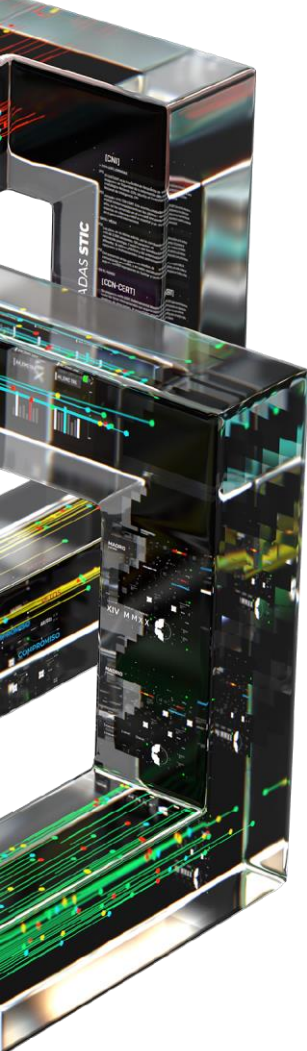




#XIVJORNADASCCNCERT

“Detección temprana de ataques a través del correo electrónico usando algoritmos inteligentes de Machine Learning y Deep Learning”



Carlos Cortés Danta

Ingenia

ccdanta@ingenia.es



Adrián Rodríguez García

Ingenia

adrianrg@ingenia.es

Agenda

- *Necesidades y modelos de ML & DL*
- *Implementación para la predicción de correos*
- *Demo - PoC*

El email sigue siendo protagonista

Emails por día a nivel mundial:



293.6
billones

2019

306.4
billones

2020

361.6
billones

2024



En 2020, el **53.95%** de los emails han sido SPAM
Principales emisores: China, USA, Rusia y Brasil



En 2019, hubo **26.2** billones de pérdidas en
ataques Business Email Compromise (BEC)

Fuentes: Statista y ENISA

Ciberamenazas y tendencias



Mejora significativa de las capacidades técnicas y operativas de actores ligados a la delincuencia económica (fraude al CEO (BEC), Human Operated Ransomware, etc.).

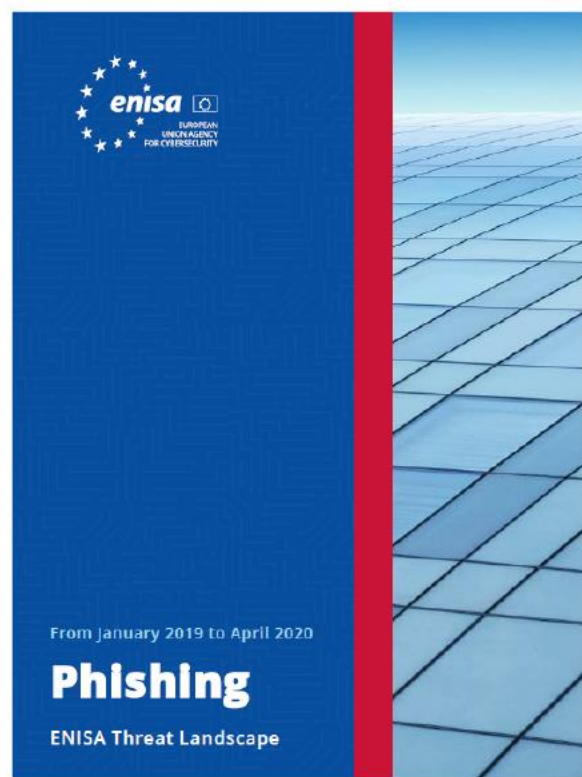


Explotación de sistemas expuestos a Internet por todo tipo de actores, hecho que se ha visto incrementado por la situación de pandemia y el incremento del teletrabajo (y la exposición no controlada de muchas organizaciones a Internet).



Necesidad, y tendencia, de los elementos ligados a **Inteligencia Artificial** en el ámbito de la seguridad, tanto para los atacantes como para los defensores.

