TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 21 No. 1, Enero-Marzo, p.48- 55 ISSN 1729-3804

SISTEMA DE DETECCIÓN Y RECONOCIMIENTO DE AMENAZAS DE CIBERSEGURIDAD EN LA NUBE

Ariel Baloira Reyes[1]

[1]Universidad Tecnológica de la Habana "José Antonio Echeverría" (CUJAE), Cuba
[1]e-mail: ariel@tele.cujae.edu.cu

RESUMEN

En la actualidad, la ciberseguridad se ha convertido en una obligación para todo proveedor de servicios. Mientras existen grupos de personas orientadas a explotar los servicios con fines malignos, otros desarrollan herramientas y mecanismos para defenderlos. El presente trabajo está orientado a este último grupo. Los usos del aprendizaje automático son disimiles y variados. Las capacidades de los algoritmos empleados permiten su integración con el campo de la ciberseguridad. Como paradigma del contexto actual, los servicios en la nube se han vuelto la diana para los ciberataques, pero de igual forma se puede emplear su potencial para hacerles frente. En función de ello, se ofrece una solución en la nube para emplear el aprendizaje automático en la ciberseguridad.

PALABRAS CLAVES: Ciberseguridad, Aprendizaje automático, Computación en la nube.

CLOUD CYBERSECURITY THREAT RECOGNITION AND DETECTION SYSTEM

ABSTRACT

Today, cybersecurity has become an obligation for every service provider. While there are groups of people oriented to exploit services for malicious purposes, others develop tools and mechanisms to defend them. The present work is oriented to this last group. The uses of machine learning are dissimilar and varied. The capabilities of the algorithms used allow their integration with the cybersecurity field. As a paradigm of the current context, cloud services have become the target for cyberattacks, but their potential can also be used to deal with them. Based on this, a cloud solution is offered to use machine learning in cybersecurity.

INDEX TERMS: Cybersecurity, Machine-Learning, Cloud Computing.

1. INTRODUCCIÓN

En los últimos años, el cibercrimen se ha manifestado de diferentes formas, con un aumento constante tanto en cantidad como en complejidad [1], [2]. En respuesta, los especialistas en ciberseguridad han desarrollado mecanismos de defensas para socavar estas actividades delictivas. A consideración del autor cada solución tecnológica de este tipo basa su funcionamiento en tres etapas: detección, reconocimiento y solución.

El principio de la detección es la monitorización en búsqueda de anomalías de seguridad. En esta etapa se monitorea el entorno, buscando *malware*, conexiones no habituales, correos maliciosos y cualquier otra actividad fuera de lo común. En la etapa de reconocimiento se revisan los registros y se indaga, buscando correlación de eventos y obteniendo toda la información posible. Conociendo que se está bajo un ataque, es importante precisar la fuente, que tipo de ataque es, a qué o a quién está dirigido y otros elementos relevantes que puedan ayudar a clasificarlo y detenerlo. La última etapa es la reacción del sistema de defensa. En ella se realizan acciones para mitigar el tipo de ataque al cual se enfrenta el sistema.

Este trabajo se centra en las dos primeras etapas, donde el aprendizaje automático tiene varios campos de acción. El aprendizaje automático (ML, por las siglas del término en inglés, *Machine-Learning*) es un campo dentro de la Inteligencia Artificial (AI, por las siglas del término en inglés, *Artificial Intelligence*) que mediante algoritmos matemáticos dota a los ordenadores con la capacidad de identificar patrones en datos masivos para realizar predicciones [3].

Manuscrito recibido: 19-08-2022, aceptado: 18-11-2022
Sitio web: http://revistatelematica.cujae.edu.cu/index.php/tele

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 21 No. 1, Enero-Marzo, p.48- 55 ISSN 1729-3804

A pesar de las cualidades del ML, se requieren de grandes cantidades de recursos de cómputo para su funcionamiento. La computación en la nube (CC, por las siglas del término en inglés, *Cloud Computing*) brinda los recursos necesarios para aprovechar al máximo los veneficios del ML. La CC ha permitido que se comercialicen y empleen servicios de infraestructura, plataforma y software de manera sencilla y accesible para todos desde cualquier lugar. Por estas razones se propone el empleo del Aprendizaje Automático como un Servicio (MLaaS, por las siglas del término en inglés, *Machine-Learning as a Service*) para detectar anomalías de ciberseguridad.

