CIBERSEGURIDAD: APLICACIÓN DE TÉCNICAS DE MACHINE LEARNING PARA LA DETECCIÓN DE INTRUSIONES EN RED

Trabajo Final de Máster

Máster en Inteligencia Artificial

Antonio Daniel Moreno Prieto
Tutor:
Madrid · 26 de Mayo de 2026

Contexto del proyecto

- La ciberseguridad es un ámbito clave en sistemas conectados
- Las redes generan grandes volúmenes de tráfico
- Es necesario detectar comportamientos anómalos o potencialmente peligrosos
- Machine Learning permite automatizar parte de esta detección

Caso planteado

- Diferenciar conexiones normales y conexiones anómalas dentro del tráfico de red
- Analizar variables relacionadas con protocolos, servicios y comportamiento de las conexiones
- Entrenar modelos capaces de detectar patrones asociados a posibles intrusiones
- Comparar distintos modelos de Machine Learning para identificar el más eficaz

Objetivos del proyecto

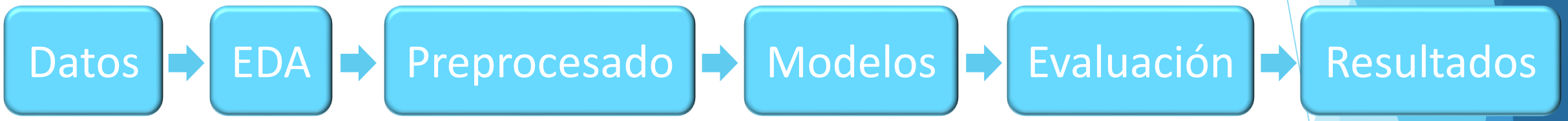
- Aplicar técnicas de Machine Learning para la detección de intrusiones en red
- Analizar un dataset de tráfico de red orientado a ciberseguridad
- Preparar y transformar los datos para el entrenamiento de modelos
- Entrenar distintos modelos supervisados de clasificación
- Evaluar y comparar el rendimiento de los modelos obtenidos

Dataset utilizado

- Dataset público obtenido desde Kaggle
- Archivos utilizados:
  - Train_data.csv
  - Test_data.csv
- Cada registro representa una conexión de red
- El tráfico se clasifica como normal o anómalo

Nº	Variable	Descripción
1	duration	Duración de la conexión
2	protocol_type	Tipo de protocolo de red
3	service	Servicio de red utilizado
4	flag	Estado de la conexión
5	src_bytes	Bytes enviados desde el origen
6	dst_bytes	Bytes enviados desde el destino
7	land	Conexión entre mismo host y puerto
8	wrong_fragment	Número de fragmentos incorrectos
9	urgent	Número de paquetes urgentes
10	hot	Número de accesos sospechosos

