Redes neuronales artificiales y estado del arte aplicado en la ciberseguridad

State of the art artificial networks applied to cybersegurity

Castellanos Rojas, Brayan Sebastian[1], Cortés Rodríguez, Carlos Uriel[2], Espitia Osorio, David Javier[1] y Garzón Bello, Yuli Tatiana[1]
Fundación Universitaria de San Gil – UNISANGIL
Facultad de Ciencias Naturales e Ingeniería, Programa en Ingeniería de Sistemas
Semillero de investigación SISLA
Chiquinquirá, Colombia

brayancastellanos@unisangil.edu.co
ccortes@unisangil.edu.co
davidespitia@unisangil.edu.co
yuligarzon@unisangil.edu.co

Fecha de Recepción: abril 08 de 2019
Fecha de Aceptación: marzo 09 de 2020

Resumen **—** El presente artículo realiza una recolección bibliográfica relacionada con las redes neuronales artificiales (RNA) aplicadas a la Ciberseguridad, este se enfoca en una recopilación de investigaciones que buscan cómo realizar detección de intrusos, posibles ataques, correo no deseado, entre otros. Adicionalmente, busca reflejar mediante esta navegación por la literatura, la eficiencia conseguida en el reconocimiento de ataques a sistemas de información utilizando métodos de inteligencia artificial, los cuales pueden brindar un campo de protección de diferentes datos, ya sean de tipo académico o industrial, con la finalidad de evitar vulnerabilidades en los diferentes sistemas. Para esto, un sistema de autoaprendizaje como las RNA pueden resultar una herramienta de protección y detección avanzada, debido a la seguridad predictiva que ofrecen, a razón de un entrenamiento que les permite aprender de la experiencia. Finalmente se pretende analizar el artículo Diseño de un sistema multiagentes híbrido basado en aprendizaje profundo para la detección y contención de ciberataques, cuya finalidad es profundizar en los resultados y adquirir una cercanía con este tipo de investigaciones que están visibilizando los riesgos de la información y diversas maneras para afrontarlos.

Palabras clave **—** Ciberseguridad, Inteligencia Artificial, redes neuronales artificiales, vulnerabilidad.

Abstract **—** The present article compiles a bibliography related to artificial neural networks (ANN) applied to cybersecurity. This focus on a collection of investigations that look for how to do the detection of intruders, possible attacks, unwanted mail, among others. Additionally, it seeks to reflect through this navigation through the literature, the efficiency achieved in the recognition of attacks on information systems using artificial intelligence methods, which can provide a field of protection of different data, whether academic or industrial, with the purpose of avoiding vulnerabilities in different systems. For this, a self-learning system such as ANNs can be an advanced protection and detection tool, due to the predictive safety they offer, due to training that allows them to learn from the experience. Finally, it is intended to analyze the article Design of a hybrid multi-agent system based on deep learning for the detection and containment of cyberattacks, whose purpose is to deepen the results and to acquire a closeness to this type of research that is making information and information risks visible Ways to face them.

Keywords**—** Cybersecurity, Artificial Intelligence, neural networks, vulnerability.

[1] Estudiante de último semestre en Ingeniería de Sistemas UNISANGIL, Chiquinquirá
[2] Docente programa en Ingeniería de Sistemas UNISANGIL, Chiquinquirá

I. INTRODUCCIÓN

Los cibernautas están expuestos a constantes amenazas de algún tipo de virus en la web y ataques a su información, lo que expone las vulnerabilidades de los diferentes sistemas, requiriendo así un interés especial sobre cómo evitar dichos ataques. No obstante, el interés primordial en el presente artículo se centra en recopilar parte de la literatura orientada a trabajar este campo, y de esta forma lograr estructurar futuras estrategias que puedan contrarrestar las brechas de seguridad existentes.

La investigación cobra vida por los riesgos que se enfrentan en la web, por el anonimato que se puede tomar, las suplantaciones y los robos de información. Sin embargo, el artículo abordará la seguridad informática tratando dos aspectos relevantes en este campo como son la navegación preventiva y la detección de fallos.