2. APLICACIÓN DEL APRENDIZAJE AUTOMÁTICO EN LA CIBERSEGURIDAD

Cada día se hacen públicas vulnerabilidades de equipos y sistemas a los cuales sus desarrolladores le dan solución para evitar ataques [4]–[9]. A pesar de esto, existen fallas conocidas como *exploit* de día cero (término en inglés, *zero day exploit*) las cuales son inexistentes para los desarrolladores y pueden ser empleadas para comprometer los servicios.

Por lo tanto, depender de un solo mecanismo de seguridad no es eficiente ni seguro. Se debe implementar lo que se conoce como modelo de defensa en profundidad. El cual se basa en la idea de poseer múltiples mecanismos de seguridad, independientemente de cuán fuerte parezca alguno de ellos. Se requiere desplegar cortafuegos, antivirus, constante actualización de los sistemas operativos, sistemas de detección y prevención de intrusos, entre otros [10]–[12].

El sistema que se propone sería un nivel adicional de protección, donde el ML tiene varios campos de acción. El aprendizaje automático se está desarrollando y aplicando en varias áreas de la sociedad, una de ellas es la seguridad informática. Su aplicación permite la detección de ataques, intrusos y *bots*, así como de fraudes *online* y con tarjetas de crédito. También permite detectar ataques de día cero, anomalías, correos no deseados y otras amenazas dependiendo de los vectores de infección. En la Fig. 1 se muestran algunos ejemplos de la aplicación del ML en la ciberseguridad [13]–[16].

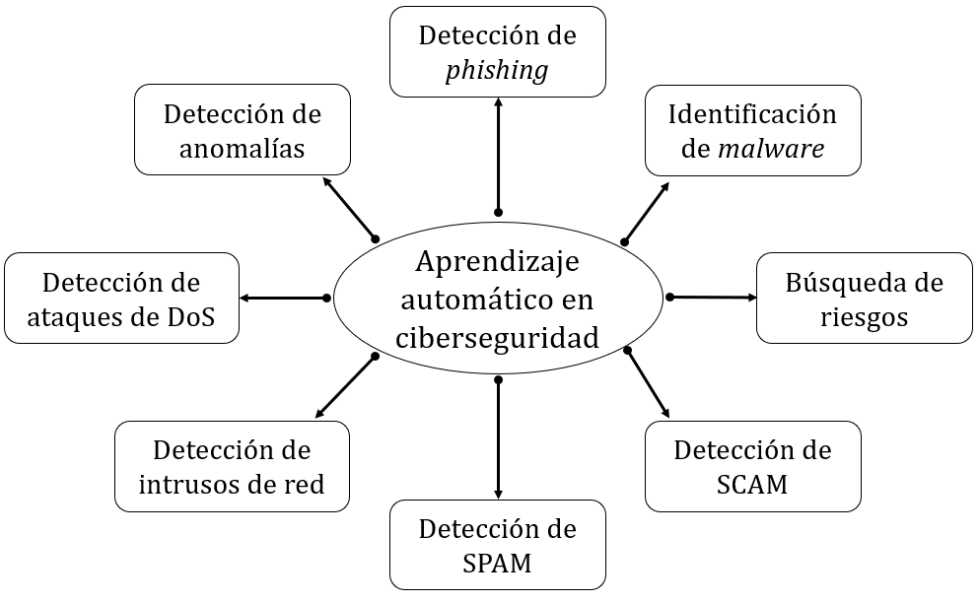

Figura 1: Campos de la ciberseguridad donde se puede emplear el ML.

3. MLAAS PARA LA CIBERSEGURIDAD

Si bien el concepto de aprendizaje automático ha existido durante décadas, los aumentos dramáticos en la capacidad informática y el volumen de datos han acelerado su desarrollo. Un flujo de trabajo de ML típico incluye: limpieza y preparación de datos, selección de algoritmos, entrenamiento de modelos, optimización del modelo, despliegue del modelo e inferencia [17]–[21].