Ciberamenazas y tendencias



26.2

billones de pérdidas en 2019 por ataques
Business Email Compromise (BEC)

42.8%

de los adjuntos maliciosos fueron documentos
Microsoft Office

667%

incremento en estafas de phishing en sólo un
mes durante la pandemia COVID-19

30%

de los mensajes de phishing se entregaron
en lunes

32.5%

de todos los emails usaron la palabra clave
"pago" como parte del asunto

Entre las acciones propuestas: Consider applying security solutions that use **Machine Learning** techniques to identify phishing sites in real-time



Atrápame si puedes

Imagen: LA Times



Machine Learning & Deep Learning para mejorar capacidades de Blue Team y Security Operations Centre (SOC)

Artificial Intelligence vs Machine Learning vs Deep Learning



AI

Una máquina es capaz de reproducir el comportamiento humano



ML

Una máquina es entrenada para reconocer patrones y hacer **predicciones**



DL

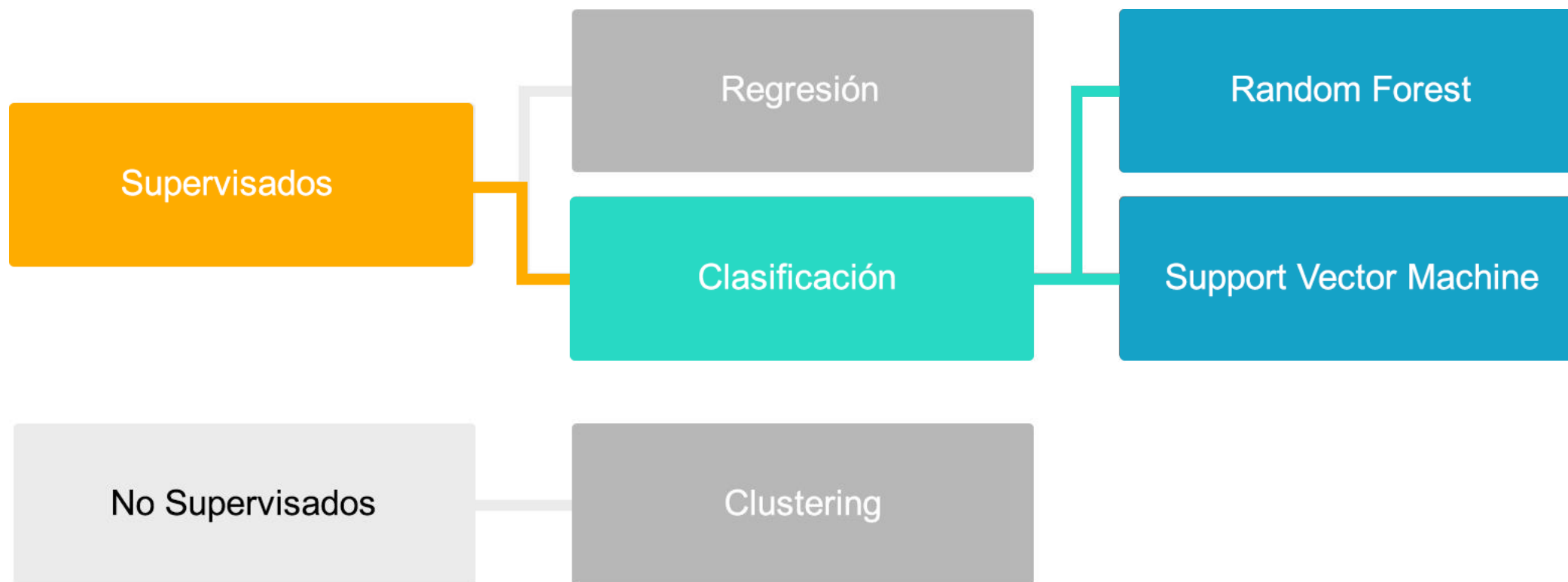
Una máquina es capaz, aprendiendo por sí misma, de razonar y sacar sus propias conclusiones para hacer **predicciones**

