UNIVERSIDAD AUTÓNOMA DE ICA

FACULTAD DE INGENIERIA, CIENCIAS Y ADMINISTRACIÓN

PROGRAMA ACADÉMICO DE INGENIERIA DE SISTEMAS

TESIS

IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO PARA LA INFRAESTRUCTURA DE TI EN EL INSTITUTO DE ENFERMEDADES NEOPLASICAS DEL SUR-IRENSUR

LÍNEA DE INVESTIGACIÓN:

GESTIÓN DE INGENIERÍA, SOFTWARE Y REDES

PRESENTADO POR:

KAROL JHUSEP NUÑEZ PARRA

CÓDIGO ORCID N°0000-0002-7603-8342

TESIS DESARROLLADA PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

DOCENTE ASESOR:

DR. ELIO JAVIER HUAMAN FLORES

CÓDIGO ORCID N°0000-0002-8461-5082

CHINCHA, 2023

DEDICATORIA

El presente trabajo de grado va dedicado a mi familia que, con su apoyo incondicional y paciencia hicieron que logre culminar este tramo de mi vida profesional.

Karol Jhusep.

AGRADECIMIENTO

Agradezco al Rector de la Universidad Autónoma de Ica, Dr. Hernando Martín Campos Martínez, al Decano (e) de la Facultad de Ingeniería, Ciencias y Administración, Dra. Mariana Alejandra Campos Sobrino, por su compromiso y apoyo a los estudiantes en el programa de titulación.

Al asesor de tesis, Dr. Elio Javier Huamán Flores, por sus valiosos aportes, conocimientos y motivaciones brindadas, para el desarrollo y culminación del estudio.

Al Hospital Regional de Enfermedades Neoplásicas del Sur-IRENSUR, representado por el Gerente General M.C. Jesús Alberto Rivera Jove, por brindarme las facilidades para la implementación del Sistema de Monitoreo, y que fuera posible culminar este estudio.

A los integrantes del área de Informática, ya que sin su ayuda no hubiera sido posible desarrollar la investigación.

El autor.

RESUMEN

Objetivo: Implementar un Sistema de monitoreo de Infraestructura de TI dentro de la red LAN del Instituto Regional de Enfermedades Neoplásicas del Sur

Metodología: La investigación tecnológica validó una tecnología utilizando como metodología Scrum, logrando una gestión eficiente del tiempo y un proceso iterativo e incremental efectivo.

Participantes: En la investigación participó toda la infraestructura de Tecnología de Información, incluyendo servicios, servidores y equipos de red de la red LAN del IRENSUR.

Resultados: La implementación del sistema de monitoreo y gestión de la red fue exitosa gracias al uso de la metodología tecnológica Scrum. En la primer Sprint se realizó el análisis y elección del sistema a implementar, mientras que en el Sprint 2 se diseñó la implementación. En el Sprint 3 se logró la puesta en ejecución del sistema, permitiendo así cumplir con los objetivos de la investigación.

Conclusiones: En conclusión, la implementación del sistema de monitoreo en el hospital IRENSUR ha cumplido con los objetivos planteados, gracias a la metodología SCRUM que ha permitido una interacción dinámica entre las partes interesadas y los ejecutores del proyecto. El tipo de monitoreo implementado ha asegurado un seguimiento preciso de los activos y equipos de la infraestructura de TI sin falsos positivos, y el sistema de alertas dinámico y simple proporciona información certera de las incidencias para la rápida solución del personal. En definitiva, este sistema ha mejorado significativamente la eficiencia del hospital y su capacidad de respuesta ante problemas tecnológicos.

Palabras claves:

Redes, Monitoreo, Infraestructura de TI, Zabbix, SCRUM.

ABSTRACT

Objective: To implement an IT Infrastructure Monitoring System within the LAN network of the Regional Institute of Neoplastic Diseases of the South

Methodology: The technological research validated a technology using Scrum methodology, achieving efficient time management and an effective iterative and incremental process.

Participants: The research involved the entire Information Technology infrastructure, including services, servers and network equipment of the IRENSUR LAN network.

Results: The implementation of the network monitoring and management system was successful thanks to the use of the Scrum technological methodology. In the first Sprint the analysis and choice of the system to be implemented was carried out, while in Sprint 2 the implementation was designed. In Sprint 3, the implementation of the system was achieved, thus allowing to meet the objectives of the research.

Conclusions: In conclusion, the implementation of the monitoring system in the IRENSUR hospital has met the objectives set, thanks to the SCRUM methodology that has allowed a dynamic interaction between the interested parties and the executors of the project. The type of monitoring implemented has ensured accurate tracking of IT infrastructure assets and equipment without false positives, and the dynamic and simple alerting system provides accurate incident information for rapid staff resolution. In short, this system has significantly improved the efficiency of the hospital and its ability to respond to technological problems.

Keywords:

Networking, Monitoring, IT Infrastructure, Zabbix, SCRUM.

ÍNDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

I. INTRODUCCIÓN

En las empresas en actualidad es importante y aún más en las comunicaciones que tiene sus diversas áreas, de esta forma mejorar su dinámica de negocio. Cuando se tiene atrasos o averías en diversos procesos, es inevitable que haya pérdidas económicas, es tal el motivo que el área de ti debe asegurar que la red sea optima y los servicios estén disponibles. Al tener estas dos premisas la empresa debe de contar con un sistema de monitoreo, que examine toda la infraestructura de TI, con la finalidad de detectar incidentes y poder atenderlos de una forma rápida. Es común que las averías afecten de una forma grave a la empresa y convirtiéndose en un desencadenado que afecte directa o indirectamente a otras áreas.

Toda empresa tiene requerimientos diferentes y procesos que no son iguales al resolver un incidente o tener seguimiento de este, en la actualidad existen diferentes soluciones de monitoreo (ya sean open source o privativos), finalmente se requiere un sistema que sea ágil al recabar información con el fin de garantizar no haya DwonTime en la empresa. Para esto debemos tener en cuenta los requerimientos, necesidades y falencias en sus procesos para elegir la herramienta adecuada que se puedan aplicar dentro del IRENSUR.

El monitoreo de equipos y dispositivos de TI integrados en los hospitales no es solo un proceso muy importante, si no que a veces incluso es crítico para salvar vidas de las personas. Una solución de monitoreo es confiable cuando hace que el flujo de información sea rápido y ahorre tiempo en el análisis y solución de un incidente.

La presente tesis consta de 6 capítulos, cada uno enfocado en puntos importantes el cual se detalla a continuación:

Capítulo I Introducción: En este capítulo hacemos una introducción a la investigación y un detalle resumido de cada capítulo que se trató en el presente trabajo.

Capítulo II Planteamiento del Problema: En este capítulo detallamos la problemática que se eligió para este estudio, la data se recogió de las personas que tienen una relación con el tema de estudio esto con el propósito de estudio por parte del investigador, por otro lado, se definirá los objetivos que permitan justificar y darle la importancia debida a esta investigación.

Capitulo III Marco teórico: Realizaremos un análisis de antecedentes, nacionales e internacionales que permitan ayudar a una investigación más profunda con casuísticas similares a la investigación, de otra manera definir bases teóricas de la investigación con el fin de tener un más claro los conceptos técnicos.

Capitulo IV Metodología: En este capítulo definimos el tipo de investigación, de igual forma se detallará las actividades desde la planificación hasta la puesta en marcha todo siguiendo la metodología SCRUM para la implantación del sistema de monitoreo de infraestructura de TI, culminando con un resumen de todo lo desarrollado de la investigación.

Capitulo V Solución tecnológica: Este capítulo se desarrolla la presentación de toda la información recolectada, de igual forma se mostrará un detalle de la data con el dar una idea del proceso de monitoreo.

Capitulo VI Discusión de resultados: En este capítulo detallaremos el presupuesto necesario para el desarrollo de la investigación

Karol Jhusep Nuñez Parra.

II. PLANTEAMIENTO DEL PROBLEMA

2.1. Descripción del problema

El estudio de Gartner sobre herramientas de monitoreo de infraestructura de TI indica que "con la aparición de arquitecturas modulares, muchas organizaciones están gastando su presupuesto de I&O descuidando el monitoreo de estas arquitecturas" (Gartner, 2017, como se citó en "Herramientas ITIM", 2017).

El ministerio de salud realizo un documento técnico de análisis de “Indicadores De Brechas De Infraestructura Y Equipamiento Del Sector Salud” (MINSA-2020), este documento indica que a “enero del 2020 se tenía 77.8% de capacidad instalada inadecuada expresada en la precariedad de su infraestructura” refiriéndose a equipos no operativos, escasos y obsoletos.

El IRENSUR (Instituto Regional de Enfermedades Neoplásicas del Sur) es un hospital especializado en enfermedades de neoplasias (Cáncer), esta fue creada el 17 de junio del 2008 por la ordenanza regional N° 057-2008-AREQUIPA , el perfil del hospital es ser reconocido como el instituto de referencia regional en oncología, para esto su fin es la promoción, prevención, diagnóstico, tratamiento y recuperación de los pacientes con Cáncer; llegando a promover la investigación, docencia y capacitación los cuales son los pilares fundamentales para su funcionamiento.

Teniendo como áreas funcionales los departamentos de:

- Control de Cáncer.
- Medicina
- Cirugía
- Radioterapia
- Apoyo y diagnóstico y tratamiento

Al tener una caída del servicio de sistema de pacientes, no se tiene detalle si eso fue por no disponer conexión a internet o fue una caída de energía o quizás el servicio como tal este fallando dentro del servidor que está instalado teniendo así un limbo de información del problema generando un DownTime(interrupción o la falta de disponibilidad de un sistema o servicio de tecnología de la información, lo que puede afectar la capacidad de las personas para acceder a información o servicios en línea.) grave de larga duración y teniendo una respuesta tardía para la resolución del problema y no preventiva.

No se tiene registro de problemas referidos anteriormente sus causas y de cómo fueron solucionados.

El personal de salud de diferentes áreas que opera en el hospital de neoplásicas IRENSUR presentan muchas quejas como: fallo de los sistemas, problemas de conexión en la red, lentitud en el uso de navegación de internet, no operatividad de equipos de impresión y la no disposición de los sistemas de SIGA, SIAF, Correo y otros.

Todos estos problemas de alguna forma generan perdidas y afectan económicamente a la empresa, por otro lado, los procesos logísticos tienden a atrasarse al igual a los centros de control de producción.

2.2. Pregunta de investigación general

¿Cómo se llega a implementar un sistema de monitoreo de infraestructura que este sea open source y desplegarlo dentro de la red LAN del Instituto Regional de enfermedades Neoplásicas del Sur-IRENSUR?

2.3. Preguntas de investigación específicas

P.E.1:

¿Qué procesos críticos y no críticos se llegarán a monitorear del Instituto Regional de enfermedades Neoplásicas del Sur-IRENSUR?

P.E.2:

¿Cuáles son los pasos por seguir para la instalación y despliegue del sistema de monitoreo?

P.E.3:

¿Dentro de un sistema de monitoreo de infraestructura de TI es posible tener alertas adelantándose a posibles fallos o cuando estos estén ocurriendo?

2.4. Objetivo general

Implementar un sistema de monitoreo que permita gestionar y administrar la infraestructura de TI y equipos de salud, esto dentro de la red LAN del Instituto Regional de enfermedades Neoplásicas del Sur-IRENSUR.

2.5. Objetivos específicos

O.E.1:

Analizar la infraestructura de TI a monitorear de los servicios y host, sean estos críticos y no críticos.

O.E.2:

Instalar y desplegar el sistema monitoreo en todos los dispositivos y equipos hospitalarios que sean de importancia.

O.E.3:

Crear un Bot chat de alarmas, sobre parámetros pendientes o algún excepcional, que se generen en el sistema de monitoreo Infraestructura de TI y notifiquen a los encargados según sea el caso.

2.6. Justificación e Importancia

2.6.1. Justificación

Se tomarán diferentes aspectos para la justificación de esta investigación.

Justificación Teórica.

El monitoreo de un sistema dentro de una empresa, de acuerdo a la definición de Mike (2017), "es la acción de observar y verificar el comportamiento y los resultados de un sistema a lo largo del tiempo" (p. 150).

Según Sun, Chiang, y Chou (2017), la implementación de un sistema de monitoreo es crucial para garantizar la continuidad del negocio, especialmente en entornos empresariales críticos. Además, Barreto, Granville, Rochol y Sperotto (2015) sugieren que el monitoreo constante del sistema es esencial para detectar y corregir rápidamente los problemas del sistema antes de que afecten a los usuarios finales.

Por otro lado, varios estudios han demostrado que la implementación de sistemas de monitoreo puede mejorar significativamente la eficiencia y el rendimiento del sistema. Por ejemplo, según el estudio de Al-Faris, Alnuem y Al-Hamad (2018), el monitoreo proactivo del sistema puede ayudar a identificar cuellos de botella en el sistema y prevenir el deterioro del rendimiento del sistema.

En resumen, la implementación de un sistema de monitoreo de sistemas es esencial para garantizar la continuidad del negocio, detectar y corregir rápidamente los problemas del sistema, mejorar la eficiencia y el rendimiento del sistema, identificar cuellos de botella y planificar la capacidad futura del sistema.

Justificación Practica

Como sucede a menudo, los sistemas pueden comportarse de formas inesperadas.

Un proceso importante en el monitoreo de una entidad salud es la atención médica y prevenir cualquier perdida de efectivo que pueda ser usada para el desarrollo y apoyo de la institución médica en este caso el proceso de monitoreo de monitorear estará dirigido a reconocer si lo resultados proyectados se han logrado según los parámetros que indique el PETI de la institución y objetivos del área de TI esta data será precisa con esto se puede tener estadística exacto sobre qué área(s) o proyectos(s) pueden tener problemas o fallas en el Sistema de TI.

Justificación metodológica

La siguiente justificación metodológica se basa en el artículo de Patricia et al. (2019):

La implementación de la metodología Scrum en el desarrollo de proyectos de software en empresas colombianas es una opción viable y efectiva para mejorar la tasa de éxito en los proyectos. Según el estudio de Patricia et al. (2019), el 60% de la población investigada implementó Scrum y logró una mejor integración y acoplamiento en el desarrollo de proyectos, en comparación con la metodología clásica. Esto se debe en gran medida a la capacidad de Scrum para fomentar la colaboración y el trabajo en equipo, así como a su enfoque en la entrega incremental de funcionalidades y la capacidad de adaptación a los cambios en los requerimientos del proyecto.

Por lo tanto, la metodología Scrum viene a ser una opción efectiva para empresas que buscan mejorar su tasa de éxito en la implementacion de proyectos de software, fomentar la

colaboración y adaptarse a los cambios en los requerimientos del proyecto.

Justificación económica

El monitoreo adecuado de la infraestructura de TI dentro de una empresa puede ser una decisión económica rentable. De acuerdo con las palabras de Burnaeva (2021), "el monitoreo inadecuado puede resultar en costos más altos, ya sea por pérdidas o reparaciones en la infraestructura de TI" (párr. 1). Por lo tanto, una solución rentable sería invertir en herramientas de monitoreo eficaces que puedan ayudar a detectar problemas en la infraestructura de TI y solucionarlos antes de que se conviertan en costosas fallas. Esta inversión inicial en herramientas de monitoreo puede ser más económica en comparación con el costo de reparar o reemplazar la infraestructura dañada. Además, el monitoreo eficaz puede ayudar a aumentar la eficiencia en la gestión de la infraestructura de TI, lo que puede traducirse en ahorros económicos a largo plazo.

Según un informe de Gartner, los costos promedio de una hora de inactividad no planificada en un entorno de TI pueden oscilar entre los 140,000 y los 540,000 dólares, dependiendo del tamaño de la empresa y de la complejidad de su infraestructura tecnológica (Lerner, 2014).

Justificación tecnológica

La creciente infraestructura exige un software de monitoreo escalable. Necesita una solución que pueda rastrear y supervisar los servicios de extremo a extremo y agregar todos los datos de todos los orígenes en una consola central. Esto esencialmente significa que necesita un software de monitoreo que tenga varias herramientas de monitoreo específicas

diferentes, todas las cuales se unen para crear el panorama general. La implementación de un sistema de monitoreo de TI radica en su capacidad para proporcionar una mayor visibilidad y control sobre los sistemas y aplicaciones de TI, detectar problemas de rendimiento y seguridad antes de que se conviertan en problemas mayores, y optimizar los recursos de TI, Según Kavis (2018), el monitoreo constante de la infraestructura de TI es crucial para mantener la disponibilidad, el rendimiento y la seguridad de los sistemas. La implementación de un sistema de monitoreo adecuado ayuda a detectar problemas temprano, reducir el tiempo de inactividad no planificado, aumentar la eficiencia y la productividad del equipo de TI, y mejorar la experiencia del usuario final. Además, Kavis destaca que la mayoría de las organizaciones no tienen la capacidad interna para desarrollar y mantener un sistema de monitoreo personalizado y que la adopción de soluciones ya existentes en el mercado es una opción más práctica y rentable.

2.6.2. Importancia

Según Mendillo V. (2009), indica que un sistema de monitoreo es de importancia para el apoyo en la gestión de redes, esto indirectamente satisface a los usuarios finales, con esto se garantiza tener disponible en la mayoría de tiempo los servicios independiente a su grado de complejidad, esto apoya a los administradores de TI en notificar o delegar posibles errores en la infraestructura de TI generando en la organización mejoras en sus procesos, y ahorro ante perdidas de información o fallas en los servicios.

Es importante que un sistema de monitoreo realice un análisis analítico basado en las premisas de proactividad y centralización, Trujillo (2020) destaca en su estudio que un sistema de monitoreo es capaz de detectar anomalías en la red

y tomar acción sobre ellas, lo que permite anticiparse a los problemas que pudieran surgir con un menor costo de tiempo. De acuerdo con estas premisas, dentro del IRENSUR se tendría una mejor visión de los diversos equipos de comunicación e innovaciones tecnológicas. Al tener varios equipos que interactúan dentro de la red del hospital, esta información sería medible y con el sistema de monitoreo se podría centralizar toda la información.

2.7. Alcances y limitaciones

2.7.1. Alcances

Alcances a nivel tecnológico:

Los alcances dentro del despliegue del sistema de monitoreo son

- Desplegar los agentes de monitoreo dentro de los servidores prioritarios que se tenga dentro de la red LAN.
- Desplegar el monitoreo SMNP en todos los switch y firewall que se tiene en la red LAN del IRENSUR.
- Hacer un monitoreo por ICMPING a equipos prioritarios dentro de las áreas de farmacia, caja y admisión.
- Monitorear los servicios de correo a nivel de puerto como SMTP, POP3, y SMTP esto desde el servidor principal que se encuentra en nube.
- Notificación de incidencias a nivel de un chat y su levantamiento de esta el cual estará registrado en el tiempo.

Alcance espacial o geográfica: El presente estudio investigará la infraestructura de TI del Hospital Regional de Enfermedades Neoplásicas del Sur (IRENSUR), ubicado en el distrito y provincia de Arequipa, en el departamento de Arequipa.

Delimitación Temporal: La investigación se desarrolló en el periodo del año 2021- 2022.

2.7.2. Limitaciones

El presente estudio se ha enfrentado a diversas limitaciones durante la implementación del sistema de monitoreo en el IRENSUR. Una de las limitaciones ha sido el acceso limitado a ciertas áreas críticas del hospital debido a la atención de pacientes COVID, lo que dificultó la identificación física de algunos activos tecnológicos. Además, la falta de información actualizada sobre la infraestructura de TI del hospital ha dificultado la identificación de los activos tecnológicos disponibles. Otra limitación ha sido el poco tiempo que ha tenido el personal de informática para la capacitación y entrevistas técnicas debido a la sobrecarga de trabajo en la atención y solución de problemas en el hospital. También se ha presentado un retraso en la implementación del servidor proxy debido a la escasez de microchips en el mercado mundial, lo que ha generado un retraso de 20 días en la implementación del sistema de monitoreo.

Es importante mencionar que estas limitaciones son comunes en la implementación de software y sistemas de monitoreo en infraestructuras de TI. Otros factores que se encontraron y afectaron la implementación fueron la falta de presupuesto para la inversión en tecnología, la falta de capacitación del personal de TI, la resistencia al cambio y la complejidad de la infraestructura tecnológica existente.

III. MARCO TEÓRICO

3.1. Antecedentes

Al examinar diversas fuentes virtuales y físicas se encontró trabajos que tiene una relación indirecta con las variables, guardando una relación importante en el desarrollo de la investigación:

Internacionales

Vallejo (2020). Realizo la tesis titulada: ***Diseño e implementación de un sistema centralizado de monitoreo, supervisión y control automático de servidores y servicios en entornos virtuales de la empresa Message Plus basado en herramientas de código abierto***. De la carrera de Ingeniería de Sistemas. Universidad Politécnica Salesiana Sede Quito, para optar el título de profesional de Ingeniero de Sistemas, esta investigación es experimental desarrollado bajo la metodología Scrum, la investigación es bibliográfica por otro lado la investigación de campo verifica el estado su infraestructura y función de esta el cual se desarrolló en las instalaciones de la empresa Message Plus, para el análisis de operatividad de la empresa se empleó cuestionarios al gerente de TI. Los resultados del monitoreo y alertas se dieron en situaciones reales mientras la empresa trabaja de forma normal, por otro lado, las pruebas críticas se dieron en ambientes controlados. Finalmente, en las conclusiones según a la entrevista que se dio con el gerente de TI permitió jerarquizar el sistema de monitoreo, al tener un monitoreo de un año se llegó a evaluar el sistema de monitoreo en contraparte con sistemas licenciados por suscripción evidenciando que el software libre puede no generar nuevos gastos de mantenimiento y puesta servicio siempre y cuando el personal este bien capacitado sin llegar a sacrificar la seguridad de la empresa.

Cedeño y Luyely (2019). Realizó la tesis C***omparativa entre herramientas de monitoreo de red de computadoras aplicadas a la empresa Puerto atún.*** Escuela Superior Politécnica Agropecuaria De Manabí Manuel Feliz López. Para Optar El Titulo De Magister En Tecnologías De La Información Mención En Redes Y Sistemas Distribuidos, la metodología de investigación se da dentro del método comparativo y experimental para su desarrollo, las pruebas de las herramientas se hicieron dos comparativas una que abarca 8 eventos de monitorización y otro que mide el grado de dificultad de implementar y administrar la herramienta de monitoreo , teniendo como resultado que el sistema de monitoreo Nagios es la más óptima para el soporte, facilidad administración y seguridad según el autor indica que esta conclusión llega a concordar con Bayas(2015), pero especifica que si los agentes de monitoreo que se usó para las pruebas eran pasivas o activas.

Remolina (2019). Quien desarrollo la tesis titulada: ***Diseño de un modelo de seguridad informática a una empresa en su sistema de monitoreo del área de tecnología***. Universidad Cooperativa De Colombia, para optar el grado de Ingeniero de Telecomunicaciones, el desarrollo metodológico que se aplico es Plan Do Check Ac y el estudio de datos se da con la metodología MAGERIT, el estudio al inventariar su infraestructura de TI agrupo en 4 amenazas del cual destaco que la confidencialidad de información es la que más afecta a la empresa, seguido por la integridad de la infraestructura de TI. Las conclusiones que se llega autor son que, al aplicar un sistema de monitoreo, este debe tener controles de seguridad de mano a una zonificación esto lograra mitigar vulnerabilidades

teniendo como resultado valores altos en seguridad de la infraestructura de TI.

Gaviria (2019). desarrollo la tesis : ***Implementación de una solución de administración y supervisión de servidores como herramienta de contingencia para la empresa EMTELCO S.A.S.*** Universidad de Antioquia, para optar el título de Ingeniero de Telecomunicaciones, el tipo de investigación es experimental , para esto llego a comparar 4 sistemas de monitoreo haciendo comparaciones de su administración y despliegue , teniendo como conclusión que al implementar un sistema de monitoreo de TI evidencia ser funcional el cual ayuda a tener un control en los eventos que se presenten dentro de la empresa , al implementar el sistema de monitoreo Zabbix se debe tener en consideración los recursos para su implementación esto a nivel de servidor ya que según el autor indica que es un requisito imprescindible para su ejecución.

Saavedra (2018). desarrollo la tesis, ***Control de servicios de red y servidores basado en herramientas de administración de red y políticas de gestión de calidad.*** Universidad Católica del Ecuador Sede Esmeraldas, para optar el título de Ingeniero de Sistemas y Computación, el tipo de investigación es de tipo cuantitativa y cualitativa, para recabar data se aplicó la técnica de la entrevista esta se aplicó a todo el personal de TI y el de la observación verificando que se tiene 9.8 de incidencias semanales. A las conclusiones que se llega es establecer requisitos funcionales y deben estar contenidos en las herramientas de monitoreo y se debe tener como un requisito importante que el sistema de monitoreo debe cumplir con estándares internacionales (iso10164).

