M1- Diseño de un sistema de supervisión de la eficiencia energética en calderas de vapor (caso de uso de economía tradicional) y el uso de componentes MLEDGE.

MLEDGE - Aprendizaje automático en la nube y en el borde

(Cloud and Edge Machine Learning)

Información sobre el entregable

Nombre del documento:

M1- Diseño de un sistema de supervisión de la eficiencia energética en calderas de vapor (caso de uso de economía tradicional) y el uso de componentes MLEDGE.

Versión actual: 1.0

Proyecto: MLEDGE - Aprendizaje automático en la nube y en el borde (Cloud and Edge Machine Learning)

Paquete de trabajo: P3 - Implementación del caso de uso de economía tradicional

Tareas: El entregable es resultado del trabajo en los diversos componentes técnicos:

- A3.1: Diseño de los componentes del caso de uso de economía tradicional

Entregable: E3.1 - Estado del arte y diseño de los componentes del caso de uso de economía tradicional.

Autores: Acuratio Europe S.L. e Inmarepro S.L.

Revisores: Santiago Andrés Azcoitia (IMDEA), Nikolaos Laoutaris (IMDEA)

Historial de Versiones

Versión	Fecha	Resumen de modificaciones
Version 1.0	14-06-2024	Versión inicial del documento

Indice

1. Introducción

En diciembre de 2022 fue adjudicado a IMDEA Networks el proyecto “MLEDGE - Aprendizaje automático en la nube y en el borde (Cloud and Edge Machine Learning)” (REGAGE22e00052829516, en adelante el ‘Proyecto’ o MLEDGE) por parte del Ministerio de Asuntos Económicos y Transformación Digital del Gobierno de España, con fondos de la Unión Europea dentro del Plan de Recuperación, Transformación y Resiliencia (European Union - NextGenerationEU/PRTR). El proyecto tiene como objetivo habilitar un ecosistema próspero de servicios FL en el borde seguros y eficientes capaces de facilitar el uso de datos personales y B2B confidenciales para entrenar modelos de ML para consumidores mientras se protege la privacidad de los datos y de sus propietarios.

Los **objetivos generales del proyecto** se pueden resumir en los siguientes:

1. Hacer del aprendizaje federado una funcionalidad accesible y de fácil uso en el borde mediante el desarrollo de una capa de software intermedio y componentes que escondan la complejidad del procesamiento y el intercambio de datos que supone.
2. Resolver problemas técnicos asociados al aprendizaje federado en el borde de la nube.
3. Demostrar esta funcionalidad en casos de uso que reflejen problemas reales de la industria que pueden ser resueltos con estas tecnologías.
4. Explotar los resultados del proyecto involucrando a agentes externos y comunicar los hallazgos al público potencial en general.

Uno de los objetivos básicos del proyecto diseñar, implementar y hacer públicos demostradores que trabajen con datos sensibles de individuos, y alimenten modelos de aprendizaje automático en diferentes campos de la industria .A tal fin, en la primera parte del proyecto se ha realizado una selección de empresas para el desarrollo de la plataforma FLaaS y el monitoreo de costes de computación, así como el diseño e implementación de casos de uso de negocio reales que se beneficien del aprendizaje distribuido en el borde de la nube. La INMAREPRO S.L. – ACURATIO EUROPE SL UTE con NIF U70842836 resultó adjudicataria del paquete de trabajo P3 cuyo objetivo es el diseño y la implementación del caso de uso de economía tradicional.

El presente documento se corresponde con el entregable E3.1 de título “Estado del arte y diseño de los componentes del caso de uso de economía tradicional” y tiene como objetivo la documentación detallada, incluyendo la necesidad y el problema que requiere el caso de uso, su impacto y potencial explotación, el diseño de su funcionamiento, y las pruebas de sistema.

La estructura del documento será la siguiente. En la sección 2 resumimos el objetivo del caso de uso, la necesidad y la arquitectura propuesta para el proyecto y cómo esta se alinea con los objetivos del mismo. Las siguientes secciones, de la 3 a la 7, presentan los avances que se han alcanzado en los diferentes componentes. Debido a que el idioma del equipo de trabajo es el inglés, estas secciones contienen material en este lenguaje, por ejemplo, las publicaciones y los papeles de trabajo. Finalmente, la sección 8 presenta las conclusiones y siguientes pasos en el proyecto.

2. Definición del problema y objetivos

En este apartado se presenta el problema que trata de resolver el caso de uso de eficiencia energética industrial de MLEDGE, comenzando por su contexto. Adicionalmente, se detalla la situación actual y el estado del arte, entendiendo como tal la infraestructura tecnológica existente sobre la cual se apoyará el caso de uso.

2.1. Contexto

" The cleanest energy is that which is not consumed at all. "

(Brigitte Zypries, ministra de Economía y Energía de Alemania, 2017)

La eficiencia energética no es simplemente una opción, sino una necesidad para Europa en el actual contexto global. **Es esencial no solo para cumplir con los objetivos climáticos y ambientales, sino también para garantizar la competitividad industrial y la seguridad energética.** La eficiencia energética juega un papel crucial en la reducción del consumo total de energía y, por ende, en la disminución de las emisiones de gases de efecto invernadero. Esto es particularmente relevante cuando se considera la ambición climática de la Unión Europea de reducir sus emisiones en al menos un 55% para 2030 en comparación con los niveles de 1990[1].

La eficiencia energética es un pilar en la estrategia de descarbonización de la UE. Al reducir la demanda de energía, disminuye la necesidad de generar energía a través de fuentes de combustibles fósiles, lo que resulta en menores emisiones de carbono. Este aspecto es fundamental para alcanzar los objetivos establecidos en el Acuerdo de París y en la Directiva de Eficiencia Energética revisada en 2023.

Objetivos de Desarrollo Sostenible (SDG)

La eficiencia energética también está intrínsecamente ligada a los Objetivos de Desarrollo Sostenible (SDG) de las Naciones Unidas, en particular el Objetivo 7, que busca "garantizar el acceso a una energía asequible, segura, sostenible y moderna para todos". Al mejorar la eficiencia energética, los países de la UE pueden hacer un uso más sostenible de sus recursos, lo que es crucial para alcanzar una mayor sostenibilidad ambiental, social y económica.

Fig. 1 - ODS - Objetivo 7

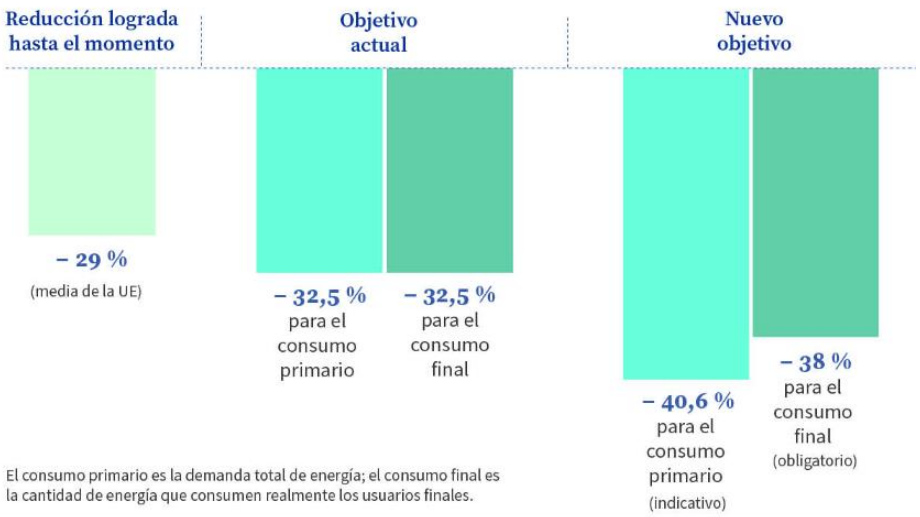
[1] Fit for 55 – European Commission –

Contexto y Antecedentes

La revisión de la Directiva de Eficiencia Energética en 2023 ha incrementado significativamente la ambición de la UE en cuanto a eficiencia energética. La directiva establece "la eficiencia energética primero" como un principio fundamental de la política energética de la UE, dándole por primera vez un estatus legal. Esto significa que la eficiencia energética debe ser considerada por los países de la UE en todas las decisiones políticas y de inversión relevantes en los sectores energético y no energético.

La directiva revisada de 2023 eleva el objetivo de eficiencia energética de la UE, haciendo que sea **obligatorio para los países de la UE asegurar una reducción adicional del 11,7% en el consumo de energía para 2030** en comparación con las proyecciones del escenario de referencia de 2020[2]. Como resultado, el consumo total de energía de la UE para 2030 no debe superar los 992,5 millones de toneladas de petróleo equivalente (Mtoe) para la energía primaria y 763 Mtoe para la energía final.

Fig. 2 - Objetivos de consumo primario y final en comparación con las previsiones de consumo para 2030 realizadas en 2007



Fuente: Consejo Europeo

Bajo las nuevas reglas, los países de la UE han acordado contribuciones nacionales indicativas utilizando una combinación de criterios objetivos que reflejan las circunstancias nacionales.

Objetivos de Ahorro de Energía Anuales

La directiva revisada más que duplica la obligación de ahorro de energía anual para 2028. Los países de la UE están obligados a lograr ahorros acumulativos en el uso final de energía para todo el período de obligación (2021-2030), equivalentes a nuevos ahorros anuales de al menos 0,8% del consumo de energía final en 2021-2023, al menos 1,3% en 2024-2025, 1,5% en 2026-2027 y 1,9% en 2028-2030.

[2] Energy efficiency directive -

Políticas y Legislación a nivel español

Normativas

En España, la eficiencia energética está regulada por varias políticas y legislaciones, entre las que cabe destacar:

1. **Real Decreto 36/2023, de 24 de enero**: Establece un sistema de **Certificados de Ahorro Energético**. Este decreto tiene como objetivo fomentar la implementación de medidas de eficiencia energética a través de un mecanismo de certificados.
2. **Real Decreto 56/2016**: Implementa la Directiva 2012/27/UE del Parlamento Europeo en cuanto a eficiencia energética. Establece la obligación de realizar **auditorías energéticas, acreditar a proveedores de servicios energéticos y promover la eficiencia en el suministro de energía**.
3. **Real Decreto 235/2013**: Establece el procedimiento básico para la certificación de **eficiencia energética de edificio**s en España.
4. **Real Decreto 1027/2007**: Reglamento de Instalaciones Térmicas en Edificios (RITE), que establece los requisitos de **eficiencia y seguridad para las instalaciones de climatización y agua caliente sanitaria en edificios.**

PNIEC

Adicionalmente, el **Plan Nacional Integrado de Energía y Clima (PNIEC) 2021-2030** si bien no es una normativa, establece la estrategia a seguir en eficiencia energética para cumplir con los objetivos europeos. En concreto, se fijan objetivos y medidas para reducir emisiones de gases de efecto invernadero (GEI) y la favorecer la penetración de energías renovables buscando la forma más adecuada y eficiente de hacerlo.

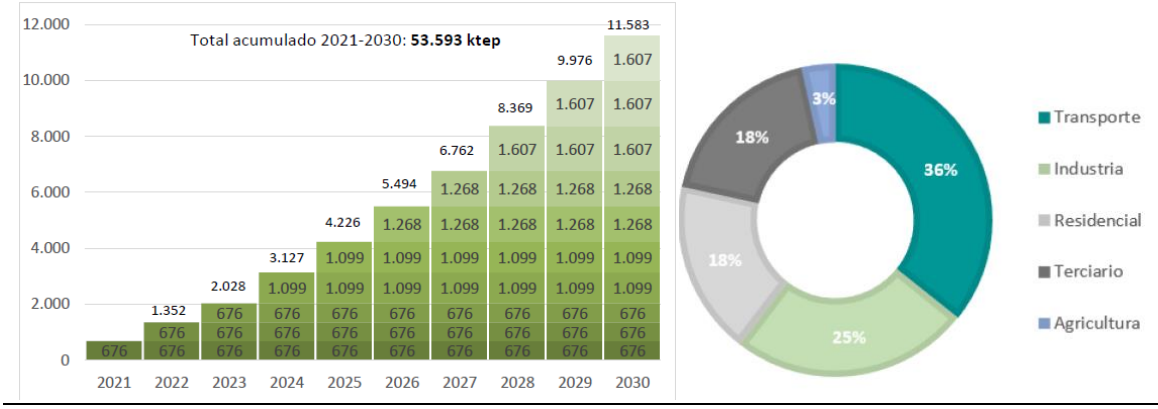
La última actualización del PNIEC tuvo lugar en junio de 2023, destacando los siguientes objetivos globales:

- 32% de reducción de emisiones de gases de efecto invernadero respecto a 1990
- 48% de renovables sobre el uso final de la energía
- 44% de mejora de la eficiencia energética en términos de energía final
- 81% de energía renovable en la generación eléctrica
- Reducción de la dependencia energética hasta un 51%

Con relación a la eficiencia energética, se plantea un 44% de mejora en términos de energía final (frente al 41,7% en el anterior PNIEC 2020). Las medidas de eficiencia energética del plan implican un **volumen total acumulado de ahorro de energía final para el periodo 2021-2030 de 53.593 ktep**.