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 21 No. 1, Enero-Marzo, p.48- 55 ISSN 1729-3804

El ML puede ayudar en la identificación de patrones de comportamiento, ordenar datos para crear interfaces adaptables según las preferencias de los usuarios, interpretar altos volúmenes de información en pocos segundos, entre otras funciones. La principal dificultad que presentan las implementaciones de ML es la necesidad de poseer elevados recursos de cómputos, complejizando la generalización de las soluciones basadas en este. Para disminuir estas dificultades se puede emplear la computación en la nube.

4. PROPUESTA DE SOLUCIÓN ML4SEC

La propuesta de solución ML4Sec, proveniente del término en inglés *Machine Learning for Security*, es el empleo del aprendizaje automático como un servicio para detectar anomalías de seguridad informática. Este comienza con la preparación de un modelo de predicción para un área de ciberseguridad. A través de una API se accede a él para realizar predicciones a una alta velocidad. Con las ventajas de la computación en la nube el modelo se encuentra disponible para quien solicite el servicio, sin importar la ubicación geográfica que tenga. A continuación, se explica este proceso detalladamente.

Ciclo de aprendizaje del sistema

Lograr detectar y clasificar correctamente las amenazas requiere que la solución se encuentre actualizada constantemente. Por este motivo, el sistema que se propone presenta un ciclo de aprendizaje dividido en tres pasos: casos de usos, analítica y obtención de datos.

El primer paso es la obtención de conjuntos de datos con registros de la amenaza a detectar junto con registros benignos. Estos son preprocesados para mantener una limpieza y claridad en los datos. En segundo lugar, se utilizan mecanismos de ML, ya sean supervisados, no supervisados o por refuerzo, para identificar patrones que permitan detectar la amenaza en cuestión. El tercer paso es la obtención de datos nuevos a partir de la información de los agentes desplegados en la red; registros de eventos, paquetes de red, dispositivos de internet de las cosas o inteligencia colaborativa. Con estos, junto con los resultados de la analítica del paso anterior, se genera un nuevo conjunto de datos con el cual se repite el proceso. Así se crea un ciclo infinito de aprendizaje.

Preparación del modelo de predicción

La obtención de modelos para identificar patrones de determinada amenaza conlleva un proceso de cuatro pasos: selección de características, selección del modelo, afinación de hiperparámetros y obtención del modelo optimizado. Un ejemplo de este proceso se muestra en la Fig. 2.

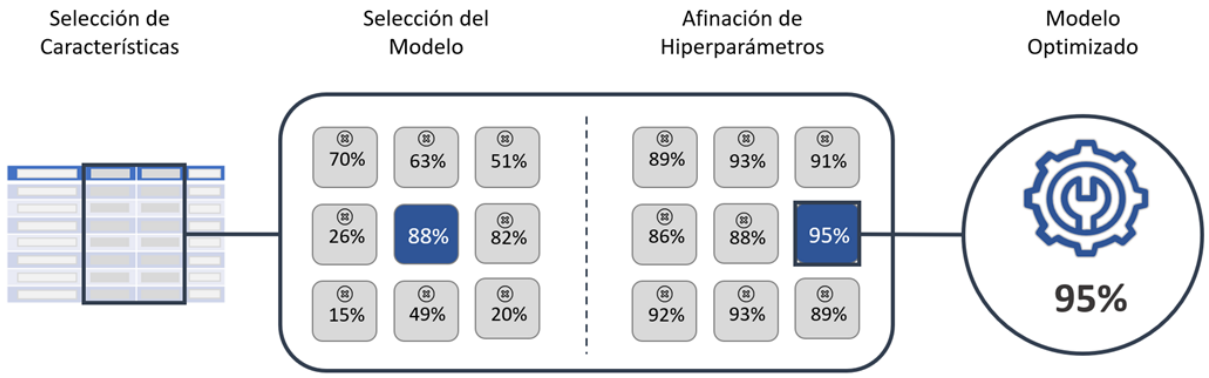

Figura 2: Proceso de obtención de un modelo optimizado.