Nacionales

Enciso (2021). Desarrollo la TSP: ***diseño e implementación de un sistema de monitoreo del centro de datos para la red del INICTEL-UNI utilizando software libre***. Universidad Nacional Tecnológica de Lima Sur, para optar el título de Ingeniero Electrónico y Telecomunicaciones, el estudio es de tipo aplicativo experimental , la muestra se recabe por encuestas con el fin de conocer el nivel de satisfacción de los trabajadores en la encuesta te tiene 3 secciones (gestión de incidentes , gestión de rendimiento, nivel de satisfacción del trabajo realizado) teniendo como resultado que la atención de incidentes es adecuada según el 61%, su detección es más rápida para el 80%, que la disponibilidad de servicios funcionan un 68 % de forma correcta y un 32 % indica con fallas leves, el trabajo concluye que el análisis de situación actual permite recopilar información de las necesidades y requerimientos , al implementar el sistema de monitoreo este le permite monitorear de forma real y visualizar graficas con parámetros gestionados de los equipos de red y energía.

Trujillo (2020), desarrollo la tesis titulada: ***Influencia de la aplicación del software Zabbix en el monitoreo de la red de área local de la SUPERINTENDENCIA NACIONAL DE LOS REGISTROS PÚBLICOS zona registral n° V - sede TRUJILLO.*** Universidad Privada Antenor Orrego, para optar el Grado De Maestro En Ingeniería De Sistemas – Mención Sistemas De Información, el tipo de estudio es Aplicada – Experimental, teniendo como la muestra poblacional la red LAN de Registros Públicos sede-Trujillo , como instrumento de recolección de datos se hizo una encuesta a los 10 operadores de la Red LAN SUNARP con 25 preguntas por otro lado se hizo una análisis documental de la institución (manuales de equipos), teniendo como resultado que antes de implementar el

software Zabbix el 61% indicaba que la gestión de monitoreo era deficiente, luego de implementar el sistema de monitoreo Zabbix el 92 % respondió que habían respondido que había mejorado la gestión de la red de la área Local. Según las encuestas y el análisis documental se evidencia que el 85% de reportes no se generó de manera correcta en el año 2016, basado en el análisis documental y trabajo de campo se identificó el incremento de eficiencia de operadores de monitoreo esto en el año 2017

Lopez y Geovanni (2020). Quien realizo la tesis: ***Implementación del software APM para monitorear eficientemente las aplicaciones en la empresa AMÉRICA MÓVIL PERÚ S.A.C***. Universidad Peruana De Ciencias E Informática, para optar el grado de Ingeniero de Sistemas e Informática, el tipo de investigación es aplicada- explicativa experimental , el muestro poblacional es de 20 usuarios del área de atención tecnológica, se concluye que el sistema de monitoreo mejora un 62% en comparación cuando no tubo implementado esto por la pruebas estadísticas de wilcoxon.

Quispe (2018) realizo la tesis de grado: ***Implementación de un sistema de monitoreo y control de red, para un canal de televisión, basado en herramientas open source y software libre , Lima 2017.*** Universidad Altiplano de Puno- UNA para optar el título de Ingeniero de Sistemas, este tipo de investigación lo catalogo como descriptiva cuasi Descriptiva , teniendo como un total de población de muestreo de 206 personas, teniendo como resultado que un 75% de su población opina que la prevención de la red que se implementó en canal de televisión se da una manera efectiva , por otro lado al consultar a la población indica un 69% que el seguimiento a fallos y su solución a estas se da en un nivel alto esto hace que

la implementación que se llegó a dar mejora en la toma de decisiones y acciones correctivas sobre estas lo cual genera que al personal de TI de una mejor solución a incidencias de mesa de ayuda y redes.

Locales o regionales

En la revisión de la literatura, no se ha podido encontrar estudios previos (regionales o locales), que guarden relación con la investigación propuesta.

3.2. Bases Teóricas

las bases teóricas que se tiene para poder desarrollar el proyecto son los siguientes:

3.2.1. Sistema informático

Según Raya (2011) define un sistema informático como "un conjunto de partes interrelacionadas, típicamente este es un conjunto de dispositivos programables que capturan, almacenan y procesan datos" (p. 18).

Típicamente está dividido en tres partes:

- Hardware. Comprende los circuitos integrados y periféricos del computador.
- Software. Viene a ser el componente lógico el cual dispone de un lenguaje que tiene la capacidad de interactuar con el hardware y tomar control de este, dentro de esto tenemos dos tipos de software: software base(comúnmente conocido como el sistema operativo el cual contiene un conjunto de programas que tienen la capacidad de trabajar con el hardware); Software aplicación(viene a ser los programas que funcionan o son usados por el usuario).
- Componente humano. Viene a ser los usuarios que hacen uso del sistema.

3.2.2. Gestión de equipos

Según Silva, Medeiros y Martins (2016), "la gestión de equipos en un parque de tecnología de la información es común que estos equipos cuenten o hagan uso de un sistema y servicio de red". El crecimiento de una empresa hace que estos equipos hagan uso de la red y sean dependiente de ello haciendo que sea necesario su gestión. Por ello Cestari Filho (2011) remarca en su investigación que los presupuestos destinados a la operatividad de TI suelen incluir gastos en personal y en el mantenimiento de la tecnología, el cual representa un mayor gasto que llega a un tope del 70% del gasto de área de Sistemas todo eso dentro de una empresa común , el otro porcentaje restante se da uso en desarrollo y adquisiciones referidas a TI, la gestión se hace importante tan igual a la implementación.

3.2.3. Gestión de Red

La gestión de red tiene a tener muchos significados Según CISCO (2018), la ejecución de una red y las actividades que se realicen en ella requieren del soporte de tecnología específica. Dentro de las tareas relevantes en la ejecución de una red se encuentra su monitoreo para comprender lo que está sucediendo en ella. Además, se suman otros aspectos como la operación, administración, mantenimiento y aprovisionamiento de la red. Por tanto, estos elementos son cruciales para el éxito en la ejecución de una red.

A esto se suma los siguientes conceptos:

- Operación: esta se ocupa de mantener la red y los servicios que se proporcionen en este, la operación se encarga de monitorear los problemas y detectar los problemas lo antes posibles teniendo como objetivo

principal es sea detectado lo antes posible sin que se afecte a las operaciones de los clientes.

- Administración: Implica hacer un seguimiento de los recursos y de cómo están asignados dentro de la red. Su fin es tener todo bajo control.
- Mantenimiento: Realiza las operaciones y actualizaciones, esto también implica que se de manera preventiva y correctiva según sea necesario, según sea necesario dentro de la red administrativa

3.2.4. Sistema de Monitoreo

Un sistema de monitoreo tiene como función principal analizar el sistema de red de comunicaciones y emitir alertas al detectar anomalías en los servidores, terminales o servicios previamente identificados. De esta manera, permite identificar y solucionar problemas en la red de manera más eficiente y oportuna.

3.2.5. Monitorización a tiempo real

Sevillano (2021,245), en estos sistemas se miden a tiempo real datos de sistemas, log y eventos esto a tiempo real ,por la rapidez que se tiene en conocer el significado de estos mismos , toman un aspecto fundamental a la hora de tener una decisión ante un incidente.

3.2.6. Monitorización a demanda

Sevillano (2021,246), la monitorización a demanda hace un análisis a posteriori que se basa en un análisis causa raíz , al llegar a presentarse un incidente que necesite saber mayor detalle de este , se llega a hacer una investigación más específica en el proceso.

3.2.7. Monitorización basada en trafico

Sevillano(2021), Este tipo de monitorización se basa en la captura de traps de comunicación que se da entre dos equipos que se comunicación ya sea esta por medio óptico o par de cobre para adquirir los traps o trama de hace uso de software diseñado para este fin

3.2.8. Monitorización basada en activos

Sevillano(2021,249), La monitorización de activos se da activos inventariados que se da de manera activa con escaneos de red mediante el uso de ping sweep o el uso de protocolos smnp o herramientas para descubrir la red, los datos que emiten este tipo de monitorización son el estado, comunicaciones y actividades todo esto dentro de nuestra infraestructura de TI.

3.2.9. Soluciones de Seguimiento

A continuación, se describe principales sistemas de monitoreo.

- ZABBIX: Zabbix (2022) Es una solución de monitoreo distribuido de código abierto de clase empresarial, que cuenta con un software que monitorea numerosos parámetros de una red y la salud e integridad de servidores, máquinas virtuales, aplicaciones, servicios, bases de datos, sitios web, la nube y más. Llegando a usar un mecanismo de notificación flexible que permite a los usuarios configurar alertas basadas en correo electrónico para prácticamente cualquier evento. Esto permite una reacción rápida a los problemas del servidor. Zabbix ofrece excelentes funciones de generación de informes y visualización de datos basadas en los datos almacenados. Esto hace que Zabbix sea ideal para la planificación de la capacidad.

- CACTI

  Cacti es una herramienta de código abierto, monitoreo de red y gráficos escrita en PHP / MySQL. Utiliza el motor RRDTool

(Round-robin data base tool) para almacenar datos y generar gráficos, y recopila datos periódicos a través de Net-SNMP (un conjunto de aplicaciones para implementar SNMP: Simple Network Management Protocol).

- NAGIOS: VELIMIROVIC (2021) indica que Nagios es una aplicación de código abierto para monitorear sistemas, redes e infraestructura de TI. La herramienta permite a los usuarios realizar un seguimiento del estado y el rendimiento. llegando ejecutar comprobaciones periódicas con umbrales y métricas para monitorear los cambios en el sistema. Si el software tiene un problema, la herramienta notifica a los administradores y también puede ejecutar scripts automáticos para contener y remediar la situación.

3.2.10. Metodología Scrum

La metodología Scrum es un framework para desarrollo ágil, el cual permite procesos de trabajo grupal o en equipo, de forma regular, para desarrollar proyectos de manera más rápida y óptima (Schwaber & Sutherland, 2016, p. 35)

Cuenta con 5 fases:

- Inicio
- Planificación y estimación
- Implementación
- Revisión y retrospectiva.
- Lanzamiento

3.2.11. Administración de incidentes

Viene a ser la gestión formal de los problemas que surgen el cual es gestionado en su mayoría por ITIL.

Según ITIL Fundation (2019) un incidente viene a ser “Una interrupción no planificada de un servicio de TI o una reducción en la calidad de un servicio de TI”

Para esto ITIL sigue unos pasos de gestión:

- Identificación de incidentes.
- Registro de incidentes.
- Categorización de incidentes.
- Priorización de incidentes.
- Inicio de diagnóstico.
- Escala de nivel de soporte en caso sea necesario.
- Resolución de Incidente.
- Cierre de incidente.
- Reporte a usuario en todo el proceso de gestión del incidente.

3.3. Marco conceptual

Agente: Rol que tiene un sistema que está siendo administrado por un sistema.

Alarma: Evento que indica el inicio de una condición de alarma

Banda Ancha: métricas de interfaz expresados Mb/s

Cliente: Entidad que es atendida por un servidor.

Contador: Variable de gestión que muestra un valor monótono (ejemplo número de tramas transmitidas).

DwonTime: Se refiere al tiempo o periodo de que un servicio o entidad no esté disponible.

Estándar SO: Métricas de carga del sistema operativo.

Evento: Ocurrencia o incidencia que se genere en la vida real.

Gestión de aplicaciones: Gestión de aplicaciones que se tiene en un sistema que esta interconectado por red esto mediante el uso de una red.

IC: Administración de incidentes.

IMCP: Hitesh (2021). Es un protocolo que se usa dentro de una red para comunicar problemas de transferencia de datos esto con el fin de determinar que si se cumple con llegar al destino y con tiempo esto hace que este protocolo sea primordial en la fase de informe y comprobación de errores.

Interfaz: Host que se usa para el consumo de la aplicación esto ejecutado por el usuario.

Implementación: Es la construcción definitiva donde se elaboran, adaptan y añaden los elementos previamente contemplados, o bien, se trabaja en casos adaptativos, es decir, se adecuan aplicaciones de código abierto ya construidas que se ajusten a los requerimientos del cliente.

IPFX: monitoreo de flujo

J-Flow: Monitoreo de flujo

MAU: Usuarios activos mensuales.

Metadatos: el código base que se encuentra dentro del sistema de código fuente interno.

MIB: Archivos base de información de gestión.

OID: Identificadores de objeto.

Runbook: Vienen a ser los pasos para llevar un proceso o tarea ejecutados por el administrado de TI o el operador de sistemas.

SLA: Es el nivel de disponibilidad del servicio.

SMNP: (CISCO,2018) el protocolo simple de administración de red se desarrolló con la finalidad de administrar nodos dentro una red IP.

Sprint: Estimado de tiempo que marca referencia a la ejecución del producto en la implementación del sistema.

Velocidad de Aplicación: Costo de una aplicación lenta.

IV. METODOLOGÍA

4.1. Tipo y nivel de la investigación.

Esta investigación es de tipo tecnológico, el cual, según Sánchez et al. (2018), implica "un proceso planificado, sistemático y metódico de investigación que busca validar tecnología, es decir, demostrar su efectividad. Está muy ligada a la innovación tecnológica" (p. 81).

4.2. Diseño de Investigación

El diseño de investigación utilizado en esta tesis es de tipo tecnológico, lo que implica un proceso planificado, sistemático y metódico de investigación que busca validar tecnología, es decir, demostrar su efectividad. Este tipo de diseño está muy ligado a la innovación tecnológica y se enfoca en el desarrollo e implementación de soluciones tecnológicas para resolver problemas específicos.

Para llevar a cabo este proceso de investigación, se empleó la metodología ágil Scrum, que es un proceso iterativo e incremental para la implementación o desarrollo de soluciones tecnológicas. El uso de Scrum permitió la planificación, el seguimiento y la adaptación constante de la implementación, lo que resultó en una solución más efectiva y eficiente.

En cuanto a las estrategias y procedimientos empleados en la obtención de datos, se utilizó una combinación de técnicas cualitativas y cuantitativas, incluyendo encuestas, entrevistas, observaciones y análisis de datos. Estas técnicas permitieron recopilar información detallada sobre los requerimientos y necesidades de los usuarios, así como también sobre el desempeño y efectividad de la solución implementada.

Una vez obtenidos los datos, se procedió a su procesamiento, análisis e interpretación, utilizando herramientas estadísticas y de visualización de datos. Esto permitió identificar patrones y

tendencias, y tomar decisiones informadas sobre el diseño y la implementación de la solución.

4.3. Metodología de Implementación SCRUM

El tipo de metodología tecnológica que se aplicó fue Scrum. Esta metodología era un proceso iterativo e incremental para la implementación o desarrollo. Esto significaba que se tenían diferentes interacciones llamadas Sprint, que eran fijas en el tiempo. El objetivo de estos Sprint era construir un incremento del producto, y a las personas que interactuaban en la implantación se les llamaba Stakeholders. Para esto, fue necesario recopilar o elaborar una pila de elementos que estuvieran ordenados según su valor e importancia dentro de la implementación, y a esto se le llamó Product Backlog.
Scrum y los elementos que lo componían se nombraron como Product Backlog Ítem(PBI).

El ProductBacklog fue gestionado por el líder del producto, conocido como el Product Owner, mientras que la implementación fue llevada a cabo por el equipo de produccion. Después de construir los PBIs (Product Backlog Items), se realizó una reunión con el Product Owner, el Scrum Master y el equipo de producción para planificar los Sprint y así crear una pila de sprint.
Durante el inicio de los sprint, el equipo de produccion se reunió diariamente con los interesados para generar un feedback. Después de estas reuniones de incremento de los sprint, se llevó a cabo otra reunión de retrospectiva con los miembros del equipo Scrum.
Para asegurarse de que se completaron todos los PBIs de cada sprint, se creó un concepto de definición de terminado, que

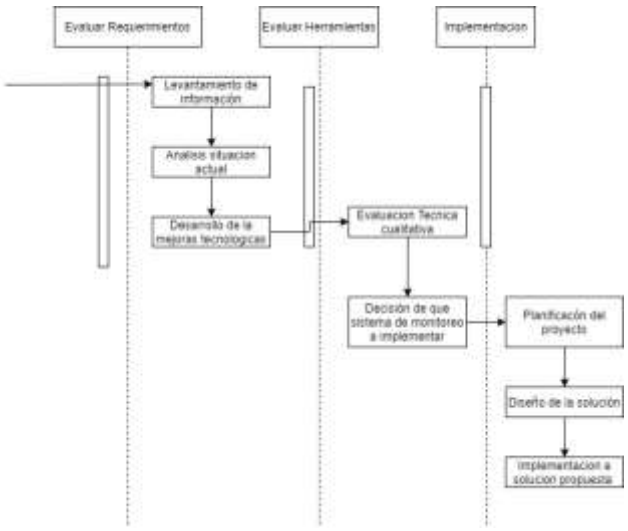
consistió en revisar una lista de acciones para concluir cada tarea o PBI.

En resumen, al aplicar scrum dentro de la implementación del sistema de monitoreo se tendrá:

- ARTEFACTOS: Se trabajaron los elementos que son la Product Backlog, Product Backlog Item, Sprint, Incremento de Producto y la Definición de Terminado.
- REUNIONES: Se tuvieron reuniones de planificación, revisión retrospectiva y reuniones diarias.
- ROLES: Se definieron las responsabilidades que se tenían que cumplir para la implementación del sistema de monitoreo.

Se desarrollaron tres Sprints, los cuales se detallan en la siguiente Figura 1:

Figura N ° 1 Planeamiento general de Sprint



Fuente: Propia

4.3.1. Inicio

4.3.1.1. Visión del proyecto.

El encargado del proyecto reunió a todos los involucrados en el proyecto con el fin de generar la visión del proyecto, teniendo en cuenta todas las necesidades que existen. Con esta visión, se obtuvo una vista general del proyecto, que se sometió a votación y se requirió el consentimiento de la mayoría de los integrantes. Después de obtener el consentimiento, la visión del proyecto se declaró formalmente ante todos.

la visión que fue definida es: “Implementar un sistema de monitoreo para la infraestructura de TI en el Instituto de Enfermedades Neoplásicas del Sur IRENSUR, como parte de ayuda auxiliar al área de TI en la gestión y administración de sus recursos tecnológicos, todo esto bajo la metodología SCRUM de esta forma mejorar la atención indirectamente del paciente oncológico y desarrollo de actividades del personal del hospital”.

4.3.1.2. Scrum Máster e interesados.

Después de establecer la visión del proyecto, es importante identificar a todos los involucrados en el proyecto y definir sus roles y responsabilidades. Esto ayudará a asegurar que todos los miembros del equipo estén alineados en cuanto a sus funciones y sepan lo que se espera de ellos.

La tabla presentada describe los roles de Scrum en la presente tesis llevado a cabo en el Hospital Irensur, en el área de Tecnología de la Información. Se especifican los nombres de los miembros del equipo y los roles asignados, incluyendo el Product Owner, Scrum Master y el Equipo de Desarrollo.

Tabla N ° 1 Roles de Interesados

Rol Scrum	Descripción	Persona asignada
Product Owner	Responsable de definir los requisitos y prioridades del proyecto	Jhusep Nuñez
Scrum Master	Responsable de asegurar que se sigan los procesos y se respeten los tiempos en el proyecto	Jhusep Nuñez
Equipo de desarrollo	Responsables de la ejecución del proyecto	Jhusep Nuñez
Stakeholders	Personas interesadas en el proyecto	Jhusep Nuñez, Victor Montes de Oca, Mauricio Gonzales
Cliente	Entidad que se beneficiará del proyecto	Hospital Irensur (TI)

Fuente: el investigador.

4.3.2. Product Backlog SPRINT 1

A continuación, en la tabla 2 se hace un listado de las pilas en detalle que llegan a componer los backlogs del sprint 1.

Tabla N ° 2 Tabla Planing del Sprint

SPRINT	INICIO	DURACIÓN
1	10-ene.-22	5

PILA DEL SPRINT

Backlog ID	Tarea	Tipo	Estado	Responsable
ISMITI01	Descripción de herramientas de monitoreo	Análisis		Prodruct owner
ISMITI02	Comparación de herramientas de monitoreo	Reunión		Prodruct owner
ISMITI03	Elección del sistema de monitoreo	Análisis		Prodruct owner
ISMITI03	Elección del sistema de monitoreo	Análisis		Prodruct owner y scrum master

Fuente : El Investigador.

En las siguientes tablas se describen en detalle las operaciones incluidas en cada pila.

Tabla N° 3 Pila 1 ISMIT01

Backlog	Descripción
ISMITI01: Descripción de herramientas de monitoreo	Se hará un listado de todas las herramientas de monitoreo que están sean open source
Nivel de priorización	**Alta**
Duración estimada	**10 horas**
Criterio de aceptación	Se deberá tener al menos 3 sistemas de monitoreo elegidos para poder pasar al siguiente paso
Flujo de proceso	• Hacer un listado de las necesidades principales • Enumerar lista de sistemas de monitoreo de • Hacer un cuadro resumen de ventajas y desventajas de cada de sistema de

Fuente : El Investigador

Tabla N ° 4 Pila 2 ISMITI02

Backlog	Descripción
ISMITI02: Comparación de herramientas de monitoreo	Se compara las herramientas según el cuadrante Gartner
Nivel de priorización	**Media**
Duración estimada	**6 horas**

Criterio de aceptación	Se escogerá el sistema de monitore que tenga mejor posición en el cuadrante Gartner
Flujo de proceso	• Hacer el listado de las 3 herramientas que se seleccionaron. • hacer cuadro de ubicación según el cuadrante • Resaltar los beneficios del sistema de monitoreo según indica Gartner

Fuente: El Investigador.

Tabla N° 5 Pila 3 ISMITI03

Backlog	**Descripción**
ISMITI03: Elección del sistema de monitoreo	Al ya tener elegido el sistema de monitoreo juntamente con jefatura de TI de IRENSUR, se hará un pre-planeamiento
Nivel de priorización	**Alta**
Duración estimada	**4 horas**
Criterio de aceptación	Documento preliminar de proyección del sistema y el versiona miento y donde se hospedará y como se instalará

Flujo de proceso	• Verificar a detalle la herramienta elegida • Hacer una lista de riesgos de implantación • Requisitos del sistema de monitoreo

Fuente: el investigador.

4.3.2.1. Desarrollo de Backlog

ISMITI01

En la reunión que se tuvo con el producto backlog y el analista se llegó a generar un listado de sistemas de monitoreo Open source los cuales son :

- Zabbix.
- Cacti.
- Nagios
- Prometeus

Los criterios para la elección de estas herramientas fueron:

- Proporcionar indicadores sobre interrupciones y degradación del servicio
- Detectar interrupciones del servicio y actividades no autorizadas
- Escalable
- Capaz de manejar y procesar grandes cantidades de datos de monitoreo
- Recopile métricas del sistema/aplicación en tiempo real
- Capaz de proporcionar información a largo plazo para una mejor planificación de la capacidad.

- Alta disponibilidad
- Admite todas las aplicaciones modernas en la nube y en contenedores.
- Admite herramientas de visualización de métricas
- Buena trazabilidad
- Tenga una buena interfaz fácil de usar.

ISMITI02

De acuerdo a Gartner (2022), se puede encontrar un listado de sistemas de monitoreo y su calificación en la publicación de IT infrastructure monitoring tools, en la siguiente tabla se muestra un resumen de estas herramientas.