Usar ML & DL para
anticiparnos y predecir
si un correo es malicioso



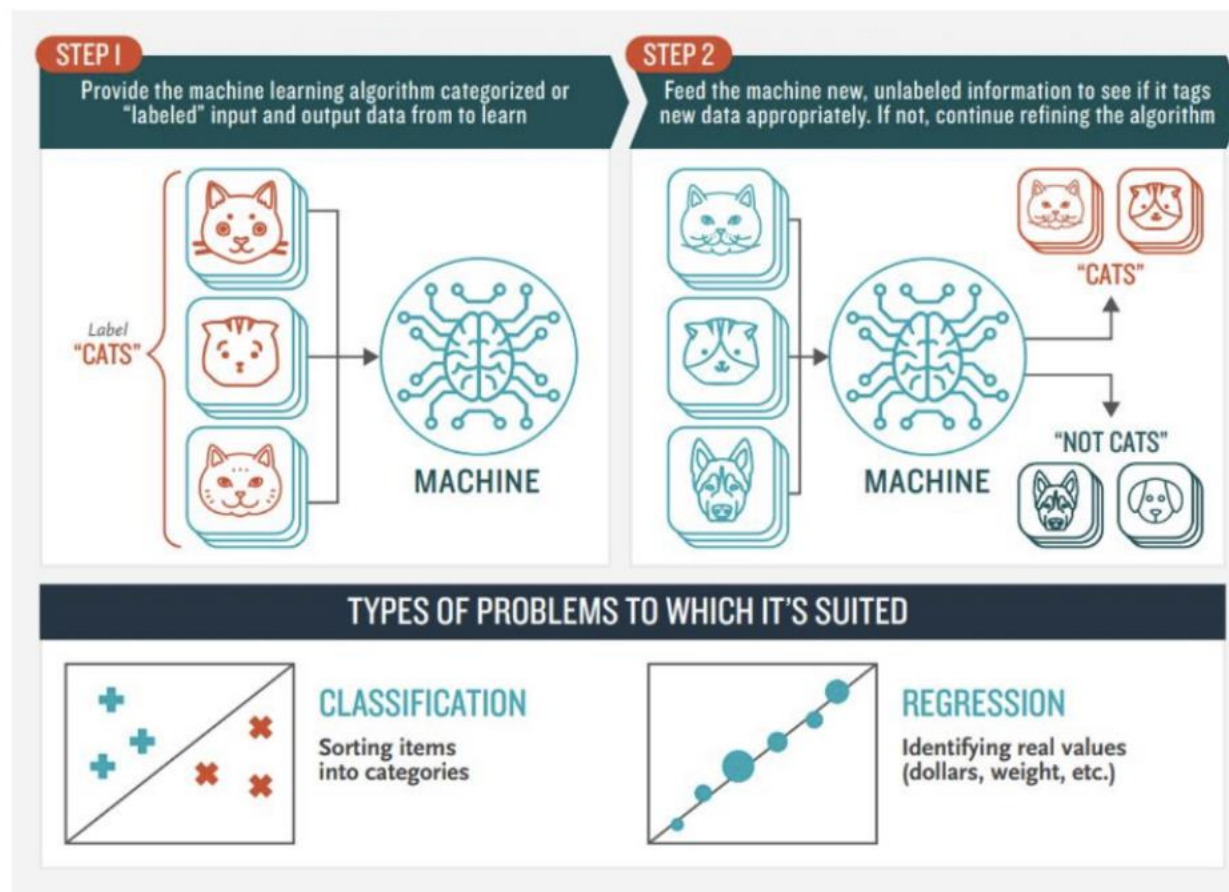
Machine Learning

Modelos



Machine Learning

