección de intrusión en redes definidas por software. (Tesis de bachillerato. Escuela de Ingeniería de Bilbao, Bilbao, España). Recuperado de https://addi.ehu.es/handle/10810/29279

Porven Rubier, J. y Montesino Perurena, R. (2015). Marco de trabajo para la gestión centralizada de trazas de seguridad usando herramientas de código abierto. *Revista Cubana de Ciencias Informáticas [online]*. *9*(3), 18-32. Recuperado de

http://scielo.sld.cu/scielo.php?script=sci_abstract&pid=S2227-18992015000300002&lng=es&nrm=iso&tlng=es

Quintero, J. (2018). Implementación de un sistema de detección de intrusos en la red interna de la alcaldía de Montería usando software libre. (Tesis de bachillerato. Universidad Nacional Abierta y a Distancia, UNAD, Colombia). Recuperado de https://repository.unad.edu.co/bitstream/10596/17438/1/8867918.pdf

Quiroz, S. y Macías, D (2017). Seguridad en informática: consideraciones. *Dominio de las Ciencias, 3(5),* 676-688. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=6137824

Resmi, A. M. y Manicka, C. (2017). Intrusion detection system techniques and tools: A Survey. *Scholars Journal of Engineering and Technology (SJET), 5*(3), 122-130. Recuperado de https://pdfs.semanticscholar.org/6bd1/1cc6bae8bc44201cceff411b998d802622c7.pdf

Rodríguez Gutierrez, A. F. (2016). *Diseño de un sistema de detección de intrusos con Snort para la compañía Silverit SAS.* (Tesis de bachillerato. Universidad Piloto de Colombia, Bogotá, Colombia). Recuperado de http://repository.unipiloto.edu.co/handle/20.500.12277/2706

Sánchez Cunalata, F. (2017). *Implementación de un sistema de monitoreo y protección de datos en la red de la facultad de ingeniería en sistemas, electrónica e industrial*. (Tesis de bachillerato. Universidad Técnica de Ambato, Ambato, Ecuador). Recuperado de http://repositorio.uta.edu.ec/jspui/bitstream/123456789/25707/1/Tesis_t1254si.pdf

Sánchez Restrepo, J. (2017). *Sistema de detección de intrusos mediante Snort y comparación con otras aplicaciones.* (Tesis de bachillerato. Universidad Estatal del Sur de Manabí, Manabí, Ecuador). Recuperado de http://repositorio.unesum.edu.ec/bitstream/53000/842/1/UNESUM-ECU-COMPR-19.pdf

Vieira, J. F. (2016). *Desenvolvimiento de un IDS basado en técnicas de Data Mining. (*Tesis de bachillerato. Universidades de Santa Cruz do Sul, Rio Grande do Sul, Brasil). Recuperado de http://repositorio.unisc.br:8080/jspui/handle/11624/2131

Vacca, J. (2014). *Computer and information security*. Recuperado de https://books.google.com.pe/books?id=zb916YOr16wC&pg=PA48&lpg=PA48&dq=Tripwire,+Qualys,+nCircle,+Verisys,+AIDE.&source=bl&ots=PSiJfLwV_C&sig=ACfU3U0QD31DIeEmvkS1ktT5jTHrUD-HdQ&hl=es&sa=X&ved=2ahUKEwjC1u6AlJ7rAhWQE7kGHQGiB58Q6AEwAHoECAwQAQ#v=onepage&q&f=false

