Una revisión del aprendizaje profundo aplicado a la ciberseguridad

A review of deep learning applied to cybersecurity

Daniel Ivan Quirumbay Yagual [1] https://orcid.org/0000-0002-6513-3520
Carlos Andrés Castillo Yagual[1] https://orcid.org/0000-0001-6578-0480
Iván Alberto Coronel Suárez [1] https://orcid.org/0000-0002-2084-189X

[1]Universidad Estatal Peninsula de Santa Elena, UPSE | Ecuador | CP 240350

✉ dquirumbay@upse.edu.ec

http://dx.doi.org/10.26423/rctu.v9i1.671
Páginas: 57- 65

Resumen

Este estudio presenta una descripción general sobre la ciberseguridad desde la perspectiva de las redes neuronales y técnicas de aprendizaje profundo de acuerdo con las diversas necesidades actuales en ambientes de seguridad informática. Se discute la aplicabilidad de estas técnicas en diversos trabajos de ciberseguridad, como detección de intrusos, identificación de malware o botnets, phishing, predicción de ciberataques, denegación de servicio, ciberanomalías, entre otros. Para este estudio se aplicó el método analítico-sintético que sirvió para identificar soluciones óptimas en el campo de la ciberseguridad. Los resultados destacan y recomiendan algoritmos aplicables a la seguridad cibernética como base de conocimiento y facilidad para investigaciones futuras dentro del alcance de este estudio en el campo. Esta investigación sirve como punto de referencia y guía para la academia y los profesionales de las industrias de la seguridad cibernética desde el punto de vista del aprendizaje profundo.

Palabras clave: aprendizaje profundo, internet de las cosas, inteligencia artificial, redes neuronales, seguridad cibernética.

Abstract

This study presents an overview on cybersecurity from the perspective of neural networks and deep learning techniques according to the various current needs in computer security environments. It discusses the applicability of these techniques in various cybersecurity works, such as intrusion detection, malware or botnet identification, phishing, cyber attack prediction, denial of service, cyber anomalies, among others. For this study, the analytical-synthetic method was applied to identify optimal solutions in the field of cybersecurity. The results highlight and recommend algorithms applicable to cybersecurity as a knowledge base and facility for future research within the scope of this study in the field. This research serves as a reference point and guide for academia and practitioners in cyber security industries from the deep learning point of view.

Keywords: deep learning, internet of things, artificial intelligence, neural networks, cyber security

Recepción: 05 marzo 2022 | Aprobación: 24 mayo 2022 | Publicación: 30 junio 2022

1. Introducción

El crecimiento de las comunicaciones, la popularización de los dispositivos móviles e inteligentes y el avance de las tecnologías como el internet de las cosas (IoT), han aumentado su importancia y complejidad, es allí donde la ciencia de datos surge con una opción de mejorar los mecanismos de análisis de requerimientos de los sistemas cibernéticos y hacer un mejor frente a los distintos tipos de riesgos de seguridad que existen en la actualidad. La ciencia de datos puede ayudar a la seguridad de la información como también puede mantener la dinámica de análisis y desarrollo de nuevas estrategias que garanticen el mejoramiento continuo de la ciberseguridad [1].

Actualmente, se genera y recopila una gran cantidad de datos con la implementación de tecnologías en auge, como internet de las cosas (IoT) y la computación en la nube. Aunque los datos se pueden utilizar para satisfacer mejor las necesidades comerciales correspondientes, los ataques cibernéticos a menudo plantean desafíos importantes. Un ciberataque suele ser un intento malicioso y concertado por parte de una persona u organización para violentar el sistema de información de un individuo u organización. Los ataques de *malware*, *ransomware*, *Denial of Service* (DoS) o denegación de servicio, *phishing* o ingeniería social, ataques de inyección SQL, *Man-in-the-Middle* (MitM) o hombre en el medio, *Exploit* de Zero-day o *exploit* de día cero; son amenazas comunes hoy en día en el área del ciberespacio. Estos tipos de incidentes de seguridad o delitos cibernéticos pueden afectar a empresas e individuos, causar interrupciones y pérdidas financieras devastadoras. Por ejemplo, según el informe de la empresa multinacional de *software* IBM, una violación de información puede llegar a costar 8,19 millones de dólares para los Estados Unidos [2].

El programa Cibersecurity Ventures proporciona datos y estadísticas sobre seguridad cibernética, el cual prevé que los costos mundiales de la ciberdelincuencia crezcan en un 15 % anual en los próximos cinco años, pudiendo alcanzar los 10,5 billones de dólares en 2025, frente a los 3 billones de dólares en el 2015. El crimen cibernético se ha incrementado entre un 30 % y 40 % en los últimos años en América Latina [3]. Por lo tanto, proteger de manera eficaz e inteligente un sistema de información, de las diversas amenazas cibernéticas, ataques, daños o accesos no autorizados, es un tema clave que debe resolverse con urgencia, siendo objeto de este estudio.

