Equipo 2

# Machine Learning Operations

# MLOps

*Catherine Rojas*
*Luis López*
*Rogelio Lizárraga*
*Adrian Pineda*
*Rodolfo Cruz*

# ¿Qué son las MLOps?

*Las MLOps son un conjunto de prácticas que automatizan y simplifican los flujos de trabajo de machine learning, uniendo el desarrollo y las operaciones para entregar valor a través de la IA.*

## AUTOMATIZACIÓN Y ESTANDARIZACIÓN DE PROCESOS DE ML

*Simplifican los flujos de trabajo y los despliegues de machine learning (ML).*

## DESARROLLO E IMPLEMENTACIÓN (DEV + OPS)

*MLOps es una cultura y una práctica de ML que une el desarrollo de aplicaciones de ML (Dev) a la implementación y las operaciones (Ops) de sistemas de ML.*

## IMPACTO EN LA ORGANIZACIÓN

*El machine learning y la inteligencia artificial son capacidades fundamentales que puede desplegar para resolver problemas complejos del mundo real y ofrecerle valor a sus clientes.*

## INFRAESTRUCTURA AUTOMATIZADA

*Automatiza y estandariza los procesos a lo largo del ciclo de vida del ML.*

thynk unlimited

# ¿Por qué se necesitan las MLOps?

***Automatización de modelos:***

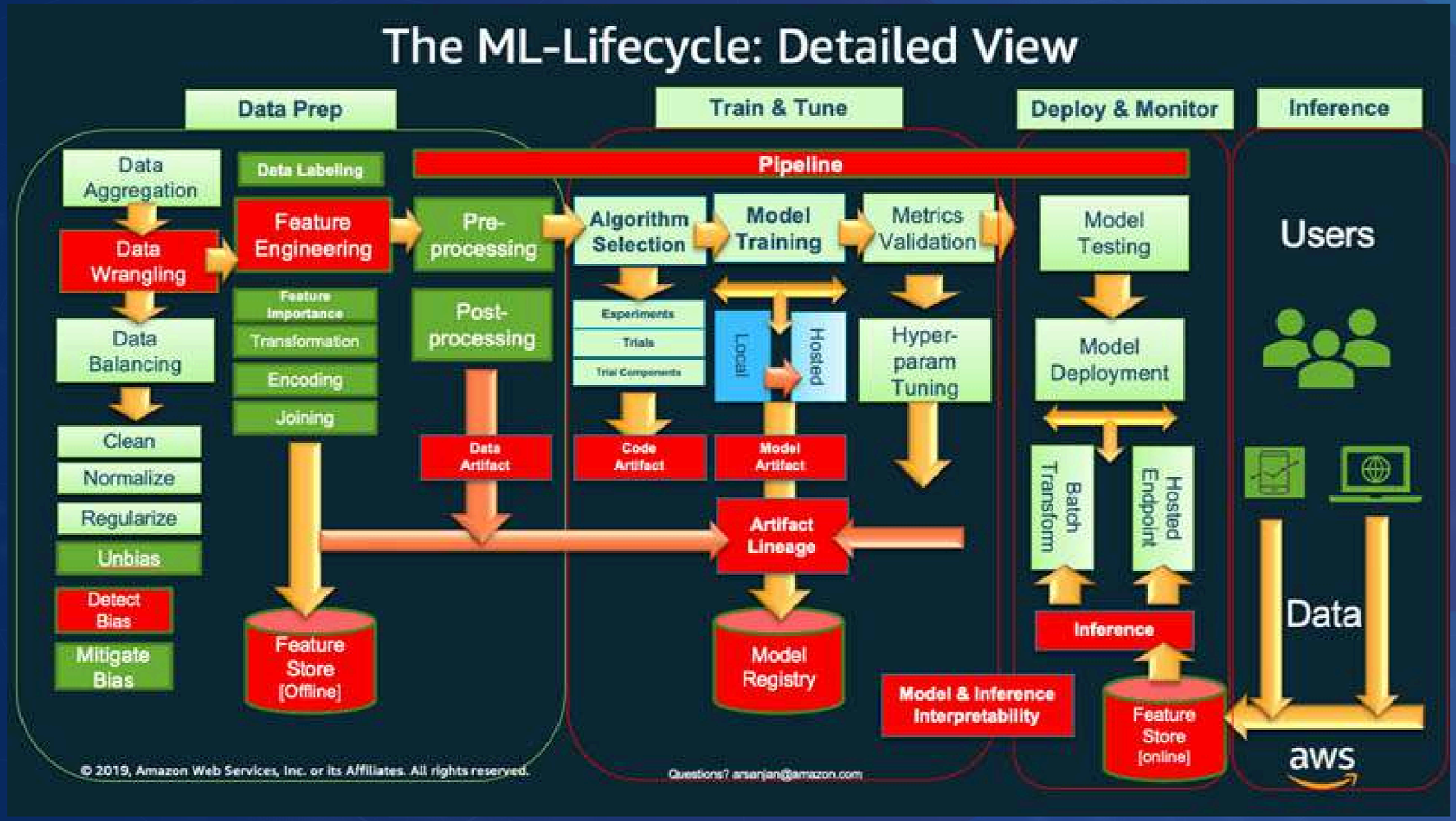
Garantiza que el entrenamiento, testing y despliegue de los modelos de ML se lleven a cabo automáticamente.

