UNIVERSIDAD NACIONAL DEL ALTIPLANO

FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA, ELECTRÓNICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE UN MODELO DE MONITOREO APLICANDO ITIL PARA MEJORAR LA DISPONIBILIDAD DE LOS SERVICIOS TIC DEL MINISTERIO DE EDUCACIÓN – LIMA

TESIS

PRESENTADA POR:

ERIKA MILLY APAZA VILCA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

PUNO - PERÚ

2024

Reporte de similitud

NOMBRE DEL TRABAJO

IMPLEMENTACIÓN DE UN MODELO DE MONITOREO APLICANDO ITIL PARA ME JORAR LA DISPONIBILIDAD DE LOS SER VICIOS TIC DEL MINISTERIO DE EDUCAC IÓN – LIMA

AUTOR

ERIKA MILLY APAZA VILCA

RECUENTO DE PALABRAS

27560 Words

RECUENTO DE CARACTERES

155960 Characters

RECUENTO DE PÁGINAS

153 Pages

TAMAÑO DEL ARCHIVO

4.0MB

FECHA DE ENTREGA

Aug 29, 2024 8:07 AM GMT-5

FECHA DEL INFORME

Aug 29, 2024 8:09 AM GMT-5

17% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 16% Base de datos de Internet
- 1% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 6% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Coincidencia baja (menos de 12 palabras)

V°B°

Firmado digitalmente por SOTOMAYOR ALZAMORA Guina Guadalupe FAU 20145496170 hard
Motivo: Doy V°B°
Fecha: 29.08.2024 08:51:22 -05:00

FIRMA DIGITAL

Firmado digitalmente por: CALDERON VILCA EDWIN FREDY FIR 42262469 hard
Motivo: Soy el autor del documento
Fecha: 29/08/2024 08:11:29-0500

Resumen

DEDICATORIA

Este proyecto de titulación es dedicado, en primer lugar, al Padre celestial por bendecirme con buenos padres, en su infinito amor que me fortaleció para que hoy este cumpliendo con una meta más.

A mis padres David Apaza Quispe y Agripina Vilca Roque por ser mi ejemplo de superación y constancia, por su amor, sus esfuerzos para darme una educación para mi formación personal y profesional, permitiéndome finalizar este trabajo logrando superar las dificultades que se presentaron en mi camino.

A mis hermanos, sobrinos y amigos que confiaron en mis capacidades y valores para culminar esta meta.

Erika Milly Apaza Vilca

AGRADECIMIENTOS

Expreso mi agradecimiento a la Escuela Profesional de Ingeniería de Sistemas y a sus destacados docentes por inculcarme sus conocimientos en mi formación profesional. En especial, expreso mi más sincero reconocimiento al Dr. Edwin Fredy Calderón Vilca, director de mi tesis, por su invaluable orientación, observaciones, paciencia y motivación, que fueron esencial para el desarrollo de este trabajo de investigación.

Asimismo, agradezco a los miembros del jurado calificador, Dr. Angel Manuel Olazabal Guerra, Dr. Miguel Romilio Aceituno Rojo y Dr. Pablo Cesar Tapia Catacora, por sus valiosas recomendaciones.

Expreso mi agradecimiento a la Oficina de Tecnologías de la Información y Comunicación del MINEDU por las facilidades brindadas.

Con un profundo sentimiento de gratitud, reconozco a quienes me han brindado amor y confianza. A aquellos que han dedicado su tiempo para enseñarme, proporcionando aportes que serán invaluable en mi crecimiento profesional.

Erika Milly Apaza Vilca

ÍNDICE GENERAL

Pág.

CAPÍTULO II

REVISIÓN DE LITERATURA

Área: Desarrollo, gestión, seguridad y auditoria de sistemas de información

Tema: Gestión de TI.

FECHA DE SUSTENTACIÓN: 04 de setiembre de 2024

ÍNDICE DE TABLAS

Pág.

ÍNDICE DE FIGURAS

Pág.

ÍNDICE DE ANEXOS

Pág.

ACRÓNIMOS

ITMS:	Gestión de servicios de Tecnología de información.
ITIL:	Information Technology Infrastructure Library o Biblioteca de Infraestructura de Tecnologías de la Información
ISO:	International Organization for Standardization u Organización Internacional de Normalización.
AENOR:	Asociación Española de Normalización y Certificación**.**
MINEDU:	Ministerio de Educación.
USAU:	Unidad de Servicio de Atención al Usuario.
OTIC:	Oficina de Tecnologías de la Información y Comunicación.
SNMP:	Protocolo Simple de Administración de Red
MIB:	Management Information Base.
SSL:	Seguridad de la capa de transporte
ICMP:	Protocolo de Mensajes de Control de Internet.
IP:	Protocolo de Internet.
UPS:	Fuente de poder ininterrumpible.
SMTP:	Simple Mail Transfer Protocol o Protocolo para Transferencia Simple de Correo

RESUMEN

La finalidad principal del presente trabajo de investigación es determinar el impacto significativo de la implementación de un modelo de monitoreo aplicando ITIL 4 en la disponibilidad de servicios de TIC en la Oficina de Tecnologías de la Información y Comunicación del Ministerio de Educación en Lima. Estos servicios deben ofrecer una disponibilidad continua las 24 horas del día, los 7 días de la semana, siendo prioritarios para las áreas, unidades y dependencias de la entidad, por lo que se abordó como una problemática. Se aplicaron los principios de ITIL 4, para implementar soluciones estratégicas estableciendo indicadores que permitieran tomar decisiones informadas y ejecutar acciones preventivas. Se realizó un análisis e identificación de los equipos de comunicación, servidores, servicios web y sistemas de información con un gran volumen de datos en la red. Dada la complejidad y la importancia de monitorear los eventos diarios, se implementó un modelo de monitoreo en base a las herramientas Nagios y Nagvis, permitiendo monitorear estados a nivel de infraestructura, enlace y servicios web, a través de los protocolos como ICMP, SMTP, TCP, SSL y HTTP. Contribuyendo al funcionamiento eficiente de los servicios TIC. La validación del modelo se realizó mediante fichas de observación y análisis de reportes del monitoreo, incluyendo estadísticas sobre el estado de los servicios y alertas vía correo electrónico notificando los eventos y restablecimiento de los servicios monitoreados. De esta manera se ha demostrado un nivel de disponibilidad del 99,35%, lo cual ha tenido un impacto significativo en comparación con la ausencia de un modelo, así mismo comprobando la hipótesis declarada.

Palabras claves: Detección, Evento, Incidencia, ITIL 4, Gestión de eventos, MINEDU (Ministerio de Educación), TIC (Tecnologías de la Información y Comunicación).

ABSTRACT

The main purpose of this research work is to determine the significant impact of implementing a monitoring model applying ITIL 4 on the availability of ICT services in the Office of Information and Communication Technologies of the Ministry of Education in Lima. These services must offer continuous availability 24 hours a day, 7 days a week, being a priority for the areas, units, and dependencies of the entity, so it was addressed as an issue. The principles of ITIL 4 were applied to implement strategic solutions by establishing indicators that would allow for informed decision-making and the execution of preventive actions. An analysis and identification of communication equipment, servers, web services, and information systems with a large volume of data on the network were carried out. Given the complexity and importance of monitoring daily events, a monitoring model based on Nagios and Nagvis tools was implemented, allowing monitoring of states at the infrastructure, link, and web service levels, through protocols such as ICMP, SMTP, TCP, SSL, and HTTP. This contributed to the efficient operation of ICT services. The validation of the model was done through observation sheets and analysis of monitoring reports, including statistics on the state of services and email alerts notifying events and restoration of monitored services. In this way, a availability level of 99.35% has been demonstrated, which has had a significant impact compared to the absence of a model, thus confirming the stated hypothesis.

Keywords: Detection, Event, Incident, ITIL 4, Event Management, MINEDU (Ministry of Education), ICT (Information and Communication Technologies).

CAPÍTULO I

INTRODUCCIÓN

El presente trabajo de investigación titulado: “implementación de un modelo de monitoreo aplicando ITIL 4 para mejorar la disponibilidad de los servicios TIC del Ministerio De Educación – Lima”, se centra en la problemática de los desafíos derivado de la constante evolución de las Tecnologías, Esta evolución trae consigo nuevos métodos, reglas, ejecución, equipos y aplicaciones que transforman las tecnologías de información y comunicación a diferentes niveles de comunicación. El crecimiento exponencial en la utilización de los servicios TIC ha forzado a la entidad a intensificar el monitoreo del desempeño de sus tecnologías. Para garantizar que la información sea oportuna, precisa y relevante para la toma de decisiones estratégicas.

La investigación surge ante el escenario crítico de los servicios TIC frente a las constantes incidencias que ponen en riesgo la continuidad del negocio de la organización. La gestión efectiva de TI se vuelve crucial para respaldar la planificación estratégica de las tecnologías de información, la toma de decisiones y de la operatividad de los servicios de TIC como una tarea crucial. El desafío radica en la limitación de disponibilidad de la mano de obra las 24 horas del día, resultando en la detección tardía de incidencias. Por ello, se destaca la importancia de contar con un modelo de monitoreo autónomo, confiable y flexible que permita una detección temprana de incidencias y una mejora en la eficiencia del personal, reduciendo costos y favoreciendo enfoques mejorados en la organización. El modelo de monitoreo de TIC se compone de los siguientes elementos:

Metodología de análisis: Define los procesos para analizar la información recopilada y detectar posibles incidencias.

Herramientas de monitoreo: Permiten recopilar información sobre el estado de los servicios TIC, como el tráfico, la disponibilidad de los dispositivos y el rendimiento de las aplicaciones.

La implementación de un modelo de monitoreo basado en ITIL 4 para mejorar la disponibilidad de los servicios TIC en el Ministerio de Educación (MINEDU) es un objetivo pertinente. Este modelo busca asegurar respuestas rápidas a eventos e incidencias en los servicios de TIC a través de una herramienta de monitoreo basada en código abierto, contribuyendo así a la mejora de la disponibilidad de los servicios de TIC.

Este trabajo de investigación se estructura en seis capítulos interrelacionados para facilitar la comprensión del lector. A continuación, se describe el contenido de cada:

En el Capítulo I: “Planteamiento del Problema de Investigación”, detalla la planificación y fórmula el objetivo, la problemática, la justificación, y los límites de la presente investigación; estos temas sitúan al lector en la problemática de la investigación; así como, de la hipótesis que será demostrada y de la operacionalización de variables.

En el Capítulo II: “Revisión de Literatura”, se presenta el respaldo teórico en tres secciones: antecedentes de investigación que se basan en estudios previos relevantes, el marco teórico que contiene la teoría esencial para una comprensión profunda, y el marco conceptual que aclara los términos fundamentales empleados en la investigación.

En el Capítulo III: “Materiales y Métodos”, se describen en detalle los métodos, instrumentos, así como la población y muestra considerados en este trabajo de investigación.

En el Capítulo IV: “Resultados y Discusión”, Se presentan y examinan los resultados de implementar un modelo de monitoreo basado en ITIL 4 con el objetivo de

mejorar la disponibilidad de los servicios TIC en el Ministerio de Educación. Se lleva a cabo una prueba de hipótesis utilizando los datos basados en cada uno de los indicadores que permiten evaluar el impacto del modelo sobre ellos mismos. Se ofrece la interpretación de los resultados obtenidos, revelando así los resultados de la evaluación de la investigación.

En el Capítulo V: "Conclusiones", se presenta las conclusiones después de la implementación del modelo.

En el Capítulo VI: "Recomendaciones", se describe las recomendaciones respectivas del trabajo de investigación

Asimismo, se proporciona la bibliografía utilizada como fundamentación con el fin el desarrollo de este trabajo, los anexos que complementan el cuerpo del documento, el glosario, así como las siglas de palabras y términos, facilitando su comprensión con sus respectivos significados.

1.1 DESCRIPCIÓN DEL PROBLEMA DE INVESTIGACIÓN

La Oficina de Tecnologías de la Información y Comunicación (OTIC), órgano dependiente de la Secretaría de Planificación Estratégica (SPE) del Ministerio de Educación (MINEDU), juega un papel fundamental en el desarrollo de la gestión educativa. Su función principal es conducir el uso de los recursos informáticos del sector educativo, poniendo a disposición las Tecnologías de Información y Comunicación (TIC) que apoyan a la gestión institucional. Las TIC se han convertido en herramientas esenciales para la gestión administrativa, educativa y pedagógica, por lo que su disponibilidad y correcto funcionamiento son imprescindibles para el desarrollo de las actividades del Ministerio.

La falta de disponibilidad de un servicio de TIC crítico para MINEDU podría tener graves consecuencias, como:

- **Paralización de los servicios**: Los usuarios internos y externos del MINEDU no podrán acceder a los servicios que ofrece la institución, como la plataforma web, el sistema de gestión de trámites, el correo electrónico, etc.
- **Afectación a la calidad de los servicios:** La interrupción de los servicios de TIC afectará la calidad de la educación, ya que los docentes y estudiantes no podrán acceder a los recursos educativos digitales, plataformas de aprendizaje, etc.
- **Discontinuidad del negocio:** La paralización de los servicios de TIC podría afectar la capacidad del MINEDU para llevar a cabo sus funciones básicas, como la gestión administrativa, financiera y pedagógica.
- **Baja productividad**: La falta de acceso a las herramientas tecnológicas reducirá la eficiencia de los trabajadores del MINEDU, impactando negativamente en la productividad de la institución.

Para el cumplimiento de sus objetos estratégicos institucional el MINEDU requiere la disponibilidad de los servicios tecnológicos, siendo un factor crucial la información, para las decisiones y acciones estratégicos para la operatividad de los servicios pedagógicos que ofrece a nivel nacional. Su gestión cuidadosa es esencial para aprovechar oportunidades y prevenir situaciones de riesgo que puedan afectar la productividad y la continuidad del negocio.

En la actualidad, las Tecnologías de la Información y la Comunicación superan barreras temporales, facilitando la interconexión global entre individuos e instituciones.

En las organizaciones, las TIC son fundamentales para respaldar las operaciones, asegurando la calidad de servicios, reduciendo tiempos de respuesta y mejorando la competitividad. Para optimizar procesos estratégicos y operativos, es crucial contar con una sólida capacidad y velocidad de almacenamiento de la información.

La información y la tecnología son activos cruciales en las organizaciones, requiriendo tareas constantes de mantenimiento, como monitoreo y supervisión para mitigar fallas en el uso de tecnologías de información. En el caso del MINEDU, aunque cuenta con una infraestructura de red eficiente, se enfrenta a desafíos debido a la evolución de su infraestructura tecnológica, fallas recurrentes, posiblemente atribuibles a eventos como fallas eléctricas y falta de mantenimiento en los cuartos de telecomunicaciones. La manipulación no autorizada de equipos también puede generar problemas en el acceso a la red y a los servicios proporcionados por la Oficina de Tecnologías de la Información y Comunicación.

La OTIC del MINEDU es responsable de garantizar la disponibilidad y el correcto funcionamiento de las TIC para el desarrollo eficiente de la gestión educativa. La inversión en infraestructura tecnológica robusta, la implementación de estrategias de soporte técnico eficaz y la capacitación del personal son factores claves para asegurar la continuidad de los servicios y la calidad de la educación en el Perú.

1.2 FORMULACIÓN DEL PROBLEMA

1.2.1 Problema general

¿En qué medida el modelo de monitoreo aplicando ITIL 4, mejora la disponibilidad de los servicios de TIC llevado a cabo por la Oficina de Tecnologías de la información y comunicación en el Ministerio de Educación – Lima?

1.3 OBJETIVOS DE LA INVESTIGACIÓN

1.3.1 Objetivo general

Implementar un modelo de monitoreo aplicando ITIL 4 para mejorar la disponibilidad de los servicios de TIC llevado a cabo por la Oficina de Tecnologías de la información y comunicación del Ministerio de Educación – Lima.

1.3.2 Objetivos específicos

- Identificar y analizar el estado actual de los servicios de web, equipos de comunicaciones y puntos de acceso monitoreados y no monitoreados aplicando ITIL 4 e identificar los indicadores de disponibilidad que serán sometidos al proceso de mejora.
- Implementar el modelo de monitoreo aplicando ITIL 4 para la detección de la degradación o interrupción de los servicios de web, equipos de comunicaciones y servicio de red, realizando las validaciones y pruebas.
- Validar la mejora del nivel de disponibilidad y el tiempo de detección de eventos e incidencias de los servicios de TIC, en el Ministerio de

Educación con la implementación de un modelo de monitoreo aplicando ITIL 4 a través de la herramienta Nagios y Nagvis.

1.4 JUSTIFICACIÓN DE LA INVESTIGACIÓN

Esta investigación es pertinente, porque el Ministerio de Educación como cualquier otra institución enfrentan un constante cambios y evolución tecnológico, a medida que pasa el tiempo, los objetivos y estrategias se adaptan a las nuevas realidades; esto significa que también sus requisitos de tecnologías de información y comunicaciones evolucionan. Siendo así, una de ellas la alta disponibilidad y performance de los servicios de web, equipos de comunicaciones y puntos de acceso, y el avance de las tecnologías que trae consigo riesgos, debiendo ser mitigados su impacto a través de acciones preventivas, los cuales se identificó a nivel de la infraestructura (Componentes y subcomponentes), enlaces y servicios web, los cuales son críticos y están en constante cambios que son denominados incidencias, donde la ocurrencia de estos, son de forma aleatoria.

Actualmente los servicios de TIC en el Ministerio de Educación van incrementando, la investigación y su posterior propuesta es un elemento fundamental para apoyar el desempeño de las áreas, unidades y dependencias del Ministerio de Educación, en este contexto, se opta por implantar un modelo que permita monitorear el estado de los servicios llevado a cabo por la OTIC, así mismo, identificar incidencias y mitigar su impacto a través de acciones preventivas adoptando los principios de ITIL 4, para obtener el nivel de desempeño necesario que permita atender las alertas que se generen de manera proactiva garantizado el nivel de disponibilidad de los servicios de web, equipos de comunicaciones y dispositivos en red en buen funcionamiento para los usuarios, así mismo, afrontar los retos que se presentan.

Además, se pretende demostrar el valor del modelo de monitoreo para organizaciones como el MINEDU. Mediante la implementación, evaluación y análisis descriptivo del modelo de monitoreo en el Ministerio de Educación, para lograr reducir el tiempo de detección de eventos e incidencias, prevenir y corregir fallos, para la toma de medidas preventivas, para evitar posibles eventualidades que interrumpan el correcto funcionamiento en comparación cuando no se contaba con un modelo.

1.5 ALCANCES Y LIMITACIONES DE LA INVESTIGACIÓN

1.5.1 Alcance

En el presente trabajo de investigación consiste en la implementación de un modelo de monitoreo aplicando ITIL 4 para mejorar la disponibilidad de los servicios de TIC del Ministerio de Educación – Lima. Este modelo será implementado única y exclusivamente en la Oficina de Tecnologías de la Información y comunicación, dependencia de la Secretaría de Planificación Estratégica (SPE).

La complejidad de la infraestructura y servicios de web exige un análisis meticuloso. Para ello, se seleccionó un segmento que abarca los equipos y servicios más críticos, satisfaciendo las necesidades fundamentales de la propuesta planteada, así mismo ampliando su aplicabilidad a otro contexto real.

1.5.2 Limitaciones

El trabajo de investigación se centra en el análisis del modelo de monitoreo. Los equipos de comunicación y los servicios utilizados en este estudio son: switches, servidores, radioenlaces, hosts Windows y Linux, y servicios web críticos. Se habilitaron protocolos específicos (agentes) en cada equipo permitiendo la transmisión de información esencial a la herramienta de monitoreo.

Esta herramienta, a su vez, generará alertas inmediatas ante cualquier evento detectado en los equipos, asegurando una respuesta oportuna. Solo se trabajó con las variables o factores monitoreados durante la investigación, limitando la implementación a los servicios que fueron objeto de estudio. Por lo que posiblemente algunos factores fueron obviados.

El estudio se enfocó en las variables o factores relevantes para el monitoreo, considerando las limitaciones de la herramienta implementada. Es importante destacar que la implementación del modelo de monitoreo está limitada por:

- **Disponibilidad de información**: La herramienta solo puede analizar la información que es enviada por los equipos y servicios de red.
- **Capacidad de la herramienta:** La herramienta tiene una capacidad limitada para procesar información y generar alertas.
- **Recursos humanos:** El personal responsable de atender las alertas debe tener la capacidad y el conocimiento para solucionar los problemas que se presenten.

1.6 HIPÓTESIS DE LA INVESTIGACIÓN

1.6.1 Hipótesis general

La implementación de un modelo de monitoreo aplicando ITIL 4 mejorará significativamente la disponibilidad de los servicios de TIC llevados a cabo por la Oficina de TIC del Ministerio de Educación - Lima.

1.6.2 Hipótesis específicas

- La identificación y análisis de los servicios web, equipos de comunicaciones y dispositivos en red críticos llevados a cabo por la Oficina de TIC del Ministerio de Educación permitirá determinar la mejora de la disponibilidad de los servicios de TIC, aplicando los principios de ITIL 4 del Ministerio de Educación en Lima.
- La implementación del modelo de monitoreo mediante la herramienta Nagios y Nagvis, aplicando ITIL 4, permitirá mejorar el tiempo de detección de eventos e incidencias, y notificarlos.
- La aplicación exitosa del modelo de monitoreo aplicando ITIL 4 mejoró el nivel de disponibilidad de los servicios TIC.

1.7 SISTEMA DE VARIABLES

1.7.1 Operacionalización de variables

- **Variable independiente**

  X. Implementación de un modelo de monitoreo aplicando ITIL 4.

  Indicadores

  X1. Usabilidad.

  X2. Gestión.

  X3. Rendimiento

- **Variable dependiente**

  Y. Disponibilidad de los servicios de TIC del Ministerio de Educación - Lima.

  Indicadores

Y1. Tiempo de notificaciones de eventos del servicio de TIC.

Y2. Tiempo de resolución eventos e incidencias.

Y3. Tiempo de interrupción de los servicios de TIC monitoreado.

Y4. Nivel de disponibilidad de los servicios de TIC en la red.

Tabla 1

Operacionalización de las variables

	VARIABLES	DIMENSIÓN	INDICADORES	ESCALA
INDEPENDIENTE	IMPLEMENTACIÓN DE UN MODELO DE MONITOREO APLICANDO ITIL 4	EVALUAR EL MODELO	Usabilidad	Alto Medio Bajo
			Gestión	Alto Medio Bajo
			Rendimiento	Alto Medio Bajo
DEPENDIENTE	DISPONIBILIDAD DE LOS SERVICIOS DE TIC DEL MINISTERIO DE EDUCACIÓN - LIMA.	MONITOREO DE SERVICIOS DE TIC	Tiempo de notificaciones de eventos del servicio de TIC.	Critico Medio Leve Insignificante
			Tiempo de resolución eventos e incidencias.	Critico Medio Leve Insignificante
			Tiempo de interrupción de los servicios de TIC monitoreado.	Critico Medio Leve Insignificante
			Nivel de disponibilidad de los servicios de TIC en la red	Critico Medio Leve Insignificante

CAPÍTULO II

REVISIÓN DE LITERATURA

2.1 ANTECEDENTES DE LA INVESTIGACIÓN

Las Tecnologías de la Información y la Comunicación (TIC) han experimentado una profunda evolución a lo largo de los años, transformándose en un elemento relevante en la sociedad actual. Su impacto se extiende a diversos ámbitos, modificando paulatinamente el estilo de vida, así como en el desarrollo de la vida académica y las actividades laborales.

Ancajima Miñán, Infante Saavedra, Aliaga Guevara & Soto Abanto (2022), Quien se planteó como marco de referencia: Las organizaciones públicas, así como privadas dependen cada vez más de herramientas tecnológicas por el incremento de la complejidad de sus procesos que, han generado una mayor demanda y necesidad de contar con modelos que faciliten la gestión de su infraestructura tecnológica de forma sencilla, permitiendo así el soporte adecuado a los objetivos de la entidad.

2.1.1 Antecedentes nacionales

Tesis: Purihuamán Venegas & Ramos Alcarraz (2021) Modelo de monitoreo para la identificación preventiva de incidencias y la ejecución de acciones correctivas en los servicios tecnológicos de las organizaciones. El objetivo principal de esta tesis fue aplicar un modelo de monitoreo para identificar el estado de los servicios de TI que identifica incidencias y mitiga su impacto a través de medidas preventivas; llegando a la conclusión:

Se completó la implementación de un modelo para monitorear el rendimiento de los servicios tecnológicos, asegurando la provisión de información

oportuna y relevante. La investigación tuvo como objetivo presentar un modelo que, mediante descripciones de la gestión de incidentes, el diseño de procesos y supervisar los indicadores de procesos, con el fin de identificar y mitigar las posibles incidencias en los servicios de TI. Con cinco componentes, incluyendo procesos de implementación y operación, el modelo se validó mediante el seguimiento de tres incidencias del servicio SAP ERP, evaluando su rendimiento en un intervalo de tiempo.

Tesis: Díaz Rosemberg (2006) Diseño e Implementación del Centro de Operación y Gestión de la red Académica Peruana en Software Libre, quien se planteó como objetivo principal. Con el objetivo principal de este trabajo de investigación fue diseñar e implementar una solución de monitoreo y control para la Red Académica Peruana. Esto implica la selección y adaptación de software para las necesidades específicas de la RAAP, con el fin de optimizar el uso de recursos y detectar rápidamente posibles fallas para asegurar un funcionamiento eficiente de la red y sus equipos llegando a las siguientes conclusiones:

Analizar las características y funciones de la RAAP, diseñando e implementando una solución automatizada para su gestión y monitoreo.

Obtener y almacenar estadísticas de la red a través de una herramienta automatizada, visualizando su realizada y su evolución histórica.

Monitorear el estado de los equipos y los servicios informáticos que corren a través de estos a través de una solución informática, reportando alertas en caso ocurra un error.

Tesis: Reque Casas & Sempértegui Tocto (2017) Implementar un sistema de monitoreo y supervisión para optimizar la administración de la red de datos y

el monitoreo continuo de dispositivos que integran la infraestructura y servicios de red en la Universidad Nacional Pedro Ruiz Gallo. Como objetivo principal identificar la necesidad de implementar un sistema de monitoreo y supervisión para optimizar la administración de la red de datos y el monitoreo continuo de los dispositivos que integran la infraestructura y servicios de red; llegando a la siguiente conclusión:

El estudio reveló que el área de Administración de Red Telemática no contaba con un sistema de monitoreo adecuado, lo que provocaba la falta de información centralizada y retrasos en la detección de caídas de red en equipos y servicios. Se evaluaron diferentes herramientas de monitoreo, seleccionando Nagios Core como la herramienta más adecuada por cumplir con la mayoría de los parámetros establecidos para la solución.

Además, el área de Administración de Red Telemática experimenta los mayores beneficios, ya que tanto la eficiencia de los recursos como la del personal encargado aumentan con el sistema de monitoreo. Este último facilita la comunicación de alertas de forma continua, sin depender de la notificación de los usuarios finales.

Tesis*:* Aceituno Rojo (2013) Modelo de monitoreo de servidores basado en SNMP y Balanced Scorecard para mejorar el tiempo de detección de incidentes en la empresa de distribución eléctrica Electro Puno S.A.A. El propósito principal fue desarrollar un modelo que permitió el monitoreo de los servidores basado en SNMP y Balanced Scorecard buscando optimizar el tiempo de detección de incidentes en la entidad de distribución eléctrica Electro Puno S.A.A.

Se desarrolló un modelo que permite el monitoreo de los servidores de la

empresa Electro Puno S.A.A. basándose en Balanced Scorecard, con dicha herramienta se determinó 14 indicadores, utilizando a su vez el protocolo SNMP y desarrollado sobre la plataforma Windows con Tecnologías .NET que mejoró el tiempo de detección de incidentes en un 87.78%.

Se logró determinar los indicadores utilizando la técnica Balanced Scorecard que son: Estado del servidor, número de procesos cargados, número de usuarios conectados, porcentaje de uso del disco duro, porcentaje de uso de la memorias virtual y física, porcentaje de uso de los procesadores, porcentaje de uso de las tarjetas de comunicación, número de errores en las tarjetas de comunicación, estado de los discos duros, fuentes de alimentación, sockets de la memoria RAM, sockets de los microprocesadores, tarjetas de comunicación los cuáles fueron utilizados para la construcción del modelo.

2.1.2 Antecedentes internacionales:

Ruiz González & Velthius Piattini (2021) Gobierno y gestión de las tecnologías y los sistemas de información. Quienes identificó en su visión general del cuadro de mando integral de la tecnología de sistemas de información; a partir de 1994 la historia del perfeccionamiento continuo del servicio de la Tecnología del Sistema de Información se enfocaba en los retos de las técnicas de evaluación y sus beneficios, pero a partir del año 2000 se genera una especialización del perfeccionamiento continuo del servicio para contener dominios del gobierno tecnológico, la gestión del conocimiento, la auditoría, entre otros.

Vega Picon (2018) llevó a cabo la implementación de un sistema de monitoreo para analizar la disponibilidad, capacidad, calidad y latencia de los enlaces corporativos de última milla. Su objetivo principal permitió implementar

una solución automatizada de uso gratuito para el monitoreo que garantizó un nivel de servicio adecuado en estos enlaces, siguiendo un SLA predefinido. Las conclusiones obtenidas fueron las siguientes:

Se examinó la importancia de realizar monitoreo de red en las empresas y cómo esta práctica contribuye significativamente a reducir los efectos negativos que podrían surgir al tener enlaces con problemas. Además, se comprobó que el monitoreo de red puede prevenir sanciones elevadas impuestas por entidades reguladoras al detectar un servicio caído. Se determinó que el protocolo SNMP es el principal mecanismo para recopilar la información importante para el monitoreo. A través de este protocolo, se intercambian mensajes entre el aplicativo de registro con el servidor permitiendo verificar el estado de los equipos supervisados. Se analizaron diversas versiones del protocolo, encontrando que la versión más segura es la versión tres, debido a sus avanzados algoritmos de cifrado. No obstante, también se utilizó la versión dos del protocolo, porque algunos equipos con Windows o Linux existen incompatibilidad con la versión tres. Las herramientas de monitoreo implementadas, Cacti y Nagios, proporcionan las métricas necesarias para analizar una red y comprender su funcionamiento. Nagios se encarga de evaluar la calidad y disponibilidad, mientras que Cacti se enfoca en medir la latencia y capacidad. Esto permite al administrador de red abordar los problemas que surjan y garantizar la estabilidad de la red.

Velasco Briones & Cagua Ordoñez (2017) llevaron a cabo la implementación de un Sistema de Monitoreo de Redes utilizando herramientas de código abierto y la provisión de Servicios de Directorio a través de Active Directory en la Facultad de Filosofía, Letras y Ciencias de la Educación de la Universidad de Guayaquil. Su objetivo principal fue monitorear servidores y

enlaces, así como establecer políticas a través de Active Directory para cumplir con las normas de la facultad. Con la implementación de Active Directory y Nagios, se logró monitorear servidores y obtener información detallada del estado de los servicios monitoreados. Nagios permitió identificar y prevenir errores, optimizar recursos y proporcionar soluciones rápidas a problemas. La instalación de Active Directory facilitó la gestión de equipos, usuarios y dispositivos, permitiendo búsquedas rápidas y acceso a información detallada del dominio.

Ruiz Quintero (2016) Diseño de un plan de gestión de servicios en el área de sistemas y Tecnologías de información de la Gobernación de Santander de acuerdo con las mejores prácticas de ITIL 4**.** El propósito principal de este trabajo de investigación fue diseñar una estrategia de gestión de los servicios en el área de Sistemas y Tecnologías de información de la dirección de Santander en alineación a las mejores prácticas de ITIL 4, asociando su cumplimiento de la eficiencia y excelencia con el cumplimiento de los objetivos organizacionales; llegando a las siguientes conclusiones:

La revisión comparativa sobre la situación actual de la organización permitió identificar la necesidad de implantar los Procesos de Administración de Incidentes, requerimientos y Mesa de Servicios con la finalidad de realizar un levantamiento de información basado en el diseñó los procesos y sus procedimientos como parte fundamental que ha permitido definir los servicios principales y los sub-servicios en conjunto de los actores responsabilizando la ejecución de los procesos y procedimientos definidos, esto tiene un alcance para un cambio cultural en los usuarios y personal de Tecnologías, para que las peticiones sean canalizadas a través de un único punto.

Abrahäo & Calero (2022) Calidad y sostenibilidad de sistemas de información en la práctica. Con el objetivo principal de esta investigación fue implementar de forma sistemática tácticas de gamificación del proceso de Gestión de Incidencias de Servicios de TI a las organizaciones de soporte TI, han diseñado una guía de pasos a seguir para solucionar los problemas y alcances de los objetivos organizacionales. Esta estrategia permite crecer el compromiso del personal de atención que pertenecen a los grupos de soporte en los procesos de alineación y amaestramiento con el fin de contar con los conocimientos y habilidades requeridas para una gestión eficiente de la atención de incidencias. Así como, impulsar y entender el impacto de la atención adecuada al resolver las incidencias que se presentan diariamente. También, conseguir un mejor rendimiento y mejorar los resultados de los KPIs del proceso.

2.2 MARCO TEÓRICO

2.2.1 Definiciones generales

- **Metodología:** De acuerdo con la RAE, el entendimiento de la Metodología es la ciencia del método. Conjunto de métodos que persiguen una investigación científica o en una exposición doctrinal. Su significado se direcciona a un plan de investigación en donde se siguen pasos, cada uno de los cuales nos va a permitir el cumplimiento de objetivos determinados para que la suma de estos nos dé como resultado final aquellos datos de la investigación que nos interesan.
- **Gestión de Incidentes:** Práctica de ITIL para minimizar el impacto negativo de los incidentes restaurando el funcionamiento del servicio lo más rápido posible. (AXELOS Limited, 2019).

- **Impacto:** Es la medición del efecto de un incidente, problema o cambio en los procesos de la Entidad. Usualmente, su impacto se basa en función de cómo los niveles de servicio se verán afectados.
- **Incidencia:** Interrupción no planificada de un servicio de TI o reducción en la calidad de un servicio de TI. (AXELOS Limited, 2019).
- **Incidencia de impacto**: Un evento se considera como tal cuando no es parte de la operación estándar de un servicio y provoca, o tiene el potencial de provocar, una interrupción o disminución en la calidad del servicio. Este evento tiene una relevancia significativa, ya que afecta tanto a los procesos comerciales como a un grupo específico de usuarios, destacándose por su prioridad alta en términos de impacto y urgencia.
- **ITMS**: (Information Technology Service Management), Gestión de servicios de Tecnología de información es un enfoque estratégico para aportar valor al negocio mediante soluciones TI combinando de forma adecuada Personas, Procesos y Tecnología, ayuda a realizar la conexión entre TI y la estrategia de negocio y ayuda a las organizaciones a entender el impacto de TI en sus distintos procesos de negocio.
- **Acuerdo de Nivel de Servicio (SLA):** Acuerdo entre el proveedor de servicios y un cliente en el cual se especifica los servicios requeridos, las responsabilidades entre ellos, tiempos de resolución, así como el nivel del servicio esperado. (AXELOS Limited, 2019)
- **Problema:** Una causa o causa potencial de un conjunto de incidentes.
- **Base de Datos de Incidentes:** Repositorio de incidentes ocurridos (historial de incidentes) con sus soluciones y tiempo de resolución. (Axelos, 2019).

