

# Trabajo Fin de Grado

## Detección de anomalías en tráfico de red con machine learning

Alba Ramos Pedroviejo

Tutor: Manuel Antonio Sánchez-Montañés Isla

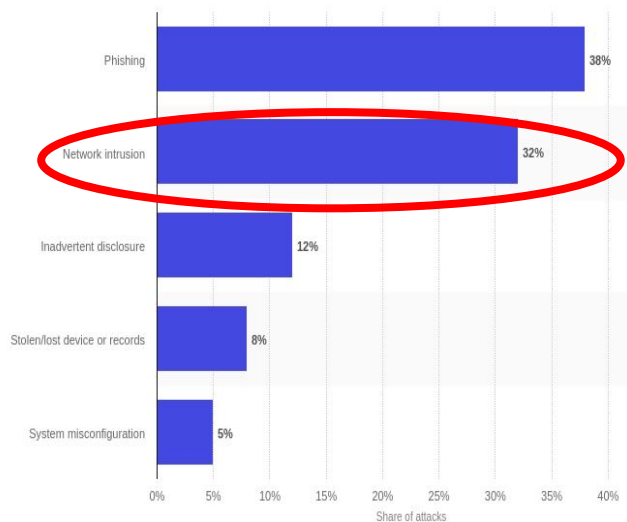
Escuela Politécnica Superior

# ÍNDICE DE CONTENIDOS

- Justificación
  - ¿Estamos protegidos?
  - ¿Por qué otro trabajo? ¿No funciona lo que hay?
- Objetivos
- Desarrollo
- Resultados
- Conclusiones

# ¿ESTAMOS PROTEGIDOS?

## Ataques de red en %



Fuente: Statista (2019)

## Distribución de ataques relacionados con la COVID-19



Fuente: Interpol (2020)

## Ciberataque SEPE

### AVISO IMPORTANTE

El SEPE ha sido objeto de un incidente de seguridad durante el cual se ha visto afectada la disponibilidad de sus sistemas de información y comunicaciones. Las primeras actuaciones urgentes efectuadas se han producido con la mayor celeridad posible y con el objetivo principal de contener el incidente, aislar y, por tanto, mitigar su impacto en los sistemas del SEPE.

Actualmente se está trabajando con el objetivo de restaurar los servicios prioritarios lo antes posible, entre los que se encuentra la Sede Electrónica del Servicio Público de Empleo Estatal. En estos momentos se encuentran disponibles:

- **Servicios de protección por desempleo** excepto:

[Servicios de protección por desempleo](#)

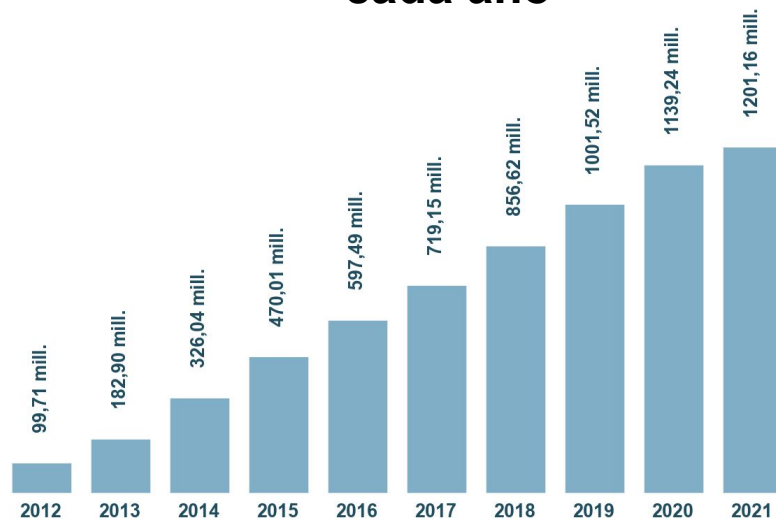
Fuente: Xataka (2021)

