Análisis de técnicas de Machine Learning aplicadas a la ciberseguridad informática para mejorar la detección de intrusiones y comportamientos anómalos en la Web

*William Ruiz Martínez**

Recibido: 13 - 10 - 2020 / Aceptado: 21 – 10 – 2020 / Publicado: 26 - 01 - 2021

Resumen

En los últimos años, se ha escuchado hablar mucho sobre Inteligencia artificial y, en especial, de una de sus ramas más destacadas, como lo es el "Machine Learning". Sin embargo, la Inteligencia artificial no es nueva; lleva con nosotros desde finales de los años 50s, donde un conjunto de científicos se reunió en Darthmoud y acuñó el término, en el año 1956. Hoy en día, su influencia ha llegado a múltiples sectores y áreas, entre otros: el sector automovilístico, la energía, la industria, el sector bancario, sanidad, defensa y ciberseguridad.

El "Machine Learning", en sí, consiste en la creación de modelos o algoritmos para analizar datos, aprender de ellos y, luego, hacer una predicción de su posible comportamiento en un rango de tiempo o situación estimada.

Por estas razones, la industria de la ciberseguridad no ha sido ajena al crecimiento, difusión e implantación de técnicas para mejorar la seguridad informática, aplicando modelos y técnicas de Machine Learning, que permitan dar una respuesta más adecuada y afín con los requerimientos actuales. Estas prácticas mejoran y permiten optimizar el análisis de las amenazas y prometen ser más efectivas a la hora de detener o evitar los incidentes de seguridad. En la actualidad, encontramos varias aplicaciones de la Inteligencia artificial, a través del Machine Learning, en la ciberseguridad informática, entre ellas: detección de fraude de tarjetas bancarias, detección de intrusos, clasificación de malware y detección de ataques de negación de servicio, por enumerar algunas de ellas.

Teniendo esto como referencia, nos pareció importante el poder presentar en este documento los diferentes tipos de sistemas existentes y su inclusión en los esquemas de ciberseguridad. Por otra parte, queremos destacar y referenciar los principales algoritmos y modelos de Machine Learning para casos y situaciones muy específicas y concretas.

Palabras clave:
algoritmos, ciberseguridad, inteligencia artificial, Machine Learning, modelos predictivos

Cómo citar: Ruiz Martínez, W. (2020). Análisis de técnicas de Machine Learning aplicadas a la ciberseguridad informática para mejorar la detección de intrusiones y comportamientos anómalos en la Web. Hashtag, (17), 44-60

* Magister en dirección estratégica de Ingeniería de software, UNINI; Especialista en Gerencia de proyectos; Ingeniero de Sistemas; Docente asociado del programa de Ingeniería de Sistemas; amplia experiencia en orientación y coordinación de proyectos de investigación y semilleros; diseñador y desarrollador WEB; miembro del grupo de investigación Axón. Correo: william_ruizmar@cun.edu.co-

Analysis of Machine Learning techniques applied to computer cybersecurity to improve the detection of intrusions and abnormal behavior on the Web

*William Ruiz Martínez**

Recibido: 13 - 10 - 2020 / Aceptado: 21 – 10 – 2020 / Publicado: 26 - 01 - 2021

Abstract:

In recent years, much has been heard about artificial intelligence and especially about one of its most outstanding branches, Machine Learning. However, artificial intelligence is not new, it has been with us since the late 1950s, when a group of scientists met in Darthmoud and coined the term in 1956. Today its influence has reached multiple sectors and areas, including others: the automotive sector, energy, industry, the banking sector, health, defense and of course cybersecurity.

Machine learning itself, consists in the model creation or algorithms for analyze data, to learn of them and later to do a prediction of your possible behavior in a time range or situation.

For these reasons, the cybersecurity industry has not been immune to the growth, dissemination, and implementation of techniques to improve computer security using Machine Learning models and techniques that allow a more appropriate response and in line with current requirements. These practices improve and enable threat analysis and promise to be more effective in stopping or preventing security incidents. Currently we find several applications of Artificial Intelligence through Machine Learning in computer cybersecurity, among them: bank card fraud detection, intrusion detection, malware classification and detection of denial-of-service attacks, to list some of them.

Taking this as a reference, it seemed important to us to be able to present in this document the different types of existing systems and their inclusion in cybersecurity schemes. On the other hand, we want to highlight and reference the main Machine Learning algorithms and models for very specific and concrete cases and situations.

Keywords: algorithms, artificial intelligence, cybersecurity, Machine Learning, predictive models

Declaración de conflictos de interés: el autor declara no tener ningún conflicto de interés

Introducción

Es innegable que la aparición de la Internet ha traído una gran cantidad de ventajas y mejoramiento en las condiciones de vida para muchas personas. Por ejemplo, el teletrabajo y la educación virtual son dos áreas o sectores que se han visto beneficiados por las herramientas y plataformas, para poder hacer trabajo en casa o cursar algún tipo de estudio, sin vernos inmersos en las caóticas y constantes problemáticas de transporte e inseguridad de nuestras grandes urbes.

Otro sector que se ha visto beneficiado por el desarrollo y masificación de la Internet ha sido, sin duda, el comercio electrónico. De acuerdo con Esparza Cruz (2017), actualmente las empresas se han visto inmersas en la necesidad de crear nuevos medios y estrategias de comunicación con sus clientes, que les permitan obtener el volumen de ventas necesario para mejorar las ganancias; por razones de este tipo, el comercio electrónico es una herramienta invaluable para el departamento de ventas de las empresas. Pero, por otra parte, así como han aumentado los beneficios y ventajas del uso de la Internet, en múltiples herramientas, plataformas, sitios de consulta, portales financieros y bancarios, etc., también es cierto que ha aumentado los riesgos, amenazas y posibilidades de intrusiones, por parte de personas inescrupulosas y mal intencionadas. De acuerdo a lo propuesto por Urcuqui López *et al.* (2019)

> La expansión y desarrollo acelerado en las comunicaciones, la masificación de los dispositivos móviles e inteligentes y el avance en tecnologías como Internet de las cosas (IoT), han aumentado su importancia y complejidad, es allí donde la ciencia de datos se erige con una opción para optimizar los mecanismos de análisis de requerimientos en los sistemas informáticos y generar una mejor opción frente a los distintos tipos de riesgos de seguridad que existen en la actualidad.