En general, la ciberseguridad se caracteriza como una colección de tecnologías y procesos diseñados para proteger computadoras, redes, programas y datos contra actividades maliciosas, ataques, daños o acceso no autorizados [4]. De acuerdo con las numerosas necesidades actuales, las soluciones de seguridad convencionales conocidas, como antivirus, *firewall*, autenticación de usuarios, cifrado, etc., pueden no ser efectivas, el problema con estos sistemas es que normalmente son operados por unos pocos analistas de seguridad, donde la gestión de datos se lleva a cabo de manera *ad hoc*, sin trabajar inteligentemente de acuerdo a las necesidades [5]. Por otro lado, la necesidad de operar de manera inteligente para la gestión de la ciberseguridad con técnicas de aprendizaje basadas en datos, cada vez es más común su uso en las empresas, y evoluciona rápidamente con el pasar de los años.

La seguridad inteligente combina aspectos del aprendizaje automático e inteligencia artificial, con aplicación a la seguridad tradicional; tendencia innovadora en estos últimos tiempos. Las herramientas son más capaces de adaptarse a nuevas amenazas y asegurar nuevos tipos de aplicaciones tal como lo expresa Panda Security [6]. Como fortaleza aprende en tiempo real y permite desarrollar los nuevos criterios de clasificación sin intervención humana. Por ejemplo, se aplica contra el *malware* y el fraude *online*, debido a los cibercriminales que evolucionan rápidamente generando amenazas capaces de adaptarse a la seguridad de los sistemas. Por consiguiente, *Deep Learning* es capaz de detectar y clasificar dichas amenazas y poner una solución de forma eficiente y veloz [6].

En este documento, se toma en cuenta varias redes neuronales populares y técnicas de aprendizaje profundo, que incluyen aprendizaje supervisado, semi-supervisado y no supervisado en el contexto de la ciberseguridad; siendo estos los más utilizados para el desarrollo de algoritmos en seguridad de la información, estos son perceptrón multicapa (MLP), red neuronal convolucional (CNN o ConvNet), red neuronal recurrente (RNN) o memoria a corto plazo (LSTM) y transferencia profunda aprendizaje (DTL o TL profundo). Estas técnicas de aprendizaje de redes neuronales profundas y enfoques híbridos, se pueden utilizar para resolver de manera inteligente diferentes problemas de ciberseguridad, tales como detección de intrusos, identificación de *malware* o *botnet*, *phishing*, predicción de ciberataques, DoS, detección de fraude o ciberanomalías. El aprendizaje profundo tiene beneficios en la construcción de modelos de seguridad, debido a su alta precisión para aprender con grandes cantidades de conjuntos de datos de seguridad [7].

La contribución de esta investigación, contiene en la sección dos un detalle de las técnicas en redes neuronales artificiales (RNA) y *deep learning* (DL), siendo estos parte de la inteligencia artificial (IA) para el funcionamiento oportuno, automatizado e inteligente en el contexto de ciberseguridad, siendo estos parte de las tecnologías de Cuarta Revolución Industrial (Industria 4.0) [8]. En la sección tres se revisa y discute varias redes neuronales populares

y técnicas de aprendizaje profundo, incluido el aprendizaje supervisado, no supervisado en el contexto de la seguridad cibernética, así como la aplicabilidad y alcance. Finalmente, se destaca varios temas de investigación y direcciones futuras dentro del alcance de este estudio para el desarrollo y la investigación en temas de la ciberseguridad.

En efecto, el objetivo final de esta investigación fue servir como punto de referencia a profesionales e industrias de la seguridad cibernética desde el punto de vista del aprendizaje profundo.

2. Materiales y métodos

2.1. Marco teórico y referencial

Deep learning y redes neuronales artificiales

El aprendizaje profundo (DL) suele considerarse parte de una familia más amplia de métodos de aprendizaje automático, así como de la inteligencia artificial (IA); estos tienen su origen en las redes neuronales artificiales (RNA) [9]. La principal ventaja del aprendizaje profundo frente a los métodos tradicionales de aprendizaje automático, es el alto rendimiento en variedad de casos, especialmente en el aprendizaje a partir de grandes cantidades de conjuntos de datos de seguridad [7]. A continuación, analizamos cuatro técnicas populares de redes neuronales y de aprendizaje profundo, en el contexto de la ciberseguridad. Estas técnicas y sus modelos de seguridad híbridos pueden utilizarse para abordar de forma inteligente diferentes problemas de ciberdelitos, como la detección de intrusiones, el análisis de *malware*, el análisis de amenazas de seguridad, la predicción de ciberataques o anomalías, etc.