Mediante el presente artículo se pretende conseguir una visión global del panorama que se presenta en la seguridad informática y el apoyo que puede brindar un sistema de inteligencia artificial basado en redes neuronales artificiales frente a esta área del conocimiento.

II. ANTECEDENTES Y RESEÑA HISTÓRICA DE LAS RNA

En un principio las redes neuronales fueron una representación del sistema neuronal biológico cuya estructura sería la base para los sistemas computacionales inteligentes actuales. Sin embargo, el primer diseño de red neuronal se propuso en 1943 por McCulloch y Pitts, el cual era un sistema binario compuesto por neuronas fijadas con un umbral de activación [1].

En 1951, un cofundador del Massachusett Institute of Technology (MIT), Marvin Minsky, construyó el SNARC, el primer simulador de cadena neuronal, el cual ajustaba los pesos sinápticos de la red neuronal automáticamente, aunque no llegó a procesar datos. Más tarde en 1956 en la conferencia internacional de inteligencia artificial, Nathaniel Rochester presentó un modelo de RNA que simulaba centenas de neuronas interconectadas en un sistema que verificaba como la red respondía a estímulos ambientales, 3 años después el padre de la neurocomputación Frank Rosenblatt creo una red de múltiples neuronas, la cual bautizó como *Perceptron*.

En los años 80 encontraron nuevos modelos de desarrollo en esta área, pero en 1986 el profesor de Psicología David E. Rumelhart y su colega James L. McClelland, publicaron el libro *Parallel Distributed Processing: Explorations in the Microstructure of Cognition (vol.1: Foundations, vol.2: Psychological and Biological Models)*, Este libro presenta un modelo matemático y computacional del entrenamiento supervisado de las neuronas artificiales, dando surgimiento al algoritmo *backpropagation*, este es el primer algoritmo de optimización global sin restricciones.

En la Figura 1 se presenta un bosquejo referente a una neurona biológica.

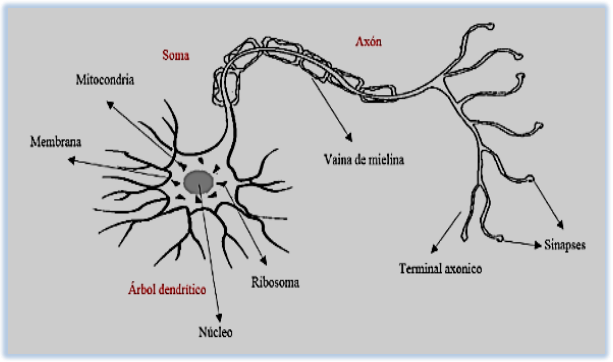

Fig. 1. Neurona Biológica [1], compilación y adaptación autores.

III. CONCEPTOS DE UNA RED NEURONAL ARTIFICIAL

Una red neuronal artificial está compuesta por nodos interconectados que interactúan, transmiten y procesan información en un ciclo computacional de muchas iteraciones que resulta en una salida aproximada de uno a más datos reales; aunque su éxito dependerá del entrenamiento de la red, que a su vez depende de diferentes factores como la arquitectura de la red, el número de datos de entrenamiento, la función de entrenamiento, entre otros. Para ello, existen diferentes tipos de algoritmos de entrenamiento como *backpropagation* y *feedforward*, que se destacan por la precisión que brindan a la red para obtener predicciones en problemas reales.