- **Workaround**: El workaround o solución alterna es una solución alterna que trabaja con el objetivo de reducir o eliminar los efectos de los errores conocidos. Este tipo de soluciones muchas veces reducen la probabilidad de incidentes. (Hällkvist, 2017).
- **Base de datos de errores conocidos**: Repositorio de problemas que se han analizado, pero no se han resuelto. (Axelo, 2019).
- **Monitoreo:** Observación repetida de un sistema, una práctica, un proceso, un servicio o una entidad con el objetivo de conocer su estado actual y detectar posibles eventos. (Limited et al., 2019).
- **24/7:** *"24 hours a day/ 7 days a week"* (Farlex Inc, 2012), su traducción al español es 24 horas un día/ 7 días una semana, por lo cual se llega a la definición de que 24/7 es disponibilidad continua.
- **Detección:** "Localización de alguna cosa que no puede observarse directamente mediante aparatos o métodos físicos o químicos" (WordReference, 2012).
- **Indicador:** *"Dispositivo o señal que comunica o pone de manifiesto un hecho"* (Word Reference, 2012).
- **Modelo:** *"Arquetipo o punto de referencia para imitarlo o reproducirlo"* (Word Reference, 2012).
- **OPEN SOURCE:** El término que se traduce como "código abierto", pero suele ser mencionado comúnmente en su expresión de la lengua inglesa Se refiere a software distribuido bajo una licencia que permite a los usuarios acceder, leer, modificar, mejorar y redistribuir su código fuente. Ejemplos destacados de software de código abierto incluyen distribuciones de Linux

(Centos, Ubuntu, Debian, Fedora), el antivirus Clam Win, el reproductor de video VideoLan, y el editor de imágenes GIMP.

2.2.2 ITIL

ITIL 4 ofrece un enfoque completo que incorpora marcos como Lean, Agile y DevOps para la entrega y operación de productos y servicios de TI. Este marco nos proporciona orientación en ITSM. No “hacemos” o “implementamos” como un objetivo fijo, sino que se ve como una caja de herramientas. ITIL 4 se diseñó para colaborar con diversos marcos y métodos en la industria de TI, permitiendo a los equipos de TI desempeñar un papel esencial en la estrategia.

Para alcanzar una gestión eficaz, se requiere la implementación de un conjunto de métodos y estándares que permitan la mejora continua, tales como: los principios de ITIL (Information Technology Infrastructure Library): Marco de referencia para la gestión de servicios de TI. Estándares ISO/IEC 20000: Norma internacional para la gestión de servicios de TI.

2.2.3 Estructura y beneficios de ITIL

ITIL 4 ofrece un enfoque practico y flexible para soportar a todas las organizaciones en una travesía hacia el mundo de la transformación digital. Los componentes clave en el marco ITIL 4 son el Sistema de Valor del Servicio (SVS) y el modelo de cuatro dimensiones como se puede apreciar en la siguiente figura:

Figura 1

Sistema de Valor del Servicio (SVS) y el Modelo de cuatro dimensiones

Nota: Resume el proceso de transformación en relación al ingreso y la salida ante un pedido de atención (AXELOS Limited, 2019)

El SVS representa cómo los diversos componentes y actividades de la organización trabajan juntos para facilitar la creación de valor mediante servicios habilitados por TI. El SVS facilita la integración y coordinación y proporciona una dirección fuerte, unificada y enfocada en el valor, para la organización.

a. **Centrarse en el valor**: ITIL se enfoca en la creación de valor, y este principio destaca que las organizaciones deben colaborar entre todas sus áreas para lograrlo.
b. **Empezar donde estás:** ITIL enfatiza que no es necesario comenzar desde cero, sino aprovechar los recursos disponibles y reutilizar procesos existentes para crear nuevo valor. Es crucial analizar la situación actual y evaluar la importancia de los roles en ese contexto.
c. **Progreso iterativamente con valor:** ITIL promueve la implementación

iterativa al desglosar las actividades, lo que reduce el esfuerzo y permite ver resultados más rápidamente, facilitando el mantenimiento a largo plazo.

d. **Colaborar y promover la visibilidad:** Siendo importante mantener un adecuado trabajo en equipo, es un punto central en ITIL, enfatiza la colaboración y el trabajo en equipo, identificando a las personas clave para implementar iniciativas de manera efectiva y asignando roles adecuados.
e. **Pensar y trabajar holísticamente:** Como mencionamos previamente, es fundamental colaborar de manera conjunta, compartiendo un enfoque y una meta comunes, para lograr una entrega efectiva de valor.
f. **Mantenerlo simple y práctico:** Este se enfoca en la reducción de procesos complejos y más bien implementar procesos sencillos que puedan optimizar los recursos con los que se cuenta para añadir mayor valor a los resultados.
g. **Optimizar y automatizar:** El último paso es la automatización, pero antes es necesario la optimización para lo cual los procesos se deben de enfocar en que estos tengan una mínima intervención humana optimizando los tiempos y recursos para posteriormente optimizar estos.

Para garantizar un enfoque holístico en la gestión de servicios, ITIL 4 define cuatro dimensiones de la gestión de servicios:

- Organizaciones y personas
- Información y tecnología
- Partes interesadas
- Flujos de valor y procesos

Para garantizar que el SVS es fundamental que los componentes y actividades de una organización colaboran como un sistema integrado para generar valor. Cada SVS de la organización se conecta con otras entidades, formando un ecosistema que facilita la creación de valor para las organizaciones involucradas, sus clientes y demás partes interesadas. El propósito del SVS es asegurar que la organización colabore continuamente con todas las partes interesadas para crear valor a través de la gestión eficaz de productos y servicios.(AXELOS Limited, 2019).

ITIL 4 Fundamentos se limita a las 15 prácticas más utilizadas. Es importante que se entienda el propósito de estas prácticas.

2.2.4 Ventajas de ITIL

Su implementación puede traer consigo una serie de beneficios para las organizaciones, entre los que se destacan:

a. **Optimización de procesos:** ITIL 4 proporciona una guía para la mejora continua de los procesos de TI, lo que se traduce en una mayor eficiencia y eficacia en la entrega de servicios.
b. **Reducción de costos:** La optimización de procesos y la automatización de tareas redundantes pueden generar una reducción significativa en los costos operativos de TI.
c. **Mejora en la calidad del servicio:** ITIL 4 pone énfasis en la experiencia del usuario y la satisfacción del cliente, lo que conduce a una mejora en la calidad de los servicios prestados.

2.2.4.1 Mayor Agilidad y Adaptabilidad:

a. **Enfoque flexible:** ITIL 4 se basa en un conjunto de principios y prácticas que pueden adaptarse a las necesidades específicas de cada organización.

b. **Capacidad de respuesta a los cambios:** La naturaleza adaptable de ITIL 4 que ha permitido a las organizaciones hacer frente a los cambios en el entorno empresarial y tecnológico.

c. **Optimiza la toma de decisiones:** ITIL 4 ofrece un enfoque estructurado para tomar decisiones, basadas en datos y métricas, mejorando así la calidad de las decisiones estratégicas.

d. **Mejor Alineación con la Estrategia Empresarial:**

- **Enfoque en la creación de valor:** En el nuevo enfoque de ITIL 4 se enfoca en cómo la organización puede generar valor a través de la gestión del servicio de TI
- **Mejora en la comunicación y colaboración:** ITIL 4 fomenta la comunicación y la colaboración entre las diferentes áreas de la organización.
- **Mayor transparencia y control:** ITIL 4 Por último, este marco también se centra en cómo puede mejorar el control y la transparencia mediante el cual se provee los servicios de TI.

e. **Beneficios adicionales:**

- **Mejora en la gestión de riesgos:** ITIL 4 proporciona herramientas para la identificación, evaluación y gestión de riesgos asociados a los servicios de TI.

- **Desarrollo de competencias:** ITIL 4 ofrece un marco para el desarrollo de las competencias del personal de TI.
- **Mejora en la cultura organizacional:** ITIL 4 promueve una cultura de colaboración, responsabilidad y mejora continua.

2.2.4.2 Prácticas de Gestión de Servicios TI.

T Service Management: La gestión de servicios de TI implica la implementación de prácticas de TI de alta calidad que satisfacen las necesidades del entorno del negocio. Al gestionar TI desde una perspectiva empresarial, se logra un alto rendimiento y se crea valor.

Para abordar los desafíos del mundo actual al gestionar los servicios de TIC y adoptar el enfoque como ITIL 4, es esencial comprender los siguientes conceptos clave:

a. Organizaciones, Proveedores y Consumidores de Servicios:

- Estos actores desempeñan roles cruciales en la prestación de servicios.
- La co-creación de valor es fundamental para lograr resultados positivos.

b. Productos y Servicios:

- Los productos son los componentes tangibles, mientras que los servicios son las experiencias intangibles que se entregan a los consumidores.
- La gestión efectiva de ambos es esencial para el éxito.

c. Relaciones de Servicios:

- Estas conexiones entre proveedores y consumidores de servicios influyen en la calidad y el valor percibido.
- Comprender y gestionar estas relaciones es clave.

2.2.4.3 Gestión de la Disponibilidad

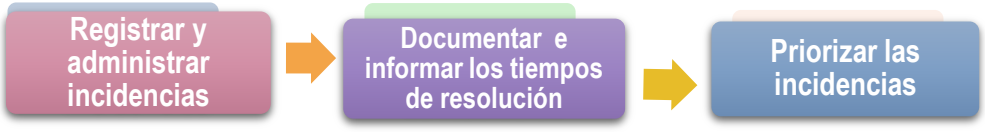
- Garantiza que los servicios estén disponibles según las necesidades de usuarios y clientes.
- Involucra establecer y negociar objetivos de disponibilidad, diseñar infraestructuras y aplicaciones con niveles de disponibilidad, recopilar datos relevantes sobre la disponibilidad, analizar e informar sobre la misma, y planificar mejoras.

2.2.4.4 Gestión de Incidentes

- Busca minimizar los impactos negativos de las incidencias en la satisfacción del usuario o cliente.
- Es fundamental registrar y abordar cada incidencia para asegurar una resolución rápida.
- Almacenar información sobre las incidencias permite detectar problemas, errores y facilita un diagnóstico eficiente para una recuperación ágil.

Figura 2

Actividades de la gestión de incidentes



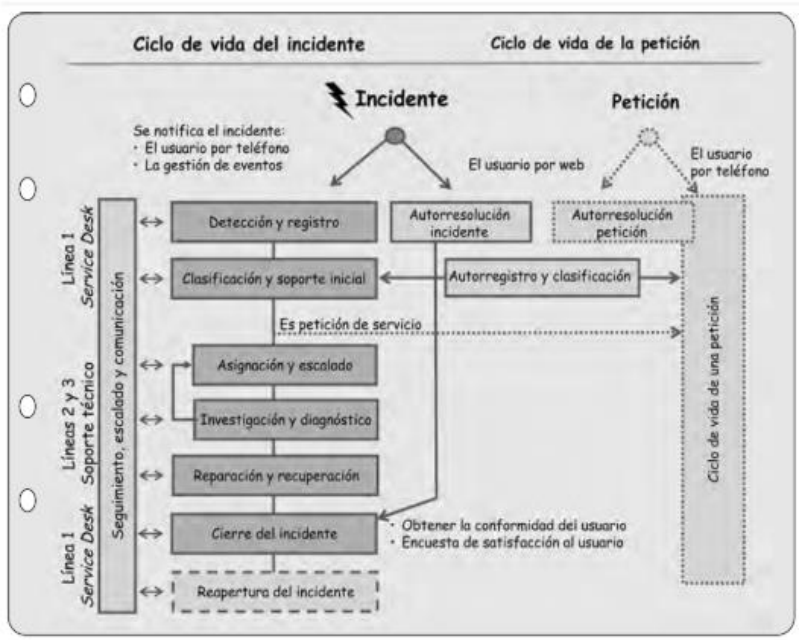
Nota: ITIL(R) Foundation Essentials ITIL 4 Edition.

2.2.4.4.1 Ciclo de vida de un incidente

El ciclo de vida de un incidente en TI se refiere a las etapas que atraviesa un incidente desde su detección hasta su resolución. Según Luis Morán Abad (2009), existen tres ciclos comunes en las organizaciones: gestión de incidentes, peticiones de usuario y cambios. La gestión de incidentes implica la implementación de niveles de escalado, una mesa de servicio TI, y diferentes canales de comunicación, los cuales se ilustran en la siguiente figura:

Figura 3

Ciclo de vida de un incidente.



Nota: Guía para la gestión de los servicios de tecnologías de la información(Morán, 2009).

De la figura N°3, se identifican diversas actividades que se detallan a continuación:

a. **Detección y Registro**:

- El usuario notifica a la mesa de ayuda sobre el incidente a través de diferentes canales.

- El incidente se registra para realizar un seguimiento adecuado.

b. Clasificación y Soporte Inicial:

- Se clasifica el incidente para identificar su categoría y facilitar la búsqueda de soluciones.
- El personal de la mesa de ayuda proporciona el primer nivel de apoyo.
- Si no se puede resolver de inmediato, se pasa al siguiente paso.

c. Investigación y Diagnóstico:

- El personal evalúa el incidente, investiga las posibles causas y brinda un diagnóstico.
- Si no se puede resolver, se escala a instancias más especializadas.

d. Reparación y Recuperación:

- Se implementa la solución para reanudar las operaciones del negocio.

e. Cierre del Incidente:

- Una vez que el usuario confirma que el problema ha sido resuelto y puede continuar con sus actividades, la mesa de servicio mantiene una comunicación directa con el usuario.

f. Reapertura del Incidente:

- En caso el usuario no esté satisfecho con la resolución o si el problema se ha solucionado parcialmente, se solicita la reapertura del ticket para un seguimiento adicional.

2.2.4.5 Gestión de eventos y monitoreo

La gestión de eventos se enfoca en registrar y manejar los cambios supervisados que se definen como eventos, con el fin analizar dichos eventos y tomar las medidas de control apropiadas para gestionarlos. “Un evento puede definirse como cualquier cambio de estado que tenga importancia para la gestión de un elemento de configuración (CI) o servicio de TI. Los eventos generalmente se reconocen a través de notificaciones creadas por un servicio de TI, CI o herramienta de monitoreo”.(AXELOS Limited, 2019).

2.2.4.6 Gestión de problemas

El objetivo principal de la gestión de problemas es minimizar la probabilidad y el impacto de las incidencias, resolviendo los problemas antes de que afecten al servicio. Se relaciona estrechamente con la gestión de errores y soluciones, identificándose mediante el análisis y la detección de problemas.

2.2.4.7 Gestión de la continuidad del servicio

Es un proceso estratégico y proactivo que garantiza la continuidad de los servicios de tecnología de la información (TI) ante eventos desastres o interrupciones, asegurando la disponibilidad y el acceso a la información y las aplicaciones críticas para la organización. Esto implica la creación de un marco resiliente para respuestas rápidas y efectivas, considerando un punto de recuperación, es decir, es un punto en el tiempo de recuperación de un estado específico, planes de recuperación ante desastres y análisis de impacto en la entidad.

2.2.4.8 Service desk

La mesa de ayuda es un servicio responsable de gestionar las solicitudes, incidencias y peticiones de los usuarios, proporcionando una primera línea de soporte y resolución de problemas relacionados con los servicios de TI.

El propósito de la práctica del Service Desk es:

a. Entender la demanda de resolución de incidentes y solicitudes de servicio.

b. Servir como el principal punto de contacto entre el proveedor de servicios y los usuarios.

c. Ofrecer una vía clara para que los usuarios informen asuntos, consultas y solicitudes, y para que dichos reportes sean reconocidos, clasificados, gestionados y resueltos.

2.2.5 Sistema de monitoreo de TI

Es una herramienta de seguimiento que permite recolectar, tratar, analizar y generar información a un grupo de actores interesados en la implementación de un determinado proyecto, con el fin de informar y contribuir a una mejor toma de decisiones (Lauriac, 2016).

Según Alestra (2020), existen tres tipos de herramientas destinadas al monitoreo de TI:

- **Herramientas de observación:** Estas herramientas recopilan datos sobre el estado y el rendimiento de los sistemas de TI. Permiten visualizar la información en tiempo real y detectar posibles anomalías.

- **Herramientas analíticas:** Estas herramientas procesan los datos recopilados por las herramientas de observación para identificar tendencias, patrones y posibles problemas. Ayudan a analizar el comportamiento de los sistemas de TI y a predecir posibles fallos.
- **Herramientas de engagement:** Estas herramientas facilitan la interacción con los usuarios y permiten resolver problemas de manera rápida y eficiente. Pueden incluir chatbots, sistemas de ticketing o plataformas de comunicación.

En cuanto a los tipos de monitoreo que los encargados de TI deben realizar, se pueden identificar los siguientes:

- **Monitoreo de desempeño:** Se enfoca en evaluar el rendimiento de los sistemas de TI, incluyendo la velocidad, la capacidad de respuesta y la eficiencia.
- **Monitoreo de sistema:** Se centra en la detección de errores, fallos y problemas en los sistemas operativos, hardware y software.
- **Monitoreo de usuario:** Evalúa la experiencia de los usuarios con los servicios de TI, incluyendo la satisfacción, la facilidad de uso y la disponibilidad.
- **Monitoreo de seguridad:** Se encarga de identificar y prevenir amenazas a la seguridad de los sistemas de TI, como ataques cibernéticos o accesos no autorizados.

Finalmente, Escobar (2015) destaca dos perspectivas para abordar el proceso de monitoreo de una red:

- **Monitoreo activo:** Implica la realización de pruebas y análisis periódicos para evaluar el estado y el rendimiento de la red.

- **Monitoreo pasivo:** Se basa en la recopilación y análisis de datos generados por la red, como registros de eventos o tráfico de red.

2.2.6 Monitoreo de redes

2.2.6.1 Monitoreo de aplicaciones

Las aplicaciones son componentes cruciales de la infraestructura. Las fallas de aplicación son, por lo general, los problemas más comunes en una infraestructura de TI. Monitorear las aplicaciones críticas con medidas preventivas ayuda a evitar fallas en las aplicaciones e identificar oportunamente las degradaciones. Algunas de las aplicaciones que se monitorean incluyen: Microsoft Exchange, MySQL, Lotus Notes, MSSQL y Oracle.

Algunos tipos de monitoreo de aplicaciones incluyen:

2.2.6.1.1 Monitoreo de protocolos de servicios:

Permite monitorear la disponibilidad y el tiempo de respuesta de los servicios que se ejecutan en los servidores. La funcionalidad de monitoreo de servicios proporciona gráficos e informes detallados sobre la disponibilidad de los servicios que se están monitoreando. Algunos de los servicios que se pueden monitorear incluyen: DNS, IMAP, SMTP, Echo, LDAP, Telnet, FTP, NNTP, Web, POP, HTTPS, etc.

2.2.6.1.2 Monitoreo de URL's web

El monitoreo de URLs permite monitorear la disponibilidad del sitio web (o sitios web, si hay más de uno) o páginas intranet y verificar si están funcionando en tiempo real. Algunos tipos de monitoreo incluyen: Monitoreo de URLs, directorios virtuales, intranet, coincidencia de contenido, servidores web y aplicaciones web.

Las herramientas de monitoreo son software de monitoreo de redes que ofrecen una combinación de monitoreo de WAN, servidores y aplicaciones con integración de mesa de ayuda, control de activos y análisis de la funcionalidad del tráfico en la WAN. Automatizan varias tareas de monitoreo y eliminan la complejidad asociada con el control de la red.

Algunos instrumentos de monitoreo tienen diversos tipos de monitoreo, los cuales son:

d. **Monitoreo de la red:** Detecta problemas de rendimiento de la red antes de que causen costosos tiempos de inactividad.
e. **Monitoreo de servidores:** Potencia la disponibilidad y el rendimiento de la infraestructura de servidores.
f. **Monitoreo de aplicaciones:** Reconocer los problemas de rendimiento de las aplicaciones proactivamente previniendo un impacto en los usuarios finales.

2.2.6.2 Arquitectura de administración de redes

La administración de redes es un campo crucial para garantizar el funcionamiento eficiente y seguro de las infraestructuras de TI. Como

menciona (Calvo García, 2014), la arquitectura de administración de redes implica supervisar, configurar y controlar tanto los componentes hardware como software de una red. Algunos de los elementos clave en esta arquitectura son la recolección de datos para supervisar dispositivos remotos y la implementación de cambios para mantener el control.

En cuanto a las definiciones, es cierto que existen diversas perspectivas. Además de los aportes de Quezada, también se pueden considerar las contribuciones de Hernández y Ford & Kim. Cada autor puede ofrecer una visión única sobre cómo abordar la gestión de red, y es importante tener en cuenta estas perspectivas variadas para desarrollar estrategias efectivas.

La arquitectura de administración de redes se compone de los siguientes elementos:

a. **Puntos de acceso administrado:** Un dispositivo administrado conforma la infraestructura de red y utiliza software especializado para enviar alertas cuando se detecta un problema. Estos dispositivos pueden incluir hosts, equipos de comunicaciones como, routers, switch's, impresoras o módems. En cada uno de estos dispositivos, existen diversos objetos que pueden ser administrados, como tarjetas de red, interfaces, CPU, disco duro, memoria RAM, entre otros. Estos objetos, están basados en parámetros de configuración específicos, proporcionarán información a la entidad administradora.

b. **Entidad responsable de administrar:** La entidad administradora es responsable de la recepción de los mensajes de

alerta. Estos mensajes son programados con la finalidad de ejecutar las actividades técnicas, con copia al administrador del servicio. También, las funciones del Centro de Operaciones de Red (NOC) incluyen el registrar, controlar, procesar, analizar y visualizar la información de administración.

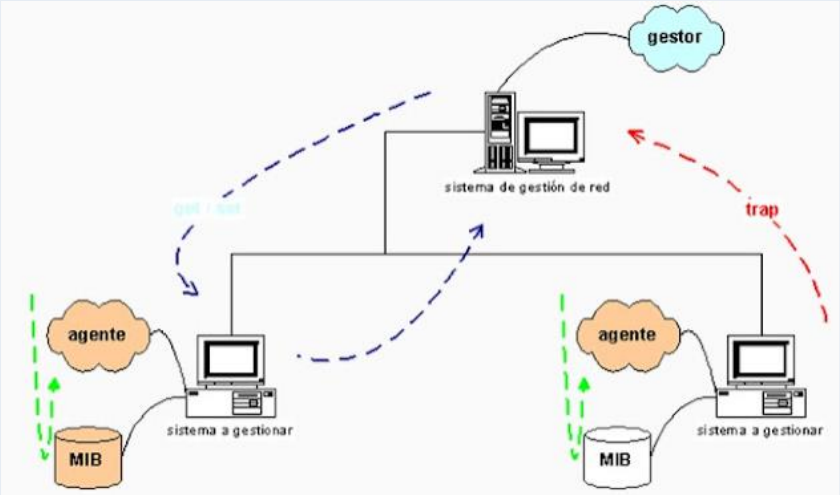
c. **Agentes de red:** El agente de red es quien comunica a la entidad administradora y el dispositivo administrado. Este último responder ante un suceso no deseado. En la instalación de un agente de red en un dispositivo administrado, se especificarán los parámetros de la entidad administradora a la que se conectará, para asegurar que los datos viajen de forma segura y estén dirigidos solo a un NOC.

d. **Base de información de administración:** La MIB (Management Information Base), de sus siglas en inglés, contiene información relacionada a los dispositivos que administra una red y es considerado como un tipo de base de datos.

e. **Protocolo de gestión de red:** Los protocolos de administración de red permiten a algún agente verificar el estado de los dispositivos y sus servicios, facilitando la realización de acciones preventivas. En escancia, la arquitectura de red actúa como un "esquema" en el que se integran y colaboran los protocolos, los agentes, la MIB, la entidad gestora y la estación terminal, con el objetivo principal de optimizar la gestión de la red.

Figura 4

Esquema de una red gestionada con SNMP.



Nota: Detalla el flujo de SNMP (Jesús & Tejedor, 2006).

Según Millán Tejedor (2006) El protocolo SNMP (Simple Network Management Protocol) aborda la heterogeneidad de los dispositivos de red mediante un enfoque que permite la interoperabilidad entre sistemas con diferentes arquitecturas y protocolos. A pesar de que los dispositivos de red utilizan diversas técnicas para la presentación de datos, lo que podría comprometer la capacidad de SNMP para intercambiar información, este protocolo utiliza un subconjunto de ASN.1 (Abstract Syntax Notation One) para facilitar la comunicación entre sistemas heterogéneos.

ASN.1 es un estándar de notación para la definición de datos y la codificación de información. Su uso en SNMP permite la representación y el intercambio de información de manera independiente del lenguaje de programación o la arquitectura del dispositivo. Esto garantiza que los dispositivos de red, a pesar de sus diferencias, puedan comunicarse de

forma efectiva a través de SNMP, permitiendo la gestión y el control de la red de manera eficiente.

2.2.6.3 SNMP: protocolo de gestión de red

El Protocolo Simple de gestión de Red (SNMP) es un estándar definido por el IETF para la administración y monitoreo de host en redes. Aunque su nombre implica simplicidad, SNMP ha evolucionado para incluir características avanzadas como autenticación y encriptación. Permite a los administradores gestionar servidores, estaciones de trabajo, routers, switches y dispositivos de seguridad en redes IP, facilitando el monitoreo del rendimiento, la detección y resolución de problemas, y la planificación del crecimiento de la red. SNMP usa el puerto UDP 162 para la comunicación entre aplicaciones de administración y agentes de red.

2.2.6.3.1 Versiones de SNMP

En la actualidad, existen tres versiones del protocolo SNMP, que son los siguiente:

a. SNMPv1:

- Primera versión, definida en 1988 en las RFC 1150 y 1157.
- Ampliamente utilizada debido a su simplicidad en la autenticación y políticas de acceso.
- Problemas: Falta de autenticación y seguridad; la cadena de comunidad se transmite en texto plano.

b. SNMPv2:

Apareció en 1993 y se define en las RFC 1901 a 1908.

- Mejoras en la seguridad, rendimiento y confidencialidad en comparación con SNMPv1.
- No fue ampliamente aceptada debido a su complejidad.
- Luego se desarrolló SNMPv2c que, intregró el sistema de seguridad tomando como base la cadena de comunidad de SNMPv1.

c. SNMPv3: Utiliza Hash-based MAC con MD5 o SHA para autenticación y DES-56 para privacidad, emplea TCP en lugar de UDP y ofrece mejor seguridad y flexibilidad.

En resumen, SNMPv3 es la versión más segura y completa, pero todas tienen su lugar según las necesidades específicas de la red.

Tabla 2

Modelos y niveles de seguridad versiones de SNMP

VERSIÓN	DESCRIPCIÓN	AUTENTICACIÓN	CIFRADO	SEGURIDAD
SNMPV1	Emplea el modelo basado en comunidades	Community string	No	No autenticación No Encriptado
SNMPV2 SNMPV2C	Emplea el enfoque basado en comunidades	Community string	No	No autenticación No Encriptado
SNMPV3	Emplea nombres de usuario para verificar la autenticación	USM	No	No autenticación No Encriptado
SNMPV3	Versión de SNMPv3 que ofrece autenticación mediante los algoritmos HMAC-SHA o HMAC-MD5	USM + MD5 o SHA	No	Autenticación No Encriptado

Nota: Consolidar las comparaciones entre versiones del SNMP (Cisco Systems, 2020)

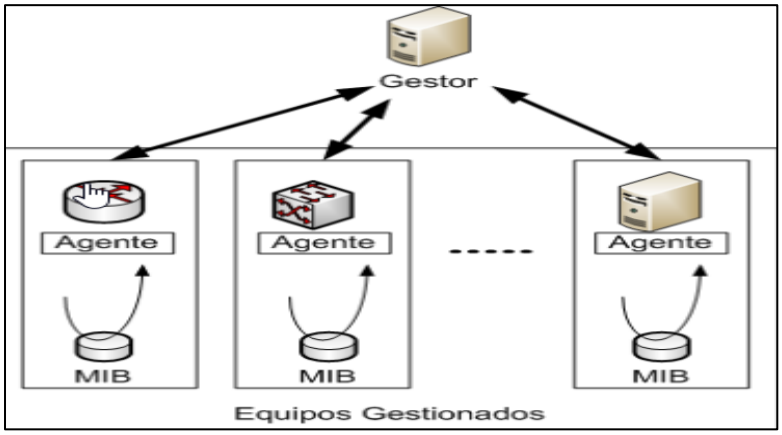
2.2.6.4 Componente de SNMP

El Protocolo Simple de Administración de Red (SNMP), ampliamente utilizado en la gestión de redes. Facilitando la obtención de la información de la cantidad de memoria libre, los dispositivos de la red, el uso de la CPU, la identificación de errores y el tiempo de actividad. El sistema SNMP se compone de tres elementos principales:

- **Gestor**: También reconocida como estación de administración, su función es supervisar y gestionar los dispositivos de red a través de un programa llamado NMS (Sistema de Gestión de Red) que, envía y recibe mensajes SNMP.
- **Agentes**: Estos programas residen en los dispositivos que se administran y permiten acceder a los datos. Los agentes atienden las solicitudes y comunican los posibles problemas.
- **Base de Información de Administración (MIB)**: La MIB describe de forma lógica de la información de los dispositivos de red gestionados.

Figura 5

Componentes del SNMP



Nota: Detalla el flujo de información del SNMP (Barth, 2006).

2.2.6.4.1 MIB

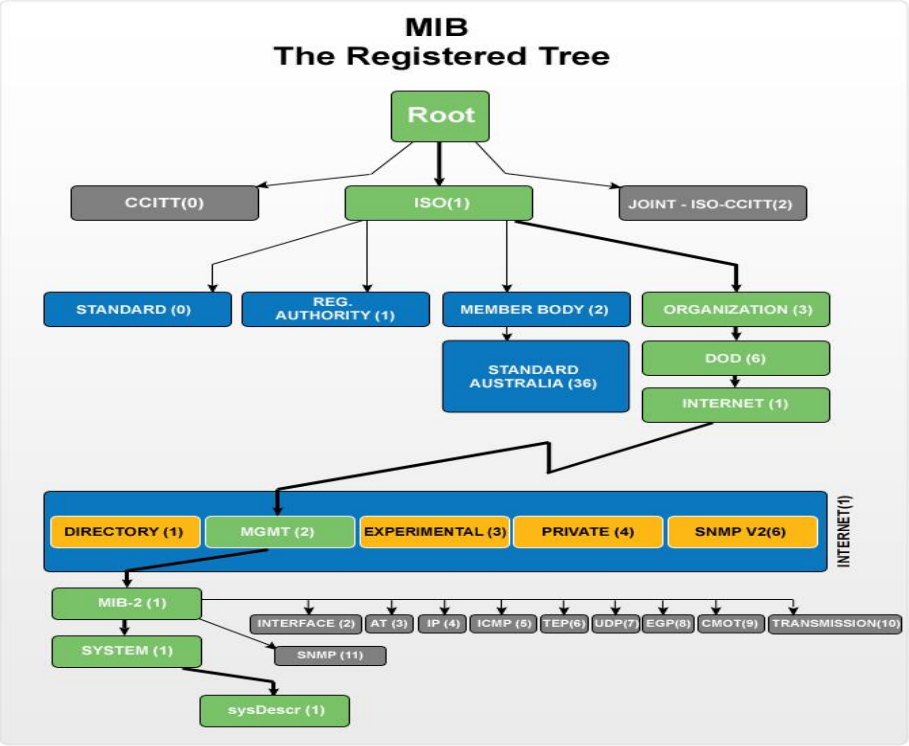
La MIB (Base de Información de Gestión) se define como una base de datos jerarquizado almacenando información de los dispositivos en la red. Organiza los datos en forma de árbol y contiene atributos de configuración y funcionamiento de los objetos administrados. Por lo general, se almacena en cada dispositivo administrado. El agente recopila datos y el administrador de SNMP solicita información específica y la traduce según sea necesario para el Sistema de Gestión de Red (NMS). La Figura N° 06 muestra la estructura del árbol MIB, donde cada rama tiene un identificador y un número que es utilizado para construir un OID.

2.2.6.4.2 OID: identificador de objeto

Los OID’s son identificadores únicos que se utilizan en cada dispositivo gestionado. El valor devuelto por estos identificadores varía según la data requerida por el gestor SNMP. Se encuentran organizados de forma jerárquica en el árbol de la MIB (Base de Información de Administración). Por ejemplo, el OID para verificar el estado de la interfaz de un puerto de switch es: .1.3.6.1.2.1.2.2.1.8.1, siendo el último valor (.1) que representa el número de puerto en el switch y puede cambiar según la solicitud del gestor.

Figura 6

Diagrama del Árbol MIB



Nota: Identificar el mejor flujo para acceder al sysDescr (Jesús & Tejedor, 2006)

2.2.6.5 Alternativas de herramientas de monitoreo

Las herramientas de monitoreo permiten evaluar el uso de recursos, el estado de aplicaciones y servicios, así como el rendimiento de hardware y software. Además, ayudan a prevenir problemas futuros y a resolver los actuales. Estas herramientas, ya sean de código abierto o comerciales, ofrecen alertas, datos históricos y resúmenes para facilitar la gestión de sistemas y redes.

El sistema de monitoreo debe satisfacer principalmente los siguientes requerimientos:

- Del tipo Software libre.
- Ser escalable.

- Representación de datos, alarmas y gráficos para su estudio.
- Manejo de agentes de monitoreo y el protocolo SNMP.
- Mostrar la topología de red.
- Envío de notificaciones al correo electrónico.

Se seleccionó NAGIOS como instrumento de monitoreo porque fue el primer sistema de código abierto en llegar al mercado. Su núcleo sirve de base para desarrollar otros programas de monitoreo. Los sistemas CINGA, CENTREON, PANDORA o LIVESTATUS pueden integrarse o complementarse con NAGIOS para mejorar sus características, como interfaces web más completas y atractivas, y métodos de almacenamiento y procesamiento de datos. Al ser pionero entre los sistemas libres de supervisión y se encuentra con mayor tiempo en el mercado, ha desarrollado abundante documentación disponible sin limitarse sólo a su página oficial, sino también en NAGIOS CHILE o NAGIOS ESPAÑA que son las comunidades del NAGIOS. NAGIOS facilita la generación de informes, la creación de gráficos y el envío de notificaciones por correo electrónico. Utiliza el protocolo SNMP para recopilar información de los equipos en la red y agentes externos para monitorear equipos Windows o LINUX.

2.2.6.5.1 Nagios

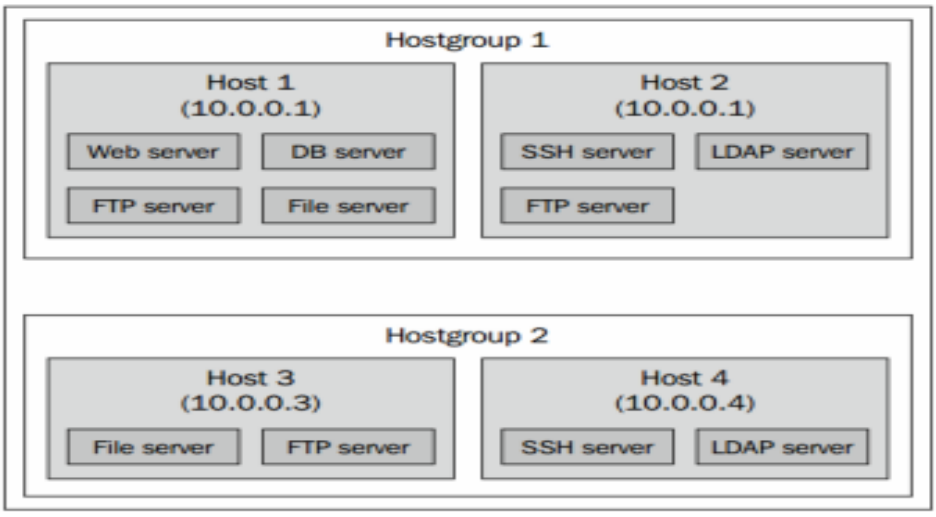
Nagios, es una herramienta de supervisión de red de código abierto. Licenciado bajo la GNU General Public License Version 2. Como instrumento de monitorización, valida que los hosts de la red funcionan como deberían. Nagios valida constantemente si los dispositivos funcionan

de forma correcta. Capaz de comprobar determinados servicios, en los diferentes equipos, están activos. Además, acepta los informes de estado de otros procesos o equipos, por ejemplo, un servidor web puede informar directamente a Nagios si no está sobrecargado (Barth, 2006).

