

Máster Universitario en Computación y Sistemas Inteligentes

Master's Degree in Computation and Intelligent Systems

Proyecto fin de máster

Master's final project

Diseño e implementación de un marco tecnológico para la adopción de prácticas modernas en proyectos de inteligencia artificial

Asier Villar Marzo

Director: Mikel Emaldi Manrique

Bilbao, julio de 2024

Máster Universitario en Computación y Sistemas Inteligentes

Master's Degree in Computation and Intelligent Systems

Proyecto fin de máster

Master's final project

Diseño e implementación de un marco tecnológico para la adopción de prácticas modernas en proyectos de inteligencia artificial

Asier Villar Marzo

Director: Mikel Emaldi Manrique

Bilbao, julio de 2024

RESUMEN

En un mundo empresarial cada vez más dinámico y competitivo, el uso de metodologías y estándares modernos se ha convertido en una necesidad para las organizaciones que buscan mantenerse relevantes y competitivas. En este contexto, la adopción de metodologías ágiles, MLOps (Machine Learning Operations) y otras prácticas modernas se presenta como un elemento fundamental para facilitar la cooperación entre equipos, mejorar la calidad del producto y reducir los tiempos de desarrollo.

Las empresas que logran adaptarse y adoptar estos enfoques modernos experimentan una serie de beneficios significativos. En primer lugar, les permite responder de manera más rápida a los cambios en el entorno empresarial, lo que otorga una ventaja competitiva crucial. Además, la incorporación de prácticas de MLOps permite a las organizaciones gestionar de manera eficiente los modelos de machine learning en producción, garantizando su rendimiento y fiabilidad a lo largo del tiempo. Esto es especialmente relevante en un contexto donde el uso de la inteligencia artificial y el machine learning está cada vez más extendido dentro de la industria.

La implementación de estos estándares no está exenta de desafíos y dificultades. Cambiar la forma en que una empresa opera y se organiza puede ser un proceso complejo que requiere un cambio cultural significativo, así como la adopción de nuevas herramientas y tecnologías. El objetivo de este proyecto es diseñar un stack tecnológico que permita a una empresa adoptar estas metodologías y estándares de manera efectiva, facilitando la transición y reduciendo la complejidad de la misma.

DESCRIPTORES

MLOps, Machine Learning, CI/CD, Automatización, Metodologías ágiles

Índice

1. Introducción	1
1.1. Motivación	1
1.2. Estructura del documento	2
2. Antecedentes y justificación	3
2.1. Justificación	3
2.2. Antecedentes	4
2.2.1. Diseño Atómico	4
2.2.2. Machine Learning Operations (MLOps)	5
2.3. Estado del arte	6
2.3.1. Irrupción de las metodologías ágiles	7
2.3.2. Problemas de replicabilidad	7
2.3.3. Calidad del software y buenas prácticas	9
3. Objetivos y alcance	11
3.1. Objetivos generales	11
3.2. Alcance	11
3.2.1. Dentro del alcance	12
3.2.2. Fuera del alcance	12
4. Desarrollo del Proyecto	13
4.1. Infraestructura y herramientas	14
4.1.1. Descripción general de la infraestructura	14
4.1.2. Selección de plataformas	15
4.1.3. Seguridad y privacidad	18
4.1.4. Despliegue Automatizado	18
4.1.5. Problemas durante el Despliegue	19
4.2. Catalogo de componentes	19
4.2.1. Adaptación del diseño atómico	20
4.2.2. Estructura del sistema de componentes	20
4.2.3. Empaquetado de componentes	22
4.2.4. Sistema de plantillas	23
4.2.5. Integración continua y despliegue continuo	24
4.3. Documentación del proyecto	24
4.3.1. Guías y manuales	25
4.3.2. Documentación de componentes y plantillas	25
4.3.3. Sistema de búsqueda y organización de documentación	26
4.3.4. Construcción automática de documentación	27
5. Estandarización de procesos de trabajo	28
5.1. Integración en el flujo de trabajo	28
5.1.1. Proceso de integración	28
5.1.2. Herramientas de desarrollo	29
5.2. Desarrollo dentro de proyectos	30
5.2.1. Flujo de trabajo	30
5.2.2. Puesta en practica de la metodología	31
5.2.3. Proyectos de forecasting	31
5.2.4. Proyectos de clasificación	33

PROYECTO FIN DE MASTER

5.2.5. Proyectos de detección de anomalías	34
5.2.6. Proyectos de automl	34
5.3. Contribución al sistema de conocimiento	35
6. Planificación y presupuesto	36
6.1. Plan de recursos humanos	36
6.2. Programa de trabajo	37
6.2.1. Fase 1: Desarrollo del MVP	37
6.2.2. Fase 2: Integración de nuevas plataformas, securizacion y despliegue . . .	38
6.2.3. Fase 3: Experimentación, pruebas y documentación	38
6.2.4. Diagrama de Gantt	38
6.3. Tabla de tareas	40
6.4. Presupuesto	40
6.4.1. Recursos humanos	40
6.4.2. Hardware	41
6.4.3. Software	41
6.4.4. Total	41
7. Consideraciones éticas	42
7.1. Cuestiones éticas	42
7.1.1. Privacidad y seguridad de los datos	42
7.1.2. Responsabilidad y transparencia	42
7.1.3. Impacto en el empleo y las condiciones de trabajo	42
7.1.4. Impacto en el empleo y las condiciones de trabajo	43
7.1.5. Sostenibilidad y Responsabilidad Social	43
7.2. Análisis desde diferente perspectivas éticas	43
7.2.1. Perspectiva utilitarista	43
7.2.2. Perspectiva de la ética de los principios	43
8. Conclusiones y trabajo a futuro	45
8.1. Conclusiones	45
8.2. Trabajo a futuro	45

Índice de tablas

4.1. Tabla comparativa de las plataformas evaluadas	17
6.1. Resumen de las tareas y fases	40
6.2. Presupuesto de recursos humanos	40
6.3. Presupuesto hardware	41
6.4. Presupuesto general	41

Índice de figuras

2.1. Inversión global en IA en miles de millones [1].	3
2.2. Estructura conceptual diseño atómico [5].	5
2.3. Ciclo de vida MLOps [6].	6
2.4. Recreación gráfico crisis de reproducibilidad en la ciencia [14]	7
2.5. Problemas con la reproducibilidad por disciplina [14]	8
2.6. Factores que contribuyen a la irreproducibilidad [14]	9
4.1. Vista general del proyecto	13
4.2. Vista general del servidor interno.	14
4.3. Ejemplo de estructura de carpetas basada en Screaming Architecture.	21
4.4. Estructura mínima de un componente empaquetado.	22
4.5. Estructura final de un componente empaquetado.	23
4.6. Sistema de búsqueda	26
5.1. Comparativa de rendimiento sobre el repositorio de CPython	29
6.1. Diagrama de planificación del proyecto.	39

1. INTRODUCCIÓN

El presente documento constituye la memoria del Proyecto de Fin de Máster (PFM) del Máster en Computación y Sistemas Inteligentes de la Universidad de Deusto, realizado en colaboración con Tecnalia Research and Innovation, un centro de investigación aplicada. Su propósito es documentar de forma rigurosa el trabajo llevado a cabo, desde la conceptualización del problema hasta la implementación de la solución.

En la actualidad, los sistemas basados en inteligencia artificial (IA) desempeñan un papel muy significativo en diversos sectores como el de la medicina o la industria. Cada vez son más las empresas que buscan incorporar soluciones de IA para mejorar su eficiencia y competitividad. Sin embargo, el desarrollo de modelos de IA es un proceso complejo que demanda considerable esfuerzo y experiencia técnica, así como un mantenimiento continuo y una monitorización constante para garantizar su rendimiento óptimo.

En el contexto de la investigación y desarrollo, es común centrar los esfuerzos en la búsqueda de nuevas soluciones que aplicar a los nuevos retos que surgen dentro de la industria. Sin embargo, esta se ve gravemente ralentizada debido a la predominancia de tareas repetitivas y procesos manuales que consumen una gran cantidad de tiempo, pero no aportan un valor diferencial. Además, la falta de un buen sistema de gestión del conocimiento, conlleva por parte de las empresas a la pérdida de información generada durante el desarrollo de proyectos previos y que podría ser reutilizada en un futuro. Todo ello sumado a la ausencia de un marco de trabajo común, dificulta en gran medida la cooperación, ya que cada miembro del equipo requiere de un tiempo adicional para adaptarse a las especificaciones de cada proyecto.

Durante los últimos años, el concepto de MLOps (Machine Learning Operations) ha ido ganando popularidad hasta convertirse en un elemento disruptivo en cuanto a desarrollo de modelos de IA se refiere. Este nuevo paradigma, que toma como base las prácticas DevOps (Development Operations), busca combinar la IA y el desarrollo de software moderno con el objetivo de tener un mayor control sobre el ciclo de vida de los modelos, permitiendo una entrega continua. Estas prácticas han demostrado ser muy efectivas en la industria, pero en cambio no han sido totalmente acogidas en el ámbito de la investigación. Esto puede deberse a multitud de factores, ya sea por la resistencia al cambio, la falta de comprensión de sus beneficios o la falta de recursos dedicados a su implementación.

Uno de los principales desafíos en la implementación de estas prácticas radica en las diferencias de conocimientos entre los miembros del equipo, lo que genera fricción. Por tanto, resulta crucial considerar el punto de partida del equipo y diseñar un proceso intuitivo. Este proyecto propone un estándar que aborda esta problemática, recopilando las mejores prácticas, tecnologías y procedimientos desarrollados hasta la fecha, y las adapta a un marco de trabajo común que facilite la cooperación y la reutilización de conocimiento.

1.1. MOTIVACIÓN

Mi motivación para empezar este proyecto surge de la necesidad identificada por Tecnalia de explorar el ámbito del software, específicamente enfocándose en la creación de una herramienta que agilice el proceso de desarrollo de modelos de aprendizaje automático. Esta herramienta tiene como objetivo permitir que los investigadores dediquen más tiempo a la investigación en sí y menos a tareas repetitivas, al mismo tiempo que fomenta la cooperación y la reutilización del conocimiento de manera eficiente.

Desde el principio, encontré este tema sumamente interesante, especialmente considerando mi experiencia previa en el desarrollo de software. Percibí la oportunidad de aportar una solución innovadora que podría ser de gran ayuda para abordar los desafíos identificados por Tecnalía.

Además, el hecho de que la integración de buenas prácticas en el desarrollo de modelos de IA sea un tema en constante crecimiento, pero aún poco explorado en el ámbito de la investigación, me motiva aún más. Esta situación me brinda la oportunidad de realizar una contribución significativa que no solo beneficiará a Tecnalía, sino que también podría ayudar a otros equipos de investigación que se enfrenten a problemáticas similares.

1.2. ESTRUCTURA DEL DOCUMENTO

En esta sección, se presenta la estructura del documento. Se brinda una visión general de cómo se han organizado los diferentes capítulos y secciones para abordar de manera general todos los aspectos relevantes del proyecto. Además, se proporciona una breve descripción de cada capítulo, destacando su contenido y su contribución al conjunto de la memoria.

- **Introducción.** En este capítulo se presenta de forma breve el objetivo principal del proyecto, su impacto deseado y la motivación detrás de su realización. Además, se realiza una breve descripción del problema a resolver y se enumeran los capítulos que componen el proyecto.
- **Antecedentes y justificación.** Se proporciona un estudio del estado del arte y las últimas tendencias, y se justifican las antecedentes existentes durante el desarrollo del proyecto.
- **Objetivos y alcance.** Se definen tanto el objetivo principal como los objetivos secundarios del proyecto. También se establece el alcance del proyecto, que se describe mediante una lista de elementos que se encuentran dentro y fuera del proyecto.
- **Desarrollo del proyecto.** Se explican en detalle todos los aspectos técnicos del mismo. Se incluyen la arquitectura del sistema integral, las herramientas utilizadas para el desarrollo, los requisitos del sistema y las incidencias encontradas entre otros.
- **Planificación y presupuesto.** Se detallan las fases y tareas del proyecto de forma cronológica e indicando su duración. También se incluye un esquema de descomposición del trabajo y el plan de recursos humanos. Además, se incluyen los costes totales del proyecto, incluyendo los materiales y los recursos humanos.
- **Dimensión ética del proyecto.** Se realiza un análisis ético del proyecto para garantizar que en su conjunto sea considerado éticamente aceptable y una contribución positiva para la sociedad.
- **Conclusiones y trabajo a futuro.** Se presentan las reflexiones realizadas tras la finalización del proyecto, así como las lecciones aprendidas y los conocimientos adquiridos. Además, se presentan ideas o propuestas que podrían ser utilizadas o implementadas en futuras investigaciones.
- **Bibliografía.** Se incluye una lista de referencias bibliográficas utilizadas durante el desarrollo de la memoria.

2. ANTECEDENTES Y JUSTIFICACIÓN

Esta sección se centra en describir el ecosistema actual del desarrollo e investigación de modelos de inteligencia artificial y justificar la necesidad de la creación de un estándar dentro de un equipo. Se presentan datos e información general sobre las tecnologías más relevantes utilizadas en el proyecto, dando una visión general de por qué se eligieron, teniendo en cuenta las últimas tendencias que están surgiendo en el ámbito del aprendizaje automático.

2.1. JUSTIFICACIÓN

Cada año, más empresas y organizaciones invierten recursos significativos en proyectos de IA. Como se muestra en la figura 2.1, en 2021 la inversión global superó los 270 mil millones de dólares [1], lo que supone un aumento del 40 % de la inversión con respecto al año anterior. Este crecimiento de la inversión busca aprovechar al máximo el potencial de la IA y sacar provecho de su ventaja competitiva. Un ejemplo notable de este fenómeno es OpenAI, una empresa que ha sido valorada en más de 80 mil millones de dólares [2] con el record de crecimiento en el número de usuarios más rápido de la historia [3]. Todo esto gracias a su modelo de lenguaje GPT-3 y sus respectivas versiones GPT-4, GPT4-turbo y GPT4-o, que han demostrado cómo una aplicación de inteligencia artificial puede llegar a impactar significativamente en la vida de las personas.

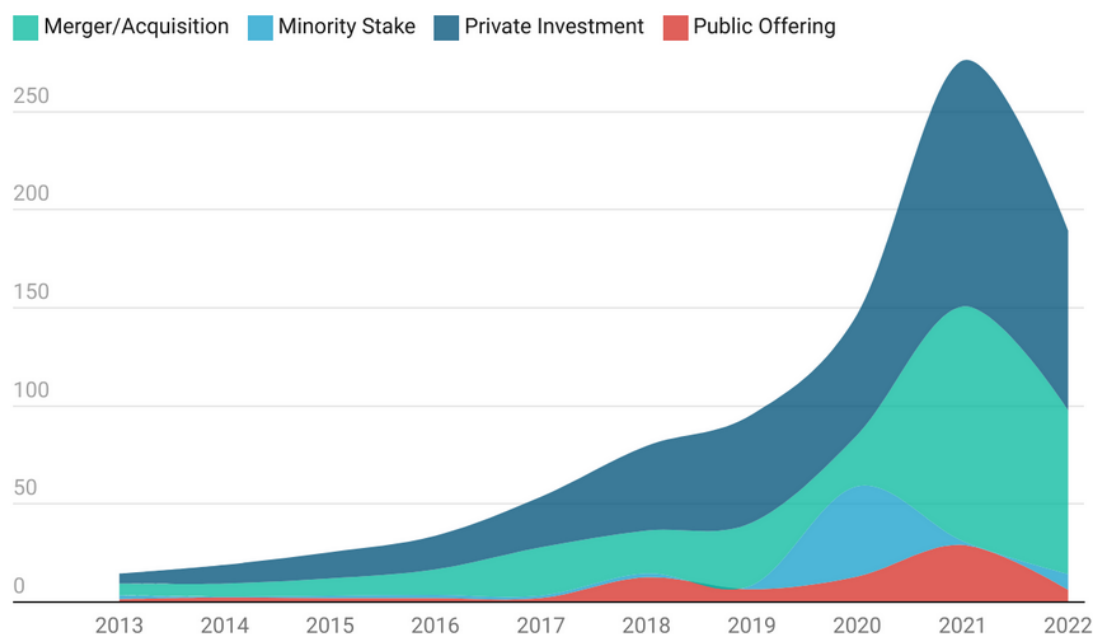


Figura 2.1: Inversión global en IA en miles de millones [1].

La demanda de equipos cualificados en el desarrollo de modelos de IA que puedan hacer frente a los nuevos desafíos es mayor que nunca. La complejidad de los proyectos de IA está en aumento, ya que las aplicaciones de IA se vuelven más sofisticadas, abarcan una gama más amplia de funciones, requieren un mayor número de datos y los modelos se vuelven cada vez más complejos. Esta situación ha forzado a las empresas a buscar nuevas formas de gestionar sus

proyectos que han llevado a la creación de nuevas metodologías, adaptadas a las necesidades a los nuevos retos que se presentan. Si bien es cierto que mucha información es compartida con la comunidad, existe un gran secretismo en torno a la forma de operar de las empresas más grandes, lo que dificulta la adopción de estas metodologías. Podemos resaltar positivamente el caso de Meta [4], que es el mayor referente en cuanto contribución y apertura de sus desarrollos en IA.

