



Machine Learning Operations (MLOps) Clase 5

Leticia Rodríguez

Septiembre 2024 - 2do Cuatrimestre - 4to. Bimestre

Universidad de Buenos Aires - FCEyN - Departamento de Computación

Asistencia

Kahoot de respaso

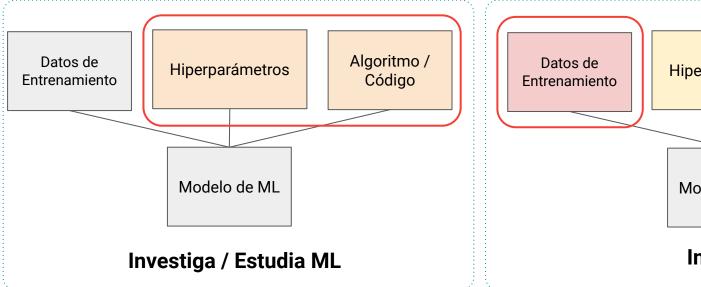
Aprendiendo de la Experiencia - Post mortem

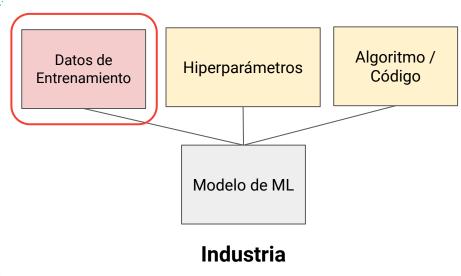
How ML Breaks:

A Decade of Outages for One Large

ML Pipeline

Armando modelos para problemas de usuarios





Modelos pre-entrenados: ejemplo MTCNN

Joint Face Detection and Alignment using Multi-task Cascaded Convolutional Networks

Kaipeng Zhang, Zhanpeng Zhang, Zhifeng Li, Senior Member, IEEE, and Yu Oiao, Senior Member, IEEE

Abstract-Face detection and alignment in unconstrained environment are challenging due to various poses, illuminations and occlusions. Recent studies show that deep learning approaches can achieve impressive performance on these two tasks. In this paper, we propose a deep cascaded multi-task framework which exploits the inherent correlation between them to boost up their performance. In particular, our framework adopts a cascaded structure with three stages of carefully designed deep convolutional networks that predict face and landmark location in a coarse-to-fine manner. In addition, in the learning process, we propose a new online hard sample mining strategy that can improve the performance automatically without manual sample selection. Our method achieves superior accuracy over the state-of-the-art techniques on the challenging FDDB and WIDER FACE benchmark for face detection, and AFLW benchmark for face alignment, while keeps real time performance.

Index Terms—Face detection, face alignment, cascaded convolutional neural network

I. INTRODUCTION

PACE detection and alignment are essential to many face applications, such as face recognition and facial expression analysis. However, the large visual variations of faces, such as occlusions, large pose variations and extreme lightings, impose great challenges for these tasks in real world applications.

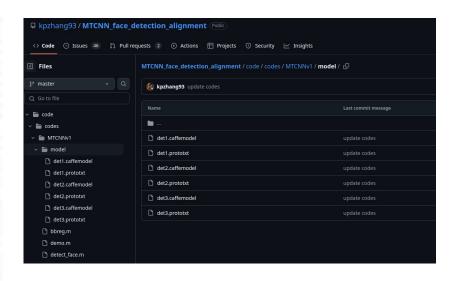
The cascade face detector proposed by Viola and Jones [2] utilizes Haar-Like features and AdaBoost to train cascaded

formance of CNNs in computer vision tasks, some of the CNNs based face detection approaches have been proposed in recent years. Yang et al. [11] train deep convolution neural networks for facial attribute recognition to obtain high response in face regions which further yield candidate windows of faces. However, due to its complex CNN structure, this approach is time costly in practice. Li et al. [19] use cascaded CNNs for face detection, but it requires bounding box calibration from face detection with extra computational expense and ignores the inherent correlation between facial landmarks localization and bounding box regression.