De este volumen, un 36% corresponden al sector transporte, un 25% a la industria, tanto el sector terciario como el residencial suponen un 18% cada uno, y el sector agricultor supone un 3% del total.

Fig. 3 - Objetivo acumulado de ahorro de energía final: 2021-2030



Fuente: PNIEC

Finalmente, se estima que para la alcanzar los nuevos objetivos del PNIEC se requerirá una **inversión total acumulada de 294.000 millones de euros hasta 2030**, lo que supone un incremento del 22% respecto al Plan original. De estas inversiones, el 29% (es decir, más de 85.000 millones de euros) corresponden a las medidas de ahorro y eficiencia.

La relevancia del sector industrial para alcanzar los objetivos de eficiencia energética

En el escenario actual de cambio climático y creciente necesidad de sostenibilidad, la eficiencia energética se ha consolidado como una de las palancas clave para alcanzar los ambiciosos objetivos de reducción de emisiones y mejora en la sostenibilidad global. En este contexto, el sector industrial es crítico para el alcance de estos objetivos.

El sector industrial es un actor principal en la economía, no solo por su contribución al PIB sino también por su relevancia en términos de consumo energético y emisiones de gases de efecto invernadero. **De acuerdo con datos de 2021, el sector industrial en Europa es responsable de aproximadamente 25,6% del consumo energético total y 22,0% de las emisiones de GEI**[3].

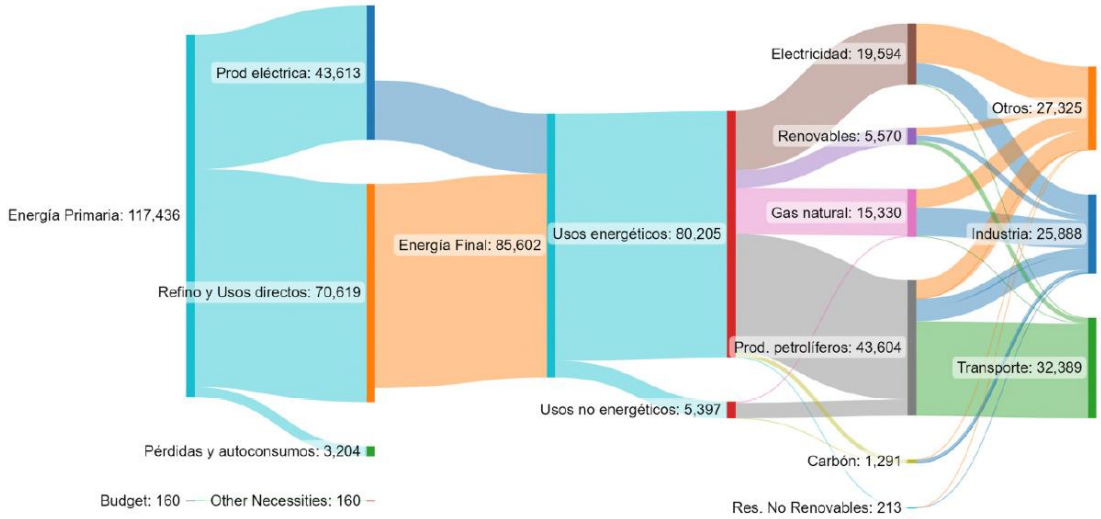
Este alto consumo energético no es, sin embargo, una sentencia de ineficiencia. Al contrario, representa un inmenso potencial para la implementación de medidas que incrementen la eficiencia energética, lo cual tendría un impacto significativo en la reducción de emisiones de carbono y otros gases de efecto invernadero. El sector industrial puede, por tanto, ser considerado como uno de los ejes centrales para alcanzar los objetivos establecidos a nivel europeo y nacional en este ámbito.

El papel del sector industrial no se limita a la sostenibilidad medioambiental, sino que también tiene un peso considerable en la competitividad económica. Implementar medidas de eficiencia energética puede llevar a una reducción de los costes operativos, aumentar la competitividad y contribuir al desarrollo sostenible y a la creación de empleo.

En el contexto español el sector industrial contribuye con alrededor de 30% al consumo total de energía. Esta cifra subraya la necesidad de centrarse en este sector como un área clave para lograr mejoras en la eficiencia energética. La energía en la industria se consume en diversos procesos, que van desde la manufactura y producción hasta el transporte y la logística.

[3] Eurostat - Final energy consumption in industry - detailed statistics, Agencia Europea del Medioambiente EEA greenhouse gases

Fig. 4 - Flujo de Energía en España, 2021



Fuente: Ministerio Transición Ecológica[4]

La naturaleza intensiva en energía del sector industrial significa que incluso pequeñas mejoras en la eficiencia pueden resultar en reducciones significativas en el consumo energético y las emisiones de gases de efecto invernadero. Medidas como la optimización de procesos, la adopción de tecnologías más eficientes, y la recuperación de calor residual pueden tener un impacto considerable. Asimismo, las tecnologías empleadas para optimizar el consumo energético están en constante evolución y mejora. Ejemplos notables incluyen la sustitución de quemadores mecánicos por electrónicos, la incorporación de bombas de calor más eficientes para climatización o procesos industriales, y la penetración de placas solares híbridas que pueden producir tanto electricidad como calor.

Dentro del amplio paraguas del sector industrial, hay subsectores específicos que presentan un mayor potencial para mejoras en eficiencia energética. Estos pueden incluir, por ejemplo, la industria química, metalúrgica, alimentaria o farmacéutica. Cada uno de estos subsectores tiene retos y oportunidades únicas en lo que a eficiencia energética se refiere.

Impacto Económico y Competitividad

El coste de la energía representa una parte significativa de los gastos operativos en muchas industrias. Según el Instituto Nacional de Estadística[5], el gasto energético total de la industria aumentó en 2021 un 27% en comparación con el 2019. De los €14.254 millones de gasto, un 62% corresponde a electricidad, un 27% a gas, un 5% a productos petrolíferos y un 5% a calor y otros productos. Reducir este coste mediante la eficiencia energética puede, por lo tanto, tener un impacto directo en la competitividad de las empresas. El ROI de las inversiones de eficiencia energética industrial puede ser muy atractivo, y dependiendo del uso de los equipos puede en muchos casos ser inferior a un año.

La transición hacia una mayor eficiencia energética en el sector industrial no solo es beneficioso en términos de ahorro de costes, sino que también tiene el potencial de crear empleo. Inversiones en nuevas tecnologías y en la modernización de infraestructuras existentes pueden llevar a la creación de puestos de trabajo tanto directos como indirectos.

[4] Balance Energético España, datos 2021

[5] El Periódico de la Energía – "El gasto energético de la industria aumentó un 27% en 2021, hasta 14.254 millones" - LINK

En resumen, el impacto económico y la competitividad en el sector industrial están estrechamente ligados a la eficiencia energética. Reducir los costes de energía a través de medidas eficientes mejora directamente la competitividad empresarial, al tiempo que proporciona un retorno de la inversión favorable. Además, la eficiencia energética ofrece potencial para el crecimiento económico y la creación de empleo, amplía el acceso a mercados internacionales y contribuye a una gestión de riesgos más robusta, especialmente en relación con la volatilidad de los precios de la energía y la dependencia de fuentes no renovables.

2.2. Objetivos

Si bien una solución MLEDGE que se desarrollaría para clientes industriales podría utilizarse con muchas tipologías de equipos (calderas, compresores, enfriadoras, electricidad, etc.), el desarrollo del componente objeto del proyecto se realizará inicialmente para una tipología de equipo específico (calderas de vapor) para simplificar la adquisición de datos y el desarrollo del modelo de ML/FL. Las calderas de vapor son adecuadas para la toma de datos debido a su operación estandarizada y medible, y son consideradas el corazón de cualquier fábrica industrial debido a su papel crucial en la generación de energía y procesos de producción. Asimismo, son equipos que se prestan a mejoras de eficiencia energética, por ejemplo, con el remplazo de quemadores mecánicos por electrónicos, o con la incorporación de recuperadores de calor.

Este tipo de procesos son idóneos para la aplicación de tecnologías federadas ya que los datos se generan en muchas ubicaciones diferentes y además son datos sensibles de los que se pueden inferir informaciones relacionadas con la marcha del negocio como el consumo energético de las plantas de producción. Por lo tanto, por motivos de privacidad, confidencialidad y eficiencia el uso de tecnologías MLEDGE es clave.

En el **caso específico de las calderas de vapor**, las tecnologías federadas permiten monitorear y optimizar el rendimiento de cada unidad de manera segura y eficiente. Estas tecnologías garantizan la protección de datos sensibles, como el consumo de combustible o su producción de vapor, y facilitan el mantenimiento predictivo y la gestión energética integral de la caldera de vapor.

2.3. Situación actual y visión de futuro

Situación Actual

La producción de vapor en la industria para las necesidades de fabricación tiene una significancia muy importante en el consumo energético de la planta, y es un proceso difícilmente descarbonizable en el corto plazo por las temperaturas implicadas en el mismo y los costes tan elevados que implica su electrificación. Las redes de vapor están muy difundidas en muchas industrias de distintos sectores con sectores como el farmacéutico o alimentario donde su uso está muy extendido. El corazón de esta producción son las calderas de vapor con sus quemadores. El conjunto puede estar formado por caldera-quemador de un fabricante o por módulos integrados de varios fabricantes que funcionan como un equipo aislado e independiente. El rendimiento energético de estos equipos está muy influenciado con distintos factores como el perfil de carga, el funcionamiento inadecuado de algunos de los distintos componentes que la componen o un desvío de la parametrización de esta por el cambio de condiciones de funcionamiento ... Desde Inmarepro lo que observamos es que la desviación del optimo funcionamiento puede suponer unos elevados costes energéticos difícilmente detectables en el funcionamiento del equipo salvo que lo analice un técnico en calderas y quemadores que conozca el funcionamiento de distintos equipos similares.

Actualmente el industrial conoce el funcionamiento de su o sus calderas y mediante la contratación de visitas periódicas chequea el funcionamiento y es en ese momento cuando optimiza el rendimiento energético hasta la siguiente intervención. El conocimiento de las actuaciones más adecuadas en términos de eficiencia reside en el equipo técnico de proveedores de servicios como Inmarepro. Los equipos de producción de vapor, aunque hagan la misma función se encuentran dispersos en distintas industrias y totalmente inconexos unos con otros sin compartir información y en muchos casos el sistema de control local no facilita información clave del rendimiento del mismo ni de cómo optimizarlo ya que no puede evaluar el comportamiento de ese equipo en referencia con otros trabajando en condiciones similares. Son los técnicos de mantenimiento en sus visitas los que ajustan el funcionamiento de la caldera a sus parámetros óptimos. Esta frecuencia de visita se hace por establecimiento de un protocolo de visitas en un mantenimiento preventivo con una periodicidad establecida en un contrato.

Visión MLEDGE

La visión de Inmarepro es desarrollar un sistema que permita compartir el conocimiento y optimizar el funcionamiento de distintas calderas en distintas industrias, determinando el mejor momento de intervención antes de que los costes energéticos alcancen cifras no deseables por desviación del funcionamiento óptimo o se produzcan averías que impliquen una parada de la producción del cliente. Un sistema que en tiempo real determine si hay desviaciones previendo cuando intervenir basado en el conocimiento del funcionamiento de multitud de equipos de una forma confidencial y federada.

Es por ello por lo que nuestra alianza con Acuratio nos permite apalancar las capacidades de la tecnología de IA especialmente en el campo de Federated Learning e implementar este sistema que nos permita cumplir con nuestra visión. El conocimiento tecnológico de Acuratio nos permite desarrollar un sistema que reciba los datos de los distintos equipos funcionando en tiempo real, gestionados con total confidencialidad, los analice y en función del conocimiento que ha adquirido el sistema con el entrenamiento de las distintas instalaciones informe sobre las anomalías de funcionamiento, la desviación sobre el óptimo funcionamiento energético y las actuaciones a realizar en tiempo real.

Este sistema dará una visión sobre el funcionamiento del equipo y las pautas para conseguir mejorar la eficiencia, aumentar la descarbonización de la industria, optimizar las actuaciones en tiempo real con una compartición confidencial de información de un conjunto disperso y heterogéneo de instalaciones que se enfrentaban a problemáticas similares.

La visión de largo plazo que tenemos en Inmarepro es extenderlo a otras producciones de servicios energéticos en las industrias como por ejemplo los sistemas de generación de aire comprimido o los sistemas de refrigeración industriales ambas con una implicación de relevancia en el consumo energético de las plantas industriales.