Por todo ello, es necesario realizar contribuciones que se centren en el como se debería operar dentro de un equipo. Se requiere de una referencia clara sobre las directrices que se deben aplicar para poder implementar un estándar tecnológico y operacional dentro de un grupo de trabajo, así como las herramientas, metodologías y buenas prácticas a seguir para hacer un uso eficiente de los recursos y obtener resultados de calidad. Este documento representa un estándar que se ha aplicado en base a unas necesidades concretas y, aunque no está pensado para poder ser adoptado de forma literal por otros equipos, se muestra el camino que se ha seguido desde la adopción de plataformas MLOps hasta la creación de un sistema de conocimiento para la reutilización de trabajo. La justificación de este documento es exponer el trabajo realizado y servir como referencia equipos que quieran implementar un estándar similar o busquen inspiración para crear el suyo propio.

2.2. ANTECEDENTES

En la sección de antecedentes, se profundiza en aquellos conceptos esenciales que son indispensables para entender el alcance y las contribuciones de este trabajo, así como para situarlo dentro de un marco conceptual adecuado. Se abordan aspectos fundamentales que no solo proporcionan contexto, sino que también establecen las bases teóricas y metodológicas sobre las cuales se construye la investigación.

2.2.1. Diseño Atómico

El diseño atómico es una metodología de diseño que se centra en la creación de sistemas modulares y reutilizables. La idea principal es dividir las diferentes funcionalidades de un sistemas en sus partes más fundamentales, de manera que cada una de estas partes pueda ser reutilizada en diferentes contextos. Este enfoque permite tener un mayor control sobre cada una de las partes del sistema, facilitando su mantenimiento, documentación y reutilización. Originalmente, el diseño atómico ha sido aplicado en el diseño de interfaces de usuario, pero su filosofía puede ser aplicada a cualquier sistema de diseño modular. En el contexto de este proyecto, el diseño atómico se aplicará al diseño de un sistema de componentes para el desarrollo de modelos de aprendizaje automático.

Dentro del diseño atómico, los componentes se dividen en cinco categorías principales, que representan diferentes niveles de abstracción. Estas categorías son: átomos, moléculas, organismos, plantillas y páginas. Cada una de estas categorías representa un nivel de abstracción diferente, y se relaciona con las demás categorías de manera jerárquica. La figura 2.2 muestra la estructura conceptual del diseño atómico.

A continuación, se describen brevemente cada una de las categorías:

- **Átomos:** Los átomos son los componentes más básicos de un sistema de diseño. Representan las funcionalidades más fundamentales, solo tienen una responsabilidad y no dependen de otros componentes.
- **Moléculas:** Las moléculas son la combinación de varios átomos para formar una funcionalidad más compleja. Representan la combinación de diferentes funcionalidades básicas para formar una funcionalidad más compleja.

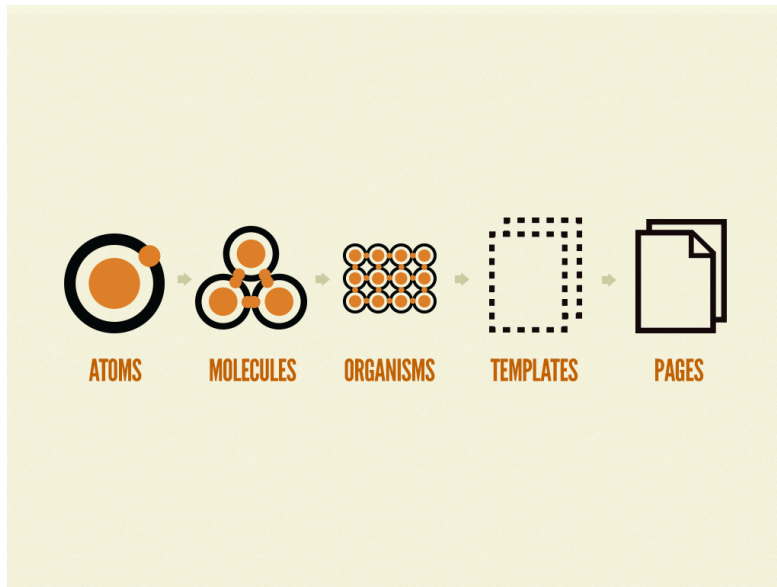


Figura 2.2: Estructura conceptual diseño atómico [5].

- **Organismos:** Los organismos son la combinación de varias moléculas y átomos para formar una funcionalidad completa.
- **Plantillas:** Las plantillas son la combinación de varios Organismos para dar forma a un contenido.
- **Páginas:** Las páginas son la combinación de varias plantillas.

Esta estructura jerárquica permite que los componentes sean reutilizados en diferentes contextos, y que cada uno de ellos pueda ser modificado de manera independiente. Además, se facilita la documentación y el mantenimiento de los componentes, ya que cada uno de ellos es independiente de los demás. Podemos ver multitud de ejemplos de diseño atómico en grandes empresas y que nosotros utilizamos a diario, como por ejemplo en la creación de sistemas de diseño Microsoft Fluent Design o Google Material Design entre otros.

Aunque el diseño atómico se ha aplicado tradicionalmente a la creación de interfaces de usuario, su filosofía puede ser aplicada a cualquier sistema de diseño modular. En el contexto de este proyecto, el diseño atómico se aplicará para la creación de un sistema de componentes en el desarrollo de modelos de aprendizaje automático. Traeremos la filosofía del diseño atómico y la adaptaremos a nuestro contexto, con las particularidades y necesidades que requiere el desarrollo de modelos de aprendizaje automático.

2.2.2. Machine Learning Operations (MLOps)

El desarrollo de modelos de aprendizaje automático es un proceso complejo que implica la recopilación de datos, la creación de modelos, la evaluación de los modelos y su puesta en producción. Cada una de estas etapas requiere de diferentes herramientas y prácticas, y es importante que estas herramientas y prácticas estén integradas de manera coherente para garantizar la eficacia del proceso. Los principios de MLOps son una serie de prácticas y herramientas que se utilizan

para gestionar el ciclo de vida de los modelos de aprendizaje automático. Como se muestra en la figura 2.3, este enfoque busca aplicar las mejores tendencias dentro de la ingeniería de software al desarrollo de modelos, con el objetivo de mejorar la eficiencia, la calidad y la escalabilidad.

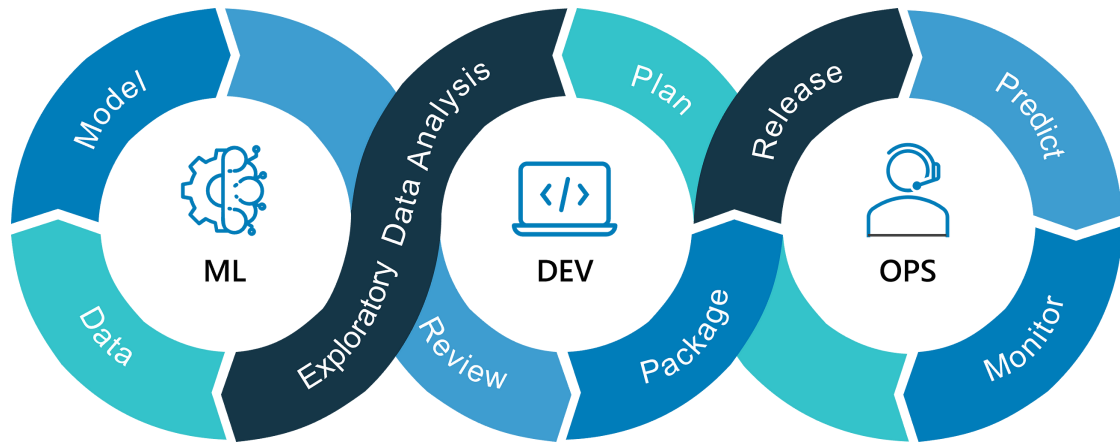


Figura 2.3: Ciclo de vida MLOps [6].

Algunos de los principios clave de MLOps son:

- **Automatización:** la automatización es esencial para mejorar la eficiencia del desarrollo de modelos y prevenir errores. Esto implica automatizar tareas como la generación de datos, el despliegue de modelos, evaluación y su puesta en producción.
- **Colaboración y reproducibilidad:** uno de los desafíos en el aprendizaje automático es lograr reproducir resultados de manera consistente, dada la naturaleza aleatoria de los algoritmos. MLOps busca, en la medida de lo posible, garantizar cierta consistencia entre los resultados obtenidos durante diferentes ejecuciones de un modelo para facilitar la colaboración entre los miembros del equipo.
- **Monitorización:** una vez que un modelo está en producción, es importante monitorizar su rendimiento para garantizar su eficacia y detectar posibles problemas. La monitorización permite crear alertas en caso de que el modelo no funcione correctamente y tomar medidas para corregirlo como por ejemplo, actualizar el modelo con nuevos datos.
- **Gestión de versiones:** controlar las versiones de los modelos y los datos es esencial para garantizar la reproducibilidad y la trazabilidad de los modelos. La gestión de versiones permite a los equipos comprender cómo ha evolucionado un modelo a lo largo del tiempo e incluso retroceder a versiones anteriores fuera necesario.

2.3. ESTADO DEL ARTE

La sección de estado del arte se centra en estudiar y analizar las tendencias actuales dentro del ámbito del aprendizaje automático y la inteligencia artificial. Debido a la diversidad de ramas que abarca la creación de un estándar tecnológico y operacional, se han seleccionado aquellas que se consideran más relevantes o presentan un mayor peso en cuanto a la toma de decisiones.

2.3.1. Irrupción de las metodologías ágiles

La aparición de metodologías ágiles en el desarrollo de software, con sus numerosas ventajas, ha dejado en desuso muchas metodologías clásicas. Las metodologías ágiles introdujeron el concepto de DevOps como un cambio de mentalidad [7] en la que los diferentes equipos colaboran para implementar procesos más rápidos y entregar nuevas funcionalidades al cliente de manera más ágil. MLOps es una extensión de DevOps que ha surgido muy recientemente y, por lo tanto, existen pocos estudios que aborden el tema [8][9].

Principalmente existen dos formas para implementar MLOps en una organización, uno es a través de los sistemas cloud que ofrecen servicios MLOps como Azure ML [10], AWS Sagemaker [11] o Google Cloud Vertex AI [12]. El otro es a través del despliegue de una plataforma open source como MLFlow dentro de la infraestructura propia. Las principales diferencias entre ambas opciones son el coste y la flexibilidad, ya que los servicios cloud ofrecen una mayor facilidad de uso y mejor experiencia de desarrollo, pero a un coste mayor. Por otro lado, la implementación de una plataforma open source requiere de un mayor esfuerzo pero ofrece se recompensa con una mayor flexibilidad y control sobre la infraestructura.

2.3.2. Problemas de replicabilidad

La crisis de replicabilidad es un fenómeno crítico en la comunidad científica, donde los resultados de los estudios a menudo no pueden replicarse con nuevos datos [13]. Este problema es muy destacado en numerosos campos científicos, que se han enfatizado particularmente en disciplinas como la psicología, la salud y la medicina [13][14], donde hallazgos incorrectos podrían tener consecuencias graves. Durante los últimos años, la crisis de replicabilidad ha sido objeto de debate dentro de la rama de la inteligencia artificial, donde la falta de transparencia, la complejidad de los modelos y la imposibilidad de replicar los resultados han sido identificados como problemas clave.

¿Existe una crisis de reproducibilidad?



Figura 2.4: Recreación gráfico crisis de reproducibilidad en la ciencia [14]

La confusión se ve incrementada por el uso variado de términos clave como reproducibilidad, replicabilidad y repetibilidad, [15] dificultando los esfuerzos para abordar estos problemas de manera efectiva. Se definen los diferentes términos de la siguiente manera:

- **Repetibilidad:** se centra en la consistencia de los resultados de la investigación cuando el equipo original re-ejecuta su experimento bajo condiciones inalteradas.
- **Reproducibilidad:** se logra cuando investigadores independientes validan los hallazgos del experimento original empleando el documentado original. Esta validación puede ser directa, utilizando los datos y el código originales, o independiente, a través de la reimplementación del experimento, probando así la fiabilidad de los resultados en diferentes equipos.

Una serie de estudios y encuestas subrayan la gravedad de la situación [14]. Como se muestra en la figura 2.4, una encuesta realizada a 1500 investigadores encontró que el 50 % de ellos afirman que hay una crisis significativa y un 40 % que hay una crisis moderada, dejando solo un 10 % que no ve una crisis en la replicabilidad de los estudios. Existen multitud de casos donde los intentos de volver a ejecutar experimentos dan como resultado a una amplia desviación, incluso bajo condiciones idénticas. Los propios investigadores tienen dificultades para reproducir sus propios experimentos. La figura 2.5 nos da una idea de lo frecuente que es este problema, donde en el caso de la física e ingeniería, el 50 % de los encuestados han tenido problemas reproduciendo sus experimentos, lo que se ve reflejado en que el 70 % de ellos haya tenido problemas al intentar reproducir los experimentos de otros investigadores.

¿Has tenido problemas reproduciendo un experimento?

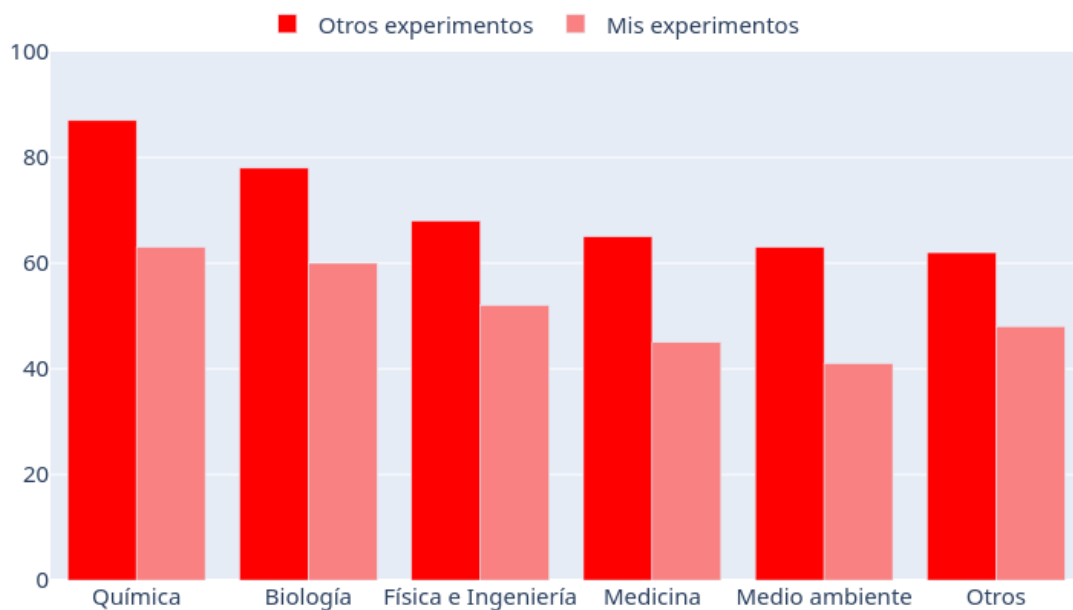


Figura 2.5: Problemas con la reproducibilidad por disciplina [14]

Estos problemas se consideran como los principales causantes como se puede ver en la figura 2.6. Factores como la falta de información sobre detalles experimentales y los tiempos de publicación, enfatizando la necesidad urgente de un enfoque más sistemático y transparente. Sin

contar los problemas directamente relacionados con el desarrollo, como son la procedencia y calidad de los datos, la elección del algoritmo, el hardware utilizado para su entrenamiento, el preprocesamiento de los datos, entre otros.

¿Qué factores afectan negativamente a la reproducibilidad?

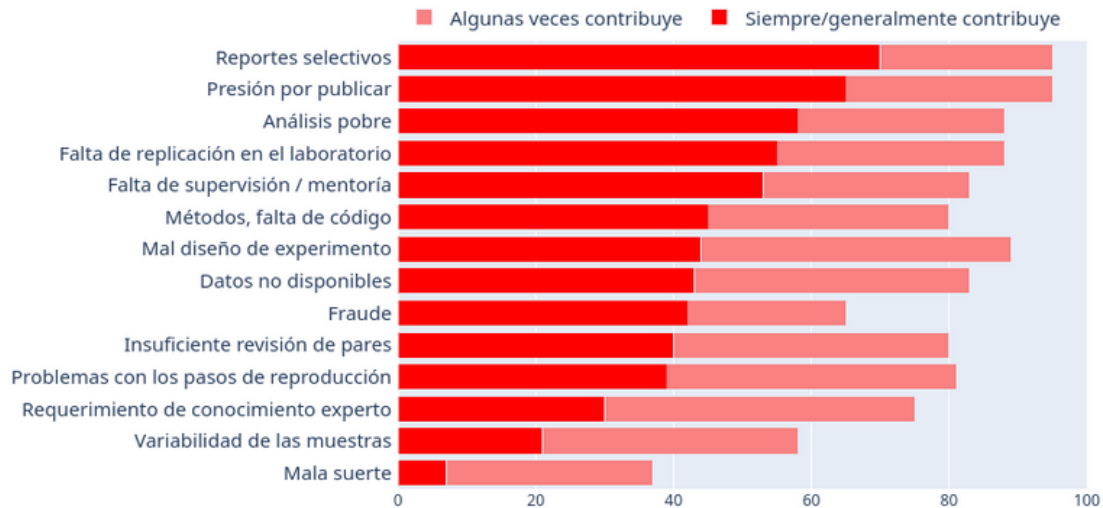


Figura 2.6: Factores que contribuyen a la irreproducibilidad [14]

Aunque la reproducibilidad es un problema complejo y multifacético, existen algunas medidas que pueden tomarse para abordarlo. Algunas de estas medidas que encontramos en la literatura son una mejor supervisión, mejora del proceso de validación, incentivar buenas prácticas de desarrollo, entre otras.