***Seguridad de los datos:***

Las MLOps se encargan de mantener la seguridad de los datos y cumplen con las normas legales en vigor, lo cual es esencial en las empresas.

***Preparación eficiente de datos:***

Las MLOps simplifican la gestión, limpieza y agrupación de datos, asegurando su calidad óptima para entrenar modelos.




*Visión detallada del ciclo de vida de un proyecto de Machine Learning (ML) desde la preparación de los datos hasta la implementación y monitoreo de modelos en producción.*

# Fases y procesos clave

## DATA PREPARATION

- *Agregación de datos, balanceo de datos, limpieza, normalización y mitigación de sesgos.*
- *Data Wrangling: El proceso de transformar y mapear datos.*
- *Feature Engineering: Selección y transformación de variables para mejorar el rendimiento del modelo.*

## TRAIN & TUNE (ENTRENAMIENTO Y AJUSTE)

- *Preprocesamiento y postprocesamiento de los datos.*
- *Selección de algoritmos.*
- *Entrenamiento del modelo.*
- *Validación de métricas y ajuste de hiperparámetros.*

## DEPLOY & MONITOR (IMPLEMENTACIÓN Y MONITOREO)

- *Pruebas del modelo.*
- *Despliegue del modelo: Hacer disponible el modelo para su uso en producción, ya sea a través de endpoints o transformaciones por lotes.*
- *Monitoreo continuo.*

## INFERENCE (INFERENCIA)

- *Inference: Aplicar el modelo para generar predicciones a partir de nuevos datos.*
- *Feature Store.*

## MODEL REGISTRY (REGISTRO DE MODELOS)

- *Registro de artefactos de modelos: Mantiene una trazabilidad y versión de los modelos entrenados para que puedan ser desplegados y monitoreados en producción.*

# Principios de las MLOps

## *Control de versiones*

*El control de versiones es esencial en cualquier sistema de machine learning, ya que facilita la capacidad de reproducir experimentos y entender cómo evolucionaron los modelos. Este principio se enfoca en rastrear los cambios a lo largo del tiempo en el código, los datos y los modelos entrenados.*

***Versionamiento de datos***

*Es crucial llevar un registro de las versiones de los datos que se utilizan para entrenar modelos, ya que los cambios en los conjuntos de datos pueden afectar significativamente el rendimiento de un modelo. El control de versiones de datos permite verificar que un conjunto de datos específico produce los resultados esperados.*

***Versionamiento de modelos***

*Los modelos de machine learning, una vez entrenados, pasan por diferentes etapas de evaluación y ajuste. Con un sistema de control de versiones para los modelos, los equipos pueden registrar exactamente qué configuración de hiperparámetros, qué conjunto de datos y qué versión de código se utilizó para entrenar un modelo específico.*

# Principios de las MLOps

## *Control de versiones*

*El control de versiones es esencial en cualquier sistema de machine learning, ya que facilita la capacidad de reproducir experimentos y entender cómo evolucionaron los modelos. Este principio se enfoca en rastrear los cambios a lo largo del tiempo en el código, los datos y los modelos entrenados.*

***Versionamiento de código***

*A medida que los modelos evolucionan, también lo hace el código que los entrena. Usar herramientas como Git para versionar el código permite que cualquier cambio en la lógica del entrenamiento pueda ser rastreado y revisado. Esto es importante para auditar modificaciones y asegurarse de que los cambios introducidos mejoran el rendimiento del modelo de manera controlada.*

***Reproducibilidad***

*Un principio clave es que cada fase del proceso de machine learning debe ser reproducible. Esto significa que, con los mismos datos de entrada y el mismo código de entrenamiento, los resultados obtenidos deben ser idénticos. La reproducibilidad es un requisito importante para validar modelos, realizar auditorías y asegurar la transparencia en el desarrollo de los modelos.*

# Principios de las MLOps

*Automatización*

*La automatización es esencial para hacer que el ciclo de vida del machine learning sea repetible, escalable y eficiente. Esto incluye la ingesta de datos, el preprocesamiento, el entrenamiento de modelos y el despliegue.*

***Automatización de ingesta de datos***

*Automatizar el proceso de obtener y actualizar datos asegura que los modelos siempre utilicen la información más reciente, sin intervención manual.*

***Automatización del preprocesamiento***

*Tareas repetitivas como la limpieza de datos y la transformación de variables deben automatizarse para asegurar consistencia y escalabilidad.*

***Automatización del entrenamiento y validación***

*Los modelos pueden ser entrenados y validados automáticamente al detectarse cambios en los datos o el código, reduciendo el tiempo que se necesita para desplegar modelos actualizados.*

