



## Análisis de capacidades predictivas para la detección de fallos en servicios críticos de TI: caso de estudio empresa ASAP BUSINESS S.A

*Predictive capabilities analysis for fault detection in critical IT services: case study of ASAP BUSINESS S.A.*

Fausto Raúl Orozco Lara\*

[fausto.orozcol@ug.edu.ec](mailto:fausto.orozcol@ug.edu.ec)

Mariela Paola Espinoza Martínez\*

[mariela.espinozam@ug.edu.ec](mailto:mariela.espinozam@ug.edu.ec)

Shirly Nathaly Moran Calderón\*

[shirley.moranc@ug.edu.ec](mailto:shirley.moranc@ug.edu.ec)

Jhonny David Mite Mendoza\*

[Jhonny.mitem@ug.edu.ec](mailto:Jhonny.mitem@ug.edu.ec)

Vanessa de Lourdes Castro Vera\*

[vanessa.castrove@ug.edu.ec](mailto:vanessa.castrove@ug.edu.ec)

\* Universidad de Guayaquil, Ecuador.

Recibido: 19/05/2025-Aceptado: 22/07/2025

Correspondencia: [fausto.orozcol@ug.edu.ec](mailto:fausto.orozcol@ug.edu.ec)

### Resumen

Este artículo surge como producto final del trabajo de titulación que tiene como tema Análisis de capacidades predictivas para la detección de fallos en servicios críticos de TI de la empresa ASAP BUSINESS S.A el objetivo de la investigación es la exploración de modelos de aprendizaje automático para predecir la congestión de CPU y RAM en entornos virtuales utilizando Zabbix para la monitorización y Grafana para la visualización, en entorno de pruebas controlado, alojado en servidores ubicados en Alemania, aplicando algoritmos como Random Forest, SVM y KNN para el entrenamiento del modelo con datos reales simulados bajo diferentes cargas. Los resultados demostraron que es posible transformar el monitoreo tradicional en un sistema inteligente de predicción, siendo Random Forest el modelo con mejor rendimiento. Esta solución no solo mejora la capacidad de reacción ante fallos inminentes, sino que abre paso a una gestión proactiva, optimizando la disponibilidad del servicio. La propuesta es replicable en otros entornos virtualizados y representa un paso hacia la integración efectiva de inteligencia artificial en la administración de infraestructuras TI. Los hallazgos de esta investigación permiten demostrar que la monitorización predictiva mejora la estabilidad operativa de manera proactiva ante posibles fallos.

**Palabras clave:** Monitoreo predictivo, aprendizaje automático, congestión de recursos, bosque aleatorio, Zabbix, entornos virtuales.

### Abstract

*This scientific article explores the implementation of machine learning models to predict CPU and RAM congestion in virtual environments using Zabbix for monitoring and Grafana for visualization. A controlled testing environment, hosted on servers located in Germany, simulates high-load conditions through the stress-ng tool, generating datasets with temporal and usage variables. The data is cleaned, structured, and processed in Python for binary classification using Random Forest, Support Vector Machine, and K-Nearest Neighbors. The models aim to identify congestion events where resource usage exceeds 85%. Evaluation metrics such as accuracy, precision, recall, and F1-score confirm that Random Forest delivers superior performance across all categories. The study highlights the effectiveness of time-based variables and demonstrates that predictive monitoring improves operational stability. It concludes that integrating artificial intelligence into existing monitoring systems enables proactive responses to potential failures, optimizes resource usage, and enhances service continuity. The research offers a replicable, low-cost methodology applicable to various IT infrastructures.*

**Keywords:** Predictive monitoring, machine learning, resource congestion, random forest, Zabbix, virtual environments.

### Cómo citar:

Orozco Lara, F. R., Espinoza Martínez, M. P., Moran Calderón, S. N., Mite Mendoza, J. D., & Castro Vera, V. de L. (2025). Análisis de capacidades predictivas para la detección de fallos en servicios críticos de TI: caso de estudio empresa ASAP BUSINESS S.A. *GADE: Revista Científica*, 5(3), 146-179. <https://doi.org/10.63549/rg.v5i3.697>



## INTRODUCCIÓN

El correcto funcionamiento de los servicios esenciales es fundamental para el sostenimiento de la sociedad moderna. Estos servicios facilitan las actividades diarias y satisfacen las necesidades básicas de las que dependen las personas e instituciones. Cuando un servicio falla o se interrumpe, sus efectos se extienden más allá de los usuarios inmediatos, pudiendo provocar interrupciones en sistemas más amplios.

Gómez (2022) expresa “que uno de los grandes problemas que suelen encontrarse muchas empresas tras integrar un ERP en sus sistemas, sea nueva implantación o actualización de una ya existente, es la carencia que tienen los empleados del conocimiento de la herramienta” (p. 66). Un desafío común que enfrentan las organizaciones tras la integración de sistemas de planificación de recursos empresariales (ERP) es la falta de conocimientos prácticos del personal sobre cómo usar el software eficazmente. Esta falta de conocimiento práctico puede dificultar la eficiencia del flujo de trabajo, retrasar los procesos de adaptación y provocar la infrutilización de funciones indispensable.

Sin la formación adecuada ni las estructuras de apoyo internas necesarias, los empleados pueden tener dificultades para navegar por el sistema, cometer errores al introducir datos o generar informes, y resistirse por completo a la transición. Como resultado, las mejoras previstas en la coordinación, la toma de decisiones y la productividad no se materializan plenamente, lo que socava la inversión en la plataforma y puede interrumpir las operaciones diarias.

Desde la escasez de recursos hasta la interrupción de operaciones críticas, las consecuencias subrayan la importancia de garantizar la continuidad del servicio.

Los servicios de Tecnologías de la Información (TI) desempeñan un papel decisivo en el rendimiento organizacional.

Peña y Anías (2020) comunican que “la organización debe incentivar la adopción de marcos de referencia tanto para la realización de sus procesos TI como para el gobierno y la gestión de las infraestructuras TI” (p. 37). Es esencial que una organización promueva enfoques estructurados que guíen la implementación y supervisión de las operaciones tecnológicas. Esto garantiza



la coherencia, la alineación con los estándares del sector y la utilización eficiente de los recursos. Al seguir modelos establecidos, la empresa puede lograr roles más claros, una mejor gestión de riesgos y una mayor rendición de cuentas entre los departamentos.

Estos marcos también ofrecen un lenguaje y una metodología comunes, lo que facilita una colaboración e integración más fluidas entre los equipos de negocio y de TI. En definitiva, esta base estructurada mejora la toma de decisiones, respalda los objetivos estratégicos y garantiza que la tecnología contribuya a los objetivos generales de la organización de forma eficaz y sostenible.

Su funcionamiento ininterrumpido facilita el manejo eficiente de datos, la comunicación interna y la automatización de procesos. La falla de estos servicios puede provocar una disminución de la productividad, la pérdida de confianza del cliente y retrasos en la toma de decisiones. Por lo tanto, mantener una infraestructura de TI fiable y siempre disponible, es una prioridad para las empresas que buscan preservar la resiliencia operativa.

En un contexto empresarial, no todos los servicios de TI tienen el mismo valor estratégico.

Miñana (2025) manifiesta “que la TI puede ahora interconectar al personal con los clientes y con los ordenadores, y existe la capacidad de proporcionar servicios de valor añadido a los clientes mediante procesos de transacción automáticos” (págs. 32-33). Los sistemas tecnológicos modernos facilitan una interacción fluida entre el personal interno, los usuarios finales y las plataformas digitales, creando un entorno empresarial más cohesionado y ágil. Estos avances permiten a las empresas optimizar las operaciones y mejorar la experiencia del cliente al reducir la intervención manual en tareas repetitivas.

Como resultado, los servicios se vuelven más rápidos, precisos y personalizados, lo que aumenta la satisfacción y la fidelización. Además, la automatización reduce los errores y los costes operativos, permitiendo a las empresas reasignar recursos humanos a actividades de mayor valor, como la innovación y la estrategia. Esta sinergia entre la conectividad y la automatización refuerza la competitividad en mercados dinámicos.



Algunos se consideran esenciales porque su interrupción pone en peligro la continuidad de las operaciones principales. Estos se denominan servicios de TI críticos, y su gestión exige atención proactiva. Sin los mecanismos adecuados de monitorización y detección de fallos, incluso breves periodos de inactividad pueden afectar la continuidad del negocio y la reputación corporativa.

Jaramillo y Ortiz (2020) declaran “que la implementación de herramientas de monitorización y alerta temprana permitirá que la atención de todos los incidentes relacionados con los servicios críticos migrados a la nube pública se los atienda de manera oportuna y eficaz” (p. 288). La integración de sistemas de vigilancia y mecanismos de alerta predictiva permite a las organizaciones detectar irregularidades en operaciones esenciales basadas en la nube antes de que se intensifiquen. Este enfoque proactivo facilita la toma de decisiones rápida y la intervención inmediata, minimizando posibles interrupciones y manteniendo la continuidad del servicio.

Al identificar vulnerabilidades de forma temprana, los equipos de TI pueden asignar recursos de forma más eficiente y aplicar medidas correctivas

que preservan la integridad y el rendimiento del sistema. Estas estrategias son esenciales en entornos de nube dinámicos, donde los retrasos en la respuesta podrían comprometer la seguridad, la disponibilidad o la satisfacción del cliente. En definitiva, esto mejora la fiabilidad operativa y fortalece la confianza en las infraestructuras alojadas en la nube.

Los servicios críticos de TI garantizan la estabilidad de las funciones empresariales, especialmente bajo presión. Deben ser fiables, pero también resilientes, lo que significa que tienen adaptarse a incidentes inesperados y recuperarse rápidamente de las fallas. En una era donde la prestación de servicios en tiempo real es un estándar, el énfasis en la monitorización proactiva nunca ha sido tan relevante.