2.3.3. Calidad del software y buenas prácticas

Las buenas prácticas en la programación, como el uso de patrones de diseño, la creación de tests y una documentación adecuada, son esenciales para asegurar un alto rendimiento y eficiencia en los sistemas de software. Estas prácticas no solo facilitan la colaboración entre los desarrolladores, sino que también ayudan a prevenir errores y mejorar la calidad del software producido. Se han encontrado evidencias [16] que sugieren que la detección y resolución temprana de problemas mejora significativamente a mayor sea la cantidad y calidad de las pruebas realizadas. Este tipo de prácticas son especialmente importantes ya que aseguran que el software desempeñe correctamente la función para la que fue diseñado y permite tener un control más en profundidad del mismo.

Dentro del campo del aprendizaje automático, la calidad del software es un aspecto crítico que puede afectar significativamente el rendimiento de los modelos. Pese a que estos sistemas son más complejos y difíciles de depurar, debido a que muchos de los modelos son en su mayoría complejos en cuanto a explicabilidad, una mala gestión del código puede llevar a errores de diferente índole. Identificar y comprender estos fallos es crucial para mejorar la calidad y fiabilidad de los sistemas de IA.

Los principales fallos relacionados con malas prácticas de código son los siguientes:

- **Introducción de sesgos:** la proliferación de tecnologías de minería de datos y la acumulación de datos sociales han llevado a su uso en decisiones cruciales que afectan la vida de las personas [17]. Este tipo de datos son muy complejos ya que la mayoría de veces carecen de consistencia, están entrelazados y ramificados, y son muy sensibles a los cambios. Es muy sencillo cometer errores en cuanto a la recolección y tratamiento de los datos, lo que puede llevar a la introducción de sesgos de manera inconsciente [18]. Además, es necesario de conocimientos avanzados de tratamiento ya que muchas veces la práctica común de eliminar ciertos datos puede no ser suficiente para reducir el sesgo [17].
- **Uso excesivo de recursos:** El uso ineficiente de recursos computacionales durante el entrenamiento y despliegue de modelos puede llevar a un gasto innecesario de tiempo y energía [19]. La optimización de algoritmos y la implementación de técnicas de programación eficiente son esenciales para minimizar estos costos. Algunas de las prácticas que más impacto tienen en la eficiencia de los modelos son el uso de librerías basadas en C [20], la compilación de modelos mediante JIT [21], el empleo de técnicas de cacheo en momentos críticos [22], entre otros. Estas practicas pueden suponer un aumento de la velocidad de ejecución de un x2 en el peor de los casos y un x4 de media [19].
- **Errores en producción:** Los errores que no se detectan durante la fase de desarrollo pueden manifestarse en entornos de producción, afectando la fiabilidad y el rendimiento del sistema. La implementación de un sistema robusto de pruebas y monitoreo continuo puede ayudar a identificar y solucionar estos problemas antes de que impacten a los usuarios finales. Algunas de las practicas recomendables se basan en el uso de librerías de validación como Pydantic [23], que permiten validar los datos de entrada en tiempo real, la implementación de tests unitarios mediante Pytest [24] y la monitorización de los modelos en producción mediante herramientas como Prometheus [25] y Grafana [26].

3. OBJETIVOS Y ALCANCE

En esta sección se introducen los objetivos del proyecto, habiéndose realizado una división entre el principal y los secundarios. Además de ello, se presentan los elementos que forman el alcance y los que quedan fuera del mismo.

3.1. OBJETIVOS GENERALES

El objetivo principal del proyecto es diseñar e implementar un estándar tecnológico y operacional que cubra las necesidades más comunes dentro de un equipo de *data science*. Se busca agilizar los tiempos de desarrollo y estandarizar los procesos, con el fin de facilitar la colaboración entre investigadores y la reutilización del conocimiento. A continuación, se detallan los objetivos específicos que guiarán el desarrollo:

- **Agilizar el proceso inicial de proyectos:** Optimizar las primeras etapas de los proyectos, identificando y eliminando aquellos procesos repetitivos que no aportan valor y que puedan retrasar su puesta en marcha.
- **Facilitar la colaboración entre investigadores:** Implementar herramientas y métodos que fomenten una cooperación fluida y efectiva entre los miembros del equipo de investigación, con el fin de potenciar la sinergia y aprovechar al máximo el conocimiento colectivo.
- **Definir procesos mediante buenas prácticas:** Establecer un marco de trabajo basado en buenas prácticas de gestión de proyectos, con el objetivo de estandarizar los procesos y garantizar su eficiencia y calidad.
- **Automatizar el desarrollo de modelos robustos:** Investigar y aplicar técnicas que contribuyan al desarrollo automático de modelos de aprendizaje automático, con el fin de reducir el tiempo y el esfuerzo necesarios para obtener resultados de calidad.
- **Promover la reutilización del conocimiento:** Desarrollar mecanismos y herramientas que faciliten la captura, organización y difusión del conocimiento generado durante el desarrollo de los proyectos, con el propósito de fomentar su reutilización en futuras investigaciones y actividades relacionadas.

El cumplimiento de estos objetivos se espera que no solo mejore la eficiencia y la calidad de los proyectos, sino que también contribuya a la creación de un entorno de trabajo más colaborativo y enriquecedor para los miembros del equipo de investigación.

3.2. ALCANCE

En esta sección se definen los límites del proyecto, estableciendo lo que está incluido y excluido dentro mismo. Se describirá de manera detallada las actividades que forman parte del desarrollo final, así como aquellos elementos que no están incluidos en el alcance del proyecto. Aunque el enfoque de este proyecto podría aplicarse a una amplia variedad de problemas en el ámbito del aprendizaje automático, en el contexto de este TFM nos centraremos en tres de los casos más comunes dentro del marco de las series temporales: forecasting, clasificación y detección de anomalías. A continuación, se detallan las actividades que forman parte del alcance del proyecto.

3.2.1. Dentro del alcance

- **Integración de sistemas externos:** Se incluirá la configuración de sistemas externos, como plataformas MLOPs o herramientas de visualización, con las plantillas de proyectos base. Esto permitirá una integración más fluida y rápida de estos sistemas con los proyectos, facilitando el flujo de datos y la visualización de resultados.
- **Plantillas de proyectos base:** Desarrollar plantillas para los tres problemas de series temporales comentados anteriormente. Estas plantillas servirán como punto de partida para proyectos específicos dentro de cada uno de estos dominios y definirán desde el principio una estructura y un conjunto de herramientas comunes. Además, se incluirán ejemplos de código y documentación que faciliten su uso y comprensión.
- **Componentes esenciales:** Identificar y almacenar los componentes esenciales de cada proyecto, incluyendo modelos, algoritmos, métricas de evaluación y preprocesamiento de datos. Estos componentes se almacenarán y documentarán de forma que puedan ser reutilizados en futuros proyectos, facilitando la transferencia de conocimiento.
- **Proceso de AutoML:** Diseñará y ejecutar procesos de AutoML (Machine Learning Automatizado) que demostrará cómo se pueden combinar los conocimientos adquiridos de todos los proyectos para desarrollar un sistema de aprendizaje automático automatizado. Este proceso utilizará las plantillas y componentes esenciales almacenados para generar modelos de forma automática.

3.2.2. Fuera del alcance

- **Desarrollo de modelos específicos:** Aunque se incluirán ejemplos de modelos y algoritmos, el desarrollo de modelos específicos para problemas concretos no forma parte del alcance de este proyecto. Se espera que los modelos desarrollados sean generales y puedan ser adaptados a problemas específicos por los usuarios.
- **Despliegue de modelos:** El despliegue de modelos en producción no forma parte del alcance de este proyecto. Se espera que los modelos desarrollados puedan ser desplegados en sistemas de producción, pero no se incluirá en este proyecto. El enfoque se centrará exclusivamente en el desarrollo de los mismos.

4. DESARROLLO DEL PROYECTO

En esta sección se detallan los aspectos más relevantes del desarrollo del proyecto. Se profundizará en los diferentes aspectos del diseño, la implementación y la prueba de los sistemas y componentes desarrollados. Además, se describirán las herramientas y tecnologías utilizadas, así como los procesos y metodologías empleadas para el desarrollo del proyecto. A continuación, se muestra una vista general de los diferentes elementos que conforman la estructura del marco de trabajo.

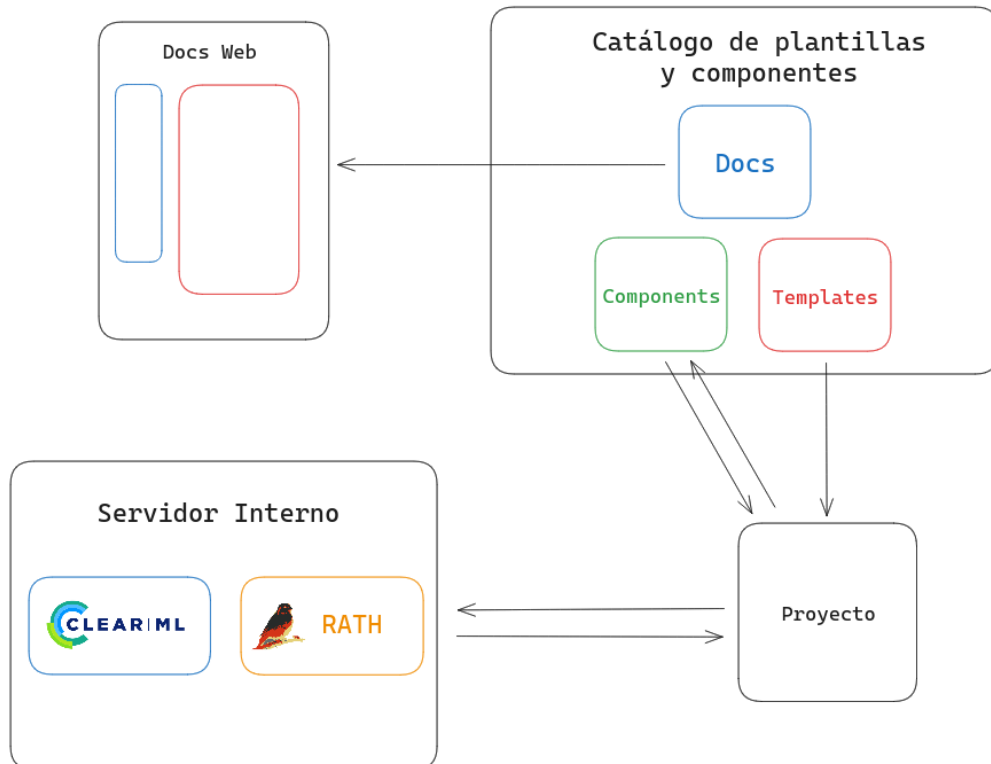


Figura 4.1: Vista general del proyecto

Dentro de la estructura general del proyecto, se pueden identificar tres elementos principales: la infraestructura y herramientas, el catálogo de componentes y la documentación del proyecto. Cada uno de estos elementos se encarga de aspectos diferentes dentro del ecosistema del proyecto, y se relacionan entre sí para formar un sistema completo. La idea principal es que la infraestructura sea complementaria al desarrollo, estando al alcance de los investigadores de una forma sencilla. El catálogo de componentes y plantillas se encarga de proporcionar una base sólida sobre la que construir los diferentes proyectos, automatizando la creación de proyectos siguiendo las mejores prácticas y proporcionando una base sólida sobre la que construir. Por último, la documentación del proyecto se encarga de proporcionar una guía clara y detallada sobre el uso de las herramientas y componentes, así como de los procesos y metodologías empleadas en el

desarrollo del proyecto.

4.1. INFRAESTRUCTURA Y HERRAMIENTAS

4.1.1. Descripción general de la infraestructura

La infraestructura y las herramientas son la base sobre la que se construirán los diferentes proyectos de aprendizaje automático. Se encargan de proporcionar un entorno de desarrollo e investigación eficiente, que permita a los miembros del equipo centrarse en el desarrollo de modelos sin tener que preocuparse por la configuración. Concretamente, se han desplegado dos plataformas que vienen a cubrir varias de las necesidades fundamentales de los proyectos como son la gestión y exploración de datasets, la monitorización de experimentos o el almacenamiento de modelos de inteligencia artificial. Además, se ha añadido un sistema de autenticación para garantizar la seguridad y privacidad de los datos.

Esta infraestructura se ha desplegado en un servidor interno de la empresa utilizando contenedores de Docker. La elección de esta tecnología se debe a que permite la creación de entornos aislados y portables, lo que facilita el despliegue de las aplicaciones. Se ha utilizado Docker Compose para sincronizar el despliegue de los diferentes servicios, lo que permite realizar despliegues automatizados mediante las acciones de GitLab CI. La figura 4.2 muestra una vista general de la infraestructura desplegada en el servidor interno de la empresa, donde se pueden observar como se integran los diferentes servicios y sus respectivas conexiones. Además, se puede observar que todos los servicios están interconectados mediante un proxy inverso mediante Nginx, que se encarga de redirigir las peticiones en función de la URL. Esto permite que todos los servicios sean accesibles desde el exterior a través de un único punto de entrada y que el sistema de autenticación sea común para todos ellos.

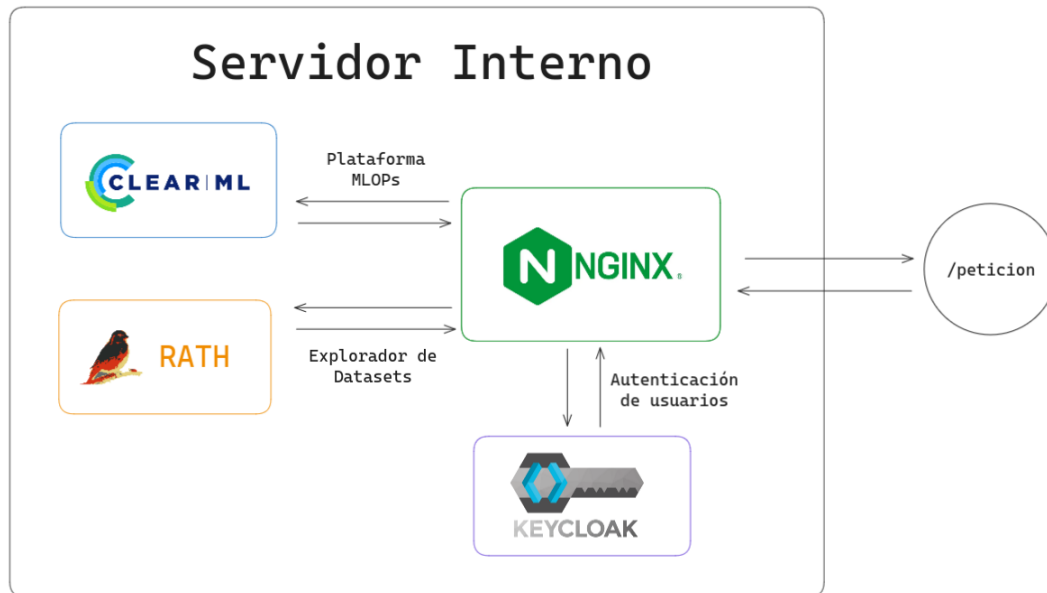


Figura 4.2: Vista general del servidor interno.

4.1.2. Selección de plataformas

Previo a la elección de las plataformas integradas, se realizó una evaluación a nivel de equipo para determinar las necesidades que se debían cubrir. Se identificaron las siguientes funcionalidades fundamentales:

- **F1:** Versionado y almacenamiento de dataset.
- **F2:** Monitorización de experimentos.
- **F3:** Almacenamiento de modelos de inteligencia artificial.
- **F4:** Integración de métricas en datasets y visualización de resultados.
- **F5:** Exploración de datasets.

Una vez identificadas las necesidades, se consensuó un criterio de selección para las plataformas integradas. Este criterio es un criterio de mínimos, es decir, se seleccionarán las plataformas que cumplan con el criterio mínimo establecido y que, además, ofrezcan funcionalidades adicionales que puedan ser de utilidad para el equipo. El criterio de selección se basa en los siguientes aspectos:

- **C1 (Facilidad de uso):** se valora muy positivamente la facilidad de uso de las plataformas, ya que se considera que no todo el equipo no tiene experiencia previa en el uso de estas herramientas.
- **C2 (Integración con otras herramientas):** es fundamental que las plataformas integradas sean compatibles con las librerías y herramientas que se utilizan generalmente en proyectos (TensorFlow, PyTorch, etc.).
- **C3 (Poca dependencia sobre la infraestructura):** se mide la dependencia sobre una plataforma como el número de acciones que se deben realizar para migrar un proyecto estándar, es decir, un proyecto que no ha sido desarrollado con la plataforma en mente. Y penalizando aquellas prácticas que sean propias de la plataforma y que no sean comunes en la industria.

