PROPUESTA DE MEJORA PARA EL MANEJO DE FALSOS POSITIVOS EN EL AREA DE ANALITICA DE DATOS DE LA EMPRESA SLB

MARIA ISABEL PATIÑO PEREZ

PROGRAMA DE INGENIERIA DE TELECOMUNICACIONES

UNIVERSIDAD SANTO TOMAS

BOGOTA D.C.

2024

PROPUESTA DE MEJORA PARA EL MANEJO DE FALSOS POSITIVOS EN EL AREA DE ANALITICA DE DATOS DE LA EMPRESA SLB

MARIA ISABEL PATIÑO PEREZ

MONOGRAFÍA PARA OPTAR AL TÍTULO DE INGENIERA DE TELECOMUNICACIONES

DIRIGIDO POR:

ING. GUSTAVO ALONSO CHICA

PROGRAMA DE INGENIERIA DE TELECOMUNICACIONES

UNIVERSIDAD SANTO TOMAS

BOGOTA D.C.

2024

Índice

LISTADO DE ILUSTRACIONES

LISTADO DE TABLAS

Agradecimientos

En primer lugar, les agradezco a mis padres, quienes me han brindado siempre su apoyo incondicional para poder cumplir todos mis objetivos personales y académicos. Ellos son los que con su amor y cariño me han impulsado incansablemente a perseguir mis metas y a nunca rendirme ante las adversidades. Además, me han proporcionado el respaldo económico necesario para dedicarme plenamente a mis estudios sin interrupciones. Les estaré eternamente agradecida por el invaluable esfuerzo que han realizado durante estos cinco años, esfuerzo que me ha llevado a estar a un paso de obtener mi título.

Asimismo, deseo expresar mi agradecimiento a mi tutor, Gustavo Chica, por su dedicación y paciencia. Sin su guía, no habría sido posible alcanzar esta meta tan anhelada. También quiero agradecer a todos los docentes que han sido parte de mi trayectoria universitaria, les agradezco por transmitirme los conocimientos necesarios para estar aquí hoy.

Finalmente, quiero agradecer a mis compañeros muchos de los cuales se han convertido en amigos. Gracias por las horas compartidas, los trabajos realizados en conjunto y las historias vividas, su apoyo y amistad han hecho de esta experiencia algo inolvidable.

Resumen

El presente documento plantea un plan de mejora continua para el área de análisis de datos en la empresa SLB. El objetivo principal es reducir los falsos positivos en la detección de alarmas basándose en las mejores prácticas de ITIL v4, este proyecto se desarrolló durante un período de prácticas llevadas a cabo en SLB entre julio de 2023 y enero de 2024.

En la actualidad, SLB ha estado implementando tecnologías como la inteligencia artificial y el análisis de datos para optimizar sus procesos. No obstante, se ha enfrentado a dificultades relacionadas con un sistema de alarmas que, debido a su alta tasa de falsos positivos, dificulta la toma de decisiones rápidas y confiables. Este sistema, utilizado para gestionar alarmas en maquinaria y equipos de la industria petrolera resulta poco eficaz cuando genera un exceso de alertas incorrectas.

La propuesta incluye medidas específicas para proporcionar ventajas y orientación con el objetivo de mejorar la precisión y confiabilidad del sistema de alarmas. Esto permitiría a los ingenieros responsables de las cuadrillas identificar problemas reales sin detener la maquinaria. Como resultado, se espera una mayor eficiencia operativa y una reducción del tiempo de inactividad innecesario, lo que contribuirá a la productividad y al ahorro de costos en SLB.

Palabras clave: Analítica de datos, datos, falsos positivos, ITIL v4, DBSCAN

Abstract

This document presents a continuous improvement plan for the data analysis area in the SLB company. The main objective is to reduce false positives in alarm detection based on ITIL v4 best practices, this project was developed during an internship period carried out at SLB between July 2023 and January 2024.

Currently, SLB has been implementing technologies such as artificial intelligence and data analytics to optimize its processes. However, it has faced difficulties related to an alarm system that, due to its high false positive rate, makes it difficult to make quick and reliable decisions. This system, used to manage alarms on machinery and equipment in the oil industry is ineffective when it generates an excess of incorrect alerts.

The proposal includes specific measures to provide benefits and guidance to improve the accuracy and reliability of the alarm system. This would allow engineers responsible for crews to identify real problems without shutting down machinery. As a result, increased operational efficiency and a reduction in unnecessary downtime is expected, which will contribute to productivity and cost savings in SLB.

Keywords: false positive, **ITIL v4, DBSCAN, data analytics, data**

Introducción

En un panorama energético en constante cambio, la industria petrolera se encuentra en un momento decisivo. La transformación digital surge como la fuerza impulsora para optimizar operaciones, mejorar la eficiencia y enfrentar los desafíos del futuro. SLB, uno de los lideres a nivel mundial en servicios petroleros está a la vanguardia de esta revolución, ofreciendo un conjunto integral de soluciones para impulsar la transformación digital en el sector.

A través de su amplia gama de servicios, SLB empodera a las organizaciones a adoptar tecnologías digitales de manera efectiva maximizando su impacto en el rendimiento y la rentabilidad. Desde consultoría especializada hasta la implementación de soluciones escalables, SLB acompaña a sus clientes en cada paso del camino hacia la transformación digital [1].

La analítica de datos es el pilar fundamental de la estrategia de transformación digital de SLB. En este sentido, la empresa aprovecha el poder de la inteligencia artificial para procesar y analizar grandes conjuntos de datos generados por maquinaria y equipos, extrayendo información valiosa que optimiza la toma de decisiones y mejora la eficiencia.

A pesar de los grandes avances logrados por la empresa en la implementación de tecnologías, aún persisten pequeños errores relacionados con la identificación y manejo de falsos positivos generados por el sistema; estos errores afectan la confiabilidad y eficiencia del sistema de alarmas utilizado para monitorear maquinaria y equipos en la industria petrolera.

En este documento, se presenta una propuesta de mejora basada en el análisis de las actividades realizadas durante la pasantía llevada a cabo entre julio de 2023 y enero de 2024. Durante este período, se adquirieron conocimientos y se enfrentaron diversos retos, entre los que se destacan:

- Aprendizaje de nuevas tecnologías
- Manejo de grandes bancos de datos
- Superar el miedo a proponer soluciones e ideas

- Gestión de la presión
- Aprendizaje de algoritmos como DBSCAN

Estos aprendizajes contribuyeron al desarrollo personal y profesional, reforzando la importancia de mantenerse a la vanguardia tecnológica. Aunque no siempre se tiene la respuesta inmediata, la confianza y la perseverancia son clave para alcanzar los objetivos y brindar soluciones efectivas a las necesidades del cliente. Todo ello, con la mejor actitud y responsabilidad en el cumplimiento de los proyectos.

1. Marco contextual del proyecto

Con el fin de proporcionar claridad sobre los temas tratados en este documento, esta sección incluye una descripción detallada del problema a resolver y aborda tanto la relevancia como el alcance que tendrá este documento.

1.1 Planteamiento del problema

En la industria actual, la transformación digital se ha convertido en una prioridad para las organizaciones que buscan optimizar sus operaciones y reducir costos mediante la implementación de tecnologías avanzadas. En este contexto SLB, una empresa líder en el sector petrolero ha estado a la vanguardia de esta revolución al adoptar tempranamente herramientas como la analítica de datos y la inteligencia artificial. Estas tecnologías no solo han sido parte integral de su estrategia durante varios años, sino que también han permitido mejoras significativas en procesos, toma de decisiones informadas y reducción de gastos. Además, han contribuido a enriquecer la experiencia tanto de los clientes como del personal.

Uno de los desafíos clave en la analítica de datos es la detección de falsos positivos. Esta técnica es fundamental para identificar datos anómalos, especialmente en un entorno donde la complejidad de los datos está en constante aumento y los valores atípicos pueden surgir debido a errores de medición o eventos inusuales, lo que resalta la importancia de una detección efectiva.

Sin embargo, a pesar de su relevancia, muchos sistemas actuales presentan deficiencias en la optimización necesaria para abordar los desafíos. Esta carencia no solo afecta la confiabilidad en la identificación de patrones anómalos, sino que también genera incertidumbre en la toma de decisiones críticas. Por lo tanto, es imperativo contar con sistemas robustos y eficientes.

En el caso específico de SLB, la falta de documentación clara y detallada sobre el funcionamiento del algoritmo de detección de outliers representa un obstáculo significativo. Por lo tanto, la ausencia de esta documentación dificulta la

comprensión profunda de los sistemas actuales y obstaculiza la implementación de mejoras sustanciales, así como la adaptación a las cambiantes demandas del entorno empresarial.

Ante este panorama, surge con urgencia la necesidad de desarrollar un plan de mejora que optimice la eficacia del sistema de detección de outliers y proporcione una documentación integral y transparente. Este enfoque integral no solo busca superar las limitaciones actuales en la identificación de patrones anómalos, sino que también contribuye al avance general en la aplicación de esta técnica en las diversas bases de la compañía a nivel global.

Dado este contexto, ¿Cuáles son las estrategias que se pueden implementar en el área de analítica de datos para disminuir la generación de falsos positivos, mejorar el monitoreo, la gestión de las alertas y, por ende, fortalecer la confiabilidad y la eficacia del sistema?

1.2 Justificación

La detección precisa de valores atípicos es crucial para el éxito de la estrategia de análisis de datos de SLB, ya que permite identificar y gestionar datos anómalos que podrían distorsionar los resultados. Actualmente, el sistema presenta deficiencias importantes en esta área, lo que lleva a un alto número de falsos positivos. Estos errores de identificación no solo disminuyen la confianza en la integridad de los datos, sino que también afectan negativamente la calidad de las decisiones que se toman basadas en esos datos.

Además, cuando la información es poco confiable, las empresas corren el riesgo de tomar decisiones inexactas, lo que puede resultar en costos operativos adicionales, pérdida de oportunidades comerciales y una gestión ineficaz de los recursos. En consecuencia, abordar estas deficiencias es fundamental para garantizar que la estrategia de análisis de datos sea efectiva y contribuya al crecimiento de la empresa.

1.3 Alcance

El objetivo de este proyecto es desarrollar una propuesta de mejora continua para optimizar los procesos y la documentación en el área de analítica de datos de SLB, con especial énfasis en la gestión de falsos positivos. Para lograr esto, se utilizarán las mejores prácticas de ITIL v4. El propósito fundamental es identificar oportunidades de mejora y proponer soluciones que permitan mejorar la detección y gestión de falsos positivos.

Como resultado, se entregará un documento detallado que analiza los procesos actuales y sus deficiencias, identifica áreas de mejora, y propone estrategias para optimizar la gestión. Este documento también incluirá una serie de recomendaciones y un plan que describe los pasos y recursos necesarios para implementar con éxito las mejoras sugeridas. Este entregable busca proporcionar soluciones prácticas y efectivas para la optimización de la gestión de falsos positivos.

Para mantener un enfoque claro y definido, esta propuesta se centrará únicamente en la optimización de la gestión de falsos positivos en el área de analítica de datos de SLB. En este sentido, se han establecido límites precisos para evitar desviaciones en el alcance:

- El alcance de la propuesta se centra exclusivamente en la gestión de falsos positivos, por lo que no se abordarán otros aspectos de la analítica de datos.
- El análisis y las recomendaciones se basarán únicamente en las actividades realizadas durante el período de la pasantía, sin incluir información sobre eventos previos a esta.
- El documento contendrá información limitada para respetar la confidencialidad y las políticas de seguridad de la empresa.

1.4 Metodología de la investigación

Para el desarrollo de este documento se tiene contemplado seguir una metodología de carácter investigativo y basado en las mejores practicas de ITIL v4 para garantizar la eficiencia y la consistencia en cada etapa del desarrollo de la propuesta.

Etapas:

- **Análisis de Procesos Existentes:** En la etapa inicial, se analiza el estado actual de los procesos relacionados con los falsos positivos para identificar debilidades y oportunidades de mejora.
- **Identificación de las Mejores Prácticas de ITIL v4:** En la segunda fase, se busca identificar las mejores prácticas de ITIL v4 que puedan ser aplicadas al diseño de la propuesta de mejora.
- **Diseño de la Propuesta de Mejora:** En la tercera etapa, se elabora un plan de mejora basado en las mejores prácticas de ITIL v4, abordando las debilidades y aprovechando las oportunidades identificadas previamente.
- **Definición de Indicadores:** En la última etapa, se definen los indicadores que medirán el éxito de la propuesta.

1.5 Objetivos

Objetivo General:

Desarrollar una propuesta de mejora continua para optimizar los procesos y la documentación en el área de analítica de datos de SLB, enfocada en la gestión de falsos positivos, utilizando las mejores prácticas de ITIL v4.