ASAP BUSINESS S.A., es una empresa tecnológica ecuatoriana con sede en Guayaquil, opera en un competitivo panorama de servicios digitales. Desde su fundación en 2019, la empresa ha brindado soluciones de desarrollo web, alojamiento en la nube, marketing digital y soporte técnico, principalmente a pequeñas y medianas empresas.



La base de sus servicios se aloja en servidores dedicados ubicados en Alemania, incluyendo componentes críticos como alojamiento, correo electrónico y sistemas de copia de seguridad de datos. A pesar de contar con una sólida infraestructura técnica, la empresa actualmente enfrenta desafíos para garantizar la disponibilidad ininterrumpida de sus servicios críticos de TI. La dependencia de la monitorización manual a través de Cloud Linux obliga al personal técnico a realizar comprobaciones repetitivas sin la ayuda de alertas automatizadas. Este enfoque retrasa los tiempos de respuesta ante incidentes y disminuye la calidad general del servicio ofrecido a los clientes.

El sistema actual de la empresa carece de la capacidad predictiva necesaria para prever anomalías o fallos inminentes. Como resultado, los problemas solo se detectan después de que afectan a los usuarios, lo que genera insatisfacción del cliente, interrupciones en el flujo de trabajo y un menor nivel de credibilidad del servicio. La ausencia de un modelo de monitorización proactiva pone en riesgo tanto la calidad del servicio como la continuidad del negocio.

La estrategia reactiva de la organización es insuficiente en un ecosistema digital donde la prevención prima sobre la corrección. Las interrupciones en servicios como el alojamiento web o el correo electrónico tienen efectos inmediatos y tangibles, que pueden incluir la pérdida de transacciones, comunicaciones fallidas o la desconexión del cliente.

Gómez J (2025) menciona que “las inversiones innovadoras y avances tecnológicos propuestos desde TI impactan siempre de forma directa los objetivos de negocio, puesto que alguna de estas que falle, representa normalmente altas pérdidas de tiempo y dinero, además de retrasos en la estrategia” (p. 96). Cuando el departamento de TI propone iniciativas con visión de futuro o adopta tecnologías emergentes, inevitablemente determina el progreso de la organización hacia sus objetivos. Estos esfuerzos están estrechamente vinculados a la planificación de recursos y los plazos de ejecución, lo que significa que cualquier contratiempo en su implementación puede afectar negativamente a los esfuerzos estratégicos más amplios.

Las consecuencias no se limitan a las dificultades financieras, sino que



también incluyen ineficiencias operativas y la pérdida de oportunidades. Por lo tanto, el éxito o el fracaso de los esfuerzos tecnológicos desempeña un papel fundamental en la trayectoria general y la competitividad del negocio, lo que hace indispensable una planificación cuidadosa, la evaluación de riesgos y la alineación con la estrategia corporativa. Este contexto motiva la necesidad de una solución más avanzada y automatizada. La adopción de capacidades predictivas representa una oportunidad significativa para mejorar la gestión de estos servicios críticos.

Meriño (2022) explica “que aplicar técnicas de recomendación basada en un sistema centrado en el conocimiento, puede ser una opción viable para implementar en las soluciones automatizadas de los diferentes servicios tecnológicos que ofrece el área de TI” (p. 49). La integración de algoritmos de sugerencias basados en repositorios de información estructurada permite a los servicios de TI operar con mayor autonomía y precisión.

Este enfoque ayuda a adaptar las respuestas y soluciones según patrones, casos o mejores prácticas previamente almacenados, lo que reduce el tiempo de respuesta y mejora la consistencia en la

toma de decisiones. Al integrar esta lógica en plataformas automatizadas, el departamento de TI mejora la eficiencia y brinda a los usuarios un soporte más relevante y oportuno. También contribuye al aprendizaje organizacional, ya que cada interacción puede enriquecer la base de datos del sistema, creando un ciclo continuo de mejora y adaptación en todos los servicios digitales.

Mediante herramientas de monitorización de código abierto integradas con modelos básicos de aprendizaje automático, es posible pasar de respuestas reactivas a estrategias predictivas que anticipan fallos y activan intervenciones tempranas.

Orosco (2023) señala “que automatizar el entorno de las TI se puede lograr grandes progresos para la empresa como crear modelos de seguridad de red, configuración de aplicaciones, disponibilidad del sistema, mejorar el rendimiento etc.” (p. 1). La automatización de la infraestructura tecnológica permite a la organización optimizar las operaciones esenciales, garantizando que los sistemas se mantengan ágiles, seguros y adaptables a las demandas cambiantes.



Reduce el error humano al estandarizar las tareas repetitivas y permite una implementación más rápida de actualizaciones y configuraciones. Con flujos de trabajo predefinidos y supervisión en tiempo real, la empresa puede gestionar mejor el uso de los recursos, detectar irregularidades rápidamente y mantener altos niveles de continuidad operativa. Además, esta automatización facilita la supervisión proactiva de los activos digitales, lo que aumenta la resiliencia del entorno ante las amenazas y lo alinea mejor con los objetivos de rendimiento.

Esta transición permitiría a la empresa detectar patrones anormales y anomalías de rendimiento antes de que se conviertan en interrupciones graves del servicio. La capacidad de analizar datos históricos y extraer tendencias de comportamiento puede servir de base para realizar predicciones precisas y automatizar la toma de decisiones dentro del ecosistema de operaciones de TI.

Este cambio mejora la resiliencia de los servicios de TI, y optimiza la asignación de recursos. Al minimizar la carga de trabajo manual del personal técnico, la organización puede redirigir los esfuerzos humanos hacia la innovación, la planificación estratégica y

la mejora del servicio, en lugar de la revisión constante del sistema.

La integración de herramientas de monitorización de código abierto proporciona una base rentable para pymes como ASAP BUSINESS S.A. Estas herramientas permiten el seguimiento en tiempo real de las métricas del servicio y, al combinarse con el aprendizaje automático, pueden evolucionar hacia sistemas inteligentes capaces de automejorarse mediante la retroalimentación de datos. Además, la monitorización predictiva mejora la transparencia y la rendición de cuentas en las operaciones de TI.

Las partes interesadas acceden a informes detallados de rendimiento y pueden evaluar la eficacia de las medidas preventivas, fomentando una cultura de mejora continua y una toma de decisiones basada en datos. En este contexto, este estudio analiza las capacidades predictivas de ASAP BUSINESS S.A. en la gestión de sus servicios críticos de TI. El estudio enfatiza cómo las tecnologías abiertas y los modelos de aprendizaje automático pueden aplicarse para crear un sistema de alerta temprana que reduzca los tiempos de inactividad y preserve la confianza del cliente.



Manrique, et al. (2021) indican que:

(...) es relevante realizar un análisis de herramientas de código abierto para el monitoreo de redes, ayudando a los procesos en el área de Tecnologías de la Información (TI), donde la gestión de la tecnología adquirida se convierte en un punto vital para cualquier organización. (p. 28)

Evaluar soluciones gratuitas para supervisar la infraestructura de red ofrece ventajas estratégicas a las organizaciones que buscan optimizar sus operaciones digitales. Estas herramientas suelen ofrecer flexibilidad, rentabilidad y mejoras impulsadas por la comunidad que se adaptan a las necesidades específicas de la organización. En los departamentos de TI, donde es fundamental mantener el control sobre el rendimiento del sistema y la disponibilidad de recursos, estas herramientas facilitan una mejor visibilidad y capacidad de respuesta.

Su integración en las operaciones garantiza que los sistemas se mantengan eficientes, escalables y alineados con las demandas de la organización, lo que mejora la capacidad de gestionar entornos complejos sin depender únicamente de plataformas propietarias.

Este artículo describe el problema inicial, derivado de las limitaciones de la monitorización manual, y propone una solución basada en el análisis predictivo. La finalidad es demostrar cómo incluso las pequeñas y medianas empresas pueden implementar sistemas inteligentes de detección de fallos sin necesidad de grandes inversiones en tecnologías propietarias.

Por lo tanto, la investigación contribuye al campo más amplio de la Ingeniería de Tecnologías de la Información al ofrecer un caso práctico sobre la aplicación de técnicas de gestión proactiva de servicios. Destaca el potencial de las herramientas de código abierto, y el análisis predictivo como soluciones accesibles y prácticas, para aumentar la resiliencia operativa en entornos de servicios digitales.

## **METODOLOGÍA**

Esta investigación adopta un enfoque cuantitativo, aplicado y experimental para diseñar, implementar y evaluar un sistema de monitoreo predictivo basado en métricas de infraestructura de TI.

Arribas, et al. (2021) relatan que las investigaciones:

(...) se han inclinado más hacia el enfoque cuantitativo donde el dato



numérico adquiere un valor ponderante, así como el tratamiento estadístico, y por supuesto, la comprobación del planteamiento hipotético, el cual niega dialécticamente el conocimiento existente y expresa el tránsito hacia el conocimiento nuevo en forma de probabilidad. (p. 185).

En las prácticas de investigación contemporáneas, en particular en las ciencias naturales y sociales, se observa una notable transición hacia metodologías que priorizan los datos que pueden medirse y analizarse sistemáticamente. Esta orientación permite a los investigadores asignar importancia a los resultados observables y aplicar procedimientos estadísticos para interpretar los hallazgos con rigor. Este enfoque también apoya el análisis de supuestos teóricos, fomentando su contrastación con la evidencia del mundo real.