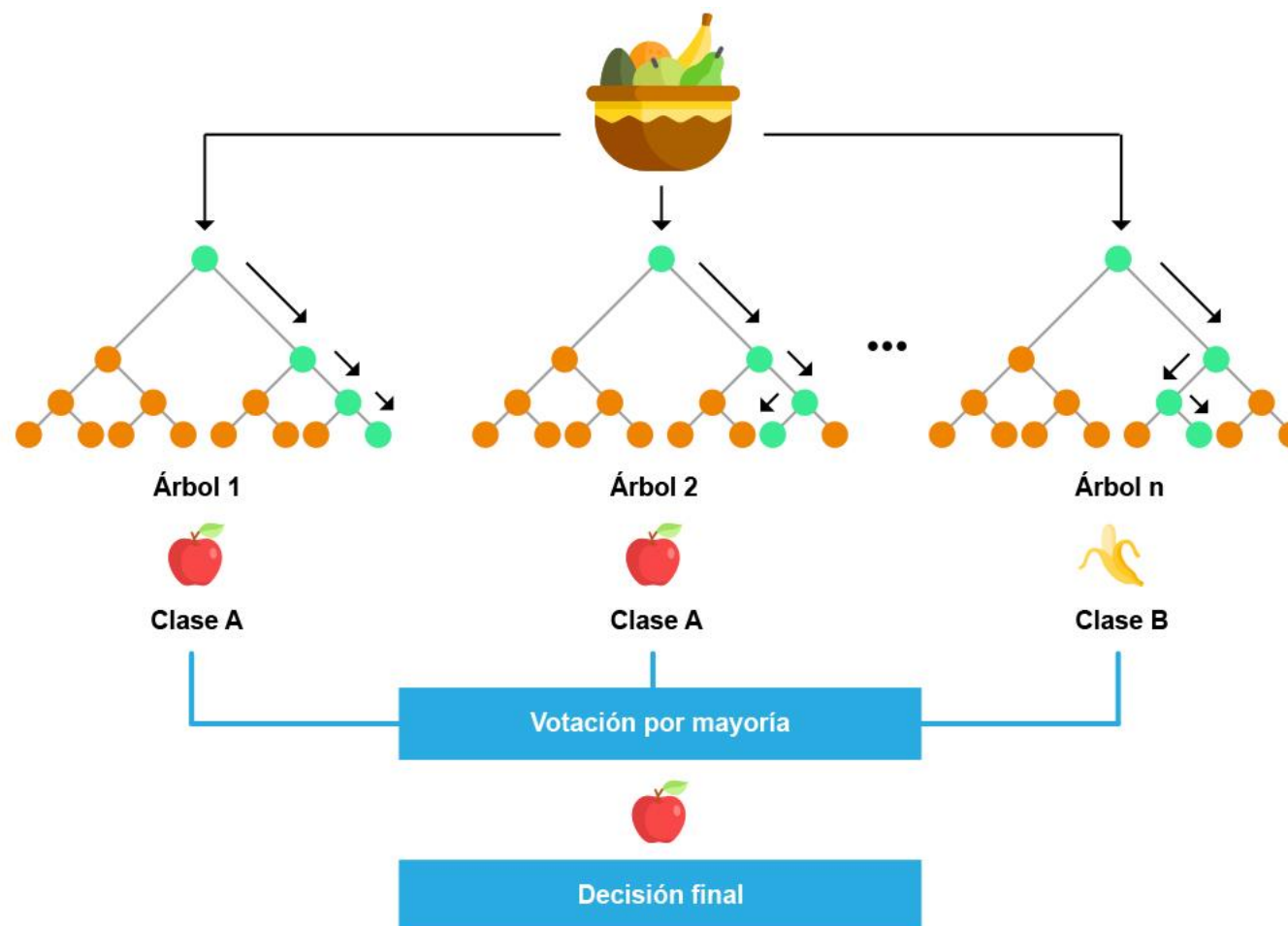
Funcionamiento de modelos supervisados



Fuentes: www.medium.com

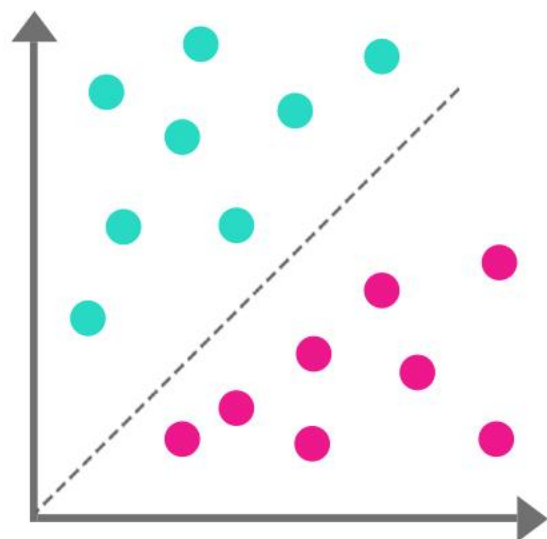
Machine Learning

Random Forest (RF)