A partir de la selección de las características distintivas del conjunto de datos se entrenan múltiples modelos y se identifica el más acertado. Este es afinado con la aplicación de hiperparámetros, hasta localizar el modelo de mejor resultado. Se constituye así un modelo optimizado con el cual se realizarán predicciones a una alta velocidad.

Para la selección de los modelos se decide la implementación de redes neuronales. Modelos matemáticos compuestos por un elevado número de elementos procesales organizados por niveles. Las redes neuronales se utilizan para

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 21 No. 1, Enero-Marzo, p.48- 55 ISSN 1729-3804

reconocer patrones, ya sea en imágenes, manuscritos o secuencias de tiempo. Tienen la capacidad de aprender y mejorar en base a la experiencia. Son lo más cercano a la inteligencia humana.

A las redes neuronales no hay que decirles o explicarles que reglas (cálculos, algoritmos) tienen que aplicar para darle solución a un problema determinado. Aprenden con ejemplos a base de prueba y error. Mientras más datos con calidad se posean, mejor y más rápido será el proceso de aprendizaje del modelo.

Para la afinación de hiperparámetros, las redes neuronales implementan optimizadores que posibilitan controlar cuán bien se está generalizando el conocimiento en la red neuronal. Entre los más empleados se encuentran los algoritmos Adam y RMSProp [22].

Despliegue de los modelos predictivos

Para el despliegue de la solución ML4Sec se proponen las tecnologías de código abierto: Docker y Kubernetes.

El modelo seleccionado (modelo optimizado) se convierte en un contenedor con ayuda de la tecnología Docker [23], lo cual permite su rápido despliegue y puesta en marcha. El contenedor base que se propone desarrollar cuenta con sistema operativo Debian 11 y el lenguaje de programación Python 3.9. Este posee librerías dedicadas a la estadística y las matemáticas, como NumPy, Pandas, Matplotlib, SciPy, Scikit-learn, TensorFlow y Keras.

La plataforma Kubernetes ofrece un entorno de administración para contenedores [24]. Orquesta la infraestructura de cómputo, redes y almacenamiento para que las cargas de trabajo no sean realizadas por los usuarios. Con el empleo de Kubernetes se logra mantener el despliegue continuo del contenedor. Posibilita la creación de instancias del modelo para balancear la carga de trabajo y mantener la disponibilidad del servicio.

5. ESCENARIO DE DESPLIEGUE

La Fig. 3 muestra un escenario típico de funcionamiento de la solución propuesta. La nube puede estar constituida por cualquiera de los tres métodos de implementación: pública, privada o híbrida. La selección depende de los recursos con que se cuente y las necesidades de los proveedores.

En la nube se encuentran los servicios comercializados por las organizaciones, ya sean de infraestructura, plataforma o aplicación; junto con los servicios de ML4Sec. Los usuarios hacen uso de sus servicios mientras los atacantes buscan vulnerabilidades que le permitan sacar provecho de estas.

Todo el tráfico desde internet a la nube es revisado por los mecanismos de seguridad desplegados, constituyendo las primeras capas de defensa. El tráfico que estos mecanismos detectan como permitido, es entregado a los modelos de ML4Sec para corroborar su decisión. De detectarse un ataque se les notifica a los mecanismos de protección perimetrales para detener el ataque a la entrada de la nube. De coincidir con la decisión, el tráfico es transmitido a su destino. Así, los usuarios legítimos pueden acceder a sus servicios y la nube queda libre de datos maliciosos. Además, los usuarios pueden solicitar los servicios de ML4Sec para mejorar sus mecanismos de protección internos.