Fig. 5 – Diagrama situación actual y visión MLEDGE

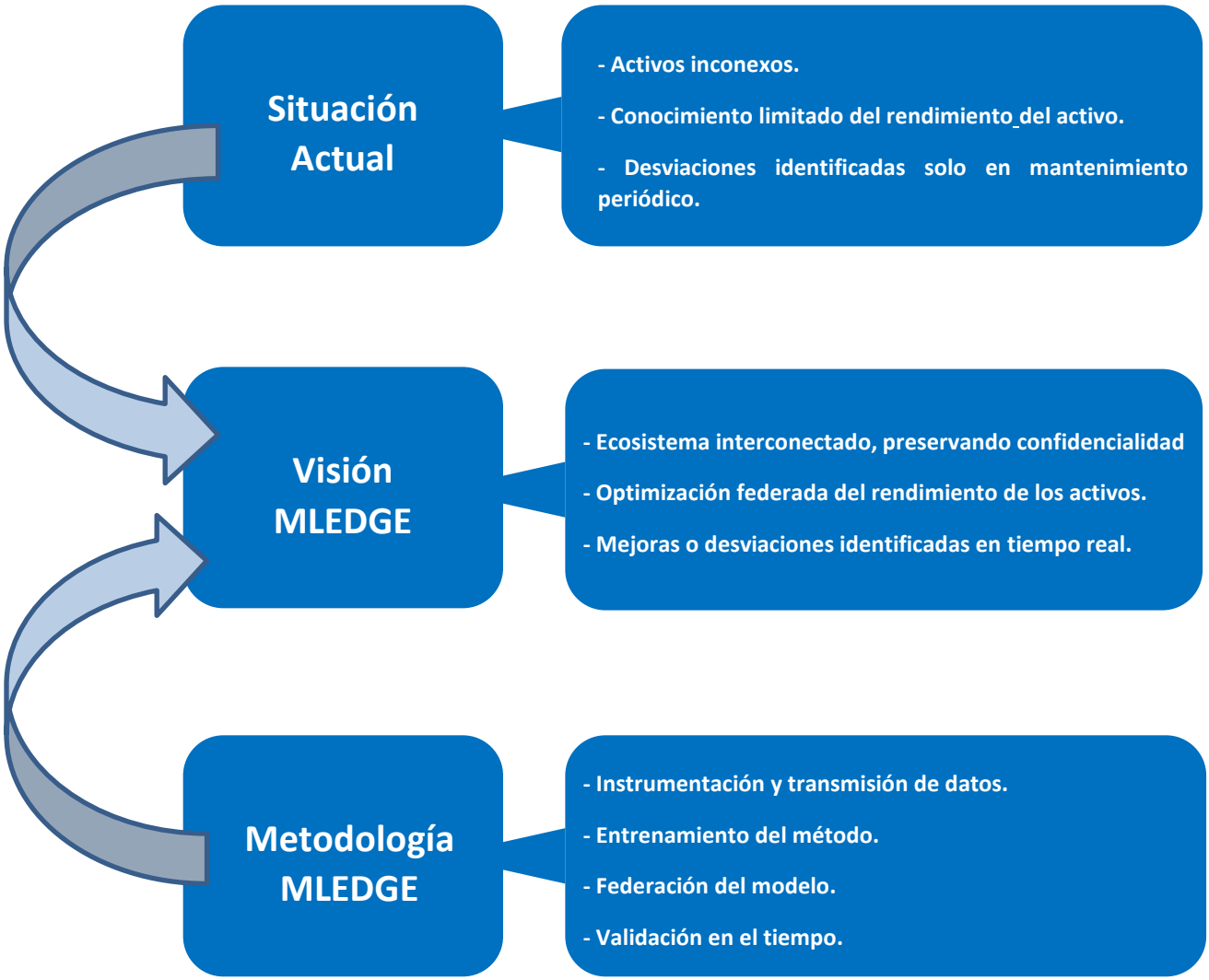
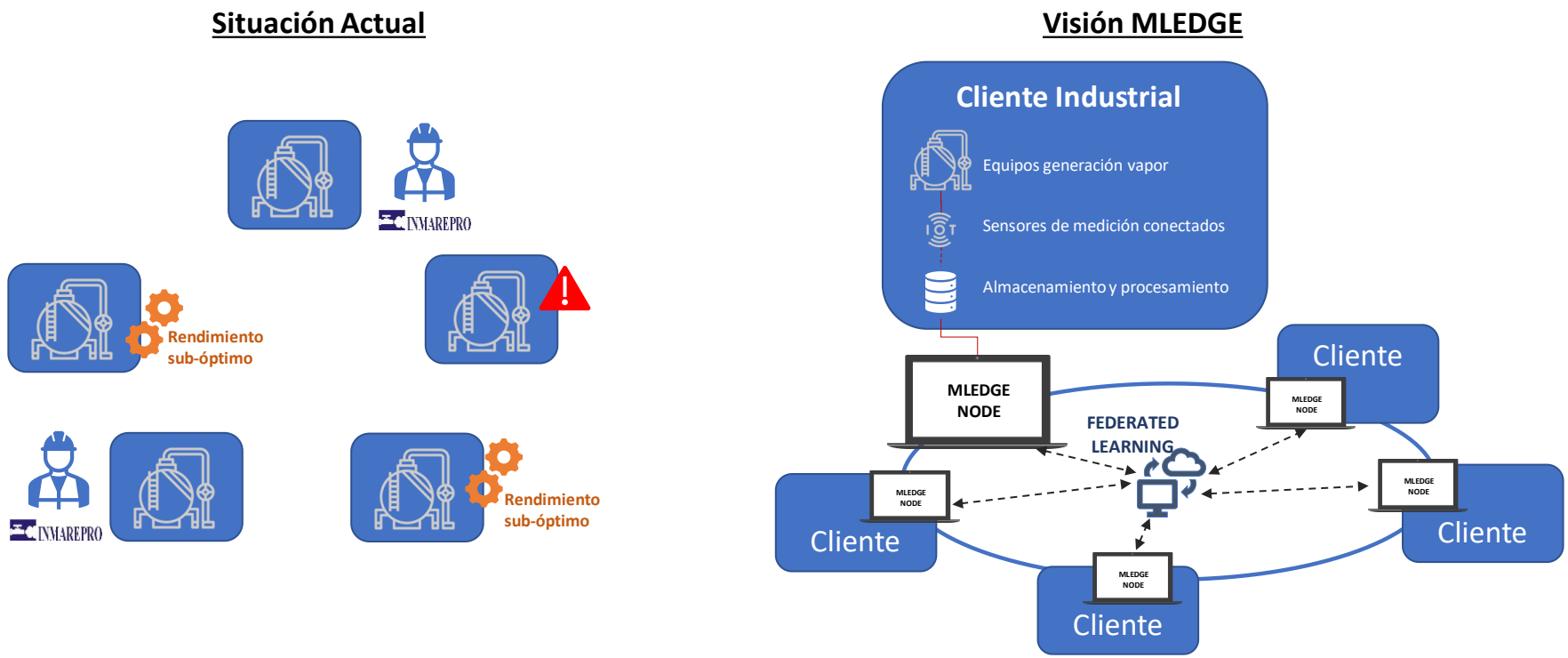


Fig. 6 – Ilustración situación actual y visión MLEDGE



2.4. La solución

El proyecto se basará en una sólida infraestructura tecnológica existente, aprovechando componentes y sistemas establecidos para mejorar la eficiencia operativa y la toma de decisiones mediante el uso de Federated Machine Learning.

Una solución que incorpore elementos debe puede aportar un alto valor a clientes industriales para evaluar el rendimiento óptimo de sus equipos, así como la toma de decisiones empresariales que aumenten la eficiencia energética de su producción. Todo esto mientras se preserva la confidencialidad de sus datos.

Desde la perspectiva de la solución, se puede considerar que hay tres niveles de posible servicio, “desbloqueado” por una capacidad tecnológica diferente, que a su vez añade mayor complejidad y valor a la anterior. De esta manera, una primera gama de características al implementar un sistema de control se vería reforzado con la introducción de capacidades de Machine Learning, y finalmente con capacidades de Federated Learning:

Nivel 1: Sistema de Control

El primer peldaño de esta solución tecnológica es un sistema de control avanzado que realiza un monitoreo constante de todas las variables relevantes, como el consumo de gas, electricidad y agua, así como la producción de energía. A través de una plataforma en línea, los operadores pueden:

- Ver la producción en tiempo real.
- Acceder al historial de consumo.
- Monitorear la eficiencia del equipo mediante indicadores como el Coefficient of Performance (COP).

Para poder llevar a cabo estos puntos técnicamente el sistema de control se apoya en los siguientes equipos de medida recogidos en el PLC de manera local:

- Caudalímetro de vapor.
- Caudalímetro de agua de alimentación caldera.
- Cuantometro de gas con correcto PT.
- Sonda de temp. de agua de alimentación caldera.
- Sonda de temp. humos de chimenea.
- Sonda de temp. depósito de condensados.
- Sonda de temp. ambiente entrada de aire al quemador.
- Contador de agua de llenado.
- Sonda de temp. de agua de llenado.

Nivel 2: Machine Learning

Al incorporar el Machine Learning, el sistema alcanza un nuevo nivel de robustez y precisión. Con el análisis de datos en tiempo real y en base a históricos, se pueden habilitar herramientas basados en modelos de ML como:

- Detección de anomalías que podrían indicar fallos o ineficiencias.
- Sugerencias de optimización para mejorar el rendimiento del equipo.
- Predicción de la producción para ayudar en la planificación.

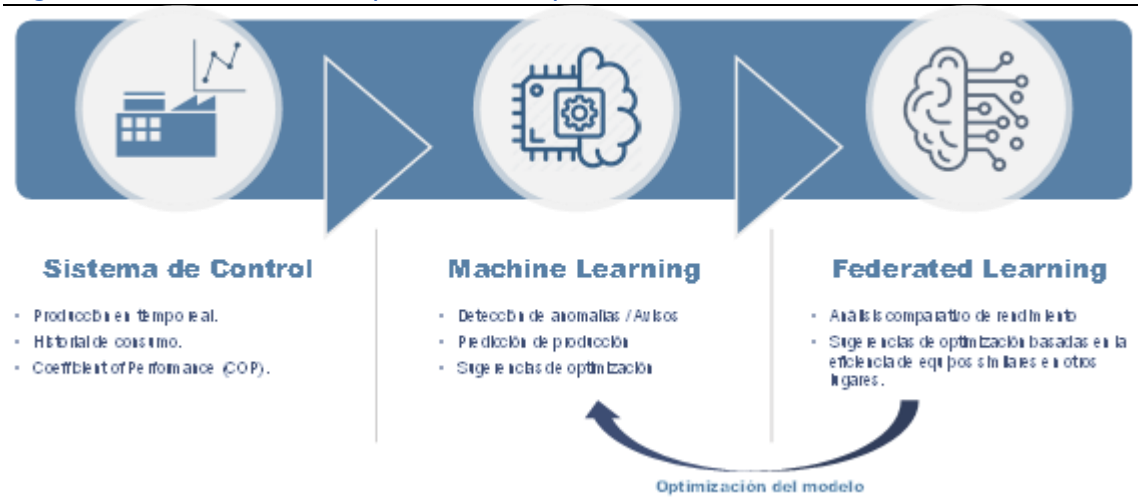
- Optimización en inversión en sensores por inferencias de variables obtenidas.
- Análisis de coste-beneficio para el ahorro de costes.

Nivel 3: Federated Learning

El nivel más avanzado utiliza el Federated Learning para aprovechar la inteligencia colectiva a la hora de entrenar estos modelos de ML. Al comparar su equipo con máquinas similares en diferentes instalaciones, los operadores obtienen:

- Un entendimiento más profundo de qué variables afectan la eficiencia del equipo.
- Recomendaciones para mejorar el rendimiento basadas en la eficiencia de equipos similares en otros lugares.
- La posibilidad de tomar decisiones informadas sobre inversiones en nuevos equipos, seleccionando aquellos con niveles de eficiencia superiores.

Fig. 7 – *Caso de Uso – Perspectiva de Capacidades*



La oportunidad y relevancia del caso de uso radican en ofrecer una solución escalable y segura que optimiza la eficiencia energética en entornos industriales. Comenzando con el sistema de control, se brindan herramientas básicas para el monitoreo en tiempo real y la evaluación de equipos. La incorporación de Machine Learning amplía estas capacidades, permitiendo la detección de anomalías y sugerencias de optimización basadas en datos. Finalmente, el Federated Learning ofrece un enfoque colaborativo para la mejora de la eficiencia, permitiendo a los clientes beneficiarse de un conjunto más amplio de datos sin comprometer la confidencialidad. En resumen, el caso de uso presenta una oportunidad para mejorar sustancialmente la eficiencia energética y la competitividad en el sector industrial, mientras se abordan las preocupaciones sobre la privacidad y la seguridad de los datos.