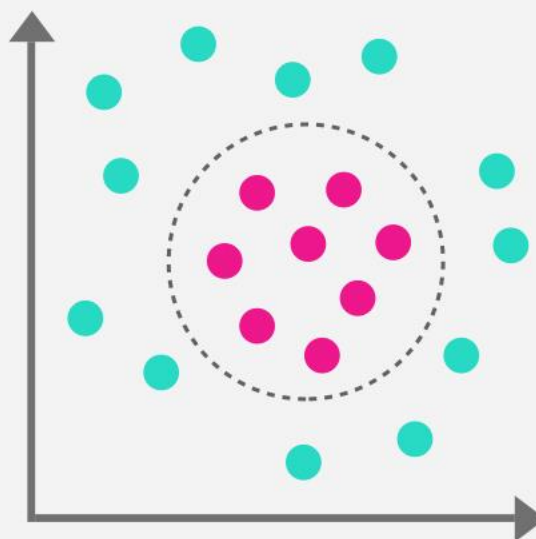


Machine Learning

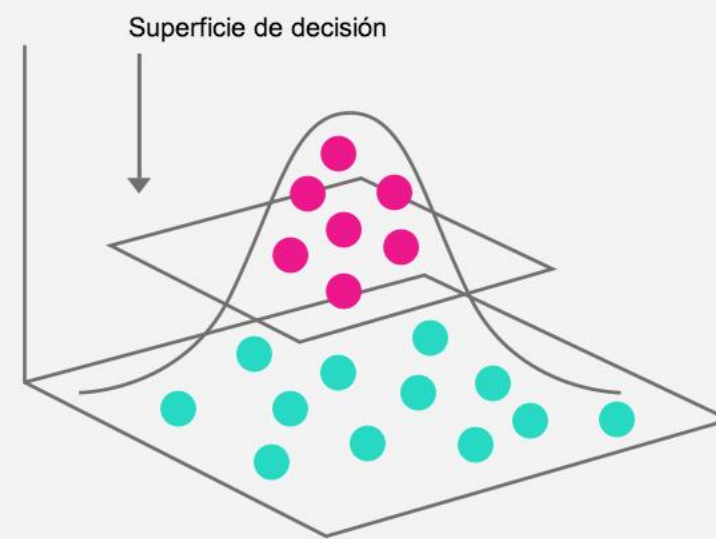
Support Vector Machine (SVM)