La superstición realizada por el sistema en Nagios se organiza en dos categorías de objetos: hosts, grupos de host y servicios. Los hosts representan un dispositivo físico o virtual en la red como servidores, routers, estaciones de trabajo, impresoras, etc. Los servicios son funcionalidades específicas; por ejemplo, un servidor SSH (Secure Shell) puede definirse como un servicio de supervisión. Cada servicio está asociado con el host en el que se ejecuta. Además, los hosts pueden agruparse en grupos de hosts (hostgroups) como se muestra la Figura:

Figura 7

Diagrama de los grupos de Host.



Nota: Describe la división de host por grupos (Barth, 2006).

La Función principal del Nagios es verificar que el host que está siendo supervisado responda a las solicitudes para comprobar su estado. Si el comportamiento no sea el esperado, Nagios lo clasifica en cinco estados

para los hosts y servicios: ‘Up’ (activo), ‘Down’ (inactivo), ‘Warning’ (advertencia), ‘Flapping’ (inestable) y ‘Critical’ (crítico). Se tendrá la visualización de todos los servicios en colores, dependiendo del estado de alerta que se alerten.

Un ejemplo: además del tiempo de respuesta, un ping también devuelve la tasa de pérdida de paquetes. Para una conexión de red lenta (RDSI, ADSL), un tiempo de respuesta de 1000 milisegundos podría considerarse como un límite de advertencia y 5000 milisegundos como crítico, ya que eso significaría que el trabajo interactivo ya no sería posible. Si hay una alta carga en la conexión de red, también podría producirse una pérdida ocasional de paquetes, por lo que se puede especificar una pérdida del 20% como límite de advertencia, el 60 % como límite crítico. Lo siguiente se aplica en todos los casos: el administrador decide qué valores deben servir como señales de advertencia o considerarse como críticos. Dado que todos los servicios se pueden configurar individualmente, los valores para cada host pueden variar, incluso en el mismo complemento.

Los complementos siempre tienen un tiempo de espera, que suele ser de diez segundos. Esto evita que el programa espere indefinidamente, evitando así que se acumulen un gran número de procesos de complemento en el host Nagios. De otras formas también, un tiempo de respuesta superior a los 10 segundos tiene poco sentido para muchas aplicaciones, ya que estas interrumpen los intentos de conexión por sí mismas después de un determinado lapso, lo que tiene el mismo efecto que la falla total del servicio correspondiente. Aquí, el administrador también puede intervenir y especificar explícitamente un tiempo de espera diferente.

La siguiente **Tabla** muestra cómo los códigos de retorno del complemento se corresponden con los estados preliminares del host:

Tabla 3

Estados del monitoreo en Nagios.

ESTADO	RESULTADO DEL PLUGIN	ESTADO PRELIMINAR DEL HOST	DESCRIPCIÓN
0	**OK**	UP	Todo en orden, los servicios TIC en la última comprobación del estado
1	**WARNING**	UP o DOWN*	Estado Warning, en la última comprobación se ha registrado algún evento que requiere atención.
2	**UNKNOWN**	DOWN	Estado Desconocido, Se ha producido un error dentro del complemento en algún servicio.
3	**CRITICAL**	DOWN	Límite crítico excedido o el complemento ha interrumpido la prueba después de un tiempo de espera que se debe solucionar con urgencia.

La siguiente Tabla muestra cómo Nagios realiza una determinación del estado final en función del estado de los hosts principales. Los hosts principales se definen en la directiva de padres en la definición de host.

Tabla 4

Cambios en los estados del host.

ESTADO PRELIMINAR DEL HOST	ESTADO DEL HOST PRINCIPAL	ESTADO FINAL HOST
DOWN	Al menos uno del host padre esta en UP	DOWN
DOWN	Todos los hosts padres están o bien desactivados o inalcanzables.	UNREACHABLE

Nota: Diferencia entre los estados final del host (Nagios Core, 2016)

2.2.6.5.2 NagVis:

Nagvis es un complemento para Nagios que ofrece una visualización gráfica de todos los objetos de monitoreo, como hosts y servicios. Además, permite representar los datos recopilados por Nagios. Funciona mediante plantillas o mapas personalizables que ofrecen una vista completa de la infraestructura de red y sus servicios de un solo vistazo.

NagVis utiliza los datos proporcionados por el motor de Nagios para actualizar los objetos en los mapas en intervalos de tiempo, reflejando su estado actual. Estos mapas permiten organizar los objetos en diferentes diseños. Además, NagVis admite distintas plantillas para personalizar los mapas. Existen dos métodos para definir los mapas: uno manual y otro automático llamado “AutoMap”, que decide la posición de los objetos en función de la directiva “parents” en su definición.

Sus principales características son:

- Visualización de los hosts y servicios individuales
- Muestra un resumen del estado de un host y todos sus servicios
- Mostrar sólo los problemas reales
- La visualización completa de los procesos de TI usando gráficos auto dibujados.
- Configuración web de los mapas.

CAPÍTULO III

MATERIALES Y MÉTODOS

3.1 TIPO Y DISEÑO DE INVESTIGACIÓN.

Este trabajo de titulación permite analizar y conocer directamente la realidad de las características de los problemas de la sociedad, considerando la descripción del problema, los objetivos, la hipótesis y su fin, enmarcado con el tipo aplicada. Gracias a esta investigación se aplicará un conocimiento adquirido para transformar en conocimiento útil y con ello obtener un conocimiento con la aplicación a una problemática determinada en la realidad (Vargas Cordero, 2009); el diseño de la investigación es cuasi experimental porque permite establecer una relación causal entre una o más variables denominadas dependiente (Y) y otras variables independientes (X), en una situación estrictamente controlada sobre una muestra no probabilística. (Bulla & María, 2010).

- **Método**: Cuantitativo.
- **Tipo de investigación:** Aplicada.
- **Nivel de investigación:** Explicativo.
- **Diseño de investigación:** Cuasi- experimental.

3.2 POBLACIÓN Y MUESTRA

3.2.1 Población

Conformada por 568 entre host y servicios críticos susceptibles en alta disponibilidad llevados a cabo por la Oficina de Tecnologías de la información y Comunicación del Ministerio de Educación Lima, como se puede apreciar en la siguiente Tabla:

Tabla 5

Población de la investigación

ITEM	GRUPO	SERVICIOS Y DISPOSITIVOS EN RED	CANTIDAD
1	INFRAESTRUCTURA (Componentes y subcomponentes):	Servidores con sistema operativo Windows	159
		Servidores con sistema operativos Linux	177
		Servidores (file servers)	3
		Switch's (Cisco)	100
		Routers (Cisco)	16
		Dispositivos UPS	4
		Dispositivos biométricos	18
		Impresoras	2
2	ENLACES	Radioenlaces locales	7
		Enlace WAN con los proveedores de internet	8
3	SERVICIOS	Servicios corporativos gestionados (correo, intranet, etc.)	3
		Sistemas y servicios web internos y públicos.	128
		Total	**456**

Nota: Datos extraído de la base de datos de inventario de OTIC.

3.2.2 Muestra

Para la presente investigación, desarrollada en la Oficina de Tecnologías de la Información y Comunicación (OTIC) del Ministerio de Educación en Lima, Se utilizó un enfoque de muestreo no probabilístico para obtener la muestra, donde Hernández Sampieri y colaboradores (2014), explican que este tipo de muestras se eligen basándose en las particularidades de la investigación y no en criterios estadísticos. Por lo tanto, la selección de la muestra fue intencional y no aleatoria. se ha considerado los servicios TIC críticos; los equipos de comunicación y servicios web que brinda la OTIC.

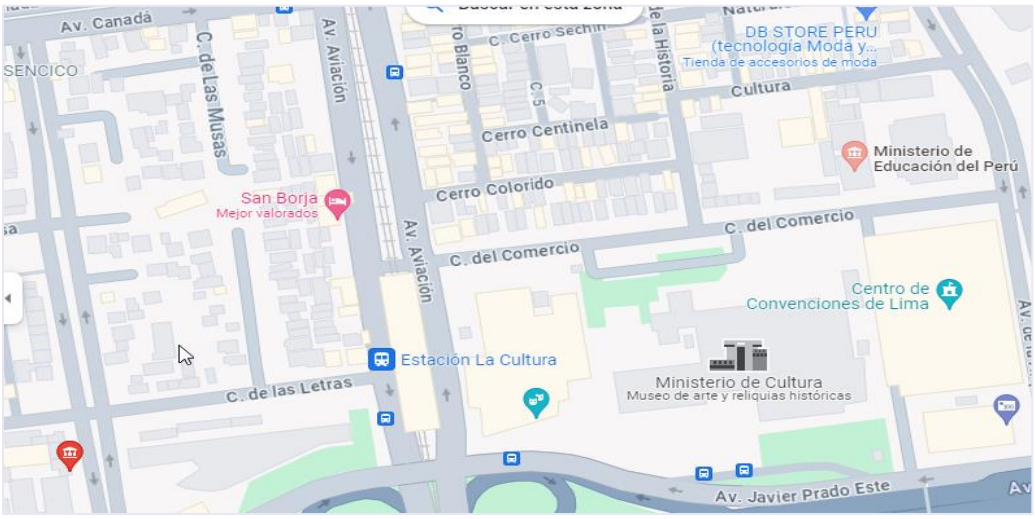
3.2.3 Ubicación y descripción de la población

El ámbito de estudio se ubica en las distintas áreas, Gerencias y Jefaturas pertenecientes al MINEDU y la ubicación de la oficina principal se detalla a continuación

- Departamento: Lima
- Provincia: Lima
- Distrito: San Borja
- Entidad: Ministerio de Educación (MINEDU)
- Dirección: Av. De la Poesía N°155

Figura 8

Ubicación geográfica del MINEDU.



Nota: Google Map de ubicación de la entidad donde se aplicó la mejora.

3.3 TÉCNICAS E INSTRUMENTOS

3.3.1 Técnicas e instrumentos para la recolección de datos

Para las actividades ejecutadas busca lograr los objetivos propuestos en esta investigación son:

- Planificación.

- Trabajo de campo (Oficina de Tecnologías de la Información y Comunicación)
- Recopilación de información
- Manejo de información, procesamiento y resultados finales.

Con el fin de ejecutar las tareas antes mencionadas de forma ordenada se aplicaron las siguientes técnicas y/o instrumentos:

Tabla 6

Técnicas e instrumentos

TÉCNICAS	JUSTIFICACIÓN	INSTRUMENTO
Revisión documental	Técnica utilizada para recopilar información con respecto a los servicios que atiende la OTIC, apuntes realizados a partir de reportes, informes y registros a fin de identificar las necesidades de la infraestructura y los servicios en la red que deben ser monitoreados, permitiendo visualizar las interacciones de las partes involucradas (áreas usuarias, proveedores y personal de la OTIC).	Diario o libreta de campo
Entrevista	Técnica que implicó la interrelación con las partes involucradas a los servicios que atiende la OTIC, para conocer la aplicación, implementación, satisfacción, entre otros, con respecto al modelo de monitoreo de los servicios de TIC.	Cuestionarios de preguntas estructuradas
Análisis documentario	Se utilizo esta técnica con la finalidad de conseguir los datos de las normas, directiva y procesos asociados con la disponibilidad de los servicios de TIC que son brindados por la OTIC, en el MINEDU.	Fichas bibliográficas
Observación directa	Se utilizo esta técnica que permitió la evaluación del sistema como parte del capítulo de la Evaluación de Resultados.	Ficha de observación

Nota: Muestra las diferencias entre los instrumentos de captura de información

3.3.2 Técnicas para el análisis de la información

Se analizaron y explicaron los resultados de la investigación, comparando el modelo con la ausencia de modelo en relación con la hipótesis y el marco teórico. A partir de esto, se obtuvieron las conclusiones correspondientes.

3.3.3 Técnicas para el procesamiento de datos

- **Diario o Libreta de Campo:** Es la herramienta utilizada para definir y guardar la recopilación de información obtenida a través de la técnica: Observación directa.

- **Cuestionario de preguntas estructuradas:** Es la herramienta utilizada para realizar las entrevistas a las partes involucradas: Personal de OTIC, gestores de los servicios.

- **Ficha bibliográfica:** Es la herramienta utilizada para recolectar datos de normativas legales, tesis, libros, manuales, reglamentos, directivas y sitios web relacionados con La implementación de un modelo de monitoreo aplicando ITIL 4 mejorará significativamente la disponibilidad de los servicios de TIC llevados a cabo por la Oficina de TIC del Ministerio de Educación - Lima.

3.4 PLAN DE TRATAMIENTO DE DATOS

El tratamiento de la información se ejecutó con el uso del programa estadístico SPSS, tomando en cuenta el siguiente procedimiento:

- La información estadística se calculó en el software estadístico SPSS 22.0 para Windows.

- La estadística descriptiva se utilizó para conocer la distribución de los datos alrededor de la media y permitió conocer su comportamiento como los de la población normal.
- Además, se usó la estadística inferencial, que permitió validar si los resultados de la muestra pueden ser generalizados y aplicados en la población.
- Se codificó y tabuló los datos.
- La presentación de los resultados se realizó en tablas y gráficas estadísticas.
- Se interpretó los resultados obtenidos de la media y desviación estándar.

3.4.1 Análisis de datos

A través del análisis y la explicación de los resultados de la investigación con modelo y sin modelo en comparación con la hipótesis de la investigación y el sustento teórico, con la finalidad de extraer las conclusiones respectivas.

3.5 APLICACIÓN DE LA METODOLOGÍA

3.5.1 Metodología en prototipo

La metodología en prototipo se considera la más adecuada para la presente investigación por las siguientes razones:

- **Enfoque práctico e iterativo**: Permite explorar ideas, obtener retroalimentación y desarrollar soluciones de manera gradual, ajustándose a las necesidades del proyecto.
- **Validación del modelo**: Se centra en la creación de prototipos iterativos para validar el modelo de monitoreo de servicios TIC, permitiendo una evaluación precisa de su funcionamiento y eficacia.

- **Enfoque centrado en el usuario**: Facilita la participación de los usuarios en el proceso de desarrollo, obteniendo retroalimentación valiosa para mejorar la usabilidad y la satisfacción con el modelo.
- **Reducción de riesgos**: Permite identificar y corregir errores en las primeras etapas del proyecto, minimizando el riesgo de fracaso en la implementación final.

Se espera que la aplicación de la metodología en prototipo contribuya a la exitosa validación del modelo de monitoreo de servicios de TIC.

3.5.2 Material experimental

Hardware

- Servidores
- switches
- UPS

Software

- Antivirus
- SPSS 20.
- Adobe Reader.
- Microsoft office
- Herramienta NAGIOS
- Herramienta Nagvis

Servicios

- Conexión a internet
- Consultoría

Materiales de oficina

- Impresora
- Computadora personal
- Folder Manila
- Plumón Acrílico
- Memoria USB

3.6 ASPECTOS ETICOS

Con la finalidad de contar con los criterios éticos se tomó consideró el código de ética de ingeniería permitiendo describir los siguientes puntos:

Con relación a la sociedad: Se implementaron proyectos innovadores que permitieron identificar el beneficio de la comunidad a través de investigaciones en el entorno. Por ello, esta investigación tendrá como beneficiario al MINEDU y al sector educativo a través de la disponibilidad de los servicios de TIC críticos.

Con relación al público: La información procesada expresados por los ingenieros son basadas en análisis de los informes objetivos y de la facilidad de comprensión. Por ello, se ha trabajado de esta forma a lo largo de esta investigación, considerando las referencias e información real de la entidad.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1 IDENTIFICAR Y ANALIZAR LA SITUACIÓN ACTUAL DE LOS SERVICIOS TIC MONITOREADOS Y NO MONITOREADOS APLICANDO ITIL 4 E IDENTIFICAR LOS INDICADORES DE DISPONIBILIDAD

Al identificar y evaluar mediante un análisis de la situación actual del Ministerio de Educación, enfrenta diversos desafíos en la gestión de sus servicios TIC soportados por herramientas de software y hardware, implicando la necesidad de contar con un modelo de monitoreo aplicando ITIL; considerando esta realidad, se ha identificado todos los servicios monitoreados y no monitoreados, clasificar los servicios por tipo, determinar los componentes de cada servicio. Este análisis permitió detectar las áreas de mejora y establecer un plan de acción para optimizar la gestión de las incidencias de los servicios TIC, el resultado de este análisis contraste con Purihuamán Venegas & Ramos, en su tesis titulada “Modelo de monitoreo para la identificación preventiva de incidencias y la ejecución de acciones correctivas en los servicios tecnológicos de las organizaciones”, implementó un modelo de monitoreo para el rendimiento de los servicios tecnológicos concluyendo la realización de un seguimiento y su identificación de tres incidentes que afectaron a los servicios del SAR ERP permitiendo identificar los intervalos de tiempos en que se presentaba cada evento, también, Axelos que publicó “ITIL 4” que resaltó la importancia de la gestión de servicios TIC, incluyendo la gestión de eventos, incidentes y problemas. La aplicación de ITIL 4 permite optimizar la disponibilidad de los servicios, mejorar la gestión de riesgos y la satisfacción del usuario final, en ese sentido Lauric en su publicación “Diseño e implementación de un sistema de monitoreo” propone

implementar herramientas de seguimiento porque ha permitido a un grupo de actores interesados en mantener en operación el servicio TIC informar y contribuir en la toma de decisiones. Para más detalle de las acciones para su implementación y resultados se describe a continuación lo siguiente:

4.1.1 Comprensión del contexto de la organización

Para lograr el primer objetivo específico de este trabajo de investigación, se llevó a cabo un diagnóstico exhaustivo. Este análisis permitió obtener un panorama inicial de los servicios de TIC ofrecidos por la Oficina de Tecnologías de la Información y Comunicación en el MINEDU. Este análisis permitió obtener la información necesaria para identificar y realizar las acciones de mejora.

Bajo este marco de referencia de ITIL 4, se consideraron los siguientes aspectos para la obtención de los indicadores:

a. La entidad:

Denominación

- Nombre: Ministerio de Educación.
- Siglas: MINEDU.
- Ubicación: Av. El Comercio 193. San Borja. Lima – Perú. El cual tiene 24 sedes adicionales en Lima Metropolitana.
- Condición: La Unidad de Servicio de Atención al Usuario de la OTIC, que a su vez depende de la SPE del MINEDU, brinda sus servicios técnicos a través de la Mesa de Servicios de la OTIC, así como la atención de documentos, y su jefatura se encuentra en la Sede La Poesía (“Excentromin”), ubicado en Av. de La Poesía N°155, San Borja.

El Ministerio de Educación es el organismo del poder Ejecutivo que ejerce la rectoría del sector Educación. Tiene competencia en materia de educación, deporte y recreación, y en las demás que se le asignen por ley. Es responsable de formular las políticas nacionales y sectoriales, en armonía con los planes de desarrollo y política general del Estado, así como de supervisar y evaluar su cumplimiento. Ejerce sus competencias a nivel nacional.

Su sede principal se encuentra ubicada Calle Del Comercio N°193 Lima - Lima - San Borja, en la cual se centraliza todas las actividades, sin embargo, para el alcance del presente modelo de monitoreo se considera las sedes que se ubican la periferia de la sede principal, que a continuación se mencionan:

- Sede Centromin (Av. de la Poesía N°111-155 Lima - Lima - San Borja - Perú).
- Sede Guardia Civil (Av. Guardia Civil N°115 Lima - Lima - San Borja - Perú)
- Sede Morelli (Calle Morelli N°109 Lima - Lima - San Borja - Perú)
- Sede Procuraduría (Av. Javier Prado N°1712 Lima - Lima - San Isidro – Perú).

b. Visión de la entidad

“Todos desarrollan su potencial desde la primera infancia, acceden al mundo letrado, resuelven problemas, practican valores y saben seguir aprendiendo, se asumen ciudadanos con derechos y responsabilidades y contribuyen al desarrollo de sus comunidades y del país combinando su capital cultural y natural con avances mundiales”.

c. Misión de la entidad

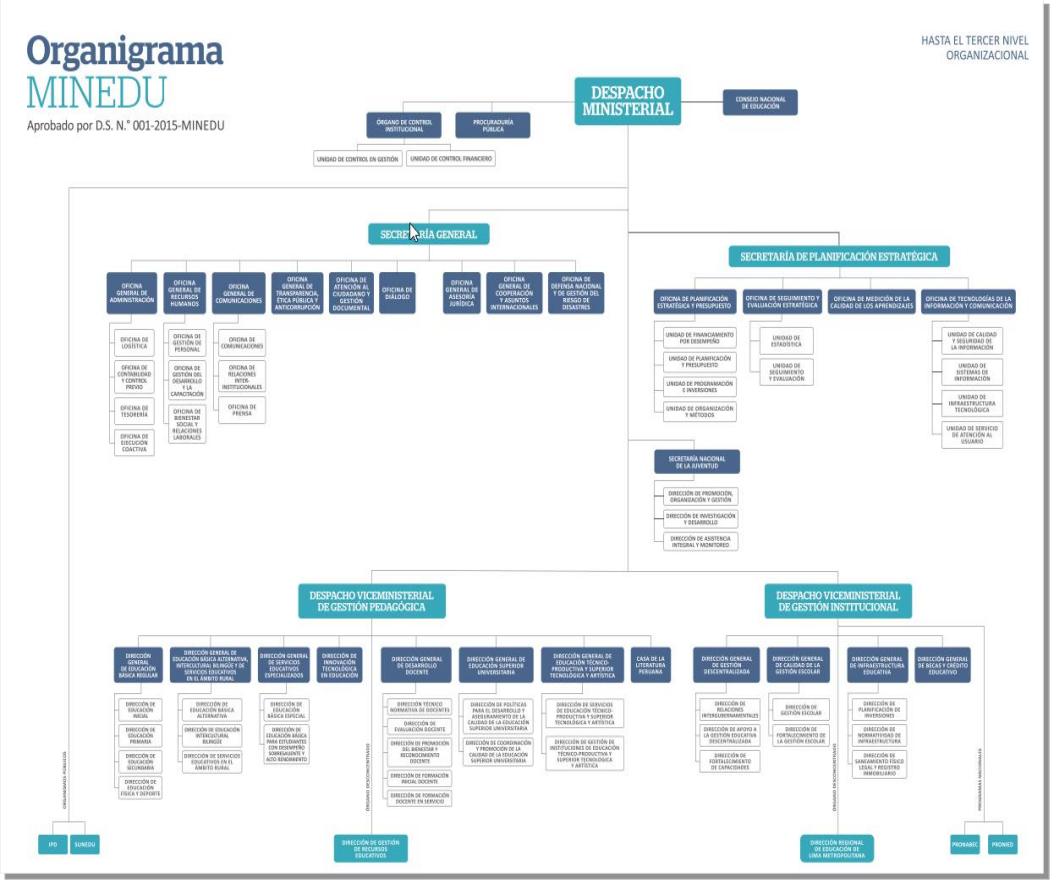
"Garantizar derechos, asegurar servicios educativos de calidad y promover oportunidades deportivas a la población para que todos puedan alcanzar su potencial y contribuir al desarrollo de manera descentralizada, democrática, transparente y en función a resultados desde enfoques de equidad e interculturalidad."

d. Estructura Organizacional

Según el Decreto Supremo N° 001-2015-MINEDU la Organización del Ministerio de Educación es la siguiente:

Figura 9

Organigrama del MINEDU.



Nota: ROF – DECRETO SUPREMO N°001 – 2015 - MINEDU(Ministerio de Educación, 2015)

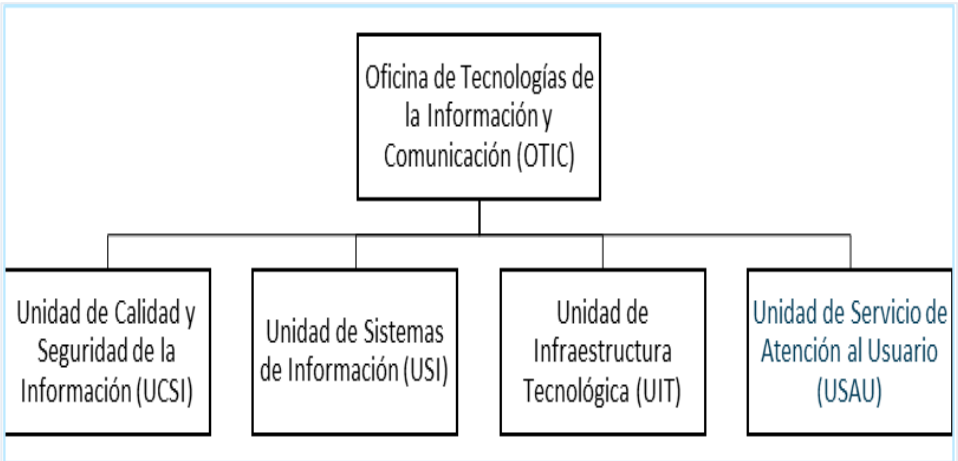
4.1.1.1 Funciones y responsabilidades

4.1.1.1.1 Organización y Funciones de la OTIC

La Oficina de Tecnologías de la Información y Comunicación dependiente de la Secretaría de Planificación Estratégica, cumple la función de proveedor de los servicios de tecnologías de la información y comunicación en el Ministerio de Educación de la República del Perú, esto en concordancia con lo establecido en el Reglamento de Organización y Funciones, aprobado mediante el Decreto Supremo N°001-2015-MINEDU, que en su artículo 45°, acápite d), precisa: "Asesorar y brindar asistencia técnica en los temas relacionados con las Tecnologías de la Información y Redes de Comunicación en el sector Educación, en coordinación con los órganos competentes". Así mismo la OTIC está conformada según se muestra en la figura N° 10, se organiza de la siguiente forma:

Figura 10

Organigrama de la OTIC.



Nota: OTIC – Matriz de Organización y Funciones - ROF – DECRETO SUPREMO N°001 – 2015 - MINEDU

- **Unidad de Calidad y Seguridad de la Información**

Es responsable de la seguridad, integridad, calidad y disponibilidad de la información del Ministerio. Depende de la Oficina de Tecnologías de la Información y Comunicación.

- **Unidad de Sistema de Información**

Es responsable de analizar, diseñar, programar, supervisar y brindar mantenimiento y soporte a los sistemas de información del Ministerio. Depende de la Oficina de Tecnologías de la Información y Comunicación.

- **Unidad de Infraestructura Tecnológica**

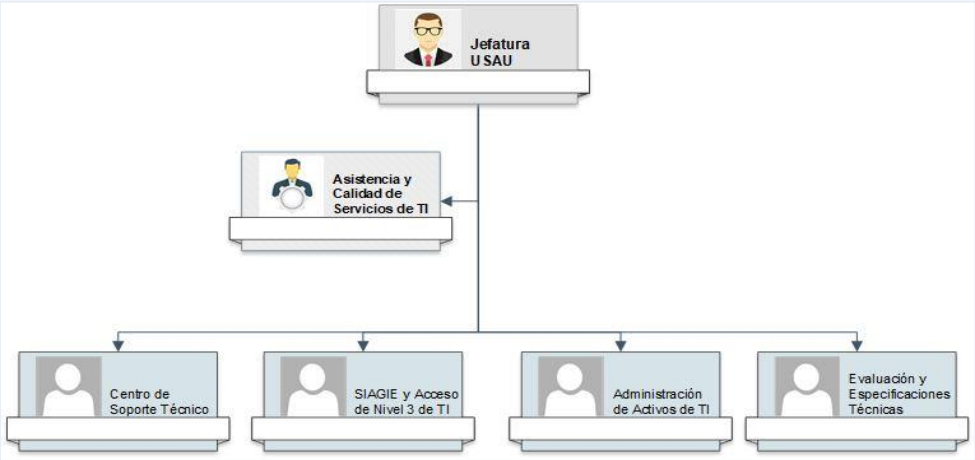
Es responsable de diseñar, implementar y administrar la infraestructura tecnológica del Ministerio. Depende de la Oficina de Tecnologías de la Información y Comunicación.

- **Unidad de Servicio de Atención al Usuario**

Es responsable del diseño e implementación de los procesos, procedimientos y métricas para la atención oportuna y asistencia técnica a los usuarios de los servicios informáticos del Ministerio. Depende de la Oficina de Tecnologías de la Información y Comunicación. Con la finalidad de atender a su responsabilidad, la Unidad de Servicio de Atención al Usuario, se ha organizado de la siguiente forma:

Figura 11

Organigrama de la USAU.



Nota: OTIC – Matriz de Organización y Funciones – ROF.

Funciones de la USAU: De acuerdo con el artículo 54 del Decreto Supremo N° 001-2015-MINEDU que aprueba el Reglamento de Organización y Funciones del Ministerio de Educación, la USAU tiene las siguientes funciones:

Elaborar e implementar los procedimientos, métricas y flujos de trabajo necesarios para ofrecer una atención eficiente y oportuna a los usuarios de los servicios informáticos del Ministerio. Además, garantizar el uso adecuado de las herramientas y equipos informáticos, así como brindar soporte técnico en sistemas operativos, software base, aplicaciones y comunicaciones a las diferentes unidades del Ministerio.

4.1.1.2 Identificación de los procesos en la OTIC

Con el objetivo de identificar los procesos actuales según el marco de ITIL 4, se realiza un análisis centrado en la FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) de la Oficina Técnica de Informática y Comunicaciones. Este análisis es fundamental para

comprender la situación actual del Ministerio de Educación, como se detalla en la siguiente Tabla:

Tabla 7

Matriz FODA de la OTIC.

	FACTORES INTERNOS	
	FORTALEZAS (+)	**DEBILIDADES (–)**
1	Contar con lineamientos de estándares de Seguridad de información (NTP/ISO 27001) y del Ciclo de Vida de Software desarrollados (NTP/ISO 12207).	Vulnerabilidad del Centro de Datos: No cuenta con plan de contingencia, infraestructura física dañada (en proceso de planeamiento para reconstrucción y mudanza).
2	Contar con un comité de Seguridad de la Información.	El Centro de Datos no es híbrido (On premise y Cloud).
3	Contar con un oficial de protección de datos personales.	Aún no se cuenta con una total integración de los sistemas de información.
4	Infraestructura de comunicaciones implementada en el Minedu para el Sector Educación.	Diversidad de plataformas de desarrollo que demandan personal de diferentes especialidades, lo que dificulta optimizar recursos y la evolución de conocimientos.
5	Adecuado servicio de administración de Hosting, instalación y/o configuración de hardware y software, gestión de servicios de TI, supervisión de las adquisiciones de recursos TIC, entre otros.	Aún existen procesos y/o procedimientos de soporte no registrados por parte de las unidades de la OTIC.
6	Centro de Datos con adecuada capacidad de procesamiento que atiende la demanda de los servicios.	Aún no se cuenta con procesos y herramientas de gestión aprobados (Eventos, Cambios, Problemas, etc)
8	Contar con aplicaciones propias de la Entidad.	No se cuenta con un proceso de la continuidad de negocio implementado.
9	Contar con una Mesa de Servicios de tecnologías de la información y comunicación con la capacidad mínima aceptable, que permite brindar atención de calidad 24x7 presencial y remota.	Aún no se cuenta con procesos implementados de gestión de la Demanda y de la Capacidad.
10	Contar con un Catálogo de Servicios de tecnologías de la información y Comunicación.	Portafolio de servicios TIC no estructurado ni priorizado.

FACTORES EXTERNOS		
	OPORTUNIDADES (+)	**AMENAZAS (–)**
1	Impulso del Estado al desarrollo de la "sociedad de la información" y la "sociedad del conocimiento"	Inestabilidad política en el país ante un posible cambio de representantes del Ejecutivo y Legislativo.
2	Rápida evolución de la tecnología y consolidación de estas para optimización de recursos y posibilidades de brindar nuevos servicios.	Procedimientos logísticos engorrosos y rigidez de la Ley de Contrataciones con el Estado.
3	Mayor prioridad otorgada en el Presupuesto Nacional para el Sector Educación.	Demanda de información no programada por parte de entidades públicas y privadas (casos urgentes, casos especiales, demandas de instituciones externas).
4	Rol estratégico asignado por el Minedu a las tecnologías de la información mediante unidades orgánicas dependientes de la Secretaría de Planificación Estratégica y del Viceministerio de Gestión Institucional.	Posición radical de algunas regiones referente a la Descentralización; negativa a facilitar información del Sector.
5	Aplicación de TIC en la gestión de instituciones educativas privadas; como modelos de referencia para el sector público.	Presencia permanente de hackers que intentan vulnerar los recursos TIC.
6	Existen planes con desarrollo tecnológico en beneficio de la comunidad estudiantil	Alta rotación del personal en las regiones que dificulta la coordinación del sector.
7	Existe un reglamento para la creación del sistema de Transformación Digital, basado en la política de Estado del Acuerdo Nacional N° 35 “Sociedad de la Información y Sociedad del Conocimiento” que fomenta la modernización del Estado mediante el uso de las Tecnologías de la Información y las Comunicaciones (TIC). DS N° 157-2021-PCM	Incremento de licencias de descanso por motivos de salud que impacte en la capacidad de atención de los servicios institucionales.
8	Contar con un procedimiento PE03.03.02 denominado "Gestionar Riesgos Organizacionales" aprobado por RSG N° 188-2020-MINEDU	Manifestación de un rebrote de la pandemia Covid-19 que conlleve a la implementación de restricciones que impacten en el cumplimiento de los proyectos en curso.
9	Contar con un presupuesto aprobado para la implementación de la NTP ISO20000	Presencia de conflictos sociales que retrasan los cumplimientos a nivel Estado.

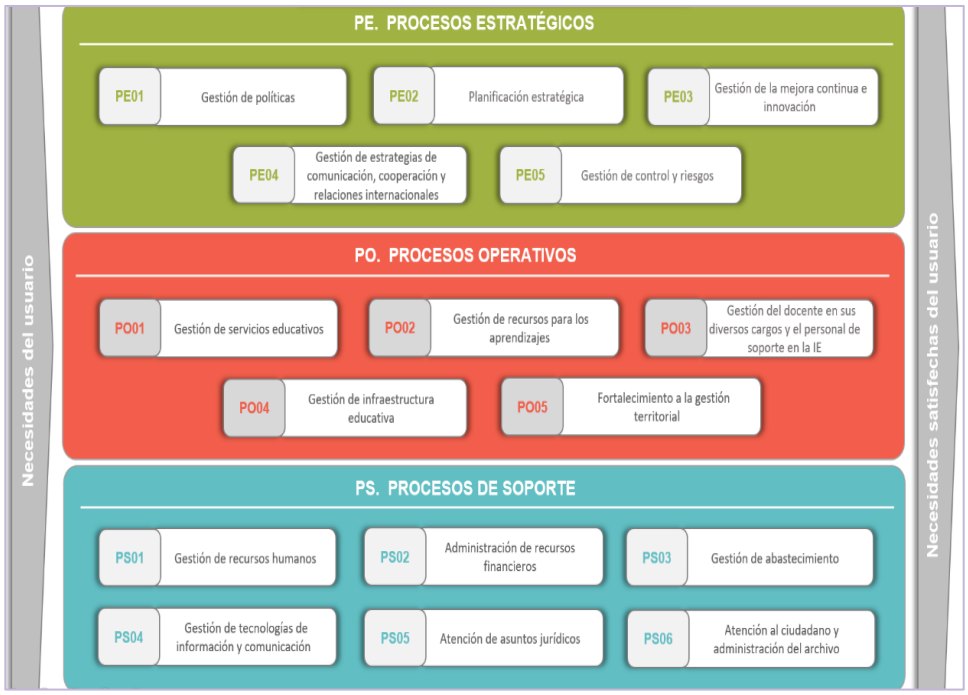
Nota: Repositorio de OTIC (OTIC, 2022)

4.1.1.3 Mapa de Procesos y Procedimientos identificados

Aprobado con el artículo 1 de la Resolución de Secretaría General N° 075-2021-MINEDU el 07 de mayo de 2021, la cual se detalla en la figura N° 12 del mapa de nivel 0 que el proceso de Gestión de Tecnologías de Información y Comunicación de código PS04 está vinculada a las actividades realizadas por esta unidad, así como en la figura N° 13 del mapa de nivel 1 se especifica que las actividades realizadas en su mayor parte están involucradas con el proceso Gestión de Servicios de Tecnologías de Información y Comunicación de código PS04.03.