Objetivos específicos:

- Realizar un análisis de los procesos existentes en el área de gestión de falsos positivos.
- Identificar áreas de mejora y oportunidades para optimizar la detección de los falsos positivos.
- Identificar las mejores prácticas de ITIL v4 aplicables a la gestión de falsos positivos.
- Elaborar una propuesta para mejorar los procesos y la documentación asegurándose que la propuesta esté alineada con los principios de ITIL v4.

2. Contextualización y marco teórico

2.1 Analítica de datos

La analítica de datos es una disciplina que se destaca por su enfoque interdisciplinario el cual incorpora métodos y enfoques de diferentes áreas como la estadística, minería de datos, aprendizaje automático, visualización de datos, entre otros. Su objetivo es extraer insights, patrones e ideas a partir del análisis de datos estructurados y no estructurados [2]. Comprende un conjunto de tecnologías y técnicas que posibilitan el examen minucioso de grandes cantidades de datos para descubrir información valiosa, tendencias y patrones que respalden una toma de decisiones más acertada como se puede apreciar en la ilustración 1.

El proceso de analítica de datos es iterativo e involucra etapas como la recolección, preparación y exploración de datos, seguidas del modelado y análisis empleando diversas técnicas analíticas, y finalmente, la interpretación y comunicación de los resultados obtenidos [3]. Este proceso permite a las organizaciones convertir los datos en información procesable, incrementar la eficiencia operativa, optimizar procesos, identificar oportunidades y mitigar riesgos.

Además, la analítica de datos no se limita al análisis de datos históricos, sino que también incorpora técnicas de análisis predictivo y prescriptivo [4]. El análisis predictivo utiliza modelos estadísticos y de aprendizaje automático para pronosticar eventos o comportamientos futuros, mientras que el análisis prescriptivo va más allá y sugiere acciones o decisiones óptimas basadas en los resultados predictivos [6].

Ilustración 1. Ejemplo de un análisis visual de datos

2.2 Falsos positivos (outliers)

En la analítica de datos, uno de los desafíos más grandes son los falsos positivos, que pueden llevar a interpretaciones incorrectas y decisiones desacertadas [7]. Los falsos positivos se producen cuando un modelo o algoritmo analítico clasifica erróneamente un evento o condición como verdadero, cuando en realidad no lo es.

Hay varias causas que pueden dar lugar a estos falsos positivos. Entre ellas se encuentran la presencia de datos ruidosos o de baja calidad, como valores atípicos, datos ausentes o errores en los conjuntos de datos que pueden sesgar los resultados. También, los sesgos en los datos de entrenamiento utilizados para construir modelos analíticos pueden llevar a la identificación incorrecta de patrones y relaciones. Además, los modelos excesivamente complejos o sobreajustados a los datos de entrenamiento pueden capturar patrones aleatorios y generar falsos positivos en nuevos datos. Por último, si el conjunto de datos contiene una proporción desigual de observaciones positivas y negativas, los modelos pueden tener dificultades para identificar correctamente los casos positivos [8].

Los falsos positivos pueden tener un impacto significativo en los resultados de los análisis de datos y las decisiones basadas en ellos. Pueden llevar a la asignación

innecesaria de recursos para investigar o abordar situaciones que no son reales, disminuir la confianza en los resultados y las decisiones basadas en ellos si los modelos analíticos pueden ser erróneas. [9]

Para mitigar el riesgo de falsos positivos en la analítica de datos, existen varias técnicas y enfoques:

- El preprocesamiento de datos, como la limpieza, transformación y tratamiento de datos de alta calidad, puede mejorar la precisión de los modelos y reducir los falsos positivos.
- El uso de técnicas de muestreo, como el oversampling o undersampling, puede ayudar a equilibrar las clases en los conjuntos de datos y mejorar el rendimiento de los modelos.
- Ajustar los umbrales de decisión de los modelos puede permitir un mayor control sobre la relación entre falsos positivos y falsos negativos.
- La combinación de múltiples modelos o algoritmos puede reducir el riesgo de falsos positivos al aprovechar las fortalezas de cada uno.
- La validación rigurosa de los modelos analíticos, utilizando conjuntos de datos de prueba independientes, puede ayudar a identificar y mitigar los falsos positivos antes de la implementación.
- el desarrollo de modelos explicables e interpretables puede facilitar la identificación y mitigación de falsos positivos al comprender mejor los factores que influyen en las predicciones.

En la ilustración 2 podemos visualizar un ejemplo de falsos positivos el cual hay un conjunto de datos aleatorios con valores atípicos (outliers) que se diferencian del resto de los datos. Los datos principales se muestran con puntos verdes y forman una distribución aproximadamente lineal ascendente. No obstante, se observan varios puntos rojos que se alejan significativamente del patrón principal, lo que indica que son valores atípicos o outliers.

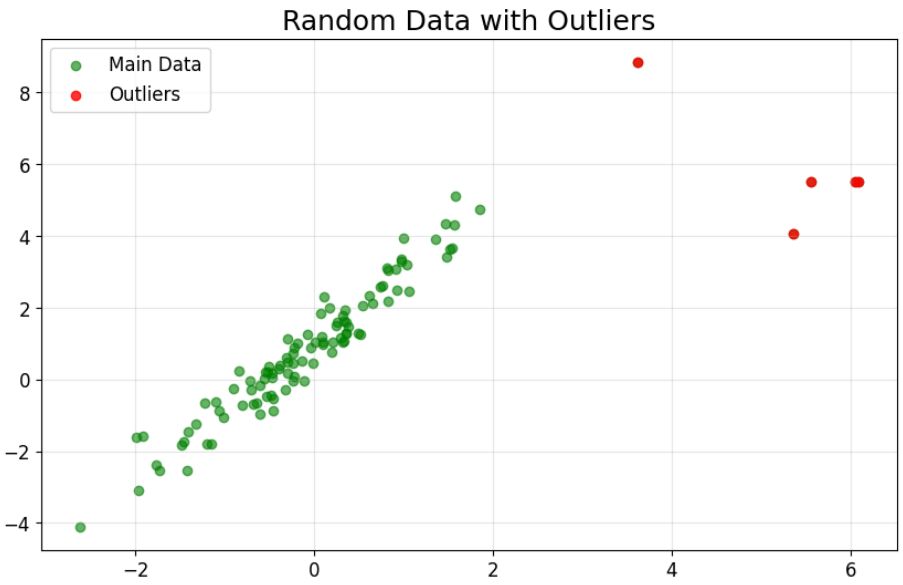

Ilustración 2. Ejemplo de Outlier (falsos positivos)

2.3 DBSCAN

DBSCAN, un algoritmo de agrupamiento que se basa en la densidad es muy popular en el análisis y la minería de datos [10]. A diferencia de los algoritmos de agrupamiento convencionales que se basan en particiones o modelos, DBSCAN agrupa los datos en función de su densidad y tiene la capacidad de identificar agrupaciones de formas variadas.

Este algoritmo se fundamenta en dos conceptos esenciales: la vecindad densa y los puntos de ruido. Una vecindad densa se define como un conjunto de puntos que están cerca entre sí y cumplen un umbral de densidad mínima dentro de un radio especificado [11]. Por otro lado, los puntos de ruido son aquellos que no pertenecen a ninguna vecindad densa y se consideran como datos atípicos o no estructurados.

DBSCAN clasifica los puntos de datos en tres categorías: puntos núcleo, puntos borde y puntos de ruido. Los puntos núcleo son aquellos que se encuentran en una vecindad densa y tienen al menos un número mínimo de vecinos dentro del radio especificado. Los puntos borde no son núcleo, pero se encuentran dentro de la

vecindad densa de un punto núcleo. Los puntos de ruido son aquellos que no son núcleo ni borde y se consideran datos atípicos [12].

El algoritmo DBSCAN inicia con un punto núcleo y expande la vecindad densa para formar un agrupamiento, incluyendo los puntos borde. Este proceso se repite hasta que se hayan visitado todos los puntos [11].

DBSCAN ofrece varias ventajas en comparación con otros algoritmos de agrupamiento. Puede identificar agrupaciones de formas irregulares y no lineales, es resistente al ruido y a los datos atípicos en los datos, ya que los clasifica como puntos de ruido en lugar de forzarlos a pertenecer a un agrupamiento. Además, no requiere conocer de antemano el número de agrupaciones, lo cual es una ventaja cuando se trabaja con datos sin etiquetar [12].

DBSCAN ha demostrado ser exitoso en diversos dominios, como análisis de datos espaciales, detección de anomalías, reconocimiento de patrones, procesamiento de imágenes, análisis de redes sociales y bioinformática.

En la ilustración 3 se presenta un ejemplo de DBSCAN, donde se puede observar dos grupos o clústeres principales representados por puntos de diferentes colores (azul y naranja). Estos grupos tienen una forma irregular y no lineal, lo cual resalta una de las principales ventajas de DBSCAN: su capacidad para detectar agrupaciones de formas arbitrarias. Además, se puede apreciar que algunos puntos no están asignados a ningún clúster, estos son los denominados "puntos de ruido" o outliers, que son tratados de manera especial por DBSCAN y no son forzados a pertenecer a ningún grupo.

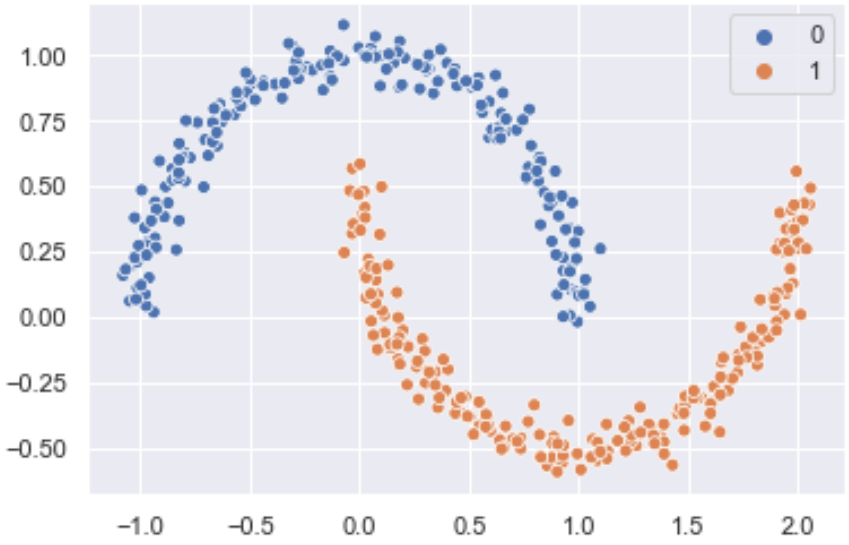

Ilustración 3. Ejemplo de DBSCAN

2.4 ITIL v4

ITIL v4, la última actualización del marco de referencia para la administración de servicios de tecnología de la información (TI), es reconocido y utilizado globalmente [13]. Esta versión, que se lanzó en 2019, ha sido modernizada para abordar las demandas y retos de las organizaciones contemporáneas en la era digital.

ITIL v4 se basa en siete principios guía que dirigen las decisiones y la aplicación de las prácticas de gestión de servicios. Estos principios comprenden la concentración en el valor, garantizando que los servicios de TI ofrezcan un valor duradero a los stakeholders; el inicio y avance desde el punto actual, adaptándose al contexto presente y avanzando de forma gradual; el progreso iterativo con feedback, mejorando de manera constante a través de ciclos de retroalimentación y aprendizaje; el enfoque integral, considerando todos los elementos del sistema de servicios, incluyendo personas, productos, socios y flujos de valor; mantener la sencillez y la practicidad, evitando soluciones innecesariamente complejas y

enfocándose en lo fundamental; la optimización y automatización, maximizando el desempeño a través de la optimización y automatización de procesos y flujos de trabajo; y la colaboración y promoción de la visibilidad, promoviendo la colaboración y la transparencia entre todos los stakeholders [14].

ITIL v4 presenta el concepto del Sistema de Valor de Servicio (SVS), que explica cómo diferentes componentes y actividades organizacionales colaboran para facilitar la creación de valor a través de servicios de TI. El SVS incluye la Cadena de Valor del Servicio, que es la secuencia de pasos necesarios para crear y entregar un servicio; las Prácticas, que son un conjunto de recursos organizacionales diseñados para realizar trabajo o alcanzar un objetivo específico; y las Guías, que son descripciones de prácticas sugeridas relacionadas con un conjunto específico de circunstancias [15].

ITIL v4 establece 34 prácticas agrupadas en tres dimensiones: General, Servicio y Técnica. La dimensión General incluye prácticas aplicables a todas las organizaciones, como la gestión de la estrategia y la gestión de portafolios. La dimensión de Servicio comprende prácticas relacionadas con la gestión del ciclo de vida del servicio, como la gestión de la demanda y la gestión de incidentes. La dimensión Técnica incluye prácticas centradas en la gestión de infraestructura y herramientas, como la gestión de la infraestructura y la gestión del despliegue [14].