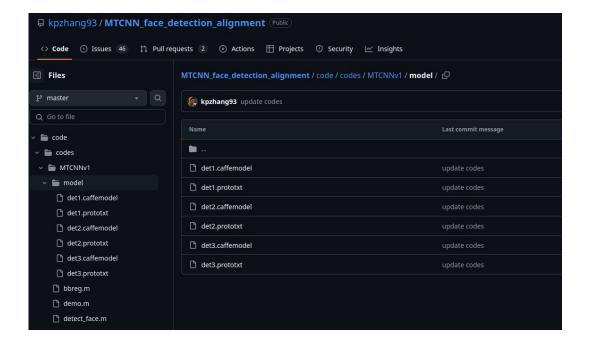
Face alignment also attracts extensive interests. Regression-based methods [12, 13, 16] and template fitting approaches [14, 15, 7] are two popular categories. Recently, Zhang et al. [22] proposed to use facial attribute recognition as an auxiliary task to enhance face alignment performance using deep convolutional neural network.

However, most of the available face detection and face alignment methods ignore the inherent correlation between these two tasks. Though there exist several works attempt to jointly solve them, there are still limitations in these works. For example, Chen et al. [18] jointly conduct alignment and detection with random forest using features of pixel value difference. But, the handcraft features used limits its performance. Zhang et al. [20] use multi-task CNN to improve the accuracy of multi-view face detection, but the detection accuracy is limited by the initial detection windows produced by a weak face detector.





Modelos pre-entrenados: MTCNN



Installation

MTCNN can be installed via pip:

```
pip install mtcnn
```

MTCNN requires Tensorflow >= 2.12. This external dependalong with MTCNN via:

```
pip install mtcnn[tensorflow]
```

Usage Example

```
from mtcnn import MTCNN
from mtcnn.utils.images import load_image

# Create a detector instance
detector = MTCNN(device="CPU:0")

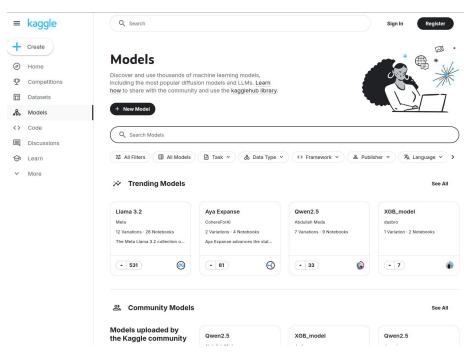
# Load an image
image = load_image("ivan.jpg")

# Detect faces in the image
result = detector.detect_faces(image)

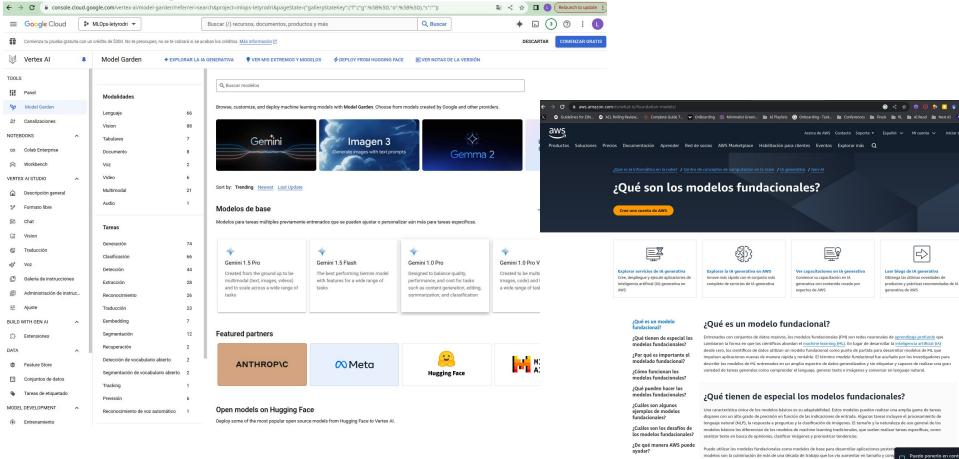
# Display the result
print(result)
```

Modelos pre-entrenados: API

- Se ofrecen distintos modelos pre-entrenados que son el estado del arte de diversas compañías. Podemos nombrar, entre otras:
 - Resnet
 - ∨GGNet
 - Inception
 - BERT
 - ChatGPT
 - Gemini
 - ROBERTa
 - o Gemma
 - Llama
 - Mistral
 - Stabble Diffusion
- Los entrenamientos de modelos llevan tiempo de procesamiento, datos y trabajo. Usar un modelo pre-entrenado evita dicha inversión y muchos estás disponible de manera gratuita.
- Incluso algunos como los modelos de lenguaje sería muy caro entrenarlos desde 0 obteniendo resultados similares.
 https://www.kaggle.com/models