# ¿POR QUÉ NO FUNCIONA LO QUE HAY?

- Continua investigación
- Falta de metodología impide comparar <sup>[1]</sup>

- Datasets
  - Obsoletos
  - Poco representativos
  - Poco realistas
- Métodos de ML supervisados
  - Desequilibrio del dataset
  - Ataques *zero-day*

## Malware conocido cada año



Última actualización: 13 de April de 2021

Copyright © AV-TEST GmbH, [www.av-test.org](http://www.av-test.org)

[1] Magán-Carrión et al, 2020, p. 6

Fuente: AV-TEST (2021)

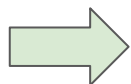
# OBJETIVOS

- Alertar ante ataques:
  - Conocidos
  - Zero-day
    - No alertar ante tráfico benigno novedoso
- Métodos supervisados + desequilibrio = problemas
- Metodología

# DESARROLLO

## Dataset ideal:

- Reciente
- Representativo
- Tráfico real



**UGR'16**


Dataset	Año	Registros	Tráfico
KDD-99	1999	4.9 M	Generado Obsoleto
UNSW-NB15	2015	2.5 M	Generado
UGR'16	2016	16.9 M	Real + generado
CIC-IDS 2017	2017	3.1 M	Generado.
CSE-CIC-IDS 2018	2018	15.4 M	Generado.
MAWI	1999 - actual.	Creciente	Real Errores

Fuente: propia

# DESARROLLO

## Extracción de atributos: FaaC <sup>[1]</sup>

- Contadores
- **Flujos de 2 minutos** <sup>[2]</sup>



Timestamp	Protocol	...
2016-07-27 16:00:20	TCP	
2016-07-27 16:00:20	UDP	
2016-07-27 16:00:21	UDP	
2016-07-27 16:00:21	TCP	
...		
2016-07-27 16:01:20	TCP	
2016-07-27 16:01:20	TCP	
2016-07-27 16:01:21	TCP	
...		

Timestamp	Protocol_TCP	Protocol_UDP	...
201607271600	2	2	
...			
201607271601	3	0	
...			

[1] Pérez-Villegas,  
García-Jiménez,  
Camacho, 2017

[2] Magán-Carrión et  
al, 2020, p. 6

Fuente: [2]

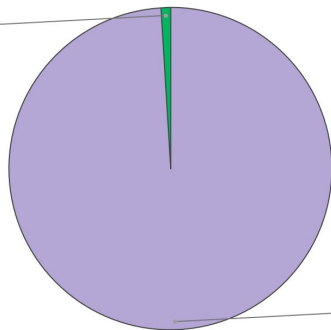
# DESARROLLO

## Preprocesamiento de datos:

- Partición train-test + reequilibrado SMOTE
- Normalización
- PCA: reducción dimensionalidad

Conjunto de training

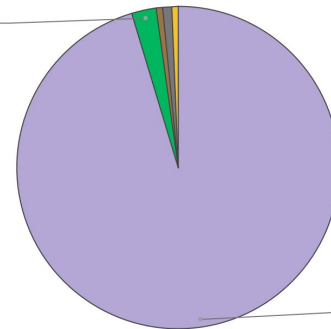
Ataques SSH  
1,0%



Tráfico benigno  
99,0%

Conjunto de test

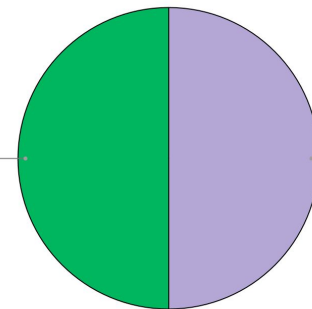
Ataques SSH  
2,5%



Tráfico benigno  
95,4%

Conjunto de training reequilibrado

Ataques SSH  
50,0%



Tráfico benigno  
50,0%

Fuente: propia



# DESARROLLO

## Métricas de rendimiento:

- Entrenamiento:
  - F1, Accuracy ⚠
  - GridSearch
- Pruebas
  - FP y FN sobre test
  - Accuracy sobre ataques