A. Arquitectura de una red neuronal

Para la creación de una RNA se deben tener en cuenta algunas características (ver Figura 2), las más relevantes según [2] son:

- Relación a ser aprendida.
- Cantidad de capas, y número de neuronas por cada capa.
- Función de activación a ser usada
- Función de desempeño.
- Algoritmo de entrenamiento

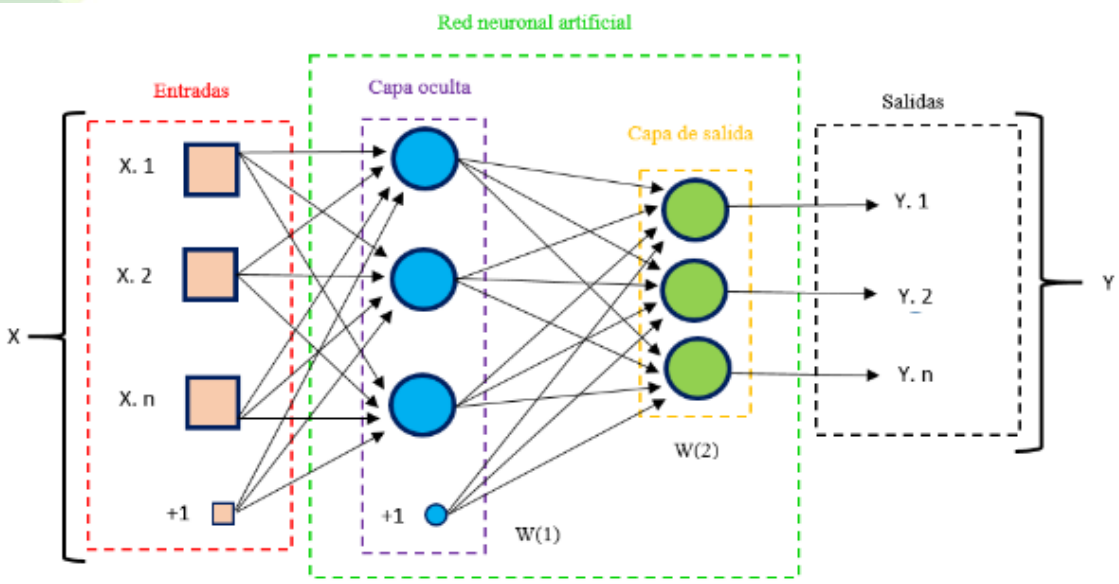

Fig. 2. Neurona Artificial.

IV. ANTECEDENTES Y RESEÑA HISTÓRICA DE LA CIBERSEGURIDAD

La ciberseguridad surge gracias a la necesidad de proteger la información, en respuesta a los diferentes ataques por software maliciosos que roban millones de datos privados de diferentes usuarios, así como también la exposición sin consentimiento de diferentes proyectos que se encuentran en desarrollo dentro de determinadas empresas; debido a esta problemática se han desarrollado diferentes estrategias para combatir el robo de datos, una de estas alternativas es la aplicación del método de inteligencia artificial, RNA. Este tipo de alternativa con aprendizaje autónomo se fortalece de cada ataque realizado a un sistema y lo puede contrarrestar con acciones preventivas que se le otorguen. Uno de los ejemplos más conocidos es la técnica de *machine learning*, aprendizaje mecánico implementado en máquinas y robots que se nutren de colecciones masivas de datos para desarrollar algoritmos y consolidar una capacidad lógica eficiente.

Como parte de esta historia y en consecuencia con los anteriores eventos, sobresale un hecho interesante en los años 80 con el nacimiento de la manifestación sobre la seguridad informática en un documento escrito por James P Anderson con el título de “Seguridad en computadores y monitoreo de amenazas y vigilancia”, pero hasta años subsiguientes fue que la IA (Inteligencia artificial) comenzó a trabajarse con el fin de mitigar las brechas de seguridad que tenían las primeras versiones de Windows y así mismo las páginas web gubernamentales financieras y empresariales de todo el mundo, ya que estas pueden ser blanco de ataques realizados por grupos conocidos como hackers que llevan a cabo ataques de denegación de servicio, por ejemplo, colapsando de esta manera las webs. Para precisar lo anterior en 1998 se siguió un criterio para seleccionar los diferentes algoritmos de aprendizaje para las RNA en el ámbito de la Seguridad de la información (SI). Estos algoritmos se entrenaron y evaluaron en conexiones normales y en un conjunto de datos de un sistema de información con miles de patrones de firmas de ataques llamado NSL, siendo esta una mejora de la base de datos KDD utilizada para la realización de la competición anual KDD CUP liderada por la Agencia de Proyectos de Investigación Avanzados de Defensa DARPA. Dicha competición propone como reto la detección de intrusos en redes informáticas, cuyo propósito es impulsar proyectos que apliquen IA para la preservación y privacidad de la información.