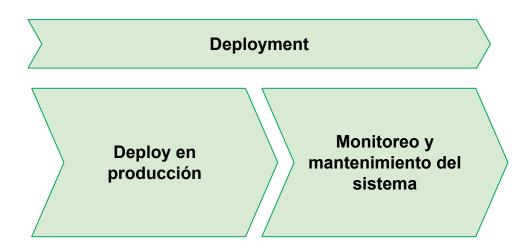


Modelos pre-entrenados: en la Nube

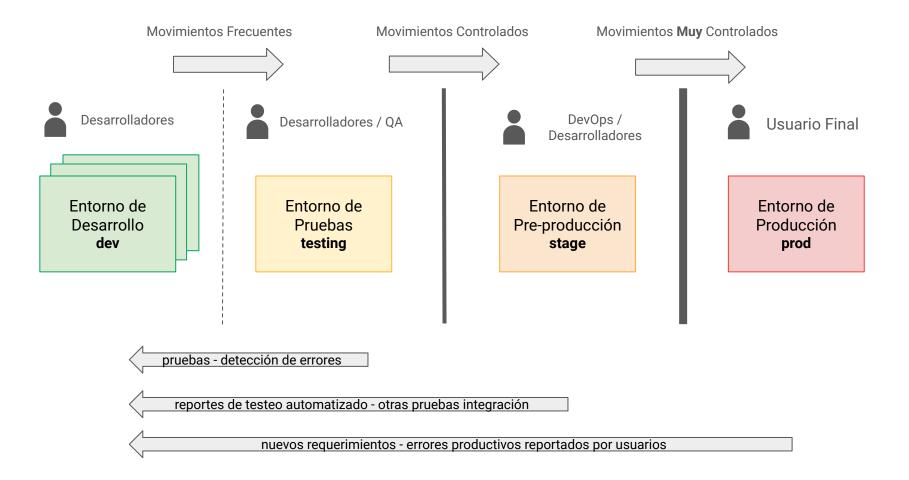


Por ejemplo, BERT, uno de los primeros modelos fundacionales bidireccionales, se lanzó en 2018. Se e parámetros y un conjunto de datos de entrenamiento de 16 GB. En 2023, solo cinco años después, OpenAl entrenó el GPT-4

Deploy



Los estándares: Ambientes del desarrollo de Software



Métricas de Negocio

- Métricas de ML son necesarias: f1-score, recall, accuracy, precision, otras.
- También, es importante demostrar el impactó que pueden generar en el negocio y esto se hace atraves de distintas métricas de negocio.
- Las Métricas de Negocio están relacionadas al problema a resolver y pueden ser más técnicas o mas orientada a los negocios. Muchas incluso llegan a los altos niveles ejecutivos. Algunos ejemplos de páginas web o marketing:
 - Impressions impresiones
 - CTR -- Click Through Rate clicks rate: Por ejemplo, en artículos recomendados por una Al, cuantos reciben click
 - Conversion Rate ratio de conversión: Por ejemplo, en artículos recomendados por una Al, cuantos se transforman en venta
 - ROI Retorno de la inversión

Actividad: Métricas de ML vs Métricas de Negocio

Del paper: 150 Successful Machine Learning Models: 6 Lessons Learned at

Booking.com

 Primero vemos como realizan la evaluación de los modelos en la sección 7. Evaluation.

Luego, en grupos, la sección
 Sección: 3. Modeling: Offline
 Model Perfomance is just a Heath
 Check y respondan.

¿Qué conclusión sacaron los investigadores respecto a las perfomance del modelo en relación al negocio?