Además, ITIL v4 introduce nuevas prácticas como la gestión de relaciones, la gestión del flujo de trabajo, la gestión del conocimiento y la gestión de seguridad de la información, entre otras, para enfrentar los desafíos actuales de las organizaciones en términos de transformación digital, agilidad y gestión del conocimiento.

ITIL v4 también resalta la importancia de la integración y la colaboración entre todas las prácticas y dimensiones, promoviendo un enfoque integral y optimizado para la entrega de servicios de TI de valor. Este enfoque integral permite a las

organizaciones adaptarse y responder a los cambios rápidos y constantes en el entorno empresarial actual, mejorando la eficiencia y la eficacia de sus servicios de TI.

3. Análisis de los procesos existentes en el área de gestión de falsos positivos.

3.1 Contextualización de la empresa

SLB es una empresa líder mundial en la provisión de servicios y tecnologías innovadoras para la industria de exploración y producción de petróleo y gas. Fundada en Alsacia, Francia, por los hermanos Schlumberger, esta compañía pionera sentó las bases al especializarse inicialmente en la realización de mediciones de pozos petroleros mediante la revolucionaria técnica de registro eléctrico. A lo largo de su trayectoria, SLB se ha establecido como un auténtico referente en el desarrollo de soluciones tecnológicas de vanguardia.

Las áreas estratégicas de enfoque de SLB abarcan desde la perforación y evaluación de formaciones, hasta la caracterización de yacimientos, la estimulación de pozos, la gestión integral de proyectos y la optimización de la producción. Con una visión vanguardista, la empresa también ha ampliado su alcance para participar activamente en segmentos emergentes como las energías renovables y la transición energética. Su amplio portafolio de productos y servicios integrales cubre todas las etapas del ciclo de vida de un campo petrolero[16].

Desde sus inicios, SLB ha demostrado una impresionante capacidad de adaptación a los desafíos cambiantes de la industria, manteniendo un liderazgo tecnológico inigualable. Esta agilidad y su compromiso inquebrantable con la innovación han cimentado su posición como líder indiscutible en el mercado global de servicios petroleros.

En la actualidad, se encuentran equipos multidisciplinarios que se dedican a la creación de servicios innovadores, aprovechando el potencial de tecnologías como la analítica de datos y la inteligencia artificial. Dentro de este panorama de innovación constante, destaca el equipo DES A2R, cuyo enfoque se centra en el desarrollo de una solución para el Monitoreo de Rendimiento de Aplicaciones (APM, por sus siglas en inglés), como podemos observar en la ilustración 4. Esta

herramienta robusta ofrece una visibilidad completa, de principio a fin, sobre el ciclo de vida de las aplicaciones que son críticas para el negocio, permitiendo la supervisión y análisis en tiempo real de su rendimiento.

Ilustración 4. APM

A pesar de los avances significativos en el desarrollo de esta herramienta, se han encontrado varios obstáculos en el camino. Uno de los desafíos más destacado es el control y supervisión de las alarmas generadas por la maquinaria utilizada en una variedad de procesos y servicios que SLB proporciona.

Este desafío se centra en el hecho de que el sistema actual genera un exceso de falsos positivos. Estos falsos positivos, o alarmas que se activan cuando no hay una condición de alarma real, pueden causar una serie de problemas. Por un lado, pueden desviar la atención de los ingenieros hacia problemas inexistentes, lo que puede llevar a una pérdida de tiempo y recursos.

Por otra parte, la cantidad de falsos positivos puede entorpecer el proceso de análisis de datos, ya que estos pueden distorsionar los resultados y hacer que sea más difícil identificar las tendencias y patrones reales. Esto puede llevar a decisiones basadas en información incorrecta, lo que podría tener consecuencias negativas para la eficiencia y efectividad de los procesos y servicios.

3.2. Funcionamiento del algoritmo

A continuación, presentaremos una serie de ilustraciones que ejemplifican las alarmas detectadas por la herramienta. Estas alarmas incluyen tanto verdaderos como falsos positivos. Además, se explicará el procedimiento que sigue el sistema cuando se encuentra con un falso positivo.

El sistema opera con un algoritmo desarrollado en Python, que utiliza el modelo DBSCAN (Density-Based Spatial Clustering of Applications with Noise) para analizar los datos. Este modelo es particularmente efectivo para identificar grupos de alta densidad separados por regiones de baja densidad. Por lo tanto, es ideal para este caso de uso, donde se necesita identificar alarmas verdaderas en medio de una gran cantidad de datos.

Es importante destacar que estos datos presentan cierta redundancia, ya que las muestras se toman en un corto intervalo de tiempo diferencial. Esta redundancia, aunque puede parecer un desafío, en realidad mejora la precisión del sistema.

La Ilustración 5 muestra los datos que la herramienta proporciona al visualizar una alarma. Estos datos incluyen detalles como el activo implicado, el equipo al que pertenece, el canal asociado, así como el día y la hora en que se detectó la alarma. También se muestra el estado o la severidad de la alarma, que en este caso específico, se identifica como crítica.

La gráfica ofrece la posibilidad de seleccionar diferentes parámetros que facilitan el análisis de la alarma. Esto permite visualizar la alarma con un número variable de muestras o en diferentes periodos de tiempo. En situaciones donde se identifica un falso positivo, la herramienta proporciona la opción de notificarlo. Por el contrario, si la alarma es legítima, la herramienta permite crear una notificación para que los ingenieros realicen la revisión correspondiente y, si es necesario, generen un número de caso.

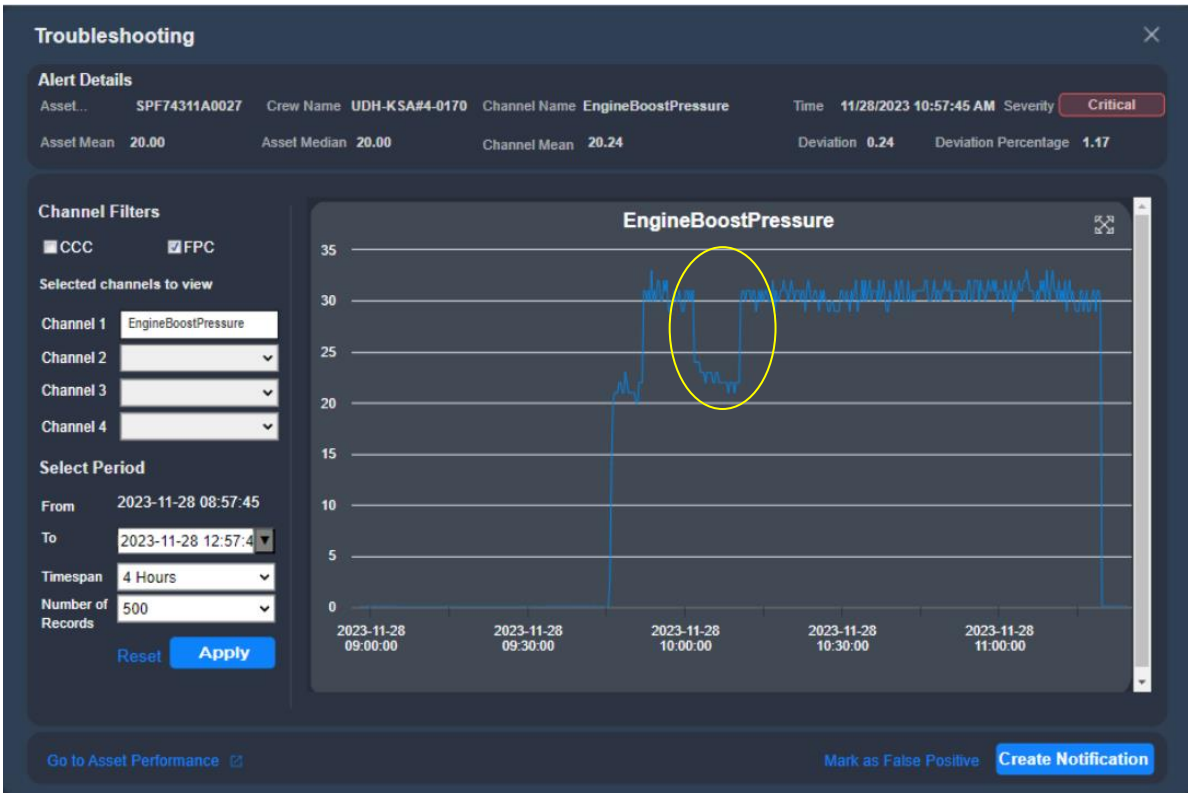

Ilustración 5. Ejemplo de alarma del canal Engine Boost Pressure

La Ilustración 5 muestra un caso de una alarma verdadera. No obstante, para confirmar su veracidad, fue esencial examinar la gráfica completa que engloba todos los activos del equipo, tal como se representa en la Ilustración 6. Actualmente, se está trabajando para determinar el clúster óptimo y los límites que indican cuándo una variación en los datos se considera una alarma. Este desafío surge debido a la naturaleza fluctuante de los datos, que varían según el canal. Además, la falta de documentación durante la creación del código y la ausencia de especificaciones claras sobre los requerimientos y los límites que deben tenerse en cuenta para identificar una alarma en ciertos canales, añaden un nivel adicional de complejidad.

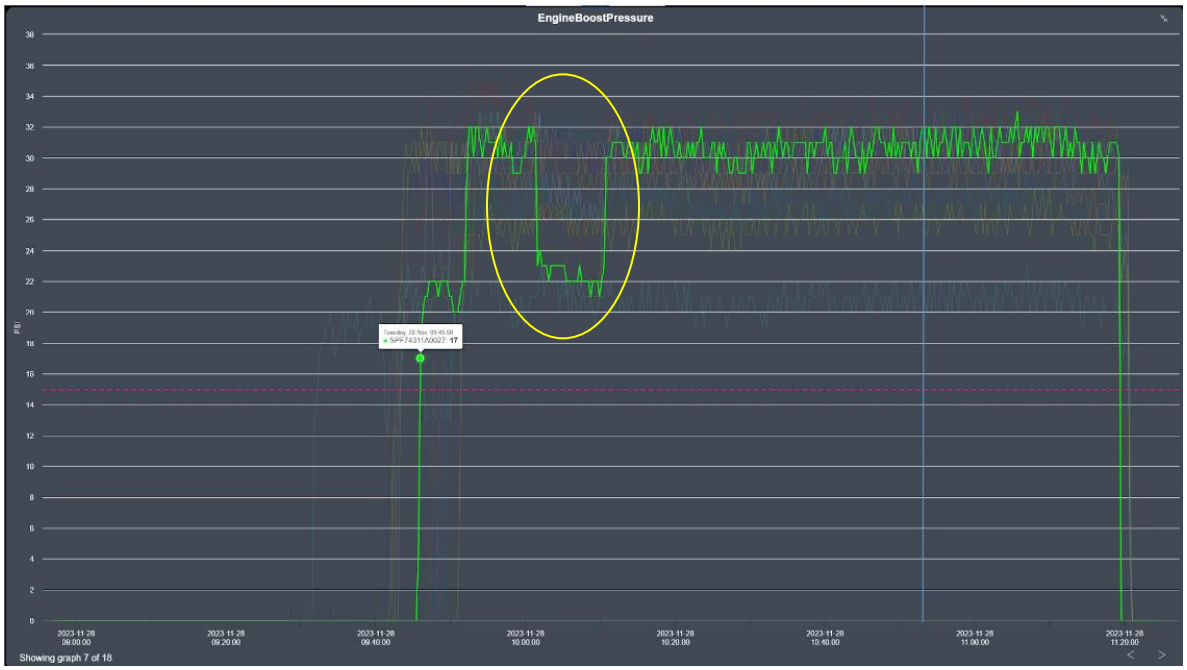

Ilustración 6. Grafica de Engine boost pressure con todos los asset del crew

En la Ilustración 7, se muestra un ejemplo de un falso positivo del mismo canal. Para verificar que se trata de un falso positivo, se aplica el mismo proceso descrito anteriormente.