Mecanismos de protección antivirus

Un ejemplo de aplicación son las soluciones de antivirus. Los agentes desplegados en la red del usuario emplean ML4Sec para detectar *malware*. Las soluciones de antivirus que empleen estos mecanismos, no necesitan grandes cantidades de recursos para detectar satisfactoriamente las amenazas. El servicio ML4Sec dedicado al *malware* es el encargado de procesar los datos en búsqueda de la nueva amenaza. Para esto hace uso de un modelo entrenado con el conjunto de datos BODMAS, el cual cuenta con 57,293 ejemplos de *malware* que fueron recolectados entre agosto de 2019 y septiembre de 2020 [25]. Este se enriquece con las experiencias y datos de eventos que se recolectan posteriormente.

Mecanismos de protección anti spam

Otro ejemplo es la detección de correo basura, no deseado o spam. Una de las mejoras de servicio, en el correo electrónico, es la posibilidad de detectar y alejar del usuario todo correo no deseado.

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 21 No. 1, Enero-Marzo, p.48- 55 ISSN 1729-3804

Entre los procesos de ML4Sec desplegados se encuentra un modelo optimizado con un conjunto de datos enriquecidos tomando como base la colección SMS Spam [26]. El servidor de correo electrónico envía los mensajes recibidos hacia el modelo de predicción, este último evalúa el contenido del mensaje y de detectar spam le envía una notificación al servidor para que realice las acciones correspondientes. Ya que se pueden generar falsos positivos, se propone una retroalimentación, donde el usuario puede decidir si el correo es realmente spam o no, permitiendo la afinación del modelo desplegado.

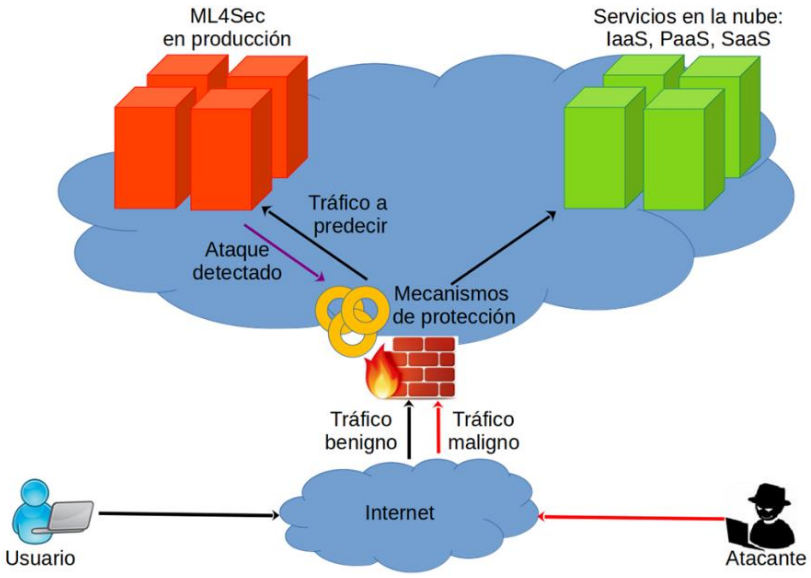

Figura 3: Estructura de la solución propuesta.

Mecanismos de protección anti DDoS

Un caso de interés para los proveedores de servicios de Internet es la detección de ataques de Denegación de Servicio Distribuido (DDoS, por las siglas del término en inglés, *Distributed Denial of Service*). La posibilidad de dejar sin servicios a millones de clientes en minutos, convierten a los ataques de DDoS en una de las principales amenazas de cualquier organización. Al igual que en los ejemplos anteriores, el sistema ML4Sec contaría con un modelo optimizado para esta amenaza. Para el entrenamiento se utilizan conjuntos de datos como NSL-KDD o CICDDoS2019 [27]. El servicio de ML4Sec complementa a los Sistemas de Detección/Prevención de Intrusos y cortafuegos en la detección y clasificación de estos ataques.

El tráfico del Protocolo de Internet (IP, por las siglas del término en inglés, *Internet Protocol*) se monitorea constantemente en búsqueda de anomalías. De detectarse alguna, se distribuyen en la red reglas de filtrado para detener dicho tráfico IP.

Como se puede observar, la solución propuesta puede tener tantos modelos desplegados como ciberataques a detectar. Permitiendo la integración con múltiples sistemas de protección.