# Principios de las MLOps

*Automatización*

*La automatización es esencial para hacer que el ciclo de vida del machine learning sea repetible, escalable y eficiente. Esto incluye la ingesta de datos, el preprocesamiento, el entrenamiento de modelos y el despliegue.*

***Automatización del despliegue***

*Implementar modelos en producción automáticamente garantiza que el mejor modelo esté disponible para hacer predicciones sin retrasos.*

***Desencadenadores de automatización***

*Factores como cambios en datos o código, eventos programados, o alertas, pueden activar automáticamente procesos de entrenamiento o implementación.*

***Pruebas automatizadas***

*La automatización también incluye pruebas constantes de datos, modelos e infraestructura para detectar problemas lo antes posible y corregirlos*

# Principios de las MLOps

*Actividades continuas*

*El concepto de "continuo" en MLOps se refiere a procesos que se ejecutan constantemente, asegurando que el pipeline de machine learning sea eficiente y adaptable a cambios.*

***Integración continua (CI)***
*Valida automáticamente los cambios en el código, los datos y los modelos. Cada cambio se somete a pruebas para verificar que no degrade el rendimiento del sistema.*

***Entrega continua (CD):***
*Implementa de forma automática los modelos nuevos en producción cuando cumplen con los estándares de calidad, asegurando que las predicciones siempre se basen en los mejores modelos.*

***Entrenamiento continuo***
*Los modelos se reentrenan automáticamente cuando se detectan nuevos datos o cambios significativos en el entorno de producción, manteniendo la precisión del modelo.*

***Monitoreo continuo***
*Se supervisa el rendimiento del modelo, lo que permite la detección temprana de problemas, como sesgos en los datos o el deterioro del modelo.*

# Principios de las MLOps

*Gobernanza de los modelos*

*La gobernanza asegura que los modelos se gestionen correctamente, cumplan con regulaciones y estándares éticos, y estén alineados con los objetivos empresariales.*

***Colaboración***

*La gobernanza fomenta la colaboración entre científicos de datos, ingenieros de ML y partes interesadas del negocio, asegurando que todas las áreas estén alineadas con los objetivos del modelo y que la comunicación sea fluida.*

***Documentación***

*La documentación clara y detallada es esencial para la transparencia y para que otros puedan entender cómo se desarrollaron y entrenaron los modelos, facilitando auditorías y revisiones.*

***Seguridad y conformidad***

*Es esencial proteger los datos sensibles y garantizar que los modelos cumplan con las regulaciones, como la privacidad de los datos o la seguridad. También se debe controlar quién tiene acceso a los modelos y la infraestructura.*

# Principios de las MLOps

*Gobernanza de los modelos*

*La gobernanza asegura que los modelos se gestionen correctamente, cumplan con regulaciones y estándares éticos, y estén alineados con los objetivos empresariales.*

***Validación y aprobación***

*Antes de que un modelo se despliegue en producción, debe pasar por un proceso estructurado de validación para garantizar que cumple con las normas éticas, es justo y no presenta sesgos. Esto también incluye evaluar las implicaciones éticas y legales de los modelos.*

***Retroalimentación***

*Implementar mecanismos de feedback es clave para evaluar el impacto de los modelos y mejorar continuamente su rendimiento. La retroalimentación ayuda a identificar áreas en las que los modelos pueden ser ajustados o reentrenados.*