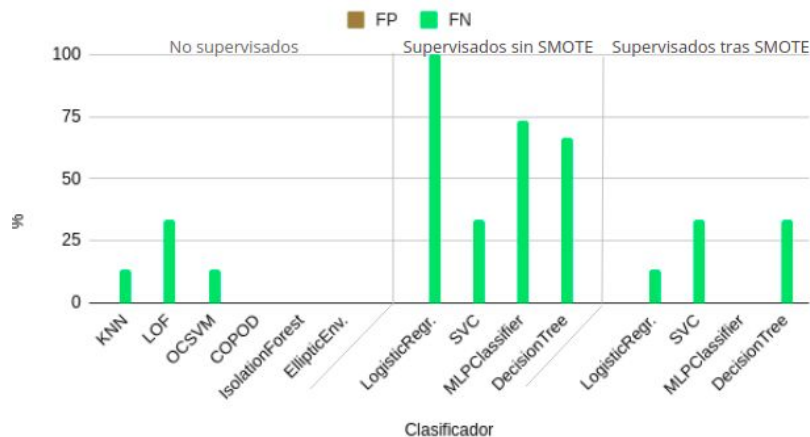
Modelos no supervisados	Modelos supervisados
KNN	LogisticRegression
LOF	SVC
OCSVM	MLPClassifier
COPOD	DecisionTree
IsolationForest	
EllipticEnvelope	