Separable linealmente



No Separable linealmente



Deep Learning

Modelos de redes neuronales

Supervisadas

Perceptrón simple

Adaline

Madaline

Perceptrón multicapa

Red de Hopfield

No supervisadas

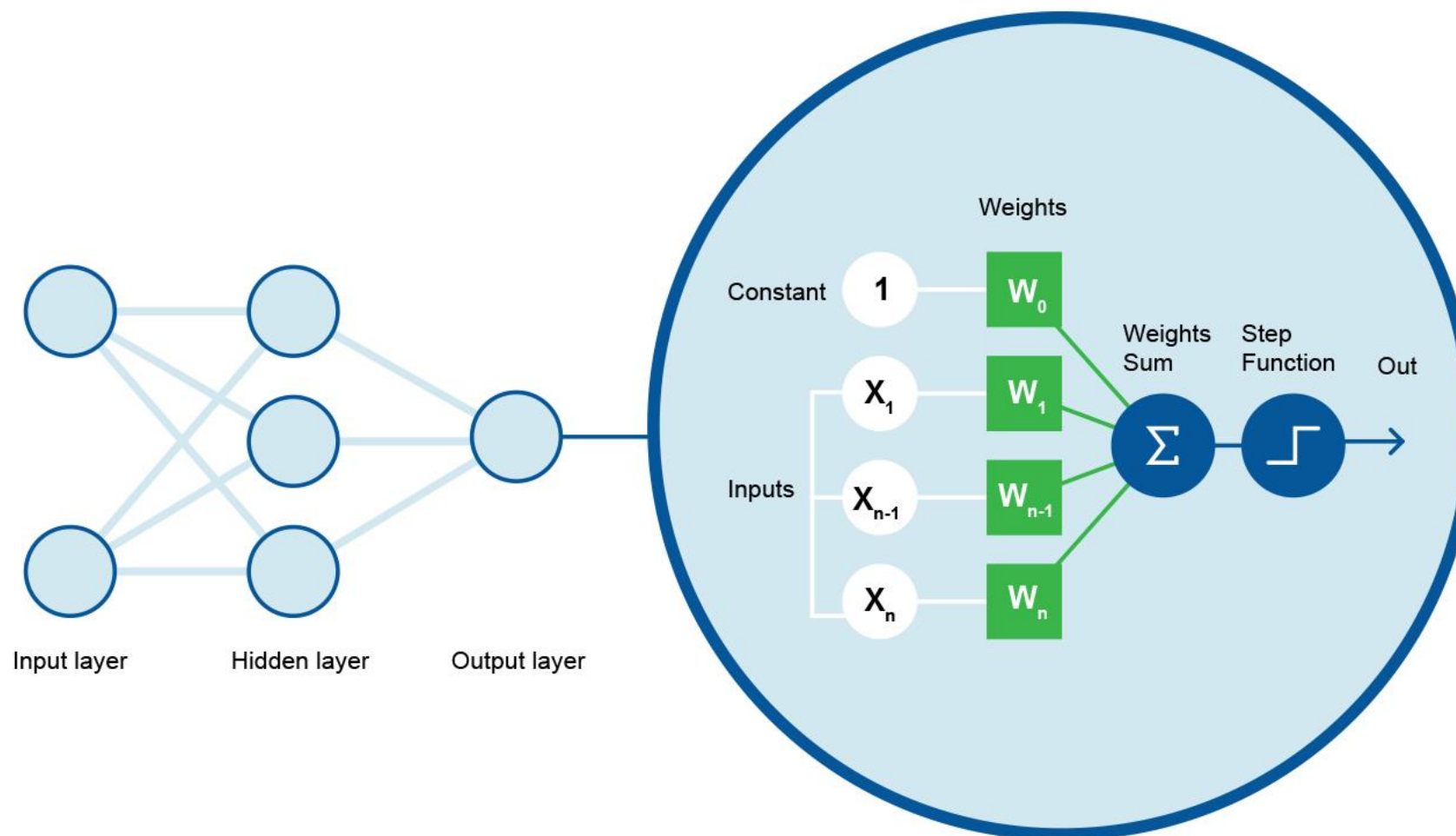
Competitiva simple

Online ART1

Convolucionales

Deep Learning

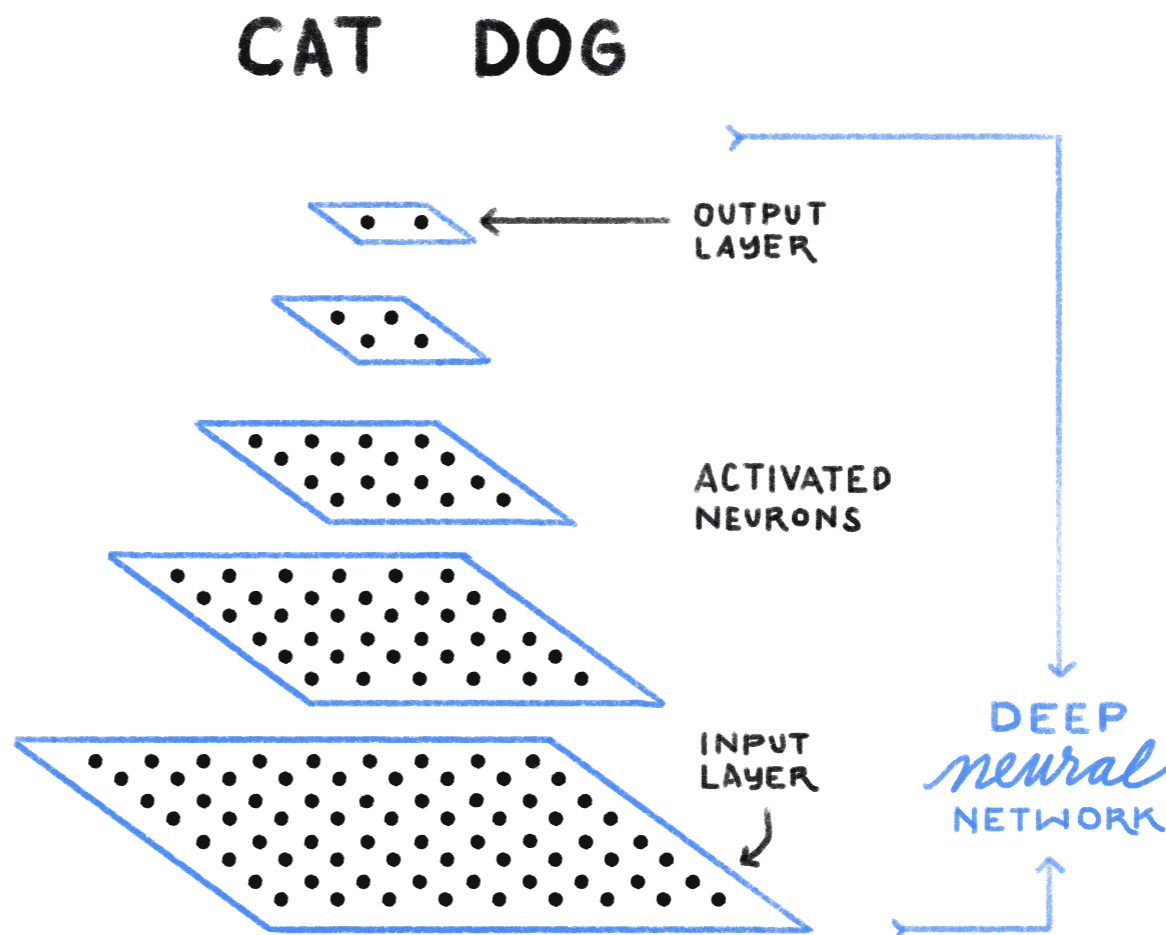
Perceptrón simple y multicapa



Deep Learning

Redes neuronales

IS THIS A
CAT or DOG?