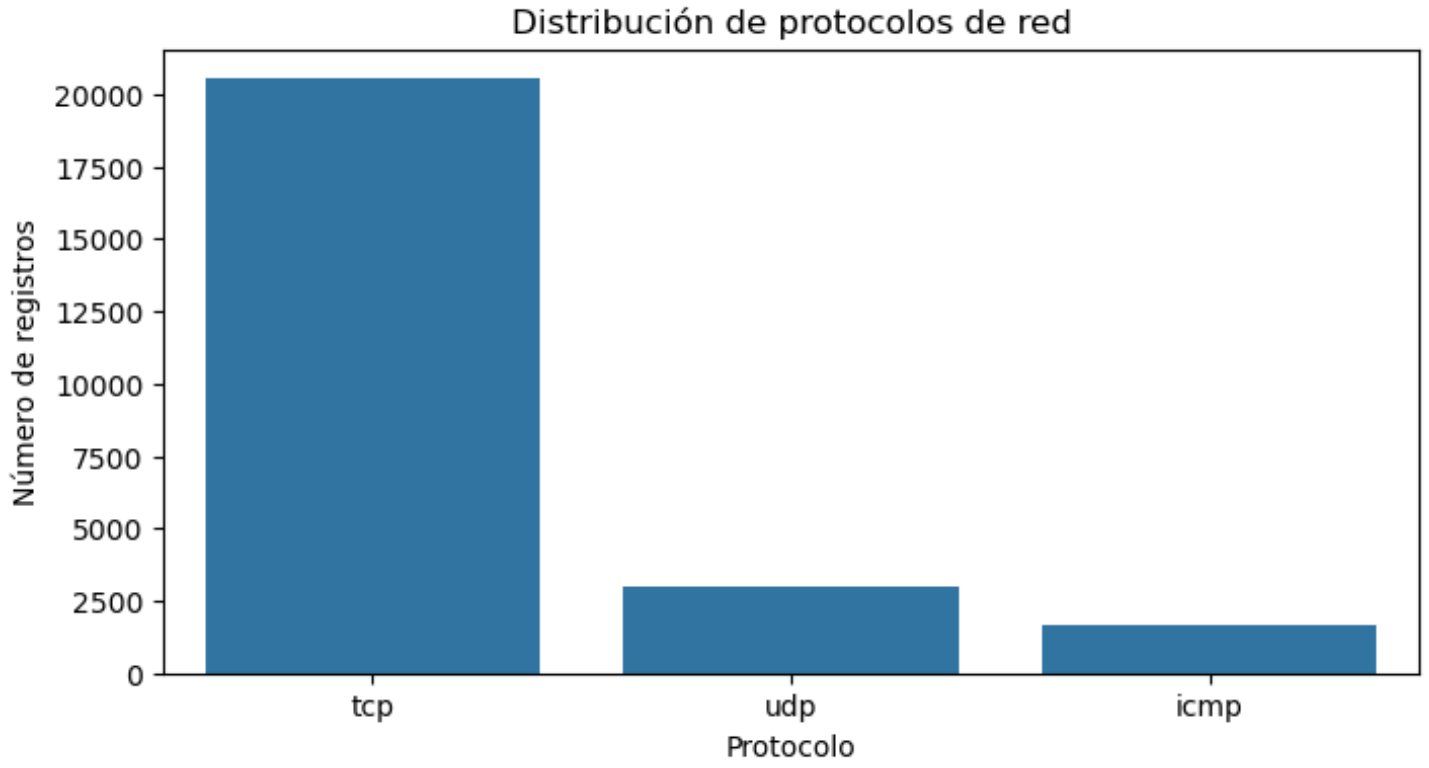
Flujo metodológico



Flujo general seguido durante el desarrollo del proyecto

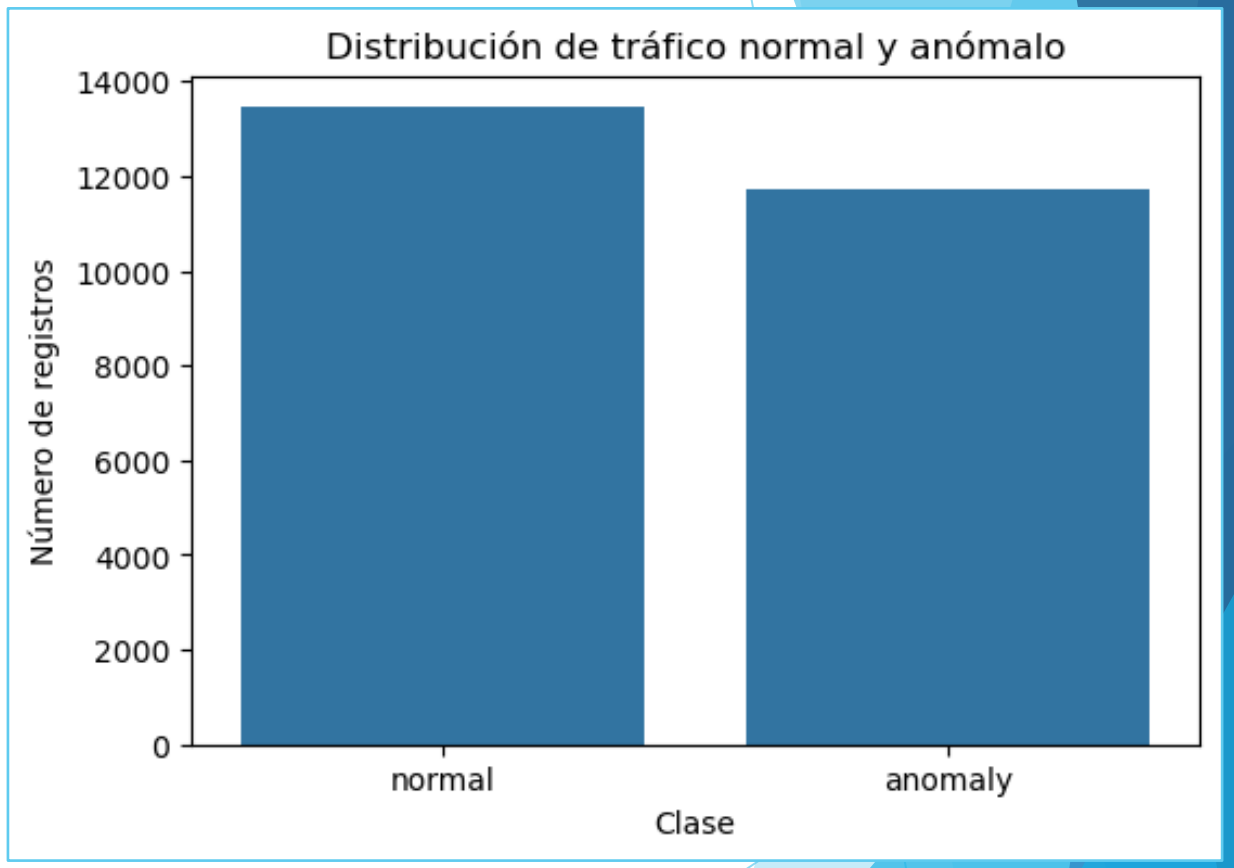
Análisis exploratorio de datos (EDA)