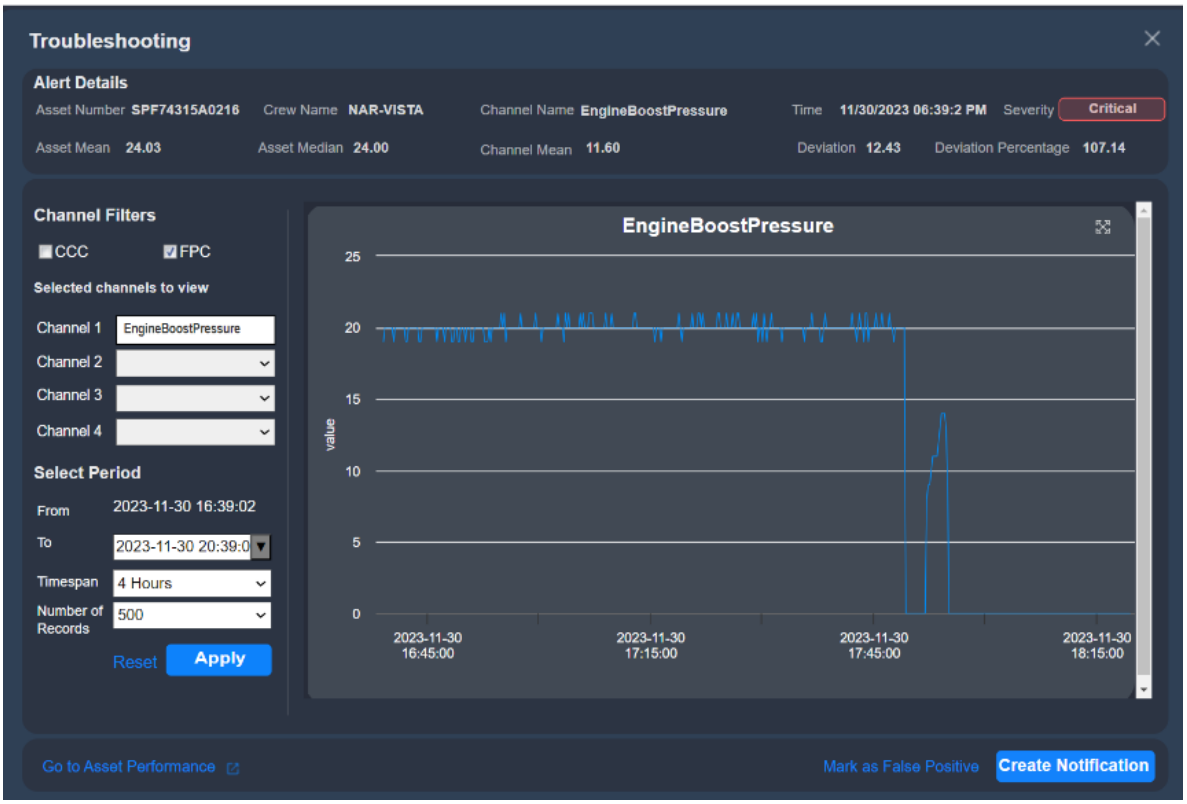

Ilustración 7. Ejemplo de falso positivo en el canal Engine boost pressure

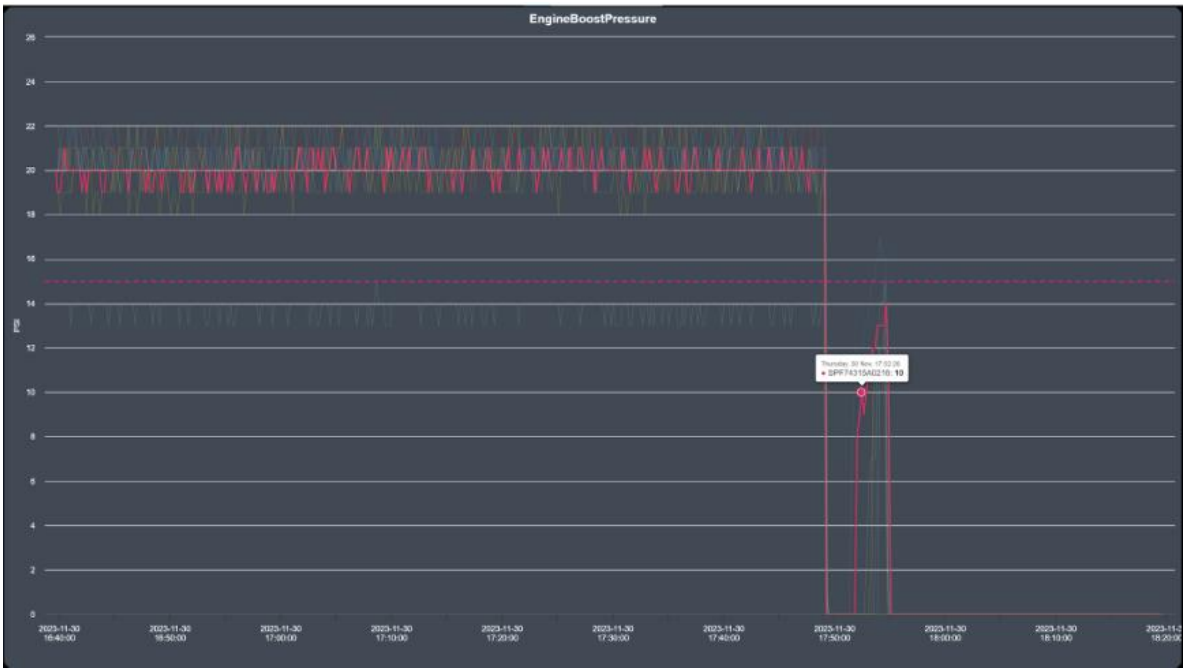

Ilustración 8. Grafica del canal Engine boost pressure con todos los asset del crew

Al comparar las Ilustraciones 7 y 8, se puede notar que todos los activos descienden a 0 en un periodo de tiempo específico. Este patrón puede ser el resultado de un apagado general o una pausa en el proceso, lo que indica que no se trata de una alarma. Sin embargo, se observa que el algoritmo aún necesita incorporar ciertos límites, como los horarios de inactividad de la maquinaria, para evitar la generación de falsos positivos.

3.3. Análisis de los falsos positivos

Anteriormente se nombró la creación de la herramienta APM, esta incluye un servicio de control de maquinaria en operación en varios lugares del mundo. Sin embargo, este servicio actualmente solo está implementado en algunas áreas del continente asiático, ya que aún se encuentra en una fase de pruebas y entrenamiento debido a problemas con las alertas.

Para realizar un análisis preciso, se extrajeron diversas alarmas generadas por el algoritmo en varios canales, incluyendo:

- Engine boost pressure
- Engine coolant temp
- Engine oil pres
- Engine voltage
- Power end oil pres

A través del análisis, identificamos ciertos datos que muestran el porcentaje de falsos positivos y alarmas correctas. Estos datos son esenciales para entender la eficacia del sistema de alerta y para hacer ajustes necesarios que mejoren su precisión y confiabilidad.

CHANNEL	CASE	FALSE POSITIVE	ALARM
ENGINE BOOST PRESSURE	1	X	
ENGINE BOOST PRESSURE	2	X	
ENGINE BOOST PRESSURE	3	X	
ENGINE BOOST PRESSURE	4	X	
ENGINE BOOST PRESSURE	5	X	
ENGINE BOOST PRESSURE	6	X	
ENGINE BOOST PRESSURE	7		X
ENGINE BOOST PRESSURE	8	X	
ENGINE BOOST PRESSURE	9	X	
ENGINE BOOST PRESSURE	10	X	
ENGINE BOOST PRESSURE	11	X	
ENGINE BOOST PRESSURE	12	X	
ENGINE BOOST PRESSURE	13	X	

ENGINE BOOST PRESSURE	14	**X**	
ENGINE BOOST PRESSURE	15	**X**	
ENGINE BOOST PRESSURE	16	**X**	
ENGINE BOOST PRESSURE	17	**X**	
ENGINE BOOST PRESSURE	18	**X**	
ENGINE BOOST PRESSURE	19	**X**	
ENGINE BOOST PRESSURE	20	**X**	
ENGINE BOOST PRESSURE	21	**X**	
TOTAL		**20**	**1**

Tabla 1. Análisis del canal Engine boost pressure

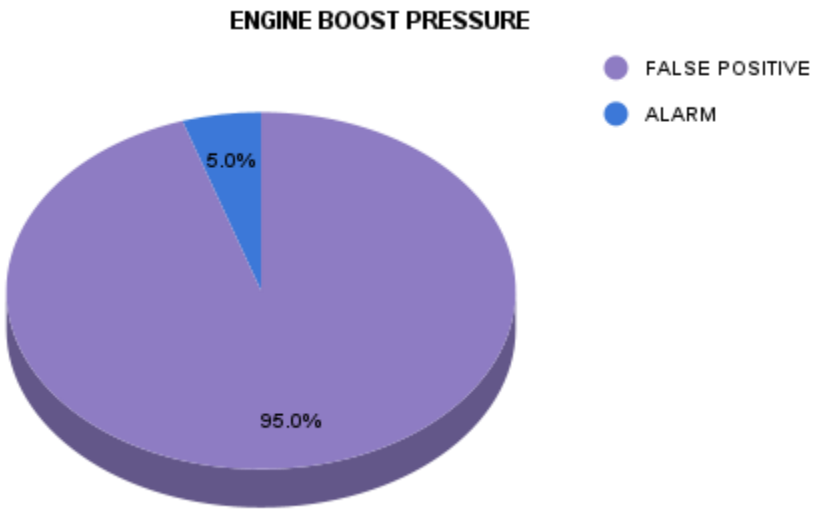

Ilustración 9. Grafica porcentajes Engine boost pressure

CHANNEL	CASE	FALSE POSITIVE	ALARM
ENGINE COOLANT TEMP	1		**X**
ENGINE COOLANT TEMP	2	**X**	
ENGINE COOLANT TEMP	3	**X**	
ENGINE COOLANT TEMP	4		**X**
ENGINE COOLANT TEMP	5	**X**	
ENGINE COOLANT TEMP	6	**X**	
ENGINE COOLANT TEMP	7	**X**	
ENGINE COOLANT TEMP	8	**X**	
ENGINE COOLANT TEMP	9	**X**	
ENGINE COOLANT TEMP	10	**X**	
ENGINE COOLANT TEMP	11	**X**	
ENGINE COOLANT TEMP	12	**X**	

ENGINE COOLANT TEMP	13		**X**
ENGINE COOLANT TEMP	14	**X**	
ENGINE COOLANT TEMP	15	**X**	
ENGINE COOLANT TEMP	16	**X**	
ENGINE COOLANT TEMP	17	**X**	
TOTAL		**14**	**3**

Tabla 2. Análisis del canal Engine coolant temp

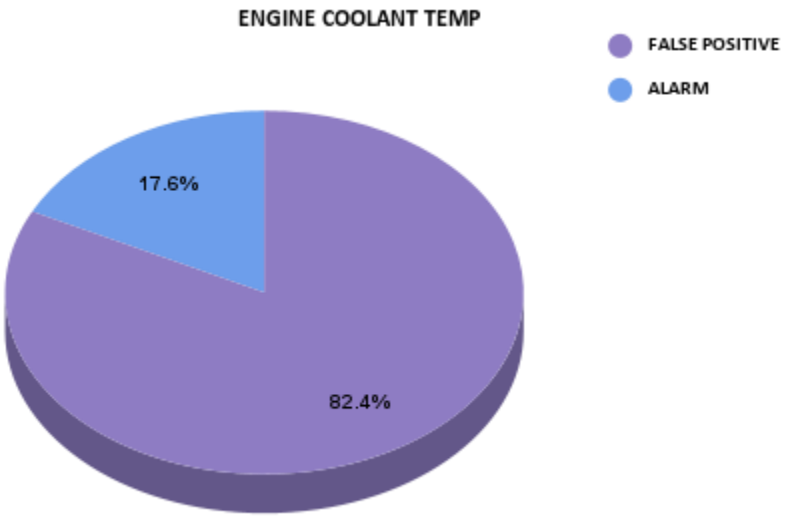

Ilustración 10. Grafica porcentajes Engine coolant temp

CHANNEL	CASE	FALSE POSITIVE	ALARM
ENGINE OIL PRES	1	**X**	
ENGINE OIL PRES	2	**X**	
ENGINE OIL PRES	3	**X**	
ENGINE OIL PRES	4	**X**	
ENGINE OIL PRES	5	**X**	
ENGINE OIL PRES	6	**X**	
ENGINE OIL PRES	7		**X**
ENGINE OIL PRES	8	**X**	
ENGINE OIL PRES	9	**X**	
ENGINE OIL PRES	10	**X**	
ENGINE OIL PRES	11	**X**	
ENGINE OIL PRES	12		**X**
ENGINE OIL PRES	13		**X**

ENGINE OIL PRES	14	X	
ENGINE OIL PRES	15	X	
ENGINE OIL PRES	16		X
ENGINE OIL PRES	17		X
ENGINE OIL PRES	18	X	
ENGINE OIL PRES	19		X
ENGINE OIL PRES	20	X	
TOTAL		14	6