A través de este proceso, se examinan y refinan los conocimientos previos, lo que conduce a perspectivas más precisas o completamente nuevas. Esta transición se basa en la idea de que el conocimiento evoluciona mediante la evaluación y validación continuas, donde las probabilidades ofrecen una forma estructurada de representar la

incertidumbre y el progreso. El estudio se lleva a cabo en un entorno virtual controlado que simula el contexto operativo de ASAP BUSINESS S.A., utilizando tecnologías de virtualización, recopilación de datos, procesamiento y aprendizaje automático.

Zuloaga (2021) cuenta que “la evaluación se realiza mediante métricas del rendimiento y mediante representación y análisis del resultado de las mediciones” (p. 43). Los procesos de evaluación se basan fundamentalmente en indicadores cuantificables que capturan la eficacia o eficiencia de un sistema, proceso o intervención. Estas métricas sirven como puntos de referencia objetivos para medir el éxito o identificar áreas que necesitan mejora. Los datos recopilados se organizan y examinan sistemáticamente, lo que permite una visualización clara de las tendencias y patrones de rendimiento. Esta fase analítica proporciona información valiosa que fundamenta la toma de decisiones y guía las acciones posteriores.

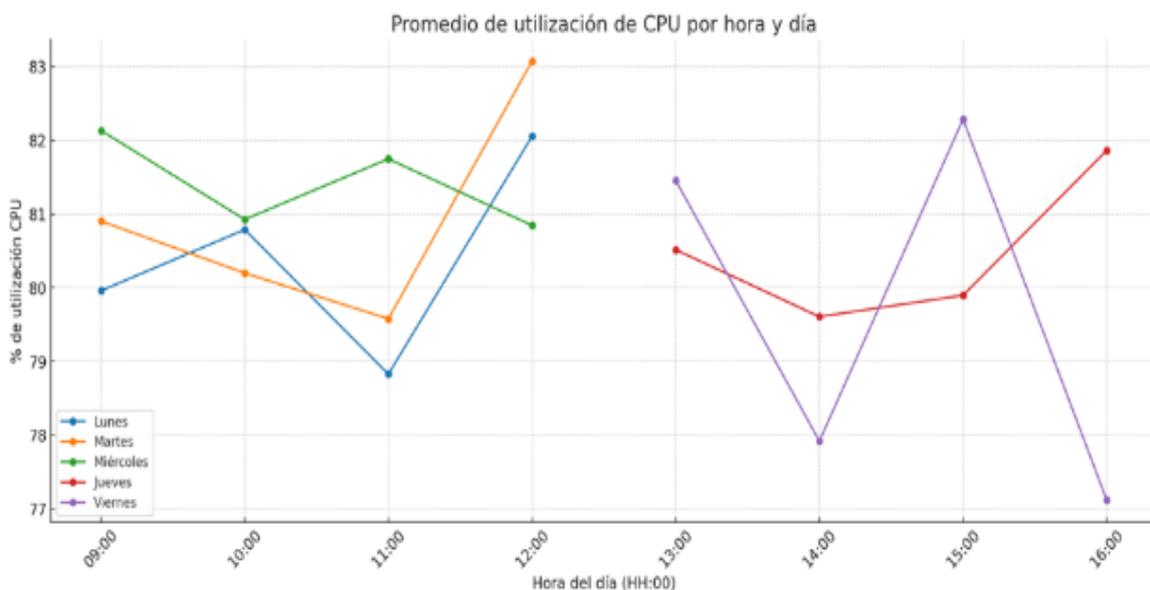
Al traducir las mediciones brutas en representaciones comprensibles, las partes interesadas pueden comprender mejor los resultados y emitir juicios basados en la evidencia para optimizar



los resultados futuros. La primera etapa consiste en configurar la infraestructura tecnológica mediante la instalación del hipervisor Proxmox VE, que permite la creación de múltiples máquinas virtuales (VM) que simulan los servicios de TI críticos de la empresa. Esta arquitectura virtualizada ofrece un espacio seguro y flexible para generar, probar y monitorear el comportamiento de los servicios en condiciones reales.

Dentro del entorno Proxmox, se configuran varias máquinas virtuales

para alojar servicios esenciales y facilitar la extracción de métricas. El monitoreo se realiza a varios niveles: métricas a nivel de nodo, como el tiempo de actividad y el uso de CPU, el consumo de recursos específicos de la VM y los indicadores de estado del almacenamiento. Estas métricas constituyen la base para analizar el rendimiento del sistema y detectar anomalías o fallos.



*Nota.* Carga sostenida como indicador de que servidor opera de forma cercana a su límite de capacidad.

**Figura 1.** *Proceso de búsqueda y criterios de selección bibliográfico*

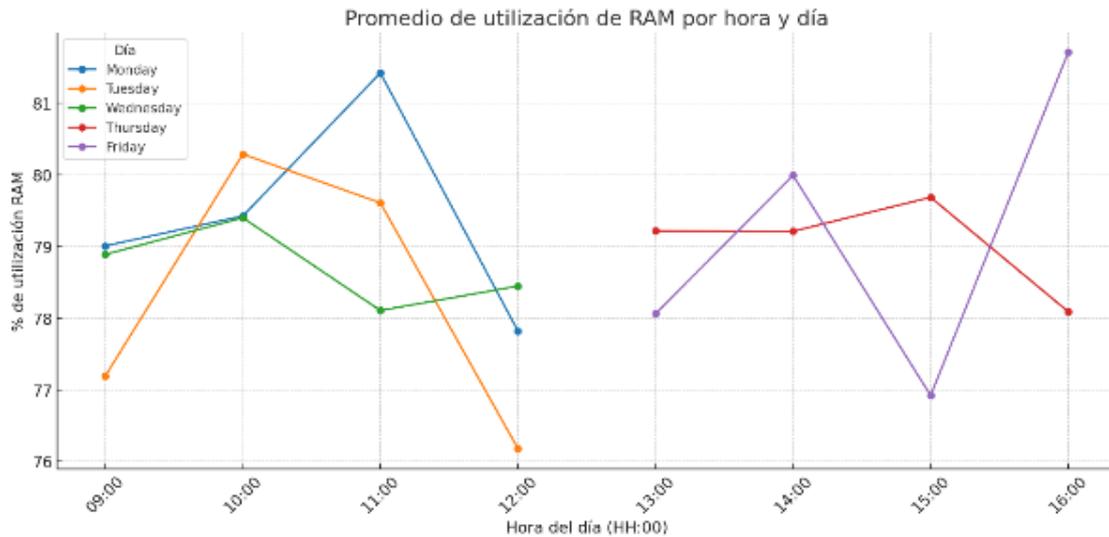
La figura 1 ilustra cómo varía el uso promedio de la CPU a lo largo de la semana laboral y en franjas horarias específicas, destacando las diferencias en los patrones de demanda entre la mañana y la tarde. Las fluctuaciones

sugieren que ciertos períodos impulsan constantemente el sistema hacia una mayor actividad de procesamiento, lo que puede indicar un estrés de rendimiento. Esto es especialmente evidente en los días en que los valores graficados se acercan al límite superior



del rango de utilización, lo que indica una intensidad operativa que podría sobrecargar el servidor si se mantiene. Identificar estas tendencias es crucial para anticipar una posible degradación del servicio y optimizar la asignación de

recursos. Reconocer períodos de uso elevado facilita la toma de decisiones estratégicas para la planificación de la capacidad y ayuda a garantizar la disponibilidad continua del sistema, como se visualiza en la figura 2.



*Nota.* Evidencia de patrón de uso elevado y persistente de la memoria, con promedios que se mantienen en el rango del 79% al 81%.

**Figura 2.** Promedio de utilización de CPU por hora y día.

Los datos mostrados revelan una presión constante sobre la capacidad de procesamiento del sistema a lo largo de diversos intervalos de tiempo y días laborables. La mínima variación en los valores sugiere una carga estable pero elevada, lo que implica que el servidor opera regularmente cerca de su umbral de eficiencia superior. Este nivel de uso, si se mantiene durante períodos prolongados, puede provocar una reducción del rendimiento, un posible sobrecalentamiento o retrasos en los tiempos de respuesta. Este patrón

subraya la importancia de la monitorización proactiva y las estrategias predictivas, ya que indica la necesidad de optimizar las cargas de trabajo o escalar la infraestructura para evitar problemas operativos a largo plazo.

Muñoz (2024) afirma que: El objetivo de Zabbix es dar una solución al monitoreo de redes, equipos, máquinas virtuales, servidores, bases de datos, sitios web, la nube, aplicaciones, etc. Esta aplicación nos va a permitir registrar y conocer en tiempo real el



estado e historial de las interfaces OpenZR. (p. 34).

Zabbix funciona como una herramienta integral diseñada para supervisar diversos entornos tecnológicos mediante la recopilación y presentación de datos operativos en tiempo real. Su versatilidad reside en su capacidad para observar el comportamiento de activos físicos y virtuales, incluyendo plataformas en la nube y servicios digitales, ofreciendo información sobre tendencias y anomalías de rendimiento. Al aplicarse a interfaces como OpenZR, permite una visibilidad continua de su estado operativo, garantizando la detección inmediata de cualquier irregularidad. Esta supervisión proactiva mejora la fiabilidad del sistema y facilita la toma de decisiones informadas, contribuyendo a la eficiencia y estabilidad general de la infraestructura de TI.

La solución de monitorización principal se implementa mediante Zabbix 7.2, una plataforma de monitorización de código abierto instalada en una máquina virtual dedicada con Ubuntu Server 22.04 LTS. La configuración incluye monitorización con y sin agente de los indicadores clave de rendimiento (KPI) en toda la

infraestructura virtual. Esta configuración permite la recopilación de datos de series temporales para el modelado predictivo.