Con estos criterios en mente, se tuvieron en cuenta las siguientes plataformas a la hora de realizar la evaluación: MLflow, ClearML, Kedro, ZenML, Data Version Controller (DVC), Rath, Apache Superset. Cada una de estas plataformas tiene diferentes enfoques y funcionalidades, pero todas ellas cubren una o varias de las necesidades fundamentales identificadas, por lo que se consideraron candidatas para su integración en la infraestructura. La infraestructura final se compondrá de una o varias de estas plataformas en función de los criterios previamente establecidos. A continuación, se muestra un análisis detallado de las plataformas evaluadas y las funcionalidades que ofrecen.

- **MLflow:** MLflow [27] es una plataforma MLOPs de código abierto para la gestión del ciclo de vida de los modelos. Ofrece una interfaz de usuario para el seguimiento de experimentos, la gestión de modelos y la implementación de modelos en diferentes entornos. MLflow es compatible con la mayor parte de librerías de aprendizaje automático, como TensorFlow o PyTorch. Uno de los puntos fuertes de MLflow es su gran comunidad, ya que es una de las plataformas más utilizadas en la industria. Sin embargo, no ofrece funcionalidades relacionadas con la gestión, evaluación o versionado de datasets ni con la exploración de los

mismos. La dependencia sobre la plataforma varía en función de la tarea que se quiera realizar, pero en general, es una plataforma que no ata al usuario a su ella. La documentación se queda corta en cuestión de claridad y ejemplos, lo que puede dificultar la adopción de la plataforma por parte de los miembros del equipo.

- **ClearML:** Similar a MLflow, ClearML [28] es una plataforma MLOps de código abierto que ofrece funcionalidades para la gestión de experimentos, pero con la ventaja de incluir herramientas para la gestión, evaluación y versionado de datasets. La dependencia sobre la plataforma es mínima, ya que con pocos cambios se pueden lanzar experimentos y adicionalmente permite el lanzamiento de pipelines, gestión de alertas, orquestación de modelos y generación de puntos de acceso para modelos ya desplegados. Aunque es compatible con muchas bibliotecas populares su comunidad es más limitada, lo que puede dificultar a la hora de encontrar soluciones a ciertas problemáticas. La documentación es clara y ofrece ejemplos en formato tanto en formato de blog como de video facilitando la comprensión. Sin embargo, carece de un sólido sistema de autenticación por defecto, lo que requiere una implementación adicional para proteger correctamente la aplicación web.
- **Data Version Controller (DVC):** DVC [29] es una herramienta de código abierto que están diseñadas para manejar grandes volúmenes de datos, modelos y experimentos. DVC se centra en el versionado y almacenamiento de datasets, mientras que DVC Studio se centra en la monitorización de experimentos, visualización de resultados y almacenamiento de modelos, pero a diferencia de DVC esta es una herramienta de pago. DVC proporciona integraciones con un número considerable de librerías de aprendizaje automático. La documentación está bien estructurada aunque no es tan clara como la de ClearML, pero cuenta con una comunidad bastante activa. En cuanto a los aspectos negativos de DVC, la principal desventaja es que la curva de aprendizaje es bastante pronunciada, lo que dificulta su adopción. Otro punto en contra es la gran dependencia que tienen los proyectos que usan DVC, ya que se necesita de varios archivos de configuración, integraciones manuales dentro del código y un dominio completo de los comandos de la herramienta para poder trabajar con ella. Además, funcionalidades clave como la visualización son funcionalidades de pago en DVC Studio, lo que limita su uso en la capa gratuita.
- **ZenML:** ZenML es una plataforma de código abierto encargado de la orquestación de pipelines en proyectos de aprendizaje automático. Ofrece una experiencia de desarrollo cómoda y modular, que facilita la reutilización de código. Además, cuenta con integraciones para las plataformas de almacenamiento mas populares, como AWS y Google Cloud. A diferencia de ClearML y MLflow, este no está enfocado en la gestión de experimentos ya que no es una plataforma MLOps, aunque si que ofrece conexiones con esta última para poder redireccionar nuestros experimentos. La documentación es clara y podemos encontrar diversos repositorios con ejemplos de uso o integración con otras herramientas. El problema de esta radica principalmente en el hecho de que al no ser una plataforma MLOps, no ofrece funcionalidades relacionadas con la gestión o versionado de datasets, lo que es un punto negativo para nuestro caso de uso. Otro de los problemas es que las plataformas que integra no comparten las mismas credenciales dentro de su capa gratuita, lo que dificulta en gran medida su uso.
- **Kedro:** Al igual que ZenML, Kedro es una plataforma de código abierto que se centra en la orquestación de pipelines en proyectos de aprendizaje automático. Otra diferencia respectiva a ZenML es que Kedro no ofrece compatibilidad con ningún tipo de plataforma MLOps, en cambio, trae su propia herramienta e implementación propia de la mayoría de funcionalidades de orquestación. Su herramienta de consola es configurable y compatible

con Cookiecutter, lo que facilita la creación de plantillas personalizadas. Por otro lado, al ser muy similar a ZenML, Kedro tampoco ofrece funcionalidades relacionadas con la gestión de experimentos, lo que es un punto negativo para nuestro caso de uso.

- **Rath:** herramienta de exploración de datasets que permite una exploración semi-automática de datasets. Muy fácil de utilizar, ya que cuenta con un modo copilot que te sugiere diferentes gráficos y estadísticas en función de los datos que estés explorando. Además, no requiere de ninguna configuración previa, ya que se puede utilizar directamente desde el navegador.
- **Apache Superset:** Apache Superset es una plataforma de visualización de datos de código abierto que ofrece una amplia gama de características para explorar y visualizar datos de manera interactiva. Con una interfaz intuitiva y basada en web, Superset permite a los usuarios crear paneles de control, gráficos y tablas dinámicas con facilidad. Además, ofrece integraciones con diversas fuentes de datos y admite la creación de paneles de control en tiempo real. Una de las fortalezas de Apache Superset es su comunidad activa y en constante crecimiento, lo que garantiza un soporte sólido y una mejora continua de la plataforma. Sin embargo, la integración con el resto de herramientas es limitada, ya que el propio Superset requiere de un formato de datos concreto para poder subir los datos a la plataforma, lo que puede dificultar su integración y generar duplicidad en cuanto a los datos almacenados, ya que se necesitaría una copia de los datos en el formato que requiere Superset. Nuestro objetivo es que esta herramienta agilice el proceso de exploración de datos, por lo que no es una opción viable por el momento.
- **Grafana:** Grafana es una plataforma de análisis y visualización de métricas de código abierto que se ha convertido en una opción popular para monitorear sistemas y aplicaciones. Con una amplia gama de complementos y paneles personalizables, Grafana permite a los usuarios crear cuadros de mando y gráficos altamente personalizados para visualizar datos de diferentes fuentes. Además, ofrece características avanzadas como alertas, anotaciones y exploración de datos en tiempo real. Grafana es altamente modular y extensible, lo que facilita su integración con diversas tecnologías y sistemas de monitorización. El problema de Grafana es el mismo que el de Superset, ya que requiere de un formato de datos concreto para poder subir los datos a la plataforma, lo que puede dificultar su integración y generar duplicidad en cuanto a los datos almacenados. Además, de su curva de aprendizaje, que es bastante pronunciada.

Tecnología	Funcionalidades					Criterios		
	F1	F2	F3	F4	F5	C1	C2	C3
MLflow	–	✓	✓	–	–	✓	✓	✓
ClearML	✓	✓	✓	✓	–	✓	✓	✓
DVC	✓	✓	✓	✓	–	–	✓	–
ZenML	–	✓	✓	–	–	✓	✓	✓
Kedro	–	–	✓	✓	–	✓	✓	✓
Rath	–	–	–	–	✓	✓	–	✓
Apache Superset	✓	–	–	✓	–	–	–	✓
Grafana	✓	–	–	✓	–	–	–	✓

Cuadro 4.1: Tabla comparativa de las plataformas evaluadas

Para finalizar con la evaluación, se puede observar en la tabla 4.1 una comparativa que muestra las funcionalidades y criterios que cumple cada una de ellas de forma resumida. De acuerdo con la evaluación realizada, se ha decidido integrar ClearML y Rath en la infraestructura como las plataformas finales. ClearML cubre la mayoría de las necesidades fundamentales identificadas, ya que ofrece soluciones para la mayoría de casos de uso, mientras que Rath complementa con la exploración de datasets de forma sencilla e intuitiva.

4.1.3. Seguridad y privacidad

La seguridad y la privacidad de los datos son aspectos fundamentales dentro de un entorno de trabajo empresarial, donde la confidencialidad de los datos es una prioridad para la empresa. Por ello, ya que ClearML y Rath no cuentan con un sistema de autenticación robusto, se ha decidido implementar un sistema de autenticación utilizando Keycloak, que es una solución de código abierto para la gestión de acceso. Keycloak permite a los usuarios autenticarse con cuentas de usuario gestionadas por la empresa, lo que garantiza que solo los usuarios autorizados puedan acceder a los datos. Además, ofrece integraciones con diferentes proveedores de identidad, lo que facilita la gestión de usuarios y la integración con otras herramientas.

Debido a que tanto ClearML como Rath no tienen integraciones directas con Keycloak, se ha decidido utilizar Nginx como proxy inverso para redirigir las peticiones a los servicios de ClearML y Rath. De esta forma, se puede utilizar Keycloak para autenticar a los usuarios y garantizar la seguridad y la privacidad de los datos. La figura 4.2 muestra cómo se ha integrado Keycloak en la infraestructura, así como las conexiones entre los diferentes servicios y el proxy inverso. En el momento actual, se ha implementado un sistema de autenticación básico, pero se espera que en el futuro este sistema se sincronice con el sistema de autenticación de Tecnalia para una mayor comodidad por parte de los usuarios.

4.1.4. Despliegue Automatizado

Para la automatización del despliegue de la infraestructura se ha utilizado GitLab CI, una herramienta de integración y despliegue continuo que permite automatizar el proceso de despliegue de aplicaciones. GitLab CI permite definir un conjunto de pasos que se ejecutarán cada vez que se realice un cambio en el repositorio, lo que facilita el despliegue de aplicaciones y la gestión de la infraestructura.

Para poder utilizar GitLab CI, es necesario primero definir un runner, que es un agente que se encarga de ejecutar los pasos definidos en el archivo de configuración. En este caso, el runner se ha desplegado en el servidor lo que permite ejecutar los diferentes flujos en el mismo entorno. Además, otro aspecto a tener en cuenta es que por seguridad, se ha configurado el sistema con variables de entorno que enmascaran las credenciales de acceso a los diferentes servicios, lo que garantiza que las credenciales no se almacenen en el repositorio. En cuanto a las pipelines, se han definido tres diferentes flujos para automatizar cada uno de los procesos de instalación y actualización:

- **Instalación de autenticación:** Se encarga de instalar Keycloak en el servidor junto con la base de datos. Este flujo se ejecutará si no se ha instalado Keycloak previamente.
- **Instalación de infraestructura:** Se encarga de instalar ClearML y Rath en el servidor. Además, también se encarga de configurar el proxy inverso para redirigir las peticiones a los servicios de ClearML y Rath. Este flujo se ejecutará si no se ha instalado ClearML previamente.

- **Despliegue de infraestructura:** Se encarga de actualizar el servidor a los nuevos cambios realizados en el repositorio. Este flujo se lanza cada vez que detecta un cambio en el repositorio, pero requiere de una aprobación manual para ejecutarse.

La idea de estos flujos es que se puedan ejecutar de forma independiente y que en caso de que se necesite realizar un cambio en la infraestructura, se pueda lanzar el flujo en otro servidor para instalar la infraestructura de forma automática. Además, facilita el trabajo en local, ya que una vez automatizado el despliegue, los cambios en local se pueden probar lanzar directamente en el servidor.

4.1.5. Problemas durante el Despliegue

A continuación se detallan la lista de problemas que se han encontrado durante el despliegue de la infraestructura y las soluciones que se han aplicado para resolverlos. Estos soluciones se detallan con el fin de que puedan ser de utilidad para futuros despliegues o como registro para mejoras futuras.

- **Clearml no es compatible con servidores no IPv6.** Por defecto, ClearML utiliza direcciones IPv4 e IPv6 para comunicarse con el servidor. Sin embargo, en el servidor interno de la empresa no está habilitado el soporte para direcciones IPv6, lo que provoca que ClearML no pueda comunicarse con el servidor. Internamente, ClearML utiliza una configuración de Nginx para esta comunicación, pero no es posible modificarla directamente ya que el contenedor de Docker lanza un script en bash que sobrescribe la configuración de Nginx y luego lanza el servidor. La solución a este problema es sobrescribe una variable interna llamada *DISABLE_NGINX_IPV6* dentro del contenedor de Webserver de ClearML. Este error es común pero no está documentado en la documentación oficial, la solución es una propuesta personal que ha sido descubierta mediante la lectura del código.
- **ClearML no renderiza correctamente en el navegador.** Otro de los problemas que encontramos al desplegar ClearML es que el servidor interno de la empresa no era capaz de servir archivos estáticos de un tamaño superior a 3.5MB. Esto provocaba que la interfaz de usuario de ClearML no se renderizara correctamente los gráficos, ya que internamente utiliza plotly para la visualización de los mismos. La solución a este problema fue recompilar la librería de plotly por nuestra cuenta incluyendo solamente los gráficos que necesitamos, de esta forma reducimos el tamaño de los archivos estáticos y conseguimos que la interfaz de usuario se renderizara correctamente.

4.2. CATALOGO DE COMPONENTES

El catalogo de componentes y plantillas es una herramienta de gestión de conocimiento que permite a los integrantes de un equipo compartir, reutilizar y colaborar en la creación de estándares para una mayor eficiencia en el desarrollo de modelos de IA. Los componentes son elementos que representan pequeñas funcionalidades dentro de un proyecto que pueden ser re-utilizados de una forma sencilla. Las plantillas por otro lado son estructuras más complejas que agrupan varios componentes, configuraciones y reglas de negocio para crear un modelo dentro de una temática específica por cada una de ellas. A todos estos elementos los hemos denominado bajo el nombre de STAC (Simple Tecnalia AI Components).

4.2.1. Adaptación del diseño atómico

La metodología de diseño atómico es una técnica que se basa en la creación de componentes que puedan ser reutilizados en diferentes partes de un proyecto. En el desarrollo de modelos de IA el posible adaptar esta técnica para crear componentes que representen funcionalidades específicas, como el preprocesamiento de datos, la selección de características, la evaluación de modelos, entre otros.

Como se ha mencionado anteriormente, los componentes se dividen a su vez en multitud de categorías (atómicos, moleculares, organismos, plantillas, etc.) esta división tiene sentido dentro de su concepción original pero, en el caso de los modelos de IA, la división de los componentes se puede hacer de una forma más sencilla, ya que en el caso de la investigación en IA, una abstracción más sencilla puede ser más útil para los investigadores. Es por ello que se propone una división de los componentes en tres categorías:

- **Componentes atómicos:** son los componentes más sencillos que representan una funcionalidad específica.
- **Componentes compuestos:** estos componentes agrupan varios componentes atómicos para realizar una funcionalidad más compleja.
- **Plantillas:** estructuras de proyectos completan que buscan solucionar un problema específico utilizando una técnica concreta. Están formadas a su vez por componentes compuestos y atómicos. Además, las plantillas también agrupan configuraciones, reglas de negocio y diversas integraciones con otros sistemas.

Todos los componentes y plantillas se almacenan en un repositorio compartido, donde los integrantes del equipo pueden colaborar en la creación de nuevos componentes y plantillas, así como en la mejora de los existentes.

4.2.2. Estructura del sistema de componentes

La arquitectura que se ha decidido implementar para el sistema de componentes es conocida como monorepo multi-paquete. Un monorepo es una práctica de desarrollo de software donde todos los proyectos relacionados se almacenan en un único repositorio de código fuente. Esto significa que en lugar de tener múltiples repositorios para cada uno de los componentes, todo se mantienen en un único lugar. Por otro lado, que sea multi-paquete significa que los diferentes elementos del monorepo se organizan mediante paquetes de software, lo que facilita su distribución de forma independiente. Este tipo de arquitectura cuenta con varias ventajas, entre las que se encuentran:

- **Facilidad de gestión:** Tener todo en un solo lugar simplifica la gestión del código, las dependencias y las versiones. No es necesario alternar entre diferentes repositorios para hacer cambios o resolver problemas.
- **Consistencia:** Todos los proyectos dentro del monorepo pueden seguir las mismas convenciones, estructura de carpetas, y configuraciones, lo que garantiza una mayor consistencia en el código. Esto permite que el código sea más fácil de mantener a largo plazo.

Uno de los principales problemas que puede surgir al utilizar un monorepo es la complejidad que puede acarrear la organización de las diferentes carpetas, ya que al tener todo en un solo lugar, la cantidad de archivos puede llegar a ser muy grande y contar con un nivel de anidamiento

muy profundo. Para evitar este problema, se ha decidido tomar una estructura de carpetas basada en *Screaming architecture*, una arquitectura de software que busca anteponer la lógica de negocio sobre las partes técnicas del sistema. En este caso, nuestra lógica de negocio se relaciona en torno a el problema que se busca resolver, es decir los diferentes conjuntos de problemas de las series temporales.