Perceptrón multicapa (MLP *MultiLayer Perceptron*)

Es un algoritmo de aprendizaje supervisado, también se considera como una arquitectura base del aprendizaje profundo o redes neuronales profundas (DNN). Una MLP típica es una red totalmente conectada, que consiste en una capa de entrada que recibe los datos; una capa de salida para tomar una decisión o predicción sobre la señal de entrada; y una o más capas ocultas entre estas dos [10], al que se considera como el verdadero motor computacional de la red, tal como se muestra en la Figura 1.

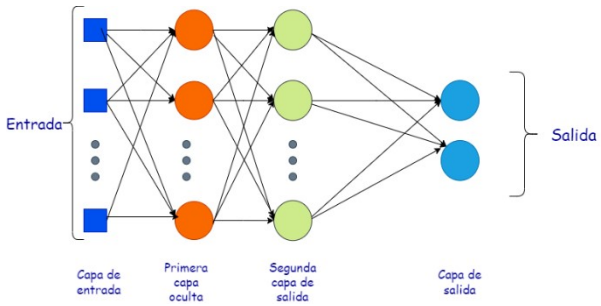

Figura 1: Multi-Capa Perceptron

MLP está totalmente enlazado, cada nodo de una capa se conecta con un determinado peso a cada nodo de la capa siguiente. Se utilizan varias funciones de activación como ReLU (Rectified Linear Unit) que determinan la salida de una red. Estas funciones de activación, también conocidas como funciones de transferencia, introducen propiedades no lineales en la red para aprender mapas funcionales complejos a partir de los datos [11]. Además, MLP utiliza una técnica de aprendizaje supervisado para el entrenamiento, llamado $BackPropagation$, este bloque de construcción es fundamental en una red neuronal; este algoritmo es ampliamente utilizado para el entrenamiento de redes neuronales $feedforward$ [12]. El objetivo del algoritmo $BackPropagation$ es optimizar los pesos de la red para asignar con precisión las entradas a las salidas objetivo.

Durante el proceso de entrenamiento se utilizan varias técnicas de optimización, como el descenso gradiente estocástico. Estas redes neuronales son aplicables, por ejemplo, en la construcción de un modelo de detección de intrusiones [13], el análisis de amenazas a la seguridad [14], así como la construcción de sistemas de IoT confiables [15]. MLP es muy sensible al escalado de características y necesita una serie de hiperparámetros, como el número de capas ocultas, las neuronas y las iteraciones que hay que ajustar; esto es lo que hace al modelo computacionalmente costoso para resolver problemas de seguridad complejas.

Red neuronal convolucional (CNN *Convolutional Neural Networks)*

Es un modelo de red de aprendizaje profundo que aprende directamente de los datos, sin necesidad de extracción manual de características. Una CNN típica consta de una capa de entrada, capas convolucionales, capas de agrupación, capas totalmente conectadas y una capa de salida, como se muestra en la Figura 2.

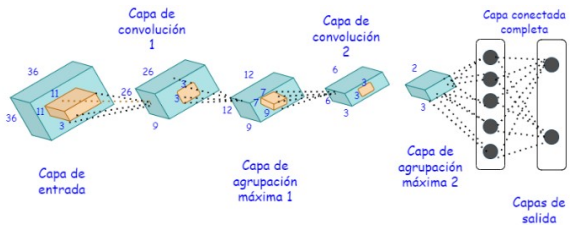

Figura 2: Red neuronal convolucional

Cada una de las capas de la CNN considera parámetros optimizados para obtener resultados significativos, así como para reducir la complejidad. Las redes neuronales convolucionales están diseñadas específicamente para tratar la variabilidad de imágenes en formas 2D. En términos de áreas de aplicación, las CNN se utilizan ampliamente en el reconocimiento de imágenes y vídeos, el análisis de imágenes médicas, los sistemas de recomendación, la clasificación de imágenes, la segmentación de imágenes, el procesamiento del

lenguaje natural, las series temporales financieras, etc. Esta arquitectura se aplica más comúnmente en el análisis de imágenes visuales, estas redes también pueden utilizarse en el ámbito de la ciberseguridad. Por ejemplo, el modelo de aprendizaje profundo basado en CNN que se utiliza para la detección de intrusiones, o en el ataques de denegación de servicio (DoS), redes IoT [16], detección de malware [17], detección de malware en Android [18], etc. Esta red neuronal artificial tiene una mayor carga computacional, pero tiene la ventaja de detectar automáticamente las características importantes sin ninguna supervisión humana, por lo que se considera que la CNN es una buena alternativa para generar soluciones de seguridad informática aplicadas.