# Beneficios de las MLOps

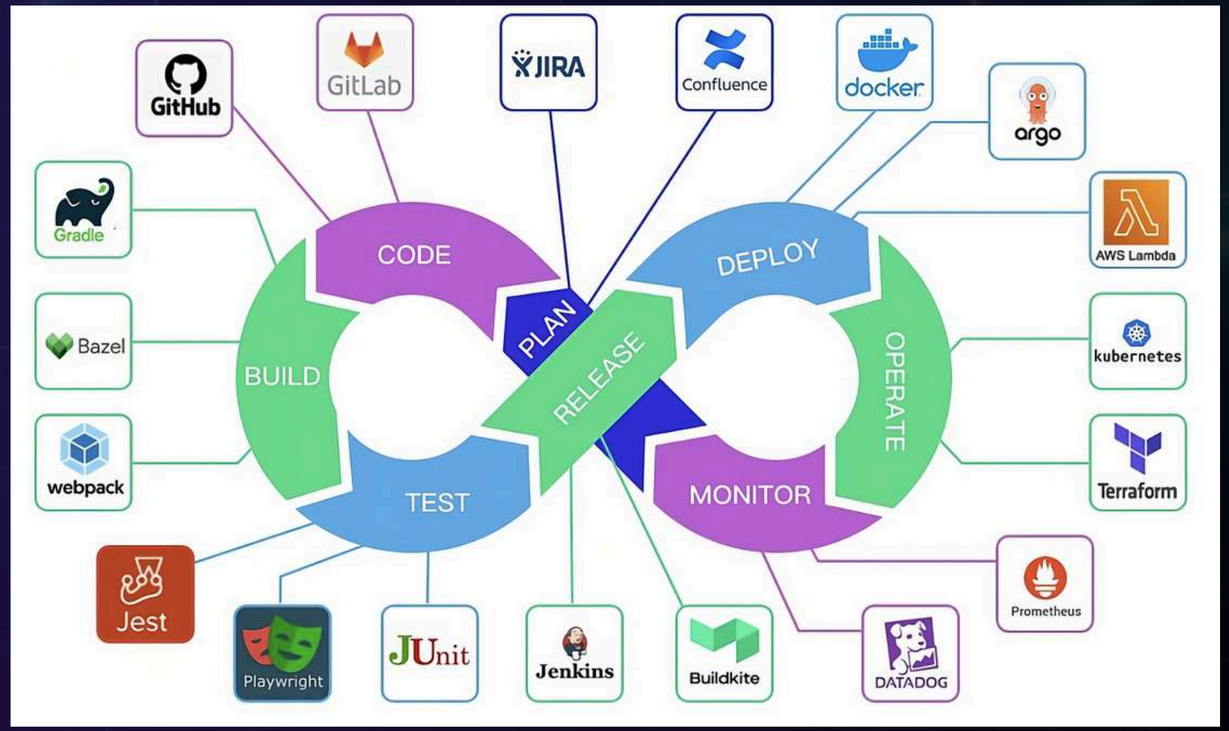
*Las MLOps brindan a las organizaciones una guía estructurada para lograr el éxito en proyectos de machine learning, superando limitaciones comunes como presupuestos, personal y tecnología.*

# Reducción del Plazo de Comercialización con MLOps

- ***Automatización del ciclo de vida del ML:*** *Las MLOps permiten automatizar tareas repetitivas en el desarrollo y despliegue de modelos.*

- ***Implementación más eficiente:*** *Los ingenieros pueden aprovisionar la infraestructura de forma más rápida y escalable, usando archivos declarativos.*

- ***Valor empresarial acelerado:*** *Al reducir tiempos, los equipos de datos pueden explotar más rápido la información para generar beneficios empresariales.*



# Productividad Mejorada con MLOps

06

- ***Estandarización de entornos:*** *Los equipos de ML pueden trabajar en entornos homogéneos, facilitando la alternancia entre proyectos y reutilización de modelos.*
- ***Aceleración del desarrollo:*** *Procesos repetibles y automatizados permiten que la experimentación y el entrenamiento de modelos sean más rápidos y eficientes.*
- ***Colaboración efectiva:*** *Equipos de ML y software pueden colaborar mejor en la integración y entrega de modelos, incrementando la productividad.*

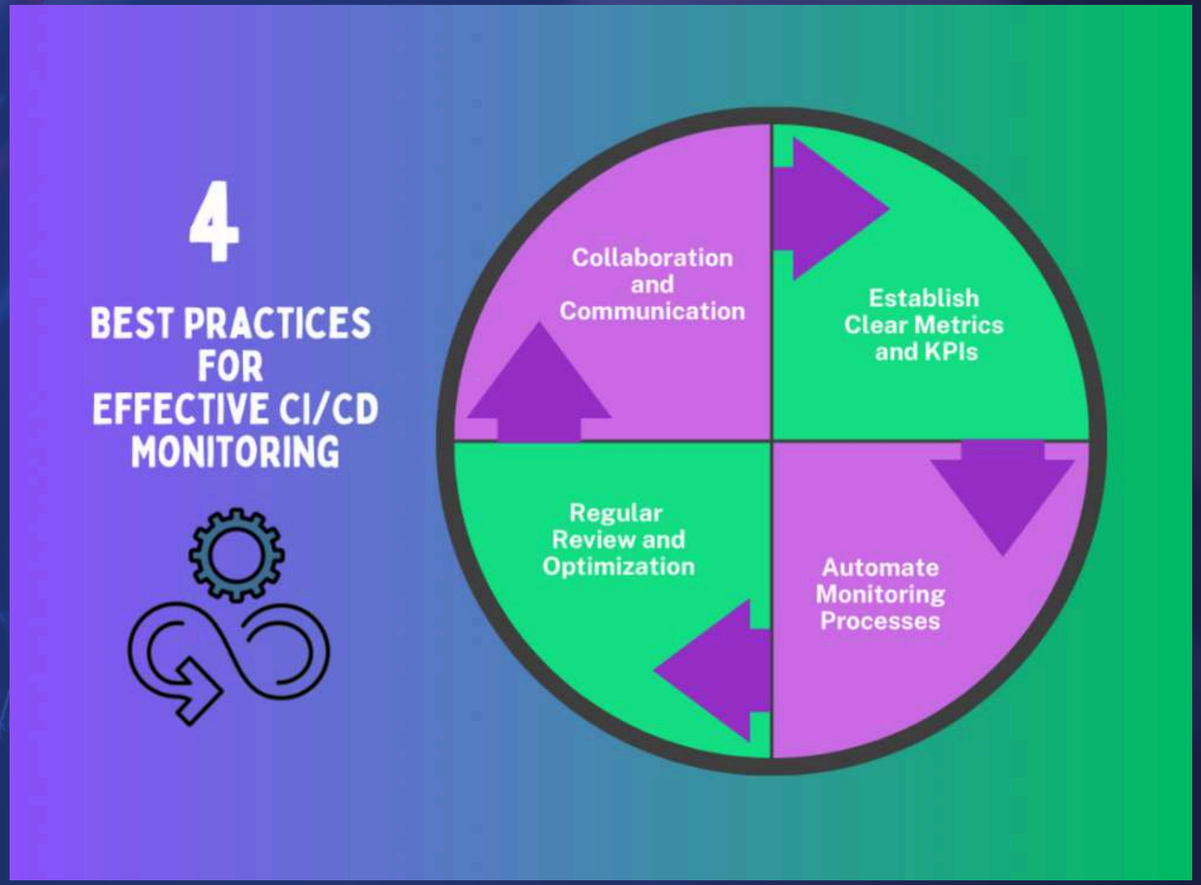
# Eficiencia en la Implementación de Modelos con MLOps