3. Especificación de requisitos

3.1. Caso(s) de uso

Desde optimizar procesos empresariales, hasta predecir anomalías de alto impacto sobre una instalación, el análisis de datos ofrece un amplio abanico de posibilidades. A través de estos cinco casos de uso que se presentan, exploraremos cómo esta poderosa herramienta impulsa la toma de decisiones y el ahorro energético-económico sobre las industrias.

Se seleccionaron cinco casos (anónimos) en la cartera de clientes de la compañía INMAREPRO S.L. con distintos sectores económicos o casos de producción de vapor, para presentar un modelo industrial más fortalecido y exportable al mercado.

ID	Caso de uso	Usuario	Objetivo	Beneficio, resultado, razón del caso de uso
US_1	COSMÉTICO	Dirección de Producción y Mantenimiento de la fábrica.	Analizar y mejorar el rendimiento de la caldera de vapor, junto a la detección predictiva de anomalías a tiempo para actuar preventivamente y así prolongar su longevidad y evitar averías de alto impacto.	Aportar datos y cuantificar el impacto económico, ecológico y funcional sobre las acciones anteriormente indicadas, junto a una supervisión continúa de los consumos para una detección inmediata de posibles desviaciones.
US_2	ALIMENTICIO			
US_3	LAVANDERIA INDUSTRIAL			
US_4	FARMACEUTICO			
US_5	COSMÉTICO			

3.2. Requerimientos funcionales

Detalle de los requerimientos funcionales de cada componente a alto nivel (de los especificados en el apartado 2. 4).

3.2.1. DUI1

El proyecto MLEDGE surge como una solución integral, combinando técnicas avanzadas de ML y FL, junto un robusto dashboard de exportación de datos para impulsar decisiones estratégicas. El objetivo es aplicar MLEDGE en la gestión de calderas de vapor, extrayendo conocimientos significativos de datos complejos para generar resultados tangibles.

El dashboard de exportación es esencial, permitiendo a las compañías visualizar y personalizar la información, representando alarmas en la interfaz de usuario, democratizando el acceso a los datos y fomentando una cultura basada en evidencia de los datos federados. Esta funcionalidad incluye gráficos interactivos, tablas dinámicas y accesibilidad desde cualquier dispositivo, lo que promueve la colaboración y mejora continua. La personalización del dashboard asegura que los datos sean relevantes para cada usuario, aumentando la utilidad y aceptación en toda la organización. La sinergia entre MLEDGE y el dashboard de exportación es fundamental para desbloquear el potencial de los datos y tomar decisiones informadas.

3.2.2. SAC1

El proyecto plantea el desarrollo de un sistema avanzado de control a través un PLC y los distintos elementos de campo para el monitoreo que abarca varios aspectos críticos de la gestión de recursos. Este sistema será capaz de realizar un seguimiento en continuo y registrado de diversas variables clave, tales como el consumo de gas, vapor y agua, así como su monetización.

Esto se logrará mediante una plataforma en línea que ofrecerá datos actualizados constantemente, permitiendo una gestión más eficaz y funcional.

3.2.3. SAC2

Además de lo mencionado en el punto anterior, el sistema almacenará un historial detallado del consumo de recursos, facilitando el acceso a registros anteriores para análisis y toma de decisiones. Esta característica permitirá identificar patrones de uso y áreas de mejora en la eficiencia de los recursos.

3.2.4. Transmisión y protección de datos

La transmisión de los datos desde las calderas de los clientes de Inmarepro hasta los nodos de Acuratio deberá cumplir los siguientes requerimientos:

Requisitos de la transmisión y protección de datos		
#	**Requisito**	**Descripción**
TPD1	Seguridad de Comunicaciones	La transmisión de datos debe utilizar protocolos de comunicación encriptados y seguros, garantizando la confidencialidad y la integridad de los datos durante todo el proceso de transferencia.
TPD2	Rapidez en la transmisión de los datos	Los datos deben ser transmitidos de manera eficiente, minimizando la latencia y asegurando que la información esté disponible para su procesamiento sin demoras significativas.
TPD3	Seguridad en el almacenamiento de los datos	Los datos recibidos deben ser almacenados en infraestructuras seguras, con medidas de protección que eviten accesos no autorizados, pérdidas o alteraciones de la información.
TPD4	Administración y gestión	Debe tener capacidades robustas para administrar y visualizar los datos en cada nodo donde se hayan guardado, permitiendo la supervisión de la información almacenada.

3.2.5. Desarrollo del modelo de ML

Las herramientas para el desarrollo de modelos de Machine Learning deberán cumplir con las siguientes características:

Requisitos para el desarrollo del modelo de ML		
#	**Requisito**	**Descripción**
MML1	Facilidad de uso	Las herramientas deben ser intuitivas y estar alineadas con las plataformas más reconocidas en el ámbito del Machine Learning.
MML2	Versatilidad	Se debe disponer de una variedad de herramientas que permitan la experimentación con distintos modelos y pipelines de preprocesamiento de datos.
MML3	Comunicación segura	Es esencial que la comunicación entre usuarios y nodos al programar los modelos sea segura siempre, garantizando la confidencialidad y la integridad de los datos y de los modelos generados.

Requisitos para el desarrollo del modelo de ML		
#	**Requisito**	**Descripción**
MML4	Rendimiento	Los nodos utilizados para el desarrollo de modelos deben contar con la capacidad computacional necesaria para procesar eficientemente los volúmenes de datos generados por los clientes de Inmarepro.

3.2.6. Desarrollo del modelo de FL

Las herramientas para el desarrollo de modelos de Federated Learning deberán cumplir las siguientes características:

Requisitos para el desarrollo del modelo de FL		
#	**Requisito**	**Descripción**
FL1	Federación de modelos	El sistema debe permitir implementar protocolos federados para el entrenamiento de modelos preservando la privacidad del dato.
FL2	Analítica federada	El sistema debe permitir coordinar protocolos de analítica federada basada en Secure Multi-Party Computation y técnicas de cifrado homomórfico entre otros.
FL3	Comunicación segura	Es esencial que la comunicación entre usuarios y nodos al programar los modelos sea segura siempre, garantizando la confidencialidad y la integridad de los datos y de los modelos generados.
FL4	Comunicaciones eficientes	En este caso no solo será crítica la capacidad computacional de los nodos, sino también el rendimiento de las comunicaciones entre ellos y con el servidor.
FL5	Rendimiento del modelo	El rendimiento del modelo de Federated Learning deberá ser similar o superior al modelo de ML centralizado.

3.3. Requerimientos no funcionales

Los requerimientos no funcionales, cruciales para el éxito de cualquier proyecto, ya que definen criterios de calidad y rendimiento que no están directamente relacionados con las funciones específicas del sistema.

En el contexto del proyecto "MLEDGE - Aprendizaje automático en la nube y en el borde", los requerimientos no funcionales aseguran que el sistema sea **eficiente, escalable, seguro y fácil de usar**, lo cual es esencial para su viabilidad y aceptación a largo plazo. A continuación, se describen algunos de los principales requerimientos no funcionales para este proyecto:

Escalabilidad

- **Escalabilidad actual y futura**: La capacidad del sistema para manejar una creciente cantidad de trabajo es fundamental. En el caso de MLEDGE, esto implica que la arquitectura del sistema debe ser capaz de gestionar un número creciente de nodos y usuarios sin degradar su rendimiento. La infraestructura debe ser flexible para adaptarse a futuras expansiones, ya sea aumentando el número de dispositivos conectados en el borde, incrementando la capacidad de procesamiento en la nube o siendo extrapolado a distintos entornos de volumen o tipo de trabajo.

Rendimiento

- **Rendimiento del modelo**: El rendimiento del modelo de aprendizaje federado (FL) debe ser comparable o superior al de un modelo de aprendizaje automático centralizado. Esto incluye la precisión del modelo y la eficiencia en el tiempo de procesamiento y uso de recursos. Los nodos deben contar con suficiente capacidad computacional para procesar eficientemente los datos generados por los clientes.
- **Rendimiento de las comunicaciones**: Es crucial que las comunicaciones entre los nodos y el servidor sean rápidas y eficientes. Esto no solo afecta la velocidad de entrenamiento del modelo sino también la experiencia del usuario al interactuar con el sistema. La latencia debe mantenerse al mínimo para asegurar que las actualizaciones del modelo y la transferencia de datos se realicen sin retrasos significativos.

Seguridad

- **Seguridad en la comunicación**: Dado que MLEDGE maneja datos sensibles y confidenciales, todas las comunicaciones deben ser seguras. Incluye el cifrado de datos en tránsito y en reposo, y protocolos de comunicación seguros. La integridad y confidencialidad de los datos deben estar garantizadas para evitar cualquier fuga de información o acceso no autorizado.
- **Seguridad del modelo**: Además de la seguridad en la comunicación, las actualizaciones de los modelos deben ser agregadas de manera segura para prevenir cualquier exposición de datos sensibles. Esto implica el uso de técnicas avanzadas como la agregación segura de actualizaciones de modelos.

Usabilidad

- **Facilidad de uso**: Las herramientas y la interfaz de usuario deben ser intuitivas y fáciles de usar. Esto es especialmente importante en el contexto de aprendizaje federado, donde los usuarios pueden no estar familiarizados con los conceptos técnicos subyacentes. La interfaz debe permitir a los usuarios interactuar con el sistema sin necesidad de conocimientos avanzados en programación o aprendizaje automático.
- **Versatilidad**: El sistema debe ofrecer una variedad de herramientas que permitan la experimentación con diferentes modelos y pipelines de preprocesamiento de datos. Esta versatilidad es clave para adaptarse a diferentes necesidades y escenarios de uso, facilitando así la adopción del sistema por un amplio espectro de usuarios.

Mantenibilidad y Actualización

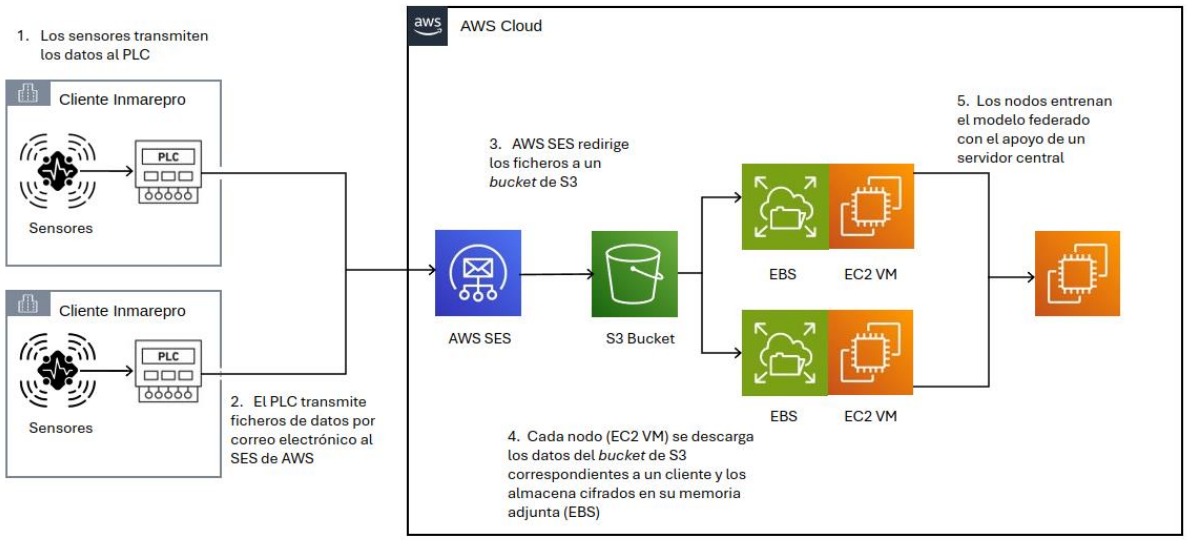
- **Mantenibilidad**: La infraestructura del sistema debe ser fácil de mantener y actualizar. Esto incluye la posibilidad de realizar actualizaciones de software con la menor interrumpir posible en el servicio y la capacidad de monitorear y diagnosticar problemas de manera eficiente. Una buena mantenibilidad asegura que el sistema pueda evolucionar y mejorar con el tiempo sin incurrir en costes excesivos o interrupciones.

Los requerimientos no funcionales están diseñados para asegurar que el sistema no solo cumpla con sus funciones específicas, sino que también lo haga de manera eficiente, segura y escalable. Estos aspectos son esenciales para garantizar la viabilidad y el éxito a largo plazo del proyecto en un entorno industrial dinámico y exigente.