La figura 4.3 muestra un ejemplo simplificado de la estructura de carpetas del proyecto. Por cada uno de los diferentes problemas, se ha creado una carpeta principal, que a su vez contiene diferentes subcarpetas que agrupan los diferentes componentes dentro de cada una de las temáticas (procesamiento, modelo, métricas). En caso de que se necesite añadir un nuevo componente, simplemente se crea una nueva carpeta dentro de la temática correspondiente. Por ejemplo, tomando la temática preprocesamiento de datos dentro de clasificación, se buscaría la carpeta *Data-Processing* dentro *TimeSeries-Classification* y en caso de no existir, se crearía una nueva carpeta, y dentro de ella se añadiría el nuevo componente.

Lo que se consigue con este enfoque es que cada uno de los diferentes problemas cuente con una estructura similar pero que a su vez tengan la posibilidad de incluir temáticas propia. En la figura 4.3 se puede ver como cada uno de los problemas cuenta con componentes de procesamiento de datos, pero que a su vez, hay algunos de ellos que cuentan con componentes específicos de modelos o métricas. Esto se puede deber a que cada uno de los problemas tiene una necesidades específicas o que no se han encontrado componentes que se puedan reutilizar en este momento.

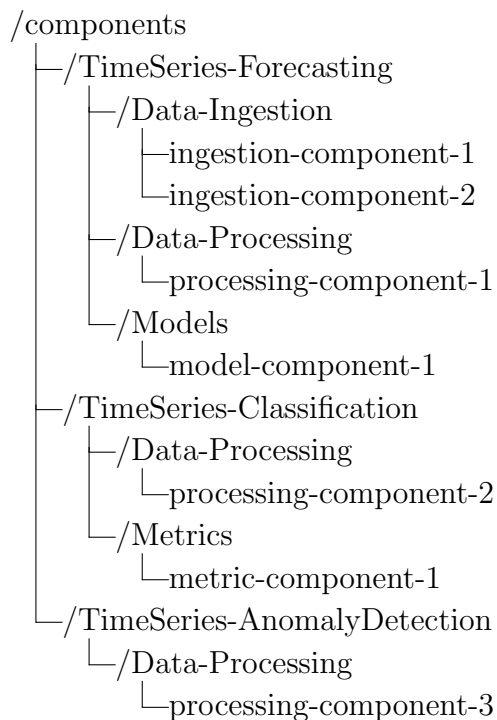


Figura 4.3: Ejemplo de estructura de carpetas basada en Screaming Architecture.

4.2.3. Empaquetado de componentes

La idea de los componentes es que sean fácilmente integrables en cualquier proyecto de una forma sencilla. Para ello, se ha decidido empaquetar cada componente de forma independiente y distribuirlos dentro de un repositorio privado, de forma que se puedan instalar utilizando pip o cualquier otro gestor de paquetes como poetry.

Dentro de nuestro caso de uso, queremos tener la posibilidad de instalar solo aquellos componentes que necesitemos en cada momento, sin tener que descargarnos todo el contenido del repositorio. Esto es especialmente importante ya que las dependencias de las librerías de IA pueden llegar a ser muy pesadas. A su vez, también se quiere que todos nuestros componentes hereden del mismo nombre de paquete, para que se puedan utilizar de una forma transparente a la hora de importarlos en un proyecto. Es decir, si tenemos por ejemplo un componentes de ingesta de datos llamado *get_data* y otro de visualización que imprime una gráfica llamado *show_graph*, la forma de importarlo en un proyecto sería la siguiente:

```
$ pip install stac-show-graph stac-get-data

>>> from stac.visualization.show_graph import show_graph
>>> from stac.data_ingestion.get_data import get_data
>>> data = get_data()
>>> show_graph(data)
```

Para conseguir este efecto es necesario comprender como funciona el empaquetado de librerías en Python. En Python, un paquete es una carpeta que contiene, por lo menos, un archivo *__init__.py* y un *pyproject.toml* o *setup.py*. La forma en la que se importan los paquetes es a través de un sistema de rutas por archivos, donde se toma la ruta hacia el paquete desde el directorio raíz del proyecto. En este caso, si queremos que todos nuestros componentes se importen desde *stac*, es necesario que el código de cada uno se encuentre dentro de una carpeta llamada *stac*, que a su vez contenga una carpeta con el nombre de la categoría del componente sin ningún *__init__.py* en su interior, ya que no queremos que se comporte como un paquete sino como una ruta. Dentro de esta, ya si se crear una carpeta con el nombre del componente y dentro de esta se añadirá el código del componente. En la figura 4.4 se puede ver como es el contenido de cada componente y la estructura de carpetas que se debe seguir.

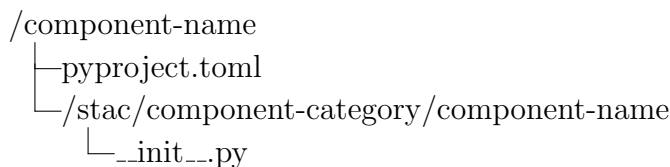


Figura 4.4: Estructura mínima de un componente empaquetado.

Esta estructura se tiene que repetir para cada uno de los componentes que se quieran añadir al repositorio. No obstante, y aprovechando que cada componente está separada en un proyecto independiente, se pueden añadir más utilidades como tests, documentación o ejemplos de uso. Como estamos utilizando poetry para gestionar las dependencias, y las configuraciones globales del proyecto, también se van a añadir sus archivos correspondientes.

Este empaquetado puede parecer tedioso si se tiene que hacer manualmente, pero en futuras secciones veremos como se puede automatizar este proceso para que sea lo más sencillo posible.

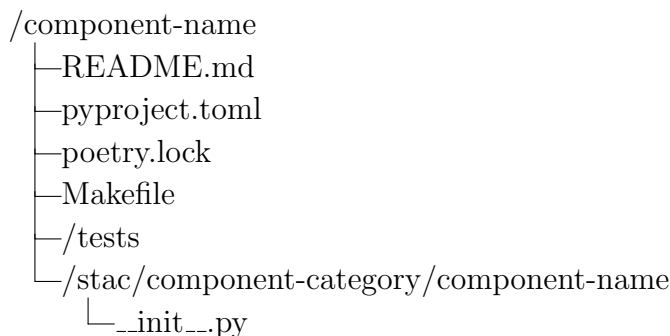


Figura 4.5: Estructura final de un componente empaquetado.

Es muy importante que la estructura sea la descrita para optimizar la experiencia de desarrollo de los integrantes del equipo.

4.2.4. Sistema de plantillas

La herramienta que hemos utilizado para la creación de plantillas es Cookiecutter. Cookiecutter es una utilidad para la generación de proyectos que te permite inicializar un proyecto a partir de plantillas predefinidas. Funciona siguiendo un principio básico: en lugar de empezar un nuevo proyecto desde cero y tener que configurar todo manualmente, puedes usar una plantilla predefinida que ya incluya la estructura de directorios, archivos básicos, configuraciones iniciales, y cualquier otro componente necesario para tu proyecto.

Esto es especialmente útil en entornos donde necesitas crear múltiples proyectos con una estructura similar donde puede haber proyectos con requisitos comunes, como la configuración de un marco de trabajo específico, estructura de directorios estándar, o incluso configuraciones de pruebas y documentación. Además, en nuestro caso son especialmente útiles ya que contamos con tres situaciones en las que tener una plantilla puede ser muy útil:

- **Creación de plantillas para problemas específicos:** este es el caso principal de el uso de plantillas. Cada una de las plantillas se crea para resolver un problema específico con una técnica concreta. Por ejemplo, una plantilla para clasificación de series temporales con redes neuronales recurrentes.
- **Creación de nuevos componentes:** en caso de que se quiera añadir un nuevo componente al repositorio, se puede utilizar una plantilla que contenga la estructura de carpetas y los archivos necesarios para empaquetar el componente. Como hemos mencionado anteriormente, esto puede ser especialmente engorroso si no se tiene una plantilla que te ayude a automatizar el proceso.
- **Creación de nuevas plantillas:** la estructura base de las plantillas al igual que los componentes es fácilmente reutilizable, ya que ciertos archivos de configuración o de documentación se pueden reutilizar en diferentes plantillas. Por lo que se pueden crear plantillas que contengan estos archivos y así automatizar el proceso de creación de nuevas plantillas.

La razón por la elección de Cookiecutter es por su facilidad de uso, ya que al utilizar el sistema de plantillas Jinja2, se pueden añadir variables a los archivos de la plantilla que se sustituirán por valores concretos al inicializar el proyecto. Este sistema de plantillas es muy

conocido especialmente ente los desarrolladores de Python, ya que es ampliamente utilizado por otros frameworks como Django. Además, Cookiecutter cuenta con una gran cantidad de plantillas predefinidas que se pueden utilizar de forma gratuita, lo que puede ser muy útil a la hora de incorporar las primeras plantillas al repositorio.

Estas plantillas se almacenan de la misma forma que podemos ver en la figura 4.3 pero sustituyendo los componentes por las plantillas. En principio, la estructura de las plantillas puede variar en gran medida entre ellas, ya que cada una de ella busca resolver un problema específico. No obstante, hay una serie de directrices obligatorias que se deben seguir para garantizar el correcto funcionamiento de las plantillas:

- **Automatización de instalación y lanzamiento:** todas las plantillas deben contar con un `makefile` que permita la instalación de las dependencias y el lanzamiento de la aplicación de forma sencilla. Por convención, el comando de instalación se llamará *make install* y el de lanzamiento *make train*. Es muy importante que estos comandos estén presentes en todas las plantillas para garantizar que con solo dos comandos y sin necesidad de consultar la documentación específica de cada plantilla se pueda poner en marcha el proyecto en concreto.

4.2.5. Integración continua y despliegue continuo

Dentro de equipos de trabajo donde hay un número elevado de integrantes, es importante no solo tener una buena organización del código, sino también contar con un sistema de CI/CD que asegure los diferentes procesos. En nuestro caso es especialmente crítico ya que los componentes son utilizados por diferentes personas en diferentes proyectos, por lo que un fallo en uno de los componentes puede afectar a un gran número de proyectos.

Para la implementación se ha utilizado GitLab CI, con una distribución de tres fases: *test*, *docs* y *deploy*. En la fase de *test* se ejecutan los test de cada uno de los componentes, en la fase de *docs* se extraen todos los archivos de documentación y se genera una pagina web estática con toda la documentación del proyecto, y en la fase de *deploy* hace una comprobación de que paquetes es necesario desplegar y en caso de que haya cambios, se despliegan las nuevas versiones de los paquetes, aclarar que se mantienen las versiones anteriores para evitar problemas de compatibilidad.

Estas fases se ejecutan en diferentes momentos, al estar la rama principal bloqueada por defecto, es necesario crear una rama con las nuevas funcionalidades y/o modificaciones y hacer una petición de merge a la rama principal. En este momento se ejecutan las fases de *test* y *docs*, para comprobar que no hay errores en el código y que la documentación se puede generar correctamente, aunque esta última no se despliega hasta que se haya aceptado la petición de merge. En caso de que se acepte la petición de merge, se ejecuta la fase de *deploy*. Existen usuarios que excepcionalmente pueden realizar modificaciones sobre la rama principal, pero solo en caso de que sea necesario y no como una práctica habitual.

4.3. DOCUMENTACIÓN DEL PROYECTO

La documentación juega un papel crucial en este proyecto, ya que proporciona una guía detallada sobre cómo utilizar los distintos componentes y plantillas disponibles. En este contexto, la adopción de Astro como herramienta para la generación de documentación automática se debe a su facilidad de uso, ya que permite crear paginas de forma sencilla utilizando Markdown, lo que facilita la creación de documentos por los distintos integrantes del equipo. Ya existen proyectos

que han utilizado Astro para la generación de documentación, como Microsoft con su proyecto Fluent UI [30] que utiliza Astro.

Concretamente, el proyecto usa Starlight, una plantilla de Astro que proporciona una estructura de documentación predefinida, lo que facilita la creación de documentación de forma rápida y sencilla. Además, Starlight incluye un sistema de búsqueda y organización de documentación, lo que facilita la navegación y búsqueda de información en la documentación. Otra de sus ventajas es la facilidad de customización, ya que permite modificar la apariencia utilizando CSS o Tailwind e incluso incorporar funcionalidades propias mediante JavaScript.

4.3.1. Guías y manuales

Para facilitar la integración de sistemas complejos como el aquí propuesto, es necesario proporcionar guías que expliquen de forma detallada cómo se debe interactuar con los diferentes procesos. En este sentido, la documentación del proyecto incluye un apartado de guías y manuales que proporciona esa información de forma detallada. Además, se incluyen ejemplos de uso y casos prácticos que ayudan a entender cómo se deben utilizar los distintos elementos de forma interactiva y dinámica.

En este momento, la documentación incluye las siguientes guías:

- **Guía de introducción:** proporciona una visión general del proyecto y que partes lo componen.
- **Guía de instalación:** explica cómo instalar las diferentes herramientas en local y conseguir acceso a los servicios.
- **Guía de plantillas y componentes:** proporciona información detallada sobre cómo utilizar los distintos componentes y plantillas disponibles.
- **Guía de ClearML:** introducción a la plataforma MLOps ClearML y cómo utilizarla en el proyecto.
- **Guía de contribución:** proporciona información sobre cómo contribuir al proyecto y cómo colaborar con otros miembros del equipo.

En el futuro, se espera ampliar la documentación con nuevas guías que no solo expliquen cómo utilizar los distintos elementos sino que también se centren en aspectos enfocados a la IA y el aprendizaje automático, como por ejemplo guías sobre cómo solucionar problemas relacionados con el día a día de la empresa.

4.3.2. Documentación de componentes y plantillas

Todos los componentes y plantillas que forman parte del proyecto cuentan con su propia documentación asociada a un archivo Readme.md. La razón de utilizar un archivo de tipo Markdown es que es un formato sencillo y fácil de escribir, lo que facilita la creación de documentación por parte de los distintos integrantes del equipo. Además, Astro lee de forma nativa archivos Markdown, lo que permite cargar las diferentes páginas sin necesidad de escribir código propio de una página web.

Aunque la documentación de los componentes y plantillas es bastante flexible y permite incluir secciones adicionales si fuera necesario, lo cierto es que por defecto incluye las siguientes secciones de forma automática:

- **Descripción:** proporciona una descripción general del componente o plantilla.
- **Instalación:** explica cómo instalar el componente o plantilla en un proyecto. Generalmente, se proporciona un único comando de consola que instala el componente o genera la estructura de archivos de la plantilla.
- **Uso:** proporciona información sobre cómo utilizar el componente o plantilla en un proyecto. Incluye ejemplos de uso.
- **Tags:** lista las etiquetas que se han utilizado para indexar en el sistema de búsqueda.

4.3.3. Sistema de búsqueda y organización de documentación

El poder encontrar información de forma rápida y sencilla es crucial en un proyecto de estas características, ya que la documentación puede llegar a crecer significativamente y ser difícil encontrar la información necesaria. Una de las ventajas de Astro con Starlight es que proporciona de forma automatizada un sistema de búsqueda que permite realizar búsquedas en base a palabras clave.

El sistema que utiliza por detrás se llama Pagefind, el cual es gratuito y de código abierto. Pagefind es un motor de búsqueda de documentos que entre sus características incluye no solo la búsqueda por palabras clave sino también el filtrado de resultados mediante etiquetas, se puede observar un ejemplo en la figura 4.6. Esta funcionalidad es clave y permiten encontrar la información de forma más precisa. Para poder indexar los documentos, Pagefind necesita que estos cuenten con unas etiquetas especiales que le permitan identificar que cierto documento pertenece a una categoría en concreto. En este sentido, ciertas páginas de la documentación cuenta con una sección llamada *Tags* en la que se incluyen las etiquetas correspondientes.

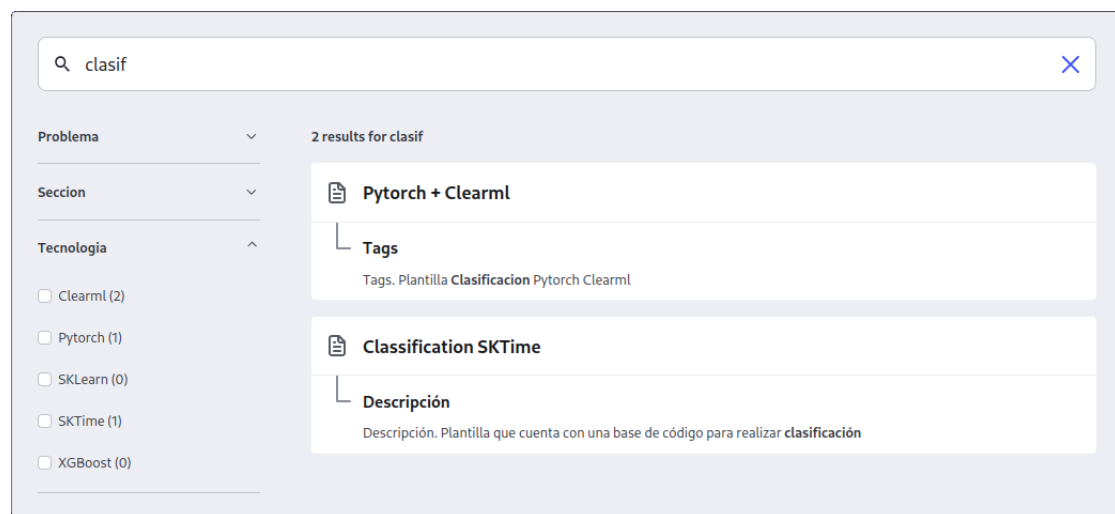


Figura 4.6: Sistema de búsqueda

Aunque de momento el sistema de búsqueda funciona correctamente, se espera en un futuro poder cambiar el motor que utiliza Astro por defecto a uno que permita búsquedas más enfocadas en la semántica de los documentos y no solo en base a palabras clave. Una alternativa que se

están considerando podría ser Algolia [31], un motor impulsado por IA muy popular dentro del mercado. El problema de Algolia es que es un servicio de pago, por lo que se debería estudiar si merece la pena ese coste adicional o si se existen alternativas gratuitas que ofrezcan un servicio similar y sean mejores que Pagefind.