Figura 12

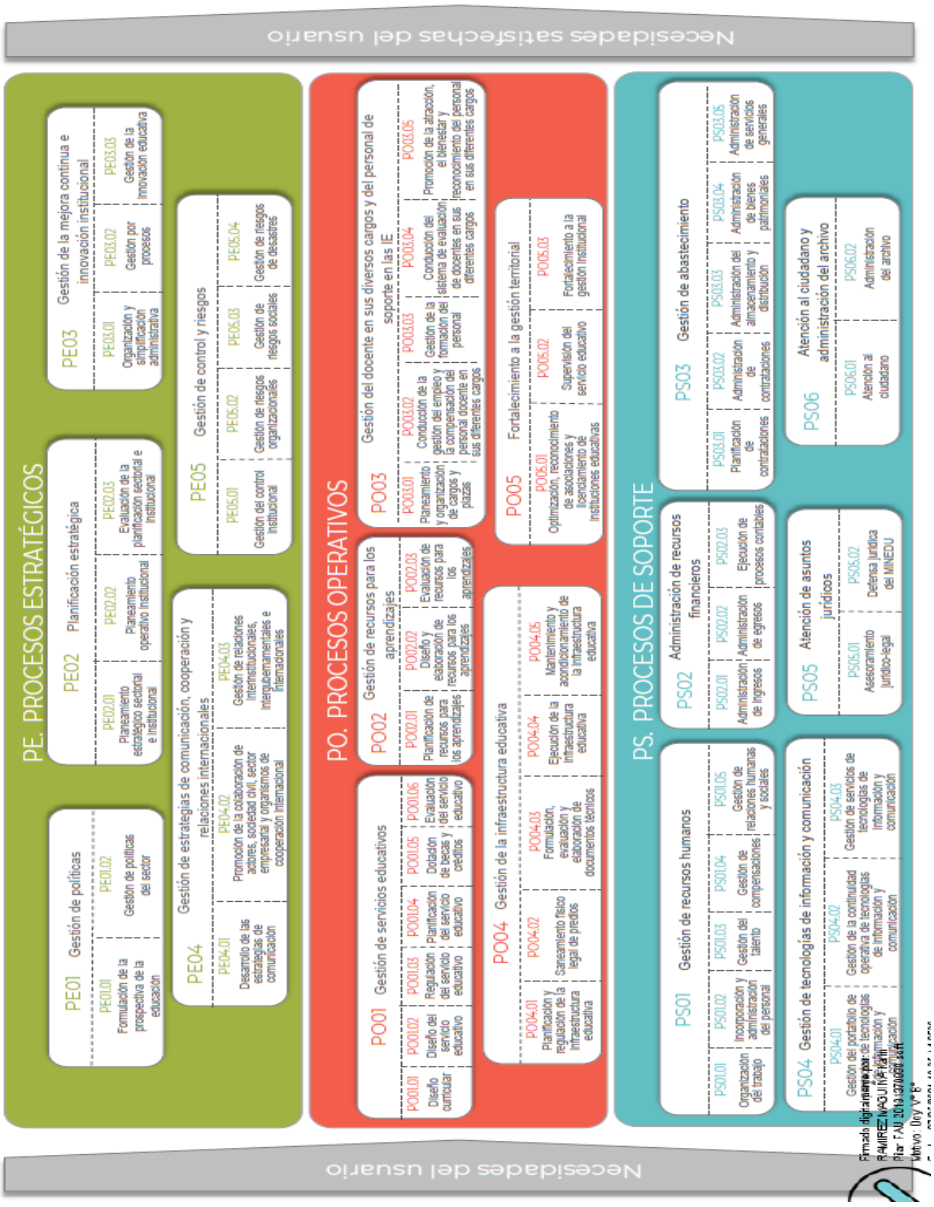
*Mapa de Procesos del Ministerio de Educación – Nivel 0***.**



Nota: Pág. 4 de la Resolución de Secretaría General N° 075-2021-MINEDU.

Figura 13

Mapa de Procesos del Ministerio de Educación – Nivel 1



Nota: Pág. 5 de la Resolución de Secretaría General N° 075-2021-MINEDU. (Ministerio de Educación, 2021).

Asimismo, en la ficha de proceso correspondiente al código PS04, adjunta a la Resolución de Secretaría General N° 075-2021-MINEDU detalla que en los elementos de entrada corresponde a los “Requerimientos de atenciones de los usuarios de hardware, software, configuración, etc.”

En ese sentido, mediante la Resolución de Secretaría General N° 006-2022-MINEDU se aprueba en su artículo 1 el procedimiento de nivel 2 denominado "*Gestionar los incidentes de tecnologías de la información y comunicación*" de código PS04.03.01 en su versión 01, la cual está vinculada al proceso de nivel 1 de código PS04.03.

De la revisión del contexto organizacional y los procesos aprobadas, se ha identificado una deficiencia crítica en la supervisión y monitoreo de los servicios web y equipos de comunicaciones esenciales. Esta falta de control compromete ejecución de la misión y visión de la organización, ya que prolonga el tiempo de detección de incidencias y afecta la gestión eficiente de las mismas. Para subsanar esta situación, se propone la implementación de una estrategia de monitoreo integral de los servicios críticos de la entidad. Esta estrategia tiene como objetivo principal reducir el tiempo de detección de incidencias y, en consecuencia, mejorar el nivel de disponibilidad de los servicios de TIC

En concordancia a la entrevista con el jefe de la USAU y los especialistas de TI, se discutió sobre la carencia de la monitorización en las estrategias de la oficina, y como resultado de esta entrevista se llegó a determinar la siguiente estrategia:

Monitorear, analizar y gestionar las incidencias que degraden los servicios de TIC.

4.1.1.3.1 Flujo de actividades del proceso PS04.03.01

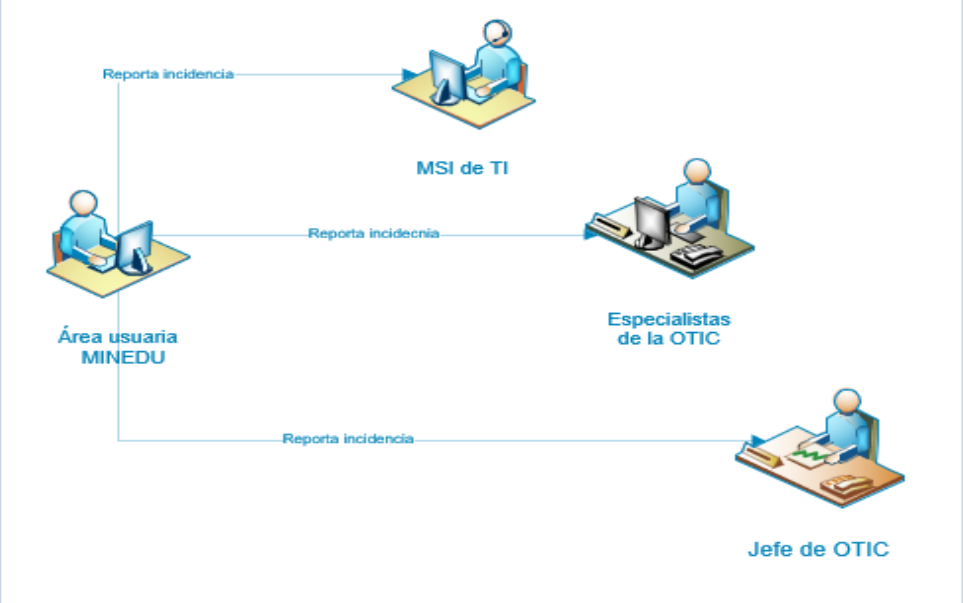
Dentro del marco de ITIL 4, la gestión de incidencias se define como el proceso de minimizar el impacto negativo de los incidentes

restaurando la operatividad normal del servicio de forma rápida. Esta gestión juega un papel crucial en la satisfacción del usuario, la disponibilidad de los servicios de TIC y la percepción que los usuarios tienen del proveedor de servicios. Se convierte en una herramienta esencial para que el proveedor cumpla con las expectativas y agregue valor.

A continuación, la Figura N° 14 presenta el flujo de tratamiento de incidencias en el ámbito de las tecnologías de la información y comunicaciones.

Figura 14

Flujo de atención a las incidencias en OTIC.



Nota: Señala el camino de la atención.

Lo mostrado en la figura N° 14, se ha identificado las siguientes problemáticas:

La gestión de incidencias en la OTIC se caracteriza por una variedad de canales de atención, incluyendo contacto directo, llamadas telefónicas y correos electrónicos, siendo la plataforma de mesa de servicios el último recurso. Esta diversidad en la recepción de reportes

refleja una cultura de atención al usuario, pero también presenta un desafío en la centralización y gestión de la información.

Además, la posibilidad de que cualquier miembro del personal, desde el jefe hasta el analista de soporte, recibe las incidencias, podría generar ineficiencias y falta de uniformidad en el proceso de resolución.

Otra situación, se identificó que el escalamiento de la incidencia se pierda en el flujo de la atención.

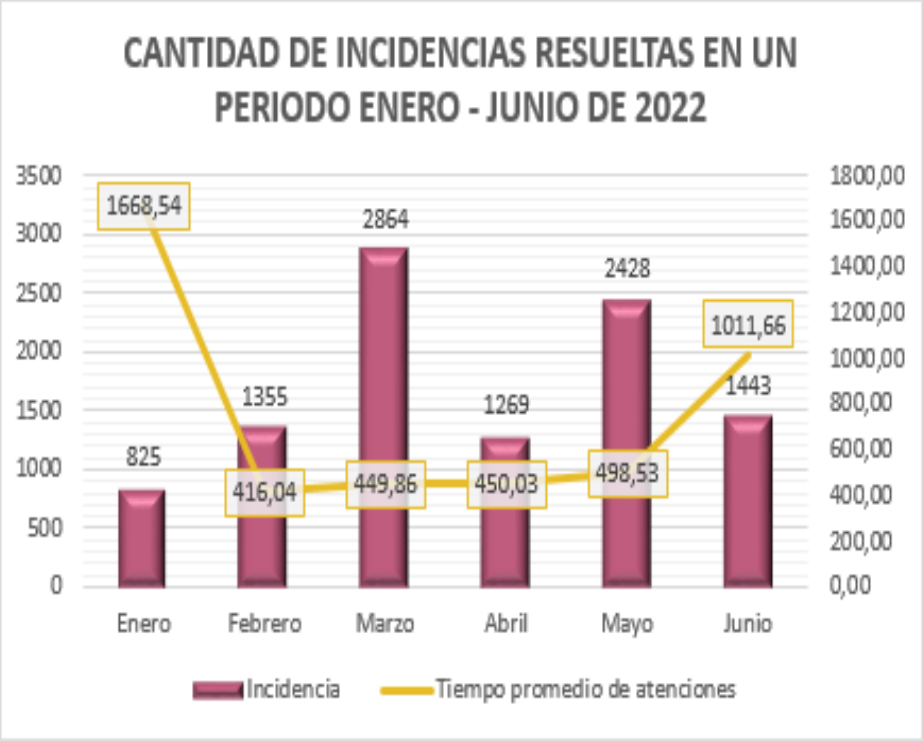
El trabajo de investigación aplicó la "gestión de incidencias, gestión de problemas y monitoreos 24/7 como un marco de referencia único integrado para un modelo de monitoreo alineado a ITIL 4. Con el objetivo de mejorar la disponibilidad de los servicios de TIC, fortalecer la habilidad de la organización y agregar valor. El enfoque consistió en documentar y compartir el proceso existente, así como aplicar lo aprendido.

4.1.1.4 Diagnóstico y análisis inicial

El diagnóstico inicial incluyó un análisis de las incidencias registradas durante un período de seis meses, desde el 01 de enero hasta el 30 de junio de 2022. Se tomaron en cuenta las incidencias reportadas a través de correos electrónicos, peticiones presenciales y registros de la mesa de servicios de TI. La Figura N° 15 muestra un resumen de los datos recopilados.

Figura 15

Gráfica Estadística del Reporte de incidencias registradas.



Nota: Base de datos de la mesa de servicios de OTIC.

Los resultados extraídos de la Figura N° 15 revelan una notable frecuencia de incidencias, destacándose en el mes de marzo, con un total de 2864 incidencias reportadas. El tiempo promedio de resolución de estas incidencias se sitúa en 749 minutos, equivalente a alrededor de 12 horas y 48 minutos desde que se reporta el caso a la Mesa de Servicios de TI. Esta demora impacta negativamente en el restablecimiento del servicio para el usuario final.

Durante el período evaluado, se registró un tiempo de resolución de incidencias significativamente más largo en el mes de mayo, alcanzando las 62 horas, 28 minutos y 45 segundos. Las entrevistas con el personal de la OTIC revelaron que la falta de claridad en las responsabilidades, los acuerdo Los resultados extraídos de la Figura N° 15 revelan una notable frecuencia de incidencias, destacándose en el mes de marzo, con un total de 2864

incidencias reportadas. El tiempo promedio de resolución de estas incidencias se sitúa en 749 minutos, equivalente a alrededor de 12 horas y 48 minutos desde que se reporta el caso a la Mesa de Servicios de TI. Esta demora impacta negativamente en el restablecimiento del servicio para el usuario final.

El análisis del periodo evaluado reveló un tiempo de resolución de incidencias significativamente prolongado durante el mes de mayo, alcanzando las 62 horas, 28 minutos y 45 segundos. Las entrevistas con el personal de la OTIC identificaron como factores contribuyentes a esta demora la falta de claridad en la asignación de responsabilidades, la ausencia de acuerdos de nivel de servicio (SLA) formalizados y la carencia de procesos establecidos. Esta situación evidencia una gestión de servicios deficiente, lo que impacta negativamente en la disponibilidad de los servicios de TIC.

4.1.1.5 Determinar los elementos más relevantes de ITIL 4 aplicables a la OTIC

Al analizar el marco de referencia de ITIL 4, se observa que su aplicación es a nivel empresarial. Sin embargo, en esta investigación no se buscó construir un modelo de negocio empresarial de ITIL 4. En cambio, se aplicaron parcialmente los principios para determinar los indicadores de monitoreo de servicios de TIC. Esto implicó adaptar la técnica, siguiendo específicamente los pasos relevantes para definir los indicadores del modelo.

- **Operación del Servicio:**
  - Gestión de incidencias
  - Gestión de problemas

- Monitorear, administrar y mantener los servicios de TI en operatividad.
- Garantizar que los servicios de TI estén disponibles y funcionando correctamente.

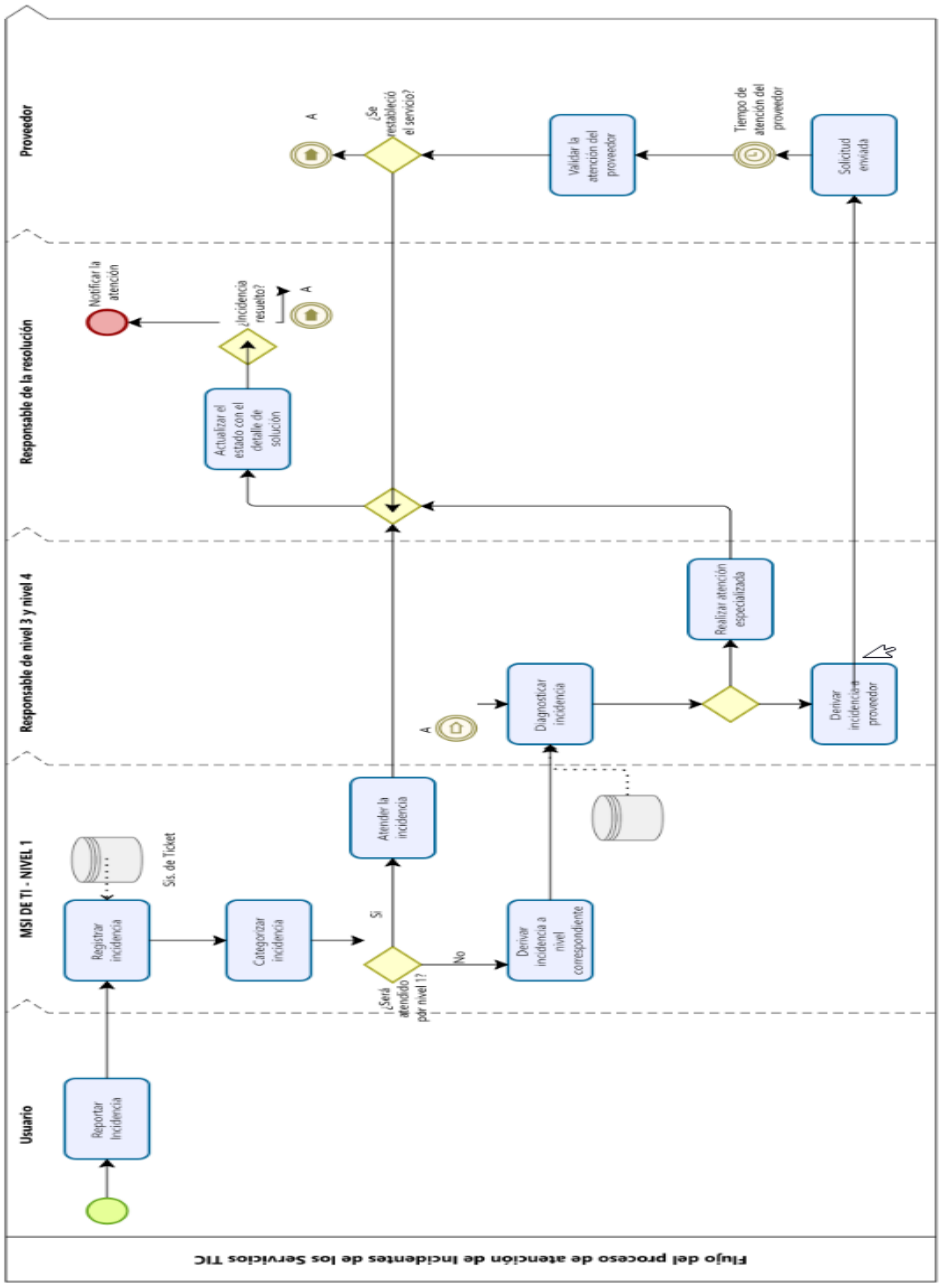
4.1.2 Desarrollo de la propuesta del modelo de monitoreo de la disponibilidad de los servicios de TIC, aplicando la adaptación de ITIL 4.

La implementación del modelo se fundamenta en los principios de ITIL 4, realizando un análisis exhaustivo de la situación actual de los servicios de TIC. Se evaluaron métricas como el tiempo de atención y el tiempo promedio de resolución de las incidencias reportadas, identificadas a partir del análisis inicial presentado en la Figura N° 14.

Con base en este diagnóstico, se propuso un flujo de procesos optimizado, alineado con los principios de ITIL 4, y se diseñó un modelo de atención por niveles. Este modelo establece un punto de contacto centralizado entre el usuario, el sistema de mesa de servicio y el sistema de monitoreo. La Figura N° 16 ilustra el flujo de procesos resultante de este análisis.

Figura 16

Flujo de la gestión de incidencias.



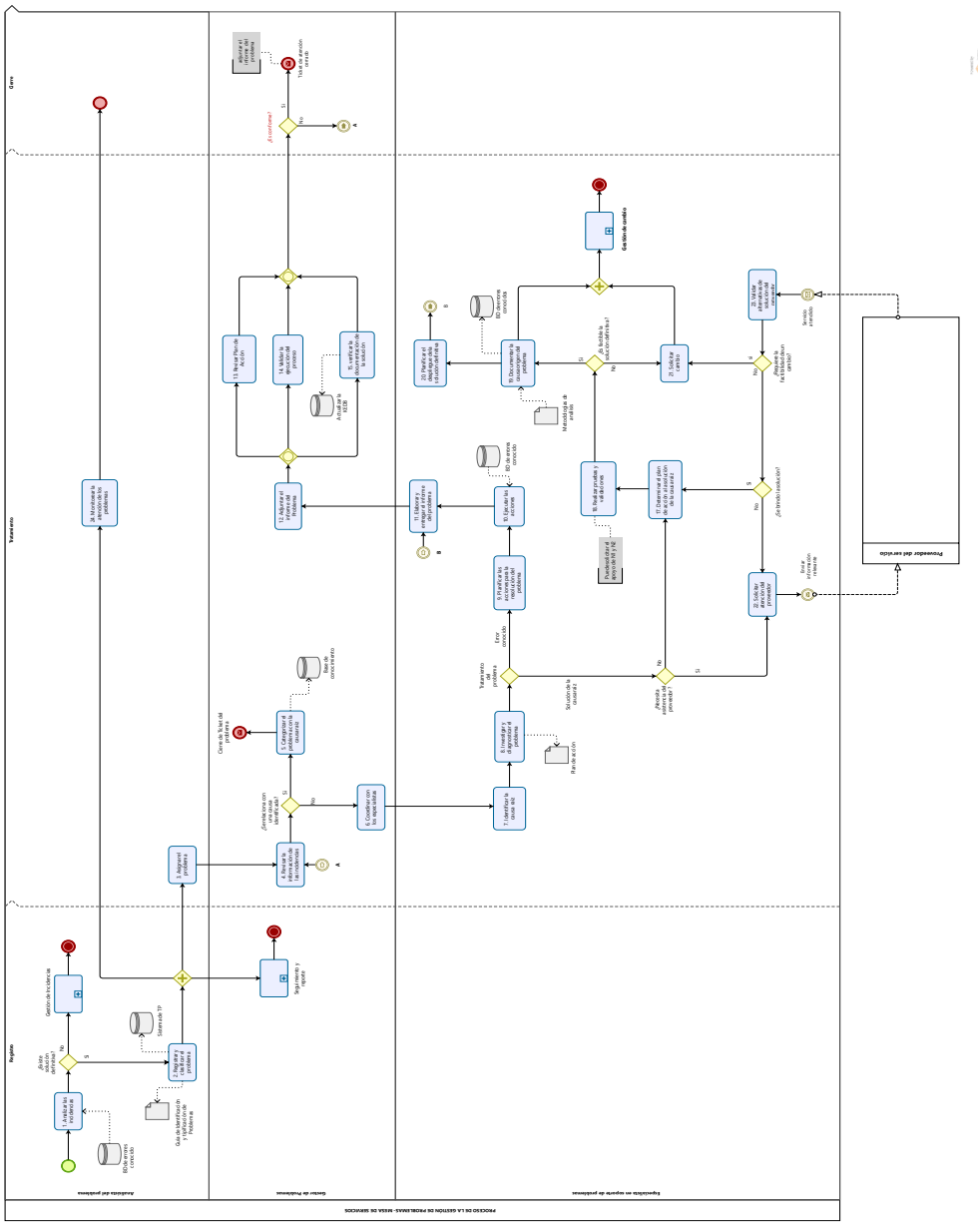
Nota: Muestra el flujo de cada actividad a realizar para completar la atención de una incidencia.

Como parte de las operaciones de servicio TIC, se identificó la ausencia de un proceso formal para la gestión de problemas. En respuesta a esta necesidad, se diseñó un flujo de proceso específico para el tratamiento de problemas, alineado con las mejores prácticas de ITIL 4. Este flujo, que se detalla en la siguiente figura,

busca garantizar una gestión eficiente y eficaz de los problemas que puedan surgir en los servicios de TIC.

Figura 17

Flujo de la gestión de problemas



Nota: Muestra el flujo de cada actividad a realizar para completar la atención de unos problemas.

El flujo de la gestión de problemas en los servicios TIC del Ministerio de Educación implica identificar problemas mediante análisis de datos y tendencias, analizar las causas raíz y determinar acciones para prevenir su recurrencia. Para un tratamiento adecuado de los problemas de los servicios TIC, se deben seguir

criterios como obtener una muestra representativa mensual de incidencias, establecer un plan de acción, desarrollar procedimientos y utilizar herramientas como el Análisis de Pareto o el diagrama Ishikawa. Además, de informar al responsable de gestionar la base de conocimiento sobre las soluciones identificadas y se categorizan los problemas para vincular las incidencias relacionadas.

4.1.2.1 Determinación de los indicadores

De los aspectos analizados, se vio con la necesidad establecer como objetivos estratégicos en la monitorización de los servicios de TIC lo siguiente:

- Monitorear los equipos de comunicación y servicios web.
- Monitorear la seguridad en los servicios web
- Monitorear la disponibilidad de los equipos de comunicación, servidores, servicios web y puntos de acceso,
- Monitorear la conectividad de los equipos de comunicación.

Tabla 8

Indicadores obtenidos según los objetivos.

OBJETIVO ESTRATÉGICO	INDICADORES
Monitorear los servicios de TIC.	Estado del servicio Tiempo de notificaciones de eventos del servicio de TIC.
Monitorear la seguridad de los servicios web	Tiempo de interrupción de los servicios de TIC monitoreado
Monitorear la disponibilidad de los equipos de comunicación y servicios web	Nivel de disponibilidad de los servicios de TIC en la red
Monitorear la conectividad de los equipos de comunicación.	Tiempo de resolución de eventos e incidencias.

Nota: Asociación entre objetivos e indicadores

Así mismo se determinó los parámetros para cada uno de los indicadores, detallados en la Tabla N° 9:

Tabla 9

Parámetros de los indicadores establecidos.

INDICADORES	PARÁMETROS
Estado del servicio	Estado: Funcionamiento Correcto. Error en los servicios
Tiempo de notificaciones de eventos del servicio de TIC.	Tiempo en segundos.
Tiempo de interrupción de los servicios de TIC monitoreado	Tiempo en minutos
Nivel de disponibilidad de los servicios de TIC en la red	Para los estados se utilizan: - Funcionamiento Correcto. - Alerta.
Tiempo de resolución de eventos e incidencias.	Tiempo en minutos

Nota: Relación entre indicadores y lo parámetros establecidos

4.2 IMPLEMENTAR EL MODELO DE MONITOREO APLICANDO ITIL 4 PARA LA DETECCIÓN DE LA DEGRADACIÓN O INTERRUPCIÓN DE LOS SERVICIOS TIC

4.2.1 Selección de la plataforma de monitoreo.

El panorama actual existe una amplia gama de herramientas para monitorear y supervisar las redes. Tanto las soluciones propietarias como las de código abierto se encuentran disponibles en el mercado. Cada herramienta posee características y funcionalidades específicas, por lo que es crucial evaluarlas a fondo para determinar cuál se adapta mejor a las necesidades de la organización.

Los requerimientos y el nivel de impacto se han definido en función de las necesidades de la OTIC. La criticidad de la infraestructura y los servicios de TIC es fundamental, y los requerimientos con un nivel de impacto "Alto" son esenciales para garantizar la disponibilidad de los servicios. La herramienta seleccionada debe cumplir con estos requisitos y ofrecer un monitoreo efectivo. Como se presenta en la Tabla **N°** 10 resume los requisitos principales:

Tabla 10

Nivel de impacto de los requisitos de la solución

REQUERIMIENTO	IMPACTO	VALOR MÍNIMO	VALOR MÁXIMO
El sistema operativo debe ser de código abierto.	ALTO	0	5
Monitoreo en tiempo real de la infraestructura de red.	ALTO	0	5
Monitoreo en tiempo real de los servicios web críticos	ALTO	0	5
Generación de Reportes y Estadísticas	ALTO	0	5
Enviar notificaciones por correo electrónico.	ALTO	0	5
Representación gráfica de datos.	MEDIO	0	3
Utilización del protocolo SNMP	MEDIO	0	3
Variedad de agentes	MEDIO	0	3
Variedad de plugins	MEDIO	0	3
Autodescubrimiento de la red.	MEDIO	0	3
Soporte y documentación	BAJO	0	2
Actualizaciones continuas de la herramienta.	BAJO	0	2
TOTAL		**0**	**44**

Nota: Resultados del nivel de impacto

4.2.1.1 Evaluar y comparar herramientas de monitoreo

En el siguiente cuadro comparativo, se detallan las herramientas de monitoreo y supervisión.

Tabla 11

Evaluación y comparación de herramientas de monitoreo

DESCRIPCIÓN	CACTI	COLLECTD	ICINGA	FRENATS	NAGIOS	PRTG	ZABBIX
El sistema operativo debe ser de código abierto.	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)	NO (0)	SI (5)
Monitoreo en tiempo real de la infraestructura de red.	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)
Monitoreo en tiempo real de los servicios web críticos	SI (5)	NO (0)	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)
Generación de Reportes y Estadísticas	SI (5)	NO (0)	SI (5)	NO (0)	SI (5)	SI (5)	SI (5)
Envío de notificaciones por correo electrónico	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)	SI (5)
Representación de gráficas de datos.	SI (2)	NO (0)	SI (2)	NO (0)	SI (2)	SI (3)	SI (3)
Utilización del SNMP	SI (3)	NO (0)	SI (3)	NO (0)	SI (3)	SI (3)	SI (3)
Variedad de agentes	SI (2)	SI (2)	SI (3)	NO (0)	SI (3)	SI (3)	SI (3)
Variedad de plugins	SI (2)	SI (2)	SI (3)	SI (3)	SI (3)	SI (3)	SI (3)
Auto-descubrimiento de la red.	NO (0)	SI (3)	SI (3)	SI (3)	SI (3)	SI (3)	SI (3)
Soporte y documentación	SI (2)	NO (0)	NO (0)	SI (2)	SI (2)	SI (2)	SI (2)
Actualizaciones continuas de la herramienta.	SI (1)	SI (1)	SI (2)	SI (1)	SI (2)	SI (2)	SI (2)
PUNTAJE TOTAL	30	23	40	29	43	36	36

Nota: Resultados de la evaluación

4.2.2 Diseño e implementación de la herramienta para el monitoreo

Tras una exhaustiva investigación, comparación y evaluación de las principales herramientas de monitoreo, y tomando en cuenta la información detallada en la Tabla N° 11, se decidió elegir Nagios y su complemento visual Nagvis. Estas herramientas son adaptables a las buenas prácticas de ITIL 4 y, al ser software libre, pueden adaptarse a la configuración según las necesidades, cumpliendo con la mayoría de los requisitos proporcionados por la OTIC.

Entre sus principales características tenemos:

- Es una plataforma respaldada por la Licencia Pública General de GNU (GPL), lo que permite la ejecución, copia, distribución, estudio, modificación y mejora del código fuente.
- Ofrece supervisión de servicios de red como SMTP, POP3, HTTP, NTP, PING, entre otros.
- Realiza seguimiento de los recursos del servidor, como la carga del procesador y el uso del disco.
- Dispone de una amplia gama de plugins en constante actualización, lo que garantiza la mejora continua de la herramienta y la corrección de posibles fallos. Esto posibilita el monitoreo de diversos dispositivos en red, como UPS, teléfonos IP, cámaras IP e impresoras.
- Proporciona soporte técnico, documentación detallada y acceso a comunidades y foros especializados.
- Utiliza protocolos de red confiables, lo que asegura la integridad de la información. Asimismo, ha sido reconocida por otras organizaciones por su eficacia y funcionalidad. EL último reconocimiento se dio el 19

de diciembre de 2016 considerado Nagios Core como el "Proyecto del Mes" por la comunidad Source Forge.(Nagios Core, 2016).

4.2.3 Requerimientos del sistema

El equipo de Nagios Enterprise, creadores de Nagios Core, proporciona una guía que incluye los requisitos de hardware y software, los tipos de equipos y servicios que pueden monitorearse, el navegador recomendado y el sistema operativo que debe usarse en el equipo cliente. Para este proyecto, se seleccionó GNU/Linux Centos 7 como sistema operativo.

Tabla 12

Requerimientos del sistema

REQUERIMIENTOS DE HARDWARE	REQUERIMIENTOS DE SOFTWARE
CPU: 1 GHz RAM: 512 MB HDD: 512 MB	S.O: todas las principales distribuciones de Linux. KERNEL: 2.4 a mas

Nota: (Nagios Core Technical Features, 2016).

Según la Tabla N° 12, la configuración del servidor se ajusta a los requisitos mínimos. Para este prototipo implementado de los servicios de TIC (456) y los equipos monitoreados, la configuración del servidor se alineó con los requisitos detallados en la Tabla N° 13.

Tabla 13

Requerimientos utilizados para el sistema.

REQUERIMIENTOS DE HARDWARE	REQUERIMIENTOS DE SOFTWARE
CPU: Procesador mínimo 2 (3.4 GHZ o superior) RAM: 16 GB	S.O: CentOS 7.x
HDD: TOTAL: 100 GB Particionamiento: /boot 1GB En Tipo LVM: /(root) 70 GB /home 21 GB [swap] 8 GB	KERNEL: 2.4 a mas Apache Pluying

Nota: Muestra las necesidades mínimas para su implementación

4.2.3.1 Requisitos básicos

El análisis de requisitos ha sido fundamental para comprender con precisión las necesidades del usuario, identificando el problema, los actores involucrados, los procesos clave, los objetos y las responsabilidades. A través de entrevistas y la observación directa, se han identificado los requisitos, los cuales han sido validados por el jefe y los especialistas de la OTIC. Los resultados obtenidos de la Tabla N° 14, han permitido determinar los requerimientos necesarios. Esta Tabla representa una síntesis de la información recopilada, detallando las funcionalidades, requisitos y expectativas necesarios para la implementación exitosa del modelo de monitoreo.

Tabla 14

Requerimientos funcionales

REQUISITOS FUNCIONALES	
	Descripción
¿Qué tipo de monitoreo y supervisión de infraestructura y servicios de red utilizan?	Con esta pregunta fue posible tener una idea clara sobre todas las funcionalidades que modelo de monitoreo debería cubrir, siendo indispensable para la elaboración de cada uno de los indicadores.
¿Qué procedimiento se debe seguir para detectar un evento o incidencia de disponibilidad de los servicios TIC?	Con esta pregunta ayudaron a conocer a detalle el proceso mediante el cual el especialista como debe proceder, evidenciando que, muchas de las veces el proceso demoraba debido a que el personal a cargo brindarla se encontraban ocupadas en otras atenciones, y al no ser necesidades operativas generaban demora en la detección de la incidencia del servicio.
¿Cuentan con recursos humanos que se dedique específicamente al monitoreo de los servicios TIC?	La última pregunta tenía como objetivo demostrar que la implementación de un modelo de monitoreo sería factible y podría ofrecer una solución valiosa.

Nota: Muestra el cumplimiento de funcionamiento básico

4.2.3.2 Requisitos no funcionales

Tabla 15

Requerimientos no funcionales.