Red neuronal recurrente de memoria a corto plazo (LSTM *Long Short Term Memory* – RNN *Recurrent Neural Networks)*

Es una red neuronal artificial, capaz de procesar una secuencia de entradas en el aprendizaje profundo y retener su estado mientras procesa la siguiente secuencia de entradas. Todas las RNN tienen bucles de retroalimentación en la capa recurrente, lo que les permite mantener la información en la ”memoria.ª lo largo del tiempo. Las redes de memoria a corto plazo (LSTM) son un tipo de RNN que utiliza unidades especiales, además de las unidades estándar, que pueden hacer frente al problema del gradiente de fuga. Las unidades LSTM tienen una çelda de memoria”que puede almacenar datos durante largos períodos en la memoria, donde ’forget gate’, ’input gate’ y ’output gate’ trabajan de forma cooperativa para controlar el flujo de información en una unidad LSTM.

Las redes LSTM son muy adecuadas para el aprendizaje y el análisis de datos secuenciales, como la clasificación, el procesamiento y la realización de predicciones basadas en datos de series temporales; lo que la diferencia de otras redes convencionales. Sin embargo, la LSTM se aplica comúnmente en el área de predicción de series temporales, detección de anomalías en series temporales, procesamiento de lenguaje natural, chatbots de respuesta a preguntas, traducción automática, reconocimiento de voz, etc.

Dado que en la actualidad se genera una gran cantidad de datos secuenciales de seguridad, como flujos de tráfico de red, actividades maliciosas dependientes del tiempo, etc., un modelo LSTM también puede ser aplicable en el ámbito de la ciberseguridad, debido al estudiado de varias soluciones de seguridad basadas en este, como la detección y clasificación de aplicaciones maliciosas [17], y la detección de phishing [19]. Aunque la principal ventaja de una red recurrente sobre una red tradicional es la capacidad de modelar la secuencia de datos, puede requerir muchos recursos y tiempo para ser entrenada. Por consiguiente, teniendo en cuenta la ventaja mencionada, una red LSTM-RNN eficaz puede mejorar los modelos de seguridad para detectar las amenazas, en particular, cuando los patrones de procedimiento de las amenazas muestran un comportamiento dinámico temporal, Figura 3.

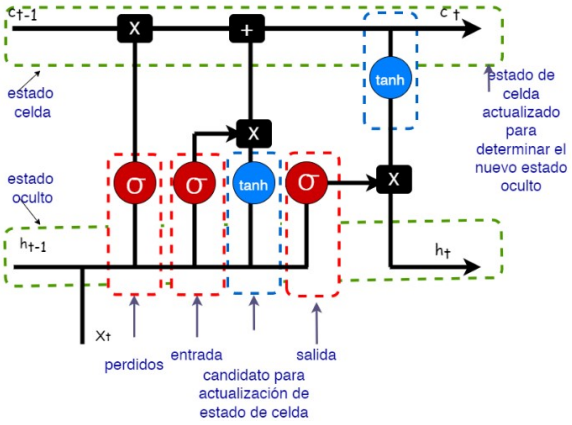

Figura 3: Red neuronal recurrente

Aprendizaje profundo por transferencia (DTL *Deep Transfer Learning)* o Deep TL

Este método permite resolver problemas fundamentales de datos de entrenamiento inadecuados. De esta forma, elimina la necesidad de entrenar modelos de inteligencia artificial (IA), esto permite entrenar redes neuronales con cantidades relativamente pequeñas de datos. En el campo de la ciencia de datos, es actualmente muy común su uso, considerando que en la mayoría de los problemas del mundo real no suelen tener millones de puntos de datos etiquetados para entrenar modelos tan complejos. El aprendizaje profundo por transferencia (DTL) puede clasificarse en tres sub-configuraciones:

- Aprendizaje por transferencia inductiva
- Aprendizaje por transferencia transductiva
- Aprendizaje de transferencia no supervisado

En la Figura 4 se muestra una gráfica del funcionamiento de un aprendizaje profundo por transferencia.