- ***Monitoreo y administración centralizada:*** *Facilita el seguimiento del desempeño de los modelos en producción, asegurando que se pueda identificar rápidamente cualquier problema.*

- ***Reproducción y ajuste continuo:*** *Los flujos de trabajo MLOps permiten realizar ajustes y actualizaciones continuas sin perder calidad en los modelos.*

- ***Prevención de la degradación del rendimiento:*** *Las canalizaciones CI/CD integradas con MLOps mantienen el rendimiento del modelo incluso después de actualizaciones o ajustes.*



# ¿Cómo se implementan las MLOps en la organización?

*MLOps, o Machine Learning Operations, es el enfoque que busca integrar el machine learning en procesos de producción automatizados. Los niveles de implementación de MLOps dependen de la madurez de la automatización dentro de la organización.*

- *Tres niveles de madurez*
- *Proceso de mejora de la automatización y eficiencia*
- *Impacto en la frecuencia de implementación y monitoreo de modelos*

# Nivel 0 de MLOps

*El Nivel 0 está destinado a organizaciones que están comenzando a trabajar con machine learning. Aquí, los flujos de trabajo son principalmente manuales y dependen mucho de la intervención de los científicos de datos.*

- *Procesos manuales: preparación de datos, entrenamiento y validación*
- *Transiciones manuales entre pasos*
- *Separación entre científicos de datos y equipo de ingeniería*
- *Lanzamientos poco frecuentes*
- *Sin integración CI/CD ni monitoreo del rendimiento*

# Características del Nivel 0

*En este nivel, los modelos se entrenan manualmente y los científicos de datos entregan el modelo como artefacto al equipo de ingeniería para su implementación.*

- ***Manual**: cada paso es gestionado de forma independiente*
- ***Desconexión** entre los científicos de datos que crean el modelo y los ingenieros que lo implementan*
- ***Falta de automatización** y monitoreo continuo*