Requisitos de Soporte	
RNF-001	Disponibilidad 24x7.
Requisitos de interfaces (Diseño)	
RNF-002	Usabilidad.
RNF-003	Intuitivo.
RNF-004	Amigable.
RNF-005	Responsive.
Requisitos de Confiabilidad	
RNF-006	Origen de datos confiable.
Requisitos de seguridad	
RNF-007	El sistema tendrá acceso restringido

Requisitos de Soporte	
	Protección de Datos.
Requisitos de Performance	
RNF-007	Repuestas eficientes.
Otros Requisitos	
RNF-009	Escalable

Nota: sobre las necesidades básicas para una mejor implementación de la solución.

4.2.3.3 Utilitarios informáticos utilizadas para el desempeño del prototipo

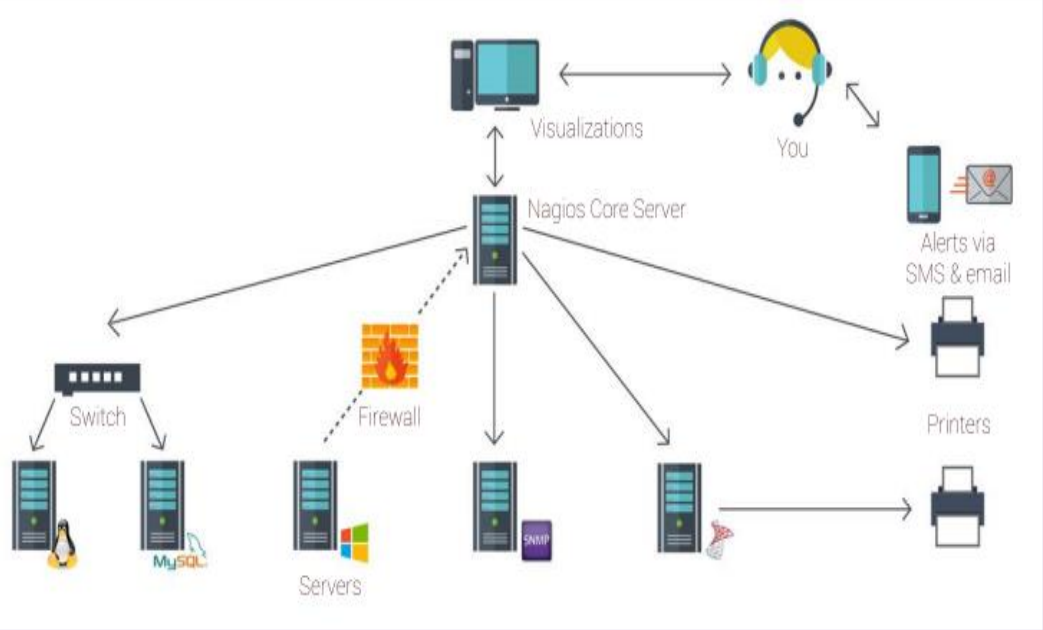
Se emplearon cuatro utilitarios informáticos clave para garantizar el buen desempeño del prototipo implementado. A continuación, se detallan estos utilitarios:

- **Vmware:** Esta herramienta fue esencial para crear máquinas virtuales con los equipos Windows y Linux que se iban a monitorear.
- **mRemoteNG:** Se usó para conectar el host cliente Windows con los servidores Linux a través de SSH, lo que facilitó la instalación de Nagios y sus complementos, además de permitir la revisión de los logs en caso de problemas de configuración.
- **WinSCP:** Esta herramienta se empleó para transferir de manera segura algunos archivos de plugins adicionales y las imágenes de personalización de la interfaz web de Nagios.

4.2.4 Diseño del Modelo del Monitoreo

Figura 18

Diagrama de funcionamiento de Nagios Core.



Nota: Muestra el diagrama de conexión lógica de su implementación (Nagios Enterprises, 2015).

4.2.4.1 Archivos y directorios en Nagios

La ubicación predeterminada de instalación de Nagios es /usr/local/nagios/. Dentro de este directorio se encuentran subdirectorios que se describen a continuación:

Tabla 16

Directorio de configuración

DIRECTORIO	DESCRIPCIÓN
bin	Contiene los archivos ejecutables principales, como el binario Nagios que se ejecuta como proceso en segundo plano.
etc	Guarda la configuración de Nagios, incluidos los componentes, hosts/servicios a monitorear, comandos de ejecución, contactos de notificación, intervalos de monitoreo, con diversos subdirectorios y archivos.

DIRECTORIO	DESCRIPCIÓN
libexec	Aquí residen los plugins ejecutables que realizan los monitoreos, que pueden ser binarios o scripts en Perl, PHP, Shell, Java, entre otros.
sbin	Almacena los ejecutables CGI utilizados para visualizar la interfaz web de Nagios.
share	Contiene el contenido web, imágenes, logotipos, así como los complementos como PNP y Nagvis, junto con los datos necesarios para su funcionamiento.
var	Guarda los datos internos de Nagios, estadísticas de monitoreo, información de ejecución actual, archivos de sockets, registros de logs y colas de monitoreo en ejecución.

Nota: Resultados de la investigación.

4.2.4.2 Descripción general de la configuración

Existen varios archivos de configuraciones que se necesitan para crear o editar antes de empezar a monitorear cualquier host/servicio. Los siguientes archivos de configuración se encuentran en el directorio /usr/local/nagios/etc/ y se detallan a continuación:

Tabla 17

Fichero de configuración en Nagios

FICHERO	DESCRIPCIÓN
nagios.cfg	El archivo principal de configuración de Nagios que incluye diversas directivas que impactan directamente en el funcionamiento del núcleo de Nagios.
resource.cfg	En este archivo de configuración se guardan los macros de ejecución. Los macros “user” son útiles para almacenar nombres de “usuario”, contraseñas y elementos comunes en definiciones de comandos (como rutas de directorio)
objects/	Directorio de archivos de configuración de los objetos que serán utilizados para definir a los hosts, servicios, contactos, comandos, etc.

FICHERO	DESCRIPCIÓN
htpasswd.users	Archivo que almacena las contraseñas encriptadas de los usuarios que se autentican a través de la web.
var/rw/	En esta ubicación se encuentra un archivo especial de socket que facilita la comunicación de comandos y órdenes desde la interfaz web hacia Nagios. Sus archivos de configuración clave son nagios.cmd y nagios.qh.

Nota: Resultados de la investigación

4.2.4.3 Interfaces principales de la herramienta

La primera tarea realizada fue la instalación de algunas dependencias necesarias, como Apache, PHP y otros paquetes adicionales. A continuación, se creó un usuario llamado nagios, encargado de ejecutar el proceso de Nagios. Posteriormente, se descargó, descomprimió e instaló una versión estable de Nagios Core, específicamente la versión 4.0.8.

Después de esto, se creó un usuario de acceso a través de Apache para iniciar sesión en Nagios. El usuario creado, nagiosadmin, requiere una contraseña para acceder a Nagios vía web. Finalmente, se iniciaron manualmente los servicios de Apache y Nagios. Tras completar estos pasos, Nagios quedó en ejecución; para confirmarlo, se accedió vía web utilizando la siguiente dirección:

ULR: http://monitoreodeservicios.minedu.gob.pe/nagios/

Figura 19

Página principal de Nagios.

Nota: Resultado de la investigación.

4.2.4.4 Configuración y habilitación los agentes en los Host remotos

Los establecer una comunicación segura con el servidor de Nagios y obtener información, es necesario habilitar los agentes en los hosts Linux, Windows, routers, switches, entre otros. Esto asegura que los datos viajen de manera segura por la red.

Los agentes utilizados son los siguientes:

- **NSClient++**: utilizado en los hosts Windows remotos.
- **NRPE**: utilizado para los hosts Linux remotos.
- **SNMP**: utilizado en switches, routers y puntos de acceso.

4.2.4.5 Configuración del agente SNMP

Los equipos de comunicación, servidores y servicios web serán monitoreados mediante el protocolo SNMP. Es necesario habilitar este

protocolo en cada uno de los hosts. Para los switches y servidores, es fundamental verificar si el host soporta SNMP. Este protocolo debe estar configurado correctamente para garantizar la confidencialidad, integridad y disponibilidad de los datos de red. SNMP proporciona una gran cantidad de información sobre el estado de los dispositivos de red.

Se utilizó la versión 3 de SNMP (SNMPv3), que proporciona acceso seguro a los dispositivos mediante la autenticación y el cifrado de los paquetes de red.

4.2.4.6 Definición de equipos de comunicación y servicios web

Finalizada la instalación de Nagios junto con sus complementos, se procedió a definir los host y servicios que serán supervisados por el servidor Nagios. Lo siguiente es definir los host Windows, Linux, Switches y ups, y los atributos propios de los hosts (Memoria RAM, CPU, uso de disco, estado de servicio y procesos).

Tabla 18

Equipos de comunicación y servicios web

TIPO DE SERVICIOS Y EQUIPOS	CANTIDAD	Grupo Host	Segmento de red
Servidores con sistema operativo Windows	159	“CENTROS DE PROCESO”	172.31.252.X
Servidores con sistema operativos Linux	177	'VPN-LINUX”	172.16.23.X
Servidores de archivos	3	“FILE SERVER”	10.36.137.X
Switch’s (Cisco y hp)	100	“SWITCHES”	10.36.73.X
Dispositivos UPS	4	“USP”	11.35.125.X
Dispositivos biométricos	18	“BIOMETRICO”	10.35.1.X
Impresoras	2	“IMPRESORAS”	10.36.133.X

Radioenlaces locales	7	"RADIO-ENLACES"	10.36.140.X
Sistemas y servicios web públicos e internos	128	Host Group 'URL'	-
Total	**456**		

Nota: Resultado de la investigación

4.2.4.7 Integrar y definir los host y servicios al Nagios

Una vez identificados los hosts de red que se monitorearán, se procedió a definir cada uno de ellos en los archivos servers-vpn.cfg, svr-glpi.cfg y sede-central.cfg. Nagios utiliza la extensión .cfg para reconocer la definición de los hosts. Estos tres archivos, que ya están disponibles como plantillas, se emplearon para definir los equipos de comunicación.

A continuación, se presenta un modelo de configuración del archivo sede-central.cfg, en el cual se configuran los hosts Linux remotos que serán monitoreados. De manera similar, se configuraron los hosts Windows, routers, switches y puntos de acceso.

Figura 20

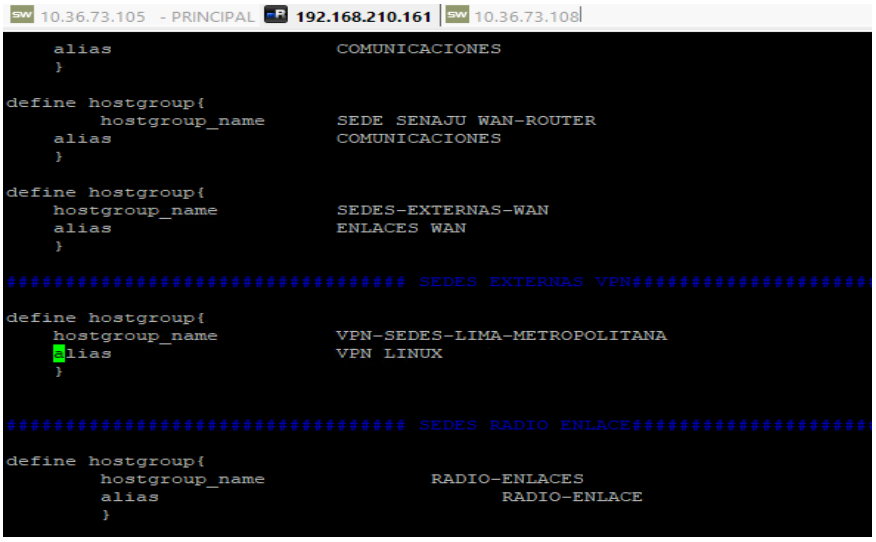
Definición de los host switches

Nota: Resultados de la investigación.

En la Figura N° 21 muestra la configuración en la que se definen los grupos de hosts para los equipos de comunicaciones. Este mismo procedimiento se aplicó a los demás dispositivos de red.

Figura 21

Definición de grupos de host switches



Nota: Resultados de la investigación.

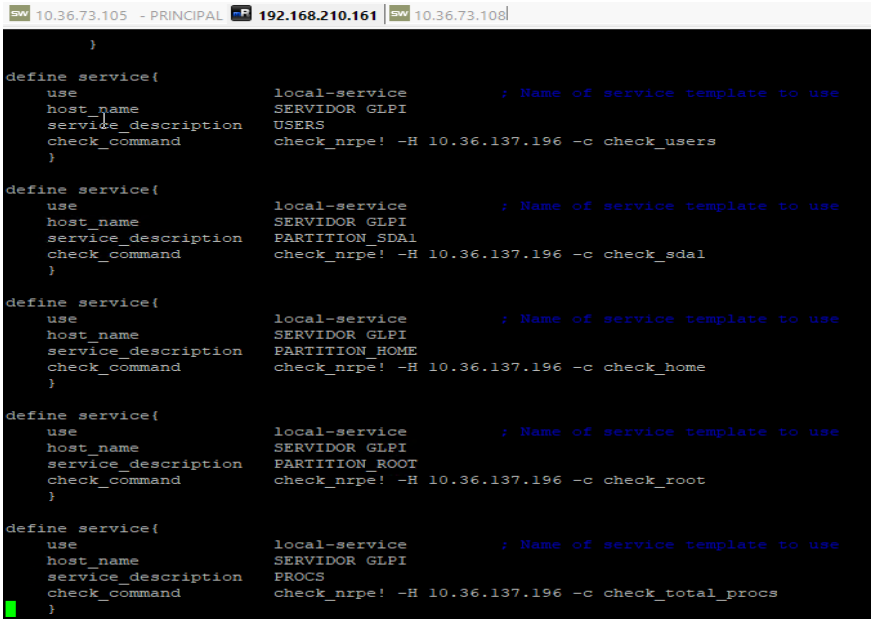
Posteriormente, en el archivo server.cfg, se estableció la configuración de los servicios a ser monitoreados en los hosts Linux. Esto incluye la supervisión de la conectividad, el tiempo de actividad, la carga de la CPU, el estado de la memoria y el disco en los servidores Linux y Windows, así como los servicios de red como HTTP, SSL, TCP, MYSQL, entre otros aspectos. La cantidad de servicios monitoreados en cada dispositivo de comunicación varía en función del tipo de agente utilizado en ellos.

Para que cada servicio definido opere correctamente, es crucial especificar los comandos en el archivo server.cfg que invoquen a los plugins correspondientes. Por ejemplo, el comando check_nrpe hace referencia al plugin check_nrpe, empleado para la supervisión de hosts

Linux remotos. La siguiente representación visual exhibe la configuración de los comandos definidos en el archivo commands.cfg.

Figura 22

Definición de los parámetros de configuración para host Linux



Nota: Resultados de la investigación.

4.2.4.8 Mapas de conectividad

Para la visualización personalizada para el monitoreo se usó Nagvis:

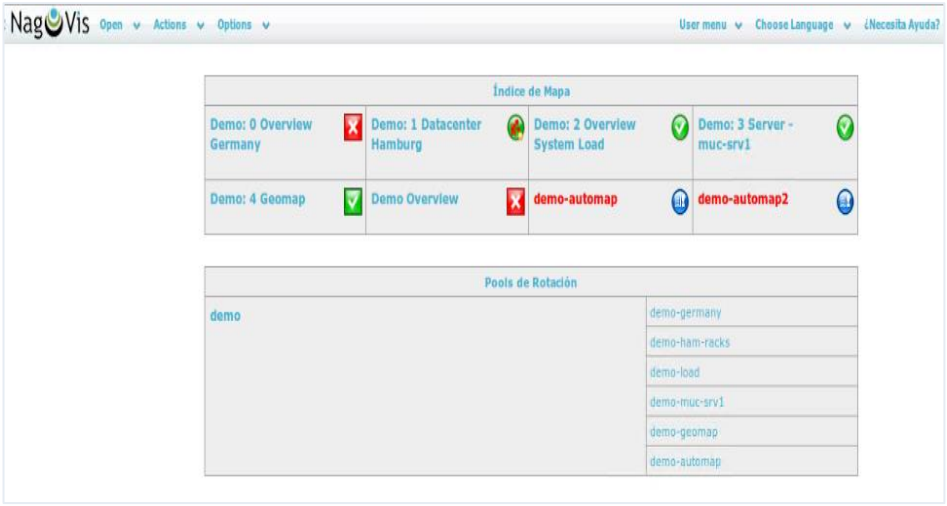
Nagvis es una apliación que facilita la creación de páginas web en el servidor Nagios con mapas interactivos que muestran la topología de red y el estado de los servicios monitoreados. Utiliza Livestatus para mostrar datos en tiempo real con una carga mínima de CPU, siendo ideal para grandes instalaciones con más de 50,000 hosts y servicios.

Para usar Nagvis, primero instala MK Livestatus versión 1.2.5i6p4 y luego la versión 1.8.2 de Nagvis. Tras la instalación, reinicia el servicio de Apache y accede a Nagvis a través de una dirección web. Después de autenticarte, podrás visualizar la página de inicio por defecto de Nagvis.

https://monitoreodeservicios.minedu.gob.pe/nagvis/frontend/nagvis-js/index.php

Figura 23

Página principal de Nagvis.

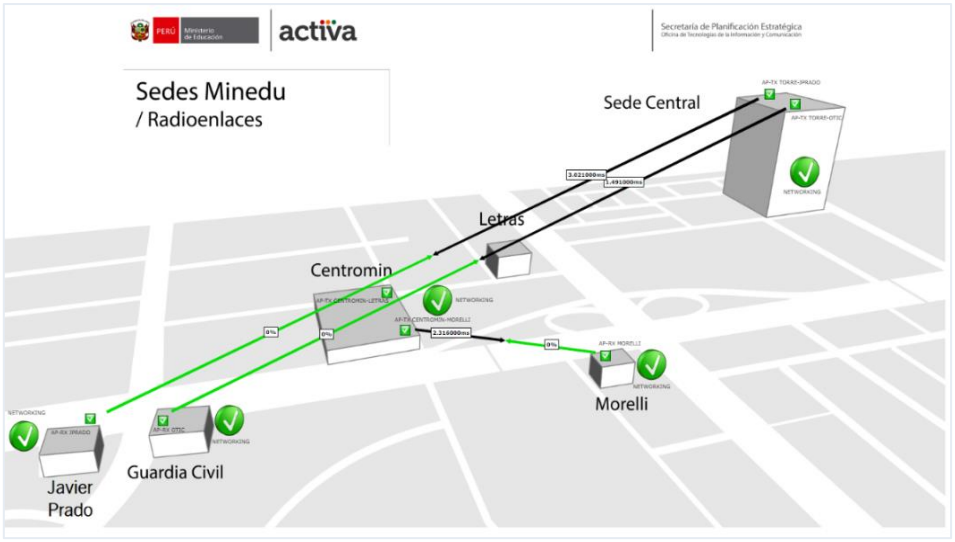


Nota: Resultado de la investigación.

Tras la implementación de la herramienta de monitoreo Nagios, que permite analizar la disponibilidad y calidad de los enlaces corporativos, parámetros que se están evaluando en este trabajo de investigación, se crean mapas personalizados utilizando imágenes de croquis del MINEDU para situar los hosts y servicios que serán monitoreados.

Figura 24

Monitoreo de disponibilidad de enlaces LAN



Nota: Resultados de la investigación.

Los parámetros de disponibilidad, también conocidos como uptime, son de gran utilidad para el administrador del servicio. Asimismo, la calidad del enlace puede ser evaluada en la sección “services” de Nagios, permitiendo verificar la existencia de intermitencias, pérdidas de paquetes o saturación. Esto facilita la identificación y resolución de problemas, así como la determinación de si la incidencia es atribuible al cliente o al proveedor.

En la sección "servicios", se puede consultar el estado de los servicios que están siendo monitoreados por la herramienta. Esto permite verificar si los servicios funcionan correctamente o si se detectan pérdidas de paquetes, con el objetivo de solucionar cualquier problema que se presente en las conexiones.

Figura 25

Monitoreo de servicios URL web críticos.

Nota: Resultados de la investigación.

Figura 26

Monitoreo de disponibilidad de los equipos de comunicación

Nota: Resultados de la investigación.

Interpretación: Del análisis de Manejo del sistema de monitoreo, cabe precisar que al detectar algún evento en los servicios web y/o en los equipos de comunicación notifica al correo de los especialistas de la OTIC y a un grupo de contactos involucrados en tiempo real, esta herramienta permite controlar y verificar los estados, disponibilidad o el comportamiento del ICMP, SMTP, TCP, SSL, HTTPS y HTTP.

4.2.4.9 Notificación

El texto destaca la importancia de monitorear constantemente las interfaces de Nagios y Nagvis para detectar incidencias. Se menciona que Nagios ofrece varias opciones de notificación, como SMS y correo electrónico, siendo este último el más utilizado. Se utiliza Postfix como herramienta para retransmitir correos salientes a través de una cuenta personalizada en archivo de configuración del Nagios. Se sugiere probar la configuración enviando un correo electrónico utilizando la librería mail.

Posteriormente, se revisó el registro de correo electrónico utilizando el comando "tail" para confirmar que el mensaje se envió correctamente y verificar que Postfix se configuró adecuadamente, se ejecuta el siguiente comando:

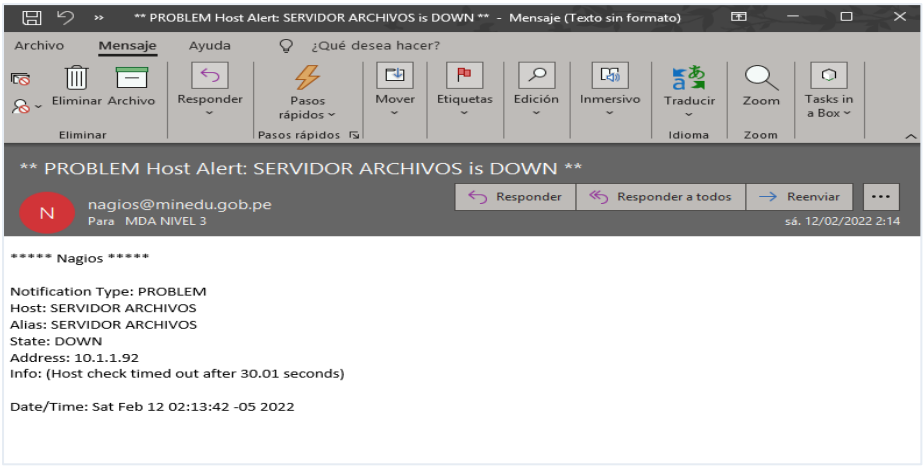
```
#: tail -f /var/log/mail.log
```

Para verificar la recepción del mensaje de prueba, es necesario acceder a la bandeja de entrada del correo electrónico configurado. Previamente, se debe realizar la configuración necesaria para "permitir el acceso de aplicaciones menos seguras" a la bandeja de entrada. Esta medida se debe a que, como medida antispam, la mayoría de los

proveedores de servicios de correo electrónico restringen el envío de correos desde fuentes externas al buzón de entrada, enviándolos a la carpeta de correos no deseados.

Figura 27

Mensaje de notificaciones de la herramienta Nagios.

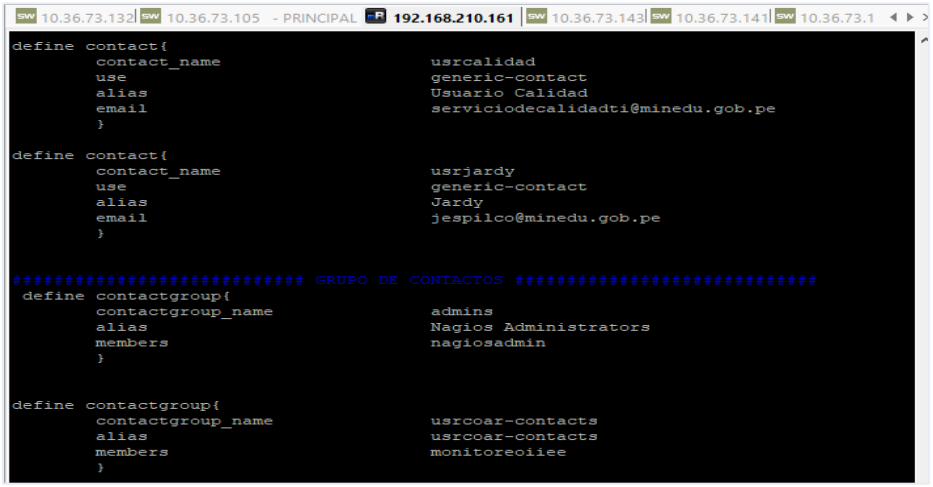


Nota: Resultados de la investigación.

Finalmente, se añadió la dirección de correo electrónico en el servidor Nagios para recibir las notificaciones correspondientes. Esta configuración se realizó en el archivo de configuración **contacts.cfg**.

Figura 28

Definición del contacto para envío de notificaciones



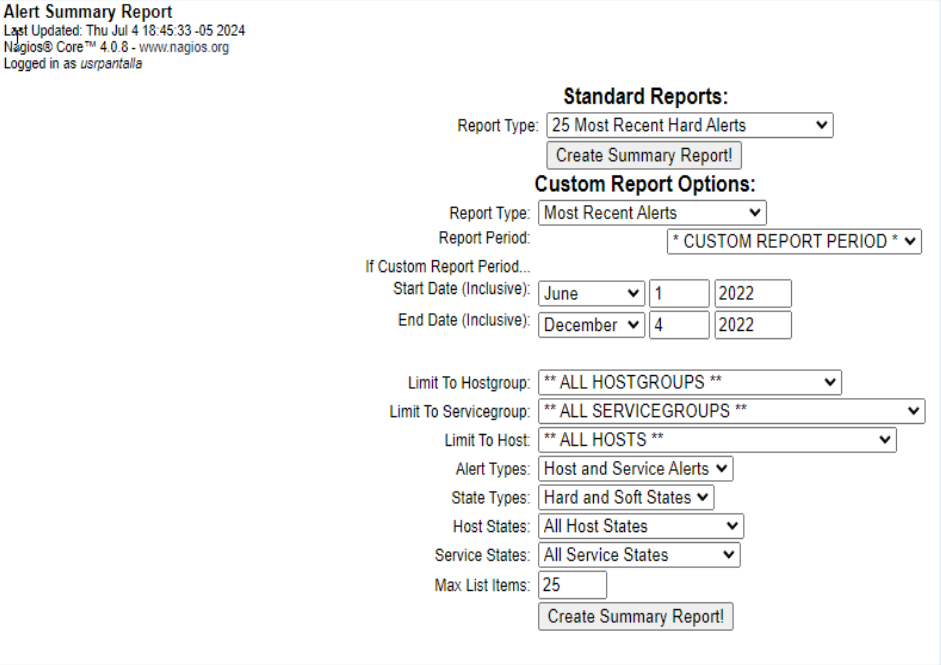
Nota: Resultados de la investigación

4.2.4.10 Reportes

La herramienta ofrece la sección de estado de disponibilidad dentro del menú de opciones de "reportes", permitiendo analizar cualquier dispositivo necesario. Se puede especificar el rango de fechas a examinar, con el objetivo de detectar posibles problemas o realizar un monitoreo proactivo.

Figura 29

Reportería del estado de operatividad de los host y servicios



Nota: Resultados de la investigación.

En el análisis que se muestra en la Figura N° 30, se observa el porcentaje de disponibilidad de un dispositivo durante los últimos siete días, mostrando un 98.665% de tiempo operativo (uptime) y un 1.335% de tiempo fuera de servicio (downtime).

Figura 30

Análisis del reporte de disponibilidad de los switches.

Hostgroup 'CENTROMIN' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
SW-CM-PA-G1-SW01-A	99.745% (99.745%)	0.255% (0.255%)	0.000% (0.000%)	0.000%
SW-CM-PA-G1-SW02-A	99.744% (99.744%)	0.256% (0.256%)	0.000% (0.000%)	0.000%
SW-CM-PA-G1-SW03-A	99.751% (99.751%)	0.249% (0.249%)	0.000% (0.000%)	0.000%
SW-CM-PA-G1-SW04-TRANSPORTE	99.751% (99.751%)	0.249% (0.249%)	0.000% (0.000%)	0.000%
SW-CM-PA-G2-SW01-A	99.751% (99.751%)	0.249% (0.249%)	0.000% (0.000%)	0.000%
SW-CM-PB-G2-SW05-A	99.713% (99.713%)	0.287% (0.287%)	0.000% (0.000%)	0.000%
SW-CM-PB-G2-SW06-A	99.708% (99.708%)	0.292% (0.292%)	0.000% (0.000%)	0.000%
SW-CM-PB-G2-SW07-A	99.725% (99.725%)	0.275% (0.275%)	0.000% (0.000%)	0.000%
SW-CM-PB-G2-SW08-A	99.706% (99.706%)	0.294% (0.294%)	0.000% (0.000%)	0.000%
SW-CM-PB-G2-SW09-A	99.665% (99.665%)	0.335% (0.335%)	0.000% (0.000%)	0.000%
SW-CM-PCD-G3-SW10-A	99.596% (99.596%)	0.404% (0.404%)	0.000% (0.000%)	0.000%
SW-CM-PCD-G3-SW11-A	99.595% (99.595%)	0.405% (0.405%)	0.000% (0.000%)	0.000%
SW-CM-PCD-G3-SW12-A	99.598% (99.598%)	0.402% (0.402%)	0.000% (0.000%)	0.000%
SW-CM-PCD-G3-SW13-A	99.591% (99.591%)	0.409% (0.409%)	0.000% (0.000%)	0.000%
SW-CM-PCD-G3-SW15-A	99.603% (99.603%)	0.397% (0.397%)	0.000% (0.000%)	0.000%
SW-CM-PCD-G3-SW16-A	99.598% (99.598%)	0.402% (0.402%)	0.000% (0.000%)	0.000%
SW-CM-PE-G2-SW19-A	99.685% (99.685%)	0.315% (0.315%)	0.000% (0.000%)	0.000%
SW-CM-PE-G4-SW18-A	99.678% (99.678%)	0.322% (0.322%)	0.000% (0.000%)	0.000%
SW-CM-PF-G2-SW21-A	99.665% (99.665%)	0.335% (0.335%)	0.000% (0.000%)	0.000%
Average	99.677% (99.677%)	0.323% (0.323%)	0.000% (0.000%)	0.000%

Nota: Resultados de la investigación

Asimismo, en la Figura N° 30 se ilustra el desempeño del servicio de ping dirigido hacia los equipos de comunicaciones (switches) de la zona L. Se constató que el equipo respondió de manera normal en un 82.266%, presentó alertas en un 0.098%, y en estado crítico o sin respuesta en un 2.031%. Estos distintos estados observados se atribuyen a las variaciones en los tiempos de respuesta del pineo, lo que valida la calidad del enlace.

4.3 VALIDAR LA MEJORA DEL NIVEL DE DISPONIBILIDAD Y TIEMPO DE DETECCIÓN DE EVENTOS EN LOS SERVICIOS TIC EN EL MINEDU A TRAVÉS DE UN MODELO DE MONITOREO ALINEADO A ITIL 4 CON NAGIOS Y NAGVI.

Después de la implementación de la herramienta se realizó las pruebas del modelo con tres servicios de TIC; equipos de comunicación (componentes y subcomponentes), enlaces y servicios web. A continuación, se presentan los resultados de la evaluación de

los indicadores propuestos en el capítulo 1 en el numeral 1.7.1, "Operacionalización de variables".

4.3.1 Primer análisis: Resultados de la evaluación del proceso de gestión de incidencias

Tabla 19

Data de la estadística de incidencias oportunas e inoportunas

INCIDENCIAS	SIN EL MODELO	CON EL MODELO
	PERIODO ENERO - JUNIO 2022	PERIODO JULIO - DICIEMBRE 2022
INCIDENCIAS ATENDIDAS DENTRO DEL TIEMPO ESTABLECIDO.	8107	12065
INCIDENCIAS ATENDIDAS FUERA DEL TIEMPO ESTABLECIDO	710	356
TOTAL, INCIDENCIAS	**8817**	**12421**

Nota: Resultados de la investigación.

Interpretación de resultados:

Al observar la Tabla N° 19, se aprecia de manera clara la comparación entre la aplicación del modelo de monitoreo basado en ITIL 4 para mejorar la disponibilidad de los servicios de TIC del Ministerio de Educación y la falta de un modelo de monitoreo. Se destaca una notable mejora en la pronta atención de incidencias, lo que se traduce en la superación de los tiempos establecidos para resolver dichas incidencias de manera oportuna.

4.3.2 Resultados de las fichas de observación

4.3.2.1 Tiempo de notificaciones de la incidencia

Para calcular el tiempo de interrupción de los servicios, se empleó la unidad de medida "minutos". Este cálculo se realizó restando el tiempo de notificación de la incidencia al momento de detección de estas, los resultados obtenidos de las pruebas registrada en el Anexo B. Los datos se recopilaron de las fichas de observación, resultando en un tiempo promedio de detección de eventos e incidencias de 1158 minutos.

4.3.2.2 Resultados antes de la implementación del modelo

En la tabla N° 20 proporciona una visión detallada de la distribución de las incidencias según su nivel de impacto antes de la implementación del modelo de monitoreo el resultado de los registros de la ficha de observación.

Tabla 20

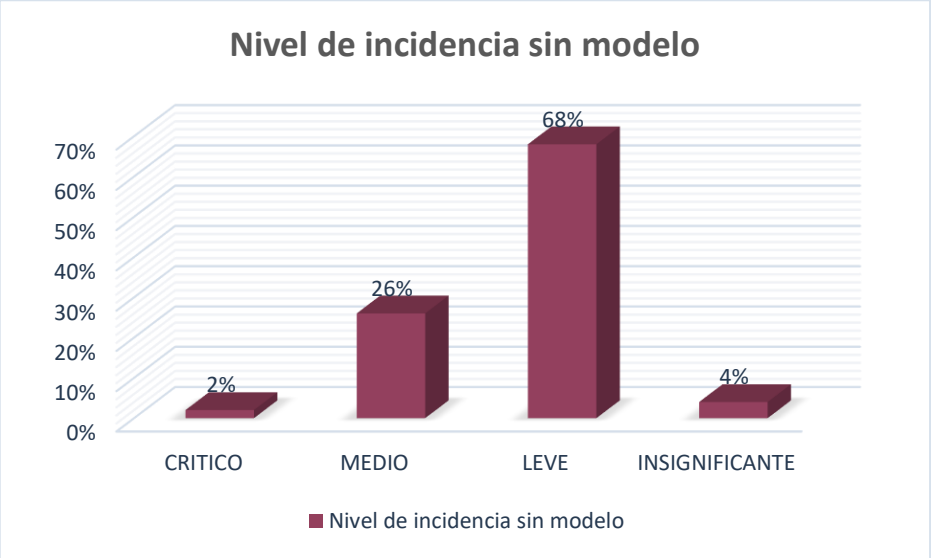
Resultado del indicador de nivel de incidencia.

	SIN EL MODELO			
NIVEL DE IMPACTO	**FRECUENCIA**	**FRECUENCIA RELATIVA ACUMULADA**	**TENDENCIA RELATIVA PORCENTUAL**	**TENDENCIA ACUMULADA PORCENTUAL**
CRITICO	3	3	2%	2%
MEDIO	37	40	26%	28%
LEVE	96	136	68%	96%
INSIGNIFICANTE	5	141	4%	100%
TOTAL,	**141**		**100%**	

Nota: Describe el nivel de impacto.