Fuente: propia

# RESULTADOS

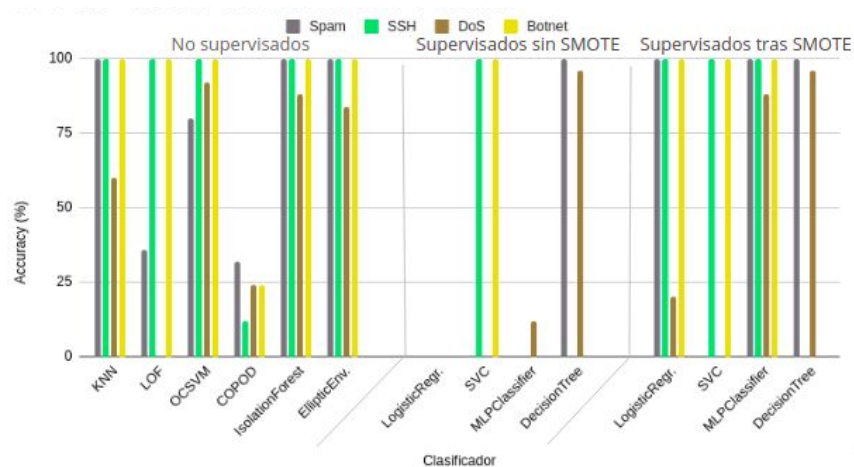
## FP y FN en test

- Normalidad aprendida
- Supervisados: más FN



## Accuracy ante ataques

- No supervisados: 0x1
- Supervisados: 0x1/2

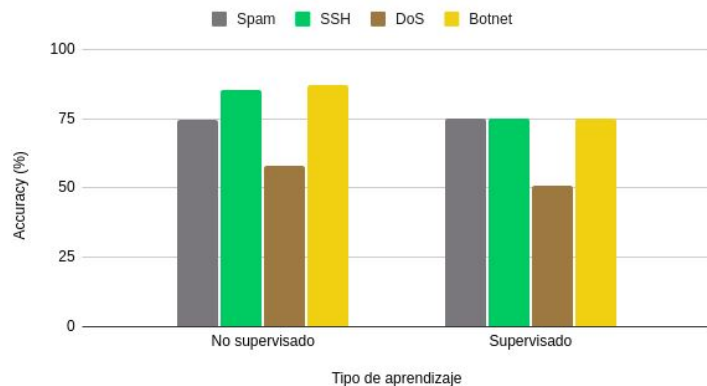


Fuente: propia

# RESULTADOS

## Accuracy acumulado por aprendizaje

- Dificultad DoS
- Facilidad Botnet



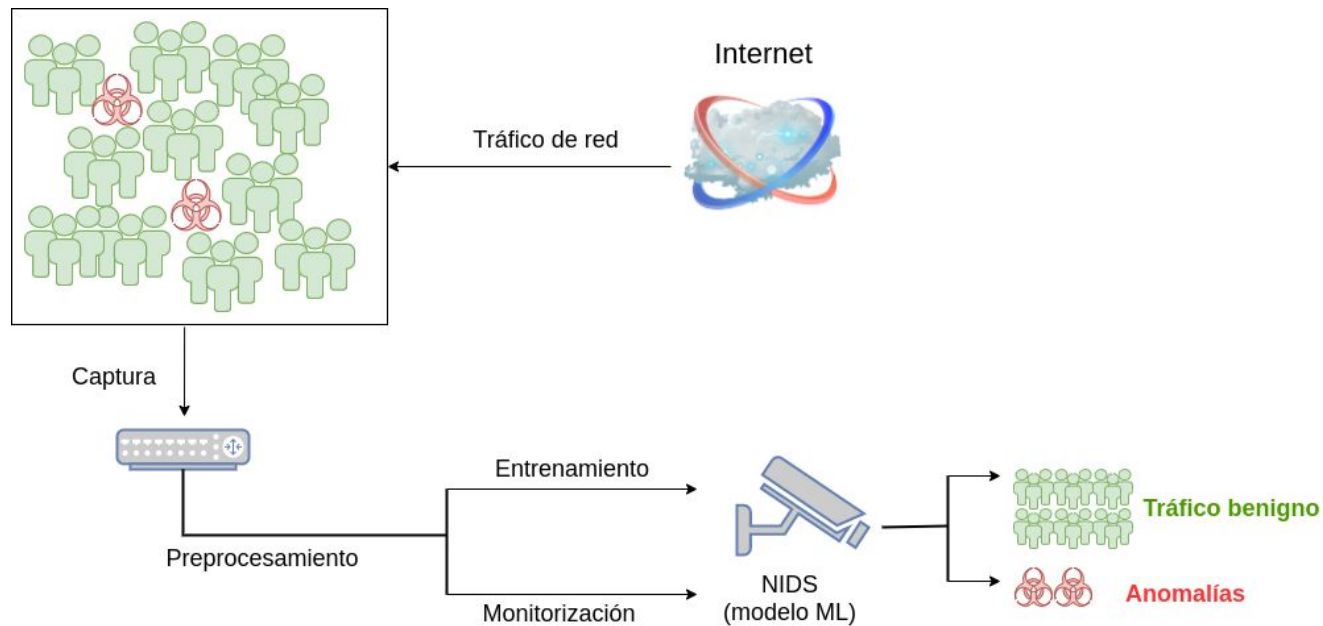
## Accuracy acumulado por modelo

- No supervisados: IsolationForest 97%
- Supervisados: MLP 97%



Fuente: propia

# RESULTADOS



Fuente: propia

# CONCLUSIONES

- Problema: detección de anomalías en tráfico de red con ML
  - Ataques conocidos y *zero-day*
  - Fuentes heterogéneas
- Solución:
  - Dataset real, actual y representativo (UGR'16)
  - Análisis temporal del tráfico (FaaC)
  - Modelos de ML
    - IsolationForest
    - MLP (reequilibrado, rapidez)

# Gracias por su atención

Alba Ramos Pedroviejo

[alba.ramosp@estudiante.uam.es](mailto:alba.ramosp@estudiante.uam.es)