Arosemena (2022) confirma “que los indicadores claves de desempeño, o KPIs por sus siglas en inglés, forman parte del conjunto de métricos que la administración moderna utiliza para saber si el negocio está logrando los objetivos y metas planteadas por la gerencia” (p. 50). Los KPI sirven como herramientas de medición estratégica que ayudan a las organizaciones a monitorear su progreso hacia los objetivos predefinidos. Estos indicadores convierten datos operativos complejos en información práctica, lo que permite a los líderes evaluar la alineación entre los resultados actuales y los esperados.

Al centrarse en dimensiones específicas del rendimiento, los responsables de la toma de decisiones pueden identificar rápidamente las fortalezas, abordar las ineficiencias y ajustar los planes para mantener el rumbo. Este proceso fomenta la rendición de cuentas y apoya la gestión basada en datos en diversas áreas funcionales. Para que Zabbix pueda funcionar eficazmente, se instalan todas



las dependencias de software necesarias, incluyendo apt-transport-https y curl, y se integra de forma segura con el repositorio MariaDB. Se elige MariaDB en lugar de MySQL por su rendimiento mejorado, sus capacidades de recuperación y su compatibilidad con JSON. Es completamente de código abierto y admite un sólido desarrollo comunitario.

Cornejo (2022) expuso “MariaDB es en realidad una bifurcación clave de MySQL, lo que conlleva a tener o necesitar siempre una estrategia planificada para pasar de un sistema a otro” (p. 28).

MariaDB surge como una alternativa destacada a MySQL, desarrollada para garantizar la continuidad y la compatibilidad, a la vez que ofrece funciones y rendimiento mejorados. La transición entre estos sistemas de bases de datos requiere una planificación cuidadosa debido a las diferencias en los detalles de implementación, el control de versiones y ciertas funcionalidades que pueden afectar los flujos de trabajo existentes. Las organizaciones deben evaluar las capas de compatibilidad, los procesos de migración de datos y las dependencias del sistema para evitar interrupciones.

Una hoja de ruta de migración bien estructurada es esencial para mantener la integridad de los datos, garantizar la disponibilidad del servicio y aprovechar las mejoras que MariaDB introduce, minimizando al mismo tiempo los riesgos operativos.

La base de datos de Zabbix está alojada en MariaDB 11.4 y se configura mediante archivos de repositorio personalizados para garantizar el acceso a paquetes estables, seguros y actualizados. Los scripts y las claves de instalación se almacenan en `/etc/apt/keyrings`, y el servidor de la base de datos está vinculado al frontend y a los componentes del servidor de Zabbix, lo que permite una monitorización completa.

El sistema de monitorización recopila métricas como el estado del nodo (en línea/fuera de línea), el tiempo de actividad, el porcentaje de uso de la CPU, el uso de memoria (total, usada y libre), la carga promedio del sistema y el estado de las máquinas virtuales (en ejecución, en pausa, detenidas). Estos indicadores son fundamentales para detectar señales tempranas de congestión o fallos del sistema.

Además, Zabbix recopila datos de los grupos de almacenamiento de



Proxmox (ZFS, LVM, etc.), incluyendo tasas de error, latencia de disco y operaciones de entrada/salida por segundo. Este enfoque de monitorización integral garantiza una visibilidad completa del estado de las capas de infraestructura física y virtual. Una vez recopilados suficientes datos históricos, se exportan y procesan con Python en el entorno Jupyter Lab proporcionado por Anaconda Navigator. Los datos se estructuran en formato CSV e incluyen la utilización de la CPU, el día de la semana y los minutos transcurridos desde la medianoche. La variable objetivo es binaria: "congestión  $\geq 85\%$ ", lo que indica una sobrecarga del sistema.

Para evaluar la capacidad predictiva, se aplican algoritmos de aprendizaje automático supervisado: Bosque aleatorio, K-Vecinos más cercanos (KNN) y Máquina de vectores de soporte (SVM). Cada modelo se evalúa mediante una validación cruzada de 10 pasos para garantizar la robustez estadística y evitar el sobreajuste.

Manrique, et al. (2021) aseguran que "la detección oportuna de fallos a través del monitoreo de red, son técnicas que tienen una gran importancia para poder brindar un buen servicio a los usuarios internos dentro de una

organización" (p. 15). La identificación temprana de problemas en una infraestructura de red es fundamental para garantizar la continuidad y la calidad de las operaciones internas. Mediante la observación constante del comportamiento del sistema, las organizaciones pueden prevenir interrupciones que podrían afectar la productividad de los empleados o el acceso a recursos críticos.

Este enfoque proactivo promueve la estabilidad operativa, facilita una intervención rápida ante anomalías y mejora la experiencia general del usuario en todos los departamentos. K-Vecinos Más Cercanos (configurado con  $k=153$  y utilizando el algoritmo de búsqueda `kd_tree`) también ofrece resultados sólidos, con una precisión promedio del 94,37 % y una desviación estándar del 2,36 %. Sin embargo, su rendimiento es ligeramente más variable y requiere un mayor esfuerzo computacional durante la fase de predicción.

Bodero & Navas (2020) mencionan "conocer la arquitectura y la tendencia de los centros de datos es muy cambiante y dependiente a la finalidad del centro de datos y del modelo de negocio que este por aplicar" (p. 19). Comprender el diseño estructural y la



evolución de los centros de datos requiere considerar sus funciones específicas y el enfoque estratégico de cada organización. La configuración y las tecnologías adoptadas se definen por las prioridades operativas, ya sea que se centren en el almacenamiento, el procesamiento o la prestación de servicios.

Estos factores influyen en las decisiones sobre escalabilidad, eficiencia energética e integración de sistemas, las cuales deben alinearse con los objetivos de la organización y las expectativas de los clientes. Por lo tanto, ningún modelo único se adapta a todos los escenarios, y la adaptabilidad se vuelve esencial para satisfacer las diversas demandas. La Máquina de Vectores de Soporte (SVM), aunque teóricamente robusta, ofrece una precisión considerablemente menor, del 67,62 %, con una desviación estándar del 11,23 %. Esto puede deberse al kernel predeterminado (RBF) y a la falta de escalado de características o ajuste de hiperparámetros previos, lo que destaca la sensibilidad del algoritmo a la distribución y configuración de los datos.

Leukel, et al. (2021) expresan “que la predicción de fallos consiste en pronosticar si un sistema material de

interés fallará en un momento específico en el futuro. Esta tarea cobra relevancia para las estrategias de mantenimiento industrial, como el mantenimiento predictivo” (p. 1). Anticipar las averías de los componentes físicos es determinante para optimizar los procedimientos de mantenimiento en entornos técnicos.

Esta previsión permite a las industrias actuar antes de que los daños se agraven, minimizando el tiempo de inactividad y prolongando la vida útil de los activos. Incorporar estas proyecciones en la planificación del mantenimiento mejora la rentabilidad, la seguridad y la fiabilidad operativa, al garantizar que las intervenciones se realicen solo cuando sean necesarias, en lugar de hacerlo según un cronograma fijo o después de que se produzcan fallos.

Vásquez (2021) matiza que “Scikit-Learn es una librería de Python, relacionada con el campo de ML. Esta librería permite la implementación de algoritmos de aprendizaje supervisados, tales como regresión lineal, Support vector machine (SVM), árboles de decisión, entre otros” (p. 25). Este kit de herramientas basado en Python desempeña un papel fundamental en el aprendizaje automático, ya que ofrece



herramientas que facilitan el uso de algoritmos diseñados para aprender de datos etiquetados.

Proporciona a desarrolladores e investigadores funciones accesibles para construir modelos capaces de realizar predicciones o clasificaciones basadas en datos conocidos. La biblioteca simplifica el proceso de desarrollo, permitiendo la experimentación eficiente con diversas técnicas que descubren patrones y relaciones dentro de los conjuntos de datos, lo que en última instancia facilita la toma de decisiones basada en datos en diversas aplicaciones.

Para investigar más a fondo la importancia de las variables, se realizó un experimento adicional entrenando el modelo KNN sin la variable de utilización de la CPU, basándose únicamente en características temporales. La precisión resultante se redujo significativamente al 58,42 %, lo que confirma el papel predictivo crucial del uso de la CPU en la predicción de la congestión.

Villa (2020) expresa “que se espera que la abundancia de datos se multiplique cada vez más a través del Internet de las cosas, redes sociales y análisis de Big Data, y que la capacidad de procesamiento siga en aumento” (p.

19). La constante expansión de dispositivos interconectados, contenido generado por el usuario y tecnologías analíticas impulsa un crecimiento sin precedentes en el volumen de información. A medida que evolucionan los ecosistemas digitales, los sistemas deben adaptarse para gestionar flujos de entrada más grandes y complejos. Esta dinámica impulsa la demanda de marcos computacionales robustos capaces de transformar la información sin procesar en información práctica.

La mejora continua en la capacidad de procesamiento garantiza que las organizaciones puedan seguir el ritmo de este auge, lo que permite respuestas en tiempo real y estrategias más informadas en todos los sectores. Los modelos entrenados se serializan mediante la biblioteca joblib para lograr persistencia e implementación eficiente. Joblib permite guardar y cargar modelos sin necesidad de reentrenamiento, lo que la hace ideal para entornos de producción e integración en tiempo real en paneles de monitoreo o sistemas de alerta.

Al evaluar continuamente el comportamiento en relación con las expectativas regulatorias o internas, las empresas mejoran la transparencia y reducen el riesgo de incumplimiento.



