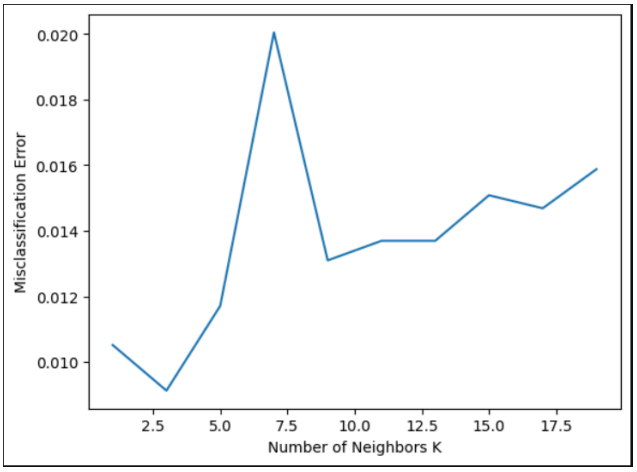
Datos, ciberseguridad e inteligencia artificial
Fecha: 17-06-2025.
Alumno: Taisen Romero Bañuelos.

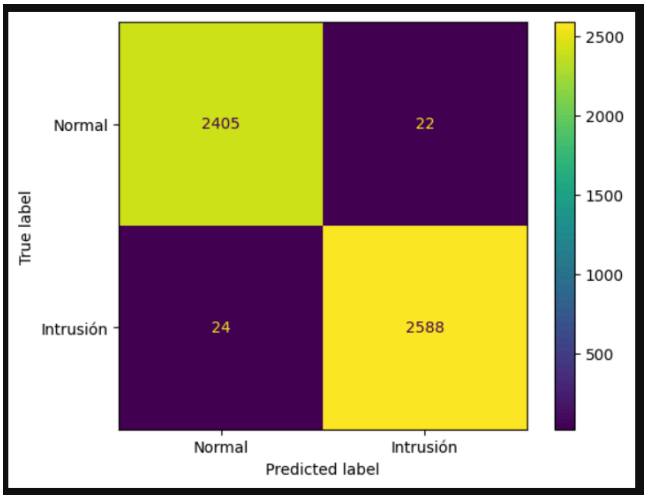
Aprendizaje supervisado - Clasificación

Las técnicas de clasificación surgen de manera orgánica como una solución ante los ataques de seguridad, tanto como una medida preventiva como una herramienta de análisis forense, y esta práctica me permitió explorar más a fondo uno de estos enfoques: el uso de k-vecinos más cercanos (k-NN) para la detección de intrusiones en redes simuladas.
Personalmente me he interesado más en un estudio de la ciberseguridad enfocado al red team, aunque por supuesto he tenido que leer algunas cosas del blue team. En esos momentos entendía las explicaciones de cómo operaba el blue team, pero ahora tengo un entendimiento más profundo ya que puedo nombrar las técnicas y metodologías de algunas estrategias de prevención y mitigación que había estudiado sin entrar en profundidad. Haber implementado un modelo de clasificación me permitió comprender con mayor claridad cómo los sistemas de defensa evalúan comportamientos y patrones de tráfico para detectar anomalías. Pero dejando de lado eso, sobre la actividad en cuestión me gustaría hablar de que tuve unas ligeras diferencias con respecto a los resultados del PDF, la más notoria fue el gráfico para el valor óptimo de k.

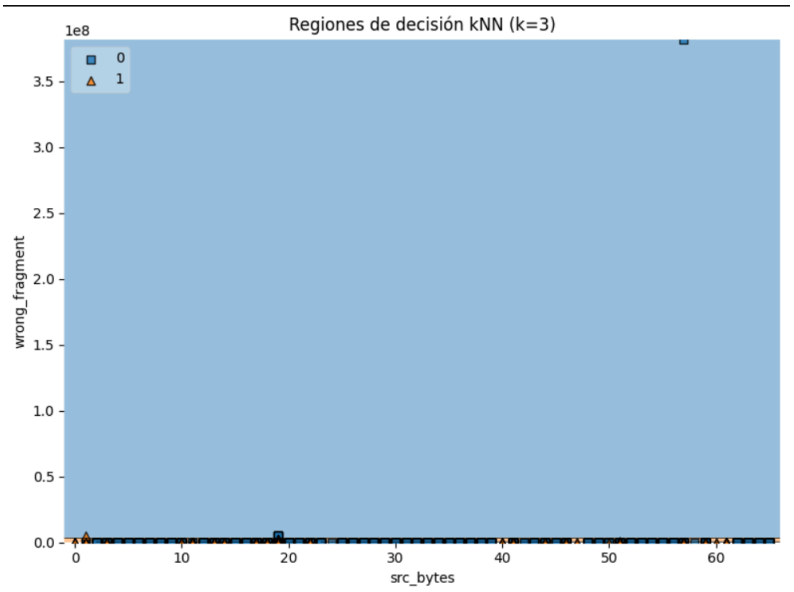


Como se ve mi gráfico muestra un repunte importante en 7.5, pero eso no afecta en nada ya que coincide en que k=3 es el k óptimo. La precisión obtenida en mi implementación fue de 0.9908712046048881 y el recall de 0.9908116385911179, valores prácticamente equivalentes a los reportados en el material original.
Pese a haber implementado correctamente el modelo k-NN y evaluado su rendimiento, sentí que no se logró una conexión profunda con el dataset en sí. Es decir, nos

enfocamos en aplicar k-NN y afinar el valor de k, pero no hubo un análisis exhaustivo del contexto de las características de las conexiones de red. Entonces, para no quedarme con el mal sabor de boca probé algunas cosas de entre las cuales destaca una matriz de confusión.



La matriz de confusión que obtuve muestra una clasificación equilibrada, sin sesgo significativo hacia falsos positivos ni falsos negativos, lo cual es bueno. También intenté generar una visualización de las regiones de decisión del modelo con k=3, pero el resultado fue poco informativo.



Es posible que las variables elegidas no hayan sido las más adecuadas para graficar, o que se requiriera una transformación previa, pero el tiempo se me fue de las manos y me resulta complicado continuar afinando detalles. Pero para cerrar, me gustaría resaltar que si bien esta implementación sirvió como práctica técnica, siento que un

paso adicional valioso sería analizar la contribución de cada variable al proceso de clasificación, tipo evaluar la importancia de las características y vincularlas al comportamiento real de una intrusión o una conexión normal. Sea como sea mantengo en mente que esto apenas es una introducción y que la práctica ya era de por si algo extensa, por lo que comprendo que algunos aspectos importantes se hayan omitido.