4.3.4. Construcción automática de documentación

Como se ha mencionado anteriormente, cada componente y plantilla viene con su propia documentación, la cual se genera dentro de su respectiva carpeta mediante un archivo `Readme.md`. La decisión de que cada componente tenga su documentación en su propia carpeta es para facilitar la experiencia de desarrollo ya que todos los elementos de cada componente se encuentran en un mismo lugar y no es necesario buscar en diferentes carpetas para encontrar la información necesaria.

Esto pese a ser una ventaja, también genera un problema a la hora de generar la documentación, ya que es necesario un sistema que sea capaz de recorrer todas las carpetas, extraer los archivos `Readme.md` y `Readme.mdx` de cada una de ellas y generar la respectiva página de documentación. Para solucionar este problema, se ha creado un script de bash que recorre las carpetas que contienen componentes o plantillas y copia estos archivos en una carpeta con el nombre de su carpeta original con el fin de evitar problemas de colisiones entre los nombres de los diferentes archivos. Una vez hecho esto, se ejecuta el comando `astro build` y se sube la documentación a la plataforma de GitLab Pages.

5. ESTANDARIZACIÓN DE PROCESOS DE TRABAJO

Esta sección describe los procesos de trabajo que se han identificado y como se han estandarizado. Se describen los tres procesos principales que se han identificado dentro del proyecto: integración de una integrante en el flujo de trabajo, desarrollo de un proyecto desde cero y contribución al sistema de conocimiento.

5.1. INTEGRACIÓN EN EL FLUJO DE TRABAJO

La integración de nuevas personas a un grupo de trabajo es fundamental dentro de una empresa. Cuando se añaden nuevos miembros, es natural que surja cierta fricción debido a diversos factores, como la adaptación a la dinámica del equipo, la comprensión de los procesos establecidos y la familiarización con las herramientas y tecnologías utilizadas. Esta fricción puede ralentizar el progreso del equipo.

Una forma efectiva de mejorar esta cuestión es mediante la automatización de procesos, como la instalación y configuración de herramientas y software necesarios para el trabajo del equipo. Al utilizar un script que realiza estas tareas de forma automática, se eliminan los posibles errores humanos y se agiliza el proceso de integración de los nuevos miembros. Además, al estandarizar la configuración, se garantiza que todos los miembros del equipo tengan el mismo entorno de trabajo, lo que facilita la compatibilidad. Otro beneficio es que este script puede ser también utilizado por miembros actuales del equipo para actualizar su entorno de trabajo actual a las últimas versiones de las herramientas y software utilizados.

5.1.1. Proceso de integración

Cuando se incorpora un nuevo miembro al equipo, existe una hoja de ruta que está definida para que este se acomode lo más rápido posible a la forma de trabajar del equipo. A continuación se describen los pasos que se siguen para la integración de un nuevo miembro al equipo:

1. **Pre-requisitos:** antes de comenzar con la integración, es necesario que el nuevo miembro tenga a su disposición el ordenador de trabajo con las credenciales de acceso a su cuenta de usuario y al servicio de verificación en dos pasos.
2. **Instalación de herramientas:** el nuevo miembro deberá ejecutar el script de instalación de herramientas que se encuentra disponible en la propia guía de *Instalación de herramientas*. Este script se encargará de instalar todas las herramientas necesarias para el desarrollo de proyectos, aunque por razones de seguridad, no se automatizará la creación de ninguna credencial para servicios de terceros. Para consultar que herramientas se instalan se pueden ver dentro de la sección *Herramientas de desarrollo*.
3. **Configuración de autenticación:** aunque las configuraciones básicas de las herramientas se han automatizado, es necesario que el nuevo miembro configure ciertas credenciales de acceso como la clave ssh de Git-Lab, el token de acceso para ClearML y cualquiera otra credencial que sea necesaria para el desarrollo de proyectos.
4. **Formación:** una vez que el nuevo miembro ha instalado las herramientas y configurado las credenciales, se le proporciona una formación básica sobre el uso de dichas herramientas y sobre como implementarlas en su flujo de trabajo.

Con estas directrices, se garantiza que el nuevo miembro pueda comenzar a trabajar en el menor tiempo posible sin requerir de una ayuda constante por parte de los miembros actuales del

equipo. Una vez terminada la formación, el nuevo miembro debe haber adquirido las siguientes competencias: uso del sistema de plantillas y componentes, conocimiento básico de las herramientas de desarrollo, conocimiento básico de la infraestructura, conocimiento sobre como contribuir en proyectos y en el sistema de conocimiento.

5.1.2. Herramientas de desarrollo

A continuación se describen las herramientas que se encuentran dentro del marco de trabajo del equipo:

- **Python3.11:** se ha elegido la versión 3.11 de Python como versión principal para el desarrollo de proyectos. La 3.11 ha traído mejoras significativas en cuanto a rendimiento y nuevas funcionalidades sobre la librería estándar como el módulo *tomlib* que facilita la lectura de los toml. Esta versión de python es el paquete del repositorio de DeadSnakes, no se utiliza conda ya que requiere de una licencia para su uso y no trae ventajas frente a la base.
- **Docker:** debido a que en la actualidad muchos proyectos han de funcionar dentro de contenedores, se ha decidido incluir Docker como una de las herramientas por dos razones, dar soporte a la virtualización de ciertos proyectos y facilitar su instalación que puede llegar a ser complicada si no se tiene experiencia previa.
- **Pipx:** es una herramienta que permite instalar otras herramientas de consola de python de forma aislada, evitando así conflictos entre las distintas versiones de las librerías.
- **Poetry:** es un gestor de dependencias y empaquetador de proyectos de python. Se ha incorporado ya que el desarrollo de componentes requiere de una forma sencilla de publicar y gestionar las dependencias de cada proyecto. Existe también alternativas como Pipenv, pero se ha preferido Poetry por que permite gestionar repositorios privados de una forma mas sencilla.
- **Cookiecutter:** es una herramienta que permite la creación de proyectos a partir de plantillas predefinidas.
- **Ruff:** es una herramienta que se encarga de corregir los errores de estilo y formatear el código fuente. Se ha elegido Ruff por encima de otras herramientas como Black o Flake8 debido a que Ruff ya combina las funcionalidades de ambas herramientas. Además, al estar escrita en rust es mucho más rápida que las otras herramientas. Se puede ver en la figura 5.1 una comparativa de rendimiento [32] sobre el repositorio de CPython.

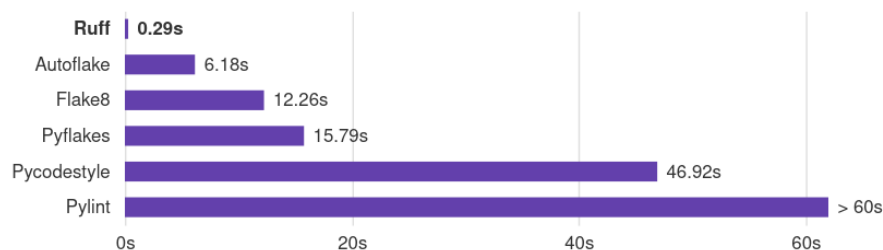


Figura 5.1: Comparativa de rendimiento sobre el repositorio de CPython

- **Visual Studio Code:** VSCode es el editor de código mayoritariamente utilizado en el mercado tecnológico. Su integración con Python y Docker, así como su facilidad de uso y la gran cantidad de extensiones disponibles, lo convierten en una herramienta ideal para el desarrollo de proyectos. Se ha elegido VSCode por encima de otras herramientas como PyCharm debido a que es más ligero y a diferencia de PyCharm, no requiere de una licencia para su uso.

5.2. DESARROLLO DENTRO DE PROYECTOS

Una vez que un nuevo miembro ha superado el periodo de integración, ya está listo para comenzar a trabajar en proyectos. En esta subsección se describen los procesos que se siguen para el desarrollo de un proyecto desde cero, así como las directrices generales para garantizar la calidad y la reproducibilidad del mismo. Para garantizar que esta metodología es funcional y de verdad aporta una mejora en la se han realizado dos proyectos para cada una de las áreas de trabajo de las series temporales, *forecasting* y *clasificación y detección de anomalías*. Por último, se ha hecho una plantilla adicional de automl para utilizar una serie de componentes dentro de un proyecto de *forecasting*.

5.2.1. Flujo de trabajo

El flujo de trabajo que se sigue para el desarrollo de un proyecto es el siguiente:

1. **Creación del proyecto:** para comenzar un proyecto, el investigador deberá revisar dentro de la documentación del equipo si existe alguna plantilla que se ajuste a sus necesidades y, en caso de que esta se adapte a lo que busca, podrá crear un nuevo proyecto a partir de esta plantilla. En caso de que no exista una plantilla que especifique para ese caso de uso, se da la alternativa de utilizar una plantilla de otro caso de uso ya que puede ser que ciertas configuraciones específicas de librerías le sean de utilidad para no partir de cero. Si no se cumplen ninguno de los dos casos anteriores, se presenta una plantilla genérica que se puede utilizar para cualquier proyecto. En casos excepcionales, se puede crear un proyecto desde cero pero debe seguir los estándares de calidad definidos en su respectiva sección y ser perfectamente reproducible.
2. **Control de versiones:** una vez que el proyecto ha sido creado, el investigador deberá subir el proyecto a un repositorio de control de versiones, en este caso se utiliza Git-Lab. El siguiente paso es utilizar las funciones de ClearML para versionar los datasets que se requieran para el desarrollo del proyecto. No existe una imposición sobre como gestionar las ramas de git, cada investigador puede decidir como adaptarlo dependiendo del proyecto, equipo o el número de integrantes. Las directrices generales son la utilización de la rama *main* para versiones estables del modelo, es decir un entrenamiento e inferencia funcional, y la rama *dev* para versiones en desarrollo.
3. **Desarrollo y experimentación:** para garantizar el buen desarrollo del proyecto, se recomienda mantener el histórico de resultados de los experimentos que se realicen en el proyecto. Por defecto, el proyecto ya viene configurado para que se guarden los resultados de los experimentos en ClearML, a si que se recomienda eliminar aquellos que hayan fallado o que sean irrelevantes con el objetivo de poder lanzar nuevamente esos experimentos en un futuro. Se recomienda seguir las indicaciones de los *linters* y *formatters* que se han configurado para garantizar la consistencia y claridad del código, aunque se puede desactivar para casos específicos como es el caso de errores de tipado. El uso del catálogo de componentes es opcional, pero es de gran utilidad para agilizar ciertas tareas repetitivas.

4. **Aportación al sistema de conocimiento:** una vez que el proyecto ha sido finalizado, se recomienda aportar al sistema de conocimiento del equipo para que otros miembros puedan beneficiarse del nuevo conocimiento. Si no existía una plantilla específica para ese caso de uso, lo ideal es crear una nueva plantilla para esa especificación ya que es mucho más sencillo y requiere menos esfuerzo que crear un componente. En caso de que ya hayamos usado una plantilla, también se podrá crear otra si la solución que se ha encontrado es significativamente diferente a la original. Por último, si no se cumplen ninguno de los dos casos anteriores, y hay funcionalidades que se pueden reutilizar en otros proyectos sería recomendable crear un componente.

5.2.2. Puesta en practica de la metodología

En este apartado se describe la experiencia de desarrollo de los proyectos de *forecasting* y *clasificación y detección de anomalías*. Esta sección no pretende centrarse en los resultados obtenidos por parte de los modelos, sino más bien llevar a cabo una reflexión sobre la aplicabilidad del marco de trabajo dentro de diferentes tipos de proyectos. Los datasets utilizados se eligieron siguiendo el criterio de pertenecer a la sección de “Industria y movilidad”, correspondiente al área de trabajo donde se quiere aplicar dicho marco, y de estar relacionados con el campo de las series temporales. Estos proyectos se han basado en datasets extraídos de la plataforma Kaggle, ya que es una plataforma que ofrece una gran variedad de datasets que no requieren un registro previo para su descarga.

Para considerar un proyecto como terminado, se requiere que el modelo sea capaz de realizar inferencias sobre nuevos datos con cierta precisión. Además, se espera que pueda generar gráficos que muestren los resultados de manera clara y comprensible. Otro de los requisitos es que las métricas de entrenamiento y evaluación sean almacenadas en ClearML, así como los modelos entrenados. Por último, se espera un ligero análisis de los parámetros con su gráfico resultante. Una vez que estas condiciones se cumplan, se considera que el proyecto está completo y listo para su evaluación. La evaluación de los proyectos se compone de dos factores, el tiempo dedicado a la realización del proyecto y el porcentaje de código que ha sido reutilizado de otros proyectos.

5.2.3. Proyectos de forecasting

Los proyectos de forecasting se basan en la predicción de una variable a lo largo del tiempo. Implica el análisis de datos históricos para identificar patrones y tendencias que ayuden a predecir el comportamiento futuro. Este tipo de proyectos pueden abordar preguntas como la demanda futura de productos, la evolución de la demanda en un mercado, entre otros aspectos. El objetivo principal es proporcionar información útil para la toma de decisiones, permitiendo a las organizaciones anticiparse a cambios y optimizar recursos.

A continuación, se detallan las características de los siguientes proyectos:

- **Proyecto 1:** en este proyecto nuestro objetivo es predecir la temperatura para un día específico dentro de una zona determinada. El nombre del dataset es *Daily Climate Temperature Data* [33]. Este dataset contiene información sobre la temperatura de la ciudad de Delhi, India desde 2013 hasta 2017. El dataset cuenta con variables como temperatura media, la humedad, la velocidad del viento, entre otras. La calidad de los datos es buena, no hay valores nulos y las variables están en un formato adecuado para su uso.
- **Proyecto 2:** en el segundo proyecto, el objetivo es predecir el consumo de energía eléctrica en una zona determinada. El nombre del dataset es *Hourly Energy Consumption* [34]. Este dataset contiene información sobre el consumo de energía eléctrica en la ciudad de Nueva

York desde 2002 hasta 2018. El dataset cuenta exclusivamente con la fecha y la cantidad de energía consumida, por lo que es ligeramente más sencillo que el anterior.

Para el primer proyecto, no se disponía de ninguna plantilla específica, por lo que se decidió comenzar el desarrollo desde cero. Con la intención de reutilizar el máximo número de código en futuros proyectos, se ha planteado el desarrollo desde un punto de vista modular, donde cada funcionalidad esta separada en un archivo diferente. Todas estas funcionalidades se importan y utilizan en el archivo de entrenamiento principal llamado *train.py*. Entre las funcionalidades que se han desarrollado podemos encontrar diferentes tipos: procesamiento, visualización, métricas, etc. A continuación, se detallan mas concretamente cada una de ellas:

- **add_time_features (Procesamiento):** esta funcionalidad se encarga de añadir características temporales a un DataFrame de Pandas. A partir de la fecha se calcula el día de la semana, el mes, el año, la estación, entre otras.
- **mean_abs_percentage_error (Métrica):** calcula el error porcentual medio absoluto entre dos valores. Utilizada para evaluar el rendimiento del modelo y al no ser una métrica nativa de Sklearn, se ha tenido que implementar.
- **compare_time_series (Visualización):** recibe un DataFrame con n columnas, una para cada serie temporal, y crea una gráfica comparativa de todas ellas. También se puede especificar un rango de fechas para visualizar solo un periodo concreto.
- **show_feature_importance (Visualización):** Recibe un array de importancia de características y un array con los nombres de las características. Crea un gráfico de barras con la importancia de cada característica.

Con estos funcionalidades y utilizando algunas propias de sklearn, como el split de los datos y XGBoost como modelo, se ha conseguido un modelo que es capaz de predecir la temperatura con un error medio absoluto porcentual del 9.5 %. Este proyecto ha tenido una duración aproximada de 3 horas y media. Una vez finalizado, se ha realizado una plantilla basada en este proyecto para futuros proyectos de forecasting donde se necesite xgboost como modelo. Esta plantilla asi como los componentes relacionados se detalla más adelante en la sección de *contribución al sistema de conocimiento*.

Para el segundo proyecto, se ha utilizado la plantilla de forecasting creada a partir del primer proyecto. Las modificaciones realizadas han sido mínimas, ya que el proyecto es muy similar al anterior. Se ha cambiado la lectura de datos para adaptarla al nuevo dataset y se han implementado algunas funcionalidades adicionales para la extracción de características ya que el dataset no cuenta con muchos datos relevantes. Antes de comenzar con la implementación de características, utilizando la funcionalidad *add_time_features*, el modelo a obtenido un error medio absoluto porcentual del 15.5 %. Tras la implementación de nuevas características que se pueden ver a continuación, el error ha disminuido hasta el 11.5 %:

- **add_lags (Procesamiento):** añade valores pasados de una serie temporal como características adicionales llamados lags. Se puede especificar el número de lags y el periodo de tiempo que se quiere utilizar.
- **add_holidays (Procesamiento):** añade una columna al DataFrame que indica si el día es festivo o no. Esta función recibe un calendario con los días festivos y crear una columna con valores booleanos. Para este proyecto se ha utilizado el calendario de festivos de Nueva York.