V. FUNCIONAMIENTO DE LAS RNA EN LA CIBERSEGURIDAD

Antes de crear una red capaz de analizar y predecir ataques, se debe contar con el volumen exacto de datos que se van a estudiar, la velocidad con la que se quieren analizar los datos y la complejidad de tratamiento de cada tipo de dato que se estudiará. Teniendo en cuenta que cada usuario genera diferentes tipos de datos, el uso de las RNA sugiere categorizar esta información, y tener cuidado a la hora de definir los datos de entrada que se proporcionarán a la red neuronal artificial para la realización de un adecuado proceso. Parte del funcionamiento de las RNA aplicadas a la ciberseguridad consiste en el uso que realizan estas de patrones de clasificación, capaces de identificar cada ataque que se ha realizado con anterioridad en los datos. Lo anterior se logra mediante una fase de entrenamiento con el propósito

de generar predicciones acertadas ante posibles vulnerabilidades y acciones alarmantes. Luego como parte de esta secuencia lógica de funcionalidad, la red debe ponerse a prueba con datos desconocidos, esto orientado a incrementar su asertividad. Al final lo que la red mostraría es una interfaz, como un programa computacional que indicará las instrucciones para su adecuado uso.

VI. ESTADO DEL ARTE DE LAS RNA APLICADAS A LA SEGURIDAD INFORMÁTICA

Dentro del trabajo efectuado se realizó una revisión de artículos enfocados a las redes neuronales aplicadas a la seguridad informática que son base para la redacción del presente artículo. Los más relevantes son:

[3] Da a conocer de forma clara y concreta la integración que existe entre Redes Neuronales y los Sistemas de Detección de Intrusos (IDS), su ayuda a los Sistemas de Información contra los ataques y amenazas. Además de realizar un análisis de las ventajas y desventajas que tiene dicha integración en los sistemas de información con respecto a su seguridad y las falencias que estas presentan al encontrarse con dichos intrusos.

[4] Diseñaron un sistema multiagente distribuido de monitoreo y alarma de eventos de seguridad en la red denominado Net-Mass. En este artículo se presentan las características del modelo de agentes distribuidos en cuanto al modelo interno del agente, la estructura organizacional y los protocolos de comunicación y notificación.

[5] Presentan una investigación que proporciona como resultado unas métricas de desempeño que dan una visión más amplia de la participación de la inteligencia artificial, en especial las redes neuronales, en el campo de la seguridad en redes informáticas. Así mismo se plantea y comprueba una nueva aproximación que implica un avance en el desarrollo de herramientas en esta área.

[6] Realizaron un proyecto IDS Inteligente que pretende unir dos ramas de la informática: el estudio y análisis de tramas para un uso en particular y la aplicación de técnicas inteligentes para tales efectos. Como resultado obtuvieron un software basado en tecnologías de última generación que captura tramas en una red de datos tradicional, las analiza y efectúa un procedimiento inteligente para identificar posibles nuevos ataques, todo basado en el análisis de puertos y una red neuronal perceptrón multicapa.

[7] Hacen una revisión de la aplicación de diferentes técnicas de inteligencia artificial aplicadas a la seguridad en sistemas informáticos. Se explica brevemente cada una de ellas y analizan la forma de aplicación y las ventajas conseguidas. Igualmente se muestran algunos proyectos realizados y la forma en que confluyen en ellos estas dos vertientes

[8] Realizaron un estudio bibliográfico relacionado con la aplicación de técnicas de Inteligencia Artificial en la Seguridad Informática, enfatizando en los Sistemas Detectores de Intrusos, detección de correo no deseado o spam, antivirus, así como otras aplicaciones en las que la utilización de la Inteligencia Artificial se considera importante.