6. CASOS DE USOS

El aprendizaje automático y la computación en la nube son aprovechados para desarrollar aplicaciones similares a la propuesta realizada. A continuación, se revisan algunas de ellas.

Kaspersky Endpoint Security Cloud

La empresa rusa Kaspersky oferta entre su gama de productos la solución "*Kaspersky Endpoint Security Cloud*". Es una aplicación multiplataforma, tanto en estaciones de trabajo como en los teléfonos inteligentes.

Revista Telemática. Vol. 21 No. 1, Enero-Marzo, p.48- 55 ISSN 1729-3804

La solución es hospedada en la nube de la empresa y disponible mediante un navegador web. La compañía apuesta por la aplicación del aprendizaje automático para disminuir el error humano y aumentar la respuesta a alertas sobre amenazas.

Con los beneficios de la computación en la nube se obtiene [28]:

1. Tiempos de protección rápidos.
2. No inversión de capital.
3. Redespliegues de recursos.
4. Pagos por uso.
5. Subcontratación amigable.

Servicio de gestión de respuesta frente amenazas de la empresa Sophos

La compañía de seguridad informática Sophos brinda el servicio de gestión de respuesta frente amenazas, el cual es un sistema de búsqueda, detección y respuesta impulsada por el aprendizaje automático y el análisis de expertos para neutralizar las amenazas. Es una solución de respuesta humana acelerada por máquinas. El aprendizaje automático busca y detecta amenazas mejoradas. Los expertos investigan a fondo las alertas y se realizan acciones para eliminar las amenazas. Al agregar telemetría en la nube, los clientes reciben monitoreo de seguridad las 24 horas del día. La aplicación de la inteligencia artificial revela información valiosa y procesable por los especialistas. Con la presencia en la nube se añade una capa de protección a los cortafuegos y terminales de la compañía [29].

Alien Vault de AT&T Cybersecurity

Entre las soluciones del sistema de Gestión de Eventos e Informaciones de Seguridad (SIEM, por las siglas del término en inglés, *Security Information and Event Management*) *Alien Vault*, se encuentra la plataforma comunitaria *Open Threat Exchange*. Esta permite a los expertos en seguridad investigar de forma colaborativa. Compara datos de diversas fuentes para integrar la información en sus respectivos sistemas de protección. Emplea tecnologías como el procesamiento del lenguaje natural y el aprendizaje automático [30].

FortiAI

La empresa de ciberseguridad Fortinet comercializa un dispositivo que aprovecha las redes neuronales para automatizar la detección y respuesta frente amenazas. El FortiAI toma el conocimiento de la inteligencia de amenazas en la nube de otra de sus soluciones, FortiGuard Labs, para llevarla al sitio de despliegue. Posibilita el respaldo directamente en el entorno de los clientes. La aplicación de aprendizaje automático permite identificar, clasificar e investigar amenazas sofisticadas en microsegundos [31].

7. CONCLUSIONES

La principal contribución de este trabajo es la aplicación de ML en la detección de anomalías de ciberseguridad en la nube. La aplicación de algoritmos de ML brinda a los sistemas de seguridad informática un poder de exactitud sorprendente mediante modelos optimizados. El empleo de la computación en la nube provee los recursos necesarios para el entrenamiento de los modelos. La adopción de ML4Sec permite disminuir los riesgos de un ciberataque a los servicios en la nube y las redes asociadas. Al utilizar tecnologías de código abierto se logra independencia tecnológica, pudiendo adaptarse a las necesidades de los proveedores de servicio.

RECONOCIMIENTOS

El autor desea agradecer el conocimiento y colaboración, respecto al desarrollo del tema de investigación, brindada por los integrantes del grupo de investigación de Telemática de la Universidad Tecnológica de La Habana. “José Antonio Echevarría”, CUJAE.