Tabla N° 6 Rating Herramientas De Monitoreo De Infraestructura De TI

Calificación	Ratings	Nombre de Sistema	Tipo de Licencia
4.5	394		Licencia comercial
4.4	306	OpManager	Licencia comercial
4.5	286	Zabbix	Open Source
4.5	211	Datadog	Shareware
4.3	202	SolarWinds Server & application Monitor	Licencia comercial
4.3	166	Nagios XI	Open Source
4.6	158	VMware vrealize Operations	Shareware

Fuente: GARTNER (https://www.gartner.com/reviews/market/it-infrastructure-monitoring-tools)

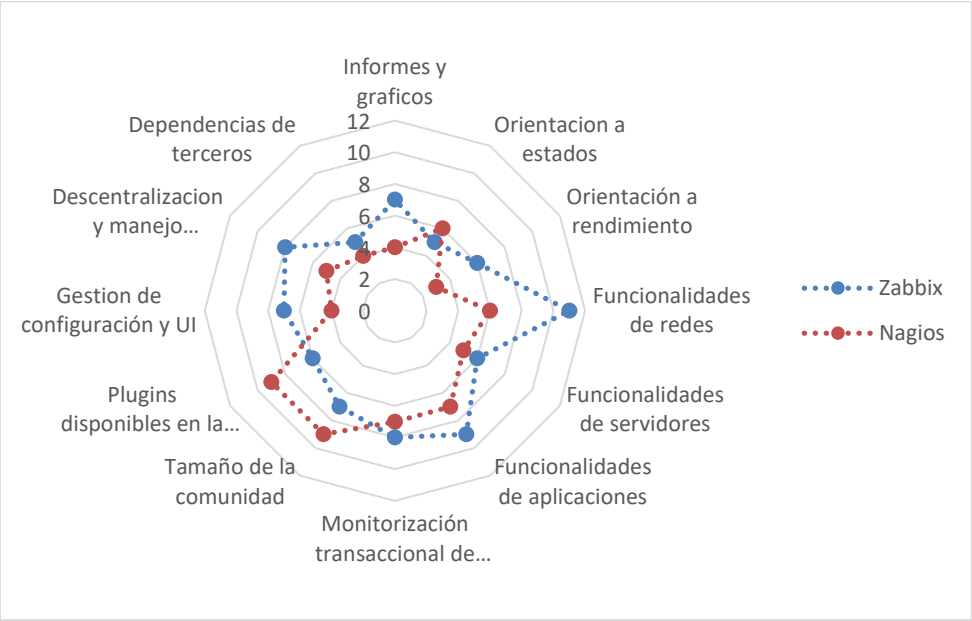
Según el cuadro que nos presente el estudio de Gartner se toma en cuenta los 10 primeros sistemas de monitoreo de los cuales se elegirá los sistemas que tienen licencia open source.

En este caso los sistemas a elegir son **Zabbix y Nagios XI.**

ISMITI03

De acuerdo con las conclusiones que se tiene en el backlog ISMITI02 se hizo un cuadro de comparación entre las herramientas de Nagios XI y Zabbix mostrando las ventajas y desventajas de cada uno.

Figura N ° 2 Comparativa de sistemas de monitoreo



Fuente: El Investigador.

En este cuadro se destaca las bondades que tiene Zabbix ante NAGIOS, teniendo como punto de quiebre las funcionalidades de red y el manejo distribuido del sistema .

Al concluir con la elección del sistema de monitoreo , se necesita ver los requisitos preliminares que se necesitaran para el desarrollo y despliegue de Zabbix, según la información oficial de Zabbix los requisitos mínimos son:

- Sistema operativo: Linux o Unix
- Procesador: CPU de 64 bits, dual-core o superior
- Memoria RAM: 2 GB o más
- Espacio en disco: al menos 10 GB de espacio libre
- Base de datos: MySQL, PostgreSQL, Oracle o SQLite

- Navegador web: Google Chrome, Mozilla Firefox, Microsoft Edge o Safari

En la siguiente figura se verifica el estado y cumplimiento de cada uno de los backlogs que se planearon en realizar para poder complementar el sprint1.

Figura N ° 3 SCRUM Board Sprint 1

Fuente : El Investigador.

4.3.3. Sprint 2 Análisis de la infraestructura de TI

4.3.3.1. Objetivo:

El objetivo de este Sprint es analizar toda la infraestructura de TI

del IREN SUR, llegando a detallar la topología existente que tiene y la identificación de los servidores y servicios críticos que se tiene de la mano y enmarcado con los objetivos que se persigue dentro de la institución.

Tabla N° 7 Plan de lanzamiento Sprint2

Enfoque	Contenido
Requisitos	Los requisitos para el desarrollo de este sprint son los siguientes. • Requerimientos de software Word, Excel , navegador, trello, draw.io. • Requerimientos de hardware: laptop, impresora,
Análisis de la topología de red	Se hará un estudio de la topología actual que se tiene dentro del IRENSUR
Identificación de servicios críticos	Se hará una reunión con el encargado de TI y redes para el análisis de los procesos críticos
Identificación de dispositivos críticos	Se llegará a identificar a los dispositivos sean estos swicth, router, ap's, servidores, que sean indispensables su funcionamiento.

Correspondencia de servicios críticos de TI y Objetivos de institucionales	Se hará un cruce de los equipos y servicios críticos y si los objetivos que persigue el IRENSUR guarda relación.
Diseño de solución	De acuerdo con los puntos anteriores se diseñará la solución a implementar para el monitoreo de la Infraestructura de TI del IREN SUR
	Nota: Estas actividades serán realizadas por el product owner.

Fuente: El investigador

4.3.3.2. Planing de sprint

La siguiente tabla se muestra los backlogs para la pila de sprint 2

Tabla N° 8 Planing del Sprint 2

SPRINT	INICIO	DURACIÓN
2	**18-ene.-22**	**5**

PILA DEL SPRINT

Backlog ID	Tarea	Tipo	Estado	Responsable
ISMITI04	Análisis de la topología de red	Análisis		Product owner
ISMITI05	Identificación de servicios críticos	Reunión		Product owner
ISMITI06	Identificación de dispositivos críticos	Análisis		Product owner
ISMITI07	Correspondencia de servicios críticos de TI y Objetivos de institucionales	Análisis		Product owner
ISMITI08	Diseño de implementación de sistema de monitoreo	Análisis		Product owner

Fuente: El investigador.

4.3.3.3. Product Backlog

A continuación, en las siguientes tablas se hace un listado en detalle que llegan a componen los backlogs del sprint 2.

Tabla N° 9 Pila 1 ISMIT04

Backlog	Descripción
ISMITI04: Análisis de la topología de red	Se hará un inventariado de todos los equipos de red y su distribución dentro de la red LAN del IRENSUR
Nivel de priorización	**Alta**
Duración estimada	**10 horas**
Criterio de aceptación	Tener claro la estructura de red del IRENSUR plasmado en un diagrama
Flujo de proceso	• Hacer un inventariado de los equipos de red. • Enumerar los segmentos de red. • Hacer diagramas de topología de red

Fuente : El Investigador

Tabla N° 10 Pila 2 ISMIT05

Backlog	Descripción
ISMITI05: Identificación de servicios críticos.	A esto se hará un listado de todos los servicios que se tiene dentro de la red LAN del IRENSUR
Nivel de priorización	**Media**
Duración estimada	**6 horas**
Criterio de aceptación	Resumen de servicios críticos identificados.
Flujo de proceso	• Enumeración de servicios. • Realizar matriz de servicios y calificación según su criticidad. • Cuadro resumen de servicios críticos.

Fuente : El Investigador

Tabla N° 11 Pila 3 ISMIT06

Backlog	Descripción
ISMITI06: Identificación de dispositivos críticos.	A esto se hará un listado de todos los dispositivos de la infraestructura de TI que se tiene dentro de la red LAN del IRENSUR
Nivel de priorización	**Media**
Duración estimada	**6 horas**
Criterio de aceptación	Resumen de dispositivos críticos identificados.
Flujo de proceso	• Enumeración de dispositivos. • Realizar matriz de dispositivos y calificación según su criticidad. • Cuadro resumen de dispositivos críticos.

Fuente : El Investigador

Tabla N° 12 Pila 4 ISMIT07

Backlog	Descripción
ISMITI07: Correspondencia de servicios críticos de TI y Objetivos de institucionales.	Se llegará a comparar los objetivos que tiene el IRENSUR con los servicios y dispositivos críticos.
Nivel de priorización	**Media**
Duración estimada	**6 horas**
Criterio de aceptación	Cuadro resumen de servicios y dispositivos críticos validados.

Flujo de proceso	• Listado de los objetivos institucionales del IRENSUR. • Matriz de objetivo – servicios y equipos críticos. • Lista de servicios y equipos a monitorear.

Fuente : El Investigador

Tabla N° 13 Pila 5 ISMIT08

Backlog	**Descripción**
ISMITI08: Diseño de implementación de sistema de monitoreo.	Diseñara la estructura del monitoreo y su implantación,
Nivel de priorización	**Media**
Duración estimada	**14 horas**
Criterio de aceptación	Diseño implementación del sistema de monitoreo.
Flujo de proceso	• Requisitos de implementación de servidor y servidor proxy. • Matriz de riesgos. • Lista de requerimientos • Diseño topológico de servidores de monitoreo. • Diseño de despliegue • Diseño de interacción del sistema de monitoreo. • Diseño interacción de notificación de alertas.

- To be – asis
- Cheklist de verificación de instalación

Fuente : El Investigador

4.3.3.4. Desarrollo de backlog

ISMITI04 Análisis de la topología de red

Se hizo un inventariado de los equipos de red, que se tiene dentro de la red LAN.

Tabla N° 14 lista de equipos IRENSUR

Marca	Cantidad
HP	31
Grandstream	32
Other devices	66
Dell	11
Hon Hai	15
Lenovo	8
MSI	7
Gigabyte	7

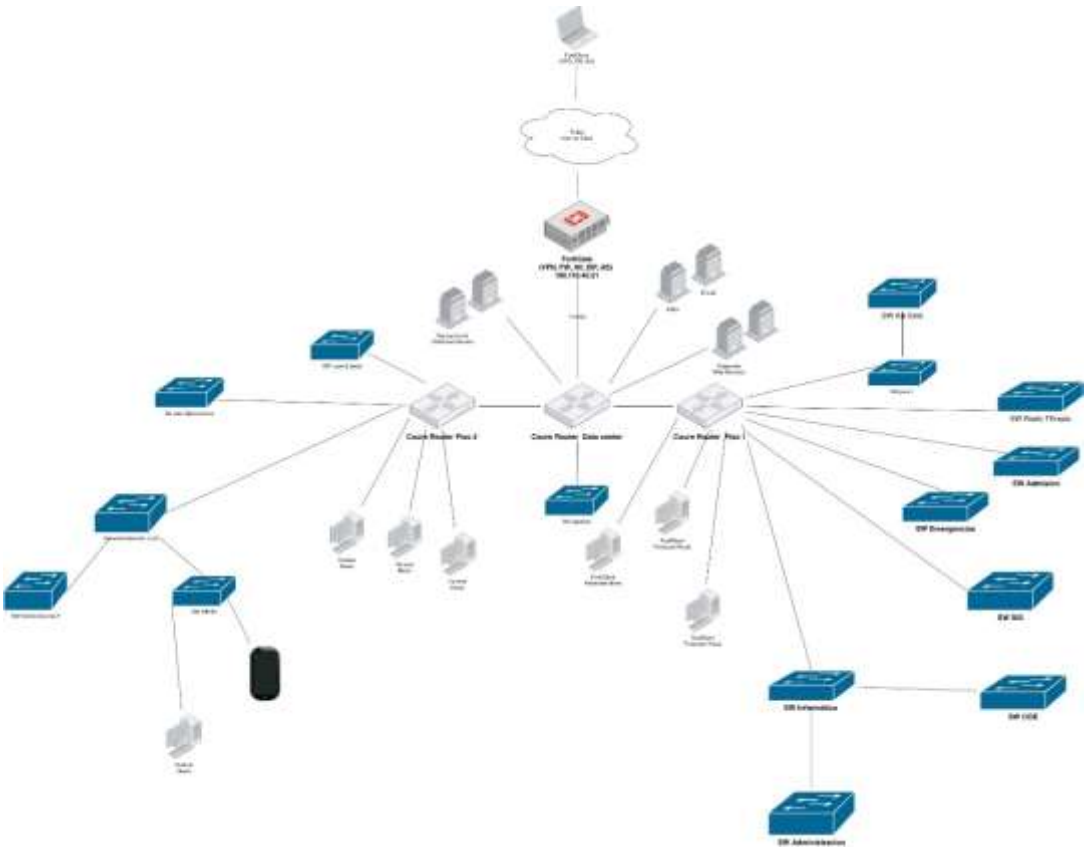
Fuente: Fortinet de IRENSUR

Los segmentos de red que tiene dentro del IRENSUR son los siguientes

- Segmento principal.
- Segmento secundario de cámaras
- Segmento secundario de teléfonos
- Segmento secundario de wifi
- Segmento de Switch

En la siguiente figura se muestra la topología de red de nuestro nodo estrella. En el centro se encuentra nuestro switch principal, del cual se ramifican varios switches secundarios que se conectan a diferentes dispositivos de red. Además, contamos con una serie de servidores y dispositivos finales que se conectan a los switches secundarios correspondientes. Todos los dispositivos están configurados con las direcciones IP y máscaras de subred correspondientes para permitir una correcta comunicación en la red.

Figura N ° 4 Topología actual del IRENSUR



Fuente: El Investigador

ISMITI05 Identificación de servicios críticos

Según descripción del encargado los servicios críticos son:

- SC1:Sistema clínico del IRENSUR.
- SC2:Base de datos

- SC3:Servicio de correo electrónico
- SC4:Servicio de archivos compartidos
- SC5: SIGA.
- SC6: SIAF.
- SC7: Historias medicas
- SC8: DICOM
- SC9: Servicio de internet.

ISMITI06 Identificación de dispositivos críticos

Los equipos críticos que se tienen son

- DC1: Firewall
- DC2: Servidor Lenovo
- DC3: Servidor de virtualización.
- DC4: NVR
- DC5: Qnap.
- DC6: Mikrotic wifi
- DC7: Servidor correo
- DC8: Reloj marcador
- DC9: Switch Core
- DC10: Switch de informática
- DC11: Impresora de admisión.
- DC12: Computadora de farmacia
- DC13: SWCORE
- DC14: Telefonía IP.

ISMITI07 Correspondencia de servicios críticos de TI y Objetivos de institucionales

Los objetivos institucionales que cuenta el IRENSUR que asemejan al área de TI indirectamente son:

- OBI1:”Incrementar el acceso a la atención oncológica de calidad, de acuerdo con las necesidades de la población en el marco de la Macro Región Sur del país y bajo criterios de equidad, dando prioridad a las personas de escasos recursos económicos.”

- OBI2: “Desarrollar un adecuado campo clínico que permita la investigación, docencia y capacitación permanente de los profesionales de la salud y técnicos del sector.”

Después de la reunión con el personal de TI del Irensur, se crearon dos matrices de comparación. La primera se enfocó en identificar los servicios críticos y determinar cuáles tienen mayor peso de acuerdo con los objetivos institucionales. La segunda matriz se centró en los equipos de TI presentes en toda la infraestructura del Iren. Estas matrices se utilizaron como punto de premisas condicionales para el monitoreo de la infraestructura de TI del IRENSUR.

Tabla N° 15 Matriz Servicios Críticos – Objetivos Institucionales

Servicios Críticos	**OBI1**	**OBI2**
SC1: Sistema clínico del IRENSUR.	Alto	Alto
SC2: Base de datos	Alto	Alto
SC3:Servicio de correo electrónico	Bajo	Medio
SC4:Servicio de archivos compartidos	Medio	Medio
SC5: SIGA.	Bajo	Bajo
SC6: SIAF.	Bajo	Bajo
SC7: Historias medicas	Alto	Alto
SC8: DICOM	Medio	Medio
SC9: Servicio de internet.	Medio	Alto

Nota: La tabla muestra la matriz de dispositivos críticos y objetivos institucionales del Iren Sur. Los colores se utilizaron para resaltar los niveles de cumplimiento de cada dispositivo crítico para cada objetivo institucional. Rojo representa un nivel alto de cumplimiento, amarillo representa un nivel medio de cumplimiento y verde representa un nivel bajo de cumplimiento.

Fuente: El Investigador.

Tabla N° 16 Matriz Dispositivos Críticos - Objetivos específicos

Dispositivos Criticos	OBI1	OBI2
DC1: Firewall	Alto	Alto
DC2: Servidor Lenovo	Alto	Alto
DC3: Servidor de virtualización.	Alto	Alto
DC4: NVR	Medio	Bajo
DC5: Qnap.	Medio	Alto
DC6: Mk de wifi	Medio	Bajo
DC7: Servidor correo	Medio	Medio
DC8: Reloj marcador	Bajo	Bajo
DC9: Switch core	Alto	Alto
DC10: Switch de informática	Medio	Bajo
DC11: Impresora de admisión.	Medio	Bajo
DC12: Computadora de farmacia	Medio	Bajo
DC13: SWCORE	Bajo	Bajo
DC14: Telefonía IP	Medio	Bajo

Nota: Los colores indican el nivel de importancia que cada servicio tiene para cada objetivo institucional. Fuente: El Investigador.

ISMITI08 Diseño de implementación de sistema de monitoreo

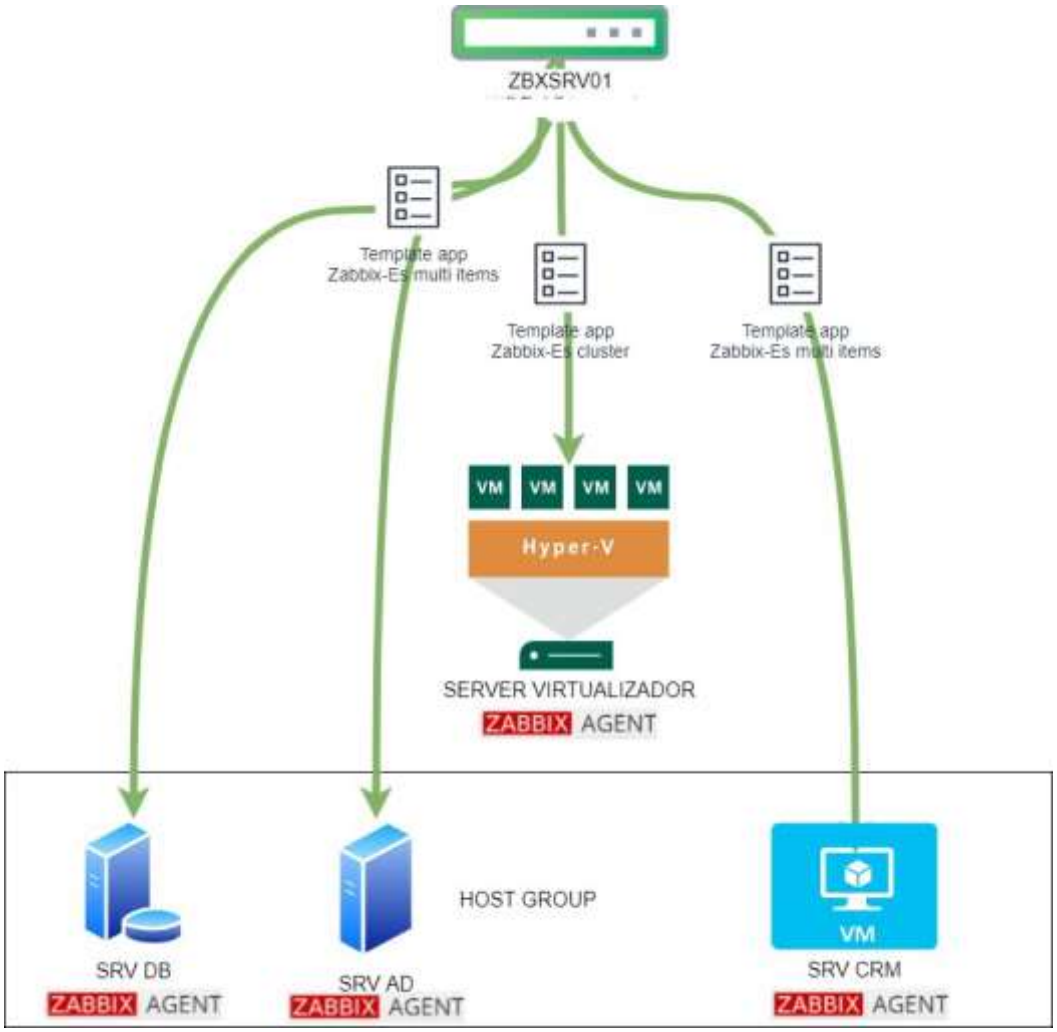
Para esto teniendo en cuenta la estructura topológica y la precariedad de disposición de servidores se propone :

- Crear un servidor en nube que tenga el monitoreo de 24*7 tanto los servicio y dispositivos críticos
- Tener un equipo remoto que sirva como conexión proxy entre el servidor de monitoreo y la LAN del IRENSUR.
- El servidor de proxy de monitoreo

A esto se tendrá tener en consideración la matriz de riesgos al implementar la solución.

La interacción entre el sistema de monitoreo y los equipos que cuenten con un agente se llevará a cabo de acuerdo con la figura siguiente.

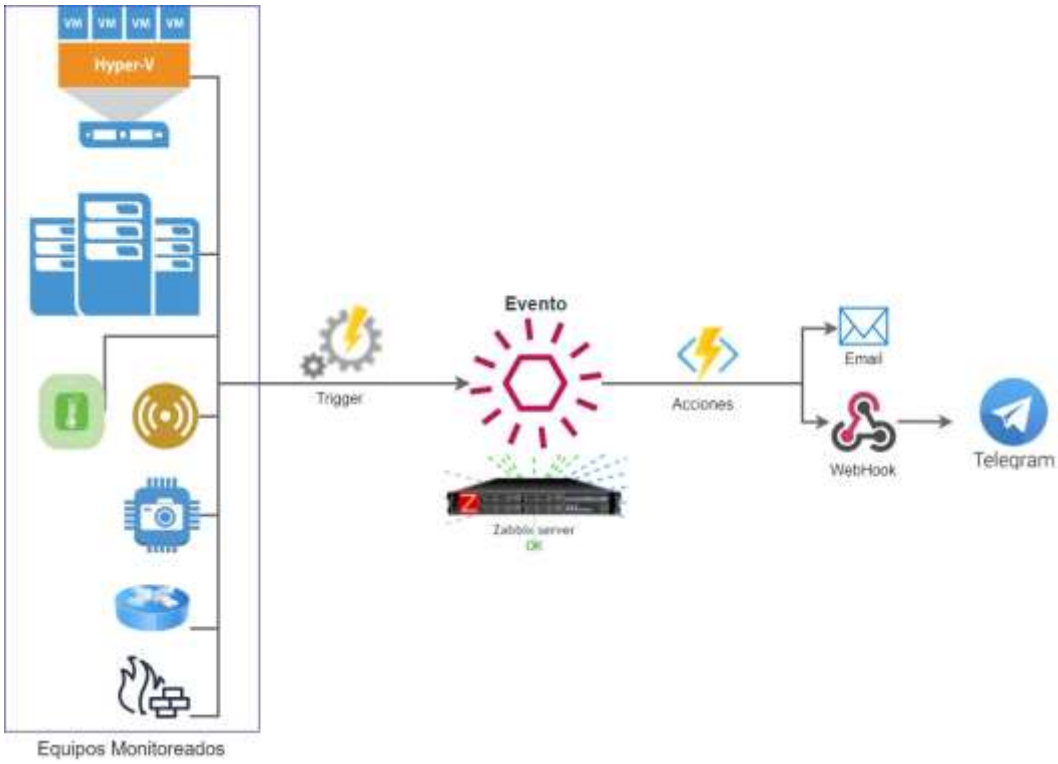
Figura N ° 5 Diagrama de control y monitoreo.



fuente: El Investigador.

En cuanto a la interacción entre el servicio y las notificaciones por correo o el uso del chat bot de Telegram, se generaron según la configuración que se tenía dentro de los eventos que se generaron de acuerdo con el monitoreo. Estos podían ser constantes o eventuales. En el siguiente diagrama se muestra la interacción de estos.

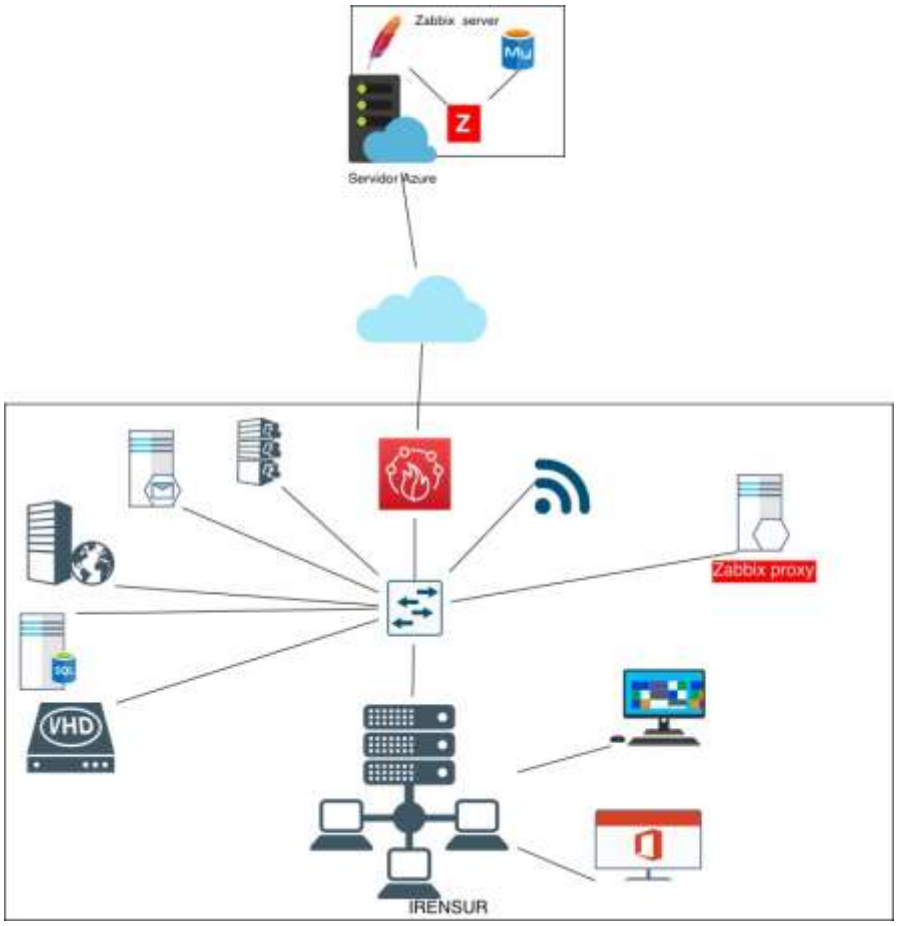
Figura N ° 6 Diagrama de ejecución de eventos y acciones de notificación



Fuente: El Investigador.