Por otra parte, para Yumbo Anis (2016)

> Los ataques e intrusiones a sistemas informáticos, sitios y aplicaciones Web, siguen incrementándose con mayor frecuencia, por lo que se hace indispensable el uso de mecanismos autónomos para evitar daños o pérdidas de información. La seguridad de los datos comerciales, personales y las aplicaciones de misión crítica son aspectos que las organizaciones deben evitar a toda costa que se encuentren comprometidos.

Es ahí donde la constante evolución y mejora en técnicas de aprendizaje automático entran en el panorama, ya que toman en consideración los datos históricos o actuales, con el objetivo de hacer predicciones o proyecciones de cierto rango de datos, o en ciertos lapsos de tiempo, para poder establecer similitudes, en relación con patrones o características de comportamiento.

Se debe tener en cuenta que, gracias al aprendizaje automático, un sistema informático tiene la capacidad de poder localizar en grandes cantidades de datos, comportamientos extraños y situaciones anómalas que son conocidas como patrones. El Machine Learning es usado para detectar intrusiones o situaciones fuera de lo normal, que quieran infiltrarse en la red de un sistema. Para ello, podemos encontrar 2 posibles soluciones, veamos:

IDS Heurístico. El cual se encarga de monitorear el tráfico entrante y saliente de un sitio Web y registrar su comportamiento.

IDS basado en reglas. En este caso, se definen un conjunto de vulnerabilidades, partiendo de las más comunes o que se presentan con más frecuencia, es decir, de una coincidencia con patrones, para que el sistema sea capaz de detectarlas de forma automática y lanzar un aviso.

Materiales y métodos

Para la obtención de las referencias documentales se utilizaron varios tipos de fuentes. Entre las principales búsquedas bibliográficas, se emplearon bases de datos, como: Microsoft Academic, Google escolar, Redalyc y Base. Una vez obtenido el material, se procedió a una evaluación y clasificación del material obtenido y se seleccionaron solo aquellos documentos que tuvieran relación directa con el análisis de técnicas de Machine Learning, aplicadas a la ciberseguridad informática, para mejorar la detección de intrusiones y comportamientos anómalos en sitios y aplicativos Web.

La ciberseguridad y su impacto en la actualidad

El desarrollo y avance de los sistemas informáticos ha estado vinculado, desde sus inicios, a diferentes tipos de intentos por violar o traspasar la seguridad, aprovechando los fallos de esta o sus vulnerabilidades. El marcado desarrollo de la Internet y la era de expansión tecnológica que se vive actualmente, en la que están inmersas la mayoría de las personas en los países desarrollados, donde se dispone de más de un dispositivo conectado a Internet, han contribuido a que estos ataques hayan tenido una tasa de aumentos bastante significativa (Arteaga, 2013).

Según lo expuesto por Jardine (2015), para tener un ejemplo más conciso, desde 2007 hasta 2014, los ataques llevados a cabo en la Web han crecido cerca de un 6.000 %, llegando a más de 1.400 millones en 2014. Esta cifra nos da a entender la importancia que cobra, cada día que pasa, el manejo y los beneficios de la ciberseguridad, de cara a las situaciones más preocupantes, como lo son las grandes pérdidas económicas. Por otra parte, como lo explica Ballestero (2020), el término "ciberseguridad" se ha puesto de moda en la actualidad en todos nuestros entornos y, junto a este, podemos encontrar otros términos similares que cobran igual importancia, entre ellos: "ciberdelincuencia", "ciberterrorismo", "ciberdefensa", etc. En general, podríamos definir "ciberseguridad" como la capacidad de resistir, con un adecuado nivel de fiabilidad, todo tipo de acciones que buscan comprometer o perturbar la disponibilidad, accesibilidad, autenticidad, integridad, y confidencialidad de los datos almacenados o transmitidos, a través de algún tipo de sistema informático o de algún tipo de servicio ofertado provenientes de medios o plataformas digitales en la Web.

Mucho se habla, hoy día, de las amenazas informáticas, pero debemos ser conscientes de que, entre más sea la interacción en la Internet, más aumenta el riesgo de recibir algún tipo de ataque. La utopía de los sistemas informáticos 100 % seguros sigue siendo inalcanzable, por parte de las compañías y expertos en la ciberseguridad; de igual manera, complementando lo anterior, Ballestero (2020) afirma que

> [...] es evidente que tanto en el mundo físico como en el virtual la seguridad total no existe, pero si se puede tratar de reducir al máximo posible los riesgos o posibilidades de que una amenaza o un suceso potencial negativo se materialice y ocasione daños en sistemas informáticos y, aún más grave , en la información que estos generan y almacenan

La "vulnerabilidad" es la debilidad, falta de protección o de control que permite que una amenaza se cristalice, ocasionando un impacto negativo en un sistema informático o en una red de datos. Por ejemplo, no contar con una adecuada protección contra incendios o tener un sistema de claves deficiente, para acceder a un determinado sistema informático o una red de datos de una organización. Asimismo, la probabilidad de que esto pueda

ocurrir, es lo que se conoce como "riesgo". Para resumir esta parte, tengamos presente que la ciberseguridad se encarga de establecer el cómo reducir los riesgos, en el ámbito digital (Ballestero, 2020).

El escenario mundial hace su entrada a una nueva era que está generando un cambio de paradigma, tal y como lo fueron —en su momento— el Renacimiento o la primera Revolución Industrial; factores de gran impacto y repercusión a nivel mundial, como la reciente pandemia COVID -19. Todas, han generado situaciones en que las personas se ven supeditadas a conducir su atención hacia los medios informáticos, encargados de mantenerse al día en relación a la las noticias y a la actualidad, como también a la posibilidad de realizar todo tipo de transacciones y operaciones bancarias, comerciales y de diversas índoles, sin necesidad de salir de la casa.

Dicha situación, representa un delicado panorama para muchas empresas y sectores empresariales que se ven beneficiadas por estos aspectos, no obstante, representan para otras un gran reto, según los resultados de las encuestas PriceWaterhouseCoo (PwC), quienes, en su artículo "The future of financial services" (2020), resaltan que los servicios de portales financieros aumentaron su tendencia hacia el comercio electrónico. Dichos incrementos fueron positivos para el sector logístico, así como también para el sector de pagos contactless y móviles; pero negativos para el sector de ventas minoristas. Ante este panorama, es evidente que si aumentan las transacciones en Internet, van a aumentar — proporcionalmente— las tasas de cibercrímenes y amenazas informáticas. Esto también lo detalla el artículo "Global Economic rime and Fraud Survey" (2020), de la empresa PriceWaterhouseCoopers, en el que se evidencia que los delitos relacionados con fraudes y estafas de clientes y cibercrimen son los que han tenido un mayor aumento; particularmente este último, con una representación del 34 % en la frecuencia de la experiencia general. Igualmente, se destaca el reporte que "cerca de 47 % de las personas encuestadas han experimentado el haber sufrido de algún tipo de fraude los pasados 24 meses; lo que se reporta como el segundo nivel de incidentes o situaciones relacionadas con seguridad informática más alta en los últimos veinte años".