REFERENCIAS

[1] «Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe | Publications». Accedido: 19 de agosto de 2022. [En línea]. Disponible en:

https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf
[2] «Análisis anual de las APT 2021». Accedido: 19 de agosto de 2022. [En línea]. Disponible en: https://securelist.lat/apt-annual-review-2021/95935/
[3] «Machine Learning and Cyber Security: A Review», *Int. J. Res. Publ. Rev.*.
[4] J. Yin, M. Tang, J. Cao, M. You, H. Wang, y M. Alazab, «Knowledge-Driven Cybersecurity intelligence: Software Vulnerability Co-exploitation Behaviour Discovery», *IEEE Trans. Ind. Inform.*, pp. 1-9, 2022, doi: 10.1109/TII.2022.3192027.
[5] V. Yosifova, A. Tasheva, y R. Trifonov, «Predicting Vulnerability Type in Common Vulnerabilities and Exposures (CVE) Database with Machine Learning Classifiers», en *2021 12th National Conference with International Participation (ELECTRONICA)*, may 2021, pp. 1-6. doi: 10.1109/ELECTRONICA52725.2021.9513723.
[6] M. Rahman y H. Jahankhani, «Security Vulnerabilities in Existing Security Mechanisms for IoMT and Potential Solutions for Mitigating Cyber-Attacks», en *Information Security Technologies for Controlling Pandemics*, H. Jahankhani, S. Kendzierskyj, y B. Akhgar, Eds. Cham: Springer International Publishing, 2021, pp. 307-334. doi: 10.1007/978-3-030-72120-6_12.
[7] K. Kioskli, T. Fotis, y H. Mouratidis, «The landscape of cybersecurity vulnerabilities and challenges in healthcare: Security standards and paradigm shift recommendations», en *Proceedings of the 16th International Conference on Availability, Reliability and Security*, New York, NY, USA, ago. 2021, pp. 1-9. doi: 10.1145/3465481.3470033.
[8] «Browse cve vulnerabilities by date». Accedido: 19 de agosto de 2022. [En línea]. Disponible en: https://www.cvedetails.com/browse-by-date.php
[9] «Offensive Security's Exploit Database Archive». Accedido: 19 de agosto de 2022. [En línea]. Disponible en: https://www.exploit-db.com/
[10] 14:00-17:00, «ISO/IEC 27002:2022», *ISO*. Accedido: 19 de agosto de 2022. [En línea]. Disponible en: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/56/75652.html
[11] R. Acosta Escobar, «Propuesta basada en la seguridad lógica perimetral en las Pymes, como estrategia para la protección contra ciberataques.», may 2022, Accedido: 18 de noviembre de 2022. [En línea]. Disponible en: http://repository.unad.edu.co/handle/10596/49276
[12] Salinas, A. P, «Modelo de ciberseguridad para cajas municipales en tiempos de transformación digital - un nuevo enfoque», Tesis de maestría, Universidad Privada del Norte, Repositorio de la Universidad Privada del Norte, 2020. [En línea]. Disponible en: https://hdl.handle.net/11537/29733
[13] R. Badhwar, «The Case for AI/ML in Cybersecurity», en *The CISO's Next Frontier*, Cham: Springer International Publishing, 2021, pp. 45-73. doi: 10.1007/978-3-030-75354-2_5.
[14] D. Dasgupta, Z. Akhtar, y S. Sen, «Machine learning in cybersecurity: a comprehensive survey», *J. Def. Model. Simul. Appl. Methodol. Technol.*, vol. 19, n.º 1, pp. 57-106, ene. 2022, doi: 10.1177/1548512920951275.
[15] Y. Xin *et al.*, «Machine Learning and Deep Learning Methods for Cybersecurity», *IEEE Access*, vol. 6, pp. 35365-35381, 2018, doi: 10.1109/ACCESS.2018.2836950.
[16] J. M. Dueñas Quesada, «Aplicación de técnicas de machine learning a la ciberseguridad: Aprendizaje supervisado para la detección de amenazas web mediante clasificación basada en árboles de decisión», jun. 2020, Accedido: 19 de agosto de 2022. [En línea]. Disponible en: https://openaccess.uoc.edu/handle/10609/118166
[17] A. D. Tamayo Palomino, «Aproximación metodológica para la integración de las metodologías DataOps y MLOps aplicadas al trading automático», Trabajo de grado - Maestría, Universidad Nacional de Colombia, 2021. Accedido: 18 de noviembre de 2022. [En línea]. Disponible en: https://repositorio.unal.edu.co/handle/unal/80671
[18] M. Schlegel y K.-U. Sattler, «Management of Machine Learning Lifecycle Artifacts: A Survey». arXiv, 21 de octubre de 2022. doi: 10.48550/arXiv.2210.11831.
[19] J. Baltensperger, P. Salza, y H. C. Gall, «Continuous Deep Learning: A Workflow to Bring Models into Production». arXiv, 29 de agosto de 2022. doi: 10.48550/arXiv.2208.12308.
[20] C. Chai, J. Wang, Y. Luo, Z. Niu, y G. Li, «Data Management for Machine Learning: A Survey», *IEEE Trans. Knowl. Data Eng.*, pp. 1-1, 2022, doi: 10.1109/TKDE.2022.3148237.
[21] S. García Alonso y S. García Alonso, «Integración del aprendizaje automático en una PYME: caso práctico en Darwinex», jul. 2021, Accedido: 18 de noviembre de 2022. [En línea]. Disponible en: https://eprints.ucm.es/id/eprint/67249/
[22] K. Team, «Keras documentation: Optimizers». Accedido: 19 de agosto de 2022. [En línea]. Disponible en: https://keras.io/api/optimizers/