Figura 31

Gráfica de nivel de incidencia sin modelo



Nota: Visualizar el impacto más significativo.

Interpretación de resultados:

De acuerdo con los resultados presentado en la Figura N° 31, se destaca que el nivel de incidencia más común es el "leve", representando un 68% del total, seguido por las incidencias de nivel "medio". Por lo tanto, se puede concluir que el impacto afecta a un servicio de TIC no crítico, lo que repercute parcialmente en la disponibilidad.

4.3.2.3 Resultados con la implementación del modelo

Para calcular el tiempo de detección de las incidencias, se empleó la unidad de medida "minutos". Este tiempo se obtuvo restando el tiempo de notificación de la incidencia al tiempo de detección de esta, obtenidos de las pruebas registrada en el Anexo B. Donde el tiempo promedio de detección de incidencias de 164 minutos en el periodo de 6 meses.

De acuerdo con los resultados de las pruebas realizadas al sistema, se obtuvo el siguiente resultado:

Tabla 21

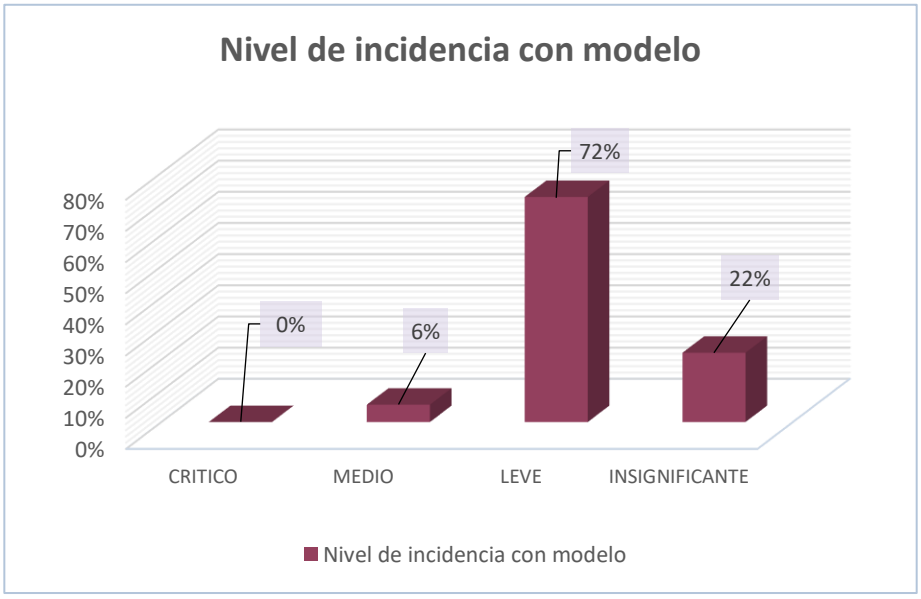
Resultados del indicador después de implementar el sistema.

NIVEL DE IMPACTO	CON EL MODELO			
	FRECUENCIA	FRECUENCIA RELATIVA ACUMULADA	TENDENCIA RELATIVA PORCENTUAL	TENDENCIA ACUMULADA PORCENTUAL
CRITICO	0	2	2%	2%
MEDIO	5	7	5%	8%
LEVE	65	72	71%	78%
INSIGNIFICANTE	20	92	22%	100%
TOTAL,	**80**		**100%**	

Nota: Describe el nivel de impacto a detalle.

Figura 32

Gráfica estadística de los resultados con modelo



Nota: Resalta el nivel de impacto con mayor valor.

Interpretación de resultados:

De acuerdo con los resultados presentados de la Tabla N° 21 y figura 32, se puede concluir que el sistema mejora significativamente el tiempo de la detección de eventos en un servicio TIC, reduciendo el tiempo de días a casi inmediato. Específicamente:

- El sistema tarda en promedio 2 minutos para detectar la caída de un servicio TIC.
- En promedio, se tarda 4 minutos en enviar la notificación de la caída del servicio TIC al correo electrónico de los especialistas.

Dando como resultado que el sistema notifica la caída de un equipo de comunicación en un tiempo no mayor de 5 minutos.

Esto significa que el sistema notifica la caída de un equipo de comunicación en un tiempo no mayor a 5 minutos.

4.3.2.4 Numero de interrupciones del servicio de TIC

Resultados antes de la implementación del modelo

Tabla 22

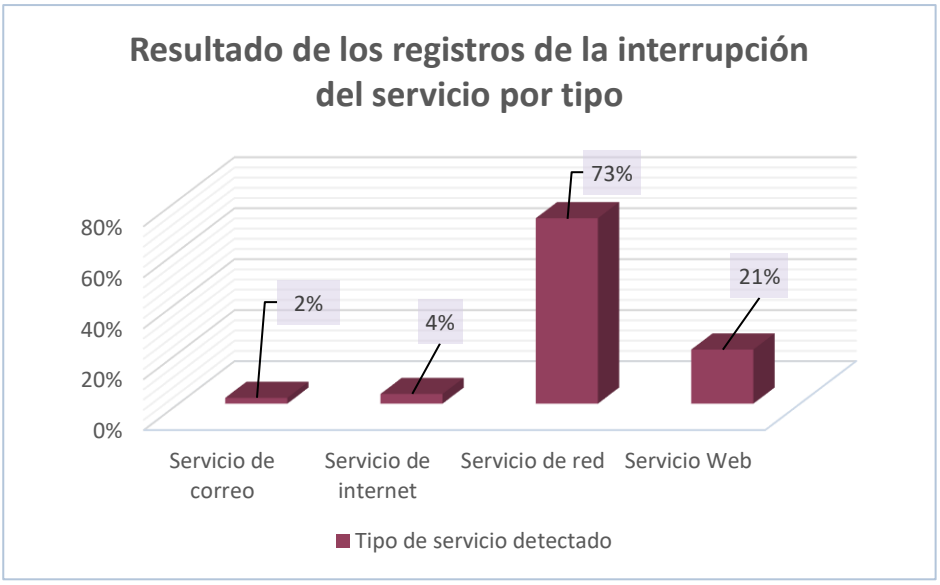
Resultado del indicador cantidad de interrupciones por servicio.

TIPO DE SERVICIO	SIN EL MODELO			
	FRECUENCIA	FRECUENCIA RELATIVA ACUMULADA	TENDENCIA RELATIVA PORCENTUAL	TENDENCIA ACUMULADA PORCENTUAL
Servicio de correo	3	3	2%	2%
Servicio de internet	5	8	4%	6%
Servicio de red	96	104	73%	79%
Servicio Web	28	132	21%	100%
TOTAL	**132**		**100%**	

Nota: Muestra los resultados de los tipos de servicios sin modelo.

Figura 33

Gráfica estadística de los resultados sin modelo



Nota: Mostrar la relevancia sobre la interrupción del servicio.

Interpretación de resultados:

De los resultados obtenidos en la Tabla N°22 y Figura N° 33, se puede observar que la incidencia detectado más recurrente es el "servicio de red" con un 73%, seguido por las incidencias de "servicios Web" con el 21%.

4.3.2.5 Resultados después de implementar el modelo

Con base en los resultados de las pruebas realizadas en el sistema a lo largo del periodo de seis meses, se pudo obtener el siguiente resultado:

Tabla 23

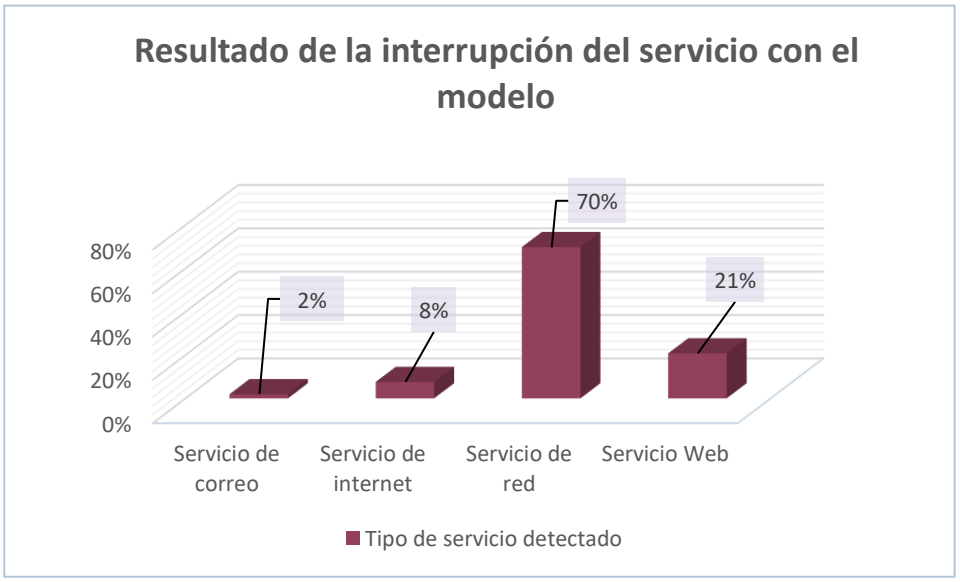
Resultado del indicador cantidad de interrupciones por servicio.

TIPO DE SERVICIO	CON EL MODELO			
	FRECUENCIA	FRECUENCIA RELATIVA ACUMULADA	TENDENCIA RELATIVA PORCENTUAL	TENDENCIA ACUMULADA PORCENTUAL
Servicio de correo	1	1	2%	2%
Servicio de internet	4	5	8%	9%
Servicio de red	37	42	70%	79%
Servicio Web	11	53	21%	100%
TOTAL,	**53**		**100%**	

Nota: Muestra el resultado por tipo de servicio aplicando el modelo.

Figura 34

Gráfica estadística de los resultados sin modelo



Nota: Resalta la interrupción con aplicación del modelo.

Interpretación de resultados:

Al analizar los resultados presentados en la Tabla N° 23 y Figura N°34, se puede apreciar que la incidencia más frecuente detectada es el "servicio de red", con una disminución del 70%, seguida por las

incidencias relacionadas con "servicios web", que han disminuido en un 21%.

4.3.2.6 Nivel de disponibilidad de los servicios TIC en la red

Resultados antes de la implementación del modelo

Para medir el nivel de disponibilidad en un periodo de 6 meses obteniendo el siguiente resultado:

Fórmula de cálculo de disponibilidad de los servicios TIC:

((A – B) /A) x 100 por ciento)

Donde:

A = Tiempo total comprometidas de disponibilidad

B = Tiempo de inactividad.

Tabla 24

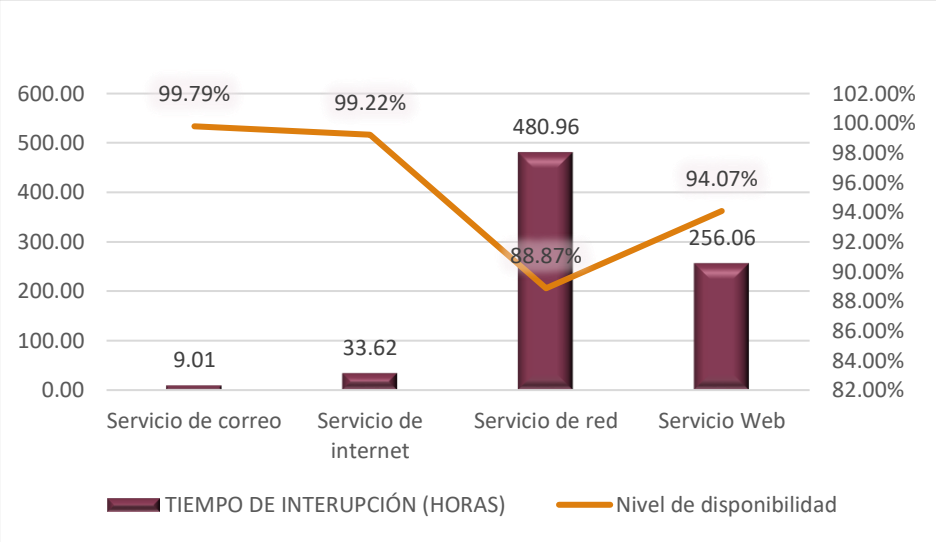
Resultado del indicador nivel de disponibilidad.

TIPO DE SERVICIO	SIN EL MODELO			
	TIEMPO DE INTERUPCIÓN (HORAS)	TIEMPO DE INTERUPCIÓN (MINUTOS)	NIVEL DE DISPONIBILIDAD	TENDENCIA RELATIVA ACUMULADA
Servicio de correo	9,01	540	99,79%	73%
Servicio de internet	33,62	2018	99,22%	76%
Servicio de red	480,96	28858	88,87%	87%
Servicio Web	256,06	15364	94,07%	100%
TOTAL,	**779,65**		**81,95%**	

Nota: Muestra el resultado del indicador de la disponibilidad sin aplicar el modelo

Figura 35

Gráfica estadística de los resultados sin modelo



Nota: Nivel de disponibilidad de los servicios TIC sin modelo

Interpretación de resultados:

Al analizar los resultados presentados en la Tabla N° 24 y la Figura N° 35, se evidencia que el nivel de disponibilidad promedio obteniendo un 81,95 % disponibles del grupo de servicios TIC.

4.3.2.7 Resultados después de implementar el modelo

Con base en los resultados de las pruebas realizadas en el sistema a lo largo de un periodo de seis meses, se logró obtener el siguiente resultado:

Tabla 25

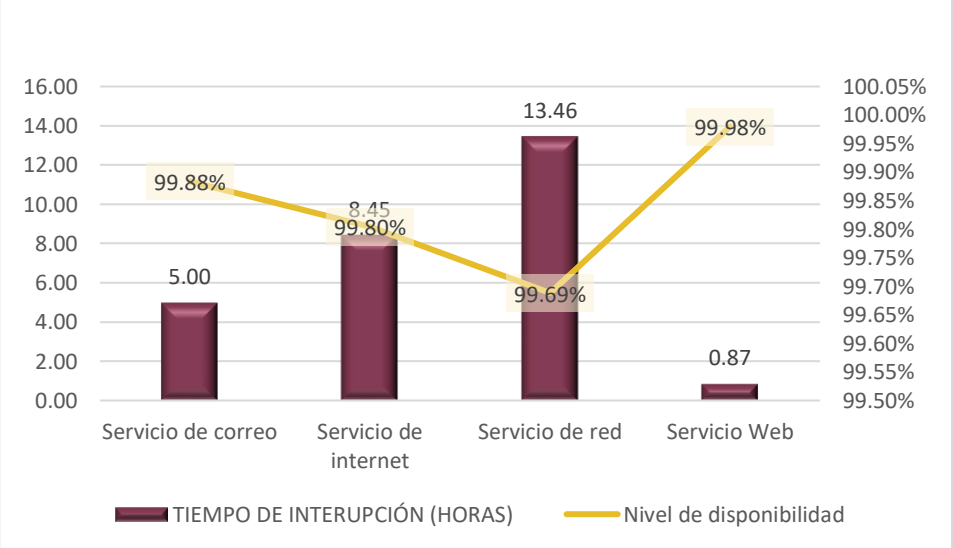
Resultado del indicador nivel de disponibilidad.

TIPO DE SERVICIO	CON EL MODELO			
	TIEMPO DE INTERUPCIÓN (HORAS)	TIEMPO DE INTERUPCIÓN (MINUTOS)	NIVEL DE DISPONIBILIDAD	TENDENCIA RELATIVA ACUMULADA
Servicio de correo	5,00	300	99,88%	18%
Servicio de internet	8,45	507,22	99,80%	48%
Servicio de red	13,46	807,48	99,69%	96%
Servicio Web	0,87	52,49	99,98%	100%
TOTAL	**27,78**	**618,55**	**99,36%**	

Nota: Muestra el impacto en los tipos de servicios luego de aplicar el modelo.

Figura 36

Gráfica estadística de los resultados con modelo



Nota: Nivel de disponibilidad de los servicios TIC con modelo.

Interpretación de resultados:

De acuerdo a los resultados presentados en la Tabla N° 25 y figura N° 36, se puede observar que el conjunto de servicios TIC alcanza un nivel de disponibilidad promedio del 99,36%, superando de manera significativa

el nivel de disponibilidad promedio sin la aplicación del modelo, el cual se sitúa en el 81,95%.

4.3.2.8 Tiempo de resolución de incidencias y eventos

Tabla 26

Análisis de los resultados obtenidos con y sin la aplicación del modelo.

REPORTE DE LOS RESULTADOS ANTES Y DESPUÉS DEL MODELO		
DESCRIPCIÓN	**SIN EL MODELO**	**CON EL MODELO**
Número de incidencias solucionadas	8504	6272
Promedio de tiempo a la atención de incidencias	45:00:44	15:01:28
Cantidad de incidencias atendidas por día	56	41
Tiempo Máximo de Solución Promedio	2532:18:49	2456:17:24
Tiempo Mínimo Solución Promedio	0:02:13	0:01:13
Media Promedio de tiempo de Atención solución	2:28:52	0:28:29

Nota: Resultados de los reportes antes y después del modelo.

Interpretación de resultados:

A partir de la Tabla N° 26, se pueden extraer las siguientes conclusiones:

- Se han atendido y solucionado 6272 incidencias, lo que representa una disminución de 2396 incidencias en comparación con las 8504 registradas anteriormente. Esta reducción en el número de incidencias contribuye a mejorar la disponibilidad y el buen funcionamiento de los servicios TIC.
- Los tiempos de atención de incidencias han mejorado significativamente, pasando de 45 horas a 15 horas. Esta

reducción de 30 horas en el tiempo de atención equivale a una mejora de 2 días en la resolución de incidencias.

Dado la similitud en los resultados obtenidos tanto con modelo y sin modelo, se llega a determinar que se puede realizar la prueba de hipótesis con los datos obtenidos.

4.3.3 Prueba de la hipótesis

H0: La implementación de un modelo de monitoreo aplicando ITIL 4 no mejorará significativamente la disponibilidad de los servicios de TIC llevados a cabo por la Oficina de TIC del Ministerio de Educación – Lima.

H1: La implementación de un modelo de monitoreo aplicando ITIL 4 mejorará significativamente la disponibilidad de los servicios de TIC llevados a cabo por la Oficina de TIC del Ministerio de Educación – Lima.

- **Planteamiento:**

$\mathbf{H_0} = 1159$

$\mathbf{H_1} \neq 1159$

Para evaluar la hipótesis, se empleó la prueba t de Student para muestras independientes. Los resultados se presentan en la Tabla N° 27 (Estadísticos de grupo) y la Tabla N° 28 (Resultados de muestras independientes). Se observó que el tiempo promedio de detección de incidencias durante el periodo de seis meses sin modelo fue de 1158.59 minutos, mientras que con modelo fue de 164 minutos. Las desviaciones estándar fueron de 1471.70 y 573.47 minutos, respectivamente. Estos resultados indican un impacto significativo en la disponibilidad de los servicios TIC.

Tabla 27

Estadístico de prueba grupal

	GRUPO	N	MEDIA	Desviación S.	Error de Desv. promedio
MODELO	1	37	1158,59	1471,70	241,95
	2	53	164,07	573,47	78,77

Nota: Muestra el resultado de las pruebas realizadas.

Tabla 28

Resultados de la comparación de las muestras independientes

		Varianza agrupada	Cálculo de la Prueba T para la igualdad de medias		
			Sig. (Bilateral)	GL.	E.T
MODELO	para dos muestras asumiendo varianzas iguales	1080379,703	0,01007	88	4,46625331
	Prueba T para dos muestras asumiendo varianzas desiguales			44	3,90857226

Nota: Muestra resultado de la prueba T de la Tabla N° 29.

- **Nivel de Significancia:**

Se utilizó un nivel de significancia del 5% y un nivel de confianza del 95%, representados como $\propto = 0.05$ y con 38 grados de libertad (n1 + n2 - 2).

Donde:

n1 = incidencias detectadas sin modelo

n2 = incidencias detectadas con modelo, se tiene el valor crítico Tç:

Valor T: $\mathbf{t\alpha 0.05} = 1,9873$

- **Estadístico de prueba:**

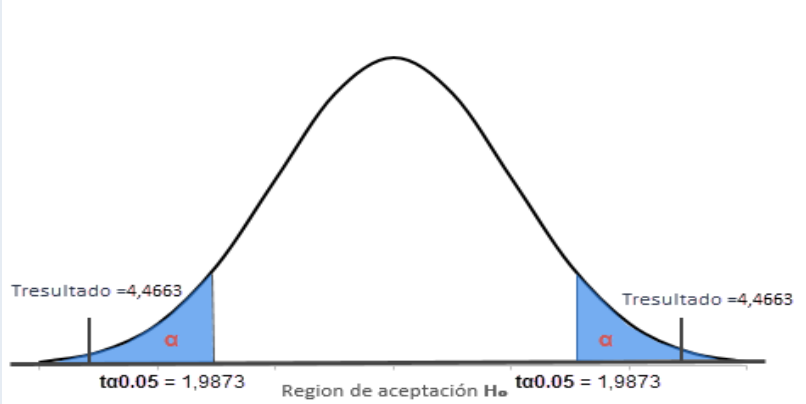
$$T = \frac{\bar{x}_1 - \bar{x}_2}{\sqrt{\frac{s_C^2}{n_1} + \frac{s_C^2}{n_2}}}$$

Y se tiene la **T** resultado que se puede observar en la Tabla N° 27. Resultados de muestras independientes:

***T** resultado* = 4,46625331

Figura 37

Representación gráfica de la prueba de la hipótesis



Nota: Muestra que está dentro de los parámetros aceptables.

- **Toma de decisión:** Se ha demostrado Tresultado ≠ 1,9873 se encuentra en la zona de rechazo, lo que lleva a rechazar la Hipótesis Nula y aceptar la Hipótesis Alternativa. Esto significa que el modelo de monitoreo basado en ITIL 4 mejora de manera significativa la disponibilidad de los servicios de TIC en el Ministerio de Educación.

4.4 DISCUSIÓN

Los resultados obtenidos para los objetivos fueron favorables para la identificación y análisis de la situación actual de los servicios TIC aplicando los principios de ITIL 4, ya que con esta técnica se identificó los indicadores, los cuales facilitaron el

desarrollo y pruebas del modelo. Los resultados que se obtuvieron concuerdan con las conclusiones de (Ruiz Quintero, 2016) indicando que de acuerdo con las mejores prácticas de ITIL 4. Se diseñaron procesos y procedimientos que permitieron definir los servicios principales y sub-servicios, La gestión de servicios basada en ITIL proporciona beneficios significativos a los servicios TI. permitiendo determinar los requisitos necesarios para la implementación del modelo.

Los resultados obtenidos para el objetivo específico impactaron de manera positiva al implementar el modelo de monitoreo para la detección de la degradación o interrupción de los servicios de TIC, realizando las validaciones y pruebas. Estos resultados inciden con las conclusiones de (Vega Picon, 2018) quien resalto resaltó la capacidad del monitoreo para reducir los efectos negativos de enlaces con problemas y prevenir sanciones cumpliendo un SLA, el estudio exploro el uso de la herramienta como Cacti y Nagios.

Los resultados obtenidos para el objetivo específico; validar la mejora del nivel de disponibilidad y el tiempo de detección de eventos e incidencias de los servicios de TIC, en el Ministerio de Educación fueron favorables alcanzado un nivel de disponibilidad promedio del 99,36%, superando de manera significativa el nivel de disponibilidad promedio sin el modelo, el cual se sitúa en el 81,95%, concordando con los resultados de (Aceituno Rojo, 2013) concluye que sus resultados determinó 14 indicadores que mejoró el tiempo de detección de incidentes en un 87.78% después del desarrollo del modelo de monitoreo de servidores.

V. CONCLUSIONES

PRIMERA: Tras análisis exhaustivo de la situación actual de los servicios de TIC en el Ministerio de Educación reveló la necesidad de implementar un modelo de monitoreo basado en ITIL 4 para garantizar su disponibilidad. A través de una evaluación detallada, que incluyó fichas de observación y entrevistas con el personal especializado de la OTIC, se identificaron los procesos iniciales de gestión de incidencias y los tiempos de atención. Esta evaluación permitió comprender a profundidad el funcionamiento actual de los servicios TIC.

SEGUNDA: Con la implementación del modelo de monitoreo aplicando ITIL para la disponibilidad de los servicios de TIC del Ministerio de Educación; se determinó los procesos, los indicadores y parámetros que se aplicaron para el desarrollo del modelo. Tras una exhaustiva evaluación de las herramientas disponibles, se seleccionó cuidadosamente la herramienta de monitoreo Nagios Core y Nagvis con un rendimiento del 92%. Estas herramientas fueron elegidas por cumplir con la mayoría de los parámetros establecidos en el estudio, demostrando ser las más adecuadas para el desarrollo del modelo propuesto en esta investigación.

TERCERA: El modelo implementado, basado en ITIL 4, mejora la disponibilidad de los servicios TIC del Ministerio de Educación en Lima. Incluye un módulo de informes detallados sobre la disponibilidad de hosts y servicios, tendencias, histogramas y alertas. Proporciona una visualización gráfica del comportamiento de los servicios en distintos periodos, ofreciendo al especialista de TI información para decisiones estratégicas. La notificación

por correo electrónico facilita la detección de incidencias para una respuesta rápida y efectiva, detalladas en el Anexo C del modelo

CUARTA: La adopción del modelo de monitoreo aplicando ITIL 4 para la disponibilidad de los servicios de TIC del Ministerio de Educación; ha demostrado un nivel de disponibilidad del 99,35%, lo cual ha tenido un impacto significativo en comparación con la ausencia de un modelo. Esta mejora se evidenció al comparar los periodos de 6 meses en 2022, tanto con modelo como sin modelo. Durante el periodo de enero a junio de 2022, se detectaron 37 incidencias con un tiempo promedio de detección de 1158,59 minutos, mientras que, en el periodo de julio a diciembre de 2022, se registraron 57 incidencias con un tiempo promedio de detección de 164 minutos. La comparación de estos resultados respalda la aceptación de la Hipótesis Alternativa, confirmando que la implementación de un modelo de monitoreo con ITIL 4 ha sido efectiva para mejorar la disponibilidad de los servicios de TIC en el Ministerio de Educación.

VI. RECOMENDACIONES

PRIMERA: Es recomendable realizar un análisis exhaustivo de los eventos detectados por la herramienta para identificar las causas raíz de los problemas. Es importante establecer un plan de acción para la atención de las alertas, incluyendo los roles y responsabilidades del personal involucrado.

SEGUNDA: Es importante implementar un sistema de notificación de las alertas por mensaje de texto a un celular. Este permite una alerta inmediata a la persona responsable, lo que contribuye a la gestión eficiente de errores, se reducen los tiempos de restablecimiento, impactando positivamente en la disponibilidad de los servicios de TIC.

TERCERA: Es recomendable el despliegue de un sistema de monitoreo de redundancia para el gestor, así como la ampliación del estudio de tesis incluyendo un mayor número de equipos monitoreados, como teléfonos IP, impresoras con soporte SNMP, UPS y cámaras IP. De esta manera, se minimizaría la posibilidad de pérdida de datos en caso de falla.

CUARTA: Es recomendable mantener la actualización y documentación de los procedimientos para el monitoreo de los servicios de TIC. Esto ayuda a reducir el tiempo necesario para validar incidencias y facilita el escalado a los administradores de los servicios.

QUINTA: Es importante realizar pruebas y evaluaciones periódicas del modelo de monitoreo para asegurar su correcto funcionamiento.

VII. REFERENCIAS BIBLIOGRÁFICAS

Abrahäo, S., & Calero, C. (2022). *Calidad y sostenibilidad de sistemas de información en la práctica. Quienes concluye*.

Aceituno Rojo, M. R. (2013). Modelo de monitoreo de servidores basado en SNMP y Scorecard para mejorar el tiempo de detección de incidentes en la empresa de distribución eléctrica Electro Puno S.A.A. En el año 2012. En *tesis de pregrado*. Universidad Nacional del Altiplano.

Ancajima Miñán, Víctor Ángel Infante Saavedra, Carmen Lucila, Aliaga Guevara, Frisa María Antonieta, Soto Abanto, S. E. (2022). *Cultura organizacional de las Tecnologías de la Información y Comunicación en las municipalidades de la Región Piura* (Religación).

AXELOS Limited. (2019). *ITIL 4 Foundation* (M. F. As, S. jo Moore, & Simone (eds.); 4 edition). IT PRENEURS TM.

Barth, W. (2006). *Nagios - System and Network Monitoring* (Munich (ed.)).

Calvo García, Á. L. (2014). *Gestión de redes telemáticas UF1880*. IC Editorial. https://doi.org/IFCT0410

Cisco Systems, I. (2020). *Software Configuration Guide - Configuring SNMP* (pp. 1-968).

Díaz Rosemberg, A. G. (2006). Diseño e Implementación del Centro de Operación y Gestión de la red Académica Peruana en Software Libre. En *tesis de pregrado*. PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ.

Hernández Sampieri, R. (2014). *METODOLOGÍA DE LA INVESTIGACIÓN* (sexta edic). INTERAMERICANA EDITORES, S.A. DE C.V.

Jesús, R., & Tejedor, M. (2006). *Management Protocol version 3)*. *3*, 45-48.

Limited, A., Limited, A., & Limited, A. (2019). *ITIL ® Foundation*.

Ministerio de Educación, M. (2015). *Reglamento de Organización y Funciones del Ministerio de Educación* (p. 63).

Ministerio de Educación, M. (2021). *Resolución de Secretaría General N° 075-2021-MINEDU* (p. 31). Lima, 07 de mayo de 2021.

Morán, L. (2009). ISO/IEC 20000. Guía completa de aplicación para la gestión de los servicios de tecnologías de la información. *AENOR(Asociación Española de Normalización y certificación)*, *1*, 53.

Nagios Core, L. (2016). *Host Checks · Nagios Core Documentation*.

Nagios Core Technical Features. (2016). *Nagios XI // Hardware Requirements*. https://assets.nagios.com/datasheets/nagioscore/Nagios Core - Features.pdf

Nagios Enterprises, L. (2015). *How Nagios Core Works*. https://assets.nagios.com/datasheets/nagioscore/Nagios Core - How It Works.pdf

OTIC. (2022). *Validación del Foda OTIC en la USAU Matriz FODA de la Gestión de TI del Ministerio de Educación*. 2.

Purihuamán Venegas, E. H., & Ramos Alcarraz, D. R. (2021). *Modelo de monitoreo para la identificación preventiva de incidencias y la ejecución de acciones correctivas en los servicios tecnológicos de las organizaciones*. Universidad Peruana Unión - Perù.

Reque Casas, R. M., & Sempértegui Tocto, M. L. (2017). Implementación De Un Sistema De Monitoreo Y Supervisión De La Infraestructura Y Servicios De Red Para Optimizar La Gestión De Ti En La Universidad Nacional Pedro Ruiz Gallo. *Rueda Montoya, Rudsvi. 2018. "Universidad Nacional Pedro Ruiz Gallo." 1–250.*, 1-155.

Ruiz González, F., & Velthius Piattini, M. G. (2021). *Gobierno y gestión de las tecnologías y los sistemas de información* (Ediciones de la U (ed.)). https://doi.org/Ra-ma Editorial

Ruiz Quintero, A. (2016). Diseño de un plan de gestión de servicios en el área de sistemas y tecnologías de información de la Gobernación de Santander de acuerdo con las mejores practicas de ITIL. En *Carbohydrate Polymers* (Vol. 17, Número 1). Universidad Autónoma de Bucaramanga Facultad de Ingeniería De Sistemas Maestría En Telemática Bucaramanga.

Vargas Cordero, Z. R. (2009). La Investigación aplicada: Una forma de conocer las realidades con evidencia científica. *Revista Educación*, *33*(1), 155. https://doi.org/10.15517/revedu.v33i1.538

Vega Picon, G. E. (2018). Implementación de un sistema de monitoreo para el análisis de la disponibilidad, capacidad, calidad y latencia de enlaces corporativos de última Milla. En *Ecuador*. Universidad catolica de santiago de Guayaquil.

Velasco Briones, C. A., & Cagua Ordoñez, G. S. (2017). *Implementación De Un Sistema De Monitoreo De Redes Utilizando Herramientas Open Source Y Proveer Servicios De Directorio a Través De Active Directory En La Facultad De Filosofía, Letras Y Ciencias De La Educación De La Universidad De Guayaquil*. Univerdidad Politécnica Salesiana Sede Guayaquil.

ANEXOS

ANEXO 1: Matriz de consistencia

ANEXO 2: Ficha de observación.

ANEXO 3: Host y servicios monitoreados.

ANEXO 4: Reportes del sistema.

ANEXO 5: Declaración jurada de autenticidad de tesis

ANEXO 6: Autorización para el depósito de tesis en el repositorio institucional

ANEXO 1: Matriz de consistencia

IMPLEMENTACIÓN DE UN MODELO DE MONITOREO APLICANDO ITIL PARA MEJORAR LA DISPONIBILIDAD DE LOS SERVICIOS DE TIC DEL MINISTERIO DE EDUCACIÓN - LIMA.

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES	METODOLOGÍA
Problema general	**Objetivo general**	**Hipótesis general**	**Variable independiente:**	
¿En qué medida la implementación de un modelo de monitoreo aplicando ITIL 4 para mejorar la disponibilidad de los servicios de TIC del Ministerio de Educación en Lima?	Implementar un modelo de monitoreo aplicando ITIL 4 para mejorar la disponibilidad de los servicios de TIC de la Oficina de Tecnología de la información y comunicación del Ministerio de Educación en Lima.	A través de la implementación de un modelo de monitoreo aplicando ITIL 4 mejorará significativamente la disponibilidad de los servicios de TIC llevados a cabo por la Oficina de TIC del Ministerio de Educación Lima.	*Modelo de monitoreo aplicando ITIL basado en Nagios y Nagvis* **Indicadores:** - Tiempo para la detección del evento e incidencia. - Número de alertas de los servicios con la aplicación del modelo. - Medir la disponibilidad de los servicios TIC críticos.	**Método**: cuantitativo **Tipo de investigación:** Aplicada **Nivel de investigación:** Explicativo **Diseño de investigación:** cuasi-experimental. **Técnicas:** Observación directa Análisis documental **Instrumentos:** Cuestionarios Fichas de observación D = A/B x 100
Problema específico	**Objetivos Específicos**	**Hipótesis específicas**	**Variable dependiente:**	
¿De qué manera la identificación y diagnóstico de la situación actual de los servicios de TIC determinará los indicadores de disponibilidad de los servicios de TIC del Ministerio de Educación – Lima?	Identificar y analizar la situación actual de los servicios de TIC monitoreados y no monitoreados aplicando ITIL e identificar los indicadores de disponibilidad que serán sometidos al proceso de mejora. Implementar el modelo de monitoreo aplicando ITIL 4 para la detección de la degradación o interrupción de los servicios de TIC realizando las validaciones y pruebas. Validar la mejora del nivel de disponibilidad y el tiempo de detección de eventos e incidencias de los servicios de TIC, en el Ministerio de Educación con la implementación de un modelo de monitoreo aplicando ITIL 4 a través de la herramienta Nagios y Nagvis.	La identificación y análisis de los servicios de TIC críticos llevados a cabo por la Oficina de Tecnología de la información y comunicación del Ministerio de Educación permitirá determinar la mejora de la disponibilidad de los servicios de TIC, aplicando los principios de ITIL 4 del Ministerio de Educación en Lima. La implementación del modelo de monitoreo mediante la herramienta Nagios y Nagvis, aplicando ITIL 4, permitirá mejorar el tiempo de detección de eventos e incidencias, y notificarlos. La aplicación exitosa del modelo de monitoreo aplicando ITIL 4 mejoró el nivel de disponibilidad de los servicios TIC.	*Disponibilidad de los servicios de TIC del Ministerio de Educación - Lima.* - **Indicadores:** - Tiempo de detección de eventos en el servicio de TIC. - Cantidad de interrupción de los servicios de TIC monitoreado - Nivel de disponibilidad de los servicios de TIC - Tiempo de resolución de eventos e incidencias.	