4. Arquitectura y descripción de los componentes del caso de uso

En el siguiente gráfico se muestra un resumen de la arquitectura propuesta.

Fig. 8 – *Arquitectura caso de uso*



4.1. Elementos software

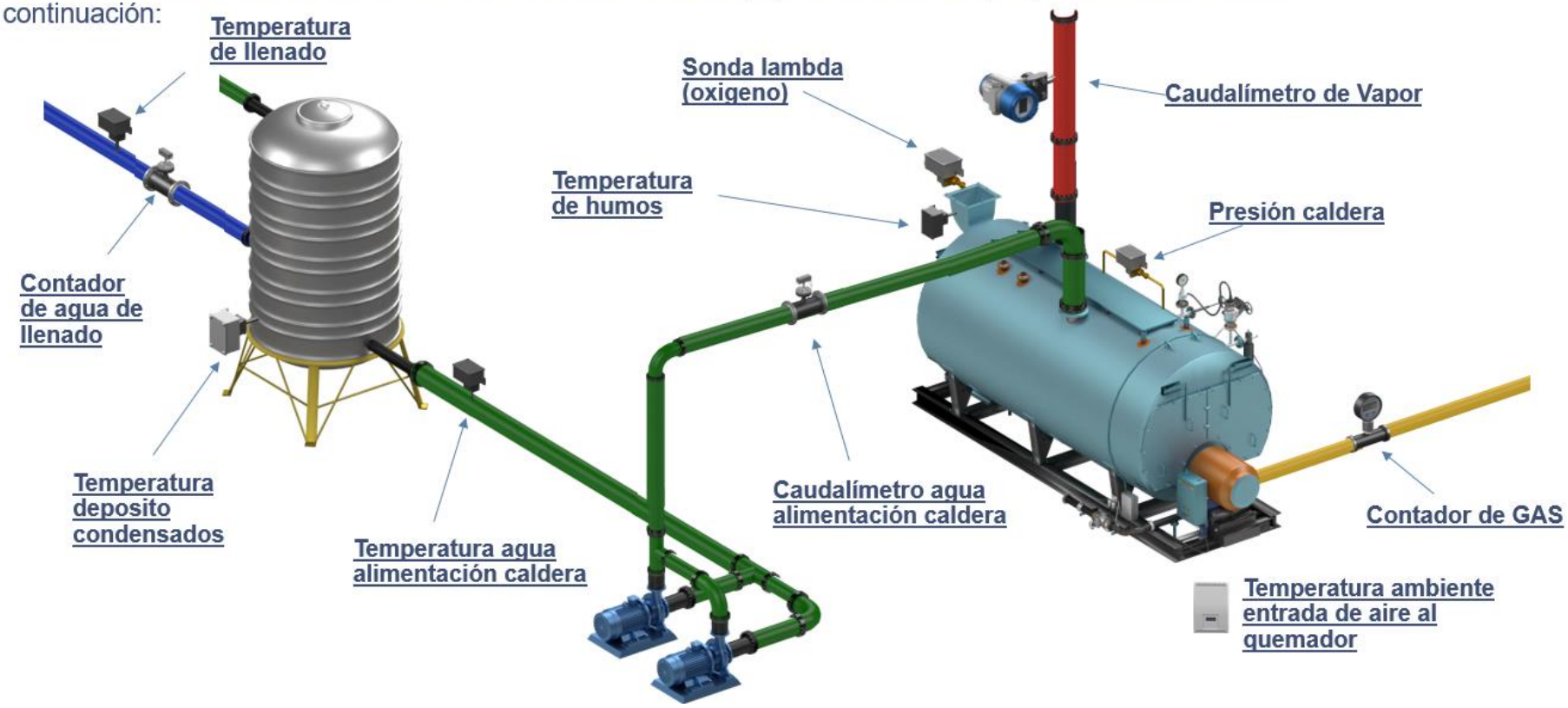
- **Python:** Este será el lenguaje principal utilizado para el desarrollo de modelos, tanto en entornos locales como federados. Estará preinstalado en el software que Acuratio implementará en las máquinas virtuales EC2.
- **Librerías Python estándar para Machine Learning:** Los nodos contarán con las librerías más populares preinstaladas para Machine Learning y Data Analytics.
- **Librería Python Acuratio para Federated Learning:** El software instalado en las máquinas virtuales EC2 incluirá una librería específica desarrollada en Python por Acuratio. Esta librería facilitará el diseño y entrenamiento de redes neuronales y XGBoost federados.
- **JupyterLab:** Esta será la interfaz que permitirá la interacción con el nodo desde la APP.
- **Aplicación web (APP):** Acuratio desarrollará una aplicación web desde la cual se podrán controlar los nodos.
- **API:** Acuratio proporcionará una API que funcionará como backend de la aplicación web. Esta API actuará como intermediario entre la aplicación y los nodos, así como coordinadora del proceso de entrenamiento.
- **Servicio SES de AWS:** Acuratio utilizará el servicio de correo electrónico de AWS, SES, para transferir datos desde los PLCs de los clientes de Inmarepro hasta los buckets de S3.

4.2. Elemento hardware

- **Sensores:** sensores en las máquinas de Inmarepro.
- **PLC:** Infraestructuras de PLC existentes en los clientes de Inmarepro.
- **Bucket S3 de AWS:** contenedor de almacenamiento altamente escalable y duradero en la nube de AWS, diseñado para almacenar una amplia variedad de datos, desde archivos simples hasta grandes conjuntos de datos y contenido multimedia.
- **Maquinas** Vrituales de AWS EC2 con almacenamiento cifrado en EBS: Una máquina virtual por cada cliente de Inmarepro y una máquina virtual que actúe de servidor en el entrenamiento federado.

Fig. 9 – *Esquema principios producción de vapor*

- Recogida de datos caldera vapor
- Para la obtención de estos datos instalaremos una serie de equipos de medición que pasamos a detallar a continuación:



4.3. Matriz de requerimientos - componentes

Requisitos de la transmisión y protección de datos		
#	**Requisito**	**Componentes**
TPD1	Seguridad de Comunicaciones	Email (SES) con protección SSL. Autenticación y autorización de los nodos para acceder al bucket de S3.
TPD2	Rapidez en la transmisión de los datos	Uso de SES para transmitir los datos entre los PLCs y el bucket de S3.
TPD3	Seguridad en el almacenamiento de los datos	Amazon Elastic Block Store (EBS) con encriptación.
TPD4	Administración y gestión	A través de un JupyterLab en cada nodo se dará al usuario acceso a los datos almacenados en él.

Requisitos para el desarrollo del modelo de ML		
#	**Requisito**	**Componentes**
MML1	Facilidad de uso	Jupyter Lab junto con Python y librerías como pandas, sklearn o tensorflow, que son ampliamente utilizadas en el mundo del Machine Learning, ofrecen una experiencia intuitiva y ya conocida para los desarrolladores.
MML2	Versatilidad	Las librerías mencionadas anteriormente permiten el desarrollo de una amplia gama de modelos de Machine Learning.
MML3	Comunicación segura	La comunicación entre el usuario y los nodos se realizará a través de la APP y JupyterLab, asegurando una conexión segura mediante HTTPS en todo momento.
MML4	Rendimiento	AWS EC2 ofrece una amplia variedad de máquinas virtuales con diferentes capacidades de procesamiento y almacenamiento, asegurando un rendimiento óptimo para el desarrollo y ejecución de modelos de Machine Learning.

Requisitos para el desarrollo del modelo de FL		
#	**Requisito**	**Componentes**
FL1	Facilidad de uso	Las herramientas desarrolladas por Acuratio para el Federated Learning utilizan las librerías anteriormente mencionadas de Python, facilitando así la transición para los desarrolladores entre los modelos locales y los federados.
FL2	Versatilidad	Acuratio ofrecerá librerías que permitan federar modelos de redes neuronales y XGboost, así como realizar pipelines de entrada y tratamientos de datos de forma distribuida
FL3	Comunicación segura	En sus librerías Acuratio implementará medidas de seguridad y encriptación para impedir que ningún nodo o servidor pueda inferir nada de los datos de entrenamiento de otros nodos.
FL4	Rendimiento	Acuratio implementará algoritmos de eficiencia y compresión de las comunicaciones dentro de sus librerías de Federated Learning.

5. Diseño detallado de la solución

5.1. Recolección de Datos

En este caso se describen los elementos de toma de los datos que serán analizados por elsoftware de FML.

Sistema de toma de datos local (Sistema de control):

Sensores 0-10V y 4-20 mA: Estos sensores son esenciales para la monitorización de ciertos parámetros críticos en el entorno industrial. El rango de voltaje de 0-10V y la corriente de 4-20 mA son estándares comunes en la instrumentación industrial debido a su fiabilidad y precisión en la medición de variables como temperatura, presión, nivel, entre otros. En el contexto del proyecto MLEDGE, la integración de estos sensores ya ha sido previamente realizada, y su funcionalidad está completamente establecida. Por lo tanto, no se requiere ningún desarrollo adicional durante la ejecución del proyecto. Estos sensores proporcionan datos fundamentales para la toma de decisiones informadas en tiempo real sobre el rendimiento y la eficiencia de los procesos industriales.

PLC: Los PLCs (Controladores Lógicos Programables) son ampliamente utilizados en entornos industriales para el control y la automatización de procesos. Estos dispositivos son vitales para garantizar la operación segura y eficiente de maquinaria y sistemas complejos. En el contexto del proyecto MLEDGE, se aprovechará la infraestructura existente de PLCs sin necesidad de desarrollar nuevos dispositivos o funcionalidades específicas. Los PLCs de proporcionan una plataforma robusta y confiable para la ejecución de lógica de control y la gestión de dispositivos en tiempo real, lo que contribuye significativamente a la optimización de los procesos industriales sin requerir modificaciones adicionales durante la fase de implementación del proyecto.

Protocolo Modbus para Integrar Caudalímetros elementos de medición: El protocolo Modbus es un estándar de comunicación ampliamente utilizado en entornos industriales para la integración de dispositivos y sistemas heterogéneos. En el contexto del proyecto MLEDGE, el protocolo Modbus ya ha sido implementado para la integración de caudalímetros de vapor y gas en el sistema. Este protocolo proporciona una interfaz de comunicación confiable y eficiente que permite la adquisición de datos de caudal en tiempo real desde múltiples dispositivos distribuidos en la planta industrial. Dado que la funcionalidad de comunicación mediante el protocolo Modbus se considera completa y satisfactoria, no se requerirá ningún desarrollo adicional en este aspecto durante la fase de ejecución del proyecto. La integración exitosa de los caudalímetros de vapor y gas a través del protocolo Modbus es fundamental para la monitorización y el control precisos de los flujos de fluidos en la planta industrial, lo que contribuye a mejorar la eficiencia operativa y reducir los costes de producción.

5.2. Transmisión y Protección de Datos

Para la transmisión de las máquinas hasta los nodos, proponemos implementar un sistema que aprovecha la infraestructura de Amazon Web Services (AWS) para gestionar este tránsito de manera segura y efectiva.

El proceso comienza con el controlador lógico programable (PLC) de la caldera, que recopila datos en tiempo real con sensores que monitorean aspectos del funcionamiento de la caldera. Una vez que el PLC ha recopilado los datos, los envía de manera automatizada a una dirección de correo electrónico específica configurada en el sistema Simple Email Service (SES) de AWS. SES actúa como un servicio de correo electrónico altamente escalable y confiable que proporciona una forma segura de transferir los datos desde el entorno industrial hasta la infraestructura de AWS.

SES puede configurarse de forma que una vez que los datos llegan a la dirección de correo configurada, se redirigen automáticamente hacia un bucket de Amazon S3.

Amazon S3, como servicio de almacenamiento de objetos altamente escalable y duradero, proporciona un destino seguro y confiable para los datos recopilados de las calderas industriales. Los datos almacenados en Amazon S3 se cifran de forma predeterminada con cifrado del lado del servidor con claves administradas de Amazon S3 (SSE-S3), garantizando con este sistema de cifrado en reposo, la confidencialidad y la integridad de la información.