Para esto se elaboró un diagrama topológico donde se mostraba cómo estaba la implementación del servidor Zabbix en la nube y de cómo se integró en la red LAN del IRENSUR.

Figura N ° 7 Topología de implementación de sistema de monitoreo.

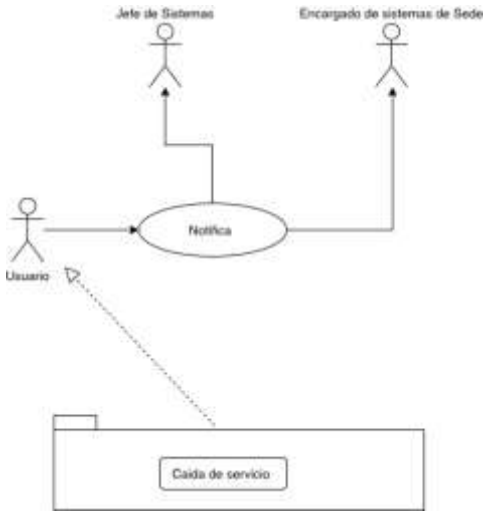


Fuente: El Investigador.

TO BE AS IS

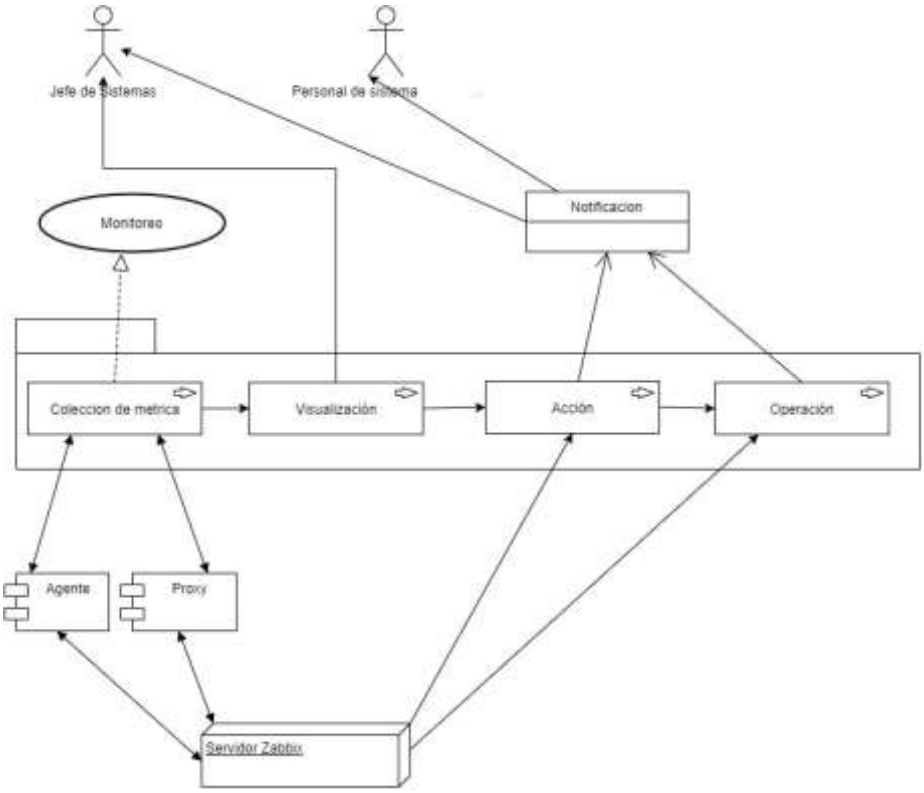
En los siguientes diagramas se muestra el **ASIS** de cómo se controlaba los servicios dentro de la LAN del IRENSUR y el **TOBE** de cómo se monitorea la infraestructura de TI del IRENSUR.

Figura N ° 8 AS IS



Fuente : El Investigador

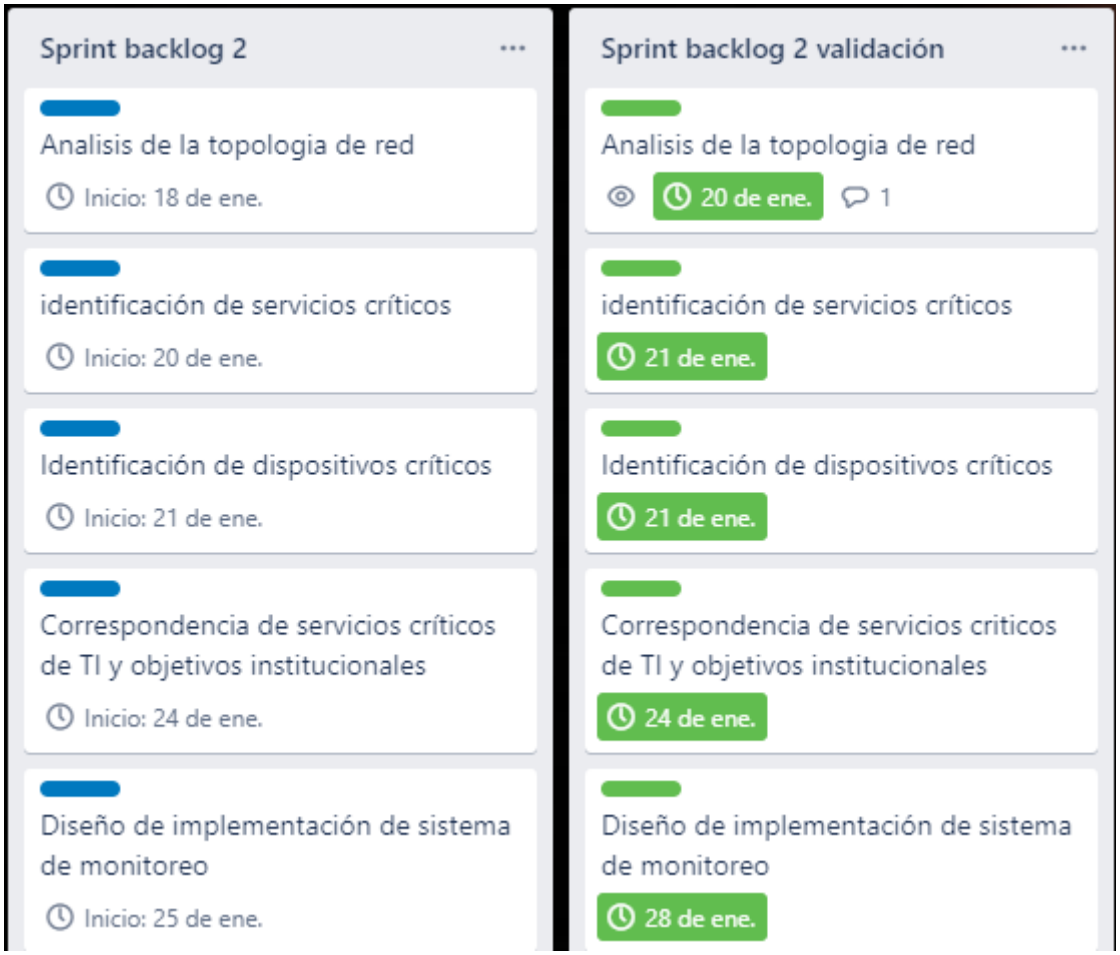
Figura N ° 9 TO BE



Fuente: El investigador.

En el siguiente gráfico se verificó el estado y cumplimiento de cada uno de los backlogs que se planearon para complementar el sprint 2.

Figura N ° 10 Scrum Board de SPRINT 2



Fuente: El Investigador.

4.3.4. Sprint 3 Instalación y Despliegue

4.3.4.1. Objetivo:

El objetivo de este Sprint es instalar el |sistema de monitoreo que se llegó a elegir en el sprint 1 y luego de esto desplegar tomando como prioridad su monitoreo los servicios y dispositivos críticos que se observaron en el sprint 2

Tabla N° 17 Plan de lanzamiento Sprint 3

Enfoque	Contenido
Requisitos	Los requisitos para el desarrollo de este sprint son los siguientes. • Requerimientos de software Word, Excel , navegador, trello, draw.io, Azure, servidor LAMP (Linux, website server Apache, servidor de base datos MySQL, PHP), Ubuntu server 20.04 • Requerimientos de hardware: laptop, impresora, servidor cloud, Raspberry pi
Creación de servidor en Nube	Se hará un estudio de la topología actual que se tiene dentro del IRENSUR
Instalación de servidor Zabbix en nube	Se hará una reunión con el encargado de TI y redes para el análisis de los procesos críticos
Instalación de servidor proxy en sede IRENSUR	Se llegará a identificar a los dispositivos sean estos swicth,

	router, ap's, servidores, que sean indispensables su funcionamiento.
Configuración de host a nivel snmp	Se hará un cruce de los equipos y servicios críticos y si los objetivos que persigue el IRENSUR guarda relación.
Configuración de agentes de monitoreo	De acuerdo con los puntos anteriores se diseñará la solución a implementar para el monitoreo de la Infraestructura de TI del IREN SUR
Configuración de alertas para Bot Telegram	Se creará un agente robot dentro de la plataforma Telegram para el servicio de notificaciones
Creación de Dashboard e informes	Ya con la data que se tiene se creara tableros de notificación y monitoreo de la infraestructura de TI del IRENSUR.
	Nota: Estas actividades serán realizadas por el implantador.

Fuente: El Investigador.

4.3.4.2. Planing de sprint

En la siguiente tabla se muestra los backlogs para la pila de sprint 3

Tabla N° 18 Planing del Sprint 3

SPRINT	INICIO	DURACIÓN
3	**03-feb.-22**	**30**

PILA DEL SPRINT				
Backlog ID	**Tarea**	**Tipo**	**Estado**	**Responsable**
ISMITI09	Creación de servidor en Nube	Ejecución		Implementador
ISMITI10	Instalación de servidor Zabbix en Nube	Ejecución		Implementador

ISMITI11	Instalación de servidor Proxy en sede de IRENSUR	Ejecución	Implementador
ISMITI12	Configuración de host a nivel de snmp	Ejecución	Implementador
ISMITI13	Configuración de agentes de monitoreo	Ejecución	Implementador
ISMITI14	Configuración de alertas para Bot Telegram	Ejecución	Implementador
ISMITI15	Creación de Dashboard e informes	Ejecución	Implementador

Fuente: El Investigador.

4.3.4.3. Product Backlog

A continuación, en las siguientes tablas se hace un listado en detalle que llegan a componer los backlogs del sprint 3.

Tabla N° 19 Pila 1 ISMIT09

Backlog	**Descripción**
ISMITI09: Creación del servidor en nube	Para esto se creará un servidor virtual con SO Linux en la nube de Azure.
Nivel de priorización	**Media**
Duración estimada	**8 horas**
Criterio de aceptación	Administración remota del servidor
Flujo de proceso	• Tener los accesos a gestor de Azure • Elegir un tipo de servidor con pocos recursos. • Poner en marcha el servidor • Publicar el puerto ssh para administración de servidor

Fuente: El Investigador

Tabla N° 20 Pila 2 ISMIT10

Backlog	Descripción
ISMITI10: Instalación del servidor Zabbix en nube	Ser creara los repositorios y permisos para puesta de ejecución del sistema de monitoreo y los servicios LAMP necesarios
Nivel de priorización	**Alta**
Duración estimada	**8 horas**
Criterio de aceptación	Puesta en ejecución de sistema de monitoreo
Flujo de proceso	• Actualización de repositorios • Instalación del servidor Apache. • Instalación de servidor de base de datos MySQL • Publicar el puerto ssh para administración de servidor. • Instalación del sistema de monitoreo Zabbix.

Fuente : El Investigador

Tabla N° 21 Pila 3 ISMIT11

Backlog	Descripción
ISMITI11: Instalación del servidor Proxy en sede del IRENSUR	Se actualizará los repositorios del rasbperry PI y los servicios

	LAMP necesarios para su ejecución
Nivel de priorización	**Alta**
Duración estimada	**8 horas**
Criterio de aceptación	Conexión con el sistema de monitoreo
Flujo de proceso	• Actualización de repositorios • Instalación de servidor de base de datos MySQL. • Instalación de servidor proxy Zabbix. • Configuración de puertos de conexión a servidor Zabbix • Publicar el puerto ssh para administración de servidor

Fuente: El Investigador

Tabla N° 22 Pila 4 ISMIT12

Backlog	**Descripción**
ISMITI12: Configuración de host a nivel snmp	Se agregará los equipos de redes y algún otro servidor por el protocolo snmp
Nivel de priorización	**Alta**
Duración estimada	**16 horas**
Criterio de aceptación	Equipos monitoreados por snmp

Flujo de proceso	• Listar equipos soportados por snmp. • Definición de key community para uso de monitoreo. • Agregar equipos a sistema de monitoreo por snmp

Fuente: El Investigador

Tabla N° 23 Pila 5 ISMIT13

Backlog	**Descripción**
ISMITI13: Configuración de agentes de monitoreo.	Se agregará equipos que no soporten o no tengan configurado el protocolo snmp al igual para servicios
Nivel de priorización	**Alta**
Duración estimada	**8 horas**
Criterio de aceptación	Equipos monitoreados por agentes
Flujo de proceso	• Listado de equipos y servicios • Agregar equipos y servicios al sistema de monitoreo

Fuente: El Investigador

Tabla N° 24 Pila 6 ISMIT14

Backlog	Descripción
ISMITI14: Configuración de alertas para Bot Telegram	Se definirá a que usuarios se les hará llegar las notificaciones y que nivel de alertas se notificará, a esto se creará un Bot en la plataforma de Telegram y luego tener que configurar la integración con el sistema de monitoreo
Nivel de priorización	**Alta**
Duración estimada	**16 horas**
Criterio de aceptación	Notificaciones de alertas por Telegram
Flujo de proceso	• Listado de usuarios a notificar. • Creación de Bot en Telegram. • Configuración de agente de Bot Telegram en el sistema de monitoreo. • Configuración de alarmas en agente Bot. • Pruebas de recepción de alertas.

Fuente: El Investigador

Tabla N° 25 Pila 7 ISMIT15

Backlog	Descripción
ISMITI15: Creación de Dashboard e informes.	Creación de centros de control de acuerdo con la matriz de servicios y dispositivos críticos, se configurará informes de los

	eventos más relevantes transcurridos en el mes.
Nivel de priorización	**Alta**
Duración estimada	**16 horas**
Criterio de aceptación	Centros de control configurados en página principal del sistema de monitoreo
Flujo de proceso	• Listado de Dashboard a diseñar. • Configuración de widgets para cada Dashboard. • Pruebas de visualización de Dashboard.

Fuente : El Investigador

4.3.4.4. Desarrollo de backlog

ISMITI09 Creación de servidor en Nube

Los pasos por seguir para la creación del servidor en nube son: la configuración del servidor para el sistema de monitoreo es

- Sistema operativo Ubuntu server 20.04 lts.
- 3GB de RAM.
- 30GB de espacio en disco.

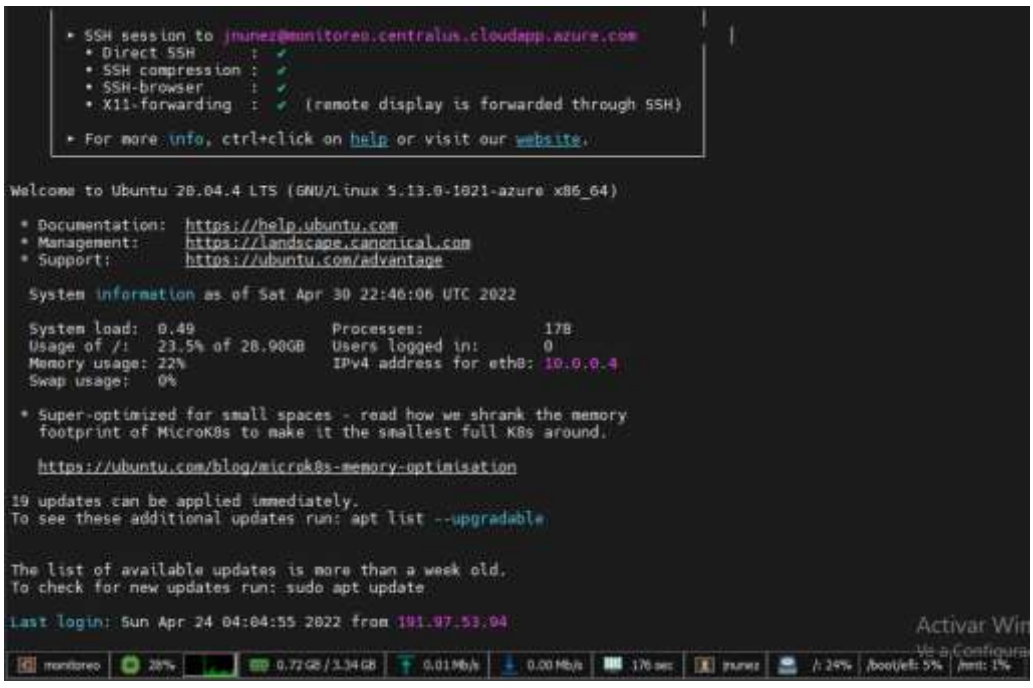
Presentando una estructura representada en la siguiente figura teniendo como estado final la ejecución del servidor

Figura N ° 11 Estatus de servidor de monitoreo a nivel de gestor Azure

Fuente: El Investigador.

En la siguiente figura se muestra a nivel consola la ejecución del equipo instalado y su operatividad.

Figura N ° 12 Estatus de servidor a nivel de aplicación



Fuente: El Investigador.

ISMITI10 Instalación de servidor Zabbix en Nube

Los requisitos previos para poder desarrollar este backlog es ya tener instalado el SO en nube

Para esto se actualizará los repositorios de conexión al servidor de Zabbix y teniendo como estado final la ejecución del sistema de monitoreo.

Figura N ° 13 Comandos de actualización de paquetes

```
wget https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/
zabbix-release/zabbix-release_6.0-1+ubuntu$(lsb_release -rs)_all.deb
sudo dpkg -i zabbix-release_6.0-1+ubuntu$(lsb_release -rs)_all.deb
sudo apt update
```

Fuente: El Investigador.

Al ejecutar este paso anterior se instaló el servicio web apache y la base de datos ejecutando unos comandos en la conexión consola como se puede ver en el siguiente gráfico.

Figura N ° 14 Comandos de instalación de servicios

```
sudo apt -y install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
```

Fuente: El investigador.

Luego de haber instalado los servicios de Zabbix y el servicio web se instalará el motor de base de datos ejecutando los siguientes comandos.

Figura N ° 15 Comandos de instalación de María DB.

```
sudo apt install software-properties-common -y
curl -LsS -O https://downloads.mariadb.com/MariaDB/mariadb_repo_setup
sudo bash mariadb_repo_setup --mariadb-server-version=10.6
sudo apt update
sudo apt -y install mariadb-common mariadb-server-10.6 mariadb-client-10.6
```

Fuente: El Investigador.

Una vez completada la instalación, se inició el servicio MariaDB y habilitar para que se inicie en el arranque utilizando los siguientes comandos:

Figura N ° 16 Comandos de habilitación

```
sudo systemctl start mariadb
sudo systemctl enable mariadb
```

Fuente : El Investigador.

Al culminar la instalación y habilitación se tiene que configurar la base de datos para eso se ejecutó los siguientes comandos.

Figura N ° 17 Comandos de invocación de configuración de base de datos

```
sudo mysql_secure_installation
```

Fuente : El Investigador.

A esto se configuro el servicio de la base de datos y se cambió la contraseña por defecto que tiene el usuario admin

Figura N ° 18 Configuración y cambio de contraseña

```
Enter current password for root (enter for none): Press Enter
Switch to unix_socket authentication [Y/n] y
Change the root password? [Y/n] y
New password: rootDBpassword
Re-enter new password: rootDBpassword
Remove anonymous users? [Y/n]: Y
Disallow root login remotely? [Y/n]: Y
Remove test database and access to it? [Y/n]:  Y
Reload privilege tables now? [Y/n]:  Y
```

Fuente: El Investigador.

Al culminar esta configuración se creará la base de datos que usará el sistema de monitoreo.

Figura N ° 19 Comandos de creación de base de datos

```
sudo mysql -uroot -p'rootDBpass' -e "create database zabbix character set utf8mb4 collate utf8mb4_bin;"
sudo mysql -uroot -p'rootDBpass' -e "grant all privileges on zabbix.* to zabbix@localhost identified by 'zabbixDBpass';"
```

Fuente: El Investigador.

A esto se le asigno el esquema de la base de datos el cual se descargó del repositorio de Zabbix.

Figura N ° 20 Comando de importación de esquema

```
sudo zcat /usr/share/doc/zabbix-sql-scripts/mysql/server.sql.gz | mysql -uzabbix -p'zabbixDBpass' zabbix
```

Fuente: El Investigador

Cuando se culminó esta lista de comandos se llegó a configurar el archivo zabbix_server.conf

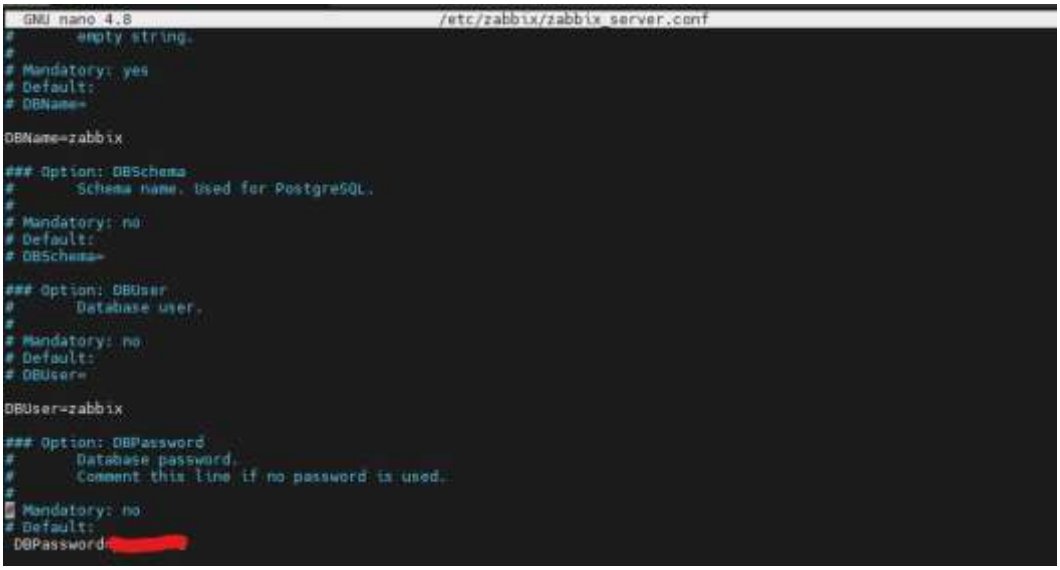
Figura N ° 21 Comando de edición de archivo de configuración de Zabbix

```
sudo nano /etc/zabbix/zabbix_server.conf
```

Fuente: El Investigador

La data que se configuro dentro del archivo de configuración fue el nombre de la base de datos, el usuario de base datos y la contraseña de conexión a la base de datos .

Figura N ° 22 Modificación de archivo de configuración



Fuente: El Investigador.

Después del seteo de parámetros del archivo de configuración se habilito e inicio el servicio de apache.