- Se analizaron variables numéricas y categóricas del dataset
- Se estudió la distribución de protocolos y servicios de red
- Se identificaron patrones relacionados con tráfico normal y anómalo



Distribución de conexiones

- El dataset contiene conexiones normales y conexiones anómalas
- Esto permite plantear el problema como una tarea de clasificación supervisada
- El modelo aprende patrones para diferenciar ambos tipos de tráfico



Preprocesado de datos

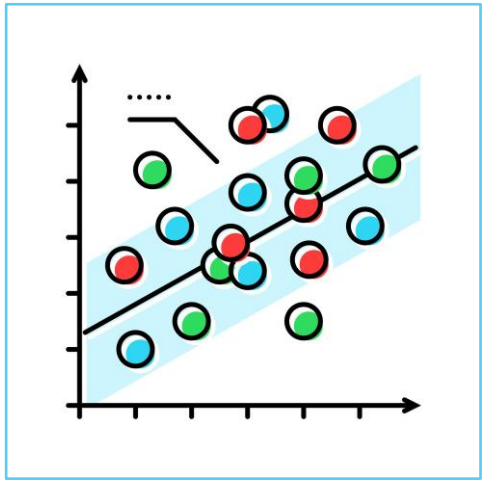
- Separación entre variables predictoras y variable objetivo
- Codificación de variables categóricas
- División en conjuntos de entrenamiento y validación
- Preparación de los datos para el entrenamiento de modelos

service_pop_3	service_printer	service_private	service_red_i	service_remote_job
False	False	False	False	False
False	False	False	False	False
False	False	True	False	False
False	False	False	False	False
False	False	False	False	False