En la transmisión de datos desde S3 hasta los nodos de entrenamiento (instancias de EC2), son estos últimos los que deben pedirle los datos a S3 y este asegurarse de que quien se los pide es efectivamente un nodo de entrenamiento con permiso para ver esos datos. Existen varias capas de seguridad en AWS, algunas de ellas implementadas por defecto y otras opcionales:

1. **Utilizar HTTPS**: Cuando se accede a los datos de S3 desde una instancia de EC2, es recomendable utilizar el protocolo HTTPS para la transmisión de datos. HTTPS cifra la conexión entre el bucket de S3 y la instancia de EC2, lo que garantiza que los datos transmitidos estén protegidos contra la interceptación y la manipulación por parte de terceros. Las llamadas a S3 se harán a través de la API de AWS para Python (boto3) que ya tiene incluida la protección HTTPS.
2. **Autenticación y Autorización**: Configurar adecuadamente los permisos de acceso en S3 y en la instancia de EC2 es esencial para garantizar que solo las instancias autorizadas puedan acceder a los datos. Se utilizarán políticas de IAM (Identity and Access Management) para restringir el acceso a los buckets y objetos de S3, y asegurarse de que solo las instancias de EC2 autorizadas tengan acceso a estos recursos. Si fuera necesario podría crearse un bucket de S3 para cada caldera y que cada instancia de EC2 tuviera acceso a su propio bucket, aumentando así la seguridad de los datos.
3. **Utilizar VPC Endpoints o Gateways de Internet**: Si la instancia de EC2 y el bucket de S3 están en la misma región de AWS, se podría utilizar la red virtual privada (VPC) para acceder a S3 directamente sin necesidad de atravesar Internet público. Esto reduce la exposición a posibles amenazas de seguridad.
4. **Cifrado de Datos**: Si se requiere un nivel adicional de seguridad, se puede cifrar los datos antes de transmitirlos desde S3 a la instancia de EC2. Puede utilizar el cifrado de cliente proporcionado (SSE-C) en S3 o implementar su propio cifrado antes de cargar los datos en S3.

Una vez que los datos están ya en el nodo de entrenamiento, se almacenarán en el disco con un cifrado en reposo. Amazon Elastic Block Store (EBS) proporciona almacenamiento persistente para los datos de las instancias de EC2 y permite crear, adjuntar, modificar y eliminar volúmenes de almacenamiento de forma dinámica según sea necesario. Será aquí donde estén guardados los datos de los nodos. Para que los datos estén cifrados se utilizará EBS Encryption. (EBS) ofrece la capacidad de cifrar los volúmenes de almacenamiento adjuntos a las instancias de EC2. El cifrado de EBS protege los datos almacenados en el volumen, incluidos el sistema operativo y los archivos de aplicación.

Si las instancias de EC2 no necesitan ningún volumen de almacenamiento más allá del disco raíz, se pueden utilizar imágenes de máquina (AMI) cifradas para lanzar instancias de EC2. Al lanzar una instancia desde una AMI cifrada, todos los datos almacenados en el disco raíz están automáticamente cifrados. AWS ofrece AMIs cifradas para varias distribuciones de sistemas operativos, como Amazon Linux en la cual se basarán las imágenes de Acuratio.

5.3. Desarrollo del modelo de ML

El desarrollo del modelo de ML tiene como objetivo principal transformar los datos recopilados en información valiosa que permita la optimización del rendimiento, identificación de anomalías y predicción de mantenimientos en calderas de vapor y otros equipos industriales.

El desarrollo del modelo inicial se hará teniendo en cuenta la necesidad de federar su entrenamiento en la siguiente fase. Por lo tanto, se considerarán las restricciones que suelen darse en entornos distribuidos para la selección del algoritmo y el procesamiento de datos.

El desarrollo del modelo se llevará a cabo en los nodos de Acuratio. Se ofrecen dos modalidades fundamentales de interacción con los nodos. La primera, a través de la interfaz integrada en la aplicación, destaca por su simplicidad y facilidad de uso, si bien presenta ciertas limitaciones en cuanto a su alcance funcional. En el caso del desarrollo del modelo de ML nos centraremos en la conexión a través de Jupyter Lab ya que es la que más flexibilidad proporciona a la hora de poder ejecutar código de python sobre los nodos.

Este desarrollo se hará enteramente en Python programando sobre notebooks de Jupyter Lab.

Por un lado, Python es el lenguaje de programación elegido debido a que es un lenguaje versátil que se puede utilizar para una amplia variedad de tareas, desde la limpieza y preparación de datos hasta el desarrollo de modelos avanzados de ML. Esto permite a los analistas de datos trabajar en un entorno familiar y utilizar las mismas herramientas para diferentes aspectos de su trabajo.

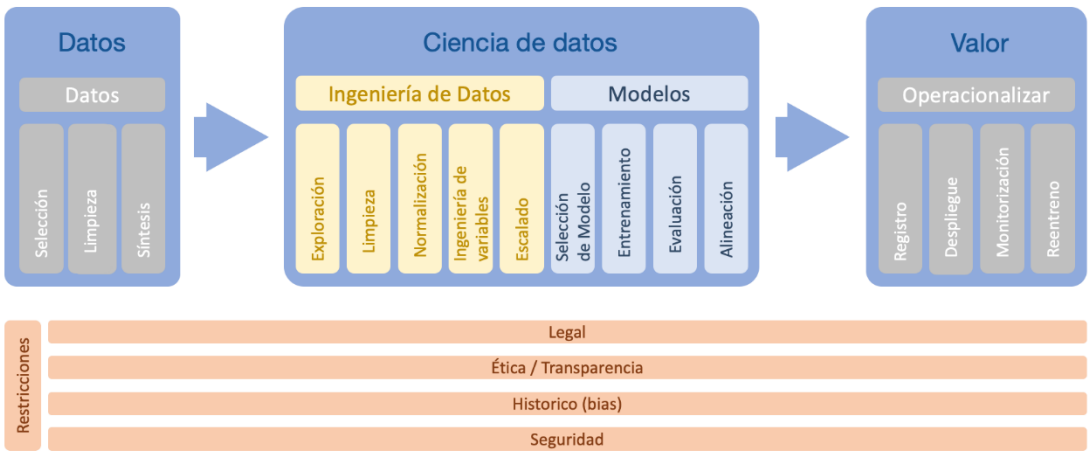
Además, al ser uno de los lenguajes más usados en análisis de datos, cuenta con una amplia comunidad de desarrolladores que han creado una amplia gama de bibliotecas especializadas en este sector, como Pandas, NumPy, SciPy, Scikit-learn, Matplotlib y Seaborn. Estas bibliotecas ofrecen herramientas poderosas y eficientes para manipular datos, realizar cálculos estadísticos, visualizar información y desarrollar modelos de aprendizaje automático. Los nodos de Acuratio tendrán incorporadas todas estas librerías, además de otras más específicas para el entrenamiento de modelos de ML como Tensorflow o XGboost. Además, existirá la posibilidad de instalar librerías nuevas en cualquier nodo si fuera necesario.

La amplia comunidad con la que cuenta Python también ayuda a que siempre haya ayuda disponible on-line cuando se busca información sobre desafíos técnicos o se necesita orientación en el análisis de datos.

Por otro lado, desarrollar sobre notebooks de Jupyter en lugar de escribir código en scripts de Python también lleva asociadas diferentes ventajas entre las que se encuentran:

1. **Interactividad**: Los notebooks de Jupyter permiten ejecutar y modificar código de manera interactiva, lo que facilita la exploración de datos y la experimentación con diferentes algoritmos y técnicas.
2. **Documentación del código**: Los notebooks de Jupyter permiten combinar código ejecutable con texto explicativo, imágenes y gráficos, lo que facilita la creación de documentos interactivos que pueden ser utilizados para la presentación y comunicación de resultados.
3. **Colaboración**: Los notebooks de Jupyter son archivos que pueden ser compartidos fácilmente entre diferentes usuarios, lo que facilita la colaboración en proyectos de programación y análisis de datos. Almacenar el código y los resultados de un análisis en un notebook de Jupyter facilita la reproducibilidad de los experimentos, ya que permite a otros investigadores ejecutar el mismo código y obtener los mismos resultados.
4. **Visualización de datos integrada**: Los notebooks de Jupyter incluyen herramientas integradas para la visualización de datos, lo que facilita la creación de gráficos y visualizaciones interactivas para explorar y comunicar los resultados de un análisis.

Fig. 10 – *Etapas de entrenamiento y puestas en producción*



En la figura se muestra un esquema clásico de las etapas de las que consta el entrenamiento y puesta en producción de un modelo de ML. En los siguientes puntos se profundizará brevemente en las etapas más significativas para este caso de uso.

1. **Selección de Variables**: El ingeniero experto del sector, el desarrollador software y el experto en ML y FL colaborarán para seleccionar las variables que se incluirán en el modelo. Esta etapa se desarrollará en Python, usando librerías como pandas, Scikit-learn o Matplotlib para identificar las variables más relevantes.
2. **Limpieza de Datos**: Antes de usar los datos para entrenar el modelo, es esencial que estos pasen por un proceso de limpieza para eliminar valores atípicos o datos incompletos que puedan sesgar el modelo. Una vez seleccionadas las variables más

relevantes, el resto se eliminarán. La limpieza de las variables seleccionadas se hará con la librería pandas, que ofrece muchas funcionalidades para limpiar datos.

3. **Separación de Datos**: Los datos se dividirán en conjuntos de entrenamiento, validación y prueba. Esto permite evaluar la eficacia del modelo en datos que no ha visto antes. Los nodos de Acuratio llevarán incorporada la librería sklearn de Python que contiene funciones para realizar este paso.
4. **Elección del Algoritmo**: El experto en ML y FL elegirá los algoritmos más adecuados para los casos de uso. Pueden incluir algoritmos de regresión, clasificación o detección de anomalías. La selección de un algoritmo estará restringida a aquellos algoritmos que puedan federarse en la siguiente fase. Por parte de Acuratio se proporcionarán algoritmos federados para el entrenamiento de modelos de redes neuronales, XGBoost y detección de anomalías.
5. **Entrenamiento del Modelo**: Utilizando el conjunto de entrenamiento, el modelo se entrena para identificar patrones y hacer predicciones o clasificaciones. Los nodos de Acuratio llevarán incorporadas librerías como Tensorflow, XGBoost o Scikit-learn para poder implementar localmente el modelo por el que se haya optado.
6. **Afinamiento de Parámetros**: Después del entrenamiento inicial, se ajustarán los parámetros del modelo para optimizar su rendimiento, utilizando el conjunto de validación. Se podrán ejecutar procesos de validación cruzada y búsqueda de hiper-parámetros para ajustar el modelo lo máximo posible.
7. **Evaluación del Modelo**: El modelo se evaluará para determinar su eficacia, usando el conjunto de prueba.
8. **Implementación**: Una vez que el modelo ha sido evaluado y afinado, se implementará en el entorno de producción para comenzar a hacer predicciones en tiempo real.

Tipos de Modelo propuestos:

La gestión eficiente de la producción y consumo de vapor se ha vuelto esencial en numerosos procesos industriales, donde su optimización se traduce en una ventaja competitiva. En este contexto, la previsión de producción de vapor emerge como un aspecto crítico para garantizar el rendimiento óptimo de las calderas industriales. A través de la aplicación de técnicas avanzadas, como el análisis de series temporales y el empleo de redes neuronales, podemos desarrollar un modelo predictivo sólido capaz de anticipar con precisión las fluctuaciones en la demanda de vapor.

El óptimo funcionamiento de las calderas de vapor puede comprometerse si la producción de vapor no coincide con los parámetros para los que la máquina se configura al principio. En este contexto, contar con una predicción certera del rendimiento en función de la configuración de la máquina y su producción de vapor se vuelve fundamental. Esta anticipación permite ajustar la configuración de la máquina de manera proactiva ante posibles variaciones en la producción, ya sea un aumento o una disminución, que puedan impactar su rendimiento.

La capacidad de anticipar estas variaciones y ajustar la configuración de la máquina no solo optimiza su rendimiento, sino que también conduce a una reducción significativa en el consumo de energía. Al prever y adaptarse a cambios en la producción de vapor, se logra una operación más eficiente y sostenible de las calderas industriales, lo que se traduce en beneficios tanto económicos como ambientales para la empresa.

Para abordar estos desafíos, proponemos la adopción de una arquitectura de redes neuronales recurrentes (RNN), reconocida por su eficacia en la modelación de datos

secuenciales como las series temporales. En esta categoría, destacan modelos como las Memorias a Corto y Largo Plazo (LSTM) o las Unidades Recurrentes de Puerta (GRU), reconocidos por capturar relaciones temporales complejas y adaptarse dinámicamente a patrones cambiantes en los datos.

Las variables de entrada para estos modelos incluyen: el caudalímetro de vapor, el caudalímetro de agua de alimentación de la caldera, el cuantómetro de gas con corrección PT, las sondas de temperatura del agua de alimentación, de los humos de la chimenea, del depósito de condensados, del ambiente de entrada de aire al quemador, el contador de agua de llenado y la sonda de temperatura del agua de llenado.

Se implementarán dos modelos principales de análisis de series temporales. Uno de ellos tendrá como output el rendimiento de la caldera y el otro la producción de vapor.

Los resultados de esta fase serán de dos tipos:

- Los propios modelos, que una vez entrenados podrá guardarse su configuración para poder cargarla en el futuro.
- Predicciones de los modelos.