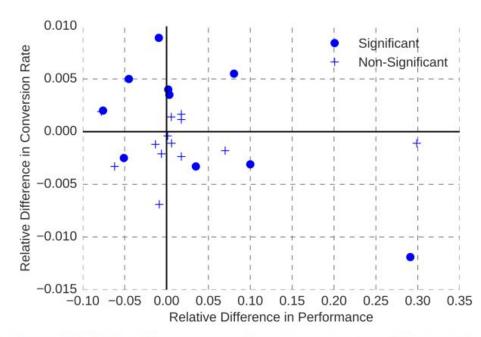
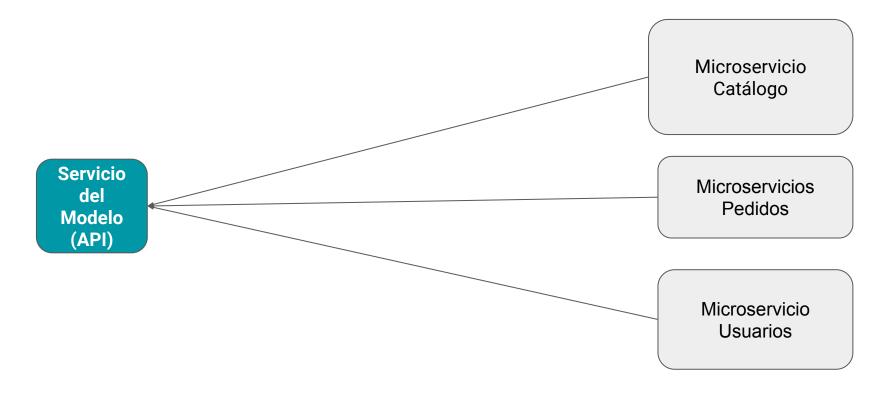


Figure 4: Relative difference in a business metric vs relative performance difference between a baseline model and a new one.

Ejemplo de Integración en el software



Ejemplo de Integración en el software





Vendo Auto 90.000 KMs

Vendedor: Cosme Fulanito

Precio: \$ 1.000.000

Comprar

Otros productos que pueden interesarte





Recomendaciones generadas con Al consultadas en la API para el usuario

Deploy - Subir a producción

Deploy: la tarea de subir / poner nuestro código en uso para los usuarios o consumidores del sistema.

Deployar un sistema es una tarea riesgosa, y desployar un sistema de ML en producción lo es aún más.

En ML, varias cosas pueden ir mal:

- Fallas, bugs, errores, páginas o APIs que no responden o accesos restrigidos
- Servidores sobrecargados de pedidos, respuesta lenta (baja latencia)
- Errores funcionales, no hace lo que se espera que haga
- Errores probabilisticos, para algunos usuarios, las respuestas no son satisfactorias

En la práctica, casi ningún sistema es disponibilizado para la totalidad de sus consumidores o los deploys se hacen de manera controlada. Casualmente, estas maneras controladas de hacer deploys pueden servir para testear en forma online el sistema de Al



Probar los sistemas de ML

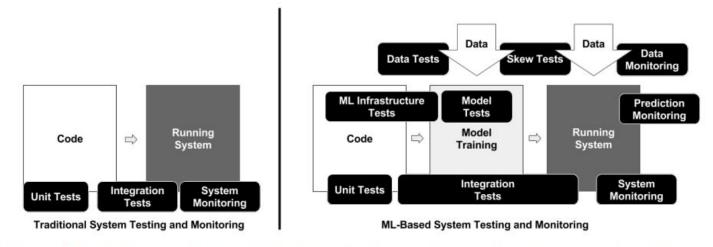
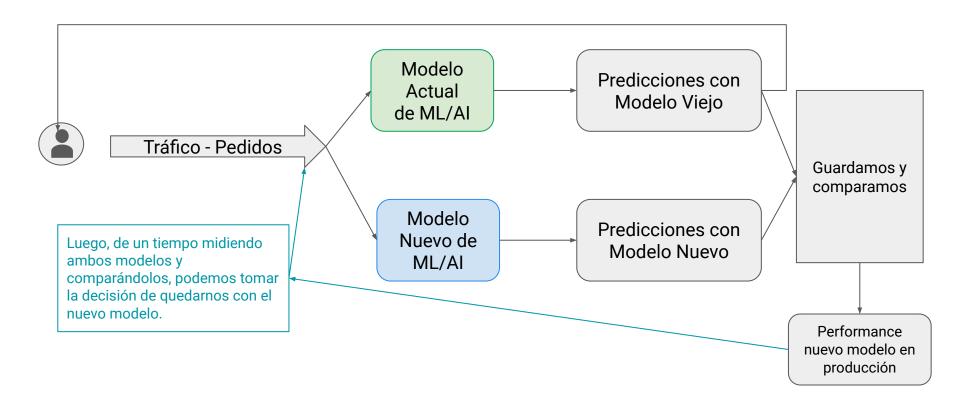


Figure 1. ML Systems Require Extensive Testing and Monitoring. The key consideration is that unlike a manually coded system (left), ML-based system behavior is not easily specified in advance. This behavior depends on dynamic qualities of the data, and on various model configuration choices.