[9] Presenta aspectos relevantes de la Inteligencia artificial y la teoría de seguridad informática aplicada a las necesidades de la red de cualquier empresa en general, los problemas abordados y las soluciones desarrolladas, también la implementación del sistema IPSVOFSL.

[10]Apunta a la detección de intrusos en la red, sin formar parte del alcance del presente proyecto de tesis, la programación de un módulo de respuesta ante ataques u otros módulos adicionales.

[11] Hicieron un estudio e identificación de la taxonomía de las amenazas que puedan llevar a un ataque en una red de datos. A partir de esta se identificaron las características más relevantes de las tramas involucradas en estos procesos con el objeto de seleccionarlas, procesarlas y clasificarlas por medio de técnicas de inteligencia artificial.

[12] Presenta los conceptos matemáticos fundamentales sobre las redes neuronales artificiales y su aplicación en la seguridad de la información, por ejemplo, intercambio de llaves.

[13] Realiza una red neuronal artificial que junto a un IDS pueda contar con baja tasa de falsos positivos, esto debido al correcto entrenamiento que junto a la base de conocimientos (base de datos) pudieran dotarle a la red un aprendizaje de alto nivel, lo que permitirá predecir los ataques además de asegurar la perdida de información sea mínima y, en consecuencia, disminuyendo la complejidad del clasificador neuronal y manteniendo estables los tiempos de entrenamiento.

[14] Proponen el diseño de una solución de ciberseguridad basada en agentes inteligentes colaborativos que permitan la detección y contención de ataques avanzados contra sistemas computacionales integrados a redes TCP/IP.

[15] Propone la comparación general de las diferentes técnicas actuales de detección de comportamiento anómalos en un sistema informático, tales como el aprendizaje de máquinas o minería de datos, así como el planteamiento de cuáles son las mejores opciones según el tipo de valor que se desea extraer de la información almacenada.

VII. ANÁLISIS DEL ESTADO DEL ARTE

[14] En su artículo *Diseño de un sistema multiagentes híbrido basado en aprendizaje profundo para la detección y contención de ciberataques*, expresa que debido al avance de tecnología la sociedad se expone a hackers maliciosos y fugas de información en las empresas. Las limitaciones a las soluciones de ciberseguridad provienen de tener un único punto de fallo, recursos de procesamiento limitados y la imposibilidad de adaptarse a los cambios de estrategia evidenciados en los ataques de última generación. Las empresas para mitigar los ataques de última generación han optado por utilizar cada vez más tecnología de diferentes fabricantes al mismo tiempo, lo que hace más complejo la gestión de la ciberdefensa.

Dentro del artículo los autores proponen un sistema de ciberseguridad distribuida multicapas y escalable compuesto por un conjunto de agentes con capacidad adaptativa que se apoyan en un sistema de aprendizaje automático avanzado, los agentes que dan solución se dividen en 3 capas:

Capa de monitorización; tiene como objetivo obtener los parámetros necesarios para facilitar la identificación de acciones maliciosas que podrían considerarse ataques contra los activos de información de cualquier empresa.

Capa de análisis: lleva a cabo las actividades de procesamiento de los parámetros obtenidos por los agentes de monitorización que son necesarios para determinar si los ordenadores en evaluación están enfrentados una situación de riesgo.

Capa de supervisión: encargada de realizar el registro de actividades de los agentes de las capas anteriores y su posterior almacenamiento persistente en una base de datos de la cual pueden extraerse reportes referentes a los eventos e incidentes de seguridad detectados.