Herramientas para el análisis y detección de Malware

De acuerdo con lo que nos presenta Valero Campaña (2015) "cualquier tipo de software que ocasione perjuicios o daños al usuario, dispositivo o red (como troyanos, virus, gusanos, rootkits o spyware) puede ser denominado con el nombre de «malware»". Así mismo, como el malware puede manifestarse en diferentes formas, las herramientas de análisis deben ser idóneas para detectarlos, determinar el daño causado y detectar si han infectado otros archivos. En los casos que identifique y localice un archivo malicioso, este es agregado a una base de datos de firmas de malware, para asegurar que este mismo archivo no tenga la capacidad de volver a ingresar en la red o dispositivo. Según lo expuesto por Sikorski y Honig (2012) "existen dos métodos fundamentales de abordar el análisis de malware, el primero se denomina análisis estático y el segundo es conocido como análisis dinámico". Veamos en detalle cada uno de ellos:

Análisis estático

Se basa en examinar el archivo y proporcionar información sobre su estructura y funcionalidad. Este tipo de análisis es más básico y seguro (ya que en ningún momento se está ejecutando código malicioso) pero no es tan efectivo contra archivos malware ofuscados. El método más usado para identificar malware es basado en firmas; cuando un fichero sospechoso entra en el sistema, se genera su hash y se compara con una base de datos de firmas de malware. El problema reside en que los autores de malware pueden modificar fácilmente su código y así evadir este tipo de análisis.

Figura 1. Configuración de una regla en Yara.

```
rule SAW
{
        meta:
                descripcion = "Ejemplo regla para los lectores de SAW"
        strings:
                $cadenaDeBytes = { 53 41 57 }
                $cadenaDeTexto = "securityartwork.es"
        condition:
                $cadenaDeBytes and $cadenaDeTexto
}
```

Fuente: Sánchez, B., 2015

Análisis dinámico

Este tipo de técnica permite observar el comportamiento de la ejecución del malware en el sistema. Además, permite detectar el funcionamiento del malware (aunque esté ofuscado). Con la finalidad de llevar a cabo un análisis dinámico de malware, es necesario disponer de un ambiente seguro, donde pueda ser ejecutado cualquier tipo de archivo malicioso, sin que haya riesgo de dañar al dispositivo o la red. Debido a ello, estos análisis se llevan a cabo en máquinas virtuales conocidas como Sandbox; una máquina virtual con software preinstalado, para analizar la ejecución de malware. Suele realizar acciones como la de generar una red virtual para observar la interacción del malware con la red.

Herramientas de análisis de malware

A continuación, presentamos algunas herramientas que han sido utilizadas con éxito en el análisis de amenazas cibernéticas:

Yara

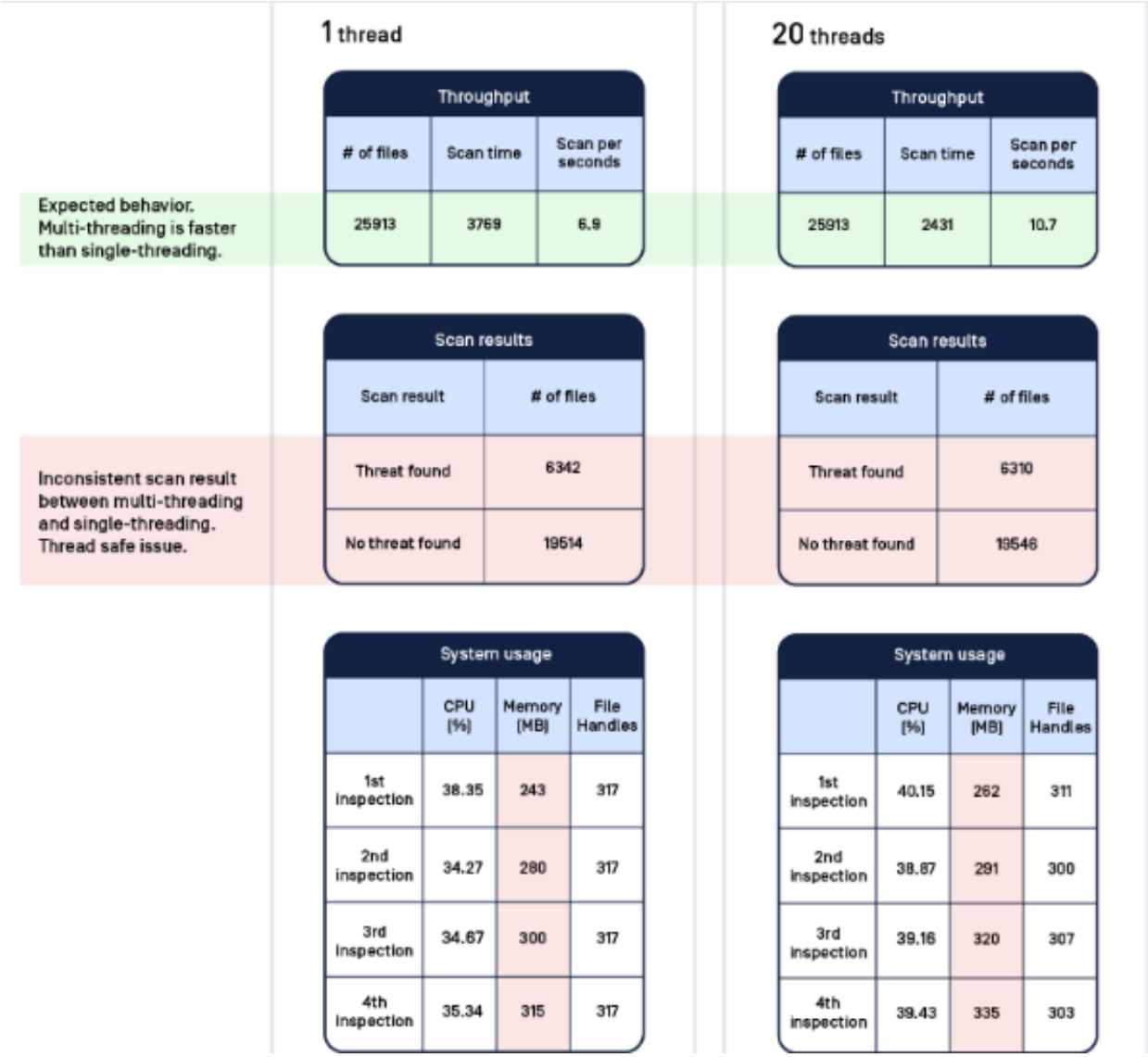
Es una aplicación multiplataforma disponible para sistemas Windows, Linux y MacOS; esta herramienta se encarga de ayudar a identificar y clasificar posibles familias de Malware, trabaja con información binaria o textual de los archivos, que son almacenadas en reglas aplicadas a los archivos, para establecer si pertenece o no a una clase (Sánchez, 2015).