Tabla 3. Análisis del canal Engine oil pres

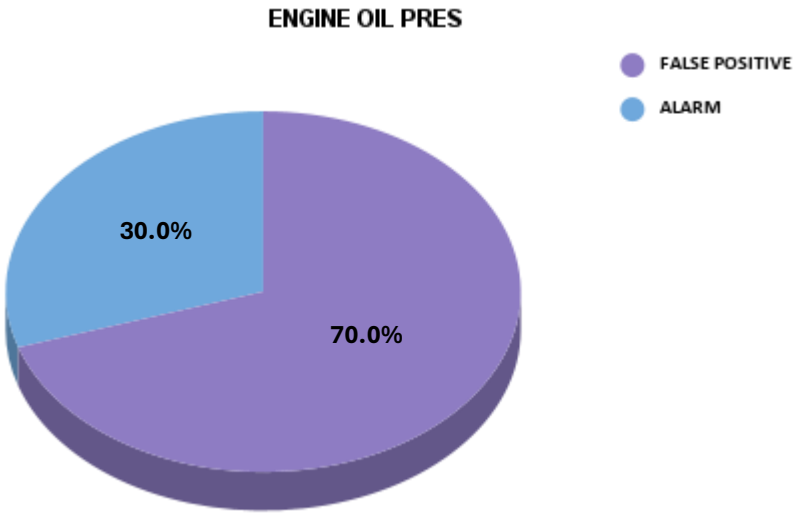

Ilustración 11. Grafica porcentajes Engine oil pres

CHANNEL	CASE	FALSE POSITIVE	ALARM
ENGINE VOLTAGE	1	X	
ENGINE VOLTAGE	2		X
ENGINE VOLTAGE	3	X	
ENGINE VOLTAGE	4		X
ENGINE VOLTAGE	5		X
ENGINE VOLTAGE	6	X	
ENGINE VOLTAGE	7	X	
ENGINE VOLTAGE	8	X	
ENGINE VOLTAGE	9	X	
ENGINE VOLTAGE	10	X	
ENGINE VOLTAGE	11	X	
ENGINE VOLTAGE	12		X

ENGINE VOLTAGE	13	**X**	
ENGINE VOLTAGE	14		**X**
TOTAL		**9**	**5**

Tabla 4. Análisis del canal Engine voltage

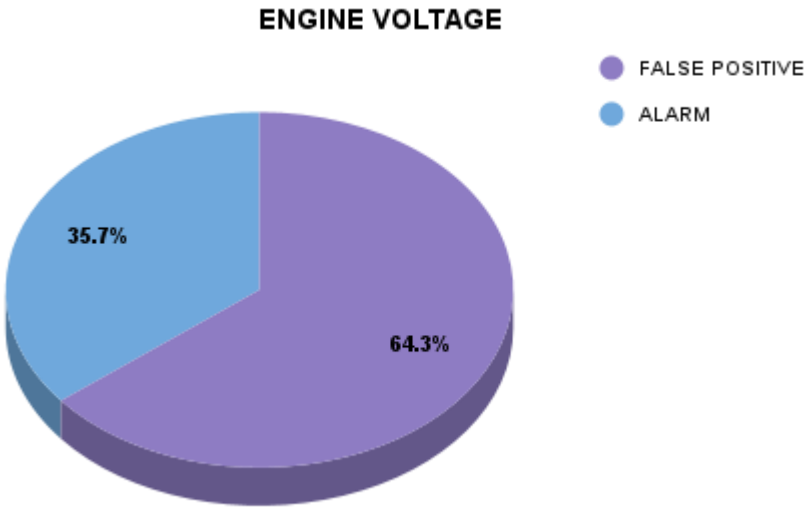

Ilustración 12. Grafica porcentajes Engine voltage

CHANNEL	CASE	FALSE POSITIVE	ALARM
POWER END OIL PRES	1	**X**	
POWER END OIL PRES	2	**X**	
POWER END OIL PRES	3	**X**	
POWER END OIL PRES	4		**X**
POWER END OIL PRES	5	**X**	
POWER END OIL PRES	6	**X**	
POWER END OIL PRES	7	**X**	
POWER END OIL PRES	8		**X**
POWER END OIL PRES	9	**X**	
POWER END OIL PRES	10		**X**
POWER END OIL PRES	11		**X**
POWER END OIL PRES	12		**X**
POWER END OIL PRES	13	**X**	
POWER END OIL PRES	14	**X**	
POWER END OIL PRES	15	**X**	
POWER END OIL PRES	16		**X**
TOTAL		**10**	**6**

Tabla 5. Analisis del canal Power end oil pres

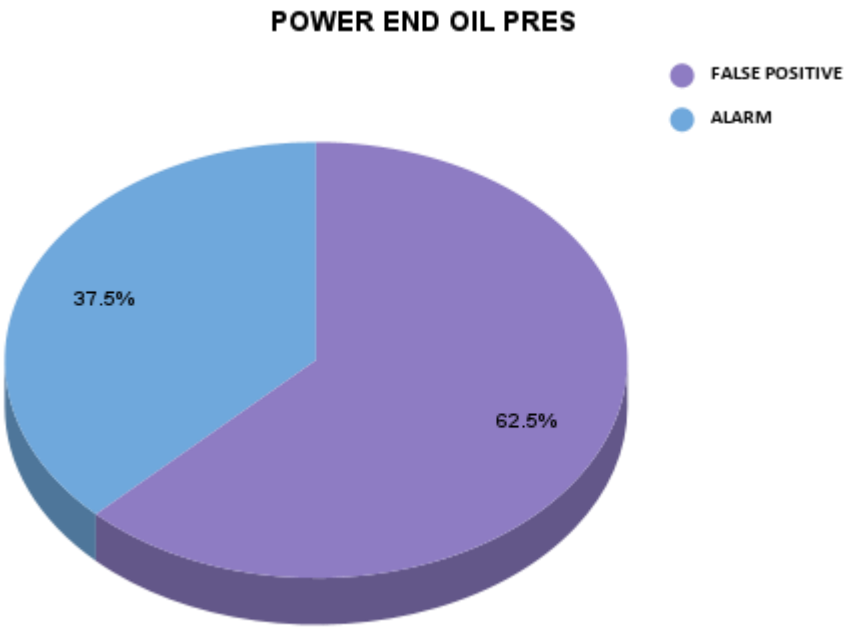

Ilustración 13. Grafica porcentajes Power end oil pres

En primer lugar, es importante destacar que la predominancia de falsos positivos, con un porcentaje superior al 60% en la mayoría de los canales, puede ser un indicativo de que los umbrales de alarma actuales podrían estar configurados de manera demasiado sensible. Esto podría llevar a una gran cantidad de alarmas innecesarias, lo que podría desensibilizar al algoritmo a las alarmas reales.

En segundo lugar, los canales “Engine voltage”(ilustración 12) y “Power end oil pres” (ilustración 13) muestran una precisión en las alarmas superior al 35%. Aunque este porcentaje puede parecer bajo en comparación con el ideal del 100%, es significativamente mayor en comparación con los demás canales. Esto sugiere que estos dos canales podrían estar configurados de manera más efectiva, o que los eventos que están monitoreando son más predecibles o fáciles de detectar. Sin embargo, un porcentaje de precisión del 35% todavía deja espacio para mejoras.

3.4. DOFA

Debilidades	Oportunidades
• Falta de documentación y especificaciones claras al momento de crear el código, dificultando la comprensión y el mantenimiento del sistema. • Falta de definición de los límites que determinan cuándo una fluctuación en los datos se considera una alarma, lo que puede llevar a una detección imprecisa de las alarmas. • Redundancia en los datos debido a que las muestras se toman en un corto intervalo de tiempo diferencial, aumentando la carga de procesamiento y almacenamiento de datos. • Variabilidad de los datos dependiendo del canal, dificultando la identificación precisa de las alarmas. • Falta de especificación de los requerimientos y de información de los límites que se deben tener en cuenta para considerar una alarma en ciertos canales. • Generación de falsos positivos en ciertas situaciones, como durante un apagado general o una pausa en	• Mejorar la precisión del sistema al especificar los límites, como los horarios de inactividad de la maquinaria, para evitar la generación de falsos positivos. • Optimizar el algoritmo para manejar la redundancia en los datos y mejorar la eficiencia del sistema. • Mejorar la documentación y las especificaciones del código para facilitar su comprensión y mantenimiento. • Definir claramente los límites y requerimientos para la detección de alarmas en diferentes canales. • Mejorar la precisión de la detección de alarmas al tener en cuenta la variabilidad de los datos dependiendo del canal. • Reducir los falsos positivos al mejorar la identificación de situaciones como un apagado general o una pausa en el proceso.

el proceso.	
Fortalezas	**Amenazas**
• Uso de Python, un lenguaje de programación de alto nivel ampliamente utilizado en ciencia de datos y aprendizaje automático, facilitando la implementación y mantenimiento del algoritmo. • Implementación del modelo DBSCAN para el análisis de datos, efectivo para identificar grupos de alta densidad, permitiendo una detección de alarmas más precisa. • Flexibilidad para visualizar y analizar alarmas con un número variable de muestras o en diferentes periodos de tiempo, adaptándose a diferentes necesidades y situaciones. • Identificación y notificación de falsos positivos, mejorando la precisión de la detección de alarmas. • Manejo de grandes volúmenes de datos, permitiendo el procesamiento de grandes cantidades de información. • Información detallada sobre las alarmas, incluyendo el activo implicado, el equipo al que	• La rápida evolución de la tecnología puede hacer que el lenguaje de programación Python o el modelo DBSCAN se vuelvan obsoletos, lo que requeriría una actualización del sistema. • La aparición de nuevas herramientas de análisis de datos en el mercado que pueden ofrecer características superiores o adicionales. • Las nuevas leyes o regulaciones sobre el manejo de datos pueden requerir cambios en el sistema, lo que podría implicar costos adicionales. • Los usuarios pueden comenzar a esperar funcionalidades adicionales o diferentes, lo que podría requerir ajustes en el sistema. • Los ataques cibernéticos o las violaciones de datos pueden comprometer la integridad de los datos manejados por el sistema. • Limitaciones de infraestructura

pertenece, el canal asociado, así como el día y la hora en que se detectó la alarma.	

Tabla 6. Matriz DOFA

4. Identificación de las mejores prácticas de ITIL v4.

Para el correcto desarrollo de la propuesta de mejora se deben identificar cuáles son las mejores prácticas de ITIL v4 para diseñarla de acuerdo con los requerimientos y necesidades de SLB.

4.1 Dimensiones de la gestión de servicios:

- **Organizaciones y personas:** La falta de documentación y especificaciones claras al momento de crear el código indica que puede haber una falta de comunicación o entendimiento entre las personas del equipo a cargo del desarrollo. Abordar este problema, mejoraría la comprensión y el mantenimiento del sistema.

- **Información y tecnología:** La falta de definición de los límites para la detección de alarmas, la redundancia en los datos y la variabilidad de los datos dependiendo del canal, se relacionan directamente con la gestión de la información y la tecnología. Mejorar en esta área podría ayudar a abordar estos problemas y optimizar el sistema.

- **Socios y proveedores:** La rápida evolución de la tecnología y la aparición de nuevas herramientas de análisis de datos en el mercado son amenazas que podrían abordarse mejorando la gestión de socios y proveedores. Esto podría implicar mantenerse al día con las últimas tendencias y estándares, y posiblemente colaborar con socios y proveedores para implementar nuevas tecnologías.

- **Flujos de valor y procesos:** La falta de especificación de los requerimientos y de información de los límites para la detección de alarmas en ciertos canales sugiere que podría haber un problema con los flujos de valor y los procesos actuales. Mejorar en esta área podría ayudar a definir claramente estos límites y requerimientos, mejorando la precisión de la detección de alarmas

4.2 Sistema de valor

- **Principios Guía:** La falta de definición de los límites para la detección de alarmas y la falta de especificación de los requerimientos sugieren que los principios guía podrían no estar claramente definidos o comunicados. Reforzar estos principios puede ayudar a proporcionar una dirección más clara y consistente para el desarrollo y mantenimiento del sistema.

- **Gobierno:** La falta de documentación y especificaciones claras, así como la rápida evolución de la tecnología, sugieren que puede haber un problema con el gobierno del sistema. Mejorar el gobierno puede ayudar a asegurar que el sistema se mantenga actualizado y sea fácil de entender y mantener.

- **Cadena de valor del servicio:** La redundancia en los datos y la variabilidad de los datos dependiendo del canal indican que la cadena de valor del servicio podría necesitar ser optimizada. Esto podría implicar mejorar la eficiencia del sistema y la precisión de la detección de alarmas.

- **Prácticas:** La generación de falsos positivos y la falta de especificación de los límites para la detección de alarmas sugieren que las prácticas actuales podrían necesitar ser revisadas y mejoradas. Esto podría ayudar a mejorar la precisión de la detección de alarmas y reducir los falsos positivos.