Métricas



Accuracy

Tasa falsos negativos

Recall

F1 Score

Precision

ROC

Tasa negativa real

AUC

Tasa falsos positivos

Pérdida logarítmica

Comparativa

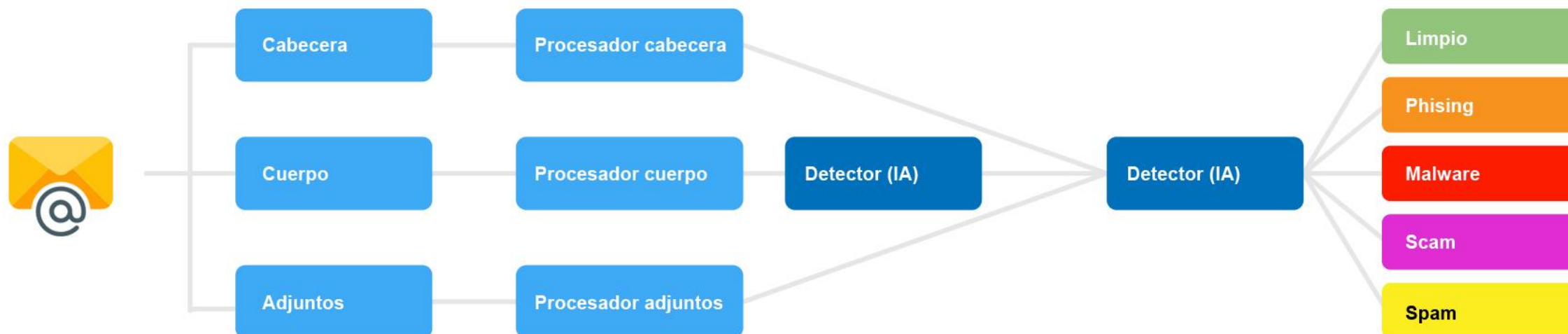
Machine Learning

-  Buenos resultados con datasets reducidos
-  Modelos rápidos de entrenar
-  Necesario probar distintas funcionalidades y clasificadores para conseguir buenos resultados
-  Precisión limitada

Deep Learning

-  Requiere datasets de gran tamaño
-  Elevado coste computacional
-  Aprende funcionalidades y clasifica automáticamente
-  Precisión ilimitada

Estructura para la predicción de correos



Extracción de datos del correo

Cabecera

Parámetros de seguridad de los servidores de correo: SPF, DKIM, DMARC

IPs y dominios de los servidores de correo

IP y dominio del servidor origen del correo

Remitente

Dirección de respuesta del correo

Cuerpo

URLs

Remitentes o correos (en caso de existir reenvíos)

Texto

Adjuntos

Ficheros

Extracción de datos del correo

Objetivo: Construcción de un vector

Comparación de dominios

Comparación de IPs

Reputación de dominios

Reputación de IPs

Reputación de ficheros

```
'seguridad': {
  'spf': 'neutral',
  'dkim': 'None',
  'dmarc': 'fail'
},
'servidores_correos': {
  'ip_servidores': ['77.227.105.140'],
  'dominios_servidores': ['prueba.com']
},
'remitente': 'probando.correo@infojobs.com.br',
'destinatario': ['adrianrg@ingenia.es'],
'en_copia': None,
'direccion_respuesta': ['prueba.com'],
'servidores_origen_ip': ['77.227.105.140'],
'servidores_origen': ['prueba.com']
}
{
  'clean_uris': set(),
  'suspicious_uris': {'http://34.66.188.11/33111456897kb.pdf'},
  'email': {'probando.correo@infojobs.com.br'},
  'sender': ['probando.correo@infojobs.com.br'],
  'receiver': [],
  'words': {'hola', 'se', 'adjunta', 'la', 'factura', 'del', 'mes', 'anterior', 'por',
    'correo', 'electrónico', 'como', 'otras', 'ocasiones', 'no', 'respuestas', 'a',
    'este', 'correo', 'saludos'}
}
{
  'filename': 'factura.pdf',
  'size': 82746,
  'extension': 'pdf',
  'hash': {
    'md5': 'b85f1732dc6c3268a62edb07c9e41320',
    'sha1': '8632f37b936c7b32a6aef0e12d4b301574cf3ee0',
    'sha256': '1389010208afe20cf60fa657d2b457282438db686876643c366bb5ed1235162d',
    'sha512': 'bd2ec015cb2079276364aea811add8b9ce9b52e3ea91322aefd9fca1e07d0808ab4eff6b0efa91eb562bfff270756053d2f45680a4bc54b2c94b23ade503ed547'
  },
  'raw': b'JVBERi0xLjQNCiWhs8XXDQoxIDAga2JqDQo8PC9Bbm5vdHNbIDQgMCBSIF0vQ29udGVudHMgMTUgMCBSIC9N2WRpYUJveFsgMCAwIDYxMiA3OTJdL1BhcmVudCA2IDAgUiAv...'
}
```