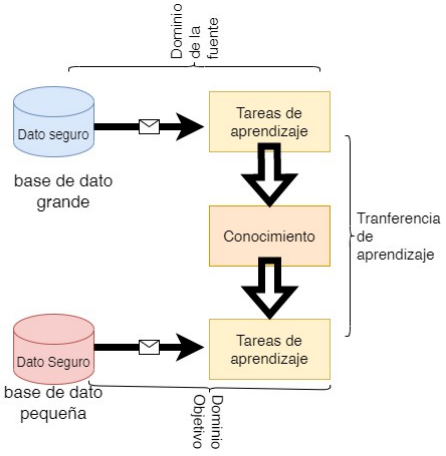

Figura 4: Red neuronal recurrente

El aprendizaje profundo por transferencia es aplicable en varias áreas tales como: la visión por computadora, la clasificación de imágenes, el reconocimiento del habla, las imágenes médicas y el filtrado de spam, etc. En el ámbito de la ciberseguridad, también desempeña un papel importante debido a sus diversas ventajas en el modelado, como el ahorro de tiempo de entrenamiento, la mejora de la precisión de los resultados y la necesidad de menos datos de entrenamiento. Por ejemplo, los autores Wu y Guo (2019) presentan un modelo ConvNet que utiliza el aprendizaje de transferencia para la detección de intrusiones en la red [20]. Nahamias (2020), proponen un método de generación de firmas basado en el aprendizaje de transferencia de características profundas que reduce drásticamente el tiempo de generación y distribución de firmas [21]. En este método se ha conseguido una precisión de clasificación superior al 99,5 % [22]. Los autores abordaron el aprendizaje de transferencia para la identificación de ataques de red desconocidos en donde presentan un enfoque de aprendizaje de transferencia basado en características, utilizando una transformación lineal [23]. El sistema de aprendizaje de transferencia acelera significativamente el entrenamiento de redes neuronales profundas al tiempo que conserva una alta eficiencia en el campo de la seguridad cibernética, incluso en conjuntos de datos más pequeños. Por lo tanto, en lugar de entrenar la red neuronal desde cero, los profesionales de la ciberseguridad pueden tener un modelo de aprendizaje profundo de código abierto previamente entrenado y ajustarlo a su propósito.

2.2. Materiales y Métodos

La metodología de esta investigación se centró en la aplicación del método analítico-sintético para abordar de forma detallada, el estudio de cuatro algoritmos de aprendizaje profundo.

Estas alternativas de redes neuronales artificiales y aprendizaje profundo fueron analizadas con el fin de adecuar una solución óptima en el campo de la ciberseguridad. Para ello, se parte de la revisión funcional de varios algoritmos utilizados en ambientes de trabajo donde se han detectado vulnerabilidades de la seguridad de la información, tales como: detección de intrusos, identificación de *malware* o botnets, *phishing*, predicción de ciberataques, denegación de servicio, ciberanomalías. Además, del estado del arte con recopilación de datos realizados por diversos autores referenciados en este artículo.

En base a la revisión de la literatura realizada, se plantea la recomendación clave en el uso de algoritmos aplicables, según el área de estudio e investigación en la seguridad cibernética.

3. Discusión y resultados

3.1. Estudio de modelos

En esta sección, se resume y discute los retos a los que se enfrenta el mundo y las posibles oportunidades de investigaciones futuras para hacer que las redes y los sistemas de información sean seguros, automatizados e inteligentes.

La eficacia y la eficiencia de una solución de seguridad basada en redes neuronales artificiales y aprendizaje profundo dependen de la naturaleza y las características de los datos de seguridad, así como del rendimiento de los algoritmos de aprendizaje. El lograr recoger los datos de seguridad en el ámbito de la ciberseguridad no es un trabajo sencillo. Por lo tanto, es necesario investigar más a fondo los métodos de recopilación de datos cuando se trabaja con registros relacionados con la ciberseguridad. Los datos históricos de seguridad recolectados en un análisis podrían contener muchos valores ambiguos, valores perdidos, valores atípicos y datos sin sentido.

Se entiende que, los algoritmos de aprendizaje supervisado y no supervisado tienen un gran impacto en la calidad de los datos y en la calidad de la información. Además, de limpiar y preprocesar con precisión los diversos datos de seguridad recogidos de varias fuentes. Sin embargo, se requieren métodos de preprocesamiento existentes o proponer nuevas técnicas de preparación de datos para utilizar eficazmente los algoritmos de aprendizaje en el ámbito de la ciberseguridad.

Con lo argumentado, se puede entender que la selección de un algoritmo de aprendizaje adecuado para la aplicación especifica en el contexto de la ciberseguridad, es un reto como lo expresa Sarker (2021) [24]. La razón es que el resultado de diferentes algoritmos de aprendizaje puede variar dependiendo de las características de los datos tal como describen Sarker *et al*. (2019) [25]. Para la realización del estudio se considera varios puntos clave de estas técnicas (Tabla 1), donde se detallan los cuatro métodos tratados en el documento. No obstante, la selección de un algoritmo de aprendizaje incorrecto daría lugar a resultados inesperados que podrían suponer una pérdida de esfuerzo, así como de eficacia y precisión del modelo. En la siguiente tabla se resumen cómo estas redes neuronales y aprendizaje profundo pueden ser aplicadas a la ciberseguridad.