- **Mejora continua:** Las oportunidades identificadas para mejorar la precisión del sistema, optimizar el algoritmo, mejorar la documentación y las especificaciones del código, y reducir los falsos positivos indican que la mejora continua es necesaria. Esto puede ayudar a asegurar que el sistema se mantenga relevante y efectivo en el tiempo.

4.3 Selección de mejores prácticas:

- **Gestión del conocimiento**: Este proceso implica la creación, compartición, uso y gestión del conocimiento y la información de una organización. Se refiere a un enfoque multidisciplinario para lograr los objetivos organizacionales mediante el uso óptimo del conocimiento. Incluye las prácticas utilizadas por las organizaciones para identificar, crear, representar, distribuir y permitir la adopción de conocimientos y experiencias [14].
- **Gestión de la configuración del servicio:** Este proceso se encarga de mantener información actualizada y precisa sobre todos los elementos de configuración y sus dependencias. Un elemento de configuración es un componente de un servicio de TI que está (o está destinado a estar) bajo control de gestión de configuración y, por lo tanto, está sujeto a un proceso formal de cambio [14].
- **Gestión de incidentes:** Este proceso se encarga de manejar todos los incidentes. Los incidentes son definidos como cualquier interrupción o degradación del servicio de calidad. El objetivo principal de la gestión de incidentes es restablecer el servicio normal tan rápido como sea posible con el mínimo impacto en el negocio [14].
- **Mejora continua:** Este es un enfoque constante para mejorar los productos, servicios y procesos de una organización. Se lleva a cabo en un ciclo de cuatro etapas: Planificar, Hacer, Verificar y Actuar (PDCA) [14].
- **Control de cambios:** Este proceso se encarga de gestionar y controlar todos los cambios en los servicios de TI. Su objetivo es asegurar que todos los cambios se realicen de manera controlada y coordinada [14].
- **Gestión de problemas**: Este proceso se encarga de gestionar el ciclo de vida de todos los problemas. El objetivo principal de la gestión de problemas es prevenir problemas e incidentes resultantes, eliminar incidentes recurrentes y minimizar el impacto de los incidentes que no pueden prevenirse [14].

- **Gestión de la continuidad del servicio:** Este proceso se encarga de asegurar que el proveedor de TI pueda proporcionar un mínimo nivel acordado de servicios en caso de desastre. Incluye la planificación, diseño, prueba y mantenimiento de las capacidades de continuidad y recuperación del servicio [14].
- **Gestión de la disponibilidad:** Este proceso se encarga de asegurar que los servicios cumplen con los niveles de disponibilidad acordados. Incluye el monitoreo, medición, análisis y reporte de la disponibilidad de los servicios de TI [14].
- **Gestión de la arquitectura**: Este proceso se encarga de definir y mantener la arquitectura de TI de una organización. Incluye la definición de los estándares y políticas de arquitectura, y la identificación de las oportunidades de mejora [14].

5. Diseño de la propuesta de mejora continua

El sistema de detección de alarmas enfrenta diversos desafíos y limitaciones que pueden comprometer su eficacia y escalabilidad a largo plazo. Desde problemas de diseño e implementación hasta factores externos, estas cuestiones deben ser abordadas para garantizar un rendimiento óptimo. A continuación, se detallan algunos de los principales problemas identificados:

Problema	Descripción
Falta de documentación y especificaciones claras	No existe una documentación clara del código fuente del sistema de detección de alarmas, ni un banco de información en el cual se encuentren las especificaciones, cambios y la explicación de todo lo que tiene que ver con el código lo que dificulta la comprensión y el mantenimiento del sistema.
Falta de definición de los límites	Al realizar el análisis del estado actual se identificó que el código no tiene una definición clara de los limites lo cual genera una detección imprecisa de las alarmas.
Redundancia en los datos	Aunque la redundancia de los datos puede parecer un desafío, en realidad mejora la precisión del sistema. Sin embargo, también aumenta la carga de procesamiento y almacenamiento de datos.
Variabilidad de los datos dependiendo del canal	El análisis reveló que el código propuesto está definido de manera general para todos los canales. Debido a la variabilidad de los datos según los diferentes canales,

	esto dificulta la identificación precisa de las alarmas.
Falta de especificación de los requerimientos	La falta de especificación de los requisitos para el desarrollo del sistema ha generado una detección imprecisa de las alarmas, ya que no se tienen detalles claros sobre lo que se desea lograr y detectar en cada canal.
Generación de falsos positivos	La generación de falsos positivos es el problema principal que impulsó esta propuesta. Desde que se desplegó el código en el sistema, más del 70% de las alarmas han sido falsos positivos, lo que ha resultado en un sistema con baja eficacia y confiabilidad. Se ha logrado identificar que estos falsos positivos suelen ocurrir en situaciones específicas, como durante un apagado general o una pausa en el proceso.
Limitaciones de infraestructura	De acuerdo con los problemas identificados podemos concluir que esto puede limitar la capacidad del sistema para manejar grandes volúmenes de datos o implementar nuevas funcionalidades.

Tabla 7. Problemas identificados

5.1 Gestión de la configuración del servicio

La gestión efectiva de la configuración del servicio es un componente crítico para garantizar el funcionamiento óptimo y confiable del sistema de detección de alarmas. Este proceso sistemático involucra el control y monitoreo de los cambios realizados en el sistema, así como la documentación y seguimiento de su configuración a lo largo de todo su ciclo de vida.

En el contexto del sistema de detección de alarmas, la gestión de la configuración del servicio juega un papel fundamental para abordar los desafíos identificados, como la falta de documentación clara, la definición imprecisa de límites, la variabilidad de los datos por canal y la especificación insuficiente de los requisitos. Estos problemas han contribuido a la detección imprecisa de alarmas y a la generación de falsos positivos, lo que ha afectado la eficacia y confiabilidad del sistema.

La implementación de la práctica de la gestión de la configuración del servicio permitirá establecer un control riguroso sobre los componentes del sistema, incluyendo el código fuente, las especificaciones, los requisitos y la infraestructura subyacente. Esto garantizará que todos los cambios realizados sean rastreables, documentados y aprobados, minimizando el riesgo de errores o inconsistencias.

Problema	Actividades Propuestas
Falta de documentación y especificaciones claras.	Desarrollar una documentación detallada del código fuente del sistema de detección de alarmas.
	Crear un repositorio centralizado con las especificaciones, cambios y explicaciones relacionadas con el código.

	Establecer procesos para mantener la documentación actualizada y accesible para el equipo de desarrollo y mantenimiento.
Falta de definición de los límites	Revisar y definir claramente los límites del sistema para una detección precisa de alarmas.
	Documentar los rangos y umbrales aceptables para cada tipo de alarma o evento a detectar.
Variabilidad de los datos dependiendo del canal	Adaptar el código para manejar la variabilidad de datos según los diferentes canales.
	Considerar implementar lógica específica por canal o configuraciones ajustables para una detección precisa.
Falta de especificación de los requerimientos	Realizar un proceso de levantamiento y especificación detallada de los requerimientos del sistema.
	Involucrar a los stakeholders para comprender las necesidades y expectativas de detección de alarmas en cada canal.
Limitaciones de infraestructura	Evaluar y mejorar la infraestructura del sistema para manejar grandes volúmenes de datos y permitir la implementación de nuevas funcionalidades.

Tabla 8. Actividades propuestas gestión de la configuración del servicio

5.2 Gestión de la infraestructura

La gestión de la infraestructura implica un conjunto de procesos y actividades diseñados para planificar, implementar, monitorear y optimizar los recursos de infraestructura necesarios para el sistema de detección de alarmas. Estos recursos incluyen hardware, software, redes, centros de datos, sistemas de almacenamiento y cualquier otro componente tecnológico que respalde el funcionamiento del sistema.

En el ámbito del sistema de detección de alarmas, la gestión de la infraestructura desempeña un papel fundamental para garantizar un rendimiento óptimo, una escalabilidad adecuada y una alta disponibilidad del sistema.

Un aspecto crucial de la gestión de la infraestructura es asegurar la alta disponibilidad del sistema de detección de alarmas. Esto implica implementar mecanismos de redundancia, monitoreo continuo, planes de respaldo y recuperación, y procedimientos de mantenimiento preventivo para minimizar el riesgo de interrupciones o fallas en el servicio.

Problema	Actividad Propuesta
Redundancia en los datos	Evaluar y dimensionar las soluciones de almacenamiento para manejar adecuadamente la redundancia de datos.
	Implementar técnicas de compresión de datos o de duplicación para optimizar el uso del almacenamiento.
	Escalar los recursos de procesamiento para manejar eficientemente la carga adicional por la redundancia de datos.
Variabilidad de los datos dependiendo	Crear soluciones de infraestructura escalables y distribuidas para manejar la variabilidad de datos por canal.
	Utilizar enfoques de segmentación de

del canal	datos por canal, ya sea a nivel de almacenamiento, procesamiento o ambos.
	Ajustar dinámicamente los recursos de procesamiento y almacenamiento según la carga de datos de cada canal.
Generación de falsos positivos	Diseñar una infraestructura separada o aislada para el manejo de falsos positivos, evitando impactar el rendimiento del sistema principal.
	Crear mecanismos de monitoreo y alerta para detectar y responder rápidamente a eventos de falsos positivos masivos.
Limitaciones de infraestructura	Realizar un análisis exhaustivo de las necesidades actuales y futuras de capacidad, rendimiento y escalabilidad del sistema.
	Optimizar la configuración y el uso de los recursos de infraestructura existentes para mejorar su eficiencia.
	Implementar mecanismos de monitoreo y alerta para detectar y resolver posibles cuellos de botella o saturación de recursos.

Tabla 9, Actividades propuestas para la gestión de la infraestructura

5.3 Gestión de la disponibilidad

La gestión de la disponibilidad implica un conjunto de actividades diseñadas para prevenir, detectar y responder de manera oportuna ante cualquier interrupción o degradación del servicio. Esto incluye la identificación de puntos únicos de falla, la implementación de mecanismos de redundancia, la definición de acuerdos de nivel de servicio (SLA) y la planificación de acciones de recuperación en caso de incidentes.

En el contexto del sistema de detección de alarmas, la gestión de la disponibilidad desempeña un papel crítico para garantizar que el servicio esté accesible y operativo en todo momento, minimizando los tiempos de inactividad y asegurando una continuidad óptima del negocio. Esta práctica se enfoca en implementar estrategias, procesos y controles para mantener altos niveles de disponibilidad del sistema, lo que es fundamental para la confiabilidad y eficacia de la detección de alarmas.

Uno de los objetivos principales de la gestión de la disponibilidad es minimizar el tiempo de inactividad no planificado del sistema de detección de alarmas. Esto se logra mediante la implementación de soluciones de alta disponibilidad, como la redundancia de componentes críticos, el balanceo de carga, la replicación de datos y la conmutación automática por error (failover).

Problema	Actividades propuestas
Falta de documentación y especificaciones claras	Mantener una documentación actualizada y clara del sistema, lo que facilitará las tareas de mantenimiento y recuperación, minimizando el impacto en la disponibilidad.
Falta de definición de los límites	Definir claramente los límites del sistema y establecer controles y alertas para monitorear y mantener el servicio dentro de los límites establecidos.
	Implementar mecanismos de balanceo

Variabilidad de los datos dependiendo del canal	de carga y distribución de datos por canal para evitar la saturación y garantizar la disponibilidad del servicio.
	Definir acuerdos de nivel de servicio (SLA) específicos para cada canal, considerando su variabilidad de datos.
Falta de especificación de los requerimientos	Especificar claramente los requisitos de disponibilidad del sistema y establecer acuerdos de nivel de servicio (SLA) acordes a los requerimientos del negocio.
Generación de falsos positivos	Implementar mecanismos de detección y filtrado de falsos positivos para evitar que saturen el sistema y afecten su disponibilidad.
	Establecer procesos de escalamiento y respuesta rápida ante eventos masivos de falsos positivos.
Limitaciones de infraestructura	Establecer procesos de monitoreo y alerta de recursos para detectar y mitigar limitaciones de infraestructura.
	Definir planes de continuidad del negocio (BCP) y recuperación de desastres (DRP) para garantizar la disponibilidad ante fallas graves de infraestructura.
Redundancia de los datos	Implementar soluciones de almacenamiento redundante y replicación de datos para garantizar la disponibilidad de los datos ante fallas.
	Establecer procesos de monitoreo y

	recuperación de datos en caso de pérdidas o corrupción.

Tabla 10. Actividades propuestas para la gestión de la disponibilidad

5.4 Control de cambios

Los sistemas críticos, como el sistema de detección de alarmas, están sujetos a cambios constantes para abordar nuevos requisitos, corregir defectos o mejorar su funcionalidad. Sin embargo, estos cambios pueden introducir riesgos y vulnerabilidades si no se gestionan adecuadamente.