Modelos aplicados

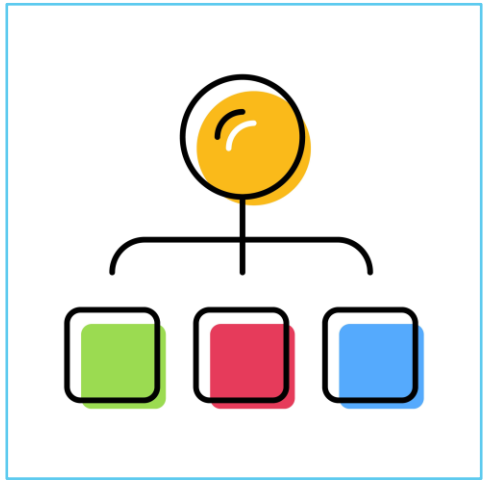
Regresión Logística

Modelo base de clasificación



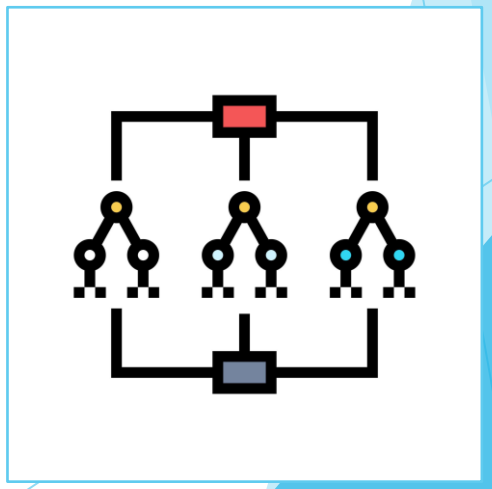
Árbol de Decisión

Modelo basado en reglas



Random Forest

Conjunto de múltiples árboles



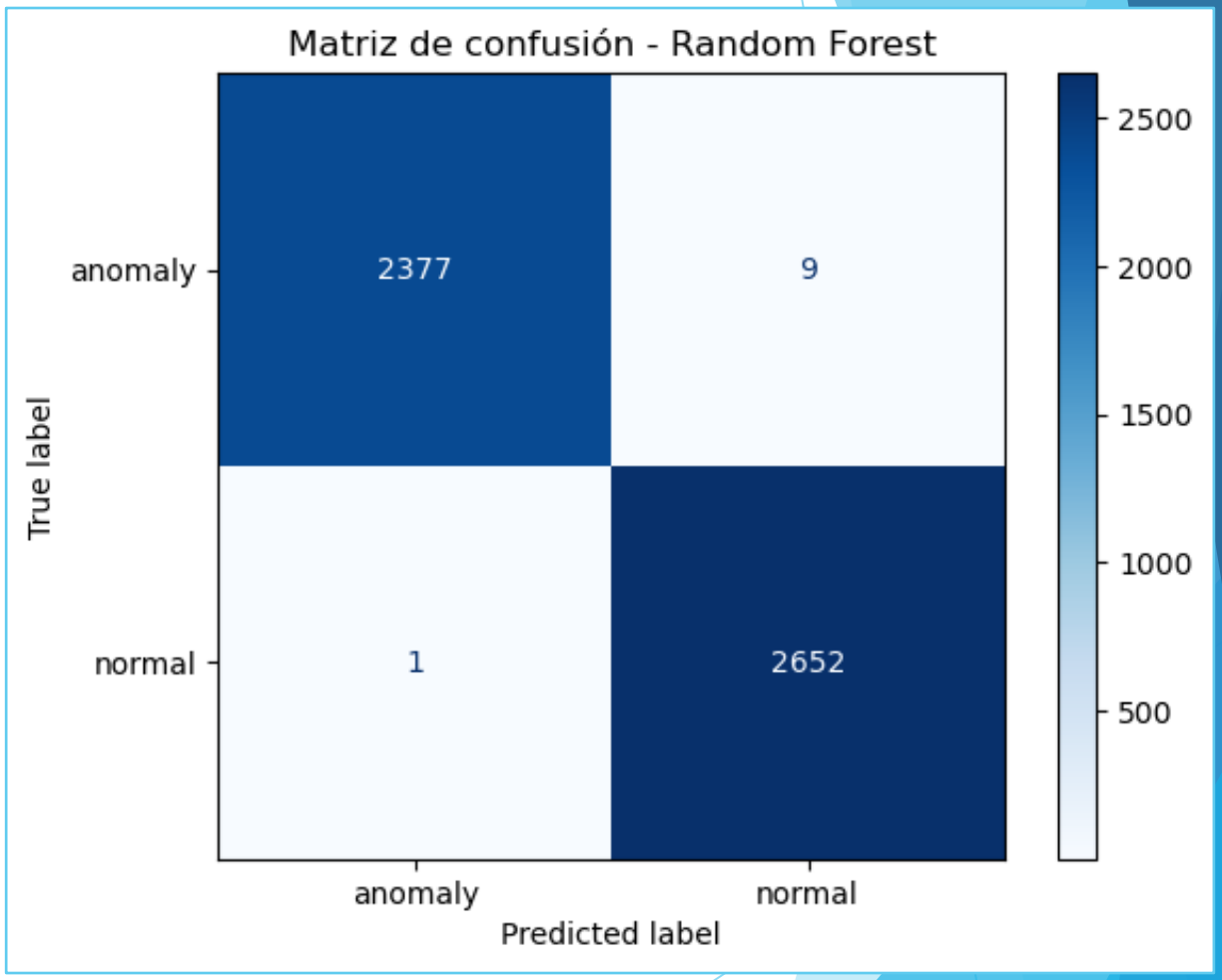
Comparativa de resultados

- Los tres modelos obtuvieron resultados elevados
- Se compararon métricas como accuracy, precision, recall y F1-score
- Random Forest alcanzó el mejor rendimiento general