Tabla 1: Resumen de las redes neuronales artificiales (RNA) y de las redes de aprendizaje profundo (DL)

Red neuronal artificial (RNA) y aprendizaje profundo (DL)	Descripción	Aplicable en el campo de la ciberseguridad
Multi-capa perceptron (MLP)	Es un algoritmo de aprendizaje supervisado. Una red neuronal artificial totalmente conectada de tipo feed-forward.	Útil para la detección de intrusiones, análisis de malware, detección de tráfico de malware o botnets, análisis de amenazas a la seguridad.
Red neuronal convolucional(CNN)	Es una versión regularizada de los perceptrones multicapa. Pueden aprender o detectar automáticamente las características clave de los datos. Comúnmente trabaja con la variabilidad de las formas en 2D, por ejemplo, la imagen. .	Útil para la detección de intrusos, detección de malware, detección de phishing, detección de usuarios maliciosos
Red neuronal recurrente de memoria a corto plazo (LSTM-RNN)	Conveniente para el aprendizaje y el análisis de los datos secuenciales. Preferido para tareas de procesamiento de lenguaje natural, procesamiento del habla y realización de predicciones basadas en datos de series temporales.	Útil para detección de intrusiones, detección de actividades maliciosas, detección de phishing, detección de malware o botnet basada en el tiempo, modelado de autenticación
Aprendizaje profundo por transferencia (DTL o Deep TL)	Puede resolver el problema básico de la insuficiencia de datos en el entrenamiento de la red neuronal. Utilizar el modelo pre-entrenado y el conocimiento se transfiere de un modelo a otro. Posee varias ventajas en el modelado, tales como el ahorro de tiempo de entrenamiento, la mejora de la precisión de los resultados y la necesidad de requerir menos datos de entrenamiento.	Útil para sistema de detección de intrusos, detección de ataques desconocidos o anómalos en la red, detección de malware, clasificación de software malicioso.

Del mismo modo, se debe conocer que, si los datos de seguridad son malos, como características no representativas, de baja calidad o irrelevantes, o una cantidad insuficiente para el entrenamiento, los modelos de seguridad de aprendizaje profundo pueden resultar inútiles o producir una precisión menor. Por lo tanto, los datos de seguridad relevantes y de calidad son importantes, para obtener mejores resultados para la toma de decisiones en la empresa.

Se conoce que los algoritmos de DL supervisados tienen una amplia aplicación en el análisis de *malware*, pero menos en la detección de intrusiones; la detección de *spam* se basa únicamente en algoritmos de DL no supervisados.

Como era de esperar, el número total de algoritmos basados en *Deep Learning* (DL) es considerablemente menor que los basados en *Machine Learning* (ML); de hecho, las propuestas de aprendizaje profundo (DL) basadas en enormes redes neuronales son más recientes que los enfoques de ML; este vacío abre muchas oportunidades de investigación como lo sustentan Geetha y Thilagam [26], Tabla 2.

Tabla 2: Lista de algoritmos de *Deep learning* aplicados en problema de seguridad cibernética

		Detección de intrusos		Análisis de malware	Detección de SPAM	Phishing	Usuarios maliciosos	Datos anómalos
		Redes	Botnet					
Deep Learning	Supervisado	Redes neuronales profundas recurrentes (RNN).	Redes neuronales profundas recurrentes (RNN). Multi-capa Perceptron (MLP).	Redes neuronales profundas totalmente conectadas (FNN) Red Neuronal convolucional (CNN). Redes neuronales profundas recurrentes (RNN). Multi-capa Perceptron (MLP).		Red Neuronal convolucional (CNN)	Red Neuronal convolucional (CNN) Red neuronal recurrente de memoria a corto plazo	Aprendizaje profundo por transferencia (DTL)
	No supervisado	Redes neuronales profundas (DBN). Autocodificadores apilados (SAE).		Redes neuronales profundas (DBN). Autocodificadores apilados (SAE).	Redes neuronales profundas (DBN). Autocodificadores apilados (SAE).			

4. Conclusiones

El presente documento forja un estudio que permite conseguir una visión general de la ciberseguridad desde la perspectiva de las redes neuronales artificiales y los métodos de aprendizaje profundo. También se revisa estudios recientes de cuatro redes neuronales para llegar a un análisis y comparación especifica de este trabajo. Además, de acuerdo con el objetivo planteado, se ha discutido brevemente cómo varios tipos de redes neuronales y métodos de aprendizaje profundo pueden ser utilizados para soluciones de ciberseguridad en diversas condiciones.

Permite generar una apreciación más clara de que en toda solución de seguridad informática exitosa se puede aplicar al menos un modelado de aprendizaje profundo pertinente en función de las características de los datos. Los algoritmos de aprendizaje profundo deben ser entrenados a través de los datos de seguridad recogidos y el conocimiento relacionado con la aplicación para que pueda ayudar a tomar decisiones inteligentes.