Las ventajas de las organizaciones frente a esta propuesta son:

- Aprendizaje adaptativo que le permite evolucionar ante los cambios de estrategia de los ataques informáticos.
- Mayor confiabilidad en la detección.
- Capacidad distribuida.
- Recuperación rápida de errores
- Tolerancia a fallos.
- Cubrimiento de nuevos tipos de ataque

VIII. CONCLUSIONES

La RNA en seguridad informática muestran un mundo amplio de diferentes enfoques en los que se pueden trabajar las redes neuronales artificiales, teniendo en cuenta que la ciberseguridad se adapta a diferentes sistemas, se puede realizar una RNA con la capacidad de predecir los diferentes ataques que se encuentren en casas inteligentes (domótica).

Es posible basados en la información previamente expuesta, generar modelos de análisis basados en RNA para estudiar los diferentes ataques y mediante el aprendizaje de la red lograr programar sistemas que contrarresten estos ataques.

Mediante la implementación de algoritmos basados en RNA en la domótica es posible proteger a las diferentes familias que son víctimas de hackers, gracias a la detección de anomalías en el tráfico de paquetes de información que se envían y se recepcionan dentro del sistema inteligente instalado en el hogar.

Las redes neuronales artificiales han demostrado ser un algoritmo eficiente cuya aplicación en la seguridad informática permite hallar patrones para detectar riesgos potenciales garantizando seguridad a la hora de navegar.

Es posible concluir que, de la mano de la inteligencia artificial con enfoque hacia la seguridad, se puede reducir la cantidad de personas que son víctimas de spam, ingeniería social o cualquier otro tipo de técnica que pretenda vulnerar los sistemas o la información privada de una persona.

La presente recopilación infiere que se puede sacar ventaja en el campo de la ciberseguridad para combatir delitos informáticos, mediante las redes neuronales artificiales, como clave en la preparación y prevención de vulnerabilidades en la información de empresas como consumidores.

REFERENCIAS

[1] "Introducción a las redes neuronales aplicadas", 2019. [En línea]. Disponible en: http://halweb.uc3m.es/esp/Personal/personas/jmmarin/esp/DM/tema3dm.pdf. [Accedido: 25-Feb-2019]

[2] J. Matich, "Redes neuronales: Conceptos básicos y aplicaciones'', Mar. 2001. [En línea]. Disponible en: https://www.frro.utn.edu.ar/repositorio/catedras/quimica/5_anio/orientadora1/monograias/matich-redesneuronales.pdf. [Accedido: 23-02-2019]

[3] M. Alanoca Paco, "Integración de redes neuronales y sistemas de detección de intrusos (IDS), para las amenazas y ataques a los sistemas de información y redes", *RITS*., no. 2, pp. 32-34, May, 2009. [En línea]. Disponible en: http://www.revistasbolivianas.org.bo/scielo.php?script=sci_arttext&pid=S1997-40442009000100008&lng=en&nrm=iso

[4] Álvarez, A. Mark y L. A. Gomez Blandón, "Sistema de seguridad en redes locales utilizando sistemas multiagentes distribuidos. Net-Mass", Facultad de Ingeniería Universidad de Antioquía, no. 34, pp. 101-113, Sep. 2005. [En línea]. Disponible en: http://www.redalyc.org/articulo.oa?id=43003409

[5] A Pérez Rivera, J. A. Britto Montoya y G. A. Isaza Echeverry, "Aplicación de redes neuronales para la detección de intrusos en redes y sistemas de información", *Scientia et technica*, vol. 1, no. 27, pp. 1-6, Abr, 2005. [En línea]. Disponible en: https://revistas.utp.edu.co/index.php/revistaciencia/article/view/6943/4091

[6] N. A. García Zuluaga y R. Salgado Giraldo, "Sistema de detección de intrusos utilizando redes neuronales para la red de datos de la Universidad de Manizales", Trabajo de grado, Facultad Ciencias e ingeniería, Programa Ingeniería de sistemas y telecomunicaciones. Univ. de Manizales, Caldas, Colombia, 2007. [En línea]. Disponible en: http://ridum.umanizales.edu.co:8080/xmlui/bitstream/handle/6789/558/180_Garcia_Zuluaga_Nelson_Andres_2007.pdf?sequence=4&isAllowed=y