Los modelos requieren una combinación de testeo al momento de la creación / desarrollo / implementación del sistema de ML (offline evaluation) y evaluaciones / monitoreos al momento de estar en producción (online evaluation)

The ML Test Score: A Rubric for ML Production Readiness and Technical Debt Reduction, Eric Breck et al.

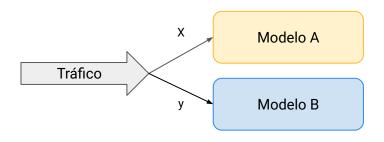
Shadow Deployment para el modelo



Lo mismo aplicaría para el sistema si estamos cambiando el sistema de Al entero

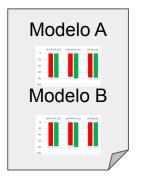
A/B Testing

A/B Testing es una forma de comparar dos variantes de un objeto, generalmente es una porción de software, un email, de alguna forma que nos permita decidir cuál es más effectiva.



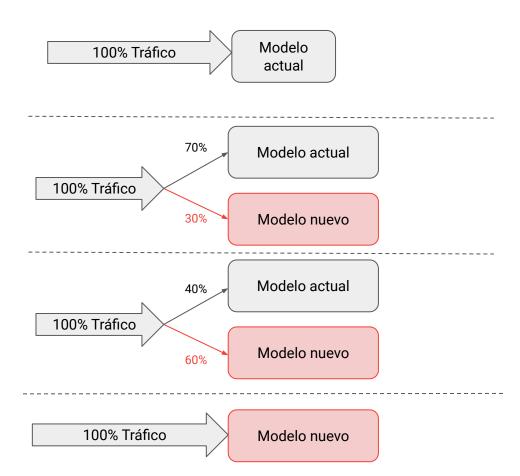
Probamos ambos modelos a ver cuál funciona mejor mandando la misma cantidad de tráfico de manera aleatoria a cada uno y viendo las métricas

x, y son porciones aletorias del tráfico disjuntas



Analizamos las predicciones de ambos modelos y el feedback del usuario, decidimos cuál vamos a usar.

Canary Deploy



Gradualmente se transfiere el tráfico al nuevo modelo.

Se va redirigiendo el tráfico de a poco y realizando verificaciones al nuevo modelo. Por ejemplo, la primera semana, se manda el 30% del trafico al nuevo modelo. Una vez que se observa que todo funciona como se espera, a semana siguiente, o más tarde, se manda el 60%. En incrementos secuenciales y validando el funcionamiento en cada paso.

Si los resultados no son los esperados, se veulve al modelo actual.

El tamaño de los incrementos y el momento depende de las características del problema y la decisión que toma el equipo de ingenieros.

Interleaving Experiments





Vendo Auto 90.000 KMs

Vendedor: Cosme Fulanito

Precio: \$ 1.000.000

Comprar

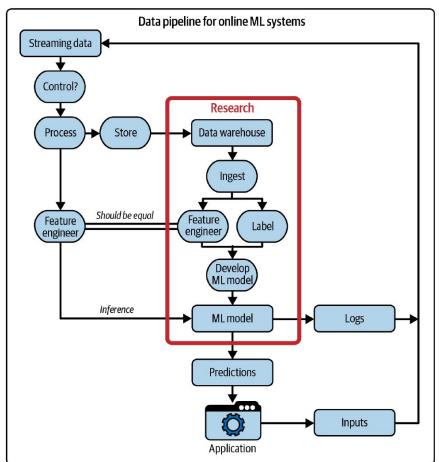
Otros productos que pueden interesarte



Modelo A

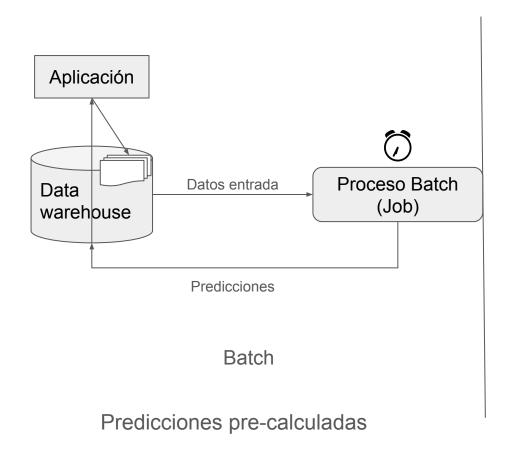
Generado por Modelo B En este experimento, se toman recomendaciones de distintos modelos y se observa cuál tiene más aceptación del usuario