	Modelo	Accuracy	Precision	Recall	F1-score
0	Regresión Logística	0.947609	0.937065	0.965322	0.950984
1	Árbol de Decisión	0.996626	0.996235	0.997361	0.996798
2	Random Forest	0.998015	0.996618	0.999623	0.998118

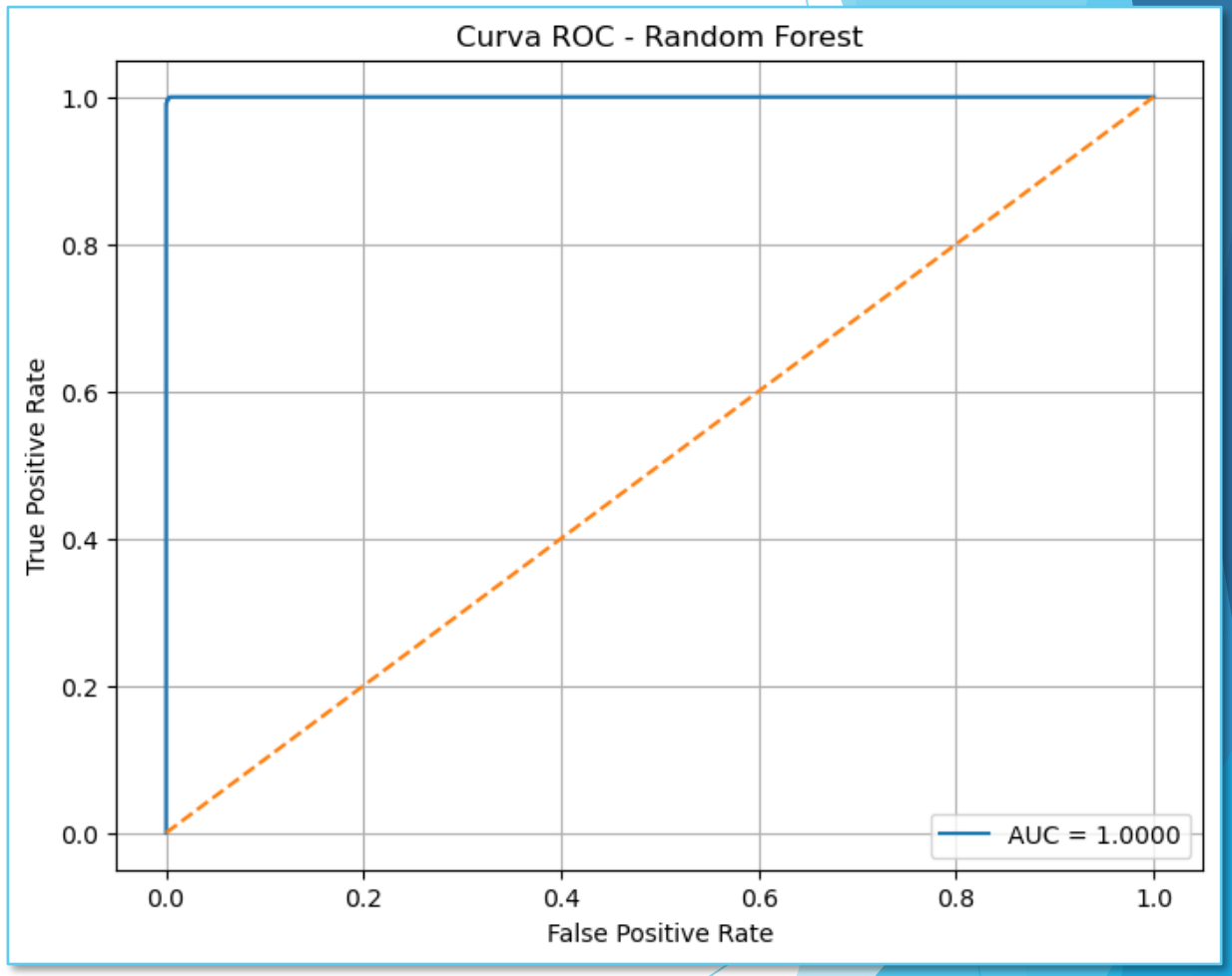
Evaluación del modelo Random Forest

- La matriz de confusión muestra muy pocos errores de clasificación
- El modelo identifica correctamente la mayoría de conexiones
- Se obtuvo un rendimiento muy elevado tanto en tráfico normal como anómalo