En la regla anterior, se aprecian dos palabras claves: “strings” y “condition”. Los “strings” son las cadenas que han sido establecidas y que YARA se encargará de hallar en el binario, mientras que la “condition” es la condición determinada de los criterios, para que se produzca su detección.

Metascan

Se basa en una herramienta en línea gratuita de análisis de malware. Este sistema emplea el escaneo de ficheros donde aplica varios motores de análisis, de igual forma, posee una API para Java y requiere de una clave conseguida al registrarse en el portal OPSWAT. Presenta un límite de 1500 peticiones de búsqueda de hash y 25 peticiones de análisis de archivos por hora (OPSWAT, s.f.)

Figura 2. Rendimiento de Metascan en análisis múltiples de Malware.

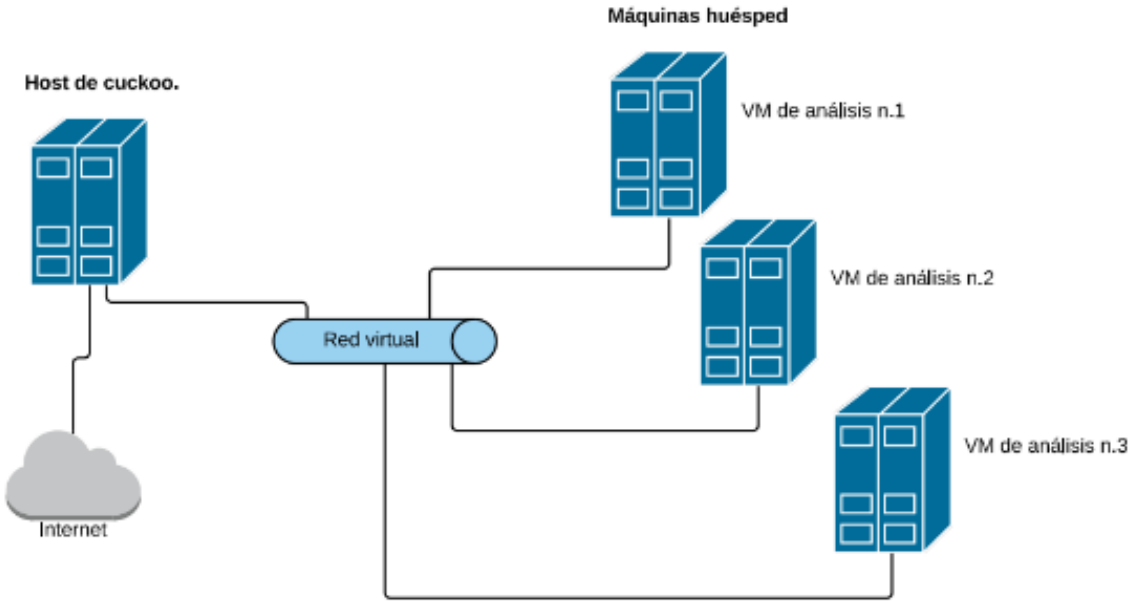


Fuente: OPSWAT, s.f.

Cuckoo

Consiste en un aplicativo de código libre, encargado de automatizar el análisis dinámico de malware. Además, actúa como un sandbox que se encarga de ejecutar y analizar archivos en tiempo real; básicamente, consiste en un software central que gestiona —como se dijo anteriormente— la ejecución y análisis de archivos, pero en máquinas virtuales aisladas. En definitiva, consiste en una máquina Host (con el software de gestión) y un subconjunto de máquinas huésped (máquinas virtuales que ejecutan los archivos). El Host se encarga de ejecutar todo el proceso de análisis, delegando en cada huésped la ejecución de los archivos de forma segura (Oktavianto & Muhardianto, 2013).

Figura 3-Arquitectura del software Cuckoo



Fuente: Oktavianto & Muhardianto, 2013

Fuzzy Hash

Podemos concluir que, en general, los algoritmos que emplean la técnica del hashing, buscan identificar archivos de forma única; si nos basamos en esta característica para la detección del Malware, resultará fácil para sus creadores modificar el código fuente y poder evadir los sistemas que lo detectan. En realidad, lo que busca el software es detectar y comparar la similitud entre dos archivos, por consiguiente, tiene la capacidad de detectar si un software puede llegar a ser la modificación de otro software, comparando el fuzzy hash de los ficheros (French y Casey, 2012).

Tipos de ciberataques

Es evidente que, para poder brindar una solución adecuada a los ataques y amenazas cibernéticas, es necesario conocerlas y saber cómo se comportan. A continuación, enumeramos los principales tipos de ataques cibernéticos:

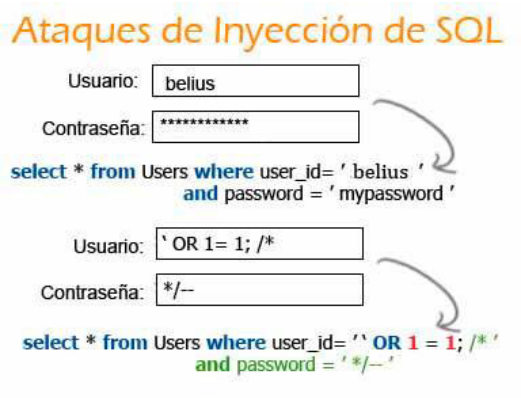
Ataque de inyección SQL

Mediante el SQL (Lenguaje estructurado de consulta) nos podemos comunicar con la información que se encuentra almacenada en una base de datos, tanto a nivel local como en servidores remotos alojados en la Web, es decir, que este lenguaje nos permite extraer —mediante consultas— y modificar —mediante scripts o pequeños programas— la información que allí se encuentra. Es así como muchos de los servidores que almacenan información de algún servicio o aplicación lo utilizan. Según lo que presenta OPSWAT (s.f.),

> [...] en realidad un ataque de inyección SQL se enfoca a este tipo de servidores y mediante la utilización de un código malicioso busca extraer información almacenada en dichos servidores; esta situación se puede tornar especialmente complicada si en el

almacenamiento se incluyen datos privados de clientes, como números de tarjetas de crédito, nombres de usuario y contraseñas, información clasificada, etc.