ANEXO 2: Ficha de observación

Código:				VERSION: 1.2 FECHA APROBACIÓN: Propuesta 04/03/2022	
FICHA DE INCIDENCIA N°	005	- yyyy	MINEDU/SPE - OTIC - USAU		
1. Identificación					
A. N° Ticket	:	297655		Fecha:	15-02-2022
B. Nombre del Registrador	:				
C. Servicio involucrado		**servicio de internet**			
C.1 Servicio afectado	:	**acceso a la red**			
C.3 Propietario	:	*OTIC*			
C.4 Administrador	:	*OTIC - UIT*			
C.2 Sub Servicio 01	:	Ninguno			
C.3 Sub Servicio 02	:	Ninguno			
C.4 Sub Servicio 03	:	Ninguno			
C.4 Proceso Afectado	:	**Disponibilidad**			
D. Detalles de síntomas:					
Se presenta problemas con la conectividad de los swtich con el acceso del internet, acceso a la red en la zona L1 y L2 de la Sede Central,					
2. Elementos Involucrados, Prioridad y Escalamiento					
A. Elementos de la configuración afectados					
Recurso de T.I.	:				
01 SubClasificación de CI	:				
02 SubClasificación de CI	:				
03 SubClasificación de CI	:				
B. Nivel de Prioridad	:	Impacto:	Alto	Urgencia: Alto	= Critico
C. Escalado de solución	:				
3. Clasificación y Solución					
A. Categoría del incidente	:	**CRITICO**			
B. Nombre del Incidente	:	INCIDENCIA GRAVE			
C. Solución del Incidente	:	N° Ticket			
D. Tiempo Aproximado	:	10 min.			
4. Cambios					
Se utilizó una solución existente					
Se elaboró una nueva solución					

Registro de pruebas en los servicios de TIC antes del modelo.

ID	SERVICIO	FECHA DE OCURRENCIA	FECHA DE NOTIFICACIÓN	TIEMPO DE DETECCIÓN
1	**Servicio de red**	06/01/2022 11:18	10/01/2022 15:02	5984
2	**Servicio Web**	06/01/2022 0:00	07/01/2022 0:00	1440
3	**Servicio de red**	06/01/2022 0:00	07/01/2022 0:00	1440
4	**Servicio Web**	16/01/2022 0:00	17/01/2022 0:00	1440
5	**Servicio de red**	16/01/2022 0:00	17/01/2022 0:00	1440
6	**Servicio de correo**	17/01/2022 11:31	17/01/2022 15:31	240
7	**Servicio Web**	01/02/2022 11:31	04/02/2022 0:00	3600
8	**Servicio de red**	07/02/2022 0:00	07/02/2022 0:00	60
9	**Servicio Web**	16/02/2022 0:00	16/02/2022 0:00	29
10	**Servicio de red**	24/02/2022 0:00	24/02/2022 0:00	0
11	**Servicio Web**	24/02/2022 0:00	28/02/2022 0:00	5700
12	**Servicio de red**	01/03/2022 0:00	01/03/2022 0:00	0
13	**Servicio Web**	01/03/2022 0:00	02/03/2022 0:00	1440
14	**Servicio de red**	03/03/2022 0:00	03/03/2022 0:00	60
15	**Servicio de red**	03/03/2022 0:00	03/03/2022 0:00	0
16	**Servicio de red**	03/03/2022 0:00	03/03/2022 0:00	40
17	**Servicio de red**	03/03/2022 0:00	04/03/2022 0:00	1400
18	**Servicio de red**	14/03/2022 0:00	15/03/2022 0:00	1440
19	**Servicio de red**	14/03/2022 0:00	15/03/2022 0:00	1440
20	**Servicio de red**	15/03/2022 0:00	16/03/2022 17:00	2400
21	**Servicio Web**	05/04/2022 0:00	05/04/2022 0:00	60
22	**Servicio Web**	05/04/2022 0:00	05/04/2022 0:00	40
23	**Servicio de red**	06/04/2022 0:00	07/04/2022 15:00	2340
24	**Servicio de red**	11/04/2022 11:15	11/04/2022 17:45	390
25	**Servicio de red**	11/04/2022 11:15	11/04/2022 17:45	390
26	**Servicio de red**	11/04/2022 11:15	11/04/2022 17:45	390
27	**Servicio de red**	11/04/2022 12:19	11/04/2022 13:52	93
28	**Servicio de red**	12/04/2022 12:19	12/04/2022 13:52	93
29	**Servicio de red**	03/05/2022 11:02	03/05/2022 13:08	126
30	**Servicio de red**	30/05/2022 9:37	30/05/2022 12:04	147
31	**Servicio de red**	26/06/2022 0:00	27/06/2022 14:00	2280
32	**Servicio de red**	26/06/2022 0:00	27/06/2022 14:00	2280

33	**Servicio de red**	27/06/2022 8:00	27/06/2022 14:00	360
34	**Servicio de red**	29/06/2022 0:00	30/06/2022 8:05	1925
35	**Servicio de red**	13/12/2022 18:28	14/12/2022 0:28	360
36	**Servicio de red**	22/12/2022 19:57	23/12/2022 19:57	1440
37	**Servicio de red**	23/12/2022 8:26	23/12/2022 18:26	600
		PROMEDIO		**1158**

Nota: Registros de las bitácoras de incidencias.

Resultados de tiempo de detección de incidentes aplicando el modelo.

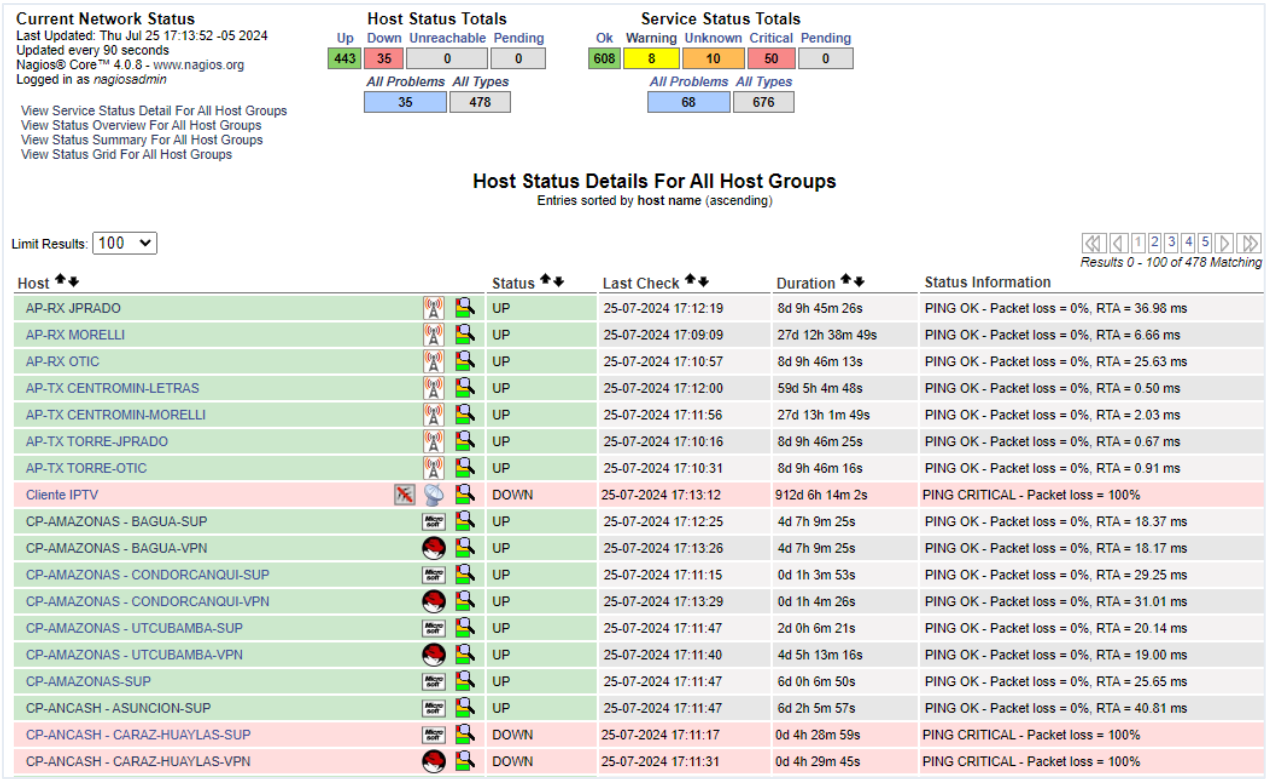
ID	SERVICIO	FECHA DE INTERRUPCIÓN	FECHA DE NOTIFICACIÓN	TIEMPO DE DETECCIÓN
1	**Servicio Web**	26/12/2022 21:15	26/12/2022 23:40	145
2	**Servicio Web**	23/12/2022 8:26	23/12/2022 8:26	6,54
3	**Servicio Web**	22/12/2022 19:57	22/12/2022 19:57	5,45
4	**Servicio de red**	19/12/2022 10:30	19/12/2022 10:59	29
5	**Servicio Web**	18/12/2022 10:30	18/12/2022 10:59	29
6	**Servicio de red**	18/12/2022 10:30	18/12/2022 10:59	29
7	**Servicio Web**	13/12/2022 18:28	13/12/2022 18:28	5,45
8	**Servicio de internet**	12/12/2022 11:31	12/12/2022 12:12	41
9	**Servicio de internet**	02/12/2022 0:00	02/12/2022 0:00	5,45
10	**Servicio de red**	30/11/2022 0:00	30/11/2022 0:00	5,45
11	**Servicio de red**	29/11/2022 0:00	29/11/2022 9:05	545
12	**Servicio de red**	28/11/2022 0:00	28/11/2022 0:00	5,45
13	**Servicio de red**	28/11/2022 0:00	30/11/2022 17:37	3937
14	**Servicio de red**	28/11/2022 0:00	28/11/2022 0:00	5,45
15	**Servicio de red**	17/11/2022 10:36	17/11/2022 11:00	24
16	**Servicio de red**	15/11/2022 11:00	15/11/2022 13:00	120
17	**Servicio Web**	14/11/2022 18:13	14/11/2022 22:13	240
18	**Servicio de red**	03/11/2022 7:06	03/11/2022 10:12	186
19	**Servicio de red**	26/10/2022 14:41	26/10/2022 15:08	27
20	**Servicio de red**	26/10/2022 0:00	26/10/2022 0:00	5,45
21	**Servicio de internet**	25/10/2022 0:00	25/10/2022 0:00	5,45
22	**Servicio de red**	25/10/2022 0:00	25/10/2022 0:00	0,54
23	**Servicio de red**	25/10/2022 0:00	26/10/2022 0:00	1440
24	**Servicio de red**	24/10/2022 0:00	24/10/2022 0:00	0,54
25	**Servicio de red**	20/10/2022 7:00	20/10/2022 9:00	120
26	**Servicio de red**	17/10/2022 7:50	17/10/2022 9:00	70

27	**Servicio de correo**	06/10/2022 10:26	06/10/2022 15:26	300
28	**Servicio de red**	19/09/2022 9:18	19/09/2022 9:20	2,00
29	**Servicio de red**	18/09/2022 19:47	18/09/2022 19:48	1,00
30	**Servicio de red**	18/09/2022 14:48	18/09/2022 14:56	8,00
31	**Servicio de red**	18/09/2022 14:27	18/09/2022 14:35	8,00
32	**Servicio Web**	18/09/2022 13:07	18/09/2022 13:14	7,00
33	**Servicio de red**	18/09/2022 12:40	18/09/2022 12:57	17,00
34	**Servicio de red**	18/09/2022 11:30	18/09/2022 11:39	9,00
35	**Servicio Web**	18/09/2022 10:02	18/09/2022 10:10	8,00
36	**Servicio de red**	18/09/2022 10:02	18/09/2022 10:13	11,00
37	**Servicio de red**	18/09/2022 9:55	18/09/2022 9:57	2,00
38	**Servicio de red**	18/09/2022 8:52	18/09/2022 9:00	8,00
39	**Servicio de red**	20/08/2022 12:18	20/08/2022 14:00	101,13
40	**Servicio de red**	18/08/2022 9:36	18/08/2022 11:15	99
41	**Servicio de red**	07/08/2022 16:09	07/08/2022 17:37	88,00
42	**Servicio Web**	03/08/2022 21:14	03/08/2022 21:28	14,00
43	**Servicio de red**	02/08/2022 1:06	02/08/2022 10:06	540
44	**Servicio de red**	30/07/2022 10:45	30/07/2022 15:46	301
45	**Servicio Web**	19/07/2022 7:59	19/07/2022 8:38	39
46	**Servicio Web**	18/07/2022 9:06	18/07/2022 9:30	24
47	**Servicio de red**	18/07/2022 9:05	18/07/2022 9:29	24
48	**Servicio de internet**	18/07/2022 8:42	18/07/2022 8:48	6,000
49	**Servicio de red**	18/07/2022 8:37	18/07/2022 8:41	4,000
50	**Servicio de red**	17/07/2022 15:31	17/07/2022 15:57	26,000
51	**Servicio de red**	17/07/2022 9:32	17/07/2022 9:37	5,000
52	**Servicio de red**	05/07/2022 0:00	05/07/2022 0:00	0,54
53	**Servicio de red**	04/07/2022 0:00	04/07/2022 0:10	10
		PROMEDIO		**164**

Nota: Registros de la herramienta Nagios.

ANEXO 3: Monitoreo de Hosts y Servicios

Al acceder a la pestaña "Hosts", se despliega una ventana que muestra una lista de todos los hosts monitoreados, con sus respectivos estados de conectividad. La siguiente imagen muestra un ejemplo de cómo se visualizan estos estados:



Current Network Status
Last Updated: Thu Jul 25 17:13:52 -05 2024
Updated every 90 seconds
Nagios® Core™ 4.0.8 - www.nagios.org
Logged in as *nagiosadmin*

View Service Status Detail For All Host Groups
View Status Overview For All Host Groups
View Status Summary For All Host Groups
View Status Grid For All Host Groups

Host Status Totals

Up	Down	Unreachable	Pending
443	35	0	0

All Problems	All Types
35	478

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
608	8	10	50	0

All Problems	All Types
68	676

Host Status Details For All Host Groups
Entries sorted by **host name** (ascending)

Limit Results: 100

Results 0 - 100 of 478 Matching

Host	Status	Last Check	Duration	Status Information
AP-RX JPRADO	UP	25-07-2024 17:12:19	8d 9h 45m 26s	PING OK - Packet loss = 0%, RTA = 36.98 ms
AP-RX MORELLI	UP	25-07-2024 17:09:09	27d 12h 38m 49s	PING OK - Packet loss = 0%, RTA = 6.66 ms
AP-RX OTIC	UP	25-07-2024 17:10:57	8d 9h 46m 13s	PING OK - Packet loss = 0%, RTA = 25.63 ms
AP-TX CENTROMIN-LETRAS	UP	25-07-2024 17:12:00	59d 5h 4m 48s	PING OK - Packet loss = 0%, RTA = 0.50 ms
AP-TX CENTROMIN-MORELLI	UP	25-07-2024 17:11:56	27d 13h 1m 49s	PING OK - Packet loss = 0%, RTA = 2.03 ms
AP-TX TORRE-JPRADO	UP	25-07-2024 17:10:16	8d 9h 46m 25s	PING OK - Packet loss = 0%, RTA = 0.67 ms
AP-TX TORRE-OTIC	UP	25-07-2024 17:10:31	8d 9h 46m 16s	PING OK - Packet loss = 0%, RTA = 0.91 ms
Cliente IPTV	DOWN	25-07-2024 17:13:12	912d 6h 14m 2s	PING CRITICAL - Packet loss = 100%
CP-AMAZONAS - BAGUA-SUP	UP	25-07-2024 17:12:25	4d 7h 9m 25s	PING OK - Packet loss = 0%, RTA = 18.37 ms
CP-AMAZONAS - BAGUA-VPN	UP	25-07-2024 17:13:26	4d 7h 9m 25s	PING OK - Packet loss = 0%, RTA = 18.17 ms
CP-AMAZONAS - CONDORCANQUI-SUP	UP	25-07-2024 17:11:15	0d 1h 3m 53s	PING OK - Packet loss = 0%, RTA = 29.25 ms
CP-AMAZONAS - CONDORCANQUI-VPN	UP	25-07-2024 17:13:29	0d 1h 4m 26s	PING OK - Packet loss = 0%, RTA = 31.01 ms
CP-AMAZONAS - UTCUBAMBA-SUP	UP	25-07-2024 17:11:47	2d 0h 6m 21s	PING OK - Packet loss = 0%, RTA = 20.14 ms
CP-AMAZONAS - UTCUBAMBA-VPN	UP	25-07-2024 17:11:40	4d 5h 13m 16s	PING OK - Packet loss = 0%, RTA = 19.00 ms
CP-AMAZONAS-SUP	UP	25-07-2024 17:11:47	6d 0h 6m 50s	PING OK - Packet loss = 0%, RTA = 25.65 ms
CP-ANCASH - ASUNCION-SUP	UP	25-07-2024 17:11:47	6d 2h 5m 57s	PING OK - Packet loss = 0%, RTA = 40.81 ms
CP-ANCASH - CARAZ-HUAYLAS-SUP	DOWN	25-07-2024 17:11:17	0d 4h 28m 59s	PING CRITICAL - Packet loss = 100%
CP-ANCASH - CARAZ-HUAYLAS-VPN	DOWN	25-07-2024 17:11:31	0d 4h 29m 45s	PING CRITICAL - Packet loss = 100%

SUP (CP-APURIMAC)

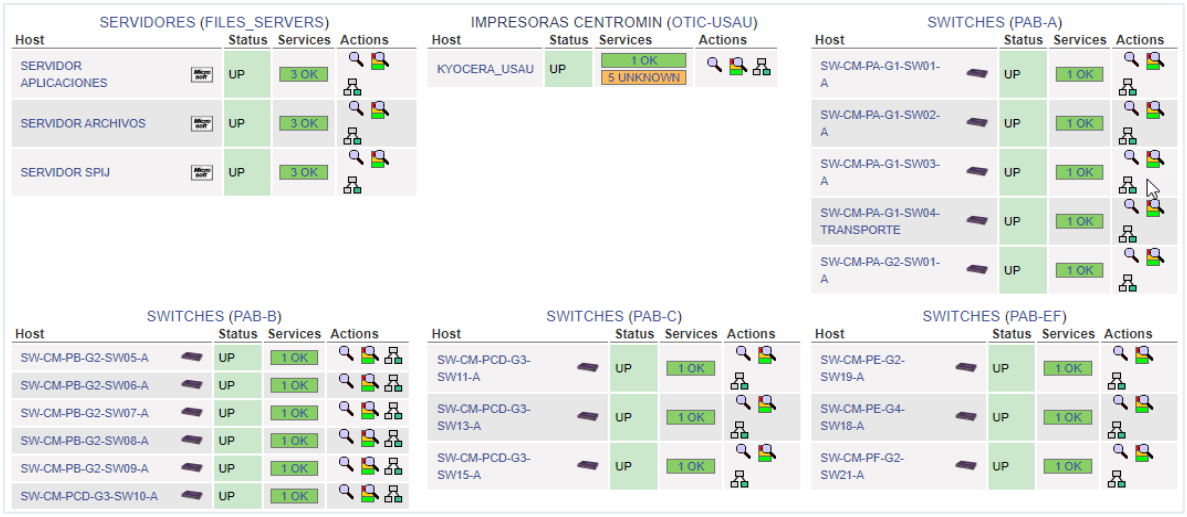
Host	Status	Services	Actions
CP-APURIMAC - ABANCAY-SUP	UP	2 OK	
CP-APURIMAC - ABANCAY-VPN	UP	1 OK	
CP-APURIMAC - ANDAHUAYLAS-SUP	UP	2 OK	
CP-APURIMAC - ANDAHUAYLAS-VPN	UP	1 OK	
CP-APURIMAC - ANTABAMBA-SUP	UP	2 OK	
CP-APURIMAC - AYMARAES-SUP	UP	2 OK	
CP-APURIMAC - AYMARAES-VPN	UP	1 OK	
CP-APURIMAC - CHINCHEROS-SUP	UP	2 OK	
CP-APURIMAC - CHINCHEROS-VPN	UP	1 OK	
CP-APURIMAC - COTABAMBAS-SUP	UP	2 OK	
CP-APURIMAC - COTABAMBAS-VPN	UP	1 OK	
CP-APURIMAC - GRAU-SUP	UP	2 OK	
CP-APURIMAC - GRAU-VPN	UP	1 OK	

SUP (CP-AREQUIPA)

Host	Status	Services	Actions
CP-AREQUIPA - AREQUIPA NORTE-SUP	UP	2 OK	
CP-AREQUIPA - AREQUIPA NORTE-VPN	UP	1 OK	
CP-AREQUIPA - AREQUIPA SUR-SUP	UP	2 OK	
CP-AREQUIPA - AREQUIPA SUR-VPN	UP	1 OK	
CP-AREQUIPA - CAMANA-SUP	UP	2 OK	
CP-AREQUIPA - CARAVELI-SUP	UP	2 OK	
CP-AREQUIPA - CARAVELI-VPN	UP	1 OK	
CP-AREQUIPA - CASTILLA-SUP	UP	2 OK	
CP-AREQUIPA - CASTILLA-VPN	UP	1 OK	
CP-AREQUIPA - CAYLLOMA-SUP	UP	2 OK	
CP-AREQUIPA - CONDESUYOS-SUP	UP	2 OK	
CP-AREQUIPA - CONDESUYOS-VPN	UP	1 OK	
CP-AREQUIPA - ISLAY-	UP	2 OK	

SUP (CP-AYACUCHO)

Host	Status	Services	Actions
CP-AYACUCHO - CANGALLO-SUP	UP	2 OK	
CP-AYACUCHO - CANGALLO-VPN	UP	1 OK	
CP-AYACUCHO - FAJARDO-SUP	UP	2 OK	
CP-AYACUCHO - FAJARDO-VPN	UP	1 OK	
CP-AYACUCHO - HUAMANGA-SUP	UP	2 OK	
CP-AYACUCHO - HUAMANGA-VPN	UP	1 OK	
CP-AYACUCHO - HUANCASANCOS-SUP	UP	2 OK	
CP-AYACUCHO - HUANCASANCOS-VPN	UP	1 OK	
CP-AYACUCHO - HUANTA-SUP	UP	2 OK	
CP-AYACUCHO - HUANTA-VPN	UP	1 OK	
CP-AYACUCHO - LA MAR-SUP	UP	2 OK	
CP-AYACUCHO - LA MAR-VPN	UP	1 OK	
CP-AYACUCHO -	UP	2 OK	



SERVIDORES (FILES_SERVERS)

Host	Status	Services	Actions
SERVIDOR APLICACIONES	UP	3 OK	
SERVIDOR ARCHIVOS	UP	3 OK	
SERVIDOR SPIJ	UP	3 OK	

IMPRESORAS CENTROMIN (OTIC-USAU)

Host	Status	Services	Actions
KYOCERA_USAU	UP	1 OK 5 UNKNOWN	

SWITCHES (PAB-A)

Host	Status	Services	Actions
SW-CM-PA-G1-SW01-A	UP	1 OK	
SW-CM-PA-G1-SW02-A	UP	1 OK	
SW-CM-PA-G1-SW03-A	UP	1 OK	
SW-CM-PA-G1-SW04-TRANSPORTE	UP	1 OK	
SW-CM-PA-G2-SW01-A	UP	1 OK	

SWITCHES (PAB-B)

Host	Status	Services	Actions
SW-CM-PB-G2-SW05-A	UP	1 OK	
SW-CM-PB-G2-SW06-A	UP	1 OK	
SW-CM-PB-G2-SW07-A	UP	1 OK	
SW-CM-PB-G2-SW08-A	UP	1 OK	
SW-CM-PB-G2-SW09-A	UP	1 OK	
SW-CM-PCD-G3-SW10-A	UP	1 OK	

SWITCHES (PAB-C)

Host	Status	Services	Actions
SW-CM-PCD-G3-SW11-A	UP	1 OK	
SW-CM-PCD-G3-SW13-A	UP	1 OK	
SW-CM-PCD-G3-SW15-A	UP	1 OK	

SWITCHES (PAB-EF)

Host	Status	Services	Actions
SW-CM-PE-G2-SW19-A	UP	1 OK	
SW-CM-PE-G4-SW18-A	UP	1 OK	
SW-CM-PF-G2-SW21-A	UP	1 OK	

RADIO-ENLACE (RADIO-ENLACES)

Host	Status	Services	Actions
AP-RX JPRADO	UP	1 OK	
AP-RX MORELLI	UP	1 OK	
AP-RX OTIC	UP	1 OK	
AP-TX CENTROMIN-LETRAS	UP	1 OK	
AP-TX CENTROMIN-MORELLI	UP	1 OK	
AP-TX TORRE-JPRADO	UP	1 OK	
AP-TX TORRE-OTIC	UP	1 OK	

SWITCHES (SEDE-CENTRAL)

Host	Status	Services	Actions
SW-A-P01-G1-SW01-A	UP	1 OK	
SW-A-P01-G1-SW02-A	UP	1 OK	
SW-A-P02-G1-SW01-A	UP	1 OK	
SW-A-P02-G1-SW02-A	UP	1 OK	
SW-A-P03-G1-SW01-A	UP	1 OK	
SW-A-P03-G1-SW02-A	UP	1 OK	
SW-A-P04-G1-SW01-A	UP	1 OK	
SW-A-P05-G1-SW01-A	UP	1 OK	
SW-A-P05-G1-SW02-A	UP	1 OK	
SW-A-P06-G1-SW01-A	UP	1 OK	
SW-A-P06-G1-SW02-A	UP	1 OK	
SW-A-P07-G1-SW01-A	UP	1 OK	

SWITCHES (SEDE-GUARDIA-CIVIL)

Host	Status	Services	Actions
SW-GUARD-PISO1-SW1-A	UP	1 OK	
SW-GUARD-PISO1-SW2-A	UP	1 OK	
SW-GUARD-PISO2-SW1-A	UP	1 OK	
SW-GUARD-PISO2-SW2-A	UP	1 OK	
SW-GUARD-SOTA-SW1	UP	1 OK	
SW-GUARDIA-GAB1-SW01-A	UP	1 OK	

WEB (URL)

Host	Status	Services	Actions
PBX ELASTIX	UP	7 OK	
URL ADMISION COAR	UP	1 OK	
URL AMP DE COBERTURA - TRANSITO	UP	2 OK	
URL AULAVIRTUAL	UP	2 OK	
URL AVANZA	UP	1 OK	
URL CNE	UP	1 OK	
URL COAR	UP	2 OK	
URL COAR-KOHA	UP	1 OK	
URL CONECTA	UP	1 OK	
URL CONFIGURACIONES	UP	1 OK	
URL CONOCEMAS	UP	1 OK	
URL CONSULTA DE TITULOS	UP	1 OK	

VPN LINUX (VPN-SEDES-LIMA-METROPOLITANA)

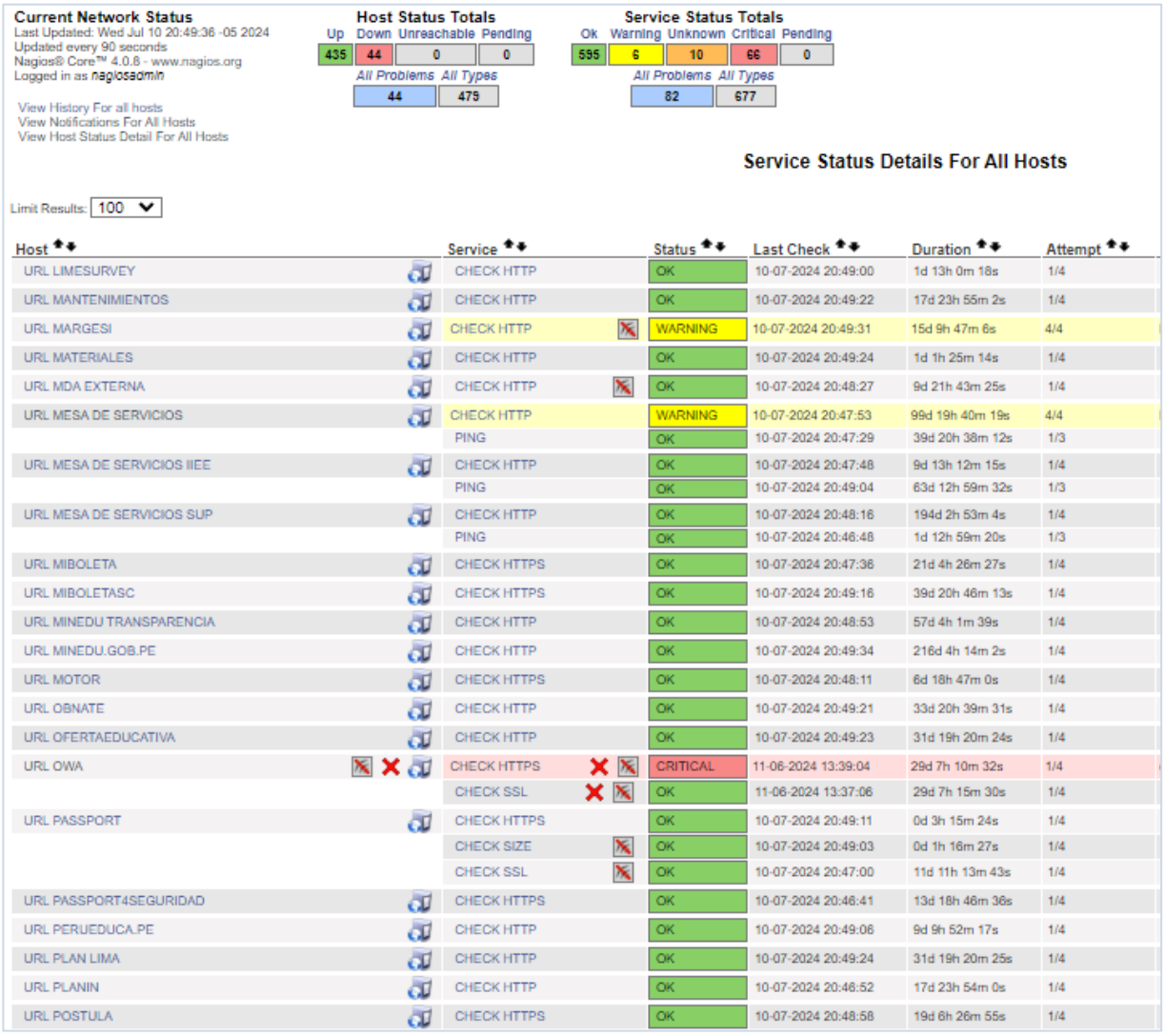
Host	Status	Services	Actions
SEDE-LURIN	UP	1 OK	

SWITCHES (ZONA-L1L2)

Host	Status	Services	Actions
SW-L-ZONEA-G2-SW01-A	UP	1 OK	
SW-L-ZONEA-G2-SW02-A	UP	1 OK	
SW-L-ZONEA-G2-SW03-A	UP	1 OK	
SW-L-ZONEA-G2-SW04-A	UP	1 OK	
SW-L-ZONEA-G2-SW05-A	UP	1 OK	
SW-L-ZONEA-G3-SW02-ADIC-3	UP	1 OK	
SW-L-ZONEB-G1-SW01-A	UP	1 OK	
SW-L-ZONEB-G2-SW01-A	UP	1 OK	
SW-L-ZONEB-G2-SW01-ADIC-1	UP	1 OK	
SW-L-ZONEC-G1-SW01-A	UP	1 OK	
SW-L-ZONEC-G1-SW02-A	UP	1 OK	
SW-L-ZONEC-G2-P2-A	UP	1 OK	

Los servicios monitoreados en red

Al acceder a la pestaña pestaña "Servicie" presenta una lista completa de los servicios monitoreados por cada host, incluyendo su estado de conectividad. Los estados se representan con colores: verde para "OK" y rojo para "DOWN", como se puede observar en las imágenes siguientes.



Current Network Status
Last Updated: Wed Jul 10 20:49:36 -05 2024
Updated every 90 seconds
Nagios® Core™ 4.0.8 - www.nagios.org
Logged in as *nagiosadmin*

View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
435	44	0	0

All Problems	All Types
44	479

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
595	6	10	66	0

All Problems	All Types
82	677

Service Status Details For All Hosts

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt
URL LIMESURVEY	CHECK HTTP	OK	10-07-2024 20:49:00	1d 13h 0m 18s	1/4
URL MANTENIMIENTOS	CHECK HTTP	OK	10-07-2024 20:49:22	17d 23h 55m 2s	1/4
URL MARGESI	CHECK HTTP	WARNING	10-07-2024 20:49:31	15d 9h 47m 6s	4/4
URL MATERIALES	CHECK HTTP	OK	10-07-2024 20:49:24	1d 1h 25m 14s	1/4
URL MDA EXTERNA	CHECK HTTP	OK	10-07-2024 20:48:27	9d 21h 43m 25s	1/4
URL MESA DE SERVICIOS	CHECK HTTP	WARNING	10-07-2024 20:47:53	99d 19h 40m 19s	4/4
	PING	OK	10-07-2024 20:47:29	39d 20h 38m 12s	1/3
URL MESA DE SERVICIOS IIEE	CHECK HTTP	OK	10-07-2024 20:47:48	9d 13h 12m 15s	1/4
	PING	OK	10-07-2024 20:49:04	63d 12h 59m 32s	1/3
URL MESA DE SERVICIOS SUP	CHECK HTTP	OK	10-07-2024 20:48:16	194d 2h 53m 4s	1/4
	PING	OK	10-07-2024 20:46:48	1d 12h 59m 20s	1/3
URL MIBOLETA	CHECK HTTPS	OK	10-07-2024 20:47:36	21d 4h 26m 27s	1/4
URL MIBOLETASC	CHECK HTTPS	OK	10-07-2024 20:49:16	39d 20h 46m 13s	1/4
URL MINEDU TRANSPARENCIA	CHECK HTTP	OK	10-07-2024 20:48:53	57d 4h 1m 39s	1/4
URL MINEDU.GOB.PE	CHECK HTTP	OK	10-07-2024 20:49:34	216d 4h 14m 2s	1/4
URL MOTOR	CHECK HTTPS	OK	10-07-2024 20:48:11	6d 18h 47m 0s	1/4
URL OBNATE	CHECK HTTP	OK	10-07-2024 20:49:21	33d 20h 39m 31s	1/4
URL OFERTAEDUCATIVA	CHECK HTTP	OK	10-07-2024 20:49:23	31d 19h 20m 24s	1/4
URL OWA	CHECK HTTPS	CRITICAL	11-06-2024 13:39:04	29d 7h 10m 32s	1/4
	CHECK SSL	OK	11-06-2024 13:37:06	29d 7h 15m 30s	1/4
URL PASSPORT	CHECK HTTPS	OK	10-07-2024 20:49:11	0d 3h 15m 24s	1/4
	CHECK SIZE	OK	10-07-2024 20:49:03	0d 1h 16m 27s	1/4
	CHECK SSL	OK	10-07-2024 20:47:00	11d 11h 13m 43s	1/4
URL PASSPORT4SEGURIDAD	CHECK HTTPS	OK	10-07-2024 20:46:41	13d 18h 46m 36s	1/4
URL PERUEDUCA.PE	CHECK HTTP	OK	10-07-2024 20:49:06	9d 9h 52m 17s	1/4
URL PLAN LIMA	CHECK HTTP	OK	10-07-2024 20:49:24	31d 19h 20m 25s	1/4
URL PLANIN	CHECK HTTP	OK	10-07-2024 20:46:52	17d 23h 54m 0s	1/4
URL POSTULA	CHECK HTTPS	OK	10-07-2024 20:48:58	19d 6h 26m 55s	1/4

ANEXO 4: Reportes del sistema

Reportes de disponibilidad

Este tipo de reporte ofrece un registro completo de los cambios de estado de los equipos y sus servicios. Se muestra el momento en que cada estado comenzó, terminó y cuánto tiempo duró.