[7] N. D. Duque Méndez, J. C. Chavarro Porras y R. Moreno Laverde, "Seguridad inteligente", *Scientia et Technica*, vol. 3, no. 35, pp. 389-394, Ago, 2007. [En línea]. Disponible en https://dialnet.unirioja.es/descarga/articulo/4805004.pdf

[8] A.Hernández Yeja, J. De la Rosa Pasteur y O. Rodríguez Huice, "Aplicación de Técnicas de Inteligencia Artificial en la Seguridad Informática: Un estudio", *Inteligencia Artificial*, vol. 51, pp. 1-8, 2013. [En línea]. Disponible en http://journaldocs.iberamia.org/articles/979/article%20(1).pdf

[9] L. F. Villegas Pacasi, "IPSVOFSL: Sistema inteligente de prevención de intrusiones", Trabajo de Grado, Facultad Ciencias Puras y Naturales, Programa Ingeniería de sistemas informáticos., Univ. Mayor de San Andrés. La paz, Bolivia, 2009. [En línea]. Disponible en: https://repositorio.umsa.bo/bitstream/handle/123456789/1490/T-1809.pdf?sequence=1&isAllowed=y

[10] H. E. Vargas, "Sistema de detección de intrusos sobre la red basado en redes neuronales", Maestría Scientiae en Computación, Dpto. Computación., Univ. Instituto Tecnológico de Costa Rica., Cartago, Costa Rica, 2012. pp. 1-151. [En línea]. Disponible en: http://ic-itcr.ac.cr/~hesquivel/documents/Tesis.pdf

[11] L. Henao Ríos, "Definición de un modelo de seguridad en redes de cómputo, mediante el uso de técnicas de Inteligencia Artificial", Maestría en Ingeniería - Automatización Industrial, Facultad Ingeniería y Arquitectura, Dpto. Ingeniería Eléctrica y Electrónica., Univ. Nacional de Colombia., Manizales, Caldas, Colombia, 2012. pp. 1-126. [En línea]. Disponible en: http://bdigital.unal.edu.co/9044/1/7107005.2012.pdf

[12] F. Girón Araya, "Redes neuronales artificiales aplicadas a la seguridad de la información". Presentado en Nombre del Congreso de Matemática Capricornio. [En línea]. Disponible en: http://www.unap.cl/~comca/pdf/cursillo_ivan_jiron.pdf.

[13] E. Luna Domínguez, "Sistema detector de intrusos ocupando una red neuronal artificial", Maestría en ciencias de la computación, Univ. Autónoma del Estado de México., Ciudad de México, México, 2015. pp. 1-103. [En línea]. Disponible en: http://ri.uaemex.mx/bitstream/handle/20.500.11799/49966/Sistema%20Detector%20de%20Intrusiones%20Ocupando%20una%20Red%20Neuronal%20Artificial.pdf?sequence=1&isAllowed=y

[14] J. Santiago y J. Sánchez Allende, "Diseño de un sistema multiagentes híbrido basado en aprendizaje profundo para la detección y contención de ciberataques", *Revista Colombiana de Tecnologías de Avanzada*, vol. 2, no. 28, pp. 1-9, Abr, 2016. DOI: https://doi.org/10.24054/16927257.v28.n28.2016.2495

[15] N. S. Raquel, "Estudio de algoritmos de detección de anomalías y propuesta de recomendaciones para su aplicación a entornos de ciberseguridad", Trabajo de Grado, Dpto. Ingeniería Telemática., Programa Ingeniería de tecnologías y servicios de telecomunicación., Univ. Politécnica de Madrid., España, 2016. pp. 1-51. [En línea]. Disponible en: http://oa.upm.es/40490/1/PFC_RAQUEL_NOBLEJAS_SAMPEDRO_2016.pdf