[23] «Docker overview», *Docker Documentation*. agosto de 2022. Accedido: 19 de agosto de 2022. [En línea]. Disponible en: https://docs.docker.com/get-started/overview/
[24] «Orquestación de contenedores para producción», *Kubernetes*. Accedido: 19 de agosto de 2022. [En línea]. Disponible en: https://kubernetes.io/es/
[25] «BODMAS Malware Dataset», *BODMAS*. Accedido: 19 de agosto de 2022. [En línea]. Disponible en: https://whyisyoung.github.io/BODMAS/
[26] «UCI Machine Learning Repository: SMS Spam Collection Data Set». Accedido: 19 de agosto de 2022. [En línea]. Disponible en: https://archive.ics.uci.edu/ml/datasets/SMS+Spam+Collection
[27] «DDoS 2019 | Datasets | Research | Canadian Institute for Cybersecurity | UNB». Accedido: 19 de agosto de 2022. [En línea]. Disponible en: https://www.unb.ca/cic/datasets/ddos-2019.html
[28] «Kaspersky Endpoint Security Cloud. Straightfor-ward protection for your business – wherever you're heading». Accedido: 19 de agosto de 2022. [En línea]. Disponible en: https://media.kaspersky.com/pdf/b2b/KES-Cloud-Datasheet.pdf
[29] «Sophos se vale del machine learning para mejorar en su lucha contra las ciberamenazas», *Computing*. octubre de 2019. Accedido: 19 de agosto de 2022. [En línea]. Disponible en: https://www.computing.es/seguridad/noticias/1114455002501/sophos-se-vale-del-machine-learning-mejorar-lucha-contra-ciberamenazas.1.html
[30] «Open Threat Exchange (OTX) | AT&T Cybersecurity». Accedido: 19 de agosto de 2022. [En línea]. Disponible en: https://cybersecurity.att.com/open-threat-exchange
[31] «Reduce the risk of cyber threats with Network Detection and Response (NDR)», *Fortinet*. Accedido: 19 de agosto de 2022. [En línea]. Disponible en: https://www.fortinet.com/products/network-detection-and-response

SOBRE LOS AUTORES

Ariel Baloira Reyes, Ingeniero en Telecomunicaciones y Electrónica, Universidad Tecnológica de La Habana "José Antonio Echeverría", La Habana, Cuba, ariel@tele.cujae.edu.cu, ORCID: https://orcid.org/0000-0001-6021-325X

CONFLICTO DE INTERESES

No existen conflictos de intereses.

CONTRIBUCIONES DE LOS AUTORES

- **Autor 1**: 100% concepción, preparación, creación, desarrollo y organización del artículo, revisión crítica de cada una de las versiones del borrador del artículo.