Figura 4. Arquitectura del Inyección de SQL.



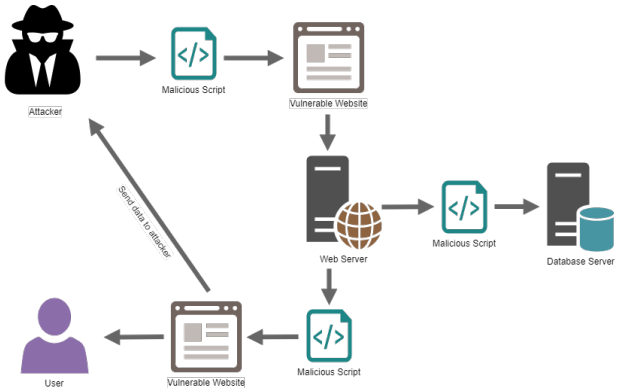
Fuente: OPSWAT, s.f.

Cross-Site Scripting (XSS)

En este tipo de ataque se persigue al usuario y no al servidor. Lo anterior, involucra la inyección de una porción de código malicioso en un sitio Web pero, a diferencia del anterior, este se ejecuta en el navegador del usuario cuando este accede al mismo, y no en el servidor. De acuerdo con Hern (2016)

> [...] una de las situaciones o formas utilizadas para implementar este tipo de ataque entre sitios es mediante la inyección de código malicioso en un comentario o un script que se ejecuta de forma automática. Los ataques de secuencias de comandos en sitios cruzados pueden afectar de manera significativa la reputación de un sitio web, al colocar en peligro la información de los usuarios sin que exista ninguna indicación o rastro de que haya ocurrido algo malicioso.

Figura 5. Un típico ataque de Cross-site Scripting

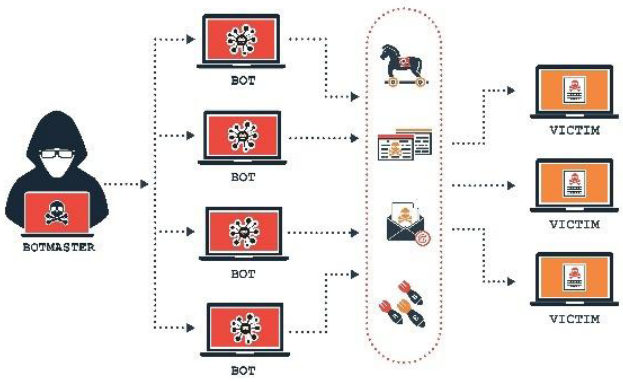


Fuente: Saytlarga, s.f.

Denegación de servicio (DoS)

Al tenor de lo que expresa Muñoz (2017), consiste en atiborrar o saturar de tráfico un sitio Web, de forma tal que su servidor se vea sobrecargado de peticiones para que le sea imposible publicar su contenido a los visitantes. En muchos casos, estos ataques DoS son realizados por varios computadores al mismo tiempo; son bastante complejos de superar, debido a que el atacante puede aparecer en forma simultánea, desde diferentes direcciones IP por todo el mundo; cosa que dificulta aún más la determinación de su posible origen

Figura 6. Típico ataque de DoS a varias víctimas utilizando Bots



Fuente: Geetest, 2020

La Ciberseguridad y el Machine Learning

De acuerdo con lo presentado por Urcuqui López *et al.* (2019), el Machine Learning es una de las ramas o áreas de la inteligencia artificial que se encarga de que un sistema o aplicación pueda tener la capacidad de aprender, en entornos variables, sin que sea programado de forma explícita, es decir, que el sistema aprenderá de la información histórica que lo alimenta (o recibe) y la compara con una serie de patrones, para determinar si se están alcanzando, o no, los resultados esperados. Su uso ha tenido un gran crecimiento, evidenciable, actualmente, en medios electrónicos (Big Data), diversos orígenes de datos y, también, en las capacidades computacionales que poseen los equipos y servidores a nuestra disposición. Por consiguiente, la ciberseguridad requiere de un esfuerzo constante que pueda garantizar modelos como la triada CID, compuesta por: la integridad, disponibilidad y confidencialidad de la información; también requiere que se puedan ampliar o incrementar las capacidades de detección y análisis de nuevas amenazas informáticas; algo nada menor, que representa un altísimo reto para los sistemas, consultores e investigadores que se encuentran en el camino, con aspectos como: la complejidad de las variables, la creciente y desmedida capacidad tecnológica, y la astucia de los ciber criminales. En la actualidad, el software convencional enfocado en aspectos o políticas de seguridad, requiere ser complementado con un esfuerzo humano, para poder identificar y analizar vulnerabilidades, mediante procesos y estándares que permitan detectar y encontrar sus características, en pro de poder desarrollar la solución sobre la herramienta. En cuanto al tema: "es una labor que puede llegar a ser más eficiente si se emplea un proceso de análisis a través de técnicas y modelos de ciencia de datos y algoritmos de Machine Learning" (Chan y Lippmann, 2006).