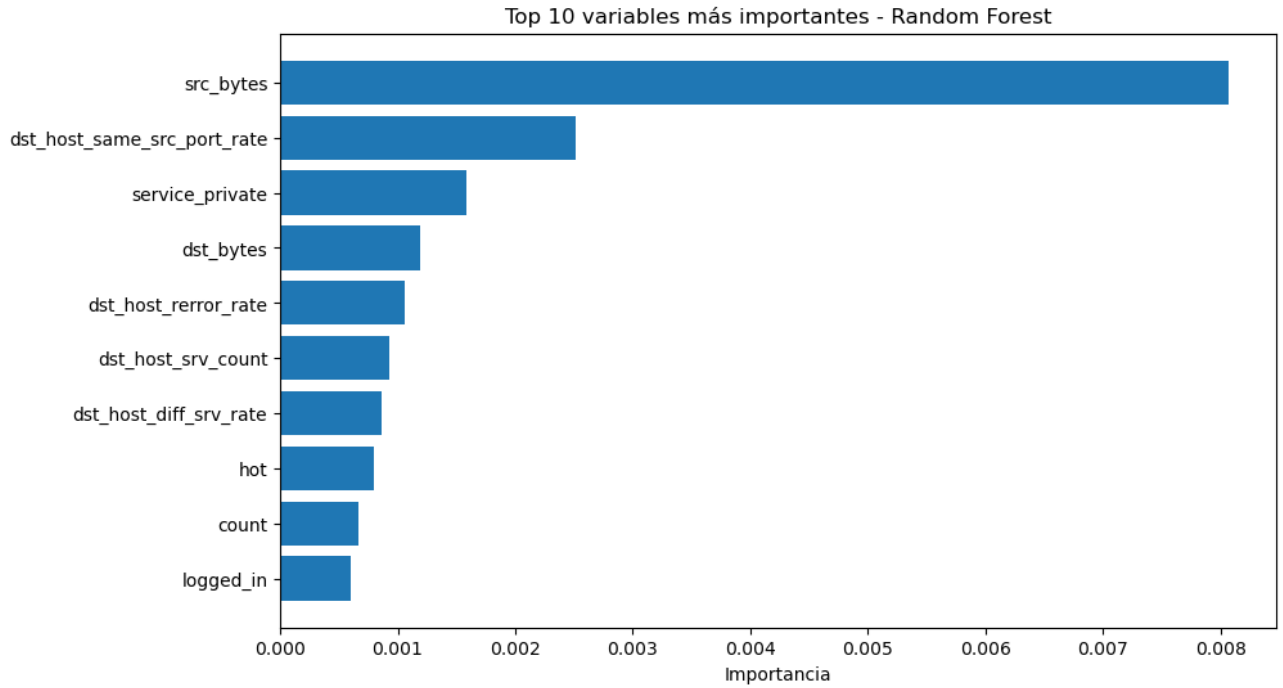
Capacidad de discriminación del modelo

- La curva ROC permite evaluar la capacidad de clasificación del modelo
- El valor AUC obtenido refleja un rendimiento muy elevado
- Random Forest distingue eficazmente entre tráfico normal y anómalo



Variables más relevantes

- El modelo identifica qué variables tienen mayor influencia en la clasificación
- Destacan variables relacionadas con volumen de tráfico y comportamiento de conexiones
- El análisis facilita una mejor interpretación del funcionamiento del modelo



Conclusiones

- Se desarrolló un flujo completo de análisis y Machine Learning aplicado a ciberseguridad
- Los modelos entrenados obtuvieron resultados muy elevados
- Random Forest presentó el mejor rendimiento general
- Las técnicas de evaluación confirmaron la calidad del modelo final
- Machine Learning resulta útil para la detección de intrusiones en red

Gracias por su atención