En principio ambas cosas se guardarán en el sistema de almacenamiento de cada máquina (EBS) pudiendo subirse a S3. Si fuera necesario para poder desarrollar alguno de los puntos de este proyecto se valorará poder transferir estos datos a algún otro lugar.

5.4. Implementación de Federated Learning (FL)

En esta fase se tomará el modelo diseñado de manera local en el punto anterior y se llevará a un entorno federado, para ello, y dependiendo de cuál sea el tipo de modelo a implementar, se ofrecen tres alternativas.

Redes Neuronales

Si el modelo elegido fuera una red neuronal (para detección de anomalías, por ejemplo), se proponen dos opciones para federarlo: Split Horizontal y Federated Averaging. En las siguientes líneas se procederá a explicar cada una de ellas.

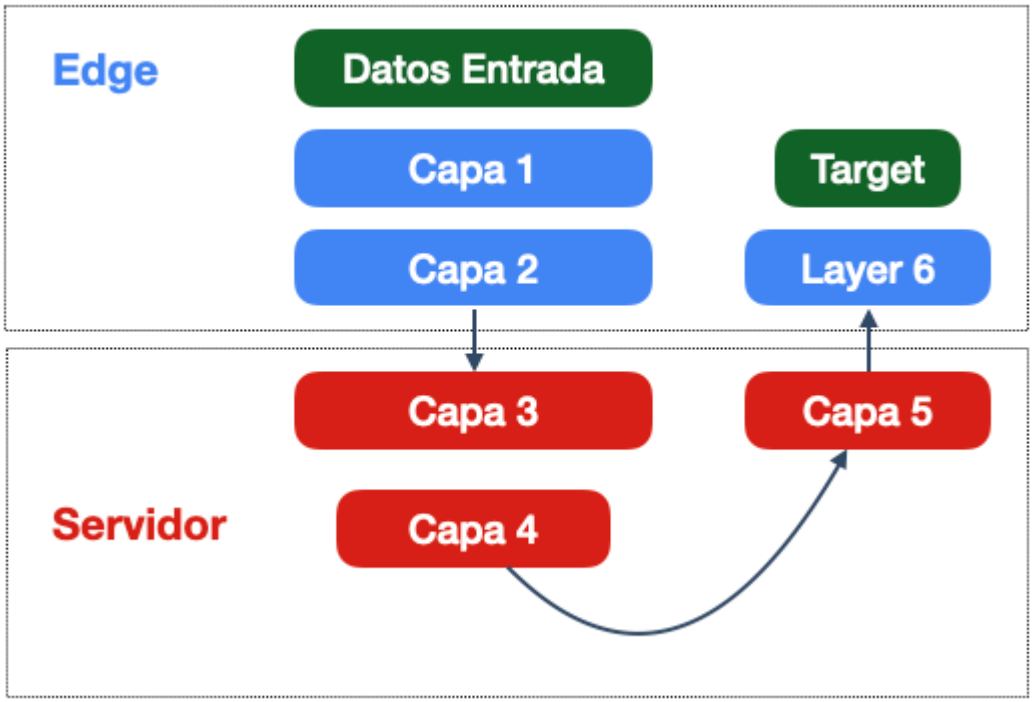
Split Horizontal

Este método de entrenamiento federado consiste en dividir la red neuronal en varias partes que serán ejecutadas y entrenadas por distintos actores.

Arquitectura

La arquitectura de la red se divide en tres partes distintas: la entrada de datos seguida de varias capas iniciales (cuantas más capas, más robusto es el método), una serie de capas intermedias en el servidor central y finalmente unas pocas capas más junto con la salida de la red. Tanto la primera como la tercera parte se despliegan en el borde (Edge), replicadas en cada dispositivo que almacena los datos. Mientras tanto, la parte intermedia reside en un servidor central.

Fig. 11 – *Split horizontal*



En la imagen se muestra un caso de Split horizontal. Cada dispositivo o nodo en el edge va rotando cada cierto tiempo.

Proceso de entrenamiento
Durante el proceso de entrenamiento, uno de los nodos que posee datos inicia la propagación hacia adelante (*forward propagation*), introduciendo un conjunto de datos (*batch*) en la red neuronal. Estos datos son computados a través de las capas iniciales de la red, siguiendo la arquitectura establecida, lo que genera una salida. Esta salida se transmite al servidor central, donde también pasa por sus propias capas y luego se devuelve al nodo inicial. El nodo completa la propagación hacia adelante por las capas restantes, generando así una salida final del modelo y calculando el error asociado. A partir de este punto, se inicia el proceso de retro propagación (*back propagation*) para actualizar los pesos de todas las etapas de la red neuronal. Los errores se van propagando hacia atrás de las últimas capas del nodo, hasta el servidor central y de allí de vuelta a las primeras capas del nodo. Una vez terminado este proceso, el nodo envía sus pesos al siguiente nodo de la red, de forma que el servidor central va repitiendo el proceso con los diferentes nodos.

Seguridad
La salida generada, que sirve como entrada para la siguiente etapa del modelo en el servidor central, representa los datos de entrada en un espacio vectorial completamente diferente. Además, es el resultado de una serie de transformaciones no lineales. Esto significa que incluso para un hipotético servidor malicioso, sería imposible recuperar la entrada original del modelo a partir de los vectores recibidos, debido a la complejidad de las transformaciones aplicadas.

Federated Averaging

Arquitectura

A diferencia de Split Horizontal que tenía una arquitectura más complicada, en este caso todos los nodos tienen al principio la misma representación exacta de toda la red. La arquitectura del entrenamiento de una red neuronal con Federated Averaging se divide en los siguientes componentes:

- **Servidor Central**: Este componente coordina el entrenamiento de la red neuronal y almacena el modelo global. Inicializa el proceso de entrenamiento, envía la arquitectura del modelo a los nodos participantes y realiza la agregación de los modelos actualizados después de cada iteración.
- **Nodos Participantes**: Cada nodo representa un dispositivo o entidad con datos locales. Estos nodos realizan el entrenamiento en sus datos locales utilizando la arquitectura del modelo proporcionada por el servidor central. Después de cada iteración de entrenamiento local, los nodos envían las actualizaciones de los pesos del modelo al servidor central.

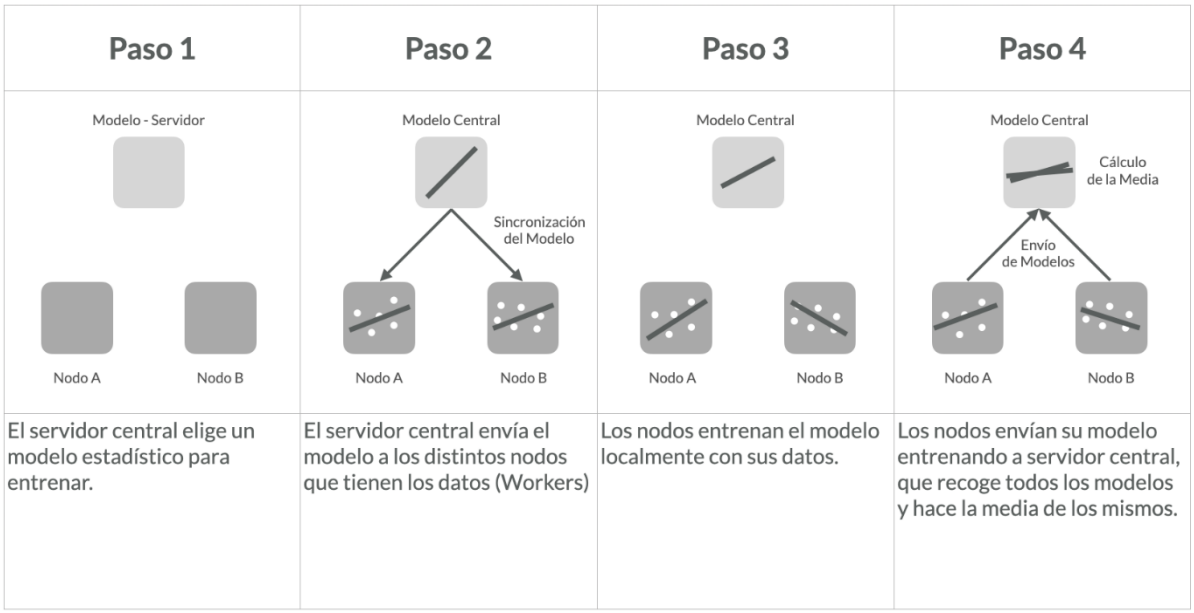
Proceso de entrenamiento

El entrenamiento en cada nodo no difiere de lo que es el entrenamiento de una red neuronal local. Lo que lo diferencia es la agregación de las actualizaciones de los pesos en el servidor cada cierto número de pasos de entrenamiento a elección del usuario. En los siguientes pasos se detalla un poco más en profundidad como es este proceso:

1. Inicialmente, se inicializan los pesos del modelo de manera aleatoria en todos los nodos participantes.
2. En cada nodo seleccionado, se realiza la propagación hacia adelante con los datos locales. Esto implica que cada nodo calcula las activaciones de cada capa del modelo y genera una salida predicha para un conjunto de datos local. Después calcula el error y actualiza los pesos de su red. Este paso se repite en cada nodo tantas veces como sea necesario hasta llegar al número de pasos de entrenamiento en los que se va a realizar la agregación.
3. Las actualizaciones de los pesos del modelo se envían desde cada nodo al servidor central. Estas actualizaciones pueden ser los gradientes del error local o los nuevos pesos del modelo después de aplicar un algoritmo de optimización local, como el descenso de gradiente estocástico.
4. En el servidor central, se promedian las actualizaciones de los pesos recibidos de todos los nodos participantes. Este promedio ponderado tiene en cuenta el tamaño del conjunto de datos local en cada nodo para garantizar una ponderación adecuada de cada actualización.
5. Utilizando el promedio ponderado de las actualizaciones de los pesos, se actualizan los pesos del modelo global en el servidor central. Estos nuevos pesos se envían de vuelta a los nodos, de forma que todos empiezan la siguiente iteración con los mismos pesos.
6. Los pasos 2 a 5 se repiten durante varias rondas de entrenamiento, permitiendo que el modelo global se ajuste gradualmente a los datos distribuidos en los nodos participantes.

7. Una vez que se completa un número predeterminado de rondas de entrenamiento o se alcanza un cierto criterio de convergencia, el entrenamiento se considera completo y se puede utilizar el modelo global para realizar predicciones en nuevos datos.

Fig. 12 – *Resumen del entrenamiento de Federated Averaging*



Resumen gráfico del entrenamiento en Federated Averaging.

Seguridad

Si bien Federated Averaging puede ofrecer beneficios significativos en términos de privacidad y seguridad al entrenar modelos en entornos distribuidos, también es importante considerar y mitigar los posibles riesgos de seguridad asociados con este enfoque. Por ejemplo, podría existir el riesgo de que los datos locales en los nodos participantes puedan contener información sensible o privada. Aunque Federated Averaging está diseñado para preservar la privacidad de los datos locales al no compartirlos directamente, aún existe la posibilidad de que la información sensible se filtre a través de las actualizaciones de los pesos del modelo. Para evitar este riesgo, Acuratio implementará dos tipos de algoritmos que aporten seguridad:

- Compresión de los pesos: Comprimir las actualizaciones de los pesos cuantizandolos a valores concretos no sólo dificulta enormemente obtener información de los datos que han causado esas actualizaciones. La compresión de los pesos en las actualizaciones de un modelo neuronal tiene varios beneficios adicionales, como mejorar el rendimiento al reducir el tamaño de las comunicaciones nodo-servidor y potencialmente ayudar en la regularización de los pesos para una mejor generalización del modelo al final del entrenamiento.
- Protocolo de agregación segura (PAS): El Protocolo de Agregación Segura (PAS) es una técnica que garantiza que el servidor no pueda aprender nada de las actualizaciones recibidas de los nodos. Esto se logra encriptando las actualizaciones utilizando protocolos de Computación Segura entre Partes. Así, las actualizaciones encriptadas son irreconocibles para el servidor, pero el resultado de la agregación sigue siendo el mismo que si las actualizaciones estuvieran desencriptadas.

Es importante destacar que el PAS es compatible con la compresión de los pesos mencionada anteriormente. Esto significa que las actualizaciones pueden ser comprimidas antes de ser encriptadas, lo que proporciona una capa adicional de seguridad y eficiencia en la comunicación entre los nodos y el servidor, sin comprometer la integridad de los datos ni el rendimiento del modelo.

Pros y contras de cada método

Al considerar los métodos de entrenamiento, la distinción clave entre ambas opciones se centra en los requisitos de computación en los nodos y el nivel de comunicación necesario. El enfoque de Split Horizontal se adapta especialmente a aplicaciones relacionadas con el Internet de las Cosas (IoT), donde los nodos tienen limitaciones en términos de capacidad de computación para entrenar redes neuronales extensas. En este escenario, los nodos se encargan de entrenar una fracción del modelo, mientras que la mayor parte del procesamiento recae en el servidor central. Sin embargo, esta configuración implica una comunicación frecuente entre el nodo y el servidor central en cada iteración de entrenamiento.