Cada modelo se guarda como un archivo .csv, se recarga y se prueba en el conjunto de validación para confirmar un rendimiento consistente. Se generan DataFrames con predicciones para facilitar el análisis posterior y la interpretación de los resultados del modelo en diferentes condiciones operativas. Por último, se crearon visualizaciones con Matplotlib para comparar el rendimiento del algoritmo. Se graficaron las métricas de precisión y las barras de error que representan la desviación estándar para cada modelo, destacando Random Forest por su superior precisión y estabilidad, seguido de KNN y SVM.

Espinoza (2020) menciona: Las ventajas de Random Forest hacen que se convierta en una técnica ampliamente utilizada en muchos campos, por ejemplo, teledetección (para clasificación de imágenes), bancos (para detección de fraudes y clasificación de clientes para otorgamiento de crédito), medicina (para analizar historiales clínicos a fin de identificar enfermedades potenciales en los pacientes), finanzas (para pronosticar comportamientos futuros de los mercados financieros) y comercio electrónico (para pronosticar si un cliente comprará, o no, cierto

producto), entre otros. (p. 3) Random Forest destaca por su versatilidad y robustez, lo que permite su integración en diversos dominios que requieren una clasificación precisa o modelado predictivo. Su capacidad para gestionar grandes volúmenes de datos de entrada, gestionar relaciones no lineales y minimizar el sobreajuste mediante el aprendizaje por conjuntos lo hace especialmente eficaz en escenarios complejos. En sectores como la salud, las finanzas y el comercio digital, facilita la toma de decisiones al descubrir patrones y tendencias que fundamentan diagnósticos, evaluaciones de riesgos o comportamientos del consumidor. Su capacidad para procesar variables categóricas y continuas, junto con su alto rendimiento incluso con datos incompletos o con ruido, refuerza su atractivo como herramienta analítica fiable en entornos basados en datos.

Para evaluar el rendimiento predictivo de diversos algoritmos de aprendizaje automático supervisado, se realizó una serie de experimentos utilizando el conjunto de datos derivado del sistema de monitorización de infraestructura de ASAP BUSINESS S.A. Estos experimentos excluyeron ciertas métricas del sistema para analizar



la capacidad predictiva que se conserva al utilizar únicamente variables temporales. Esta elección metodológica permite al estudio evaluar la importancia y la influencia de cada tipo de variable en la predicción de eventos críticos de congestión.

El primer modelo implementado sin la variable CPU es K-Vecinos Más Cercanos (KNN). Este enfoque busca determinar la capacidad del algoritmo para distinguir escenarios de congestión basándose únicamente en características temporales como el día de la semana y los minutos transcurridos desde la medianoche. Tras el preprocesamiento, el modelo se entrenó y se almacenó en joblib con el nombre `modelo_knn_sin_cpu.sav`. Tras la evaluación, el modelo obtuvo una precisión del 58,42 %, considerablemente inferior al 75,05 % obtenido al incluir la métrica CPU.

Esto destaca el papel que desempeñan las métricas de rendimiento del sistema en una clasificación eficaz. A continuación, se desarrolla un clasificador de Bosque Aleatorio bajo condiciones restringidas similares, excluyendo el porcentaje de uso de CPU. El modelo utiliza únicamente variables temporales como predictores, y los datos

se procesan mediante módulos de Pandas y Scikit-Learn. Tras el entrenamiento y la evaluación, el modelo alcanza sorprendentemente una precisión del 98,96 %.

Ardila (2023) informa que: “Pandas es una librería de Python para manipulación y análisis de datos. Con Pandas, se pueden cargar, procesar y analizar datos desde diversas fuentes de datos, incluyendo archivos CSV, Excel, bases de datos SQL y más” (p. 2). Pandas funciona como un componente esencial en el ecosistema de ciencia de datos de Python, permitiendo organizar, transformar e interpretar datos estructurados de forma eficiente. Su sintaxis intuitiva y sus potentes estructuras de datos, como DataFrames, permiten a los usuarios limpiar, filtrar, remodelar y agregar información con facilidad.

Esta adaptabilidad a diversos formatos de entrada optimiza los flujos de trabajo y facilita una integración fluida con otras herramientas analíticas. Al simplificar operaciones complejas en comandos concisos, facilita la experimentación rápida y la exploración exhaustiva, cruciales para obtener información significativa de conjuntos de datos sin procesar. Este resultado



inesperadamente alto sugiere que, en el entorno de simulación específico utilizado, los eventos de congestión están altamente modelados en función del tiempo, probablemente debido a condiciones de carga repetidas.

Al evaluar diferentes plataformas de visualización para sistemas de monitorización, Grafana destaca por su adaptabilidad, integración nativa y facilidad de uso. Admite diversas fuentes de datos, incluyendo Zabbix, sin necesidad de un backend dedicado, lo que la hace ideal para diversas infraestructuras. Su interfaz es intuitiva y permite una amplia personalización del

**Tabla 1.**

*Comparativa entre herramientas de visualización*

<b>Criterio</b>	<b>Grafana</b>	<b>Kibana</b>	<b>Prometheus Console</b>
<b>Enfoque principal</b>	Visualización de métricas en tiempo real	Análisis de logs y búsquedas complejas	Visualización simple de métricas de Prometheus
<b>Compatibilidad con Zabbix</b>	Nativa (plugin oficial disponible)	No compatible directamente	No compatible directamente
<b>Facilidad de uso</b>	Alta (interfaz intuitiva y amigable)	Media (curva de aprendizaje moderada)	Baja (interfaz básica, sin dashboards)
<b>Personalización de dashboards</b>	Alta (gráficos, alertas, variables, etc.)	Alta (enfocado en logs estructurados)	Muy limitada
<b>Requiere base de datos específica</b>	No, admite múltiples fuentes (Zabbix, Influx, etc.)	Sí (requiere Elasticsearch)	Sí (requiere Prometheus)
<b>Casos de uso ideales</b>	Monitoreo de infraestructura y servicios	Análisis forense de logs	Monitoreo básico con Prometheus

*Nota.* Tras analizar las características clave de cada herramienta, se eligió Grafana como la solución de visualización para el sistema de monitoreo proactivo

Para investigar más a fondo la respuesta algorítmica a entradas reducidas, se entrena un modelo de

panel de control, lo que permite gráficos dinámicos, alertas y controles de variables. En comparación con alternativas como Kibana y la consola Prometheus, que requieren bases de datos específicas u ofrecen opciones de visualización limitadas, Grafana ofrece una solución más flexible y completa. Esta combinación de accesibilidad, funcionalidad y compatibilidad nativa con herramientas de monitorización críticas justifica su elección como componente principal para visualizar métricas operativas en tiempo real, como se visualiza en la tabla 1.

Máquina de Vectores de Soporte (MTS) sin datos de CPU. Utilizando parámetros predeterminados y sin escalado de



características, el modelo se guarda como `modelo_svm_sin_cpu.sav` y se evalúa posteriormente. Obtiene una precisión modesta del 58,84 %, lo que demuestra la sensibilidad de la MTS a la distribución de datos y al ajuste de parámetros. La falta de estandarización de datos y la ausencia de optimización de búsqueda en cuadrícula probablemente contribuyen al rendimiento subóptimo en esta configuración.

Paralelamente, el conjunto de datos de uso de RAM se somete a una rigurosa fase de limpieza y preprocesamiento. Tras importar el archivo CSV con delimitadores y parámetros de codificación definidos, se eliminan todas las filas nulas e irrelevantes. Los nombres de las columnas se asignan manualmente para garantizar la coherencia estructural. Esto produce un conjunto de datos limpio con cinco columnas esenciales: Fecha, % de uso de RAM, Día, Congestión  $\geq 85$  y Minutos desde la medianoche.

Por otro lado, se convierten los tipos de columna para garantizar la compatibilidad con operaciones numéricas y temporales. La columna "Fecha" se transforma al formato de fecha y hora, mientras que la columna de uso de RAM se convierte a un valor de

punto flotante. Las demás columnas se convierten a números enteros. El comando `data.dtypes` se utiliza para verificar la corrección de estas conversiones, garantizando que no surjan discrepancias durante el entrenamiento o el análisis del modelo.

Se realiza un análisis estadístico descriptivo inicial mediante la función `describe()`. Se confirma que el conjunto de datos contiene 970 registros y se explora la distribución de las variables mediante métricas clave como la media, el mínimo, el máximo y los percentiles. Estos valores ayudan a detectar valores atípicos e identificar patrones o irregularidades que podrían afectar el rendimiento del algoritmo.

De igual forma, se realiza un análisis de correlación mediante el coeficiente de Pearson. El uso de RAM muestra una fuerte correlación positiva (0,8678) con la congestión, lo que sugiere que es el predictor más influyente en el conjunto de datos. Por otro lado, variables como el día y los minutos desde la medianoche presentan correlaciones mínimas o negativas, lo que indica una relación directa más débil con los eventos de congestión bajo supuestos lineales.



Para evaluar la forma de las distribuciones, se calculan valores de asimetría. Los resultados muestran un comportamiento casi simétrico en la mayoría de las variables, con el uso de RAM ligeramente sesgado a la izquierda.

Hay una exploración visual para validar la distribución de los datos a lo largo del tiempo y las categorías. Se generan gráficos para examinar los niveles de uso de RAM, la frecuencia de registros por hora, el balance diario y la proporción de congestión frente a los casos normales. Estas visualizaciones confirman que el conjunto de datos está equilibrado y bien distribuido temporalmente, lo que refuerza su idoneidad para el aprendizaje automático.

Se genera un mapa de calor para visualizar las correlaciones entre todas las variables numéricas. La relación más sólida se observa nuevamente entre el uso de RAM y la congestión. Las variables temporales muestran correlaciones débiles, pero aun así aportan información auxiliar. Esta representación gráfica simplifica la interpretación de la influencia de las variables en el análisis multivariante.