El control de cambios es un proceso esencial en la gestión de seguridad de la información que garantiza que todos los cambios realizados en el sistema de detección de alarmas sean evaluados, aprobados, implementados y rastreados de manera controlada y estructurada. Este proceso permite minimizar los riesgos asociados con los cambios, asegurando la integridad, confidencialidad y disponibilidad de la información manejada por el sistema.

Problema	Actividades propuestas
Documentación y especificaciones claras	Crear un proceso formal de control de cambios que asegure que todas las modificaciones al código fuente del sistema, así como a la documentación y especificaciones, sean debidamente evaluadas, aprobadas y rastreadas.
	Definir roles y responsabilidades claras para el control de cambios, incluyendo la revisión por parte de expertos y la aprobación por parte de los stakeholders correspondientes.
	Asegurar que cualquier cambio en los límites del sistema o en las reglas de detección de alarmas sea cuidadosamente evaluado y aprobado a través del proceso de control de

Definición de límites del sistema	cambios.
	Documentar detalladamente los cambios en los límites del sistema y sus impactos potenciales en términos de seguridad, rendimiento y precisión.
	Realizar pruebas exhaustivas y validaciones antes de implementar cambios en los límites del sistema de detección de alarmas.
Especificación de requerimientos	Establecer un proceso de control de cambios para la documentación y actualización de los requisitos del sistema, asegurando que cualquier modificación sea debidamente evaluada, aprobada y comunicada a todas las partes interesadas.
	Implementar mecanismos de trazabilidad entre los requisitos, el código fuente y las pruebas, para facilitar la identificación y gestión de los impactos de los cambios en los requisitos.
Manejo de falsos positivos	Incluir en el proceso de control de cambios la revisión y aprobación de cualquier modificación en las reglas o algoritmos utilizados para identificar y mitigar los falsos positivos.
	Documentar detalladamente los cambios realizados en el manejo de falsos positivos, incluyendo la justificación, los impactos esperados y

	las pruebas realizadas.
	Realizar pruebas exhaustivas y validaciones antes de implementar cambios en el manejo de falsos positivos, para asegurar que no se introduzcan nuevos problemas o vulnerabilidades.

Tabla 11. Actividades propuestas para el control de cambios

5.5 Gestión de incidentes

La gestión de incidentes, que comprende un conjunto de procesos y procedimientos diseñados para identificar, registrar, analizar, resolver y monitorear incidentes de manera sistemática y eficiente, es crucial para minimizar el impacto negativo en el sistema de detección de alarmas y asegurar la continuidad del servicio.

En el contexto del sistema de detección de alarmas, la gestión de incidentes es una práctica vital para asegurar una respuesta rápida y efectiva a cualquier interrupción o evento inesperado que pueda afectar el funcionamiento óptimo del sistema. Un incidente puede ser cualquier evento que provoque una interrupción o degradación del servicio, como falsos positivos, detecciones erróneas, fallas de hardware o software, entre otros.

Uno de los principales objetivos de la gestión de incidentes es establecer un único punto de contacto para reportar y gestionar los incidentes, facilitando así la comunicación y coordinación entre los diferentes equipos involucrados. Esto implica la implementación de un sistema de registro y seguimiento de incidentes, donde se documenten todos los detalles relevantes, como la descripción del incidente, su gravedad, impacto y las acciones tomadas.

Problema	Actividades propuestas
	Establecer un proceso de registro y categorización de incidentes relacionados con falsos positivos en el sistema de detección de alarmas.
	Documentar detalladamente cada incidente de falso positivo, incluyendo la descripción del evento, el contexto, la gravedad y el impacto.

Generación de falsos positivos	Realizar un análisis exhaustivo de los incidentes para identificar patrones y situaciones específicas que conducen a falsos positivos, como apagados generales o pausas en el proceso.
	Implementar soluciones temporales o ajustes en los algoritmos de detección para mitigar los falsos positivos mientras se investiga una solución permanente.
	Documentar las soluciones implementadas y las lecciones aprendidas en una base de conocimientos de incidentes.
	Establecer acciones preventivas y correctivas para reducir la ocurrencia de falsos positivos en el futuro.
Limitaciones de infraestructura	Registrar y categorizar incidentes relacionados con limitaciones de infraestructura que afecten el rendimiento, la capacidad o la disponibilidad del sistema de detección de alarmas.
	Implementar soluciones temporales, como limitación del procesamiento o almacenamiento, para mitigar el impacto mientras se investiga una solución permanente.
	Coordinar con los equipos de infraestructura y operaciones para evaluar las necesidades de escalamiento o mejora de la infraestructura.

	Documentar las soluciones implementadas y las lecciones aprendidas en la base de conocimientos de incidentes.
	Establecer planes de acción para abordar las limitaciones de infraestructura a largo plazo, como la adquisición de recursos adicionales o la optimización del sistema.

Tabla 12. Actividades propuestas para la gestión de incidencias

Además, se proponen algunas actividades para implementar la gestión de incidentes, dado que el equipo encargado del desarrollo del sistema no cuenta con un manejo adecuado de incidentes o problemas:

- Definir canales de comunicación y procedimientos para reportar y registrar incidentes relacionados con otros problemas, como detecciones imprecisas, falta de documentación, entre otros.
- Establecer criterios de priorización y escalamiento para abordar los incidentes según su impacto y urgencia.
- Realizar análisis de causa raíz para identificar las razones subyacentes de los incidentes y establecer acciones preventivas.
- Mantener una base de conocimientos actualizada con soluciones, mejores prácticas y lecciones aprendidas de incidentes anteriores.
- Implementar procesos de comunicación efectiva con los stakeholders involucrados, manteniendo informados sobre el estado de los incidentes y las acciones tomadas.

5.6 Gestión de problemas

La gestión de problemas implica un conjunto de procesos y actividades diseñados para registrar, analizar, priorizar y resolver los problemas de manera estructurada y sistemática. En el contexto del sistema de detección de alarmas, la gestión de problemas desempeña un papel crucial para abordar de manera proactiva y permanente los diversos desafíos y problemas que puedan surgir. Esta práctica se enfoca en identificar las causas raíz de los problemas y establecer soluciones efectivas para evitar su recurrencia, lo que contribuye a mejorar la precisión, confiabilidad y eficiencia del sistema.

Dado que la empresa no tiene una gestión de problemas definida, es necesario establecer un proceso estructurado para abordar los problemas identificados de manera proactiva y permanente. A continuación, se describe cómo se puede implementar la gestión de problemas para abordar los problemas mencionados:

Propuesta para la creación de la Gestión de Problemas:

- **Crear un sistema de registro de problemas:** Implementar una herramienta o sistema centralizado para registrar y documentar todos los problemas identificados, incluyendo detalles como la descripción, impacto, prioridad y estado actual.
- **Definir roles y responsabilidades:** Asignar roles y responsabilidades específicos para la gestión de problemas, como el propietario del problema, el equipo de análisis de causa raíz, el equipo de resolución y el comité de revisión.
- **Establecer procesos y procedimientos:** Definir procesos y procedimientos claros para el registro, análisis, priorización, resolución y monitoreo de los problemas, asegurando un enfoque sistemático y consistente.

Problema	Descripción
Falta de documentación y especificaciones claras	Realizar un análisis de causa raíz para identificar las razones de la falta de documentación.
	Establecer un plan de acción para crear y mantener actualizada la documentación.
Falta de definición de los límites	Realizar un análisis de causa raíz para identificar por qué no se han definido los límites.
	Involucrar a expertos y stakeholders para definir los límites y rangos aceptables.
Redundancia en los datos	Analizar las causas y el impacto de la redundancia de datos.
	Establecer un plan de acción para optimizar la redundancia de datos.
Variabilidad de los datos dependiendo del canal	Realizar un análisis de causa raíz para comprender por qué el código no maneja la variabilidad por canal.
	Establecer un plan de acción para adaptar el código o implementar lógica específica por canal.
Falta de especificación de los requerimientos	Analizar las causas de la falta de especificación de requisitos.
	Involucrar a expertos y stakeholders para realizar un levantamiento y especificación de requisitos.
Generación de falsos positivos	Realizar un análisis exhaustivo de las causas de los falsos positivos.
	Establecer un plan de acción para ajustar algoritmos, reglas de detección o configuraciones del sistema.

Tabla 13. Actividades propuestas para la gestion de problemas

5.7 Gestión del conocimiento

La gestión del conocimiento implica un conjunto de prácticas y procesos diseñados para capturar, organizar, compartir y aplicar el conocimiento relevante dentro de la organización. El conocimiento es un activo invaluable que, cuando se gestiona adecuadamente, puede impulsar la mejora continua, la toma de decisiones informadas y la eficiencia en el desarrollo y mantenimiento del sistema.

En el caso del sistema de detección de alarmas, la gestión del conocimiento desempeña un papel fundamental para abordar los desafíos y problemas identificados. En este contexto se centra en aprovechar el conocimiento colectivo de los expertos, desarrolladores, analistas y otros stakeholders involucrados en el ciclo de vida del sistema.

Uno de los principales objetivos de la gestión del conocimiento es crear un repositorio centralizado y accesible que contenga información detallada sobre el código fuente, las especificaciones, los cambios realizados, las lecciones aprendidas y las mejores prácticas. Este repositorio de conocimiento servirá como una fuente confiable para comprender el sistema, sus límites, la variabilidad de datos por canal y los requisitos específicos de detección de alarmas.

Además, la gestión del conocimiento promoverá la colaboración y el intercambio de conocimiento entre los miembros del equipo, fomentando un ambiente de aprendizaje continuo. Esto permitirá abordar de manera más efectiva los desafíos relacionados con la documentación, la definición de límites, la variabilidad de datos y la especificación de requerimientos.

Problema	Actividades propuestas
	Crear un repositorio centralizado de conocimiento que contenga la documentación detallada del código fuente, las especificaciones, los cambios realizados y las explicaciones relacionadas con el sistema de detección

Falta de documentación y especificaciones claras.	de alarmas.
	Establecer procesos y prácticas para capturar y mantener actualizado el conocimiento sobre el sistema, incluyendo lecciones aprendidas, mejores prácticas y experiencias del equipo de desarrollo y mantenimiento.
Falta de definición de los límites	Documentar y compartir el conocimiento sobre los límites y rangos aceptables para la detección precisa de alarmas.
	Fomentar la colaboración y el intercambio de conocimiento entre los stakeholders y el equipo de desarrollo para definir adecuadamente los límites del sistema.
Variabilidad de los datos dependiendo del canal	Capturar y compartir el conocimiento sobre las características y variabilidad de los datos en los diferentes canales.
	Crear una base de conocimiento que permita a los desarrolladores acceder y comprender las implicaciones de la variabilidad de datos por canal.
Falta de especificación de los	Establecer un proceso de gestión del conocimiento que involucre a los stakeholders para capturar y documentar los requerimientos detallados del sistema.

requerimientos	Mantener un repositorio accesible con las especificaciones de requerimientos y el conocimiento asociado a las necesidades de detección de alarmas en cada canal.
Generación de falsos positivos	Analizar los patrones y situaciones que conducen a falsos positivos, y documentar el conocimiento adquirido sobre estos casos.
	Compartir el conocimiento sobre las soluciones y ajustes implementados para minimizar los falsos positivos en situaciones específicas.
Limitaciones de infraestructura	Capturar y compartir el conocimiento sobre las capacidades y limitaciones de la infraestructura actual del sistema.
	Documentar las lecciones aprendidas y mejores prácticas relacionadas con el escalamiento y optimización de la infraestructura para manejar grandes volúmenes de datos y nuevas funcionalidades.

Tabla 14. Actividades propuestas para la gestión del conocimiento

5.8 Gestión de la continuidad del servicio

El sistema de detección de alarmas enfrenta desafíos como la falta de documentación clara, la definición imprecisa de límites, la variabilidad de datos según el canal, la falta de especificación de requerimientos y la generación de falsos positivos. Estas deficiencias pueden provocar interrupciones o fallas en el sistema, comprometiendo la disponibilidad y la integridad de la información manejada. Por lo tanto, es crucial implementar una gestión efectiva de la continuidad del servicio para asegurar la recuperación oportuna del sistema y minimizar el impacto de las interrupciones.

Actividades propuestas:

Análisis de Impacto en el Negocio (BIA):

- Evaluar el impacto de una interrupción del sistema de detección de alarmas en términos de pérdida de datos, generación de falsos positivos y afectación a las operaciones críticas.
- Identificar los requisitos de disponibilidad y los objetivos de tiempo de recuperación aceptables.

Plan de Continuidad del Servicio:

- Desarrollar un plan detallado que incluya procedimientos para garantizar la continuidad del servicio de detección de alarmas en caso de interrupciones.
- Definir estrategias de recuperación de datos y procedimientos para mitigar los efectos de los falsos positivos durante la interrupción.