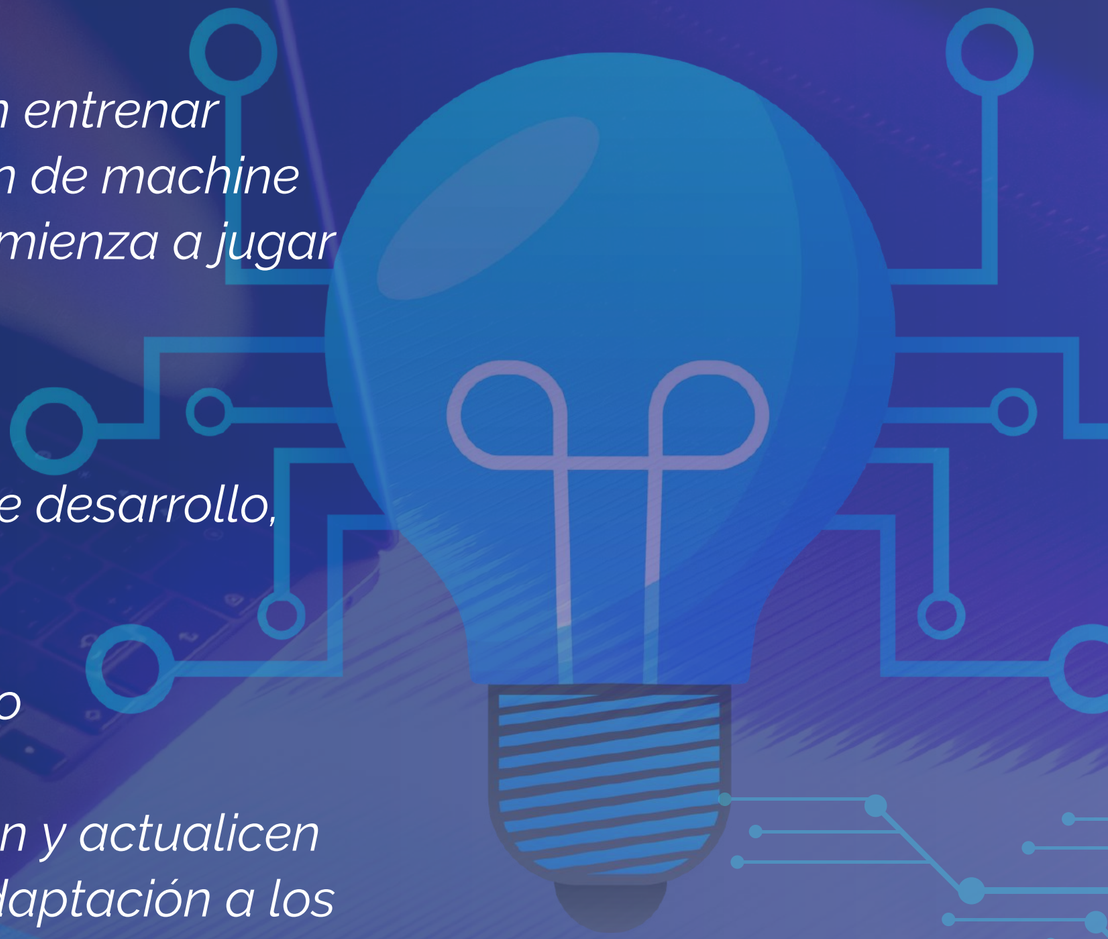
*Este enfoque resulta en una baja frecuencia de actualizaciones y dificultades para mantener el rendimiento de los modelos en producción.*

# Nivel 1 de MLOps

*El Nivel 1 está diseñado para organizaciones que necesitan entrenar modelos con mayor frecuencia, utilizando una canalización de machine learning automatizada. En este nivel, la automatización comienza a jugar un rol clave.*

- *Automatización del entrenamiento con datos nuevos*
- *Reutilización de componentes de código en entornos de desarrollo, preproducción y producción*
- *Entrega continua del servicio de predicción*
- *Creación de un almacén de características centralizado*

*Esta automatización permite que los modelos se reentrenen y actualicen de forma más frecuente, lo que mejora la capacidad de adaptación a los cambios en los datos.*



# Características del Nivel 1

*El nivel 1 de MLOps incluye una mayor integración entre científicos de datos e ingenieros, con procesos más automáticos y la reutilización de componentes en distintos entornos.*

- ***Entrenamiento continuo**: reentrenamiento recurrente con datos frescos*
- ***Colaboración mejorada**: ingenieros y científicos trabajan juntos en componentes reutilizables*
- ***Estandarización:** almacén de características para ML centralizado*
- ***Automatización en diferentes entornos**: desarrollo, preproducción y producción*

*Esto permite a las organizaciones escalar sus flujos de trabajo de machine learning de manera más eficiente.*

# Nivel 2 de MLOps

*En el Nivel 2, la organización ya cuenta con múltiples modelos de machine learning, que requieren entrenamiento continuo y una implementación rápida a gran escala. Este nivel es ideal para organizaciones tecnológicas que actualizan sus modelos en tiempo real o casi en tiempo real.*

- *Creación e implementación de canalizaciones de ML de forma repetida*
- *Uso de un orquestador de canalizaciones para gestionar múltiples flujos*
- *Registro de modelos para gestionar versiones y actualizaciones*
- *Automatización avanzada para manejar miles de servidores simultáneamente*