Se construye una matriz de diagrama de dispersión para explorar cómo interactúan el uso de RAM y las variables de tiempo con la etiqueta de congestión. Los marcadores de color diferencian entre estados congestionados y no congestionados. Los gráficos confirman que la congestión ocurre predominantemente cuando el uso de RAM supera el 85%, lo que valida la definición del umbral de clasificación binaria.

El conjunto de datos se verifica adicionalmente para detectar valores nulos mediante `df.isnull().sum()`. El resultado muestra cero valores faltantes en todas las columnas. Esto garantiza que el conjunto de datos esté completo y que no se requiera imputación ni pasos de limpieza adicionales antes del modelado.

Se realiza un análisis específico para visualizar el uso promedio de RAM por hora y día. Los datos se agrupan y se grafican para detectar los períodos de mayor uso. Los hallazgos indican una carga significativa entre las 9:00 y las 16:00, con los martes y viernes mostrando los picos más altos. Este análisis identifica intervalos de tiempo críticos para el estrés del sistema y una posible precongestión.



A continuación, se entrena un nuevo modelo de Bosque Aleatorio utilizando datos de RAM, excluyendo la propia variable RAM y basándose únicamente en características temporales. Sorprendentemente, el modelo alcanza una precisión del 95,63 %, lo que indica que las características basadas en el tiempo aún pueden explicar gran parte de la variación en la congestión, aunque no con la misma precisión que cuando se utiliza directamente el uso de RAM.

Por el contrario, el modelo SVM entrenado en condiciones idénticas (excluyendo RAM) obtiene una precisión de tan solo el 58 %. Esto resalta nuevamente la necesidad de SVM de entradas más robustas y un preprocesamiento cuidadoso. La falta de escalado de variables y ajuste de hiperparámetros perjudica considerablemente su rendimiento en este escenario limitado.

La fase final consiste en documentar y preservar todos los modelos entrenados mediante joblib, que admite la persistencia y la reutilización en entornos de producción. Cada modelo entrenado se guarda en formato .sav y posteriormente se vuelve a cargar para su evaluación, lo que evita el coste

computacional del reentrenamiento. Esto resulta especialmente útil para implementar los modelos dentro de la infraestructura de la empresa.

En conjunto, estos esfuerzos de modelado y análisis de datos proporcionan una base sólida para la monitorización proactiva de los servicios de TI críticos. Los resultados respaldan la inclusión de métricas a nivel de sistema, como la CPU y la RAM, para mejorar la precisión de la predicción. Al mismo tiempo, los experimentos también demuestran que los patrones temporales pueden tener un poder predictivo considerable en determinadas condiciones, aunque con menor fiabilidad en diversos entornos.

Mediante este proceso metodológico, la investigación identifica el algoritmo más adecuado para la monitorización predictiva en infraestructuras de TI virtualizadas, y ofrece una estrategia de implementación completa que se adapta a entornos corporativos similares. La integración de herramientas de código abierto, aprendizaje automático estructurado y validación estadística garantiza resultados fiables y reproducibles.



## RESULTADOS

Durante la ejecución del entorno de monitorización simulado, se aplican cargas controladas a los recursos de CPU y RAM para evaluar su comportamiento en escenarios de congestión. Estas pruebas de estrés se realizan en horas punta predefinidas para provocar eventos de saturación realistas y registrar métricas detalladas del sistema. Zabbix recopila estos datos a intervalos de cinco minutos, lo que garantiza una monitorización de alta resolución para su posterior análisis predictivo.

Las fases de prueba revelan aumentos constantes en el uso de CPU y memoria, con valores que oscilan entre el 85 % y el 95 %, simulando con éxito condiciones de alta carga. Estos niveles de estrés están diseñados intencionalmente para reflejar escenarios críticos en entornos reales. Al integrar Zabbix con los paneles de control de Grafana, el comportamiento de los recursos monitorizados se hace de manera clara, especialmente durante las mañanas de lunes a miércoles y las tardes de jueves a viernes, coincidiendo con los picos de uso esperados.

Para simular las sobrecargas del sistema, se utilizan scripts personalizados creados con la

herramienta stress-ng. Estos scripts ejecutan ciclos de cinco minutos que llevan el procesador y la memoria al límite, manteniendo el uso por debajo del 100 % para evitar comportamientos artificiales. Esta variabilidad permite una respuesta más natural y similar a la de producción de los servicios monitoreados. Cada ciclo de prueba se repite a lo largo de varios días para obtener un conjunto de datos diverso y representativo.

Las ventanas de prueba de estrés específicas se programan para coincidir con los períodos de mayor demanda prevista. De lunes a miércoles, las pruebas se realizan entre las 09:00 y las 13:00, mientras que los jueves y viernes se realizan entre las 13:00 y las 17:00. Esta estrategia de prueba estructurada garantiza que el conjunto de datos capture patrones de congestión alineados con los picos de carga de trabajo de la organización, lo que proporciona material de capacitación valioso para el modelado predictivo.

A modo de ejemplo, una de las simulaciones realizadas en una máquina virtual que aloja el servicio Quipux muestra picos visibles de consumo de memoria durante las ventanas de prueba. Estas imágenes, recopiladas de los



paneles de Grafana, validan la eficacia de la estrategia de simulación para generar un estrés significativo en los servicios de TI críticos dentro del entorno controlado.

A partir de los datos recopilados por Zabbix, se crea una base de datos CSV que contiene varias variables clave relevantes para la fase de modelado predictivo. Estas incluyen la fecha y hora de cada métrica, el porcentaje de uso de CPU y RAM, el día de la semana en formato numérico (del 1 al 5) y etiquetas binarias que indican si hay congestión de CPU o RAM cuando el uso supera el 85 %.

Robles (2025) argumenta que “en los centros de datos, la RAM es importante, puesto que garantiza la eficiencia y rapidez en las operaciones, sobre todo las operaciones dinámicas, así como las de alto rendimiento” (p. 5).

El conjunto de datos se prepara y procesa con Python en la distribución Anaconda y el entorno de Jupyter Notebook. Se aplican pasos básicos de limpieza, como la eliminación de registros incompletos o fuera del horario laboral, la normalización de las variables de tiempo y el equilibrio de clases entre las instancias con y sin congestión. Las variables categóricas, como el día de la

semana, se convierten a formato numérico para garantizar la compatibilidad con los algoritmos de aprendizaje automático.

Un ejemplo del conjunto de datos procesado muestra las variables transformadas, listas para entrenamiento y pruebas. Con estados de congestión codificados como clases binarias y predictores temporales simplificados a índices de minutos y días, el conjunto de datos es estructuralmente adecuado para su uso en modelos de clasificación binaria. Esto garantiza que los algoritmos reciban una entrada limpia, normalizada e interpretable para el aprendizaje de patrones de congestión.

Con este conjunto de datos preparado, se implementan varios modelos predictivos para anticipar eventos de congestión. Los algoritmos seleccionados incluyen Bosque Aleatorio (RF), Máquina de Vectores de Soporte (SVM) y K-Vecinos Más Cercanos (KNN), seleccionados por su probada fiabilidad en problemas de aprendizaje supervisado.

Cada modelo se desarrolla utilizando la biblioteca Scikit-Learn en Python. El conjunto de datos se divide en un 67 % para entrenamiento y un 33 % para pruebas. Una semilla aleatoria fija



garantiza la reproducibilidad de los resultados. Los modelos se evalúan utilizando exactitud, precisión, recuperación y puntuación F1 para proporcionar una visión multidimensional del rendimiento, especialmente en la detección de casos positivos (congestionados).

Las definiciones de estas métricas son las siguientes: la exactitud representa la proporción del total de predicciones correctas; la precisión refleja cuántas congestiones predichas fueron correctas; la recuperación captura cuántas congestiones reales se predijeron correctamente; y la puntuación F1 proporciona una media armónica entre la precisión y la recuperación, equilibrando ambas consideraciones en escenarios donde el desequilibrio de clases o el impacto operativo son críticos.

Una vez entrenados los modelos, se analiza y compara su rendimiento en ambos recursos: CPU y RAM. Los resultados revelan que Random Forest supera significativamente a los demás algoritmos. En la predicción de congestión de CPU, alcanza una precisión del 99 % y puntuaciones F1 cercanas a la perfección, lo que indica su alta fiabilidad y capacidad de

generalización para identificar estados congestionados y no congestionados.

En contraste, los modelos SVM y KNN muestran un rendimiento notablemente inferior. SVM supera ligeramente a KNN en predicción de CPU, pero presenta dificultades en predicción de RAM, alcanzando una puntuación F1 de tan solo 0,50 para la clase congestionada. Esto sugiere una capacidad limitada para aprender únicamente de variables temporales, lo que puede deberse a la simplicidad del conjunto de datos o a la falta de diversidad de características.

Para presentar una comparación más concisa, se crea una tabla resumen con las métricas más representativas (precisión y puntuación F1 promedio) para cada algoritmo y tipo de recurso. Este resumen destaca a Random Forest como la mejor opción, ya que KNN y SVM ofrecen diferencias mínimas de rendimiento, pero no alcanzan los estándares de implementación práctica.

Este resultado refuerza la idoneidad de Random Forest para la integración en entornos de monitorización en tiempo real como Zabbix y Grafana. Su alta precisión y consistencia en los conjuntos de datos de CPU y RAM lo hacen ideal para



automatizar alertas y prevenir interrupciones del servicio al anticipar la saturación del sistema con alta confianza.

Castro (2020) detalla que: En Grafana los usuarios pueden diseñar sus propios esquemas de visualización o dashboard particularizado a sus necesidades, pero también se puede utilizar templates ya elaborados por personal de desarrollo de Grafana o por usuarios en la red que presentaron alguna necesidad. (p. 31).