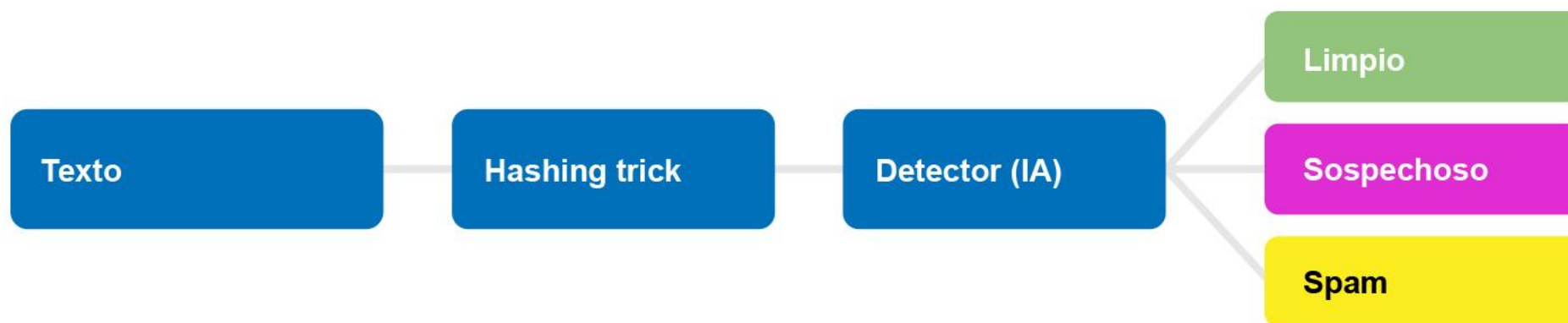
Resultado: Vector = [3, 0, 2, 1, 1, 2, 0, 1, 1, 1, 1, 1, 2, 2, 1, 10, 4, 0, 2, 2, 0, 1]

Predicción del texto del correo

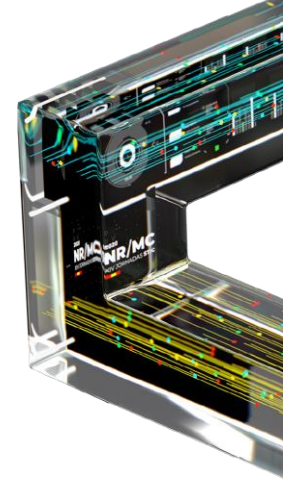
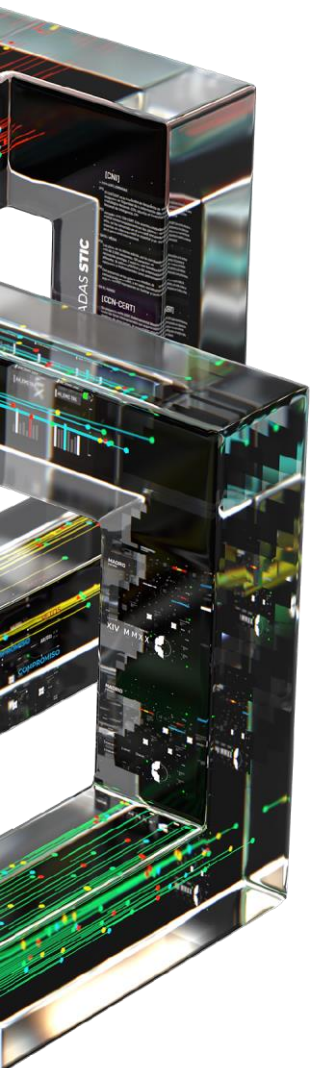
Hashing Trick

“Esto es un spam de manual” $\rightarrow$ [121 54 71 644 14 892] $\rightarrow$ [0, ..., 1, ..., 1, ..., 1]

- Para que funcione bien el vector debe ser de un tamaño grande
- El tamaño debe tener como valor una potencia de 2 para que computacionalmente su rendimiento sea óptimo
- En este caso 2^{19} (524.288) para que quepan todas las palabras en diferentes idiomas



Demo



MUCHAS GRACIAS

#XIVJORNADASCCNCERT