Hostgroup 'URL' Host State Breakdowns:

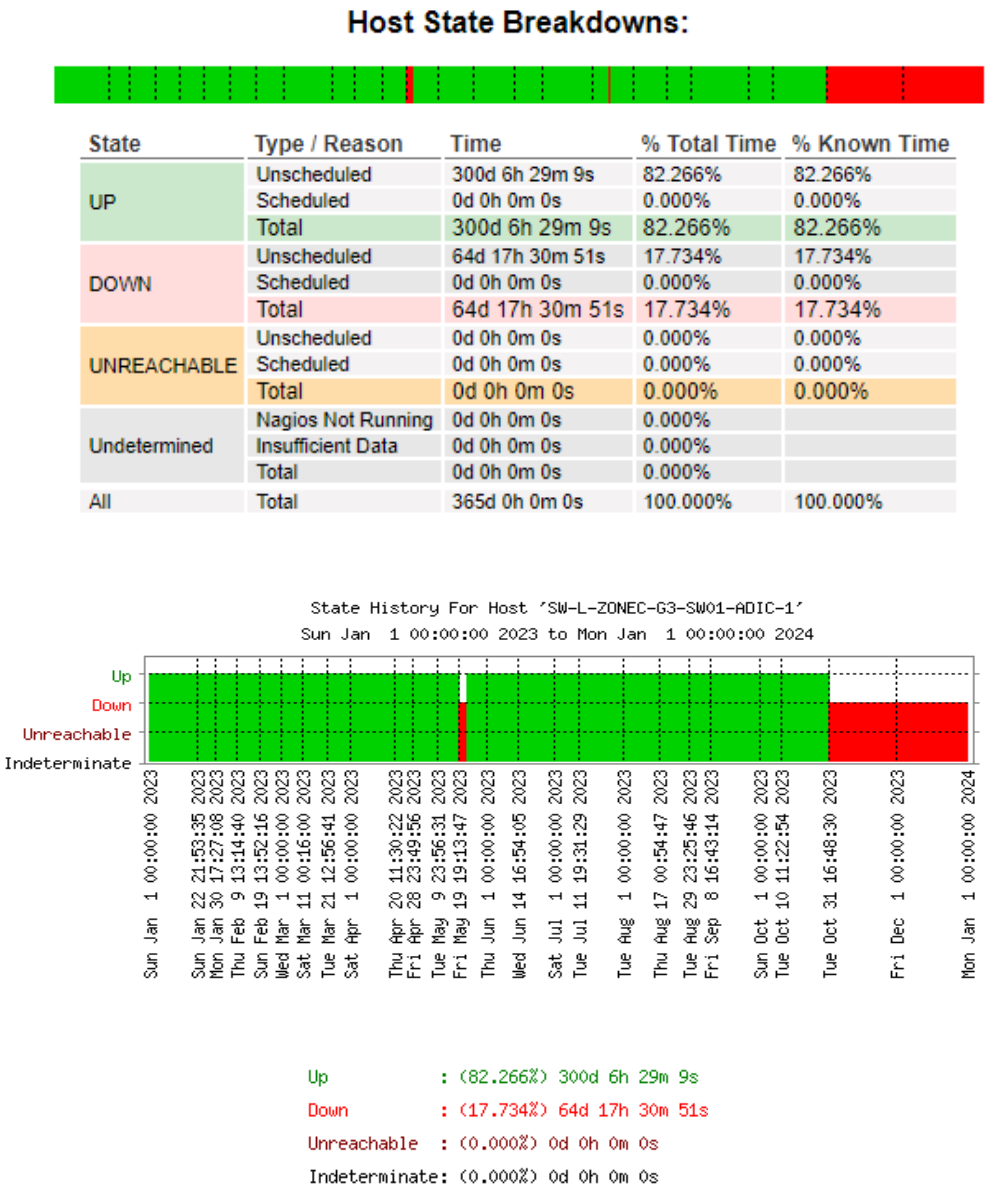
Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
PBX ELASTIX	99.761% (99.761%)	0.239% (0.239%)	0.000% (0.000%)	0.000%
URL ADMISION COAR	99.785% (99.785%)	0.215% (0.215%)	0.000% (0.000%)	0.000%
URL AMP DE COBERTURA - TRANSITO	99.771% (99.771%)	0.229% (0.229%)	0.000% (0.000%)	0.000%
URL AULAVIRTUAL	99.713% (99.713%)	0.287% (0.287%)	0.000% (0.000%)	0.000%
URL AVANZA	99.786% (99.786%)	0.214% (0.214%)	0.000% (0.000%)	0.000%
URL CNE	99.785% (99.785%)	0.215% (0.215%)	0.000% (0.000%)	0.000%
URL COAR	99.786% (99.786%)	0.214% (0.214%)	0.000% (0.000%)	0.000%
URL COAR-KOHA	99.785% (99.785%)	0.215% (0.215%)	0.000% (0.000%)	0.000%
URL CONECTA	99.787% (99.787%)	0.213% (0.213%)	0.000% (0.000%)	0.000%
URL CONFIGURACIONES	99.786% (99.786%)	0.214% (0.214%)	0.000% (0.000%)	0.000%
URL CONOCEMAS	99.785% (99.785%)	0.215% (0.215%)	0.000% (0.000%)	0.000%
URL CONSULTA DE TITULOS	99.790% (99.790%)	0.210% (0.210%)	0.000% (0.000%)	0.000%
URL CONSULTA RENIEC	99.704% (99.704%)	0.296% (0.296%)	0.000% (0.000%)	0.000%
URL DECLARACION DE GASTOS	99.771% (99.771%)	0.229% (0.229%)	0.000% (0.000%)	0.000%
URL E-SINADMED_1	99.784% (99.784%)	0.216% (0.216%)	0.000% (0.000%)	0.000%
URL E-SINADMED_2	99.785% (99.785%)	0.215% (0.215%)	0.000% (0.000%)	0.000%
URL E-SINADMED_3	99.783% (99.783%)	0.217% (0.217%)	0.000% (0.000%)	0.000%
URL E-SINADMED_4	99.783% (99.783%)	0.217% (0.217%)	0.000% (0.000%)	0.000%
URL E-SINADMED_5	99.784% (99.784%)	0.216% (0.216%)	0.000% (0.000%)	0.000%
URL E-SINADMED_6	99.784% (99.784%)	0.216% (0.216%)	0.000% (0.000%)	0.000%
URL E-SINADMED_7	99.784% (99.784%)	0.216% (0.216%)	0.000% (0.000%)	0.000%
URL E-SINADMED_8	99.784% (99.784%)	0.216% (0.216%)	0.000% (0.000%)	0.000%
URL EBUZON	99.787% (99.787%)	0.213% (0.213%)	0.000% (0.000%)	0.000%
URL ENLINEA	99.752% (99.752%)	0.248% (0.248%)	0.000% (0.000%)	0.000%
URL ESCALAFON	99.770% (99.770%)	0.230% (0.230%)	0.000% (0.000%)	0.000%
URL ESCALE	99.753% (99.753%)	0.247% (0.247%)	0.000% (0.000%)	0.000%
URL ESTADISTICA-ONLINE	99.784% (99.784%)	0.216% (0.216%)	0.000% (0.000%)	0.000%
URL EVALUACION DOCENTE	99.930% (99.930%)	0.070% (0.070%)	0.000% (0.000%)	0.000%
URL FORMACION EN SERVICIO	99.930% (99.930%)	0.070% (0.070%)	0.000% (0.000%)	0.000%
URL HAKUYACHAQ	99.753% (99.753%)	0.247% (0.247%)	0.000% (0.000%)	0.000%

Hostgroup 'CENTROMIN' Host State Breakdowns:

Host	% Time Up	% Time Down	% Time Unreachable	% Time Undetermined
SW-CM-PA-G1-SW01-A	99.745% (99.745%)	0.255% (0.255%)	0.000% (0.000%)	0.000%
SW-CM-PA-G1-SW02-A	99.744% (99.744%)	0.256% (0.256%)	0.000% (0.000%)	0.000%
SW-CM-PA-G1-SW03-A	99.751% (99.751%)	0.249% (0.249%)	0.000% (0.000%)	0.000%
SW-CM-PA-G1-SW04-TRANSPORTE	99.751% (99.751%)	0.249% (0.249%)	0.000% (0.000%)	0.000%
SW-CM-PA-G2-SW01-A	99.751% (99.751%)	0.249% (0.249%)	0.000% (0.000%)	0.000%
SW-CM-PB-G2-SW05-A	99.713% (99.713%)	0.287% (0.287%)	0.000% (0.000%)	0.000%
SW-CM-PB-G2-SW06-A	99.708% (99.708%)	0.292% (0.292%)	0.000% (0.000%)	0.000%
SW-CM-PB-G2-SW07-A	99.725% (99.725%)	0.275% (0.275%)	0.000% (0.000%)	0.000%
SW-CM-PB-G2-SW08-A	99.706% (99.706%)	0.294% (0.294%)	0.000% (0.000%)	0.000%
SW-CM-PB-G2-SW09-A	99.665% (99.665%)	0.335% (0.335%)	0.000% (0.000%)	0.000%
SW-CM-PCD-G3-SW10-A	99.596% (99.596%)	0.404% (0.404%)	0.000% (0.000%)	0.000%
SW-CM-PCD-G3-SW11-A	99.595% (99.595%)	0.405% (0.405%)	0.000% (0.000%)	0.000%
SW-CM-PCD-G3-SW12-A	99.598% (99.598%)	0.402% (0.402%)	0.000% (0.000%)	0.000%
SW-CM-PCD-G3-SW13-A	99.591% (99.591%)	0.409% (0.409%)	0.000% (0.000%)	0.000%
SW-CM-PCD-G3-SW15-A	99.603% (99.603%)	0.397% (0.397%)	0.000% (0.000%)	0.000%
SW-CM-PCD-G3-SW16-A	99.598% (99.598%)	0.402% (0.402%)	0.000% (0.000%)	0.000%
SW-CM-PE-G2-SW19-A	99.685% (99.685%)	0.315% (0.315%)	0.000% (0.000%)	0.000%
SW-CM-PE-G4-SW18-A	99.678% (99.678%)	0.322% (0.322%)	0.000% (0.000%)	0.000%
SW-CM-PF-G2-SW21-A	99.665% (99.665%)	0.335% (0.335%)	0.000% (0.000%)	0.000%
Average	99.677% (99.677%)	0.323% (0.323%)	0.000% (0.000%)	0.000%

Reportes de tendencias

Este reporte se visualiza las tendencias en los tiempos de respuesta de los hosts y servicios mediante una gráfica. Las barras de colores (marrón, verde y rojo) en la imagen inferior representan los cambios en el comportamiento de los estados.



Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	300d 6h 29m 9s	82.266%	82.266%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	300d 6h 29m 9s	82.266%	82.266%
DOWN	Unscheduled	64d 17h 30m 51s	17.734%	17.734%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	64d 17h 30m 51s	17.734%	17.734%
UNREACHABLE	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	365d 0h 0m 0s	100.000%	100.000%

Al pasar el cursor sobre las áreas coloreadas en verde, marrón o rojo, en función del estado del host, se desplegará una ventana emergente similar a la mostrada en la imagen inferior. Dicha ventana muestra la fecha de definición del host, su período de actividad y la información del estado.

UP
Time Range: *Fri Dec 1 00:00:00 2023* **to** *Thu Dec 7 00:23:00 2023*
Duration: *6d 0h 23m 0s*
State Info: *PING OK - Packet loss = 0%, RTA = 0.52 ms*

Reportes de alertas

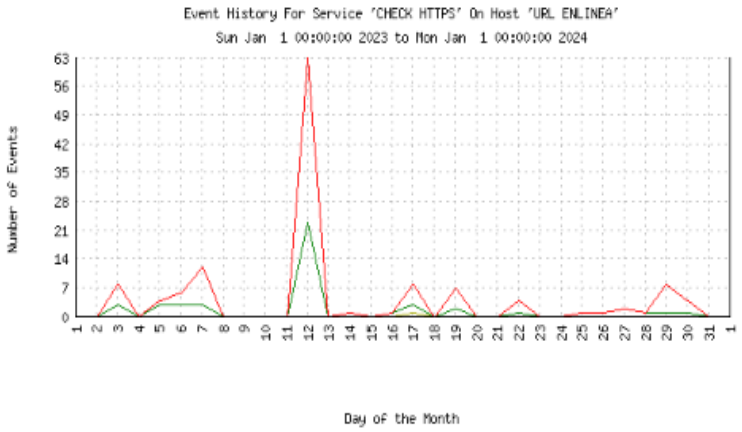
Las alertas se clasifican por fechas y se estructuran en periodos de una hora. El historial completo puede visualizarse ordenado cronológicamente por fechas y horas, o filtrarse según la preferencia del host seleccionado, tal como se muestra en las siguientes imágenes:

Displaying most recent 25 of 4358 total matching alerts

Time	Alert Type	Host	Service	State	State Type	Information
10-07-2024 19:07:27	Host Alert	CP-ANCASH - HUARMEY-SUP	N/A	DOWN	HARD	PING CRITICAL - Packet loss = 100%
10-07-2024 19:07:13	Service Alert	CP-ANCASH - HUARMEY-SUP	PING	CRITICAL	HARD	PING CRITICAL - Packet loss = 100%
10-07-2024 19:06:57	Service Alert	CP-ANCASH - HUARMEY-SUP	TCP	CRITICAL	HARD	CRITICAL - Socket timeout after 10 seconds
10-07-2024 18:51:46	Service Alert	CP-CAJAMARCA - SAN IGNACIO-SUP	TCP	CRITICAL	HARD	connect to address 172.16.34.5 and port 5000: No route to h
10-07-2024 18:51:24	Service Alert	CP-CAJAMARCA - SAN IGNACIO-SUP	PING	CRITICAL	HARD	CRITICAL - Host Unreachable (172.16.34.5)
10-07-2024 18:49:49	Host Alert	CP-CAJAMARCA - SAN IGNACIO-SUP	N/A	DOWN	HARD	CRITICAL - Host Unreachable (172.16.34.5)
10-07-2024 18:14:01	Host Alert	CP-AMAZONAS - CONDORCANQUI-SUP	N/A	UP	HARD	PING OK - Packet loss = 0%, RTA = 28.32 ms
10-07-2024 18:12:59	Host Alert	CP-AMAZONAS - CONDORCANQUI-SUP	N/A	DOWN	HARD	CRITICAL - Host Unreachable (172.31.218.3)
10-07-2024 17:41:20	Service Alert	CP-AYACUCHO - SUCRE-VPN	PING	OK	HARD	PING OK - Packet loss = 0%, RTA = 40.53 ms
10-07-2024 17:37:20	Service Alert	CP-AYACUCHO - SUCRE-VPN	PING	WARNING	HARD	PING WARNING - Packet loss = 0%, RTA = 252.78 ms
10-07-2024 17:36:11	Host Alert	CP-CAJAMARCA - SAN PABLO-SUP	N/A	DOWN	HARD	PING CRITICAL - Packet loss = 100%
10-07-2024 17:36:10	Service Alert	CP-CAJAMARCA - SAN PABLO-SUP	PING	CRITICAL	HARD	PING CRITICAL - Packet loss = 100%
10-07-2024 17:35:41	Service Alert	CP-CAJAMARCA - SAN PABLO-SUP	TCP	CRITICAL	HARD	CRITICAL - Socket timeout after 10 seconds
10-07-2024 17:34:53	Service Alert	CP-AREQUIPA - LA UNION-SUP	PING	OK	HARD	PING OK - Packet loss = 0%, RTA = 130.70 ms
10-07-2024 17:32:54	Service Alert	CP-AREQUIPA - LA UNION-SUP	PING	WARNING	HARD	PING WARNING - Packet loss = 16%, RTA = 295.61 ms
10-07-2024 17:29:04	Service Alert	CP-AYACUCHO-SUP	PING	OK	HARD	PING OK - Packet loss = 16%, RTA = 9.83 ms
10-07-2024 17:28:46	Host Alert	CP-AYACUCHO-SUP	N/A	UP	HARD	PING OK - Packet loss = 0%, RTA = 9.76 ms
10-07-2024 17:28:41	Service Alert	CP-AYACUCHO-SUP	TCP	OK	HARD	TCP OK - 3.018 second response time on 10.15.1.4 port 500
10-07-2024 17:26:46	Service Alert	CP-APURIMAC - GRAU-SUP	PING	OK	HARD	PING OK - Packet loss = 0%, RTA = 51.88 ms
10-07-2024 17:26:42	Service Alert	CP-AYACUCHO - SUCRE-SUP	PING	OK	HARD	PING OK - Packet loss = 0%, RTA = 90.53 ms
10-07-2024 17:25:11	Service Alert	CP-CAJAMARCA - CELENDIN-SUP	PING	CRITICAL	HARD	PING CRITICAL - Packet loss = 100%
10-07-2024 17:24:49	Service Alert	CP-APURIMAC - GRAU-SUP	PING	WARNING	HARD	PING WARNING - Packet loss = 37%, RTA = 53.04 ms
10-07-2024 17:24:49	Service Alert	CP-CAJAMARCA - CELENDIN-VPN	PING	CRITICAL	HARD	PING CRITICAL - Packet loss = 100%
10-07-2024 17:24:41	Host Alert	CP-CAJAMARCA - CELENDIN-SUP	N/A	DOWN	HARD	PING CRITICAL - Packet loss = 100%
10-07-2024 17:24:35	Service Alert	CP-CAJAMARCA - CELENDIN-SUP	TCP	CRITICAL	HARD	CRITICAL - Socket timeout after 10 seconds

Histogramas

Los histogramas proporcionan una representación visual del comportamiento de los estados de los hosts y servicios, mostrando su evolución hasta la fecha actual.



EVENT TYPE	MIN	MAX	SUM	AVG
Recovery (OK):	0	23	50	1.61
Warning:	0	1	1	0.03
Unknown:	0	0	0	0.00
Critical:	0	63	131	4.23

Según el tiempo seleccionado para evaluar el comportamiento del estado de los hosts y servicios, siempre se considera desde la fecha y hora actual del servidor Nagios hacia atrás.

Notificaciones

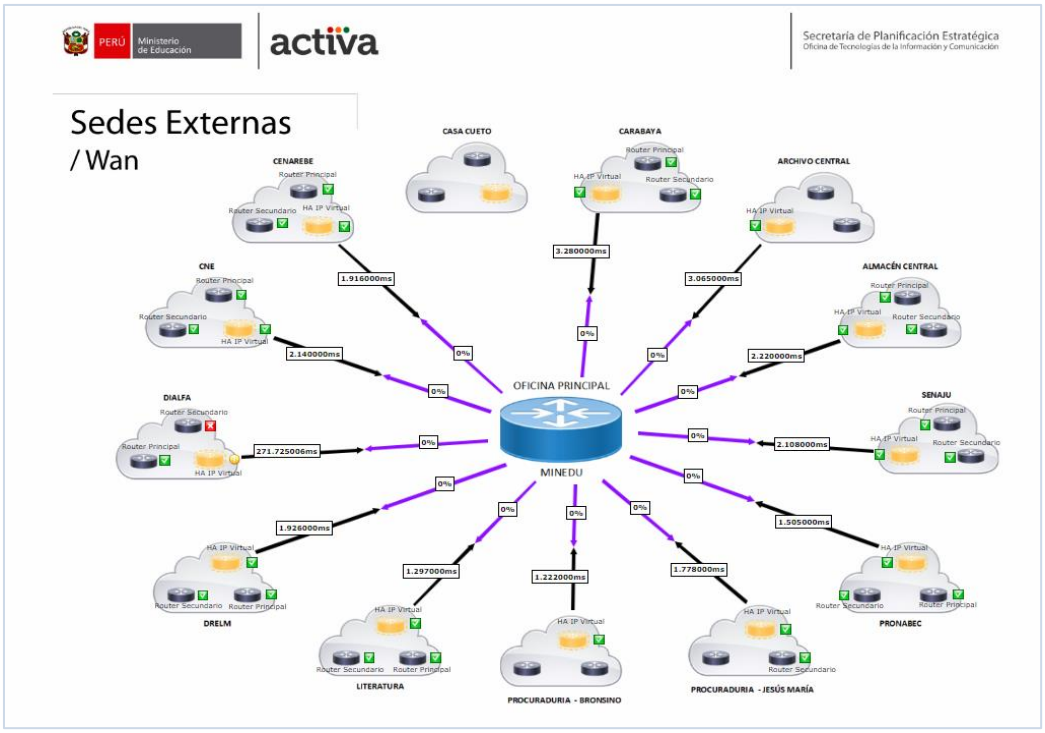
Las notificaciones muestran la lista de hosts y sus servicios, incluyendo el estado actual, la fecha y hora del último chequeo, el contacto responsable de la configuración y la información específica que el plugin proporciona sobre el estado del host o servicio, incluyendo la información que se enviará por correo electrónico.

File: /usr/local/nagios/var/nagios.log

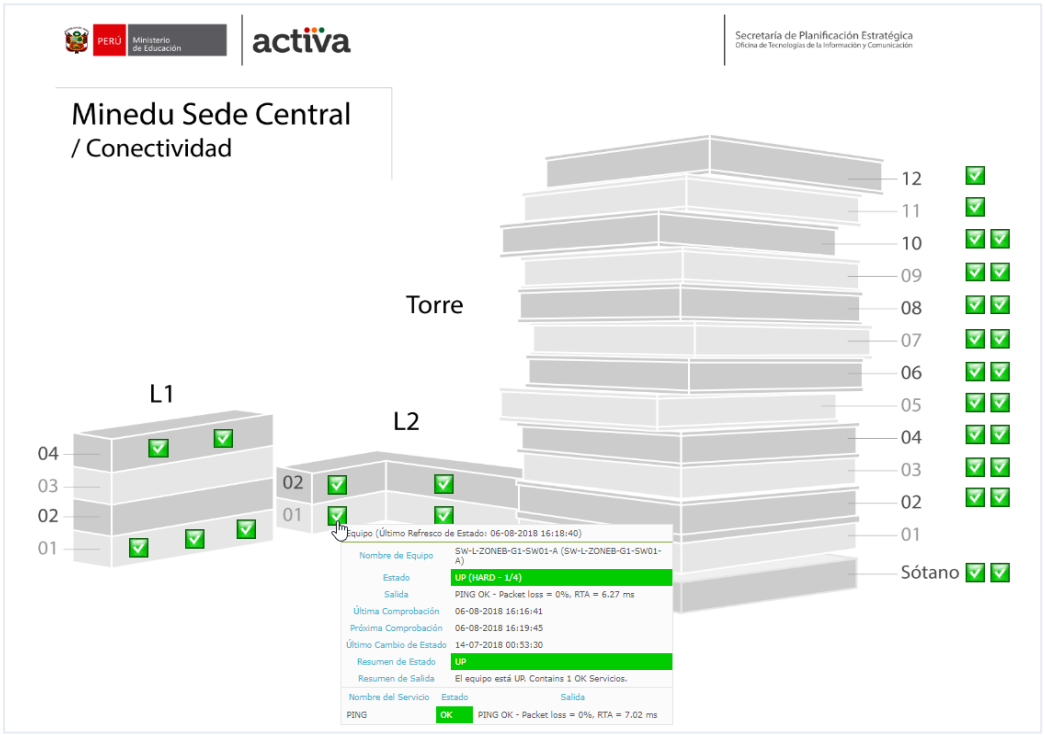
Host	Service	Type	Contact	Notification Command	Information
CP-CAJAMARCA - CAJABAMBA-SUP	N/A	HOST DOWN	mesadeayuda	notify-host-by-email	PING CRITICAL - Packet loss = 100%
CP-CAJAMARCA - CAJABAMBA-SUP	N/A	HOST DOWN	usrsup	notify-host-by-email	PING CRITICAL - Packet loss = 100%
CP-CAJAMARCA - CAJABAMBA-SUP	N/A	HOST DOWN	nagiosadmin	notify-host-by-email	PING CRITICAL - Packet loss = 100%
KYOCERA_USAU	Mensaje en pantalla	UNKNOWN	nagiosadmin	notify-service-by-email	Plugin check_snmp_printer failure - snmpwalk command error.
CP-JUNIN - UGEL JUNIN-VPN	N/A	HOST DOWN	mesadeayuda	notify-host-by-email	CRITICAL - Time to live exceeded (172.16.161.1)
CP-JUNIN - UGEL JUNIN-VPN	N/A	HOST DOWN	usrsup	notify-host-by-email	CRITICAL - Time to live exceeded (172.16.161.1)
CP-JUNIN - UGEL JUNIN-VPN	N/A	HOST DOWN	monitoreoiiee	notify-host-by-email	CRITICAL - Time to live exceeded (172.16.161.1)
KYOCERA_DEBEDSAR	Nivel de Consumible	UNKNOWN	nagiosadmin	notify-service-by-email	Plugin check_snmp_printer failure - snmpwalk command error.
CP-PIURA - TALARA-VPN	N/A	HOST DOWN	mesadeayuda	notify-host-by-email	PING CRITICAL - Packet loss = 100%
CP-PIURA - TALARA-VPN	N/A	HOST DOWN	usrsup	notify-host-by-email	PING CRITICAL - Packet loss = 100%
CP-PIURA - TALARA-VPN	N/A	HOST DOWN	monitoreoiiee	notify-host-by-email	PING CRITICAL - Packet loss = 100%
KYOCERA_DEBEDSAR	Modelo	UNKNOWN	nagiosadmin	notify-service-by-email	Plugin check_snmp_printer failure - snmpwalk command error.
CP-ANCASH - HUARMEY-SUP	N/A	HOST DOWN	mesadeayuda	notify-host-by-email	PING CRITICAL - Packet loss = 100%
CP-ANCASH - HUARMEY-SUP	N/A	HOST DOWN	usrsup	notify-host-by-email	PING CRITICAL - Packet loss = 100%
CP-ANCASH - HUARMEY-SUP	N/A	HOST DOWN	nagiosadmin	notify-host-by-email	PING CRITICAL - Packet loss = 100%
CP-CAJAMARCA - CAJABAMBA-VPN	N/A	HOST DOWN	mesadeayuda	notify-host-by-email	PING CRITICAL - Packet loss = 100%
CP-CAJAMARCA - CAJABAMBA-VPN	N/A	HOST DOWN	usrsup	notify-host-by-email	PING CRITICAL - Packet loss = 100%
CP-CAJAMARCA - CAJABAMBA-VPN	N/A	HOST DOWN	monitoreoiiee	notify-host-by-email	PING CRITICAL - Packet loss = 100%
KYOCERA_DEBEDSAR	Mensaje en pantalla	UNKNOWN	nagiosadmin	notify-service-by-email	Plugin check_snmp_printer failure - snmpwalk command error.
CP-CAJAMARCA - CAJAMARCA-VPN	N/A	HOST DOWN	mesadeayuda	notify-host-by-email	PING CRITICAL - Packet loss = 100%
CP-CAJAMARCA - CAJAMARCA-VPN	N/A	HOST DOWN	usrsup	notify-host-by-email	PING CRITICAL - Packet loss = 100%
CP-CAJAMARCA - CAJAMARCA-VPN	N/A	HOST DOWN	monitoreoiiee	notify-host-by-email	PING CRITICAL - Packet loss = 100%
CP-CUSCO - CANCHIS-SUP	N/A	HOST DOWN	mesadeayuda	notify-host-by-email	PING CRITICAL - Packet loss = 100%
CP-CUSCO - CANCHIS-SUP	N/A	HOST DOWN	usrsup	notify-host-by-email	PING CRITICAL - Packet loss = 100%
CP-CUSCO - CANCHIS-SUP	N/A	HOST DOWN	nagiosadmin	notify-host-by-email	PING CRITICAL - Packet loss = 100%
KYOCERA_DEBEDSAR	Bandejas	UNKNOWN	nagiosadmin	notify-service-by-email	Plugin check_snmp_printer failure - snmpwalk command error.
CP-LORETO - REQUENA-SUP	N/A	HOST DOWN	mesadeayuda	notify-host-by-email	PING CRITICAL - Packet loss = 100%
CP-LORETO - REQUENA-SUP	N/A	HOST DOWN	usrsup	notify-host-by-email	PING CRITICAL - Packet loss = 100%
CP-LORETO - REQUENA-SUP	N/A	HOST DOWN	nagiosadmin	notify-host-by-email	PING CRITICAL - Packet loss = 100%
KYOCERA_DEBEDSAR	Impresiones	UNKNOWN	nagiosadmin	notify-service-by-email	Plugin check_snmp_printer failure - snmpwalk command error.
KYOCERA_USAU	Bandejas	UNKNOWN	nagiosadmin	notify-service-by-email	Plugin check_snmp_printer failure - snmpwalk command error.
KYOCERA_USAU	Nivel de Consumible	UNKNOWN	nagiosadmin	notify-service-by-email	Plugin check_snmp_printer failure - snmpwalk command error.
KYOCERA_USAU	Modelo	UNKNOWN	nagiosadmin	notify-service-by-email	Plugin check_snmp_printer failure - snmpwalk command error.
CP-AYACUCHO-SUP	N/A	HOST DOWN	mesadeayuda	notify-host-by-email	PING CRITICAL - Packet loss = 100%

Mapas de conectividad Gráfica

Para visualizar la red de forma gráfica, se integró Nagvis. Esta herramienta muestra la disposición de los hosts, sus conexiones y estados, basándose en la relación padre-hijo. Con un sistema de monitoreo basado en el SNMP, se detectan las interrupciones o degradaciones de los servicios. Esta información se utiliza para validar y descartar problemas, identificando la ubicación del fallo. Con Nagvis permite crear mapas de red personalizados. Se puede subir una imagen con la ubicación física de cada host y añadir los servicios principales.



La herramienta Nagvis ofrece la posibilidad de generar mapas de red automáticos, siempre que los hosts se encuentren configurados con sus relaciones jerárquicas. De esta manera, se facilita la comprensión de la topología de la red.



ANEXO 5: Declaración jurada de autenticidad de tesis

Universidad Nacional del Altiplano Puno | VRI Vicerrectorado de Investigación | Repositorio Institucional

DECLARACIÓN JURADA DE AUTENTICIDAD DE TESIS

Por el presente documento, Yo Erika Milly Apaza Vilca,
identificado con DNI 46965416 en mi condición de egresado de:

☒ **Escuela Profesional,** ☐ **Programa de Segunda Especialidad,** ☐ **Programa de Maestría o Doctorado**
Ingeniería de Sistemas,
informo que he elaborado el/la ☒ **Tesis** o ☐ **Trabajo de Investigación** denominada:
"IMPLEMENTACIÓN DE UN MODELO DE MONITOREO APLICANDO ITIL PARA MEJORAR LA DISPONIBILIDAD DE LOS SERVICIOS TIC DEL MINISTERIO DE EDUCACIÓN - LIMA"

Es un tema original.

Declaro que el presente trabajo de tesis es elaborado por mi persona y **no existe plagio/copia** de ninguna naturaleza, en especial de otro documento de investigación (tesis, revista, texto, congreso, o similar) presentado por persona natural o jurídica alguna ante instituciones académicas, profesionales, de investigación o similares, en el país o en el extranjero.

Dejo constancia que las citas de otros autores han sido debidamente identificadas en el trabajo de investigación, por lo que no asumiré como suyas las opiniones vertidas por terceros, ya sea de fuentes encontradas en medios escritos, digitales o Internet.

Asimismo, ratifico que soy plenamente consciente de todo el contenido de la tesis y asumo la responsabilidad de cualquier error u omisión en el documento, así como de las connotaciones éticas y legales involucradas.

En caso de incumplimiento de esta declaración, me someto a las disposiciones legales vigentes y a las sanciones correspondientes de igual forma me someto a las sanciones establecidas en las Directivas y otras normas internas, así como las que me alcancen del Código Civil y Normas Legales conexas por el incumplimiento del presente compromiso

Puno 28 de Agosto del 2024

FIRMA (obligatoria) Huella

ANEXO 6: Autorización para el depósito de tesis en el repositorio institucional

Universidad Nacional del Altiplano Puno | VRI Vicerrectorado de Investigación | Repositorio Institucional

AUTORIZACIÓN PARA EL DEPÓSITO DE TESIS O TRABAJO DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL

Por el presente documento, Yo Erika Milly Apaza Vilca,
identificado con DNI 46965416 en mi condición de egresado de:

☒ **Escuela Profesional,** ☐ **Programa de Segunda Especialidad,** ☐ **Programa de Maestría o Doctorado**

Ingeniería de Sistemas,

informo que he elaborado el/la ☒ **Tesis** o ☐ **Trabajo de Investigación** denominada:

" IMPLEMENTACIÓN DE UN MODELO DE MONITOREO APLICANDO ITIL PARA MEJORAR LA DISPONIBILIDAD DE LOS SERVICIOS TIC DEL MINISTERIO DE EDUCACIÓN - LIMA "

para la obtención de ☐**Grado,** ☒ **Título Profesional** o ☐ **Segunda Especialidad.**

Por medio del presente documento, afirmo y garantizo ser el legítimo, único y exclusivo titular de todos los derechos de propiedad intelectual sobre los documentos arriba mencionados, las obras, los contenidos, los productos y/o las creaciones en general (en adelante, los "Contenidos") que serán incluidos en el repositorio institucional de la Universidad Nacional del Altiplano de Puno.

También, doy seguridad de que los contenidos entregados se encuentran libres de toda contraseña, restricción o medida tecnológica de protección, con la finalidad de permitir que se puedan leer, descargar, reproducir, distribuir, imprimir, buscar y enlazar los textos completos, sin limitación alguna.

Autorizo a la Universidad Nacional del Altiplano de Puno a publicar los Contenidos en el Repositorio Institucional y, en consecuencia, en el Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto, sobre la base de lo establecido en la Ley N° 30035, sus normas reglamentarias, modificatorias, sustitutorias y conexas, y de acuerdo con las políticas de acceso abierto que la Universidad aplique en relación con sus Repositorios Institucionales. Autorizo expresamente toda consulta y uso de los Contenidos, por parte de cualquier persona, por el tiempo de duración de los derechos patrimoniales de autor y derechos conexos, a título gratuito y a nivel mundial.

En consecuencia, la Universidad tendrá la posibilidad de divulgar y difundir los Contenidos, de manera total o parcial, sin limitación alguna y sin derecho a pago de contraprestación, remuneración ni regalía alguna a favor mío; en los medios, canales y plataformas que la Universidad y/o el Estado de la República del Perú determinen, a nivel mundial, sin restricción geográfica alguna y de manera indefinida, pudiendo crear y/o extraer los metadatos sobre los Contenidos, e incluir los Contenidos en los índices y buscadores que estimen necesarios para promover su difusión.

Autorizo que los Contenidos sean puestos a disposición del público a través de la siguiente licencia:

Creative Commons Reconocimiento-NoComercial-CompartirIgual 4.0 Internacional. Para ver una copia de esta licencia, visita: https://creativecommons.org/licenses/by-nc-sa/4.0/

En señal de conformidad, suscribo el presente documento.

Puno 28 de Agosto del 2024

FIRMA (obligatoria)

Huella