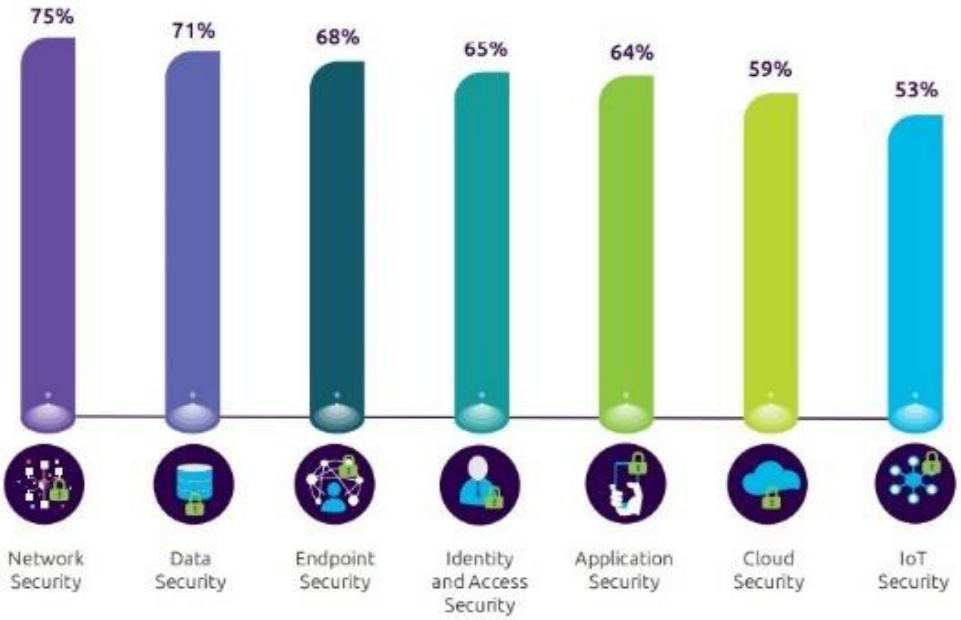
A partir de otros estudios, como el propuesto por Gandotra *et al.* (2014), se plantea generar una clasificación de los malware en MS-Windows, a partir del empleo de características extraídas de los análisis estáticos y dinámicos; para dicho estudio, se emplearon algoritmos de clasificación, como: MultiLayer Perceptron (MLP), IB1, Decision Tree (DT) y Random Forest (RF). En cuanto a eso, se concluyó que es posible conseguir excelentes resultados utilizando, en conjunto, la información de los análisis estáticos y dinámicos. Trayendo a colación a Urcuqui López *et al.* (2019), un camino prometedor es la aplicación de la ciencia de datos para el desarrollo de soluciones de software, por ejemplo, el uso de modelos predictivos especializados para la detección de malware y la predicción de ciberataques Web.

De otro lado, los autores definen "ciberseguridad" como el área de las ciencias de la computación que se encarga de llevar a cabo el desarrollo e implementación de los mecanismos de protección de la información y de la infraestructura tecnológica de una organización, ante posibles ataques externos o internos. En un estudio de Capgemini Research Institute (2019), se identificó una fuerte y creciente tendencia a incorporar tecnologías de Inteligencia Artificial en la ciberseguridad. Por lo menos, un 69 % de las empresas tenía planes de hacerlo a lo largo de 2020, en los siguientes cinco casos de uso: detección de intrusión, clasificación del riesgo en la red, detección del fraude, análisis del comportamiento de usuarios y dispositivos, y detección de malware.

Técnicas, soluciones y modelos de Machine Learning aplicados a la ciberseguridad

Los informes de áreas y sectores empresariales de todo tipo siguen generando alertas sobre falsas percepciones de seguridad; de la tendencia o alza en el cibercrimen; de que no se están generando suficientes políticas o directrices en la prevención; y de la capacidad de reacción ante los ataques cibernéticos.

Figura 7. Áreas donde actualmente se usa la Ciberseguridad.



Fuentes: Capgemini Research Institute, 2019

Sin embargo, los fabricantes que impulsan la introducción de Inteligencia Artificial en la ciberseguridad hablan sobre la aparición de un nuevo paradigma, que podría reducir de una forma eficaz las vulnerabilidades en el dispositivo final (EndPoint); dicho de otro modo, se reduce la superficie de exposición. Desde otra orilla, según lo señalado por EY (2020), el 70 % de los incidentes y eventualidades presentadas se generan en el dispositivo final conectado a la red y, dentro de estos, los más implicados son el ordenador personal y el smartphone. Tal vez nos encontramos habituados a la saturación del término "Inteligencia Artificial", pero el mismo CCN reconoce que estos avances se estarían encargando de acelerar, considerablemente, la identificación de nuevas amenazas y sus posibles respuestas, para frenar o evitar los ataques, antes de que estos puedan presentarse o propagarse.

Según Azcoitia (2019), hoy día, muchas empresas están utilizando herramientas para analizar la seguridad de sus productos; dentro de este gran cúmulo de herramientas, entre las más destacadas son las conocidas como GANS (Generative Adversarial Networks), las cuales permiten detectar los fallos que hay en un modelo de Machine Learning. Adicionalmente, pueden ser utilizadas para entrenar determinados modelos y hacerlos más robustos. Las GANS hacen referencia a algoritmos de inteligencia artificial diseñados para llevar a cabo aprendizajes automáticos no supervisados, y se encuentran compuestos por un sistema de redes neuronales que compiten entre sí. Enseguida, presentamos 3 *Frameworks*, para entrenar los modelos de *Machine Learning*:

Deep -Pwing

Consiste en un framework desarrollado en Tensorflow[1], que permite experimentar con modelos de *Machine Learning*, cuya finalidad es evaluar su nivel de robustez, frente a un posible ataque, además, permite que sus conocimientos puedan ser ampliados en forma paulatina, generando la posibilidad de que, en un futuro, pueda llegar a ser una herramienta para realizar test de penetración y posibilitar estudios estadísticos sobre algunos modelos de *Machine Learning* (Azcoitia, 2019).

Adversarial Lib

Consiste en una librería escrita en lenguaje Python y que se encuentra diseñada para evaluar la seguridad en base a clasificadores *Machine Learning*, frente a posibles ataques o intrusiones; cuenta con la posibilidad de lanzar un script o pequeño trozo de código y soporta una amplia gama de algoritmos de *Machine Learning*, que optimiza y reescribe en C++. Adicionalmente, en caso de necesitar un algoritmo que no esté disponible en la librería, cuenta con la posibilidad de añadirlo, lo que la convierte en una herramienta cada vez más completa (Zambrano, 2018).

The Gan Zoo

Es una página de referencia en la que se pueden encontrar una gran cantidad de GANS con las que es posible entrenar y evaluar modelos de *Machine Learning*. The GAN Zoo tiene detrás de sí una gran comunidad de desarrolladores, que cada semana añaden nuevos pappers a su repositorio en GitHub (The Gan Zoo, 2018). En suma, el *Machine Learning* se ha convertido en una herramienta de gran valor para investigadores y desarrolladores en el campo de la ciberseguridad, ya que implica la posibilidad de llevar a cabo o ejecutar numerosos tests que, en cuanto a seguridad y penetración, permiten un ahorro de tiempo y esfuerzo considerable (Flores Sinani, 2020).