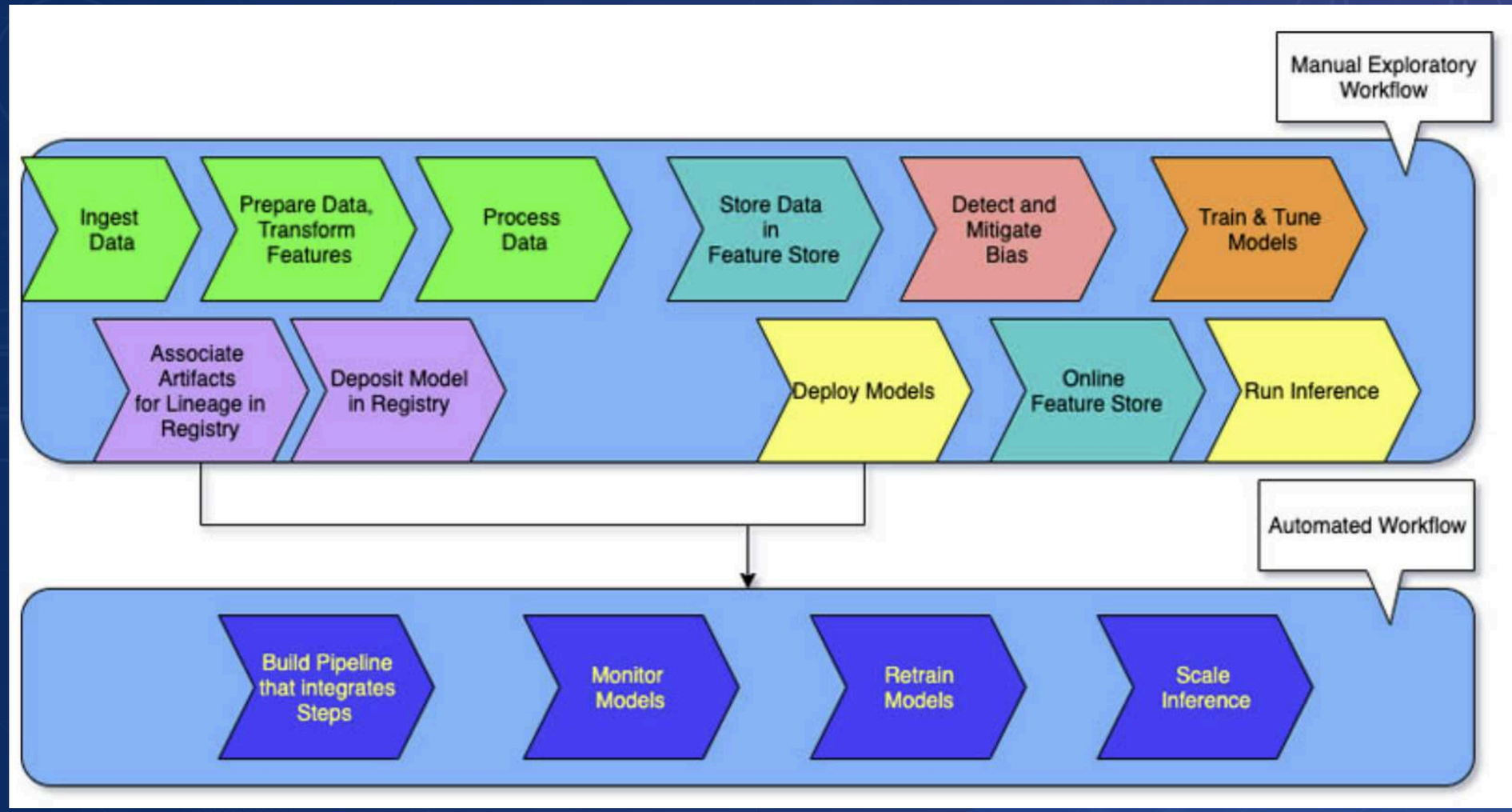
# Características del Nivel 2

*El Nivel 2 introduce herramientas avanzadas para manejar múltiples modelos y canalizaciones de machine learning, garantizando su entrenamiento, implementación y monitoreo en tiempo real.*

- ***Orquestación:*** *gestión de múltiples canalizaciones con un orquestador*
- ***Ciclo completo:*** *creación, implementación y empleo de las canalizaciones a gran escala*
- ***Monitoreo continuo:*** *estadísticas en tiempo real para el servicio de predicción*
- ***Automatización masiva:*** *ideal para empresas tecnológicas que manejan miles de servidores*

*Este enfoque permite a las organizaciones experimentar, entrenar e implementar nuevos modelos de manera rápida y eficaz.*

# Flujos de trabajo



# FLUJO DE TRABAJO EXPLORATORIO MANUAL

- I**ngesta de datos:** La fase inicial donde se recopilan datos de diversas fuentes.
- **Preparación de datos y transformación de características:** Limpieza, transformación y procesamiento de los datos para que sean utilizables en el entrenamiento del modelo.
- **Procesamiento de datos:** Los datos se procesan para obtener el formato adecuado antes de almacenarse.
- **Almacenamiento en el almacén de características**: Las características transformadas se almacenan en un almacén centralizado que las estandariza para su reutilización.
- **Detección y mitigación de sesgos:** Se evalúa el sesgo en los datos y se aplican técnicas para reducirlo.
- **Entrenamiento y ajuste de modelos:** Se entrena el modelo de machine learning y se ajusta con los hiperparámetros adecuados para maximizar su rendimiento.
- **Despliegue de modelos:** El modelo entrenado se implementa en el entorno de producción.
- **Inferencia:** Se utiliza el modelo para realizar predicciones en tiempo real.
- **Registro de artefactos:** Se asocian los artefactos del modelo y su linaje en un registro para un seguimiento continuo.
- **Depósito de modelo en el registro:** El modelo entrenado se deposita en un repositorio para su uso posterior.