Se logra entender que, el estudio sobre las redes neuronales y el análisis de seguridad basado en el aprendizaje profundo se convierte en una guía de referencia para la investigación y las aplicaciones potenciales, tanto para el mundo académico como para los profesionales de la industria en el ámbito de la ciberseguridad, tomando como bases cada una de las citas registradas que dan un ejemplo de la aplicabilidad en este ámbito.

En general, se concluye que el éxito de una solución de seguridad basada en datos depende tanto de la calidad de los datos de seguridad como del rendimiento de los algoritmos de aprendizaje. Finalmente, queda para futuros debates los retos y mejoras que proporcione este campo de la ciencia de datos que va evolucionando con el transcurso de los años.

5. Referencias

1. NAVARRO, Andrés; URCUQUI, Christian; OSORIO, José y GARCÍA, Melisa. *Ciberseguridad: un enfoque desde la ciencia de datos* [En línea]. Universidad Icesi, 2019 [Consulta: 28 abr. 2022]. Disp. desde DOI: doi:10.18046/EUI/ee.4.2018.

2. SECURITY, IBM. IBM: Cost of a Data Breach Report 2019. *Computer Fraud & Security* [En línea]. 2019, vol. 2019, n.º 8, págs. 4-4. ISSN 1361-3723. Disp. desde DOI: 10.1016/s1361-3723(19)30081-8.

3. MORGAN, Steve. Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics. *Cybercrime Magazine* [En línea]. 2022 [Consulta: 28 abr. 2022]. Disponible en: https://cybersecurityventures.com/cybersecurity-almanac-2022.

4. AFTERGOOD, Steven. Cybersecurity: The cold war online. *Nature 2017 547:7661* [En línea]. 2017, vol. 547, n.º 7661, págs. 30-31. ISSN 1476-4687. Disp. desde DOI: doi:10.1038/547030a.

5. FOROUGHI, Farhad y LUKSCH, Peter. Data Science Methodology for Cybersecurity Projects [En línea]. 2018, págs. 1-14. Disp. desde DOI: 10.5121/csit.2018.80401.

6. Tendencias de ciberseguridad para 2020. *Panda Security* [En línea]. 2019 [Consulta: 29 abr. 2022]. Disponible en: https://www.pandasecurity.com/spain/mediacenter/mobile-news/tendencias-ciberseguridad-2020/.

7. XIN, Yang; KONG, Lingshuang; LIU, Zhi; CHEN, Yuling; LI, Yanmiao; ZHU, Hongliang; GAO, Mingcheng; HOU, Haixia y WANG, Chunhua. Machine Learning and Deep Learning Methods for Cybersecurity. *IEEE Access* [En línea]. 2018, vol. 6, págs. 35365-35381. ISSN 21693536. Disponible en: 10.1109/ACCESS.2018.2836950.

8. JOYANES, Luis. Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0). *Cuadernos de estrategia*. 2017, n.º 185, págs. 19-64. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6115620.

9. SARKER, Iqbal; KAYES, A.; BADSHA, Shahriar; ALQAHTANI, Hamed; WATTERS, Paul y NG, Alex. Cybersecurity data science: an overview from machine learning perspective. *Journal of Big Data* [En línea]. 2020, vol. 7, n.º 1. ISSN 21961115. Disp. desde DOI: 10.1186/s40537-020-00318-5.

10. SARKER, Iqbal; FURHAD, M. y NOWROZY, Raza. AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. *SN Computer Science* [En línea]. 2021, vol. 2, n.º 3, págs. 1-18. ISSN 2662-995X. Disp. desde DOI: 10.1007/s42979-021-00557-0.

11. AGARAP, Abien. Deep Learning using Rectified Linear Units (ReLU) [En línea]. 2018. Disponible en: http://arxiv.org/abs/1803.08375.

12. ZAJMI, Leke; AHMED, Falah y JAHARADAK, Amril. Concepts, Methods, and Performances of Particle Swarm Optimization, Backpropagation,

and Neural Networks. *Applied Computational Intelligence and Soft Computing* [En línea]. 2018. ISSN 16879732. Disp. desde DOI: 10.1155/2018/9547212.

13. DE ALMEIDA, Felipe; MORENO, Edward; MACEDO, Hendrik; DE BRITO, Ricardo; DO NASCIMIENTO, Filipe y OLIVEIRA, Flavio. Concepts, Methods, and Performances of Particle Swarm Optimization, Backpropagation, and Neural Networks. *Applied Computational Intelligence and Soft Computing* [En línea]. 2018. ISSN 16879732. Disp. desde DOI: 10.1155/2018/9547212.

14. HODO, Elike; BELLEKENS, Xavier; HAMILTON, Andrew; DUBOUILH, Pierre-Louis; IORKYASE, Ephraim; TACHTATZIS, Christos y ATKINSON, Robert. Concepts, Methods, and Performances of Particle Swarm Optimization, Backpropagation, and Neural Networks. *Applied Computational Intelligence and Soft Computing* [En línea]. 2018. ISSN 16879732. Disp. desde DOI: 10.1155/2018/9547212.