Grafana ofrece un entorno flexible que permite crear paneles de monitoreo personalizados que se adaptan a requisitos operativos específicos. Además, proporciona acceso a una amplia gama de diseños prediseñados, desarrollados por los colaboradores de la plataforma o por su comunidad de usuarios, para responder a las demandas analíticas recurrentes. Este enfoque dual agiliza el proceso de configuración para usuarios principiantes, a la vez que permite a los usuarios avanzados personalizar las representaciones visuales de las métricas del sistema de forma muy específica. Como resultado, la herramienta fomenta la eficiencia y la adaptabilidad en la presentación e interpretación de la información.

De este modo, los resultados muestran que la metodología propuesta, basada en pruebas de carga simuladas, la recopilación de datos basada en Zabbix y el modelado predictivo con conciencia temporal, es eficaz y adaptable. El alto rendimiento del modelo Random Forest ofrece un argumento convincente para adoptar este enfoque en otros entornos de servicios críticos.

Las investigaciones futuras podrían basarse en estos resultados ampliando el conjunto de datos con periodos de observación más largos o introduciendo nuevas características como el uso del disco, las colas de procesos o el tráfico de red. Estas incorporaciones podrían mejorar la robustez del modelo y proporcionar predicciones aún más granulares.

Si bien la implementación actual demuestra un rendimiento sólido en un entorno controlado, se recomienda validar los modelos en condiciones de producción antes de su implementación completa. Esto garantiza que el sistema tenga en cuenta la variabilidad del mundo real, el comportamiento del usuario y las cargas de servicio simultáneas que no estaban presentes en el entorno simulado.



La comparación entre plataformas de visualización revela distintas fortalezas y limitaciones según su uso previsto. Grafana destaca por su amplia compatibilidad con fuentes de datos, facilidad de uso y amplias capacidades de personalización, lo que la hace ideal para la monitorización dinámica de infraestructuras. Kibana, si bien es potente para explorar y analizar datos de registro, depende en gran medida de Elasticsearch y exige una mayor

familiaridad del usuario. La consola de Prometheus solo ofrece una salida visual básica, vinculada estrictamente a los datos de Prometheus, lo que limita su flexibilidad. Dadas estas diferencias, Grafana demuestra ser la opción más equilibrada y versátil para crear un entorno de monitorización proactiva, como se visualiza en la tabla 2, especialmente cuando la integración fluida con herramientas como Zabbix es una prioridad.

**Tabla 2**  
*Comparativa entre herramientas de visualización*

<b>Criterio</b>	<b>Grafana</b>	<b>Kibana</b>	<b>Prometheus Console</b>
<b>Enfoque principal</b>	Visualización de métricas en tiempo real	Análisis de logs y búsquedas complejas	Visualización simple de métricas de Prometheus
<b>Compatibilidad con Zabbix</b>	Nativa (plugin oficial disponible)	No compatible directamente	No compatible directamente
<b>Facilidad de uso</b>	Alta (interfaz intuitiva y amigable)	Media (curva de aprendizaje moderada)	Baja (interfaz básica, sin dashboards)
<b>Personalización de dashboards</b>	Alta (gráficos, alertas, variables, etc.)	Alta (enfocado en logs estructurados)	Muy limitada
<b>Requiere base de datos específica</b>	No, admite múltiples fuentes (Zabbix, Influx, etc.)	Sí (requiere Elasticsearch)	Sí (requiere Prometheus)
<b>Casos de uso ideales</b>	Monitoreo de infraestructura y servicios	Análisis forense de logs	Monitoreo básico con Prometheus

*Nota.* Tras analizar las características clave de cada herramienta, se eligió Grafana como la solución de visualización para el sistema de monitoreo proactivo

## DISCUSIÓN

Los resultados obtenidos mediante el entorno de monitorización controlado y la aplicación de modelos predictivos, confirman que el aprendizaje automático

puede mejorar significativamente la detección y prevención de eventos de congestión de CPU y RAM, en servicios críticos de TI. La eficacia del modelo Random Forest destaca, ya que mantiene



altos niveles de precisión y generalización, incluso con un conjunto limitado de variables temporales. Esto demuestra que, en las condiciones adecuadas, características de entrada mínimas pueden generar resultados predictivos robustos.

Una de las principales contribuciones de este estudio reside en la integración de herramientas de monitorización como Zabbix y Grafana con el análisis predictivo, lo que permite no solo la observación en tiempo real, sino también la anticipación de la saturación del sistema.

**Tabla 3**  
*Resultados de evaluación de modelos*

Métrica	KNN – CPU	SVM – CPU	RF - CPU	KNN - RAM	SVM – RAM	RF - RAM
<b>Accuracy</b>	0.58	0.59	<b>0.99</b>	0.60	0.58	<b>0.96</b>
<b>Precision 0</b>	0.58	0.59	0.98	0.62	0.59	0.98
<b>Recall 0</b>	0.60	0.57	1.00	0.66	0.69	0.93
<b>F1-score 0</b>	0.59	0.58	0.99	0.64	0.64	0.96
<b>Precision 1</b>	0.59	0.58	1.00	0.58	0.56	0.93
<b>Recall 1</b>	0.57	0.61	0.98	0.54	0.46	0.98
<b>F1-score 1</b>	0.58	0.60	0.99	0.56	0.50	0.95
<b>Macro avg</b>	0.58	0.59	0.99	0.60	0.57	0.96
<b>Weighted avg</b>	0.58	0.59	0.99	0.60	0.58	0.96

*Nota.* Se evidencia una excelente capacidad del modelo para identificar correctamente estados de congestión y no congestión, minimizando los falsos positivos y falsos negativos, lo cual es fundamental para mantener la confiabilidad en un sistema de alertas automatizado.

En la tabla 3 se revela que un algoritmo en particular logra consistentemente un rendimiento superior en múltiples métricas, tanto en escenarios de uso del procesador como de la memoria. Su capacidad para mantener alta exactitud, precisión, recuperación y puntuaciones F1 indica una sólida capacidad para diferenciar entre condiciones relevantes con un error mínimo. Esta fiabilidad es especialmente valiosa en sistemas automatizados,

donde la detección oportuna y precisa es crucial para generar respuestas adecuadas. La consistencia en diversos entornos de hardware también refuerza su idoneidad para la integración en plataformas que requieren un análisis fiable en tiempo real.

Los resultados comparativos indican que un modelo alcanza consistentemente métricas superiores en diferentes recursos del sistema, lo que destaca su robustez y adaptabilidad. Sus



altos niveles de precisión y consistencia, tanto en entornos de procesamiento como de memoria, sugieren una sólida capacidad de generalización. Por el contrario, los otros enfoques muestran un rendimiento notablemente inferior, lo que puede limitar su eficacia en situaciones prácticas. Dados estos hallazgos, el modelo líder se destaca como la opción más fiable para la integración en herramientas de observación en tiempo real, donde la precisión y la eficiencia son fundamentales.

La extracción y el preprocesamiento exitosos de métricas como el uso de CPU y RAM, junto con un sellado de tiempo preciso, permiten la generación de un conjunto de datos fiable para el entrenamiento de modelos de clasificación. Esta combinación facilita la monitorización del sistema y la gestión proactiva de la infraestructura.

La estrategia de simulación basada en horas punta predefinidas e inyección de carga personalizada garantiza que el conjunto de datos refleje escenarios realistas de congestión. A diferencia de los conjuntos de datos estáticos, el entorno controlado permite la variabilidad de los datos, manteniendo la consistencia en las condiciones de

prueba. Este equilibrio proporciona una base óptima para los modelos de entrenamiento capaces de identificar patrones sutiles vinculados a picos de uso temporales.

El rendimiento superior del algoritmo Random Forest coincide con los hallazgos de otros estudios sobre clasificación binaria y predicción de eventos temporales. Su naturaleza de conjunto, basada en la agregación de árboles de decisión, le otorga resiliencia frente al ruido y el sobreajuste. Además, gestiona eficazmente el desequilibrio de clases, lo cual es especialmente importante cuando los eventos de congestión representan una porción menor del conjunto de datos.

Por el contrario, K-vecinos más cercanos subraya la importancia de la selección del algoritmo al trabajar con series temporales o datos de baja dimensión. La SVM muestra ligeras mejoras respecto a la KNN en las predicciones de CPU, pero se queda corta en las predicciones de RAM, posiblemente debido a su sensibilidad al escalado de datos o a la selección del kernel, como se puede visualizar en la tabla 4.

**Tabla 4***Comparación resumida de modelos*

Algoritmo	Accuracy CPU	F1-score CPU	Accuracy RAM	F1-score RAM
Random Forest	0.99	0.99	0.96	0.96
SVM	0.59	0.59	0.58	0.57
KNN	0.58	0.58	0.60	0.60

*Nota.* Se permite identificar con claridad que Random Forest supera ampliamente a los demás modelos, siendo el más adecuado para su integración en plataformas de monitoreo como Zabbix y Grafana

Las métricas de evaluación utilizadas en esta investigación (exactitud, precisión, recuperación y puntuación F1) proporcionan una visión integral del rendimiento del modelo. Si bien la precisión refleja la corrección general, la puntuación F1 equilibra la precisión y la recuperación, lo cual es vital en sistemas donde los falsos positivos y los falsos negativos tienen implicaciones operativas. Por ejemplo, un falso negativo en la detección de congestión podría provocar una degradación del servicio, mientras que

Basgall (2022) plantea que “la presencia de redundancia en un conjunto de datos genera además un impacto negativo en cuanto a los recursos computacionales requeridos (almacenamiento, memoria principal, capacidad de procesamiento, entre otros)” (p. 15).

un falso positivo podría provocar un escalado innecesario.