Deep Learning en Ciberseguridad

El "aprendizaje profundo", o Deep Learning, es un área —dentro del *Machine Learning*— que consiste en un método de aprendizaje automático. Es usado para entrenar una Inteligencia Artificial y poder predecir "x" salidas, teniendo en cuenta un

1 Es una biblioteca de código abierto para la computación numérica y *Machine Learning* a gran escala.

conjunto de entradas; cosa que permite predecir resultados con la combinación de un conjunto de datos. Su gran fortaleza estriba en que aprende en tiempo real y es capaz de desarrollar nuevos criterios de clasificación, sin que exista intervención humana. Entre otros usos, se está aplicando contra el malware y el fraude online, dado que los cibercriminales y piratas informáticos evolucionan rápidamente, ocasionando amenazas capacitadas para adaptarse a la seguridad de los sistemas. Por lo tanto, Deep Learning es capaz de detectar y clasificar dichas amenazas, además de generar una solución de forma eficiente y veloz.

Sus aplicaciones pueden llegar a ser infinitas, verbigracia, se utilizan como método de identificación; lo que les permite determinar si el usuario es un humano o un Bot; o si un cibercriminal está pretendiendo suplantar la identidad de un usuario; o si está interactuando con la cuenta de un usuario desde cualquier parte del mundo (Universidad de Alcala, s.f.)

Figura 8. *Funcionamiento de un sistema de Deep Learning*

Fuente: Feedzai, s.f.

Check Point
Empresa de origen israelí, creada en 1993 y especializada en cortafuegos, enfocada en la protección integral, mediante la actualización permanente de aprendizaje de sus motores de ML. Su servicio centralizado, *Campaing Hunting*, explora todos los puntos de la red y analiza anomalías. Todo esto crea una plataforma de protección desde la nube.

Crowdstike
Se enfoca en el análisis exhaustivo del comportamiento del usuario y sus dispositivos, con la finalidad de identificar virus, malware, robo de credenciales y amenazas internas, entre otros. El fundamento de este tipo de protección consiste en la creación de técnicas de *Machine Learning*, a partir de un modelo de actividad normal, o línea base, que permite identificar (en tiempo real) las desviaciones respecto al modelo y actuar en forma preventiva.

Dakrtrace
Consiste en una plataforma que modela una línea base y se encuentra más enfocada en la prevención de intrusiones en redes WAN, LAN y WiFi. Sus mecanismos de *Machine Learning* mejoran el modelo en forma constante, sin necesidad de intervención humana, y de forma adaptativa a las necesidades e idiosincrasia del cliente, mejorando la capacidad de defensa en forma indefinida.

Deep Instinct

Empresa cuyo origen se remonta a 2015, con la idea específica de crear una plataforma de *Deep Learning* para la prevención de ataques en los dispositivos finales del usuario. Su finalidad principal radica en reducir por debajo de los 20 ms el tiempo de reacción, frente a una amenaza en el dispositivo final, entre otras cosas, ponen de relieve el potencial alcance de la tecnología de *Deep Learning*. *Deep Instinct* ha colocado su esfuerzo de 5 años en entrenar su red neuronal y producir un agente desplegable en dispositivos de todo tipo.

Aplicaciones del *Machine Learning* para mejorar la ciberseguridad en los entornos empresariales

Un ejemplo ilustrativo es el del lavado de dinero, ya que se pueden crear equipos más eficientes y efectivos para poder automatizar el enriquecimiento y priorización de casos para los investigadores. Por medio de la automatización, se logra reducir significativamente la cantidad de falsos positivos generados. Dependiendo del tamaño del banco, los analistas pueden llegar a investigar entre 20 y 30 alertas de falsos positivos al día. A menos que se cuente con recursos ilimitados para revisar alertas, se debe plantear una estrategia diferente (Feedzai, 2022).

De acuerdo a lo expuesto por Fernandez Khatibou (2019), el *Machine Learning*, dentro del ámbito financiero, puede ser aplicado a la detección de fraudes bancarios, por ejemplo, la firma Visa ha estado usando y mejorado continuamente su tecnología, para detección de fraudes, enfocándose en modelos escalables de aprendizaje automático y en el aprendizaje profundo, lo que les ha permitido variar el rango de datos a utilizar, para llegar a una conclusión en diferentes contextos; asimismo, se enfocan en soluciones que incluyen otras técnicas, como el análisis predictivo en tiempo real. En ciberseguridad son empleados potentes algoritmos de *Machine* y *Deep Learning*, con la finalidad de realizar análisis de malware, de detección y prevención de intrusos. El desarrollo de estos algoritmos se basa en el enfoque de anticiparse a un ciberataque y de restringir el acceso a los archivos o programas infectados (Handa *et al.*, 2019).

En relación con los drones, también se han presentado grandes avances en el contexto de la seguridad; con el uso de dicho tipo de vehículos no tripulados, se puede ampliar el campo de visión en la videovigilancia de grandes superficies; al respecto tomemos como ejemplos: parques, terrenos agrícolas y naves industriales. Se trata, a su vez, de vehículos versátiles que pueden programarse para realizar inspecciones rutinarias y automáticas, o bien ser pilotados en forma manual; de igual modo, pueden ser configurados y enfocados para realizar tareas de reconocimiento facial y detectar la presencia de intrusos, a quienes busca y localiza. Además, al no ser sistemas fijos, hace que sea más complicado evadirlos o destruirlos (Prevent Security Sistems, s.f.).

Discusión

Es irrefutable el papel que viene adquiriendo la Inteligencia artificial y, en especial, el *Machine* y *Deep Learning*, en el campo de la ciberseguridad personal y empresarial. Se trata, pues, de un panorama tecnológico en constante evolución, que va de la mano con el incremento de cibercrímenes y ciberataques; cuyas innovaciones nos conducen a desafíos de seguridad, cada vez más complejos e intrincados. Es por ello que, actualmente, las empresas ya han comenzado a explorar cómo el *Machine Learning*, aplicado a la ciberseguridad, puede ayudar a mitigar estos riesgos. Se ha visto, últimamente, que las tasas de adopción de la Inteligencia artificial en la ciberseguridad están en constante aumento. Al mismo tiempo, es claro que las organizaciones deben identificar dónde implementarla, para aportar, así, en mayor valor y, posteriormente, establecer metas más acordes con su rendimiento o expectativas.