15. PANIAGUA, Omar; HERNÁNDEZ, Juan; RUIZ, Juan; REYES, Mauricio; FERREIRA, Heberto y HERNÁNDEZ, Anastasio. Diseño De Un Prototipo Iot Para Pruebas De Penetración Y Monitoreo De La Seguridad En Un Sistema De Domótica [En línea]. 2019, pág. 14. Disponible en: https://www.researchgate.net/profile/Juan_Roberto_Hernandez_Herrera2/publication/339136248_Diseno_de_un_prototipo_IoT_para_pruebas_de_penetracion_y_monitoreo_de_la_seguridad_en_un_sistema_de_domotica/links/5e403bbda6fdccd9659620d4/Diseno-de-un-prototipo-I.

16. SUSILO, Bambang y SARI, Riri. Intrusion detection in IoT networks using deep learning algorithm. *Information (Switzerland)* [En línea]. 2020, vol. 11, n.º 5. ISSN 20782489. Disp. desde DOI: 10.3390/INFO11050279.

17. YAN, Jinpei; QI, Yong y RAO, Qifan. Detecting Malware with an Ensemble Method Based on Deep Neural Network. *Security and Communication Networks* [En línea]. 2018. ISSN 19390122. Disp. desde DOI: 10.1155/2018/7247095.

18. MCLAUGHLIN, Niall; DEL RINCÓN, Jesús; KANG, Boo; YERIMA, Suleiman; MILLER, Paúl; SEZER, Sakir; SAFAEL, Yeganeh; TRICKEL, Erik; ZHAO, Ziming; DOUPE, Adam y AHN, Gail. Detecting Malware with an Ensemble Method Based on Deep Neural Network. *Security and Communication Networks* [En línea]. 2018. ISSN 19390122. Disp. desde DOI: 10.1155/2018/7247095.

19. ADEBOWALE, Moruf; LWIN, Khin y HOSSAIN, M. Intelligent phishing detection scheme using deep learning algorithms. *Journal of Enterprise Information Managemen* [En línea]. 2020. ISSN 17410398. Disp. desde DOI: 10.1108/JEIM-01-2020-0036.

20. WU, Peliun; GUO, Hui y BUCKLAND, Richard. A Transfer Learning Approach for Network Intrusion Detection. *2019 4th IEEE International Conference on Big Data Analytics, ICBDA 2019* [En línea]. 2019, págs. 281-285. Disp. desde DOI: 10.1109/ICBDA.2019.8713213.

21. NAHMIAS, Daniel; COHEN, Aviad; NISSIM, Nir y ELOVICI, Yuval. Deep feature transfer learning for trusted and automated malware signature generation in private cloud environments. *Neural Networks* [En línea]. 2020, vol. 124, págs. 243-257. ISSN 18792782. Disp. desde DOI: 10.1016/j.neunet.2020.01.003.

22. NAHMIAS, Daniel; COHEN, Aviad; NISSIM, Nir y ELOVICI, Yuval. TrustSign: Trusted Malware Signature Generation in Private Clouds Using Deep Feature Transfer Learning. *Proceedings of the International Joint Conference on Neural Networks* [En línea]. 2019, págs. 1-8. ISSN 18792782. Disp. desde DOI: 10.1109/IJCNN.2019.8851841.

23. ZHAO, Juan; SHETTY, Sachin; PAN, Jan; KAMHOUA KAMHOUA, Charles y KWIAT, Kevin. Transfer learning for detecting unknown network attacks. *Eurasip Journal on Information Security* [En línea]. 2019, n.º 1. ISSN 2510523X. Disp. desde DOI: 10.1186/s13635-019-0084-4.

24. SARKER, Iqbal. Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective. *SN Computer Science* [En línea]. 2021, vol. 2, n.º 3. ISSN 2662-995X. Disp. desde DOI: 10.1007/s42979-021-00535-6.

25. SARKER, Iqbal; KAYES, A y WATTERS, Paul. Effectiveness analysis of machine learning classification models for predicting personalized context-aware smartphone usage. *Journal of Big Data* [En línea]. 2019, vol. 6, n.º 1. ISSN

21961115. Disp. desde DOI: 10.1186/s40537-019-0219-y.

26. GEETHA, R. y THILAGAM, T. A Review on the Effectiveness of Machine Learning and Deep Learning Algorithms for Cyber Security. *Archives of Computational Methods in Engineering* [En línea]. 2021, vol. 28, n.º 4, págs. 2861-2879. ISSN 18861784. Disp. desde DOI: 10.1007/s11831-020-09478-2.