Figura N ° 23 Comando de habilitación e inicio de servicio

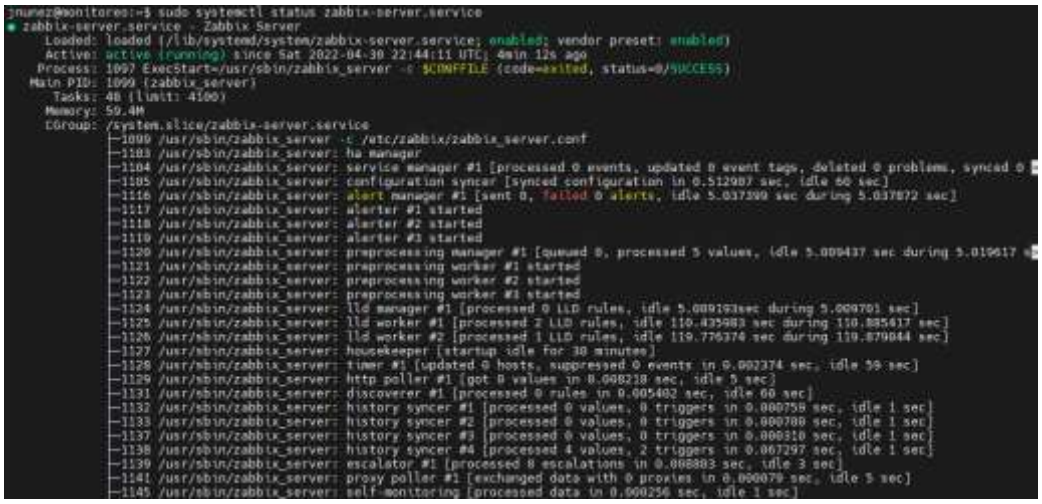
```
sudo systemctl restart apache2
sudo systemctl enable apache2
```

Fuente: el investigador.

Para poder iniciar la instalación del servicio de monitoreo se ingresó a la dirección web http://monitoreo.centralus.cloudapp.azure.com/ el cual se generó en la consola de gestión de servidor del Azure, con esto paso se completa la instalación del sistema de monitoreo todo esto teniendo en cuenta con los requisitos mínimos que se indicó en la pila 4 del sprint 2.

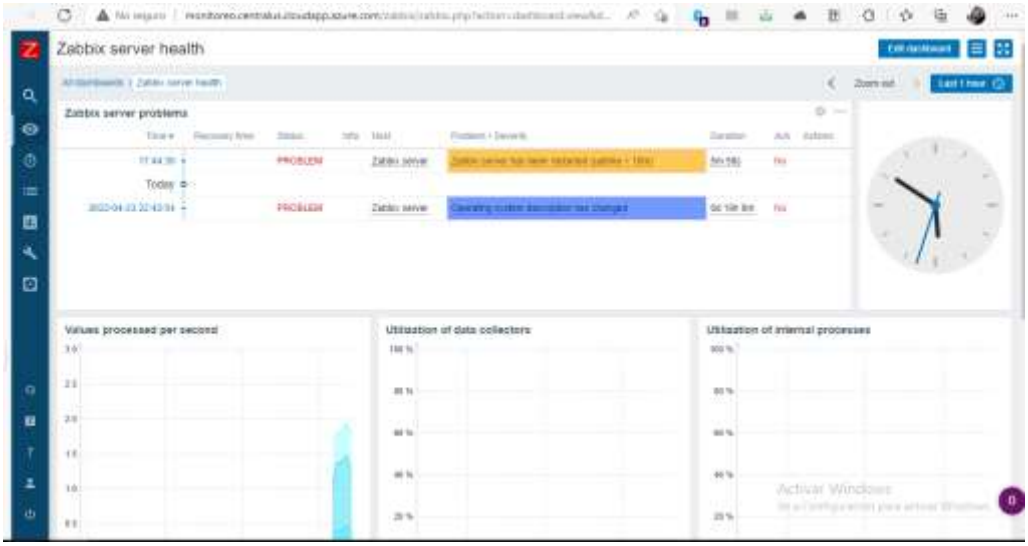
Teniendo como parte final la puesta en linea el servicio

Figura N ° 24 Estatus de servicio a nivel de servidor



Fuente: El investigador

Figura N ° 25 Estatus a nivel de aplicación web



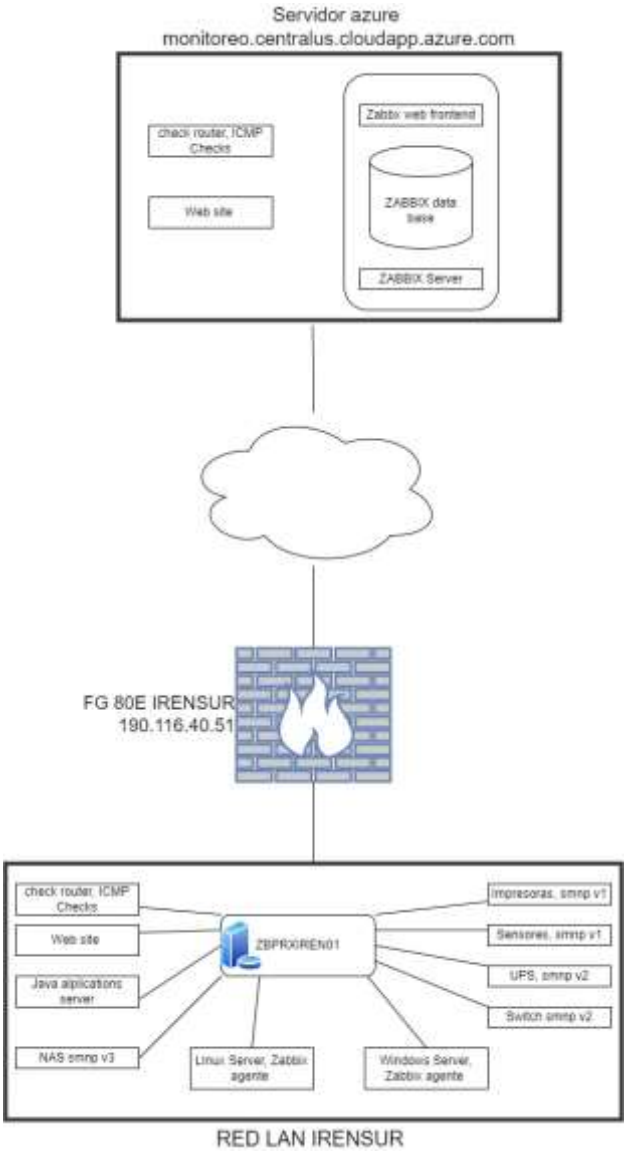
Fuente: El investigador.

ISMITI11 Instalación de servidor Proxy en sede de IRENSUR

La función del servidor proxy es recabar toda la información que se programe desde el servidor central y este trabaje dentro de la red LAN del IRENSUR todo esto sin atenuar o influir en el tráfico de la red, su integración y despliegue se muestra en la siguiente figura. Los requisitos del servidor proxy son

- Raspberry Pi 4 de 2GB
- Raspberry Pi OS 10

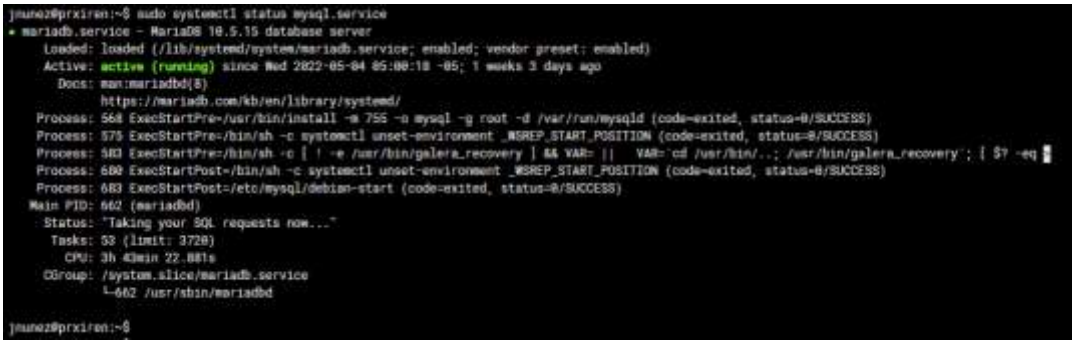
Figura N ° 26 Despliegue de conexión entre el servidor principal de monitoreo y el servidor proxy instalado en el IRENSUR



Fuente: El investigador

Como primer paso se actualizo la lista de paquetes del servidor rasbperry PI para tener las ultimas actualizaciones y parches para una un funcionamiento correcto, se inicia con la instalación del servidor de base de datos MySQL al culminar se tiene que comprobar el status de este servicio, así como se muestra en la figura N° 27.

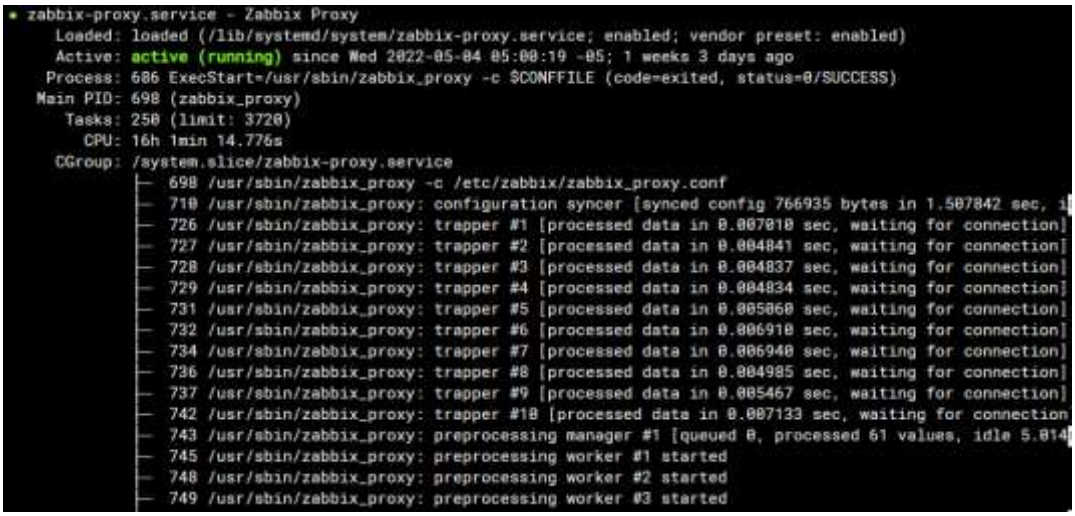
Figura N ° 27 Estatus de servicio de base de datos en servidor proxy.



Fuente: El investigador.

Al culminar la instalación del servidor proxy se tendrá operativo el servicio del servidor proxy

Figura N ° 28 Estatus de servidor proxy en IRENSUR.



Fuente: El investigador.

Se tiene que iniciar los servicios y habilitar del puerto 22 para el control remoto del servidor.

Figura N ° 29 Estatus del servicio ssh en servidor proxy IRENSUR

```
jnunez@prxiren:~$ sudo systemctl status ssh.service
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2022-05-04 05:00:15 -05; 1 weeks 3 days ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 570 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 599 (sshd)
      Tasks: 1 (limit: 3720)
        CPU: 1.052s
     CGroup: /system.slice/ssh.service
             └─599 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
jnunez@prxiren:~$
```

Fuente: El Investigador.

Configurado el servidor Zabbix proxy este tiene que apuntar con dirección al servidor principal hospedado en la nube de Azure teniendo como premisa que el archivo de configuración tiene que indicar que trabajara en modo proxy activo.

Figura N ° 30 Configuración de dirección de servidor central de sistema de monitoreo

```
############ GENERAL PARAMETERS #################

### Option: ProxyMode
#       Proxy operating mode.
#       0 - proxy in the active mode
#       1 - proxy in the passive mode
#
# Mandatory: no
# Default:
# ProxyMode=0

### Option: Server
#       If ProxyMode is set to active mode:
#               IP address or DNS name (address:port) or cluster (address:port;address2:port) of Zabbix server to get c
send data to.
#               If port is not specified, default port is used.
#               Cluster nodes need to be separated by semicolon.
#       If ProxyMode is set to passive mode:
#               List of comma delimited IP addresses, optionally in CIDR notation, or DNS names of Zabbix server.
#               Incoming connections will be accepted only from the addresses listed here.
#               If IPv6 support is enabled then '127.0.0.1', '::127.0.0.1', '::ffff:127.0.0.1' are treated equally
#               and '::/0' will allow any IPv4 or IPv6 address.
#               '0.0.0.0/0' can be used to allow any IPv4 address.
#               Example: Server=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.example.com
#
# Mandatory: yes
# Default:
# Server=

#Server=13.89.58.250
Server=monitoreo.centralus.cloudapp.azure.com
```

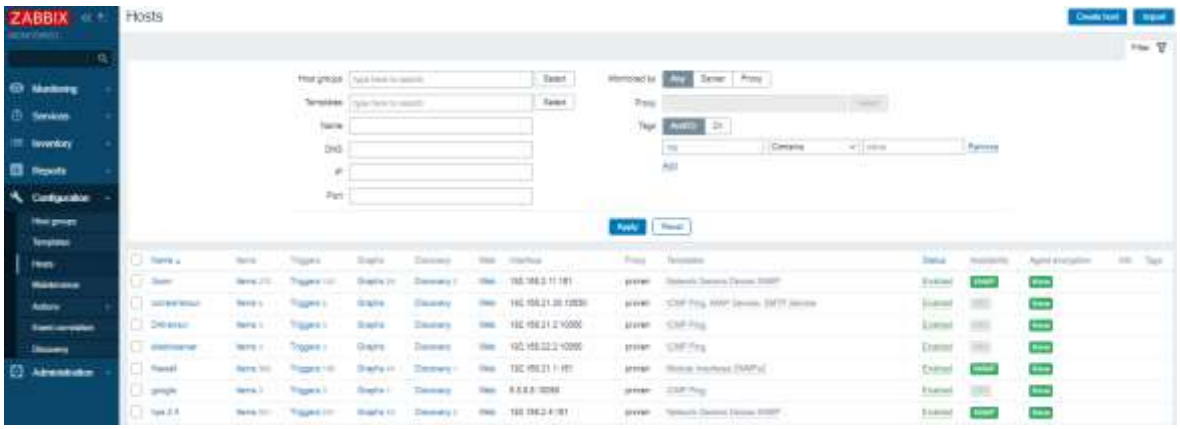
Fuente: El investigador.

ISMITI12 Configuración de host a nivel de snmp

Los pasos para configurar un host a nivel snmp dentro del sistema de monitoreo son los siguientes.

Como primer punto iremos a la ubicación **configuration>> host** y luego haremos clic en el botón **créate host**

Figura N ° 31 Gestión de los hosts monitoreados desde la parte frontend

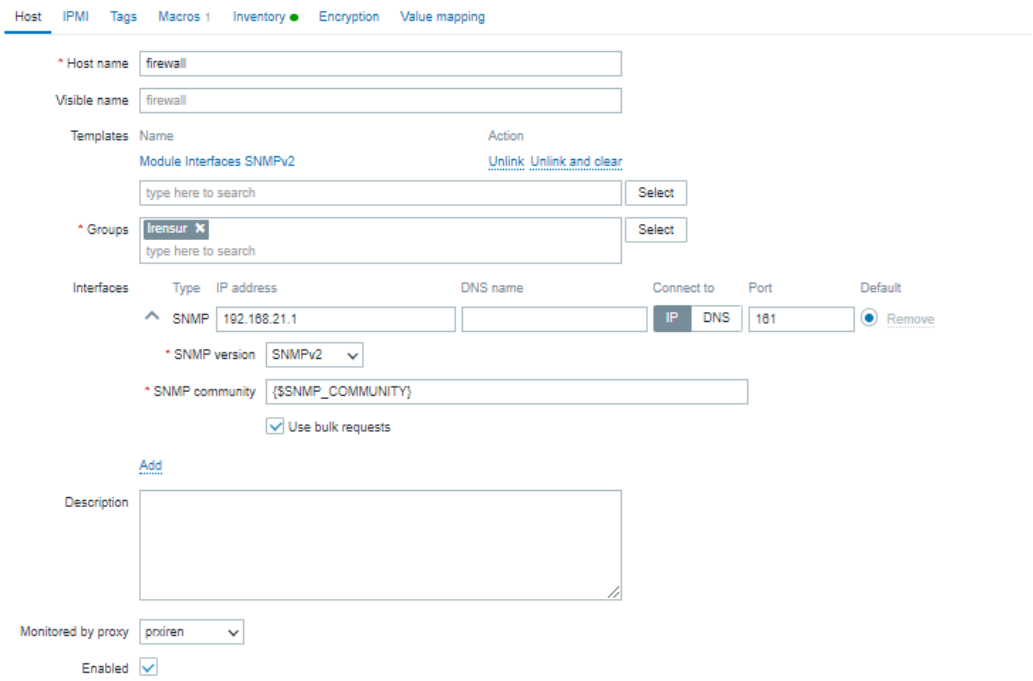


Fuente: Sistema de monitoreo.

A esto se definirá los siguientes datos :

- Hostname: Nombre del equipo
- Template: se elige el perfil que usara el equipo para su monitoreo
- Groups: el grupo por defecto a usar será IRENSUR.
- Interfaces: Se define la ip con que e identifica el equipo y el puerto de monitoreo será el que se usa por defecto para snmp que es el 161
- Snmp versión: La versión por defecto se usará es el snmp v2
- Snmp community: se dará un nombre de comunidad para el uso del snmp
- Monitored to proxy: se habilitará el proxy y se elegirá el prxiren

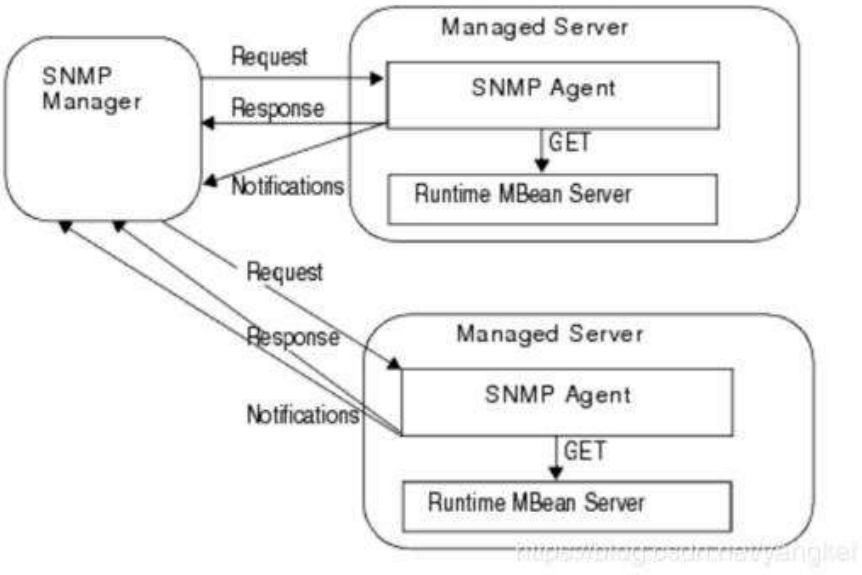
Figura N ° 32 Configuración de smnp



Fuente: Sistema de monitoreo.

La dinámica de monitoreo que se da a nivel de snmp se muestra en el siguiente gráfico.

Figura N ° 33 Monitoreo a nivel de snmp



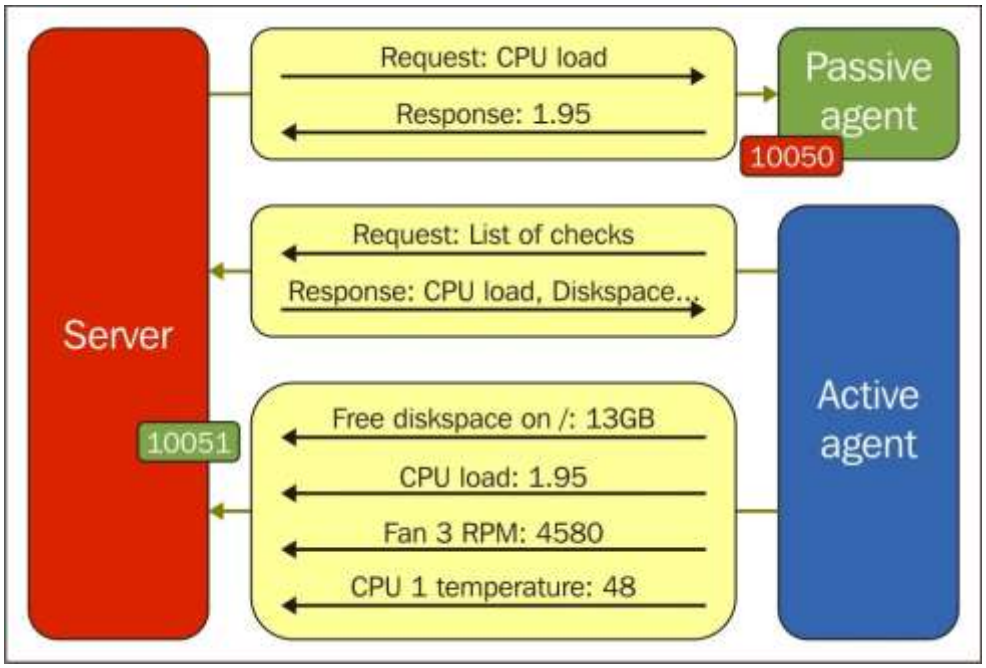
Fuente : www.zabbix.com

ISMITI13 Configuración de agentes de monitoreo

Los pasos para la configuración de los hosts monitoreados por el agente de Zabbix del sistema de monitoreo son los siguientes.

Este tipo de monitoreo tendrá la siguiente dinámica el cual nos muestra el tipo de conexión apuntando a la ip del servidor proxy , el tipo de monitoreo será activo.

Figura N ° 34 Monitoreo a nivel de agente

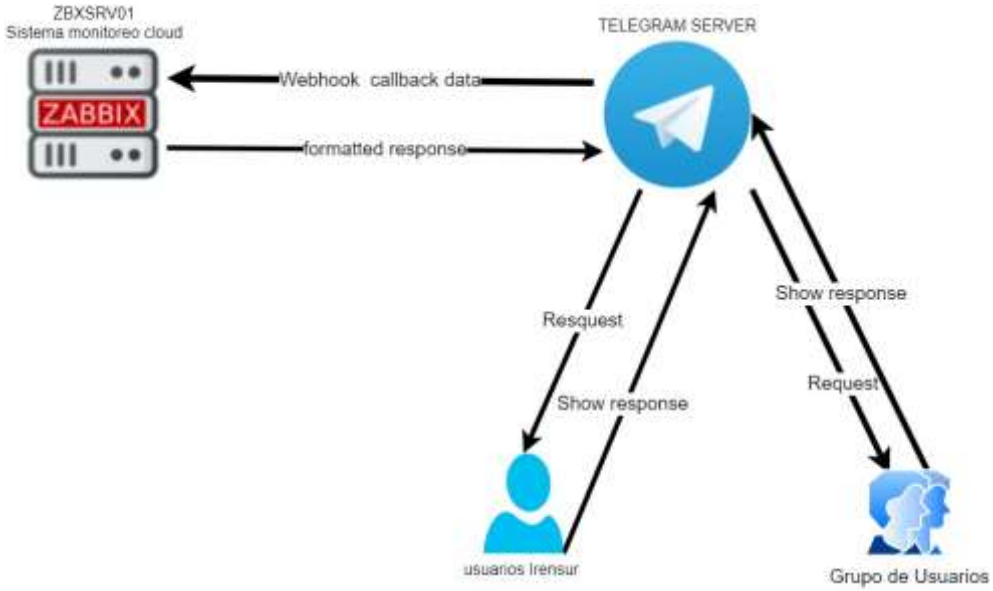


Fuente: Sistema de Monitoreo

ISMITI14 Configuración de alertas para Bot Telegram

La dinámica de alertas mediante el uso del Bot de Telegram se dará según el siguiente grafico:

Figura N ° 35 Interacción servidor de monitoreo y Bot Telegram



Fuente: El Investigador.