# FLUJO DE TRABAJO AUTOMATIZADO

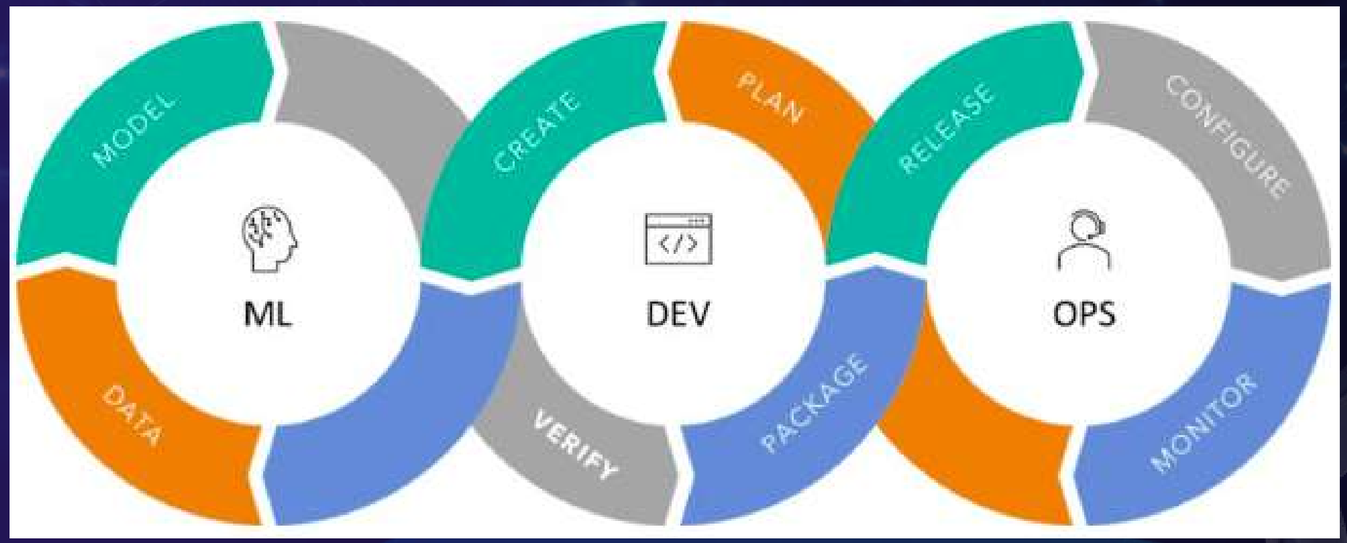
Este flujo toma el trabajo exploratorio realizado en el flujo manual y lo integra en un proceso automatizado para escalar y monitorizar la operación del modelo en producción:

- **Construcción de la canalización**: Se construye una canalización que integra todos los pasos del flujo manual, pero de manera automática.
- **Monitoreo de modelos**: Se supervisa el rendimiento del modelo en producción para detectar problemas como el desajuste de datos.
- **Reentrenamiento de modelos**: Se reentrenan los modelos automáticamente cuando el rendimiento disminuye o cuando hay nuevos datos.
- **Escalado de la inferencia**: Las predicciones del modelo se escalan para servir a miles o millones de solicitudes en producción.

# ¿En qué se diferencian las MLOps de las DevOps?

*Tanto MLOps como DevOps son prácticas que buscan mejorar los procesos de desarrollo, implementación y monitoreo de software, pero con enfoques distintos.*

- ***DevOps**: Orientado al software tradicional*
- ***MLOps**: Enfocado en proyectos de machine learning*



| ¿QUÉ ES MLOPS? | ¿QUÉ ES DEVOPS? |
| --- | --- |
| MLOps se centra en los desafíos únicos de los proyectos de machine learning, automatizando todo el ciclo de vida del ML. | DevOps busca cerrar la brecha entre los equipos de desarrollo y operaciones, promoviendo la colaboración y acelerando los ciclos de lanzamiento. |
| • **Objetivo**: Automatizar el ciclo de vida del machine learning<br>• **Enfoque en datos:** Recopilación, entrenamiento y validación de modelos<br>• **Monitoreo continuo:** Garantiza el reentrenamiento y la actualización de modelos<br>• **Mayor precisión y valor empresarial:** Mejora el rendimiento del modelo con el tiempo | • **Objetivo**: Garantizar que los cambios de código se prueben, integren e implementen eficientemente<br>• **Colaboración**: Equipos de desarrollo y operaciones trabajan juntos<br>• **Ciclos de lanzamiento:** Más rápidos y de mayor calidad<br>• **Uso eficiente de recursos:** Optimización del uso de infraestructura |

# Diferencias clave entre MLOps y DevOps

*Aunque ambos comparten principios de automatización y colaboración, MLOps aborda los desafíos específicos del machine learning, mientras que DevOps está orientado al software tradicional.*

- ***DevOps**: Enfocado en la integración y despliegue continuo de aplicaciones*
- ***MLOps**: Además de la integración, añade reentrenamiento y monitoreo de modelos*
- ***Datos**: En MLOps, los datos son cruciales; en DevOps, el foco está en el código*
- ***Ciclo de vida:** MLOps tiene ciclos más largos y complejos debido a la dependencia de los datos*

Equipo 2

# Gracias!