Aunque, como hemos visto, existen muchas técnicas, soluciones y modelos, que hacen uso del *Machine* y *Deep Learning*, para el análisis de datos, aún hace falta un largo camino, teniendo en cuenta que

los ciberdelincuentes —al igual que los avances tecnológicos— se encuentran en constante cambio. Se ha podido evidenciar, finalmente, cómo en Latinoamérica el tema relacionado con el cibercrimen ha ido creciendo exponencialmente y, cómo las estrategias para contrarrestar los mismos, también. Tomemos, como ejemplo, a uno de los países con más afectación al respecto (México), que ha logrado contrarrestar este tipo de acciones con una serie de contramedidas, adoptadas con base en la experiencia, al igual que Chile o Brasil, aunque queda bastante camino por andar en el tema.

Referencias

Arteaga, F. (2013). La estrategia de seguridad nacional. Madrid: Comentario Elcano.

Azcoitia, S. S. (2019). Machine Learning para el Pentesting: La Importancia de la IA en el ámbito de la Ciberseguridad [Recurso en línea]. *Telefonica Tech*. Recuperado de https://empresas.blogthinkbig.com/machine-learning-para-el-pentesting-la/

Ballestero, F. (2020). La ciberseguridad en tiempos difíciles. *Revistas ICE*, 39-48.

Capgemini Research Institute. (2019). *Reinventing Cybersecurity with Artificial Intelligence. The new frontier in digital security* [en línea]. *Capgemini Research Institute.* Recuperado de https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf

Chan, P. y Lippmann, R. (2006). Machine learning for computer security. *The Journal of Machine Learning Research*, 669-672.

Esparza Cruz, N. K. (2017). El Comercio Electrónico en el Ecuador [en línea]. *Journal of science and research*, 29-32. Recuperado de doi:https://doi.org/10.26910/issn.2528-8083vol2iss6.2017pp29-32

EY. (2020). Why a culture change program is key to effective cybersecurity [en línea]. Recuperado de https://www.ey.com/en_se/giss/why-a-culture-change-program-is-key-to-effective-cybersecurity

Feedzai. (s.f.). La verdad sobre el lavado de dinero [en línea]. Recuperado de https://feedzai.com/es/deep-learning-prevencion-de-fraude-online

Fernandez Khatiboun, A. (2019). *Machine Learning en Ciberseguridad.* Madrid: UOC.

Flores Sinani, C. (2020). Inteligencia Artificial, Machine Learning, Deep Learning aplicados a la Ciberseguridad. *Investigación, Ciencia y Tecnología en Informática*, 11-13.

French, D. y Casey, W. (2012). *Fuzzy Hashing Techniques in Applied Malware Analysis.* Ontario: SEI.

Gandotra, E., Bansal, D., & Sofat, S. (2014). Integrated framework for classification of malwares. *Proceedings of the 7th International Conference on Security of Information and Networks ACM* (pág. 417). Glasgow: ACM.

Geetest. (2020). Spam Bots and Comment Spam Explained: How to Keep Your SEO and Credibility. Recuperado de https://blog.geetest.com/en/article/spam-bots-and-comment-spam-explained-how-to-keep-your-seo-and-credibility

Handa, A., Sharma, A. y Shukla, S. (2019). *Machine Learning in cybersecurity: A review.* Ontario: WIREs Data Mining and knowledge discovery.

Hern, A. (2016). Cyber-attacks and hacking: what you need to know [en línea]. Recuperado de https://www.theguardian.com/technology/2016/nov/01/cyber-attacks-hacking-philip-hammond-state-cybercrime

IT Sitio. (2018). Cómo afecta el Deep Learning a la seguridad [en línea]. Recuperado de https://www.itsitio.com/ar/como-afecta-el-deep-learning-a-la-seguridad/

Jardine, E. (2015). *Global cyberspace is safer than you think: real trends in cybercrime.* Waterloo -Ontario: Chatam House.

Muñoz, A. (2017). Machine learning aplicado a ciberseguridad.

Oktavianto, D. y Muhardianto, I. (2013). *Cuckoo Malware Analysis.* Washington: Packt Publishing Ltd.

OPSWAT. (s.f.). OPSWAT Announces New Malware Analysis Tool in Metascan Online. [Entrada de blog]. Recuperado de https://www.opswat.com/blog/opswat-announces-new-malware-analysis-tool-metascan-online

Prevent Security Sistems. (s.f.). Videovigilancia y RGPD [en línea]. Recuperado de https://www.prevent.es/

Sánchez, B. (2015). Detección de código malicioso con YARA [en línea]. Recuperado de https://www.securityartwork.es/2015/03/20/deteccion-de-codigo-malicioso-con-yara-i/

Saytlarga (s.f). Community uzbekcoders [en línea]. Recuperado de https://community.uzbekcoders.uz/post/saytlarga-xss-hujum-turi-haqida-6001b5d9eb078050507f5110

Sikorski , M. y Honig, A. (2012). *Practical Malware Analysis.* San Francisco: no starch press.

The Gan Zoo. (2018). Github [en línea]. Recuperado de https://github.com/hindupuravinash/the-gan-zoo

Universidad de Alcalá. (s.f.). El camino de deep learning hacia la ciberseguridad [en línea]. Recuperado de de https://master-deeplearning.com/camino-deep-learning-ciberseguridad

Urcuqui López, C. C., García Peña, M., Navarro Cadavid, A., y Osorio Quintero, J. L. (2019). *Ciberseguridad: un enfoque desde la ciencia de datos* [en línea]. Cali: Universidad Icesi. Recuperado de doi:https://doi.org/10.18046/EUI/ee.4.2018

Valero Campaña, M. (2015). *Detección de malware usando herramientas de Big Data* [Tesis de grado]. Sevilla: Universidad de Sevilla.

Yumbo Anis, L. (2016). *Análisis de técnicas para la detección de amenazas de seguridad utilizando machine learning* [Tesis de grado]. Guayaquil: Universidad de Guayaquil.

Zambrano, J. (2018). ¿Aprendizaje supervisado o no supervisado? [en línea]. Recuperado de https://medium.com/@juanzambrano/aprendizaje-supervisado-o-no-supervisado-39ccf1fd6e7b