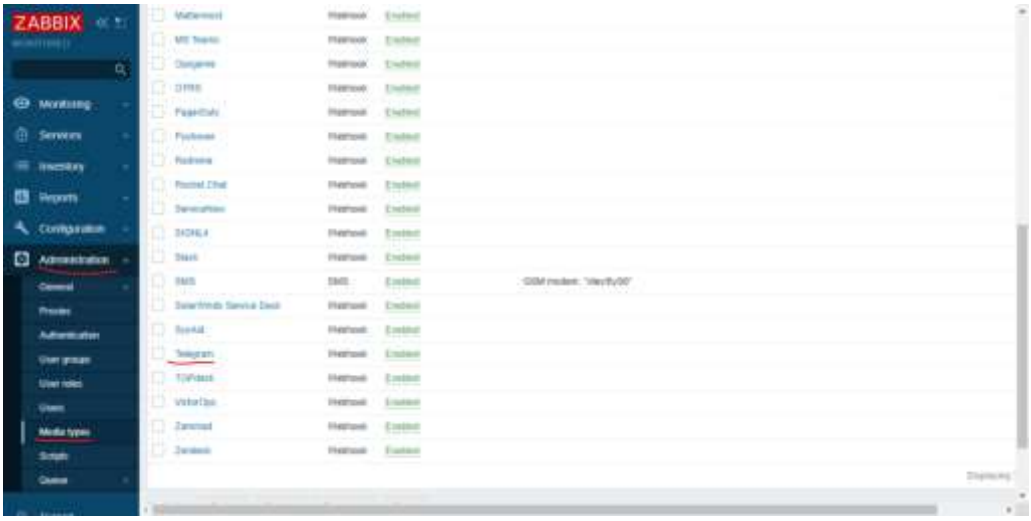
Los pasos para la creación del agente Bot en Telegram se da en el anexo 4

Después de haber seguido todos estos pasos para se tendría como resultado el groupid que viene a ser el identificador único del grupo de chat de Telegram donde se tiene configurador el Bot @irensurbot

A esto se tendrá que hacer varias configuraciones dentro de la administración y notificación del sistema de monitoreo

Para esto se tiene que ir a la siguiente ruta “Administration > Media types"

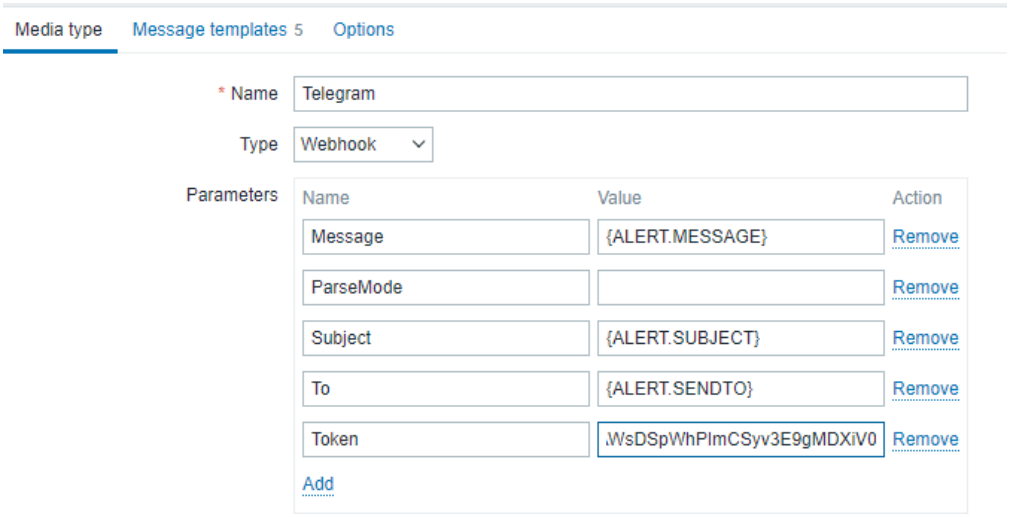
Figura N ° 36 Ubicación de configuración de alerta



Fuente: Sistema de monitoreo

Dentro del tipo de mensaje se tendrá que agregar el token que se generó al crear el Bot.

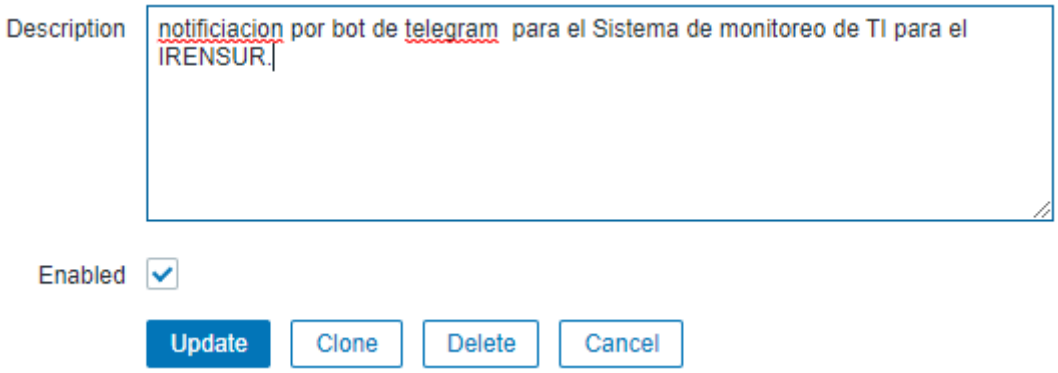
Figura N ° 37 Datos configuración de notificación



Fuente: Sistema de monitoreo.

A esto se tiene habilitar el sistema de notificación dando clic sobre el recuadro enable

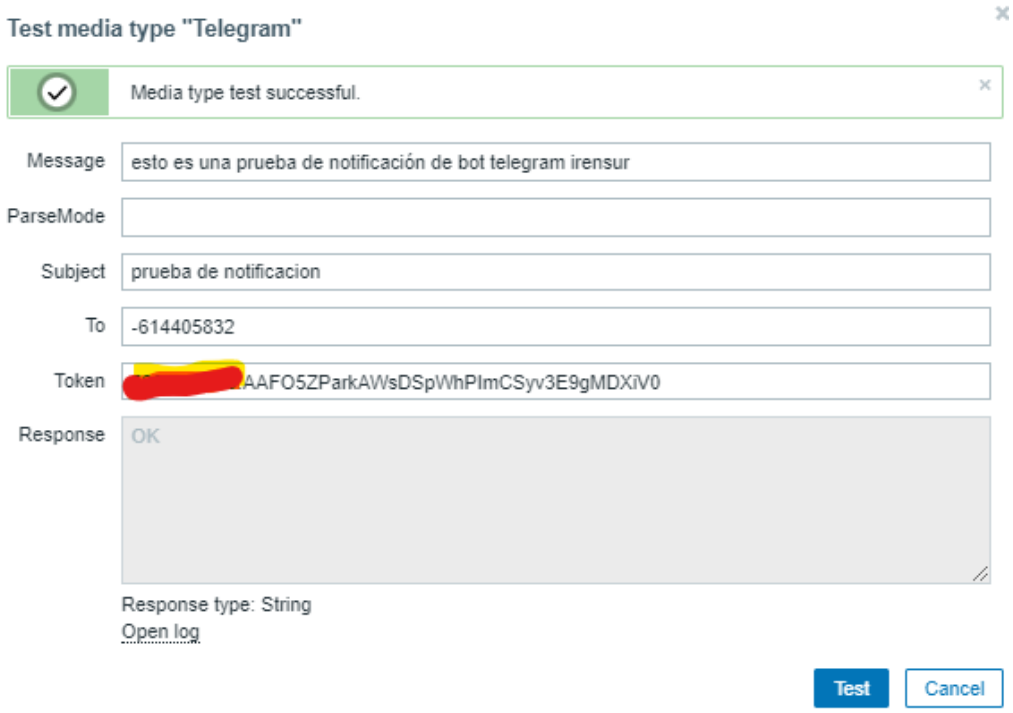
Figura N ° 38 Habilitación de sistema de notificación



Fuente: sistema de monitoreo

Luego se tendrá que hacer una prueba del notificador indicando el token del Bot y el id del grupo de Telegram

Figura N ° 39 Configuración de prueba de notificador de agente Bot



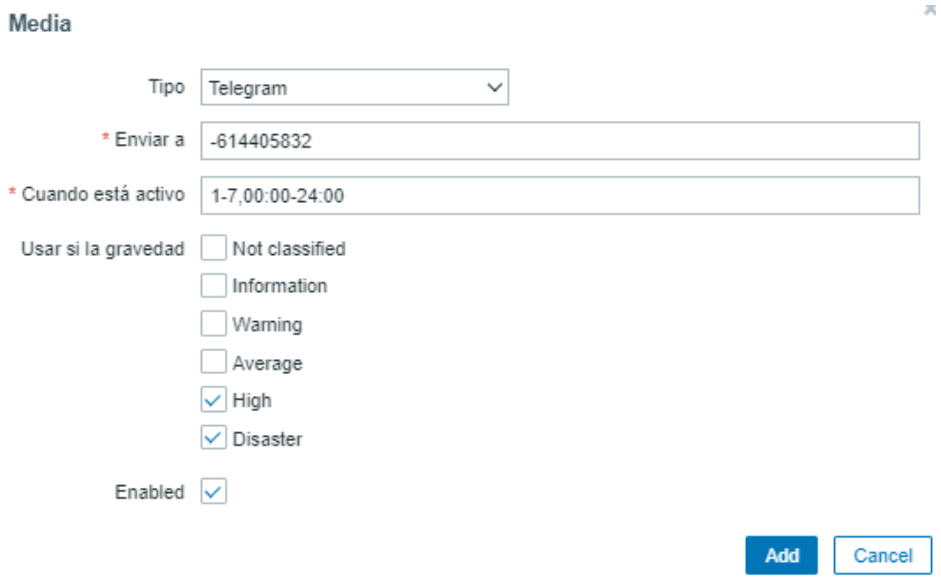
Fuente: Sistema de monitoreo

Figura N ° 40 Prueba de recepción de mensaje de sistema de monitore

Fuente: chat Telegram

Para recibir las alertas de los sistemas y servicios del IRENSUR se tendrá que crear una alerta dentro del sistema de monitoreo, esto se agregará a un usuario del sistema de monitoreo, como condicionante se necesitará el id de grupo de chat de Telegram donde se encuentra el agente Bot.

Figura N ° 41 Configuración de notificación

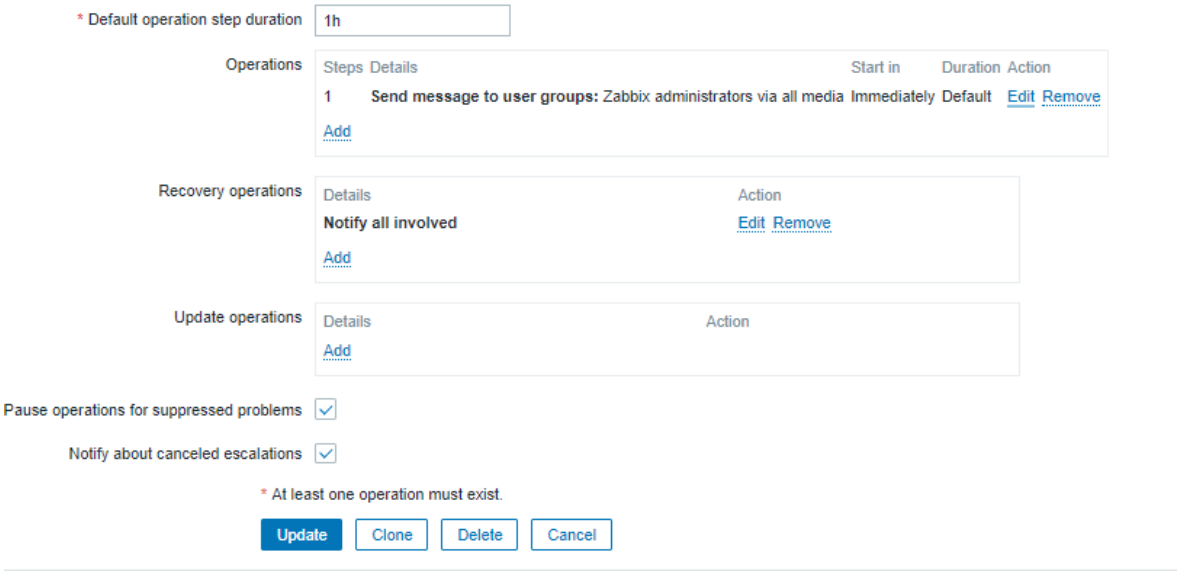


Fuente: Sistema de monitoreo

Según la figura 41 se indica el numero de la sala a notificar, la actividad que tendrá las notificaciones el cual será de 24x7 y el nivel de gravedad que se notificara son las alarmas que sean consideradas como altas y desastre

El trigger de notificación para el sistema de alertas su configuración es la siguiente el cual se muestra en la figura 42.

Figura N ° 42 Configuración de trigger



Fuente: Sistema de monitoreo

Las notificaciones que llegan al grupo de monitoreo mediante el Bot se muestran en la siguiente captura:

Figura N ° 43 Notificación de Bot Telegram

Fuente: Sistema de monitoreo

Teniendo como review del sprint el cumplimiento de todo lo programado el cual se detalla en la siguiente figura.

ISMITI15 Creación de Dashboard e informes

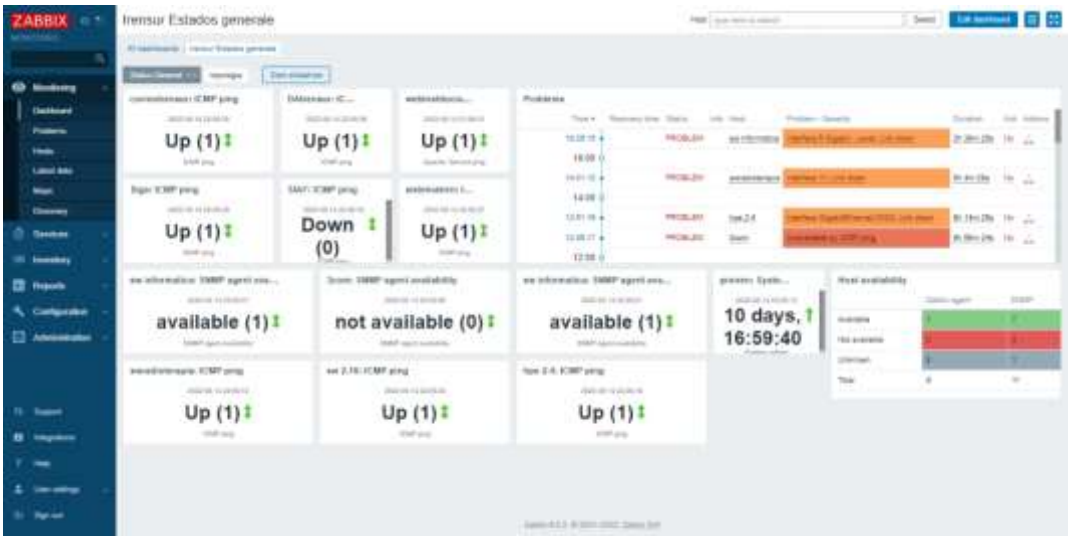
La lista de Dashboard que se tendrá son los siguientes

- Estatus de operatividad de servicios y dispositivos.
- Detalle de tráfico y operatividad de firewall fortinet
- Operatividad de Swicht y Servidores.

Estatus de operatividad de servicios y dispositivos

Este Dashboard nos da una vista general de todo los dispositivos críticos y servicios primordiales esto basado según a la matriz servicios críticos y objetivos operaciones.

Figura N ° 44 Tablero general de estados de equipos y servicios.

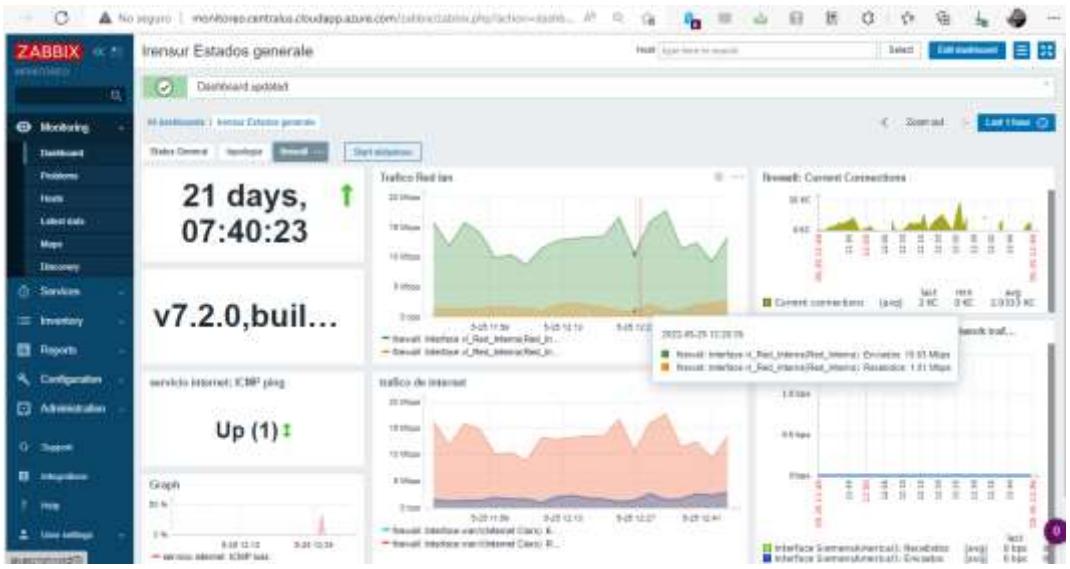


Fuente: Sistema de monitoreo.

Detalle de operatividad de firewall fortinet

En este tablero de mando se tiene una descripción detallada de las conexiones que se tiene dentro del firewall el tráfico por segmento de red y las conexiones de vpn al firewall a esto se verifica el tiempo de uptime del firewall.

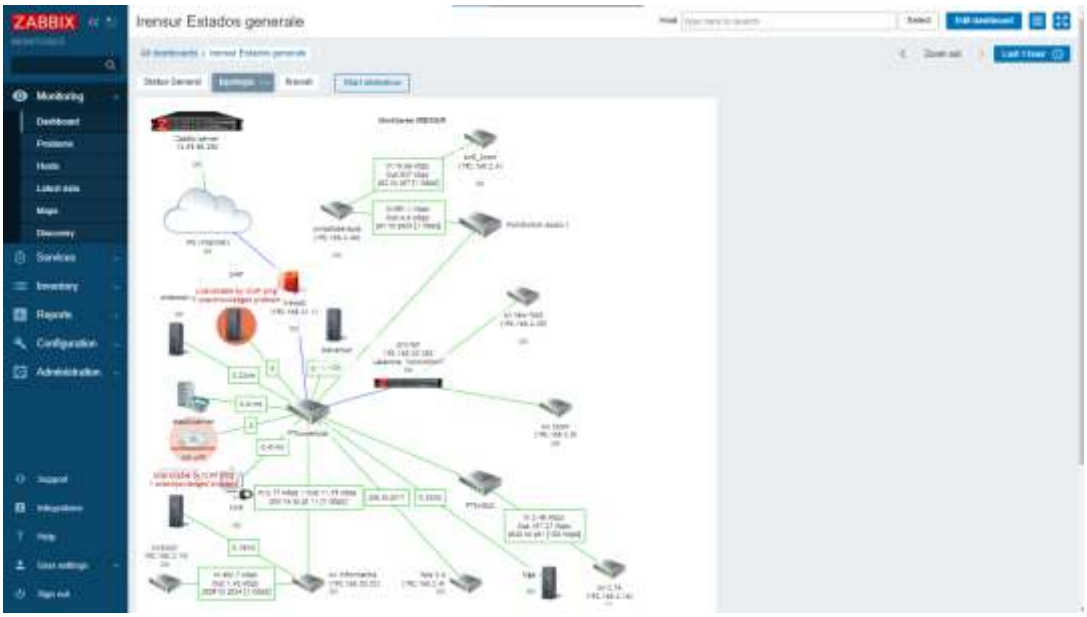
Figura N ° 45 Detalle de monitoreo a firewall fortinet



Fuente: Sistema de monitoreo.

En el tablero de topología se especifica toda la interacción de los equipos de conforman la infraestructura de red del IRENSUR con esto se muestra el ancho de banda que consume cada uno y su estado de Down Time (tiempo de caída de servicio) de cada uno, así como su disponibilidad de operatividad de estos.

Figura N ° 46 Vista de la topología de IRENSUR con data en línea



Fuente: Sistema de Monitoreo.

Figura N ° 47 Seguimiento de cronograma ejecutado en sprint 3

Fuente: El Investigador.

4.4. Recolección de datos

Se detallarán los procedimientos que se utilizarán para la recolección de la información necesaria para alcanzar los objetivos de la presente investigación. Asimismo, se describirán los instrumentos que se utilizarán para el proceso de recolección de datos.

4.4.1. Procedimientos para la recolección de la información:

4.4.1.1. Identificación de fuentes de información: Para llevar a cabo la recolección de la información necesaria, se identificaron las fuentes de información que permitieron recopilar los datos requeridos para la investigación. En este caso, se consideró la información obtenida de los registros de notificaciones del sistema de monitoreo de infraestructura de TI del IRENSUR, y se realizó un análisis AS-IS/TO-BE del personal de TI.

4.4.1.2. Selección de la muestra: la selección se realizó de la siguiente manera:

- Para obtener los registros de notificaciones del sistema de monitoreo de infraestructura de TI del IRENSUR, se selecciono una muestra aleatoria de los registros generados en un período de tiempo específico, que este caso sera el mes de setiembre La muestra utiliza se hizo por un método de muestreo aleatorio simple, en el que se registro 10,000 registros en un mes, y se tomo una muestra aleatoria de 500 registros para ver la data seleccionada ver anexo 6. La extructura del registro de la tabla tiene el siguiente registro

Tabla N° 26 Muestra de registro de notificaciones de sistema de monitoreo de infraestructura de TI

ID	Severity	Time	Recovery time	Status	Host	Problem	Duration	ACK	Actions
1	Warning	30/09/22 07:12	30/09/22 07:28	RESOLVED	3com	High ICMP ping response time (Value: 0)	16m		
2	Information	16/09/22 18:45	16/09/22 19:10	RESOLVED	sw informatica	Interface 41 Gigabit - Level: Ethernet has changed to lower speed than it was before (Current reported speed: 0 bps)	25m		
3	Average	20/09/22 01:46	22/09/22 20:11	RESOLVED	Zabbix server	Load average is too high (per CPU load over 1.5 for 5m) (Load	2m		

						averages(1m 5m 15m): (0.17 0.21 0.41), # of CPUs: 1)		
4	High	21/09/22 19:39	22/09/22 20:11	RESOLVED	3com2928sfp	Unavailable by ICMP ping	1d 32m	Actions (2)
5	High	17/09/22 06:30	17/09/22 11:27	RESOLVED	3com	Unavailable by ICMP ping	4h 57m	Actions (2)

Fuente: Sistema de Monitoreo de infraestructura de TI IRENSUR

- Para realizar el análisis AS-IS/TO-BE del personal de TI, se utilizo un cuestionario (ver anexo 7), de manera que recogió información sobre las actividades y procesos actuales en el departamento de TI, así como sobre las posibles mejoras que se podrían implementar con el nuevo sistema de monitoreo de TI.

Tabla N° 27 Respuestas al cuestionario AS-IS / TO-BE al implementar el nuevo sistema de monitoreo de infraestructura TI

Pregunta	Respuesta AS-IS	Respuesta TO-BE
¿Cuáles son las principales responsabilidades de su rol en el departamento de TI?	Alta	Alta
¿Cuáles son los principales procesos y actividades que se realizan en el departamento de TI actualmente?	Alta	Alta
¿Cómo se realiza actualmente el monitoreo de la infraestructura de TI? ¿Qué herramientas y sistemas se utilizan para este fin?	Media	Baja
¿Cuáles son los principales desafíos o problemas que se han enfrentado en el monitoreo de la infraestructura de TI?	Alta	Baja
¿Qué información se considera crítica para el	Alta	Alta

monitoreo de la infraestructura de TI?		
¿Qué mejoras se podrían implementar con un nuevo sistema de monitoreo de TI?		
¿Cómo se espera que este nuevo sistema mejore el monitoreo de la infraestructura de TI?	Alta	Alta
¿Qué características o funcionalidades son importantes para el nuevo sistema de monitoreo de TI?	Alta	Alta
¿Cómo se espera que el nuevo sistema de monitoreo de TI impacte en la eficiencia y eficacia del departamento de TI?	Alta	Alta
¿Qué recursos serían necesarios para implementar el nuevo sistema de monitoreo de TI?	Media	Baja

Fuente: el investigador

- Validación de los datos: Una vez recopilados los datos, se verificará la calidad de la información para garantizar la confiabilidad de los resultados. Se comprobará la integridad y coherencia de los datos obtenidos, y se eliminarán los datos que presenten inconsistencias.