Respaldo y Recuperación de Datos:

- Implementar estrategias de respaldo periódico de los datos manejados por el sistema de detección de alarmas, incluyendo la documentación, las especificaciones y las reglas de detección.
- Establecer procedimientos de recuperación de datos para garantizar la integridad y disponibilidad de la información crítica del sistema.

Pruebas y Mantenimiento:

- Realizar pruebas periódicas del plan de continuidad del servicio y los procedimientos de recuperación, incluyendo la validación de la documentación y las especificaciones recuperadas.
- Mantener actualizado el plan de continuidad del servicio en función de los cambios en el sistema, los límites, los requisitos y las reglas de detección.

Capacitación y Concientización:

- Proporcionar capacitación al personal involucrado en la implementación del plan de continuidad del servicio, incluyendo la comprensión de la documentación y las especificaciones del sistema.
- Fomentar la conciencia sobre la importancia de la continuidad del servicio y las responsabilidades individuales en la gestión de interrupciones.

Al abordar estos aspectos en la gestión de la continuidad del servicio, el equipo puede mitigar los riesgos asociados con interrupciones o incidentes que afecten al sistema de detección de alarmas, garantizando la disponibilidad y la protección de la información crítica manejada por el sistema, así como la capacidad de recuperación ante situaciones adversas.

5.9 Mejora continua

La mejora continua es un enfoque sistemático que busca mejorar de manera constante los procesos, productos y servicios. En el contexto del sistema de detección de alarmas, la implementación de esta práctica es fundamental para abordar los desafíos existentes, como la falta de documentación clara, la definición imprecisa de límites, la variabilidad de datos según el canal, la falta de especificación de requerimientos y la generación de falsos positivos. Mediante un ciclo continuo de revisión, análisis y acciones correctivas, se puede mejorar continuamente la eficacia, precisión y confiabilidad del sistema.

Actividades propuestas:

Monitoreo y Medición:

- Establecer métricas e indicadores clave de rendimiento (KPI) para evaluar la eficacia del sistema de detección de alarmas.
- Monitorear y registrar los falsos positivos, las alertas correctas y los incidentes relacionados con el sistema.

Revisiones Periódicas:

- Realizar revisiones periódicas de la documentación, las especificaciones, los límites del sistema y las reglas de detección de alarmas.
- Evaluar la precisión, eficiencia y efectividad del sistema en función de los KPI establecidos.

Acciones Correctivas:

- Implementar acciones correctivas para abordar las deficiencias identificadas en el sistema de detección de alarmas.

- Actualizar la documentación, las especificaciones, los límites del sistema y las reglas de detección de alarmas según sea necesario.

Lecciones Aprendidas:

- Documentar y compartir las lecciones aprendidas de los incidentes, las revisiones y las acciones correctivas.
- Utilizar estas lecciones para mejorar la capacitación, los procesos y el sistema de detección de alarmas.

Mejora Continua del Sistema:

- Utilizar los hallazgos y las lecciones aprendidas para mejorar continuamente el sistema de detección de alarmas.
- Incorporar nuevas tecnologías, algoritmos o enfoques para mejorar la precisión y eficiencia del sistema.

Mediante la implementación de un enfoque de mejora continua, el equipo puede identificar y abordar de manera proactiva las deficiencias del sistema de detección de alarmas.

5.10 KPI

Para impulsar un enfoque efectivo de mejora continua en el sistema de detección de alarmas, es fundamental establecer y monitorear Indicadores Clave de Rendimiento (KPI). Estos indicadores cuantificables brindan visibilidad sobre aspectos críticos del sistema, permitiendo evaluar su eficacia, identificar áreas de mejora y realizar un seguimiento de los progresos alcanzados [17].

Los KPI actúan como señales de advertencia temprana, destacando problemas potenciales o áreas que requieren atención inmediata. Además, permiten medir el impacto de las acciones correctivas implementadas, brindando una base sólida para evaluar el progreso y ajustar estrategias según sea necesario

A continuación, se presentan los KPI propuestos, seleccionados para abordar los desafíos actuales del sistema y guiar el ciclo de mejora continua. Estos indicadores cubrirán áreas clave como la precisión, la eficiencia, la disponibilidad, la documentación, el cumplimiento de requisitos y la satisfacción del usuario.

- **Tasa de falsos positivos:** Mide el porcentaje de alarmas generadas por el sistema que resultaron ser falsas o incorrectas. Un valor bajo de este KPI indica una mayor precisión en la detección de alarmas reales.
- **Tasa de alarmas perdidas:** Mide el porcentaje de eventos o incidentes reales que no fueron detectados por el sistema como alarmas. Un valor bajo de este KPI indica una mayor capacidad de detección del sistema.
- **Tiempo promedio de respuesta:** Mide el tiempo transcurrido entre la generación de una alarma y la respuesta o acción tomada por el personal correspondiente. Un valor bajo de este KPI indica una mayor rapidez en la gestión de incidentes.
- **Disponibilidad del sistema:** Mide el porcentaje de tiempo que el sistema de detección de alarmas está operativo y accesible. Un valor alto de este KPI indica una mayor continuidad del servicio.

- **Cobertura de documentación:** Mide el porcentaje de componentes, funcionalidades y procesos del sistema que están debidamente documentados. Un valor alto de este KPI indica una mayor claridad y comprensión del sistema.
- **Conformidad con los requisitos:** Mide el grado en que el sistema cumple con los requisitos y especificaciones definidos. Un valor alto de este KPI indica una mayor alineación con las necesidades del negocio.
- **Eficiencia en el procesamiento de datos:** Mide la capacidad del sistema para procesar y analizar los datos de entrada de manera eficiente. Un valor alto de este KPI indica una mayor optimización de recursos y escalabilidad.
- **Satisfacción del usuario:** Mide el nivel de satisfacción de los usuarios o partes interesadas con respecto al rendimiento y la calidad del sistema de detección de alarmas. Un valor alto de este KPI indica una mayor aceptación y confianza en el sistema.

6. Conclusiones

El sistema actual de detección de alarmas presenta tanto puntos fuertes como áreas de mejora que requieren atención. Aunque el uso de Python y el modelo DBSCAN ofrecen ventajas, hay aspectos clave que deben mejorarse para aumentar la precisión, eficiencia y fiabilidad del sistema.

Un análisis detallado del código fuente y los falsos positivos generados fue fundamental para desarrollar una propuesta de mejora sólida que abordara los problemas identificados. Además, el análisis DOFA realizado permitió identificar áreas clave en las que se debía centrar la propuesta, proporcionando una visión clara y completa de las áreas a mejorar.

La implementación del plan de mejora continua propuesto, permitirá a la empresa fortalecer el sistema de detección de alarmas, mantenerlo actualizado y eficiente ante los nuevos desafíos y requisitos.

Es esencial involucrar a todas las partes interesadas, desde los usuarios hasta el personal técnico y operativo, en el proceso de mejora continua. Esta participación activa garantizará que el sistema se adapte a las necesidades y que se mantenga una comunicación efectiva y una gestión adecuada de los cambios. Además, promoverá una mayor comprensión y apropiación del sistema por parte de todos los actores involucrados.

Al adoptar las recomendaciones propuestas y comprometerse con la mejora continua, SLB podrá maximizar el valor del sistema de detección de alarmas, reducir los falsos positivos, mejorar la precisión y aumentar la confianza de los usuarios en el sistema. Esto, a su vez, se traducirá en una mayor eficiencia operativa, una reducción de los tiempos de inactividad innecesarios y, en última instancia, un ahorro de costos para la empresa.

7. Bibliografía

[1] "Digital Transformation Services". SLB, a global technology company | SLB. Accedido el 22 de mayo de 2024. [En línea]. Disponible: https://www.software.slb.com/services/digital-transformation-services

[2] R. Sharda, E. Turban y D. Delen, Analytics, Data Science, & Artificial Intelligence: Systems for Decision Support. Pearson, 2019.

[3] R. Hurley, *Big Data: A Guide to Big Data Trends, Artificial Intelligence, Machine Learning, Predictive Analytics, Internet of Things, Data Science, Data Analytics, Business Intelligence, and Data Mining*. Ationa Publ., 2020.

[4] D. A. Saxena, D. D. Yadav, A. Pandey y D. S. Kumar, Eds., Introduction to Data Analytics. Rubicon Publ., 2022.

[5] Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. International Journal of Information Management

[6] J. Brownlee, "What is a False Positive in Machine Learning?," Machine Learning Mastery, 08-Mar-2020. [Online]. Available: https://machinelearningmastery.com/false-positives-in-machine-learning/

[7] C. C. Aggarwal, *Outlier Analysis*. Springer, 2018.

[8] J. Han, M. Gupta, J. Gao y C. Aggarwal, *Outlier Detection for Temporal Data*. Springer Int. Publishing AG, 2014.

[9] "Detecting and Treating Outliers | Treating the odd one out!" Analytics Vidhya. Accedido el 16 de mayo de 2024. [En línea]. Disponible: https://www.analyticsvidhya.com/blog/2021/05/detecting-and-treating-outliers-treating-the-odd-one-out/

[10] "DBSCAN Clustering in ML | Density based clustering - GeeksforGeeks". GeeksforGeeks. Accedido el 16 de mayo de 2024. [En línea]. Disponible: https://www.geeksforgeeks.org/dbscan-clustering-in-ml-density-based-clustering/

[11] J. Han, J. Pei, and M. Kamber, Data Mining: Concepts and Techniques, 3rd ed. Amsterdam, Netherlands: Elsevier, 2011.

[12] "How to Master the Popular DBSCAN Clustering Algorithm for Machine Learning". Analytics Vidhya. Accedido el 22 de mayo de 2024. [En línea].

Disponible: https://www.analyticsvidhya.com/blog/2020/09/how-dbscan-clustering-works/

[13] "¿Qué es ITIL y para que sirve?" GlobalSuite Solutions. Accedido el 16 de mayo de 2024. [En línea]. Disponible: https://www.globalsuitesolutions.com/es/que-es-itil-y-para-que-sirve/#:~:text=Las%20siglas%20ITIL%20significan%20Information,de%20la%20información%20(TI).

[14] "Guía completa del marco ITIL v4" freshworks. Accedido el 16 de mayo de 2024. [En línea]. Disponible: https://www.freshworks.com/latam/freshservice/itil/itil-4/

[15] "SVS ITIL v4: ¿Cuál es el valor del Service Value System?" Proactivanet. Accedido el 16 de mayo de 2024. [En línea]. Disponible: https://www.proactivanet.com/blog/itil/svs-itil-v4-service-value-system/

[16] "Who We Are". SLB, a global technology company | SLB. Accedido el 22 de mayo de 2024. [En línea]. Disponible: https://www.slb.com/about/who-we-are

[17] SYDLE. "KPIs: ¿Qué son, cuál es su importancia y cómo utilizarlos? Ve ejemplos". Blog SYDLE. Accedido el 16 de mayo de 2024. [En línea]. Disponible: https://www.sydle.com/es/blog/kpi-615de90225ce5d3ef29a557

[18] T. A. Runkler, *Data Analytics: Models and Algorithms for Intelligent Data Analysis*. Springer Vieweg, 2020.

[19] J. Hush, *Python para el análisis de Datos: Una Guía para Principiantes para Aprender el análisis de Datos con la Programación Python*. Draft2Digital, 2020.

[20] A. Zhou, C. Jin y J. Mao, *Clustering and Outlier Detection for Trajectory Stream Data*. World Sci. Publ. Co., 2020.

[21] C. C. Aggarwal y C. K. Reddy, *Data Clustering: Algorithms and Applications*. Taylor Francis Group, 2018

[22] C. M. Bishop, *Pattern Recognition and Machine Learning*. Springer, 2016.

[23] "DBSCAN". scikit-learn. Accedido el 22 de mayo de 2024. [En línea]. Disponible: https://scikit-learn.org/stable/modules/generated/sklearn.cluster.DBSCAN.html

[24] A. Barrios. “Tutorial del Algoritmo DBSCAN en Python”. Medium. Accedido el 22 de mayo de 2024. [En línea]. Disponible: https://medium.com/latinxinai/tutorial-del-algoritmo-dbscan-en-python-d7c187c1b24f

[25] D. Llerena. “ITIL V4 101 ¿Qué es lo que necesitas saber?” Medium. Accedido el 22 de mayo de 2024. [En línea]. Disponible: https://medium.com/@davidshaek/itil-v4-101-qué-es-lo-que-necesitas-saber-adbe97111257

[26] “Delfi Data Science”. SLB, a global technology company | SLB. Accedido el 22 de mayo de 2024. [En línea]. Disponible: https://www.software.slb.com/delfi/openness/delfi-data-science