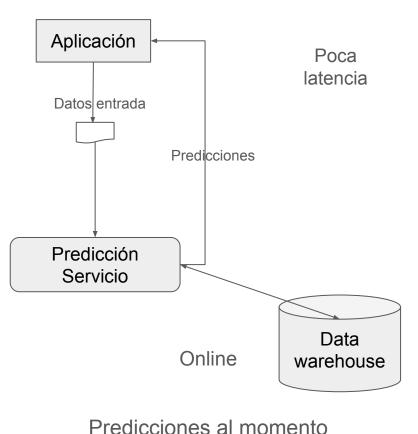
Ejemplo de Arquitectura



Chip Huyen, Designing Machine Learning System, 2022

Predicción Batch vs. Online



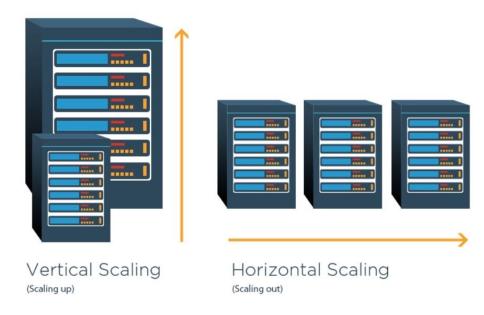


Escalabilidad

La infraestructura tiene que ser capaz de agregar más equipos (upscaling) o remover equipos en desuso (downscaling). Esto require el monitoreo del equipo y en caso de ser posible, configuraciones de escalamiento automático a partir de métricas. Por ejemplo, cantidad de requests por segundo (solicitudes web http).

Por otro lado, el escalamiento se puede hacer de dos maneras: vertical u horizontal.

- Escalamiento Horizontal: agregar más equipos de las mismas características para contener el incremento de tráfico o recursos requeridos.
- Escalamiento Vertical: aumentar las capacidades de los equipos actuales por ejemplo, agregando más memoria o mejorando los procesadores.



Monitoreo

Monitoreo es el acto de traquear, medir y loguear las diferentes métricas que nos pueden ayudar a ver las cosas que pueden salir mal. Generalmente, esa información puede ser usada para investigar que falló o encontrar algún error, a esto se lo denomina observabilidad.

La información de logueo y performance lo de los diferentes niveles son ampliamente usadas en la construcción de software.

Suceden a distintos niveles:

- Equipamiento CPU GPU Memoria Discos
- Red Paquetes enviados
- Servidor Web requests / solicitudes
- Aplicación Logueo de determinados eventos, funciones

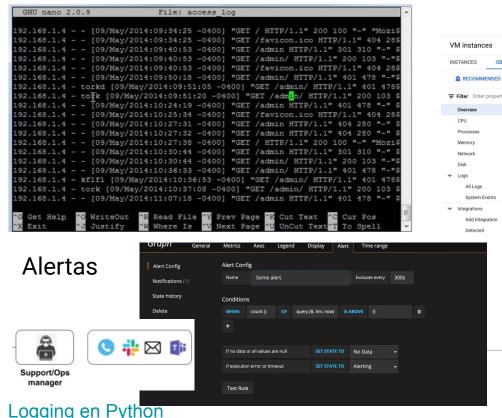
Tenemos que considerar también motorear métricas de ML