4.5. Técnica de análisis de datos

En la siguiente tabla se detalla el resumen de procedimientos realizados:

Tabla N° 28 Detalle de resumen de procedimientos para el sistema de monitoreo de infraestructura TI

SPRINT	DURACION	OBJETIVOS	BACKLOGS	PROCEDIMIENTOS	HITOS ALCANZANDOS
1	1 semana	Describir, comparar y elegir herramientas de monitoreo	ISMITI01, ISMITI02, ISMITI03	1. Identificar las herramientas de monitoreo existentes. 2. Describir cada una de ellas. 3. Comparar las herramientas de monitoreo. 4. Elegir la herramienta de monitoreo más adecuada para la institución.	Elección de la herramienta de monitoreo más adecuada.
2	1.5 semanas	Analizar la topología de red, identificar servicios y dispositivos críticos, corresponderlos con objetivos institucionales y diseñar la	ISMITI04, ISMITI05, ISMITI06, ISMITI07, ISMITI08	1. Analizar la topología de red de la institución. 2. Identificar los servicios y dispositivos críticos. 3. Correspondender los servicios y dispositivos críticos con los objetivos institucionales. 4. Diseñar la implementación del sistema de monitoreo.	Diseño de la implementación del sistema de monitoreo y correspondencia de servicios críticos con objetivos institucionales.

		implementación del sistema de monitoreo			
3	3 semanas	Crear un servidor en la nube, instalar y configurar el servidor Zabbix, instalar y configurar el servidor Proxy en la sede de IRENSUR, configurar los hosts y agentes de monitoreo, configurar alertas para Bot Telegram y crear dashboard e informes	ISMITI09, ISMITI10, ISMITI11, ISMITI12, ISMITI13, ISMITI14, ISMITI15	1. Crear un servidor en la nube. 2. Instalar y configurar el servidor Zabbix en la nube. 3. Instalar y configurar el servidor Proxy en la sede de IRENSUR. 4. Configurar los hosts y agentes de monitoreo. 5. Configurar las alertas para Bot Telegram. 6. Crear el dashboard e informes del sistema de monitoreo.	Implementación y configuración del sistema de monitoreo, y creación de dashboard e informes.

Fuente: El investigador.

Se están utilizando técnicas de recolección de datos de tipo cuantitativo y el uso de la observación directa del sistema monitoreo de infraestructura de TI, la medición de indicadores de desempeño y el análisis de registros y datos históricos para determinar la eficiencia y efectividad del sistema de monitoreo. También se está aplicando un cuestionario con preguntas cerradas para obtener información precisa y específica sobre el rendimiento del sistema y la satisfacción del personal de TI. Esto nos proporciona una visión más completa y precisa de la situación de la infraestructura de TI y el sistema de monitoreo implementado en IRENSUR.

V. SOLUCION TECNOLOGICA

5.1. Presentación de Resultados

Según los 3 Sprint que se proyectaron para el desarrollo del presente proyecto se obtuvo los siguientes resultados

En el sprint 1 se buscó describir, comparar y elegir herramientas de monitoreo con el objetivo de seleccionar la mejor opción para IRENSUR. Para ello, se creó el backlog ISMITI01, con alta prioridad y una duración estimada de 10 horas, que incluyó la descripción de herramientas de monitoreo open source y la elaboración de un cuadro resumen de sus ventajas y desventajas. El criterio de aceptación fue tener al menos 3 sistemas de monitoreo elegidos para pasar al siguiente paso.

En el backlog ISMITI02, con prioridad media y una duración estimada de 6 horas, se compararon las herramientas seleccionadas según el cuadrante Gartner y se escogió el sistema de monitoreo con mejor posición en este cuadrante.

Finalmente, en el backlog ISMITI03, con alta prioridad y una duración estimada de 4 horas, se realizó un pre-planeamiento para la implantación del sistema de monitoreo elegido en colaboración con la jefatura de TI de IRENSUR. Se verificó la herramienta seleccionada, se elaboró una lista de riesgos de implantación y se establecieron los requisitos del sistema de monitoreo.

La selección de la herramienta de monitoreo se realizó mediante una comparativa entre Nagios XI y Zabbix, destacando las ventajas de este último en cuanto a funcionalidades de red y manejo distribuido del sistema. Con los requisitos preliminares establecidos, se inició el desarrollo y despliegue de Zabbix para el monitoreo de la infraestructura de IRENSUR.

Durante la fase del Sprint 2, se llevó a cabo un análisis detallado de la infraestructura de TI del IREN SUR, con el objetivo de identificar y analizar la topología existente, así como los servidores y servicios críticos disponibles. El equipo responsable realizó varias tareas para lograr este objetivo.

En primer lugar, se realizó un estudio de la topología de red actual del IRENSUR. Se llevó a cabo un inventariado de todos los equipos de red y su distribución dentro de la red LAN, lo que permitió elaborar un diagrama claro de la estructura de red del IREN SUR.

En segundo lugar, se identificaron todos los servicios críticos disponibles en la red LAN del IREN SUR. Se elaboró una matriz de servicios y una calificación de su criticidad, lo que permitió obtener un resumen de los servicios críticos identificados.

En tercer lugar, se identificaron los dispositivos críticos de la infraestructura de TI que se encontraban en la red LAN del IREN SUR. Se elaboró una matriz de dispositivos y se calificaron según su criticidad, lo que permitió obtener un resumen de los dispositivos críticos identificados.

En cuarto lugar, se compararon los servicios y dispositivos críticos identificados con los objetivos institucionales del IREN SUR. Se elaboró una matriz de objetivos, servicios y equipos críticos, lo que permitió validar los servicios y dispositivos críticos identificados y establecer una lista de servicios y equipos a monitorear.

Finalmente, se diseñó la implementación del sistema de monitoreo, que fue el hito y resultado clave de este Sprint. Se elaboraron requisitos de implementación de servidor y servidor proxy, una matriz de riesgos, una lista de requerimientos, un diseño topológico de servidores de monitoreo, un diseño de despliegue, un diseño de interacción del sistema de monitoreo y

un diseño de interacción de notificación de alertas. Se elaboró un To be - asis y un Cheklist de verificación de instalación para garantizar la correcta implementación del sistema de monitoreo. En general, este Sprint logró diseñar la implementación del sistema de monitoreo y su correspondencia de servicios críticos con los objetivos institucionales del IREN SUR.

Para el Sprint 3 del proyecto, que tenía como objetivo instalar y desplegar un sistema de monitoreo en el IRENSUR, se llevaron a cabo diversas actividades por parte del product owner y equipo de desarrollo.

En primer lugar, se realizó un estudio de la topología actual de la infraestructura del IRENSUR para crear un servidor en la nube con SO Linux en Azure. Este servidor se configuró para permitir la administración remota a través del puerto SSH. El criterio de aceptación para esta actividad fue la administración remota del servidor, y el flujo de proceso consistió en tener los accesos al gestor de Azure, elegir un tipo de servidor con pocos recursos, poner en marcha el servidor y publicar el puerto SSH para su administración.

Luego, se instaló el servidor Zabbix en la nube. Se crearon los repositorios y permisos necesarios para la ejecución del sistema de monitoreo, así como los servicios LAMP necesarios. El criterio de aceptación para esta actividad fue la puesta en ejecución del sistema de monitoreo, y el flujo de proceso incluyó la actualización de repositorios, la instalación del servidor Apache, la instalación del servidor de base de datos MySQL, la publicación del puerto SSH y la instalación del sistema de monitoreo Zabbix.

Se procedió a la instalación del servidor proxy en la sede del IRENSUR, para lo cual se actualizaron los repositorios del Raspberry PI y se instalaron los servicios LAMP necesarios para su ejecución. El criterio de aceptación para esta actividad fue la

conexión con el sistema de monitoreo, y el flujo de proceso consistió en la actualización de repositorios, la instalación del servidor de base de datos MySQL, la instalación del servidor proxy Zabbix, la configuración de los puertos de conexión al servidor Zabbix y la publicación del puerto SSH para la administración del servidor.

Se procedió a la configuración de los equipos y servicios críticos para su monitoreo a nivel snmp, lo que incluyó la definición de la key community para uso de monitoreo, la lista de equipos soportados por snmp y la adición de equipos al sistema de monitoreo por snmp. El criterio de aceptación para esta actividad fue que los equipos fueran monitoreados por snmp.

Por último, se configuraron los agentes de monitoreo para aquellos equipos y servicios que no soportaban o no tenían configurado el protocolo snmp. Se realizó un listado de equipos y servicios y se agregaron al sistema de monitoreo.

Además, se definió a qué usuarios se les haría llegar las notificaciones y qué nivel de alertas se notificaría, y se creó un Bot en la plataforma de Telegram para configurar la integración con el sistema de monitoreo. Finalmente, se crearon tableros de notificación y monitoreo de la infraestructura de TI del IRENSUR.

En resumen, durante el tercer Sprint del proyecto se logró instalar y desplegar el sistema de monitoreo en el IRENSUR, incluyendo la creación de un servidor en la nube, la instalación del servidor Zabbix y del servidor proxy, la configuración de los equipos y servicios críticos para su monitoreo, la configuración de los agentes de monitoreo y la configuración de alertas para el Bot Telegram.

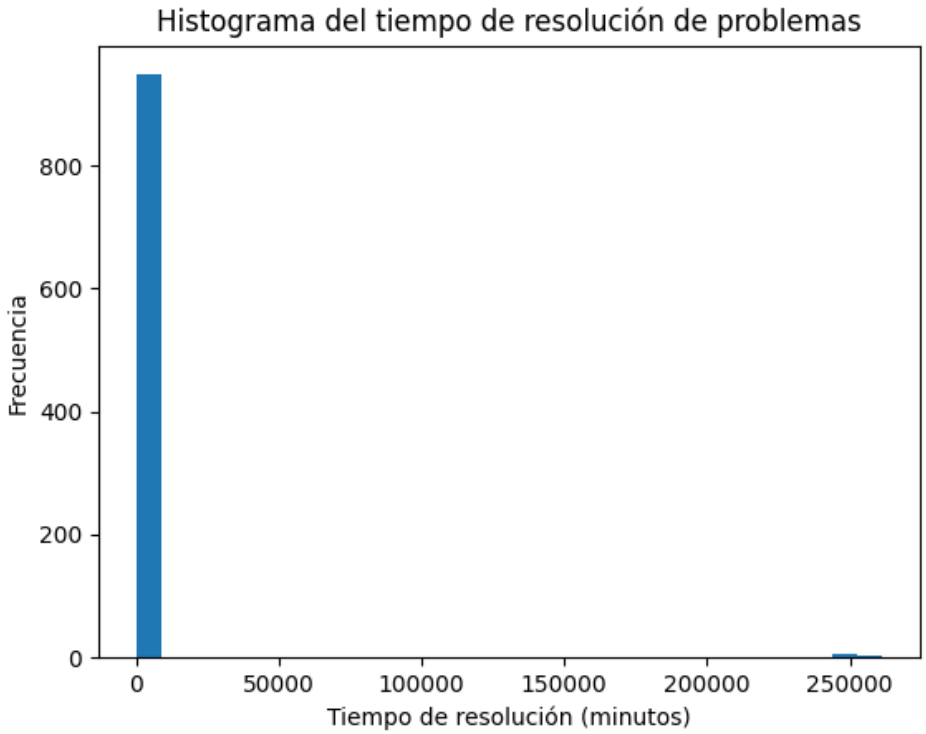
Es importante mencionar que durante la implementación del sistema de monitoreo se contó con la supervisión de un experto que certificó el presente estudio(VER ANEXO 2), análisis y la implementación del sistema de monitoreo se llevó a cabo de manera correcta.

Para validar el sistema de monitoreo de infraestructura de TI, se trabajó con una serie de KPIs que nos permiten evaluar su efectividad. Los resultados obtenidos se basaron en la tabla 26, la cual muestra el registro de notificaciones del sistema de monitoreo.

Los KPI por mostrar son:

- Tiempo de resolución de problemas: Este KPI mide la cantidad de tiempo que toma resolver un problema detectado por el sistema de monitoreo. Se calcula restando el tiempo de recuperación del problema del tiempo en que se detectó el problema.

Figura N ° 48 KPI tiempo de Resolución



Fuente: Sistema de monitoreo de infraestructra de TI

- Porcentaje de problemas resueltos: Este KPI mide el porcentaje de problemas que se resolvieron

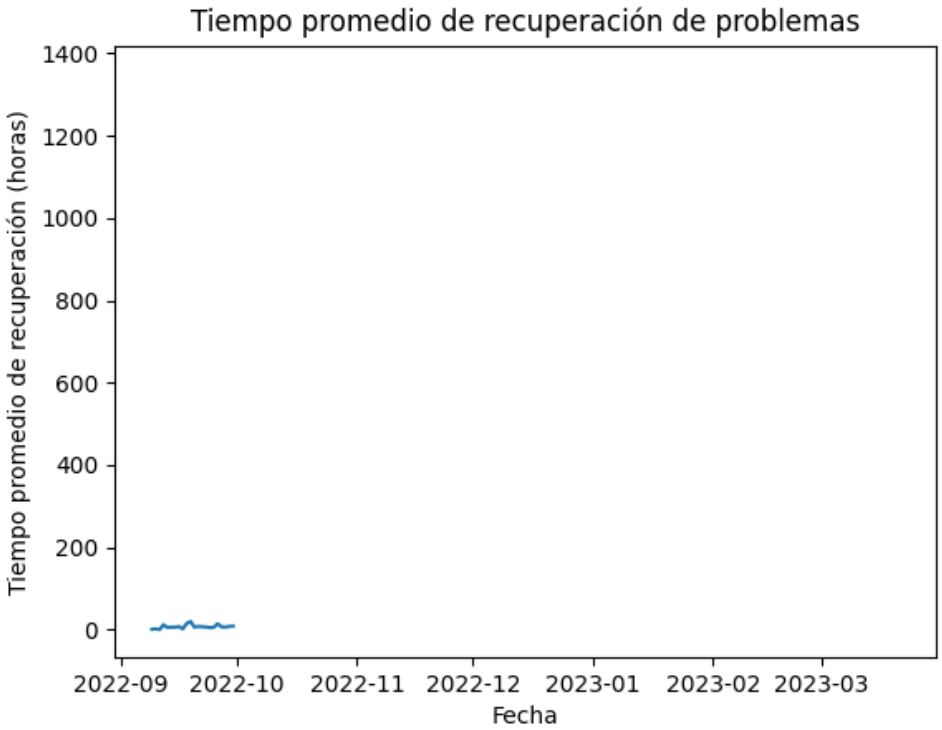
satisfactoriamente en comparación con la cantidad total de problemas detectados por el sistema de monitoreo.

Figura N ° 49 KPI Porcentaje de problemas resueltos.

Fuente: Sistema de monitoreo de infraestructra de TI

- Tiempo promedio de recuperación: Este KPI mide el tiempo promedio que toma recuperar un sistema o servicio después de que se detectó un problema. Se calcula dividiendo el tiempo total de recuperación de todos los problemas por la cantidad total de problemas.

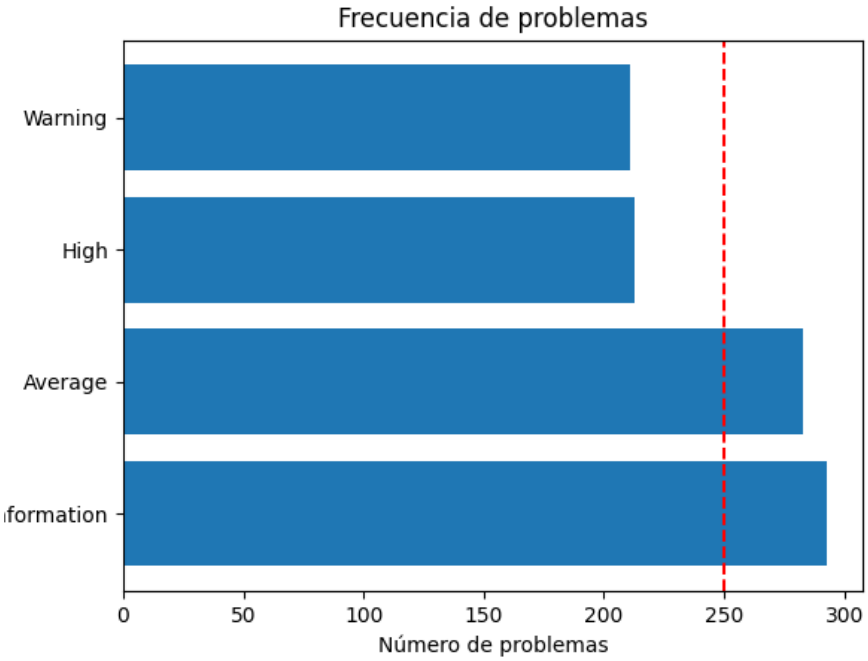
Figura N ° 50 KPI Tiempo promedio de Recuperación.



Fuente: Sistema de monitoreo de infraestructra de TI

- Frecuencia de problemas: Este KPI mide la cantidad de problemas que ocurren en un período de tiempo específico. Se calcula dividiendo la cantidad de problemas por el tiempo total en el que se detectaron los problemas.

Figura N ° 51 KPI Frecuencia de problemas.



Fuente: Sistema de monitoreo de infraestructra de TI

Además, se llevó a cabo un análisis AS-IS/TO-BE y se recopilaron las respuestas al cuestionario por parte del personal de TI del IRENSUR. La tabla 27 muestra los resultados de este análisis y nos da una idea clara de cómo se ha mejorado el sistema de monitoreo de infraestructura al implementar las mejoras sugeridas.

Para el análisis AS-IS se tiene el siguiente resultado(ver tabla 29).

Tabla N° 29 Resultado de AS-IS

Desafío/Problema	**Frecuencia**
Falta de visibilidad de la infraestructura	Alta
Falta de tiempo para la resolución de problemas	Media
Herramientas de monitoreo obsoletas	Alta

Fuente: El investigador.

Y para el análisis TO-BE se tiene el siguiente resultado (ver tabla 30).

Tabla N° 30 Resultado de AS-IS

Mejora	**Impacto**
Mayor visibilidad de la infraestructura	Alta
Reducción en el tiempo de resolución de problemas	Alta
Mejora en la disponibilidad de la infraestructura de TI	Alta

Fuente: El investigador.

Como resultado general se tiene:

1. Se logra el diseño e implementación de un sistema de monitoreo para la infraestructura de TI de IRENSUR, gracias al trabajo del equipo de desarrollo. Durante los sprints, se seleccionó la herramienta de monitoreo Zabbix y se realizó un análisis detallado de la topología existente, así como de los servidores y servicios críticos disponibles. Se elaboraron requisitos de implementación, una matriz de riesgos, una lista de requerimientos y un diseño topológico y de despliegue para garantizar la correcta instalación del sistema. Finalmente, se instalaron y configuraron el servidor en la nube y el servidor Zabbix, cumpliendo con los criterios de aceptación establecidos. Con este resultado, se logra garantizar la disponibilidad y continuidad de los servicios críticos del IRENSUR.

2. El trabajo de validación del sistema de monitoreo de infraestructura de TI fue necesario para evaluar su efectividad y asegurar que cumpla con los estándares de calidad esperados. Se trabajó con una serie de KPIs, los cuales permitieron medir aspectos clave como el tiempo de resolución de problemas, porcentaje de problemas resueltos, tiempo promedio de recuperación y frecuencia de problemas. Además, se llevó a cabo un análisis AS-IS/TO-BE y se

recopilaron las respuestas del personal de TI del IRENSUR, lo que permitió identificar los desafíos y problemas del sistema y proponer mejoras para superarlos. En general, los resultados obtenidos permiten afirmar que el sistema de monitoreo de infraestructura de TI es efectivo y ha mejorado significativamente gracias a las mejoras implementadas.

VI. DISCUSIONES DE RESULTADOS

6.1. Comparación de los resultados con antecedentes

En comparación con la tesis de Vallejo(2020), se tiene que ambos trabajos enfatizan la importancia de seleccionar la herramienta de monitoreo adecuada y realizar un análisis detallado de la infraestructura existente antes de implementar el sistema de monitoreo. Sin embargo, la tesis de Vallejo se enfoca en el análisis costo-beneficio de soluciones de código abierto versus pagadas, mientras que el estudio de la implementacion del sistema de monitoreo para el IRENSUR se enfoca en la efectividad del sistema de monitoreo y su impacto en los servicios críticos.

En comparación con la tesis de Gaviria(2019) se denota que Ambos proyectos tienen en común que se seleccionó la herramienta de monitoreo Zabbix y se trabajó en la configuración y validación del sistema de monitoreo. Sin embargo, hay algunas diferencias en la implementación.
En el proyecto de EMTELCO S.A.S., se presentaron dificultades al configurar el monitoreo de los servidores con sistema operativo Windows utilizando el protocolo SNMP, por lo que solo fue posible configurarlos utilizando el agente. Además, debido a la falta de conocimiento y un estudio detallado de la herramienta, solo fue posible realizar el monitoreo de conectividad mediante ping cada 3 minutos, pero el proyecto de IRENSUR se realizó un análisis más detallado y exhaustivo para garantizar la correcta instalación y configuración del sistema,

Por otro lado se tiene que al comparar resultados con la tesis de Quispe(2018) No es es posible comparar directamente los resultados con la implementación del sistema de monitoreo del

IRENSUR, ya que se trata de dos proyectos diferentes con objetivos y contextos distintos. Sin embargo, podemos observar que ambos proyectos involucran la implementación de sistemas de monitoreo, lo que indica que comparten ciertos objetivos y metodologías. Además, en ambos proyectos se realizó un análisis detallado de la topología y de los servicios críticos involucrados, y se establecieron criterios de aceptación para garantizar la calidad del sistema implementado. También se trabajó en la validación y mejora continua del sistema de monitoreo, lo que sugiere una preocupación por la efectividad y la optimización de los servicios de TI.

CONCLUSIONES

Se puede concluir que.

La implementación del sistema de monitoreo para la infraestructura de TI y equipos de salud en la red LAN del Instituto Regional de enfermedades Neoplásicas del Sur-IRENSUR fue posible gracias a la realización de los objetivos específicos planteados. En el sprint 1 se seleccionó la herramienta de monitoreo Zabbix, la cual presentó ventajas en cuanto a funcionalidades de red y manejo distribuido del sistema. En el sprint 2, se realizó un análisis detallado de la infraestructura de TI del IRENSUR para identificar y analizar la topología existente, los servidores y servicios críticos disponibles, y así, establecer una lista de servicios y equipos a monitorear. Además, se diseñó la implementación del sistema de monitoreo, con una lista de requerimientos, diseño topológico, diseño de despliegue, interacción del sistema de monitoreo y un diseño de interacción de notificación de alertas. Con la implementación del sistema de monitoreo, se logra gestionar y administrar de manera eficiente la infraestructura de TI y equipos de salud del IRENSUR.

RECOMENDACIONES

Se recomienda lo siguiente:

1. Continuar con la implementación del sistema de monitoreo: Con este sistema de monitoreo seleccionado y diseñado, es importante continuar con su implementación y despliegue en el IRENSUR. Para ello, es necesario seguir las recomendaciones de instalación y configuración establecidas en el Sprint 3.
2. Realizar una evaluación continua del sistema de monitoreo, es importante realizar una evaluación continua del mismo para verificar su correcto funcionamiento y detectar posibles errores o fallas. Establecer otras métricas y KPIs que permitan medir la eficacia del sistema y asegurar que cumpla con los objetivos institucionales del IRENSUR.
3. Capacitación constante en el uso del sistema de monitoreo: Es importante que el personal del IRENSUR encargado del mantenimiento de la infraestructura de TI esté capacitado en el uso del sistema de monitoreo. Esto permitirá que puedan interpretar y analizar los datos generados por el sistema, y tomar decisiones informadas para el mantenimiento y mejora de la infraestructura.
4. Documentación y mantenimiento del sistema de monitoreo: Es fundamental que se documenten las nuevas configuraciones y procesos relacionados con el sistema de monitoreo. Además, es necesario realizar un mantenimiento continuo del sistema para garantizar su correcto funcionamiento a largo plazo.
5. Integración con otras herramientas de TI: El sistema de monitoreo puede integrarse con otras herramientas de TI para mejorar su funcionalidad y facilitar el mantenimiento de la infraestructura. Se pueden considerar herramientas de automatización, gestión de configuraciones, entre otras.

REFERENCIAS BIBLIOGRÁFICAS

Alexander C., *Network Management Fundamentals*, Cisco Press, 2007.

Al-Faris, A., Alnuem, M., & Al-Hamad, A. (2018). Proactive monitoring system to improve the performance of cloud-based web applications. Journal of Cloud Computing, 7(1), 1-15.

Barreto, R. V., Granville, L. Z., Rochol, J., & Sperotto, A. (2015). Monitoring cloud services using active probing. IEEE Communications Magazine, 53(6), 36-42.

Barreto, R. V., Granville, L. Z., Rochol, J., & Sperotto, A. (2015). Monitoring cloud services using active probing. IEEE Communications Magazine, 53(6), 36-42.