Este proyecto ha tenido una duración aproximada de 1 hora y 40 minutos. Una vez finalizado, se ha actualizado la plantilla de forecasting con nuevas funcionalidades y extraído cierta lógica de la plantilla a componentes para facilitar la reutilización de código. Hemos visto una mejora en cuanto a la velocidad de desarrollo ya que el tiempo desde la creación del proyecto hasta la finalización ha sido reducido a menos de la mitad.

5.2.4. Proyectos de clasificación

Un proyecto de clasificación de series temporales implica el desarrollo de modelos para categorizar o etiquetar datos temporales en diferentes categorías. La clasificación de series temporales implica generalmente la extracción de características relevantes de las series temporales y el objetivo es identificar y asignar correctamente una etiqueta a cada serie temporal.

Para los proyecto de clasificación contamos con la siguiente temáticas.

- **Proyecto 1:** clasificación de la estación en del año en base al consumo de energía eléctrica. Se ha utilizado el dataset *Daily Energy Consumption* [34] al igual que en el proyecto de forecasting. De por si este dataset no cuenta con la variable estación, por lo que parte de la tarea es la de identificar la estación en base a la fecha.

- **Proyecto 2:**

Siguiendo la misma metodología que en los proyectos de forecasting, se ha comenzado el desarrollo del primer proyecto pero esta vez partiendo de la plantilla de forecasting, ya que viene configurada con todas las utilidades necesarias y solo se necesita cambiar aspectos puntuales para adaptarla a un problema de clasificación. Como ya hemos mencionado en la descripción del proyecto, nuestro dataset no cuenta con la variable estación, por lo que tendremos que añadirla, agruparlas en ventanas temporales y hacer las respectivas modificaciones para que pueda ser interpretado por el modelo.

A continuación, se detallan la lista de modificaciones y funcionalidades que se han llevado a cabo:

- **add_time_features (Procesamiento):** añade una nueva funcionalidad que consiste en una aportar de una columna adicional al DataFrame que indica la estación en la que se encuentra una fecha en concreto. Esta se representa con un número entero que va del 0 al 3, siendo 0 invierno, 1 primavera, 2 verano y 3 otoño.
- **get_window (Procesamiento):** realiza una agrupación de los datos en ventanas temporales. Se puede especificar el tamaño de la ventana y el periodo de tiempo que se quiere utilizar. En este caso, se ha agrupado los datos en ventanas de 10 días.
- **cross_validation (Métrica):** realiza una validación cruzada de los datos para evaluar el rendimiento del modelo. Se puede especificar el número de splits y el tamaño de los splits.
- **display_roc_curve (Visualización):** recibe un array con las etiquetas reales y otro con las predicciones del modelo. Crea una curva ROC que muestra la relación entre la tasa de verdaderos positivos y la tasa de falsos positivos. Este gráfico sirve para las diferentes clases de un modelo de clasificación.
- **modificación del modelo:** se ha cambiado el modelo de xgboost regressor a un modelo de clasificación, en concreto se ha utilizado un xgboost classifier.
- **modificación de la métrica:** se ha cambiado la métrica de error medio absoluto porcentual por la de precisión.

5.2.5. Proyectos de detección de anomalías

Un proyecto de detección de anomalías se enfoca en identificar patrones inusuales o atípicos en datos temporales. Estas anomalías pueden indicar problemas, riesgos o eventos inesperados en sistemas. La detección de anomalías es crucial en campos como la seguridad informática, el mantenimiento predictivo, la detección de fraudes, entre otros. Los proyectos de detección de anomalías implican la exploración y modelado de datos históricos para comprender los patrones normales e identificar desviaciones significativas de esos patrones.

Podemos encontrar los siguientes proyectos de detección de anomalías:

- **Proyecto 1:** detección de anomalías en el tráfico de coches en una ciudad.
- **Proyecto 2:**

5.2.6. Proyectos de automl

AutoML, o aprendizaje automático automático, es un enfoque que utiliza algoritmos para automatizar el proceso de selección, entrenamiento y ajuste de modelos de machine learning. Con la intención de mejorar el rendimiento de los modelos y explorar que tan útil puede ser esta herramienta en el desarrollo de proyectos de series temporales, vamos a reutilizar el dataset del proyecto 1 de forecasting para realizar una plantilla de automl enfocada en el forecasting.

El AutoML se encarga de probar una variedad de modelos y configuraciones para encontrar la combinación óptima que maximice la precisión de nuestras predicciones, lo que potencialmente nos permitirá obtener resultados más precisos y robustos en comparación con nuestro modelo inicial. La idea es crear una plantilla que reutilice el contenido previo y con la mínima intervención del usuario, sea capaz de probar diferentes modelos de forecasting de manera automática.

La arquitectura de la plantilla en AutoML se basa en la utilización del patrón de diseño de estrategia. Este patrón de diseño permite definir una familia de algoritmos, encapsular cada uno de ellos y hacerlos intercambiables. En este caso, estos algoritmos recibirán la lista de modelos con sus diferentes hiperparámetros y los resultados de las iteraciones anteriores. Gracias a esto, las diferentes estrategias podrán realizar la búsqueda de una manera inteligente. La plantilla base es muy simple y cuenta con dos estrategias y siete modelos pero la idea es que en un futuro pueda ser ampliada.

La lista de modelos que esta plantilla soporta es la siguiente: *LinearRegression*, *DecisionTreeRegressor*, *RandomForestRegressor*, *XGBRegressor*, *LGBMRegressor*, *CatBoostRegressor* y *Neural Network*. Por otro lado, las estrategias que se han implementado son las siguientes:

- **Prueba de la lista de modelos:** para garantizar que la lista de modelos y sus correspondientes sets de hiperparámetros sean válidos, se realiza una primera pasada de todos los modelos con los hiperparámetros por defecto. Esta serie de hiperparámetros por defecto se han seleccionado de manera que sean los que mejor se suelen ajustar a la mayoría de los casos. Cada modelo tiene una lista diferente de hiperparámetros.
- **Optimización mediante Optuna:** una vez que se ha probado todos los modelos con los hiperparámetros por defecto, se seleccionan los tres mejores modelos de esa lista de resultados y se realiza una optimización de hiperparámetros mediante Optuna. Optuna es una librería de optimización de hiperparámetros que se encarga de encontrar la combinación de hiperparámetros que maximiza una métrica dada. En nuestro caso, la métrica que se utiliza es el error medio absoluto porcentual.

PROYECTO FIN DE MASTER

Después de lanzar este proceso sobre el dataset de forecasting, se ha obtenido un error medio absoluto porcentual del 8.3% con el modelo XGBRegressor. Esta proceso ha tenido una duración aproximada de 1 hora y 20 minutos y ha supuesto una mejora de 1.2 puntos porcentuales en comparación con el modelo base.

5.3. CONTRIBUCIÓN AL SISTEMA DE CONOCIMIENTO

6. PLANIFICACIÓN Y PRESUPUESTO

En esta sección se detallará la organización y planificación del proyecto, así como el presupuesto necesario para llevarlo a cabo. Se utilizarán diagramas para facilitar la comprensión de los diferentes aspectos del proyecto.

6.1. PLAN DE RECURSOS HUMANOS

Uno de los activos más vitales en cualquier proyecto es el equipo humano. En este plan, se detallan las funciones y responsabilidades de cada miembro del equipo, con el fin de fomentar una colaboración efectiva y alcanzar los objetivos del proyecto. Entre los perfiles involucrados en el proyecto se encuentran el director del proyecto, el director Tecnalia y el estudiante.

1. Director del proyecto

- Descripción: El director del proyecto es a efectos prácticos el encargado de supervisar que el proyecto siga la normativa de la universidad y la memoria sea correcta. Este perfil es ocupado por el tutor universitario asignado al proyecto.
- Responsabilidades:
 - Supervisar que el proyecto cumpla con las normativas de la universidad.
 - Validación del proyecto y trabajo del alumno.
 - Supervisar las actividades del proyecto.
 - Revisar y asegurar la corrección de la memoria del proyecto.
 - Ayudar a que se cumplen los plazos establecidos por la universidad.
 - Aportar orientación académica al estudiante.
- Disponibilidad:
 - Disponibilidad para realizar reuniones semanales de seguimiento.
 - Disponibilidad para resolver dudas via correo electrónico.

2. Director Tecnalia

- Descripción: El director Tecnalia es el encargado de supervisar que el proyecto se alinee con las necesidades de la empresa y aportar su experiencia en el desarrollo de sistemas de IA. En este perfil se incluyen dos directores, uno de ellos enfocado en el desarrollo del sistema y otro en la parte de pruebas y validación.
- Responsabilidades:
 - Recolección de requisitos y definición de objetivos.
 - Asegurar que el desarrollo del proyecto se alinee con las necesidades de la empresa.
 - Proporcionar apoyo en la investigación.
 - Supervisar las actividades del proyecto.
 - Ofrecer feedback constante sobre el desarrollo del proyecto.
 - Ayudar al estudiante proporcionándole recursos para las pruebas del sistema.
- Disponibilidad:
 - Horario laboral estándar, con flexibilidad para reuniones con el estudiante.
 - Disponibilidad para resolver dudas via correo electrónico.

3. Estudiante

- Descripción: El director del proyecto es a efectos prácticos el encargado de supervisar que el proyecto siga la normativa de la universidad y la memoria sea correcta. Este perfil es ocupado por el tutor universitario asignado al proyecto.
- Responsabilidades:
 - Desarrollar el proyecto bajo la orientación de los tutores.
 - Redactar la memoria del proyecto.
 - Realizar pruebas del sistema.
 - Presentar avances periódicos al equipo de tutores.
- Disponibilidad:
 - Horario laboral estándar, con flexibilidad para reuniones con el estudiante.

6.2. PROGRAMA DE TRABAJO

La siguiente sección detallará el plan de trabajo seguido en el proyecto, incluyendo las diferentes tareas generales realizadas con su duración planificada y real, junto con el diagrama de Gantt del proyecto. Las tareas del proyecto se han dividido en tres fases distintas. La primera fase incluye las tareas necesarias para el desarrollo del MVP del proyecto, que incluye la creación de un sistema funcional y su respectiva presentación al equipo de trabajo. La segunda fase incluye la implementación de las diferentes plataformas y automatizaciones necesarias para garantizar la seguridad y escalabilidad del sistema. La tercera fase se basa en probar el sistema con diferentes problemas de series temporales y recaudar información sobre los resultados, contenido relevante para el sistema de conocimiento y la documentación final del proyecto.

6.2.1. Fase 1: Desarrollo del MVP

Esta fase está formada por una serie de tareas que se deben completar para la creación del producto mínimo viable. Las tareas incluidas en esta fase son aquellas indispensable para realizar una prueba de concepto y valorar la viabilidad técnica del proyecto. Las tareas incluidas en esta fase son las siguientes:

- **Tarea 1.1:** Investigación inicial sobre el estado del arte, tecnologías y herramientas necesarias para el proyecto.
- **Tarea 1.2:** Definición del alcance del MVP y la hoja de ruta para su desarrollo.
- **Tarea 1.3:** Definición del plan de trabajo y el como debe ser utilizada la herramienta.
- **Tarea 1.4:** Desarrollo del sistema de componentes y plantillas.
- **Tarea 1.5:** Despliegue básico de ClearMl y configuración de
- **Tarea 1.6:** Implantación de empaquetado automático de los paquetes y subida a un repositorio de artefactos. los experimentos.
- **Tarea 1.7:** Presentación del MVP y validación de la viabilidad.

6.2.2. Fase 2: Integración de nuevas plataformas, securización y despliegue

Esta fase está formada por una serie de tareas que incluyen la implementación de las diferentes partes del proyecto. Las tareas incluidas en esta fase son las siguientes:

- **Tarea 2.1:** Integración de nuevas plataformas para la visualización de los experimentos.
- **Tarea 2.2:** Securitización de la infraestructura utilizando un proxy inverso con Nginx y Keycloak.
- **Tarea 2.3:** Despliegue de la infraestructura de forma automática utilizando GitLab CI/CD.
- **Tarea 2.4:** Automatización de la creación de componentes y plantillas proporcionando una plantilla base para cada caso.
- **Tarea 2.5:** Creación de la documentación técnica y de usuario.
- **Tarea 2.6:** Lanzamiento de pruebas unitarias de los componentes.

6.2.3. Fase 3: Experimentación, pruebas y documentación

El último bloque de tareas incluye la experimentación, el análisis de los resultados obtenidos y la documentación final del proyecto. Esta última es fundamental debido a que el proyecto se desarrolla en un entorno de investigación y es necesario documentar todo el procedimiento para que puede ser aplicado por otros investigadores. Las tareas incluidas en esta fase son las siguientes:

- **Tarea 3.1:** Prueba del sistema para un problema de forecasting.
- **Tarea 3.2:** Prueba del sistema para un problema de clasificación.
- **Tarea 3.3:** Prueba del sistema para un problema de detección de anomalías.
- **Tarea 3.4:** Implantación del sistema en el entorno de trabajo del equipo.
- **Tarea 3.5:** Encuesta de satisfacción y feedback de los resultados.
- **Tarea 3.6:** Redacción de la memoria del proyecto.

6.2.4. Diagrama de Gantt

A continuación se muestra el diagrama de Gantt del proyecto, donde se puede observar la planificación temporal de las diferentes tareas descritas anteriormente. El proyecto al estar dividido en tres fases se ha utilizado el color azul para representar la fase 1, el color verde para la fase 2 y el color morado para la fase 3. Se ha respetado cuidadosamente el tiempo de cada tarea y el proyecto no ha sufrido ningún retraso durante su desarrollo.

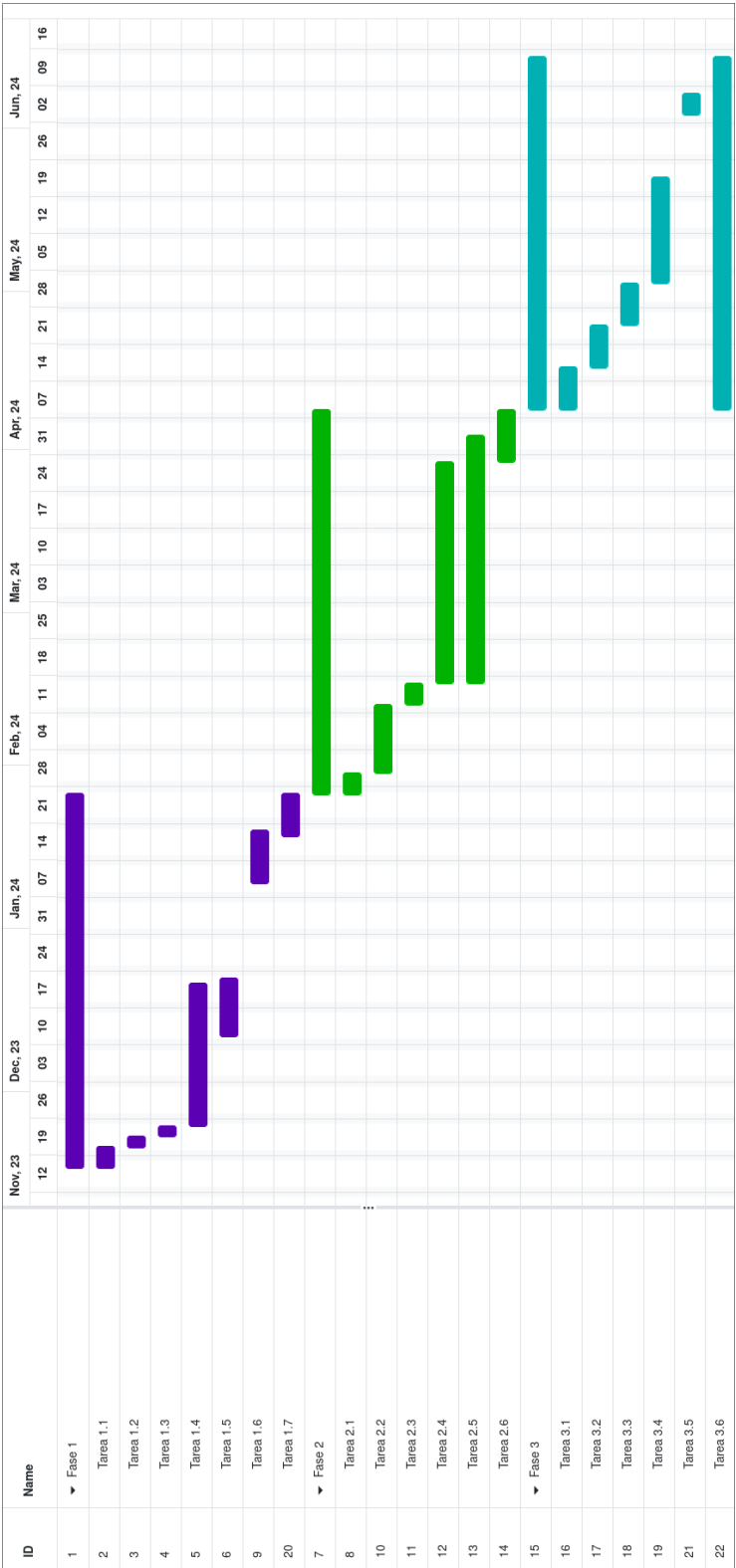


Figura 6.1: Diagrama de planificación del proyecto.