Monitoreo en Machine Learning

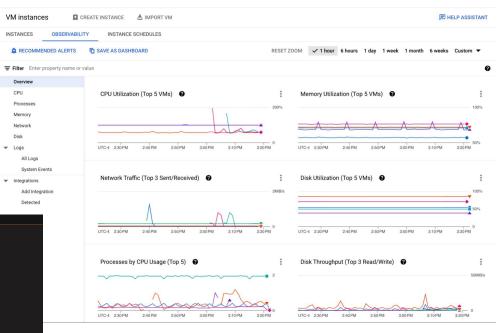
- Entradas de datos en crudo
- Features: validación de schema (test unitarios para datos o table validation o table testing)
 - min, max en rango aceptable
 - valores que satisfagan alguna expresión regular
 - valores pertenezcan a un conjunto determinado
- Predicciones: distrucción, predicciones individuales
- Métricas específicas: Accuracy, F1-score, Precision, Recall
- Cambios en la distribución de los datos entre entranamiento y los usados en producción para predicción
- Recolecciones de feedback

Monitoreo - Herramientas

Logs



Dashboards



Degradación de los modelos - Concept drift / Data drift

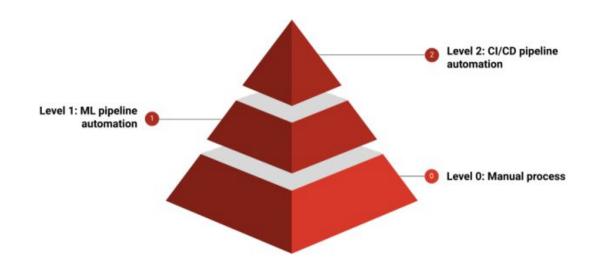
Existen razones para cambiar los modelos o reentrenarlos por el paso del tiempo:

- Los modelos se degradan naturalemente debido a que los datos productivos pueden cambiar en distrubución (Data Drift)
- También, los sistemas productivos pueden tener con el correr de los años cambios en los features, ya sea que se agreguen o se eliminen, en incluso que tomen nuevos valores que representen algo nuevo. (Concept Drift)
- La tecnología de Al avanza, surgen nuevos modelos, nuevas optimizaciones, nuevos casos de uso
- Se puede también mejorar el modelo mediante ensemble de modelos
- La llegada de nuevos datos o más información lleva a que sea requerido reentrenar el modelo frecuentemente (ej. en recomendadores)

Niveles de Maduración de MLOps

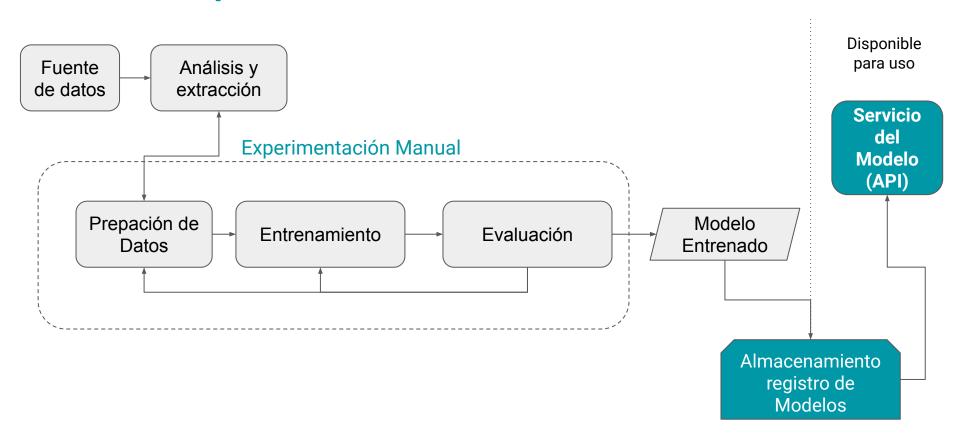
Acorde al grado de automatización / maduración de los distintos pipelines se definen niveles de manduración:

- → Nivel 0: Procesamiento Manual
- → Nivel 1: ML Pipeline automatizado
- → Nivel 2: CI/CD pipeline automatizado