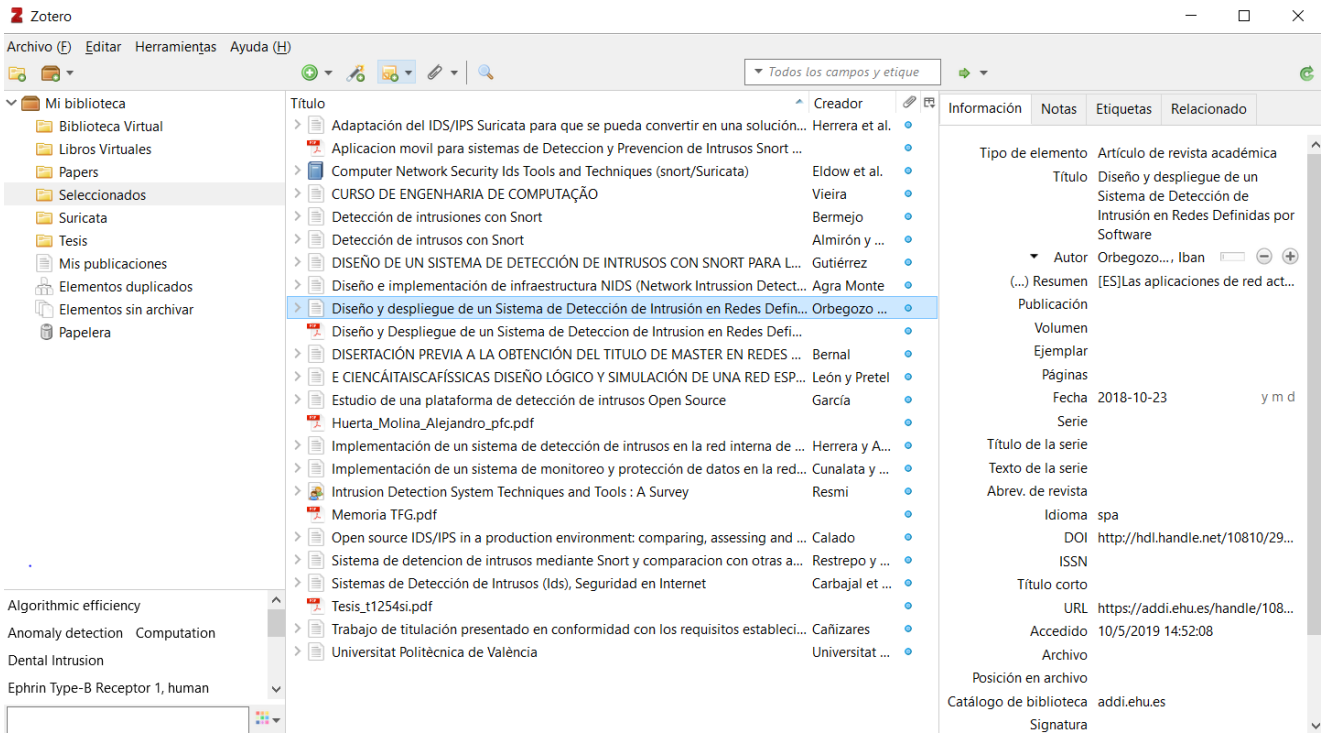
Yauri, E. (2017). *Aplicación móvil para sistemas de detección y prevención de intrusiones basados en Snort.* (Tesis de bachillerato. Universidad Nacional de Ingeniería, Lima, Perú). Recuperado de https://alicia.concytec.gob.pe/vufind/Record/UUNI_4a678157566f7e7b6262ff66bb01febb

Baca, G. (2016). *Introducción a la seguridad informática*, México: Editorial Patria. Recuperado de https://books.google.com.pe/books?id=IhUhDgAAQBAJ

Dios, S. y Ortiz, D. (2018). *Diseño lógico y simulación de una red espejo virtual (HONEYNET) para la detección de intrusos informáticos en zona perimetral*. (Tesis de bachillerato. Universidad Nacional de Trujillo, Trujillo-La Libertad, Perú). Recuperado de https://alicia.concytec.gob.pe/vufind/Record/UNIT_650e5cb8b3303d03e41a6f21a169c425

ANEXOS

1. Gestor de investigación



2. Formato de encuesta para especialista en seguridad informática.

Encuesta dirigida a ingenieros de sistemas y expertos tecnológicos

Instrucciones: Lea atentamente y responda cada pregunta marcando con un aspa (X) en cada cuadro que corresponda.

1. ¿Cuánto tiempo lleva siendo responsable y trabajando en el área de sistemas?

1 - 2 años	
2 - 4 años	
4 - 6 años	

	SI	NO
2. ¿Está de acuerdo con la importancia de un software de IDS/IPS para el área de sistemas?		
3. ¿Está de acuerdo con que se utilice software Open Source para prevenir ataques informáticos?		
4. ¿En su opinión, ha tenido algún incidente o anomalía en la red administrativa que ha evidenciado o perjudicado a la red informática que tuvo a cargo?		
5. ¿Conoce alguna herramienta para el sistema de detección y prevención de intrusos?		
6. En su opinión, ¿la red administrativa que tiene a su cargo puede prevenir posibles ataques y tomar acciones ante un evento sospechoso?		
7. En su opinión, ¿le gustaría que exista un mejor control de seguridad en el área de sistemas con un sistema de detección y prevención de intrusos?		
8. En su opinión, ¿cree usted que es demasiada inversión para una implementación del sistema de prevención y detección de intrusos?		