En Federated Averaging sin embargo el grueso de la computación se realiza en los nodos. Las comunicaciones entre nodos y servidor central ocurren con menor frecuencia, generalmente después de varias iteraciones de entrenamiento. Además, el diseño de la arquitectura es más simple en Federated Averaging en comparación con Split Horizontal.

Para el caso presente, que implica la implementación de un demostrador con datos y computación en la nube, Federated Averaging parece ser la opción más adecuada. No obstante, es importante tener en cuenta las ventajas que Split Horizontal podría ofrecer, especialmente cuando se valora la posibilidad de entrenar modelos, o al menos una parte de ellos, directamente en el hardware integrado en dispositivos como calderas u otras máquinas.

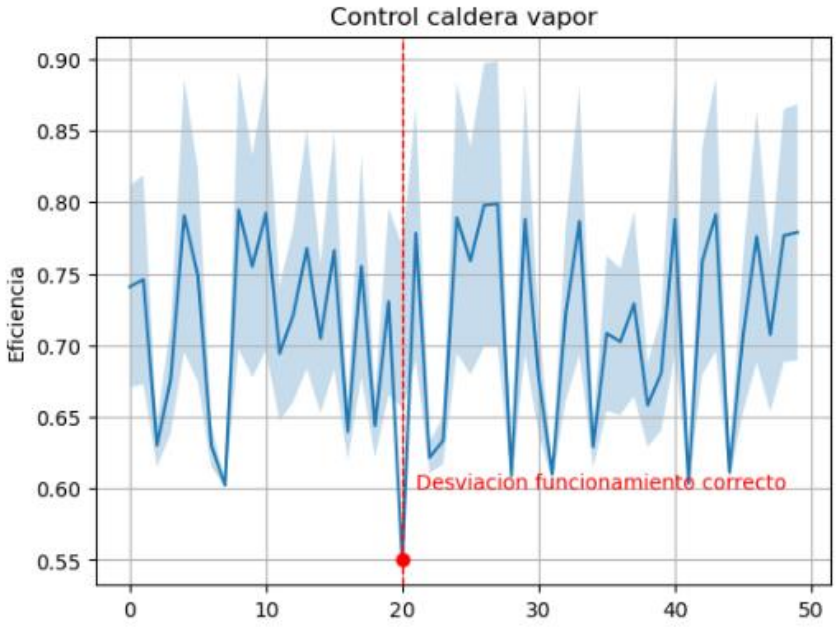
6. Demostrador

El proyecto MLEDGE se centra en mejorar la gestión de calderas de vapor mediante el uso de técnicas avanzadas de Machine Learning (ML) y Federated Learning (FL), soportadas por la adquisición de datos de un sistema de control local y complementadas con un robusto dashboard de exportación de datos. Estos modelos permiten analizar grandes volúmenes de datos operativos de las calderas para identificar patrones y anomalías que pueden afectar su rendimiento y eficiencia. Por ejemplo, pueden predecir fallos antes de que ocurran, optimizar el uso de combustible, y ajustar parámetros de operación en tiempo real para maximizar la eficiencia energética y prolongar la vida útil de las calderas.

Estos modelos permiten analizar grandes volúmenes de datos operativos de las calderas utilizando algoritmos de aprendizaje automático, los modelos procesan datos históricos y en tiempo real provenientes de sensores y sistemas de monitoreo instalados en las calderas. Esta capacidad de análisis avanzado permite detectar tendencias que podrían pasar desapercibidas mediante métodos tradicionales, revelando problemas incipientes que podrían llevar a fallos si no se abordan a tiempo.

Además, estos modelos pueden predecir fallos antes de que ocurran. Mediante técnicas de predicción y mantenimiento predictivo, se pueden anticipar eventos adversos basándose en signos tempranos de deterioro o funcionamiento anómalo. Al prever estos problemas, se pueden planificar intervenciones de mantenimiento preventivo, evitando paradas no programadas y costosos tiempos de inactividad.

Fig. 13 – *Representación gráfica de desviaciones dentro del modelo*



En términos de eficiencia, los modelos optimizan el uso de combustible ajustando los parámetros de operación de las calderas. Analizan el consumo de combustible en relación con la producción de vapor, identificando oportunidades para mejorar la combustión y reducir el desperdicio de energía. Esto no solo disminuye los costes operativos, sino que también contribuye a la sostenibilidad al reducir las emisiones de gases de efecto invernadero.

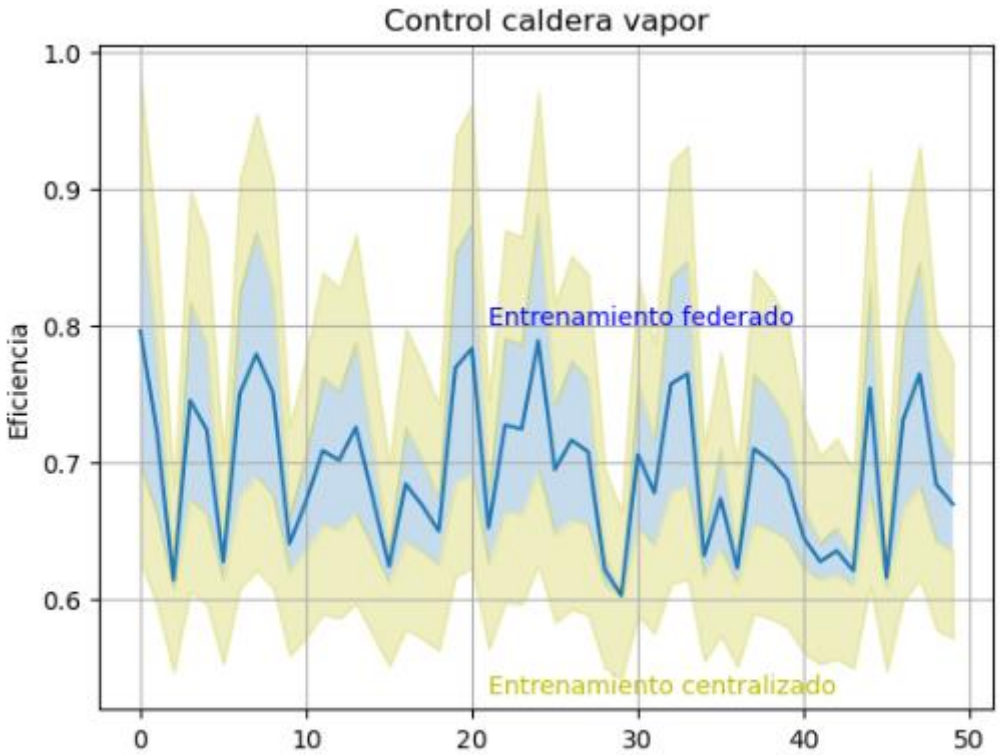
Finalmente, estos modelos ajustan los parámetros de operación en tiempo real para maximizar la eficiencia energética. Utilizan algoritmos adaptativos que responden a las condiciones cambiantes del entorno y las demandas de producción. Esta capacidad de ajuste dinámico no solo mejora la eficiencia energética, sino que también reduce el estrés y el desgaste de los componentes de la caldera, prolongando su vida útil.

En conjunto, la integración de estos modelos con el dashboard de exportación y el sistema de control local permite una gestión avanzada y eficiente de las calderas, asegurando su rendimiento óptimo y una operación sostenible a largo plazo.

Este dashboard mostrará el consumo histórico y esperado de las calderas, tanto en graficas como en datos tabulares para su análisis. Estos datos se generarán de manera sintética en base a los datos históricos reales. El dashboard mostrará estimaciones de consumo durante la próxima semana y el tiempo esperado para la próxima intervención de mantenimiento en función de la eficiencia esperada.

Como demostrador final del proyecto, en la parte concerniente a los modelos desarrollados, se llevará a cabo una exhaustiva comparativa entre modelos de Machine Learning centralizados y federados. Esta comparativa evaluará el rendimiento y la precisión de los modelos en ambas arquitecturas, analizando cómo cada enfoque maneja los datos y optimiza los resultados. Se presentarán gráficas como la mostrada en la figura comparando las desviaciones respecto a los rendimientos reales de las máquinas de los modelos locales y federados.

Fig. 14 – *Representación gráfica comparativo entrenamiento federado vs centralizado*



La comparativa incluirá una serie de herramientas visuales y analíticas para ilustrar las diferencias y ventajas de cada enfoque. Se presentarán gráficas que mostrarán la precisión de las predicciones en cada caso. También se utilizarán tablas comparativas para detallar

métricas clave como el tiempo de entrenamiento o el uso de recursos computacionales y de comunicaciones.

Y como valor final y diferenciador de este aplicativo, se buscará una mejora real en la operativa y en los tiempos de respuesta a los clientes que implemente este modelo, creando protocolos de actuación dentro del departamento de mantenimiento de calderas a tiempo real a través de reportes en formato alerta de incidencia al cliente o a un sistema de supervisión y monitorización centralizado desde el cual se coordinará la actuación requerida ya sea de un técnico de Inmarepro S.L. o de un responsable en la planta del cliente.

Con base en este protocolo, ya no solo se pone el valor el dato, sino que se hace una acción anticipada para generar un menor impacto en costes económicos, operativos y medioambientales para el cliente.

7. Conclusión

La implementación del proyecto MLEDGE se encamina a desarrollar una solución avanzada para la optimización de la eficiencia energética en entornos industriales mediante el uso de técnicas de aprendizaje automático federado. Esta tecnología busca abordar los desafíos de privacidad y seguridad de los datos mientras mejora el rendimiento de equipos críticos como las calderas de vapor.

En la actualidad, la producción de vapor es un proceso crucial pero intensivo en energía y difícil de descarbonizar a corto plazo. Las calderas de vapor, esenciales en sectores como el farmacéutico y alimentario, a menudo operan de manera ineficiente debido a la falta de monitoreo continuo y ajustes técnicos realizados solo durante visitas periódicas de mantenimiento. Esta situación reactiva lleva a costes operativos elevados y un significativo desperdicio energético.

MLEDGE pretende transformar esta realidad mediante el desarrollo de un sistema que optimice el funcionamiento de las calderas en diversas industrias, utilizando tecnología de aprendizaje federado. Este sistema permitirá predecir y detectar desviaciones en el rendimiento de las calderas antes de que los costes energéticos aumenten o se produzcan fallas que interrumpan la producción. La solución ofrecerá recomendaciones precisas basadas en datos agregados de múltiples instalaciones, sin comprometer la privacidad de los datos.

La arquitectura técnica propuesta para el proyecto combina hardware y software para maximizar la eficiencia operativa y la toma de decisiones. Los sensores instalados en las calderas recopilarán datos críticos en tiempo real, gestionados por Controladores Lógicos Programables (PLCs) utilizando el protocolo Modbus. Los datos serán transmitidos de manera segura utilizando la infraestructura de Amazon Web Services (AWS) y almacenados en Amazon S3, donde se cifrarán para garantizar su seguridad. Los nodos de procesamiento, utilizando instancias EC2 con almacenamiento cifrado en Elastic Block Store (EBS), accederán a estos datos para su análisis.

Los modelos de Machine Learning se desarrollarán y entrenarán localmente en los nodos utilizando herramientas como JupyterLab y librerías de Python. Posteriormente, se implementará el aprendizaje federado para agregar los conocimientos de múltiples nodos sin necesidad de compartir datos sensibles. Dependiendo del tipo de modelo, se utilizarán métodos como Split Horizontal, que distribuye el entrenamiento de las redes neuronales entre los nodos y el servidor central, y Federated Averaging, que promedia los pesos de los modelos entrenados en los nodos para actualizar el modelo global. Se implementarán medidas de seguridad como el cifrado de datos en tránsito y en reposo, protocolos de comunicación seguros y la agregación segura de actualizaciones de modelos para prevenir la exposición de datos sensibles.

El proyecto espera demostrar que la aplicación del aprendizaje federado en la industria es viable y altamente beneficiosa. La solución MLEDGE tiene el potencial de optimizar el rendimiento energético de las calderas, reduciendo costes operativos y emisiones de gases de efecto invernadero. Además, establecerá una plataforma escalable que puede extenderse a otros equipos y procesos industriales, como sistemas de generación de aire comprimido o refrigeración industrial.

En resumen, MLEDGE apunta a contribuir significativamente a la sostenibilidad y la reducción de emisiones, a la vez que potencia la competitividad industrial y fomenta la innovación en la gestión de recursos energéticos. La implementación de esta solución representará un paso importante hacia una industria más eficiente y sostenible, con un impacto positivo en la economía y el medio ambiente.