6.3. TABLA DE TAREAS

Fase/Tarea	Fecha inicio	Fecha fin	Duración
Fase 1	Noviembre 22, 2023	Enero 26, 2024	52 días
T1.1	Noviembre 22, 2023	Noviembre 24, 2023	03 días
T1.2	Noviembre 24, 2023	Diciembre 21, 2023	20 días
T1.3	Diciembre 11, 2023	Diciembre 22, 2023	10 días
T1.4	Enero 09, 2024	Enero 19, 2024	09 días
T1.5	Enero 18, 2024	Enero 26, 2024	07 días
Fase 2	Enero 26, 2024	Abril 08, 2024	52 días
T2.1	Enero 26, 2024	Enero 30, 2024	03 días
T2.2	Enero 30, 2024	Febrero 12, 2024	10 días
T2.3	Febrero 12, 2024	Febrero 16, 2024	05 días
T2.4	Febrero 16, 2024	Marzo 29, 2024	31 días
T2.5	Febrero 16, 2024	Abril 03, 2024	34 días
T2.6	Marzo 29, 2024	Abril 08, 2024	07 días
Fase 3	Abril 08, 2024	Junio 14, 2024	50 días
T3.1	Abril 08, 2024	Abril 16, 2024	07 días
T3.2	Abril 16, 2024	Abril 24, 2024	07 días
T3.3	Abril 24, 2024	Mayo 02, 2024	07 días
T3.4	Mayo 02, 2024	Mayo 22, 2024	15 días
T3.5	Junio 03, 2024	Junio 07, 2024	05 días
T3.6	Abril 08, 2024	Junio 14, 2024	45 días

Cuadro 6.1: Resumen de las tareas y fases

6.4. PRESUPUESTO

La siguiente sección detallará el presupuesto necesario para llevar a cabo el proyecto, incluyendo los diferentes recursos necesarios y su coste. El presupuesto se ha dividido en tres categorías principales: recursos humanos, hardware y software.

6.4.1. Recursos humanos

La siguiente tabla muestra el coste de los diferentes perfiles involucrados en el proyecto, así como el número de horas invertidas por cada uno de ellos y el coste total de cada perfil.

Perfil	Coste/Hora	Horas Invertidas	Precio Total
Director del proyecto	40€	20h	800€
Director Tecnalia 1	90€	60h	5.400€
Director Tecnalia 2	90€	20h	1.800€
Estudiante	6.5€	540h	3.500€
Total	17.95€	640h	11.500€

Cuadro 6.2: Presupuesto de recursos humanos

6.4.2. Hardware

La siguiente tabla muestra el coste de los diferentes recursos hardware necesarios para llevar a cabo el proyecto, así como el número de unidades necesarias y el coste total de cada recurso.

Recurso	Coste por unidad	Unidades	Precio Total
Hora máquina virtual	0.2€	200u	40€
Portátil	700€	1u	700€

Cuadro 6.3: Presupuesto hardware

6.4.3. Software

Los recursos software necesarios para llevar a cabo el proyecto son gratuitos en su mayoría, a excepción de la licencia de GitHub Copilot que tiene un coste de 10€/mes. Aun así, se ha utilizado la versión gratuita que viene incluida con la licencia de GitHub Pro por ser estudiante.

6.4.4. Total

Recurso	Precio Total
Recursos humanos	14.000€
Hardware	740€
Software	0€
Total	14.740€

Cuadro 6.4: Presupuesto general

7. CONSIDERACIONES ÉTICAS

La implementación de nuevas tecnologías y paradigmas, como es el caso de MLOps, no solo transforma las prácticas técnicas y operativas dentro de una organización, sino que también plantea una serie de desafíos y consideraciones éticas que deben ser abordadas de manera rigurosa y consciente.

Estas tecnologías prometen mejoras significativas en eficiencia y productividad, pero también traen consigo preocupaciones en términos de equidad, responsabilidad, privacidad y seguridad. La adopción de estas prácticas disruptivas debe ser guiada no solo por criterios técnicos y económicos, sino también por principios éticos que aseguren un impacto positivo en todos los aspectos involucrados. Al considerar estos diversos enfoques éticos, se busca proporcionar una comprensión integral de los efectos potenciales de este proyecto y ofrecer recomendaciones para una adopción ética.

7.1. CUESTIONES ÉTICAS

7.1.1. Privacidad y seguridad de los datos

Es crucial garantizar que los datos utilizados y generados por el sistema estén protegidos contra accesos no autorizados. Esto incluye tanto los datos personales de los investigadores como la información sensible de la empresa. La transparencia en el uso de datos es fundamental, los involucrados deben ser informados sobre cómo se recopilan, almacenan y utilizan sus datos dentro del sistema. Además, es importante considerar cómo se gestionan los datos al finalizar los proyectos, asegurando su correcta eliminación o anonimización conforme a las nuevas normativas europeas, como el Reglamento General de Protección de Datos (RGPD).

7.1.2. Responsabilidad y transparencia

Se debe especificar quiénes son los encargados de crear y mantener el sistema, asegurando su correcto funcionamiento y evitando fallos que puedan tener consecuencias negativas. Los desarrolladores deben garantizar que el sistema esté diseñado de manera robusta y eficiente, mientras que el equipo debe garantizar su desempeño y solucionar cualquier problema que surja. Además, es esencial que todos los procedimientos y algoritmos utilizados sean comprensibles para los miembros del equipo que requieran de su uso, de modo que se mantenga la confianza y la toma de decisiones bien formadas. La claridad en la asignación de responsabilidades ayuda a evitar la ambigüedad y asegura que cada miembro del equipo sepa exactamente cuáles son sus deberes y compromisos.

7.1.3. Impacto en el empleo y las condiciones de trabajo

La implementación debe ir acompañada de programas de formación para asegurar que todos los empleados puedan adaptarse a las nuevas tecnologías. La falta de formación puede resultar en inseguridad laboral y desmotivación entre los empleados. Además, es crucial integrar a todos los miembros del equipo en el proceso de adopción, garantizando que no se beneficie solo a unos pocos integrantes dentro del equipo, sino que todos los integrantes puedan aprovechar las ventajas que ofrece. Equilibrar la automatización con las necesidades humanas es esencial para evitar la pérdida de empleos y asegurar que los empleados sigan realizando tareas significativas. La inclusión de todo el personal en la transición tecnológica fortalece la cohesión del equipo y maximiza los beneficios para la organización en su conjunto.

7.1.4. Impacto en el empleo y las condiciones de trabajo

Es esencial respetar los derechos de autor y la propiedad intelectual al reutilizar conocimiento. Las contribuciones de todos los miembros del equipo deben ser reconocidas adecuadamente, asegurando que nadie se apropie indebidamente del trabajo de otros. Fomentar un entorno donde el conocimiento se comparta de manera justa y equitativa es crucial para la colaboración y el avance del proyecto. Además, se debe tener cuidado al incorporar contenido que no haya sido creado por los miembros del equipo y que se haya obtenido de internet. Es fundamental asegurarse de que cualquier material externo utilizado cuente con la licencia adecuada, como la licencia MIT, para evitar infracciones legales y éticas. La retención de información valiosa por parte de ciertos individuos puede perjudicar estos objetivos, por lo que la transparencia y el respeto a la propiedad intelectual son indispensables.

7.1.5. Sostenibilidad y Responsabilidad Social

Se debe considerar cuidadosamente el impacto ambiental, especialmente en términos de consumo de energía y recursos. Es muy importante buscar soluciones sostenibles y eficientes que minimicen el impacto negativo en el medio ambiente. Además, es importante que las este sistema no solo beneficien a la empresa, sino que también contribuyan positivamente a la sociedad. Al integrar la sostenibilidad en cada etapa del ciclo de vida del proyecto, desde la conceptualización hasta la implementación y el mantenimiento, se asegura que el desarrollo tecnológico avance de manera responsable y con un compromiso claro hacia el bien común.

7.2. ANÁLISIS DESDE DIFERENTE PERSPECTIVAS ÉTICAS

7.2.1. Perspectiva utilitarista

Desde la perspectiva del utilitarismo, que se centra en maximizar el bienestar general y minimizar los aspectos negativos, debe evaluarse en términos de sus beneficios y perjuicios para todos los involucrados. La implementación del sistema puede incrementar significativamente la eficiencia y productividad al automatizar tareas repetitivas y facilitar la reutilización de conocimientos, lo que beneficia a la empresa y a sus empleados. Sin embargo, para maximizar el bienestar, es crucial proporcionar formación adecuada a todos los empleados, asegurando que todos puedan adaptarse y beneficiarse de la nueva tecnología, evitando que solo un pequeño grupo se vea favorecido. Además, es esencial garantizar la equidad en el acceso a las herramientas y recursos, proteger la privacidad y seguridad de los datos conforme a normativas como el RGPD, y mantener un equilibrio entre la automatización y las tareas humanas significativas.

7.2.2. Perspectiva de la ética de los principios

Podemos identificar varios principios éticos que deben ser considerados en la implementación de este sistema.

- **Justicia:** este principio implica tratar a todas las personas de manera equitativa y justa, asegurando que no haya discriminación y que todos tengan las mismas oportunidades y beneficios.
- **Autonomía:** la autonomía se refiere al derecho de los individuos a tomar decisiones informadas y libres sobre su propia vida y acciones, respetando su capacidad para autodeterminarse y actuar según sus propias convicciones y deseos.

- **Beneficencia:** la beneficencia actúa en beneficio de otros, promoviendo su bienestar y previniendo o eliminando cualquier daño. Este principio guía a las acciones que buscan maximizar los beneficios y contribuir positivamente al bienestar de las personas.
- **No maleficencia:** este principio se centra en la obligación de no causar daño a otros. Incluye la prevención de acciones que puedan resultar en perjuicio o daño, asegurando que las decisiones y prácticas no tengan consecuencias negativas para los involucrados.
- **Respeto a la propiedad intelectual:** Este principio se refiere al reconocimiento y protección de las creaciones, ideas y trabajos de los individuos. Implica garantizar que las contribuciones sean debidamente acreditadas y que se respeten las leyes y normas relacionadas con el uso y distribución del conocimiento y la información.

En base a estos principios, la implementación de este sistema debe garantizar que todos los empleados tengan acceso igualitario a la formación y a las nuevas oportunidades que brinda la tecnología, evitando que solo un pequeño grupo se vea beneficiado. Es crucial proteger la privacidad de los datos de los individuos y asegurar que estos tengan la información necesaria para tomar decisiones informadas sobre su uso. El sistema debe diseñarse de manera que maximice los beneficios, como la eficiencia y productividad, tanto para la empresa como para los empleados. Asimismo, es importante implementar medidas para minimizar cualquier daño potencial, incluyendo la protección de datos sensibles y la prevención de la pérdida de empleos mediante programas de formación y adaptación. Fomentar un entorno de trabajo donde las contribuciones individuales sean reconocidas y donde se utilice contenido externo de manera legal y ética es fundamental. Además, incorporar prácticas que reduzcan el impacto ambiental del sistema, promoviendo el uso eficiente de recursos y energías renovables, asegura una implementación ética y responsable del sistema, beneficiando a la organización, sus empleados y la sociedad en general.

8. CONCLUSIONES Y TRABAJO A FUTURO

8.1. CONCLUSIONES

8.2. TRABAJO A FUTURO

BIBLIOGRAFÍA

- [1] John Letzing y World Economic Forum. *To really grasp AI expectations, look to the trillions being invested*. en. <https://www.weforum.org/agenda/2024/04/appreciate-ai-expectations-trillions-invested/>. Abr. de 2024.
- [2] «Microsoft-backed OpenAI valued at \$80bn after company completes deal». En: *Guardian* (feb. de 2024).
- [3] Mauricio Hernández Armenta. *ChatGPT bate el récord de crecimiento más rápido de usuarios en la historia*. es. <https://www.forbes.com.mx/chatgpt-bate-el-record-de-crecimiento-mas-rapido-de-usuarios-en-la-historia/>. Feb. de 2023.
- [4] <https://ai.meta.com/>.
- [5] Brad Frost. *Atomic design*. Brad Frost Pittsburgh, 2016.
- [6] Rick Merritt. *What is MLOps?* en. 2020. URL: <https://blogs.nvidia.com/blog/what-is-mlops/>.
- [7] R. D. E. G. C. D. A. B. C. E. Salvucci. «MLOps - Standardizing the Machine Learning Workflow». En: (2021).
- [8] D. Kreuzberger, N. Kühl y S. Hirschl. «Machine Learning Operations (MLOps): Overview, Definition, and Architecture». En: (2022). URL: <https://arxiv.org/abs/2205.02302>.
- [9] G. Recupito et al. «A Multivocal Literature Review of MLOps Tools and Features». En: (2022). URL: <https://github.com/gilbertrec/MLR-MLOps-Tools-Features-Appendix>.
- [10] Microsoft. *What is Azure Machine Learning? - Azure Machine Learning — Microsoft Learn*. 2023. URL: <https://learn.microsoft.com/en-us/azure/machine-learning/overview-what-is-azure-machine-learning>.
- [11] Amazon Web Services. *Amazon SageMaker*. 2024. URL: <https://aws.amazon.com/sagemaker/>.
- [12] Google. *Vertex AI — Google Cloud*. 2023. URL: <https://cloud.google.com/vertex-ai#section-5>.
- [13] Stephen J Puetz et al. «The replication crisis and its relevance to Earth Science studies: Case studies and recommendations». En: *Geoscience Frontiers* 15.4 (2024), pág. 101821.
- [14] Monya Baker. «1,500 scientists lift the lid on reproducibility». en. En: *Nature* 533.7604 (2016), págs. 452-454. ISSN: 0028-0836. DOI: 10.1038/533452a. URL: <https://www.nature.com/articles/533452a>.
- [15] ReadyTensor.ai. *Define Reproducibility*. 2024. URL: https://www.readytensor.ai/resources/define_reproducibility/.
- [16] D. Athanasiou et al. «Test Code Quality and Its Relation to Issue Handling Performance». En: *IEEE Transactions on Software Engineering* 40 (2014), págs. 1100-1125. DOI: 10.1109/TSE.2014.2342227.
- [17] Toshihiro Kamishima et al. «Fairness-aware classifier with prejudice remover regularizer». En: *Machine Learning and Knowledge Discovery in Databases: European Conference, ECML PKDD 2012, Bristol, UK, September 24-28, 2012. Proceedings, Part II* 23. Springer. 2012, págs. 35-50.
- [18] Sainyam Galhotra, Yuriy Brun y Alexandra Meliou. «Fairness testing: testing software for discrimination». En: *Proceedings of the 2017 11th Joint meeting on foundations of software engineering*. 2017, págs. 498-510.

- [19] Jun Li y Ling Lianghe. «Comparative research on Python speed optimization strategies». En: *2010 International Conference on Intelligent Computing and Integrated Systems* (2010), págs. 57-59. DOI: 10.1109/ICISS.2010.5655011.
- [20] Cottom T.L. «Using SWIG to bind C++ to Python». En: *Computing in Science Engineering* 5.2 (2003), págs. 88-97. DOI: 10.1109/MCISE.2003.1182968.
- [21] John Aycock. «A brief history of Just-In-Time». En: *ACM Computing Surveys* 35 (ene. de 2003), págs. 97-113.
- [22] *functools Higher-order functions and operations on callable objects*. en. URL: <https://docs.python.org/3/library/functools.html>.
- [23] *Welcome to pydantic - pydantic*. en. URL: <https://docs.pydantic.dev/latest/>.
- [24] *Pytest: Helps you write better programs - pytest documentation*. en. URL: <https://docs.pytest.org/en/8.2.x/>.
- [25] Prometheus. *Overview*. en. URL: <https://prometheus.io/docs/introduction/overview/>.
- [26] Grafana. *The open observability platform*. URL: <https://grafana.com/>.
- [27] *What is MLflow?* en. URL: <https://mlflow.org/docs/latest/introduction/index.html>.
- [28] *What is ClearML?* en. URL: <https://clear.ml/docs/latest/docs/>.
- [29] *DVC - Data Version Control*. en. URL: <https://dvc.org/doc>.
- [30] *Web Pages in Half the Time: Why Microsoft Chose Astro to Build Their Fluent 2 Design System Website — Astro — astro.build*. <https://astro.build/case-studies/microsoft/>.
- [31] *What is Algolia? — Algolia algolia.com*. <https://www.algolia.com/doc/guides/getting-started/what-is-algolia>.
- [32] charliermarsh. *Ruff — docs.astral.sh*. <https://docs.astral.sh/ruff/>.
- [33] *Daily Climate time series data*. Ago. de 2019. URL: <https://www.kaggle.com/datasets/sumanthvrao/daily-climate-time-series-data>.
- [34] Rob Mulla. *Hourly energy consumption*. Ago. de 2018. URL: <https://www.kaggle.com/datasets/robikscube/hourly-energy-consumption>.