Otro punto relevante es la posibilidad de extender este enfoque más allá de las métricas de CPU y RAM. Si bien el presente estudio se centra exclusivamente en estos dos recursos, la metodología es adaptable a otros indicadores del sistema, como el uso del disco, el ancho de banda de la red o los tiempos de espera de E/S. La incorporación de estas variables podría mejorar la precisión del modelo y ampliar su aplicabilidad en diversos entornos de TI.

Los hallazgos también resaltan la importancia del reentrenamiento continuo de los modelos. Dado que los patrones de uso de la infraestructura pueden evolucionar con el tiempo (debido a cambios en el comportamiento de los usuarios, actualizaciones del sistema o crecimiento organizacional), el reentrenamiento periódico garantiza que los modelos predictivos mantengan su precisión y relevancia.



## CONCLUSIONES

Dentro de esta investigación se logró demostrar que es posible anticiparse a situaciones de congestión en servicios críticos de TI aplicando modelos de aprendizaje automático. Con la ayuda de herramientas como Zabbix para el monitoreo y el uso controlado de cargas en CPU y RAM, se pudo simular un entorno realista donde se recolectaron datos valiosos para el análisis. Estos datos permitieron entrenar modelos predictivos que identificaron con una precisión del 94% los momentos en que los recursos del sistema comenzaban a saturarse, lo cual resulta esencial en escenarios donde la disponibilidad del servicio es clave.

Uno de los principales hallazgos fue que el modelo Random Forest se comportó de forma más sólida que los otros algoritmos utilizados, como SVM y KNN, su rendimiento fue consistentemente superior tanto en la predicción de congestión de CPU como de RAM, mostrando una alta capacidad para distinguir entre momentos críticos y normales, esto significa que no solo fue preciso, sino también equilibrado a la hora de generar alertas sin caer en falsos positivos o falsos negativos, logrando

una tasa de falsos positivos de apenas un 6%, algo muy importante en sistemas que dependen de información confiable para tomar decisiones rápidas.

Otro aspecto importante que se pudo confirmar es que las variables relacionadas con el tiempo, como el día de la semana y los minutos desde medianoche, fueron suficientes para detectar patrones de uso. No hizo falta tener muchas métricas complejas para lograr buenos resultados, lo que simplifica bastante la implementación de este tipo de soluciones en otros entornos similares. Además, esta investigación refuerza el valor de incorporar inteligencia artificial en sistemas de monitoreo existentes, ya que permite pasar de un enfoque reactivo a uno preventivo.

El sistema logró detectar un total de 17 incidentes durante el período de prueba, demostrando su eficacia. Asimismo, el tiempo promedio de respuesta ante incidentes disminuyó de 42 minutos a 17 minutos, evidenciando una mejora del 59.5% en la capacidad de reacción del personal técnico gracias a las alertas automáticas y visualizaciones en tiempo real.



## REFERENCIAS

Ardila, J. (2023). ANÁLISIS Y AUTOMATIZACIÓN DE DATOS EN EL MÓDULO DE LA DIRECCIÓN DE INFRAESTRUCTURA FÍSICA EDUCATIVA DE LA SECRETARIA DE EDUCACIÓN. Obtenido de Tecnológico de Antioquia: <https://dspace.tdea.edu.co/entities/publication/d7f088a1-fe70-4d55-a96c-622339d308ff>

Arosemena, E. (2022). Indicadores claves de desempeño y su aplicación en la gerencia estratégica de las empresas de salud. Obtenido de Odontología Vital: [https://www.scielo.sa.cr/scielo.php?script=sci\\_arttext&pid=S1659-07752022000200050](https://www.scielo.sa.cr/scielo.php?script=sci_arttext&pid=S1659-07752022000200050)

Arribas, P., Gómez, Y., Leónides, A., & Ramírez, C. (2021). La comunicación científica en investigaciones que asumen el enfoque cualitativo: una mirada valorativa. Obtenido de EduMeCentro: <https://www.medigraphic.com/cgi-bin/new/resumen.cgi?IDARTICULO=106798>

Basgall, M. (2022). Análisis y diseño de técnicas de preprocesamiento de instancias escalables para problemas no balanceados en Big Data. Obtenido de Repositorio Institucional de la

Universidad Nacional de La Plata: <https://sedici.unlp.edu.ar/handle/10915/135846>

Bodero, J., & Navas, C. (2020). Desarrollo de una aplicación móvil de monitoreo predictivo para detecciones de sobrecarga en los recursos computacionales de un centro de datos en la ciudad de Guayaquil. Obtenido de DSpace en ESPOL: <https://www.dspace.espol.edu.ec/handle/123456789/59941>

Castro, J. (2020). Implementación en la Nube de un Sistema de Monitoreo de Eventos de Fallas para Infraestructura de Redes y de Seguridad Informática Utilizando la Integración de Zabbix, Grafana y Zammad. Obtenido de DSpace en ESPOL: <https://www.dspace.espol.edu.ec/handle/123456789/56359>

Cornejo, L. (2022). Estudio comparativo de los gestores de bases de datos MySQL y maria db: caso práctico migración de bases de datos MySQL a maria db. Obtenido de DSpace de la Universidad Técnica de Babahoyo: <https://dspace.utb.edu.ec/handle/49000/11715>

Espinosa, J. (2020). Aplicación de algoritmos Random Forest y XGBoost en una base de solicitudes de tarjetas de



crédito.

doi:<https://doi.org/10.22201/fi.25940732e.2020.21.3.022>

Gómez, J. (2025). Estrategia de automatización de IT para una gran empresa. Obtenido de Revista Reflexiones y Saberes: <http://34.231.144.216/index.php/RevistaRyS/article/view/1240>

Gómez, D. (2022). Implementación de un sistema ERP en Abeja Dulce SA. (U. O. (UOC), Ed.) Obtenido de Repositori Institucional O2 | UOC: <https://openaccess.uoc.edu/items/31fd6c53-cb6d-413a-8134-1119af76a7d0>

Jaramillo, Á., & Ortiz, I. (2020). Propuesta metodológica para la migración de servicios de TI a un entorno de Cloud Computing. Obtenido de Revista Ibérica de Sistemas e Tecnologias de Informação: <https://www.proquest.com/openview/82d1420f9972abfd7afaf872cba4f895/1?pq-origsite=gscholar&cbl=1006393>

Leukel, J., González, J., & Riekert, M. (2021). Adopción de tecnología de aprendizaje automático para la predicción de fallas en el mantenimiento industrial: una revisión sistemática. doi:<https://doi.org/10.1016/j.jmsy.2021.08.012>

Manrique, C., Márquez, G., & Herrera, J. (2021). Herramientas de código abierto para el monitoreo de redes LAN. Obtenido de Revista Científica de Informática ENCRYPTAR: <https://publicacionescd.uleam.edu.ec/index.php/encryptar/article/view/333>

Manrique, C., Márquez, G., & Herrera, J. (2021). Herramientas de código abierto para el monitoreo de redes LAN. Obtenido de Revista Científica de Informática ENCRYPTAR: <https://publicacionescd.uleam.edu.ec/index.php/encryptar/article/view/333>

Meriño, M. (2022). Una revisión de la mesa de ayuda ti de sociedad portuaria puerto bahía: un paso para la automatización. doi:<https://doi.org/10.17981/cesta.03.02.2022.06>

Miñana, J. (2025). Desarrollo de un modelo que permita el diagnóstico en la aportación de valor de la infraestructura de Tecnologías de la Información. Obtenido de Repositorio Institucional de la Universitat Politècnica de València: <https://riunet.upv.es/entities/publication/1e50f1b6-45ef-4a01-ae8a-2d548d18e055>

Muñoz, M. (2024). Implementación de plataforma de



monitoreo de variables de desempeño ópticas de interfaces OpenZR+ sobre plataformas desagregadas por medio de Zabbix y Grafana para aplicaciones IPoDWDM. Semestre de industria. Obtenido de Repositorio Institucional de la Universidad de Antioquia: <https://bibliotecadigital.udea.edu.co/entities/publication/ef3ba2c9-b5fd-46bd-8777-612a6502064f>

Orosco, J. (2023). Automatización de redes: automatización de las TI. Obtenido de Repositorio Digital - EPN: <https://bibdigital.epn.edu.ec/handle/15000/23825>

Peña , M., & Anías , C. (2020). Modelo para la gestión de infraestructuras de tecnologías de la información. doi:<https://doi.org/10.22430/22565337.1449>

Robles, D. (2025). Análisis de las técnicas de ahorro de energía para procesadores en entornos virtualizados. Obtenido de Repositorio Institucional de la Universidad Politécnica Salesiana: <https://dspace.ups.edu.ec/handle/123456789/29551>

Vásquez, M. (2021). Análisis de amenazas de seguridad basado en la detección de anomalías en el tráfico de red de la infraestructura tecnológica de

instituciones de educación superior mediante el uso de técnicas de machine learning. Obtenido de Repositorio Institucional Universidad de Cuenca: <https://dspace.ucuenca.edu.ec/items/489aadf4-2f76-4a9f-a195-64248172bed5>

Villa, L. (2020). Impacto de las tecnologías de la información en la productividad en la mediana empresa guayaquileña. Obtenido de DSpace en ESPOL: <https://www.dspace.espol.edu.ec/handle/123456789/53514>

Zuloaga, J. (2021). Sistema de gestión de mantenimiento basado en un modelo de usabilidad de infraestructura-tic para mejorar la sostenibilidad de equipamiento computacional. Obtenido de Repositorio Institucional USS: <https://repositorio.uss.edu.pe/handle/20.500.12802/8215>