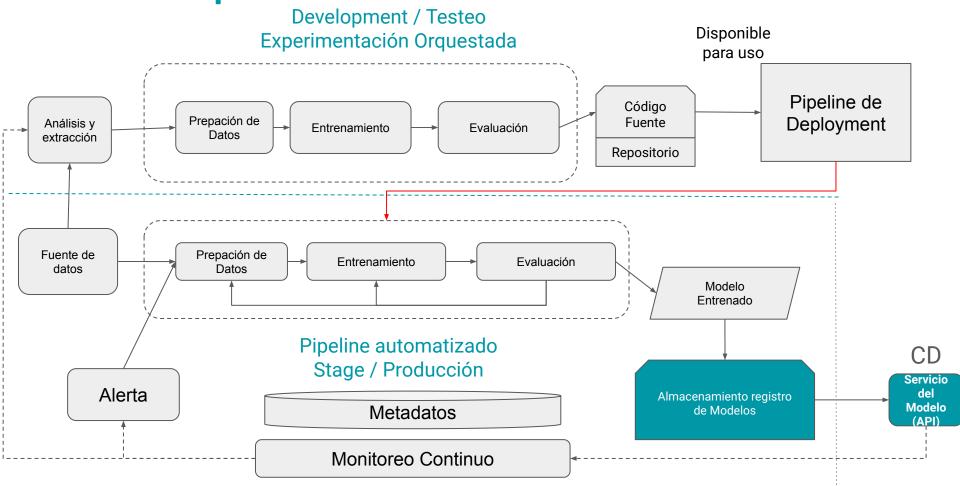
- Los provedores de cloud pueden definir otros niveles: <u>Symeonidis at el. MLOps Definitions, Tools and Challenges, 2022</u>
- Hay trabajos que buscan definirlos: <u>John at.el., Towards MLOps: A Framework and Maturity Model, 2021</u>

Nivel 0 MLOps



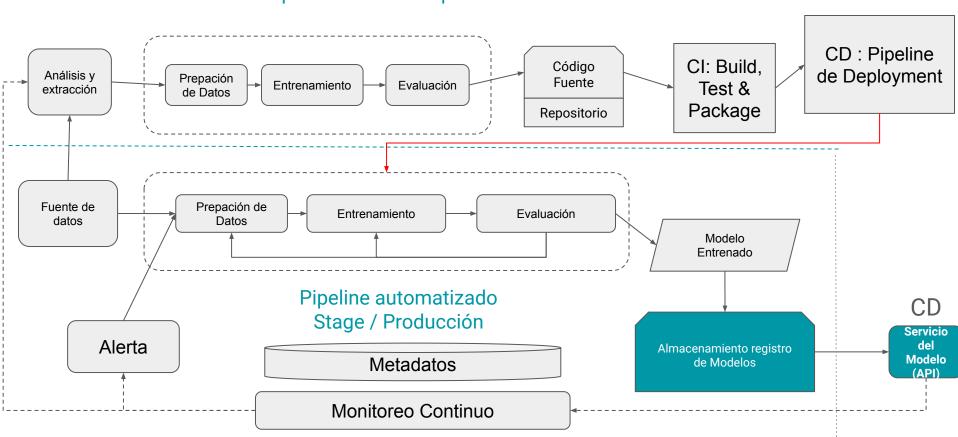
Nivel 1 MLOps

Entrenamiento automatizado y delivery continuo



Nivel 2 MLOps

Development / Testeo Experimentación Orquestada

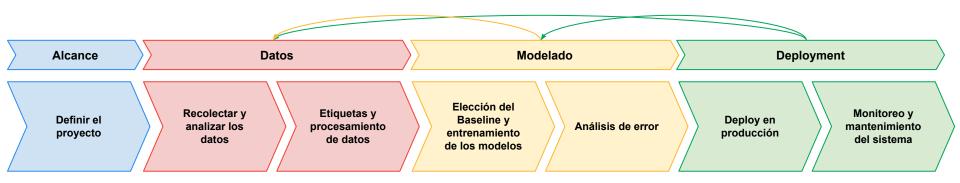


Principios de un buen Sistema de ML por Chip Huyen

- 1. Resuelve el problema
- 2. Está testeado
- 3. Es accesible a los usuarios
- 4. Es ético
- 5. Sus componentes son modulares, integrados pero separados
- 6. Es tan simple como es posible pero no más simple
- 7. Es transparente
- 8. Permite el desarrollo iterativo
- 9. Está versionado
- 10. Está documentado



El flujo de creación de un modelo de ML



Importante: las diferentes etapas tienen flechas que hace que se itere entre las etapas anteriores

Material Recomendado de esta semana

Stanford MLSys Seminar Episode 5: Chip Huyen

Rules for ML Engineers

BERT Paper

KPI in Marketing - Ejemplo metricas de negocio

The surprising Power of Online Experiments

<u>Vertex Al Pipelines - Ejemplos</u>

<u>Grafana</u>