**Resumen**

Las Redes Definidas por Software (SDN) representan un nuevo modelo de red que separa la funcionalidad de control de la gestión de datos, lo que puede mejorar significativamente la eficiencia y flexibilidad de esta última. Sin embargo, se enfrenta a importantes amenazas, que ponen en peligro la seguridad y disponibilidad de los datos y servicios. Este trabajo tiene como objetivo definir un modelo de clasificación de ataques mediante técnicas de aprendizaje automático, para mejorar la capacidad de defensa y aumentar la seguridad de la gestión de datos en SDN. Para esto, se realizó una revisión sistemática de la literatura (SLR) siguiendo la metodología de Bárbara Kitchenham, cuyos resultados muestran información de los principales conjuntos de datos y las técnicas de aprendizaje automático más utilizadas en SDN. Además, se aplicó las metodologías de investigación en ciencia del diseño (DSR), el descubrimiento de conocimiento en bases de dato (KDD) y el análisis exploratorio de datos (EDA) para desarrollar los modelos de aprendizaje automático. Se utilizó dos conjuntos de datos públicos con tráfico SDN y se entrenaron tres modelos de aprendizaje automático: árboles de decisión (DT), bosques aleatorios (RF) y máquinas de soporte vectorial (SVM), con la aplicación de diferentes grupos de características. Los resultados obtenidos en la fase de entrenamiento fueron 99,76%, 99,31% y 99,50% de precisión, para DT, RF y SVM respectivamente. Sin embargo, en la fase de implementación, con la captura de tráfico de datos de red en directo y la clasificación de ataques en la plataforma SDN emulada en Mininet, se obtuvieron los siguientes resultados: 43,28%, 24,14% y 23,97% de precisión, para SVM, DT y RF respectivamente. Por lo tanto, los resultados obtenidos en este trabajo son mejores que el estado del arte y muestra el despliegue de un modelo de aprendizaje automático en una SDN.

***Palabras clave:*** Redes Definidas por Software, Ataques, Aprendizaje Automático

**Abstract**

Software-Defined Networking (SDN) represents a new network model that separates control functionality from data management, which can significantly improve the efficiency and flexibility of the latter. However, it faces significant security threats that endanger the security and availability of data and services. This work aims to define a model for classifying attacks using machine learning techniques to improve defense capabilities and increase data management security in SDN. To achieve this, a systematic literature review (SLR) was conducted following the methodology of Barbara Kitchenham, whose results provide information on the main data sets and machine learning techniques most used in SDN. In addition, research methodologies in design science (DSR), knowledge discovery in databases (KDD), and exploratory data analysis (EDA) were applied to develop the machine learning models. Two public datasets with SDN traffic were used, and three machine learning models were trained: decision trees (DT), random forests (RF), and support vector machines (SVM), with the application of different feature sets. (SVM), with the application of different feature sets. The results obtained in the training phase were 99.76%, 99.31%, and 99.50% accuracy for DT, RF, and SVM, respectively. However, in the implementation phase, with the capture of live network data traffic and attack classification on the SDN platform emulated in Mininet, the following results were obtained: 43.28%, 24.14%, and 23.97% accuracy for SVM, DT, and RF, respectively. Therefore, the results obtained in this work are better than state-of-the-art and demonstrate the deployment of a machine learning model in an SDN.

***Keywords:*** Software Defined-Networking, Attacks, Machine Learning.