Beltrán, M., & Al, E. (2021). *Ciberseguridad industrial e infraestructuras críticas*, RA-MA(Ed) Madrid

Burnaeva, O - Infrastructure Monitoring Blog. (2021, January 13), from Virtual Metric - Infrastructure Monitoring Blog website: https://www.virtualmetric.com/blog/infrastructure-monitoring-challenges

Carlos, L. (2020). *Diseño de un modelo de seguridad informática a una empresa en su sistema de monitoreo del área de tecnología.* [Tesis de grado, Universidad Cooperativa Colombia]. https://repository.ucc.edu.co/bitstream/20.500.12494/18082/1/2020_Dise%C3%B1o_modelo_seguridad.pdf

Cedeño, I., y Luyely, M. (2019). *Comparativa entre herramientas de monitoreo de red de computadoras aplicadas a la Empresa Puerto*

Atún. [Tesis de grado, Escuela Superior Politécnica Agropecuaria de Manabí]. http://repositorio.espam.edu.ec/handle/42000/1083

Cestari F. - *ITIL v3 Fundamentos-Rede Nacional de Ensino e Pesquisa – RNP (2011). (2013)*., https://www.studocu.com/cl/document/universidad-tecnologica-de-chile/gestion-de-servicios-y-gobernabilidad-de-ti/escola-superior-de-redes-felicio-cestari-filho-itil-v3-fundamentos-rede-nacional-de-ensino-e-pesquisa-rnp-2011/14558056

Cisco. (2018). *Conexión de redes.* http://www.static-course-assets.s3.amazonaws.com/ConnectNet6/es/index.html#5.2.1.1

De, J., Schwaber, K., & Sutherland, J. (2016). *La Guía de Scrum TM La Guía Definitiva de Scrum: Las Reglas del Juego.* https://scrumguides.org/docs/scrumguide/v2016/2016-Scrum-Guide-Spanish.pdf#zoom=100

Drouet, S. (2018). *Control de servicios de red y servidores basado en herramientas de administración de red y políticas de gestión de calidad*. [Tesis de grado, Universidad Pontificie Universidad Católica del Ecuador]. https://repositorio.pucese.edu.ec/handle/123456789/1463

Dallos, L. P., et al. (2019). Análisis comparativo entre metodologías ágiles y tradicionales para la gerencia de proyectos [Tesis de especialización, Universidad EAN]. Recuperado de: http://hdl.handle.net/10882/9559.

Enciso, H. (2021). *Diseño e implementación de un sistema de monitoreo del centro de datos para la red del INICTEL-UNI utilizando software libre.* [Tesis de grado, Universidad Nacional Tecnológica de Lima Sur] http://repositorio.untels.edu.pe/jspui/handle/123456789/581

Gaviria. (2019). *Implementación de una solución de administración y supervisión de servidores como herramienta de contingencia para la Empresa EMTELCO S.A.S*. [Tesis de grado , Universidad de Antioquia]. http://bibliotecadigital.udea.edu.co/bitstream/10495/16689/1/GaviriaFabio_2019_AdministracionSupervisionServidores.pdf.

Gartner. (2017). Gartner's Top 10 Strategic Technology Trends for 2017. Recuperado de https://www.gartner.com/smarterwithgartner/gartners-top-10-strategic-technology-trends-for-2017/

Gartner, Inc. (s. f.). *IT Infrastructure Monitoring Tools Reviews 2022 | Gartner Peer Insights*. Gartner. https://www.gartner.com/reviews/market/it-infrastructure-monitoring-tools

Herramientas ITIM. (2017, 6 de junio). ¿Qué son las herramientas de ITIM? Recuperado de https://pandorafms.com/blog/es/herramientas-itim/

Hitesh J. (2021, March 26). What is the Internet Control Message Protocol (ICMP)? Retrieved January 19, 2022, from ITT Systems website: https://www.ittsystems.com/what-is-icmp/

ITIL FOUNDATION. (2019). En AXELOS, ITIL FOUNDATION.

Janaina, S. (2015). *Software livre no gerenciamento de redes: solucao eficiente e de baixo custo numa empresa alfa do polo industrial* [Tesis de Maestría, Belém, Brasil: Universidade Federal do Pará.] https://ppgep.propesp.ufpa.br/ARQUIVOS/dissertacoes/Dissertacao2015-PPGEP-MP-JanainaSilvadeSouza.pdf

Kavis, M. J. (2018). Architecting for Scale: High Availability for Your Growing Applications. Apress.

Kundu, D., & Ibrahim, M. (2009). Cacti 0.8 network monitoring : monitor your network with ease! Retrieved from https://www.packtpub.com/product/cacti-0-8-network-monitoring/9781847195968

Lerner, A. (2014, 16 Julio). *The Cost of Downtime*. Andrew Lerner. https://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/

López, S., & Geovanni, J. P. (2020). Implementación del software APM para monitorear eficientemente las aplicaciones en la Empresa América Móvil Perú SAC. [Tesis de grado. Universidad Peruana De Ciencias E Informática]. http://repositorio.upci.edu.pe/handle/upci/124

Mike, K.. (2017). *Practical Monitoring. Retrieved January 17, 2022, edición y editorial O'Reilly Online Learning* website: https://www.oreilly.com/library/view/practical-monitoring/9781491957349/

Patricia, A., Rueda, A., & Ávila, J. (2019). *Análisis comparativo entre las metodologías clásica y SCRUM en el desarrollo de proyectos de software en empresas colombianas.*[Tesis de grado, Universidad Pontificia Bolivariana, Medellín, Colombia.] https://repository.upb.edu.co/bitstream/handle/20.500.11912/9610/226_1%20%281%29.pdf?sequence=1&isAllowed=y

Piere, J. (2020). *Implementación del software APM para monitorear eficientemente las aplicaciones en la Empresa América Móvil Perú S.A.C* [tesis de grado, Universidad Peruana de Ciencias e Informática] https://doi.org/http://repositorio.upci.edu.pe/handle/upci/124

Quispe, J.(2018). *Implementación de un sistema de monitoreo y control de red, para un canal de televisión, basado en herramientas Open Source y Software Libre, Lima-2017.* [Tesis de grado, Universidad del Altiplano] http://repositorio.unap.edu.pe/handle/UNAP/9019

Raya, L. (2011). *Sistemas informáticos (GRADO SUPERIOR).* https://www.ra-ma.es/libro/sistemas-informaticos-grado-superior_48431/

Remolina Becerra, L. C. (2019). Diseño de un modelo de seguridad informática a una empresa en su sistema de monitoreo del área de tecnología. [Tesis de grado, Universidad Cooperativa de Colombia]. https://repository.ucc.edu.co/bitstreams/a9395c18-9953-4d1a-9631-21b832c66dbd/download

Saavedra Drouet, C. (2018). *Control de servicios de red y servidores basado en herramientas de administración de red y políticas de gestión de calidad.* [Tesis de grado, Universidad Católica del Ecuador Sede Esmeraldas). https://repositorio.pucese.edu.ec/handle/123456789/1463

Schwaber, K., & Sutherland, J. (2016). La guía definitiva de Scrum: las reglas del juego. Scrum.org. https://scrumguides.org/docs/scrumguide/v2016/2016-Scrum-Guide-Spanish.pdf

Sevillano Jaén, F. (2021). Ciberseguridad Industrial e Infraestructuras Críticas (1.a ed.). RA-MA. https://www.ra-ma.es/libro/ciberseguridad-industrial-e-infraestructuras-criticas_119432/

Silva, Martins, R. S., & Medeiros, R. (2016, January 13). *Análise e gerenciamento de redes usando uma metodologia proativa com zabbix*. Retrieved January 19, 2022, from ResearchGate website: https://www.researchgate.net/publication/290475139_ANALISE_E_GERENCIAMENTO_DE_REDES_USANDO_UMA_METODOLOGIA_PROATIVA_COM_ZABBIX

Trujillo, S. (2020). *Influencia de la aplicación del software Zabbix en el monitoreo de la red de área local de la Superintendencia Nacional de los Registros Públicos zona registral N° V - sede Trujillo.*[tesis de maestra, Universidad Privada Antenor Orrego]. https://hdl.handle.net/20.500.12759/6085

Vallejo, L. (2020). *Diseño e implementación de un sistema centralizado de monitoreo, supervisión y control automático de servidores y servicios en entornos virtuales de la empresa Mensaje Plus basado en herramientas de código abierto.* [Tesis de grado, Universidad Politécnica Salesiana]. http://dspace.ups.edu.ec/handle/123456789/19100

VELIMIROVIC, A.: *What is Nagios {Installation, How It Works, Features}.* (2021, October 7)., del Blog phoenixNAP: https://phoenixnap.com/blog/nagios-monitoring-tutorial

Zabbix. (2022). *Zabbix Documentation 5.4*, desde la web de Zabbix: https://www.zabbix.com/documentation/current/en/manual/introduction/manual_structure

ANEXOS

Anexo 01: Matriz de consistencia

Título: IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO PARA LA INFRAESTRUCTURA DE TI EN EL INSTITUTO DE ENFERMEDADES NEOPLASICAS DEL SUR-IRENSUR

Responsable: Karol Jhusep Nuñez Parra.

PROBLEMA	OBJETIVO	HIPÓTESIS	VARIABLES	METODOLOGÍA
Problema general ¿Cómo se llega a implementar un sistema de monitoreo de infraestructura que este sea open source y desplegarlo dentro de la red LAN del Instituto Regional de enfermedades Neoplásicas del Sur-IRENSUR ? **Problemas específicos** **P.E.1** ¿Qué procesos críticos y no críticos se llegarán a monitorear del Instituto Regional de enfermedades Neoplásicas del Sur-IRENSUR? **P.E.2** ¿Cuáles son los pasos por seguir para la instalación y despliegue del sistema de monitoreo? **P.E.3** ¿Dentro de un sistema de monitoreo de infraestructura	**Objetivo general** Implementar un sistema de monitoreo que permita gestionar y administrar la infraestructura de TI y equipos de salud ,esto dentro de la red LAN del Instituto Regional de enfermedades Neoplásicas del Sur-IRENSUR **Objetivos específicos:** **O.E.1**. Analizar la infraestructura de TI a monitorear de los servicios y host, sean estos críticos y no críticos **O.E.2** Instalar y desplegar el sistema monitoreo en todos los dispositivos y equipos hospitalarios que sean de importancia. **O.E.3** Crear un Bot chat de alarmas, sobre parámetros		-	**Enfoque:** Tecnológico. **Tipo de investigación:** Tecnológico. **Diseño de Investigación:** No Aplica. **Diseño:** No Aplica. **Metodología de investigación:** SCRUM **Población:** No aplica. **Muestra:** No aplica. **Técnica e instrumentos:** **Técnica:** No aplica **Instrumentos:** No aplica **Métodos de análisis de datos** No aplica.

de ti es posible tener alertas adelantándose a posibles fallos o cuando estos estén ocurriendo?	pendientes o algún excepcional, que se generen en el sistema de monitoreo Infraestructura de TI y notifiquen a los encargados según sea el caso.			

Anexo 2: Instrumentos de investigación y Ficha de validación del diseño y/o software

Validacion de Implementacion de Sistema de Monitoreo de Infraestructura de TI

DATOS GENERALES:

Apellidos y Nombres experto: Vidas Aguilar, Cesit

Cargo donde Labora: Residente Analista NOC - BNP

Objetivo de la evaluación: Validación de sistema de Monitoreo

Autor (a) de implementacion: Karol Thiseo Muñoz Payva

ASPECTOS DE VALIDACIÓN:

GENERALIDADES

Generalidades	Deficiente 0 – 20%	Regular 21 - 40%	Buena 41 - 60%	Muy Buena 61 -80%	Excelente 81 -100%
¿El sistema de monitoreo permite la identificación temprana de problemas en la infraestructura de TI?					96
¿El sistema de monitoreo proporciona información precisa sobre el rendimiento de los sistemas y aplicaciones de TI?					92
¿El sistema de monitoreo permite la identificación de problemas de seguridad en la infraestructura de TI?				76	
¿El sistema de monitoreo proporciona alertas en tiempo real sobre eventos críticos en la infraestructura de TI?					89
¿El sistema de monitoreo es fácil de usar y configurar?					90
¿El sistema de monitoreo proporciona informes y análisis detallados sobre el rendimiento y la salud de la infraestructura de TI?					92
¿El sistema de monitoreo es escalable para adaptarse a las necesidades futuras de la infraestructura de TI?				80	
¿El sistema de monitoreo ha mejorado la capacidad del equipo de TI para detectar, diagnosticar y solucionar problemas en la infraestructura de TI?					88

Promedio de Valoracion: 83%

Fecha: 13-06-2022

D.N.I: 41832804

Anexo 3: Informe de Turnitin al 14% de similitud

"IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO PARA LA INFRAESTRUCTURA DE TI EN EL INSTITUTO DE ENFERMEDADES NEOPLASICAS DEL SUR-IRENSUR"

INFORME DE ORIGINALIDAD

14%	14%	1%	5%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

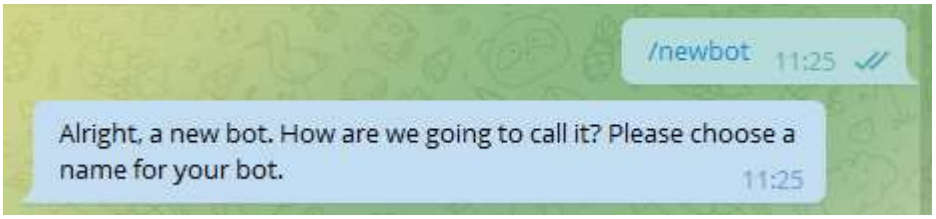
1	repositorio.autonomadeica.edu.pe Fuente de Internet	3%
2	repositorio.unsa.edu.pe Fuente de Internet	1%
3	1library.co Fuente de Internet	1%
4	Submitted to Ministerio de Educación de Perú - COAR Trabajo del estudiante	1%
5	devopslatam.com Fuente de Internet	1%
6	repositorio.espam.edu.ec Fuente de Internet	<1%
7	dgsa.uaeh.edu.mx:8080 Fuente de Internet	<1%
8	Submitted to Universidad Alas Peruanas Trabajo del estudiante	<1%

Anexo 4: Creación de agente Bot Telegram

.Pasos para creación de chat Bot en Telegram

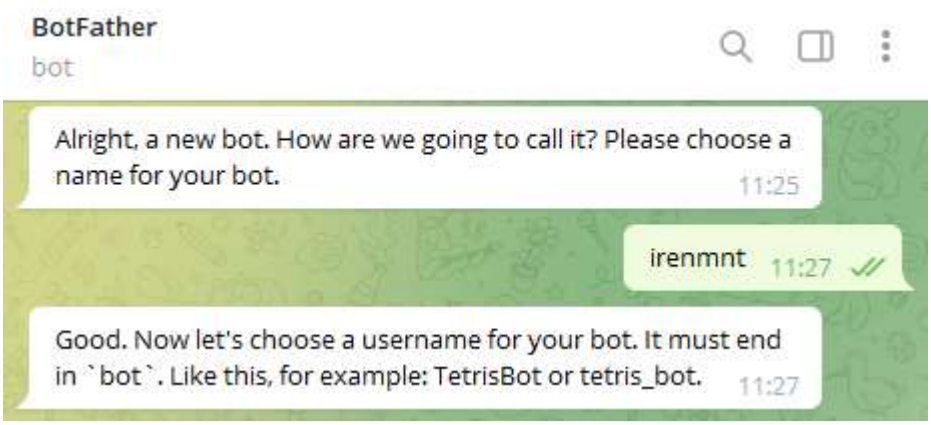
1. Acceder a la cuenta @botfather de Telegram

2. Se tendrá que ejecutar el siguiente comando para crear la cuenta Bot

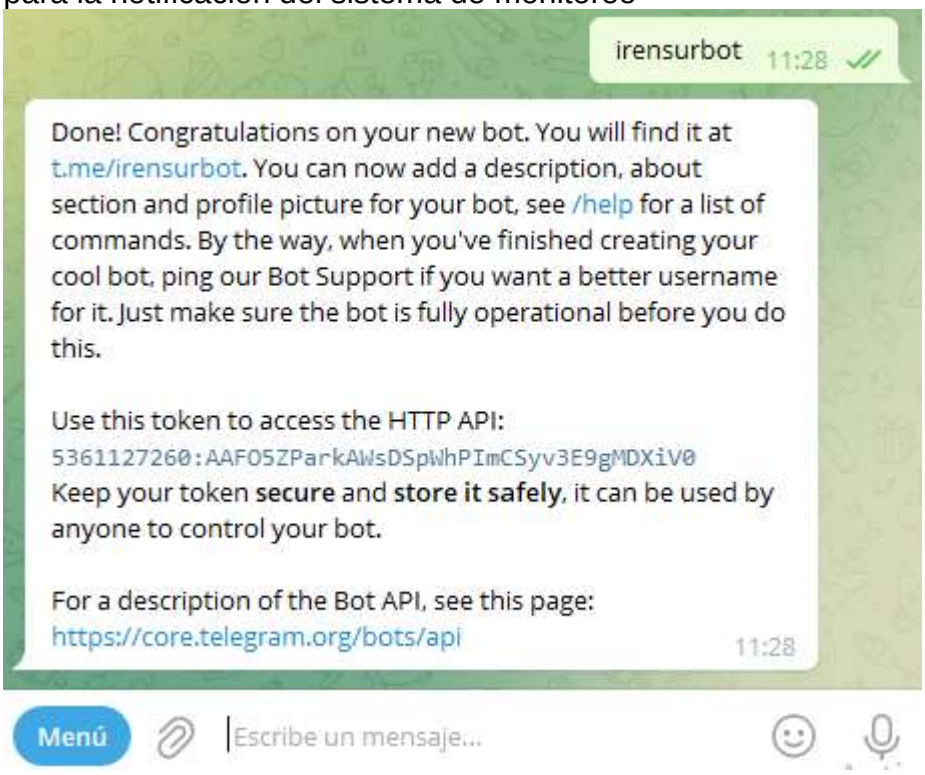


3. Luego de esto nos pedirá un nombre, que se le dará a la cuenta Bot a lo cual se le nombrará como **irenmnt**

4. A esto nos pedirá que se nombre a la cuenta juntamente a la apostrofe **Bot,** el nombre de la cuenta Bot es

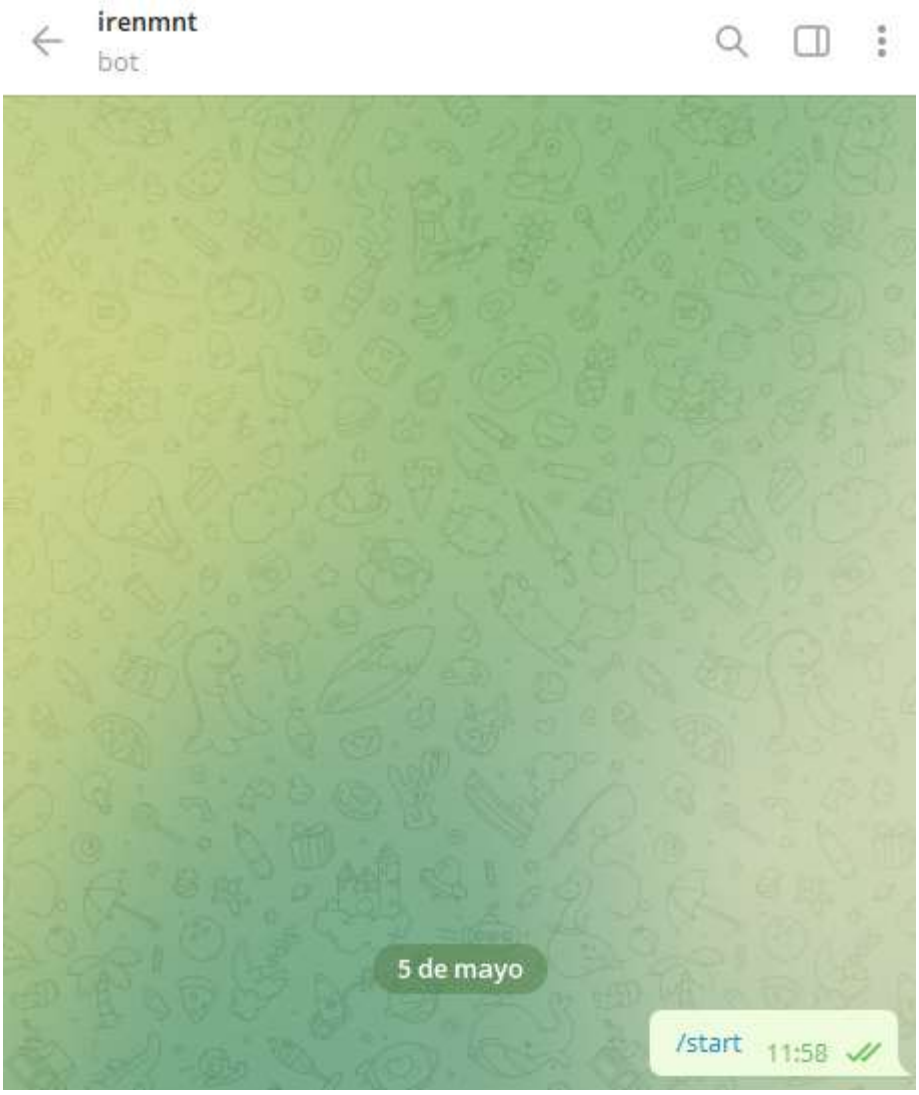


5. Luego de poner el nombre se nos mostrara que la cuenta esta ya creada y a lo cual se tiene que anotar el token http que se usara para la notificación del sistema de monitoreo



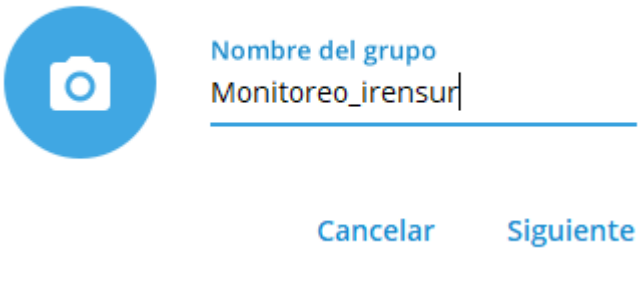
Token:
5361127260:AAFO5ZParkAWsDSpWhPImCSyv3E9gMDXiV0

6. Habilitar la sesión de Bot chat
Para esto se tendrá que enviar el comando /start dentro del chat Messenger que se tiene con el Bot, este es un requisito primordial para poder usarlo

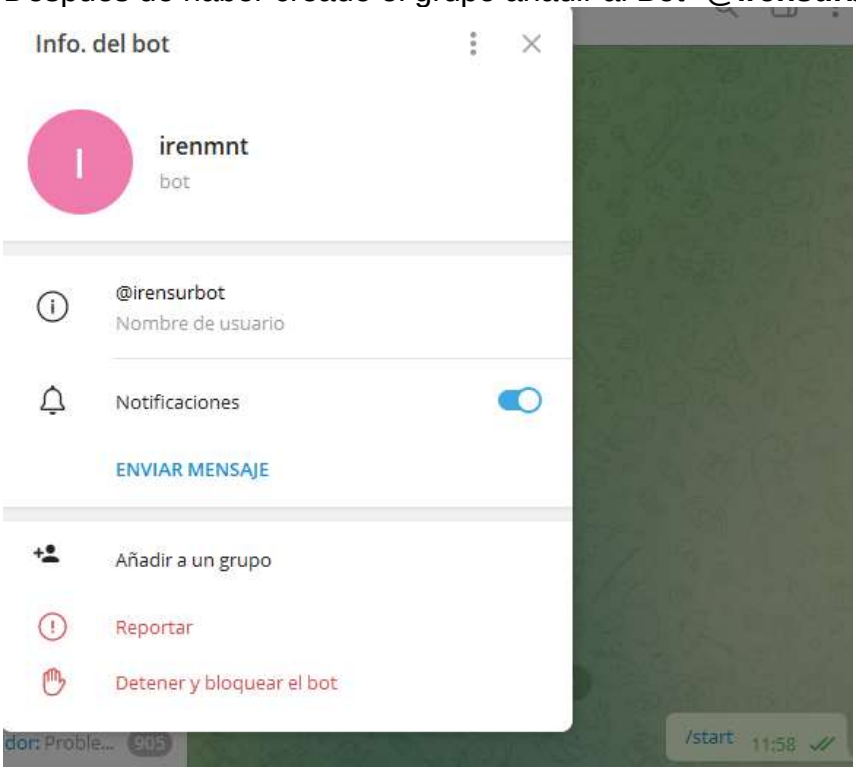


7. Se enviará las notificaciones al grupo **irensur_monitoreo**, para realizar estas notificaciones deberemos tener el ID de grupo, para esto se tendrá que hacer lo siguiente:

   Crear un grupo de chat de nombre **monitoreo_irensur**



8. Después de haber creado el grupo añadir al Bot "**@irensurbot**"

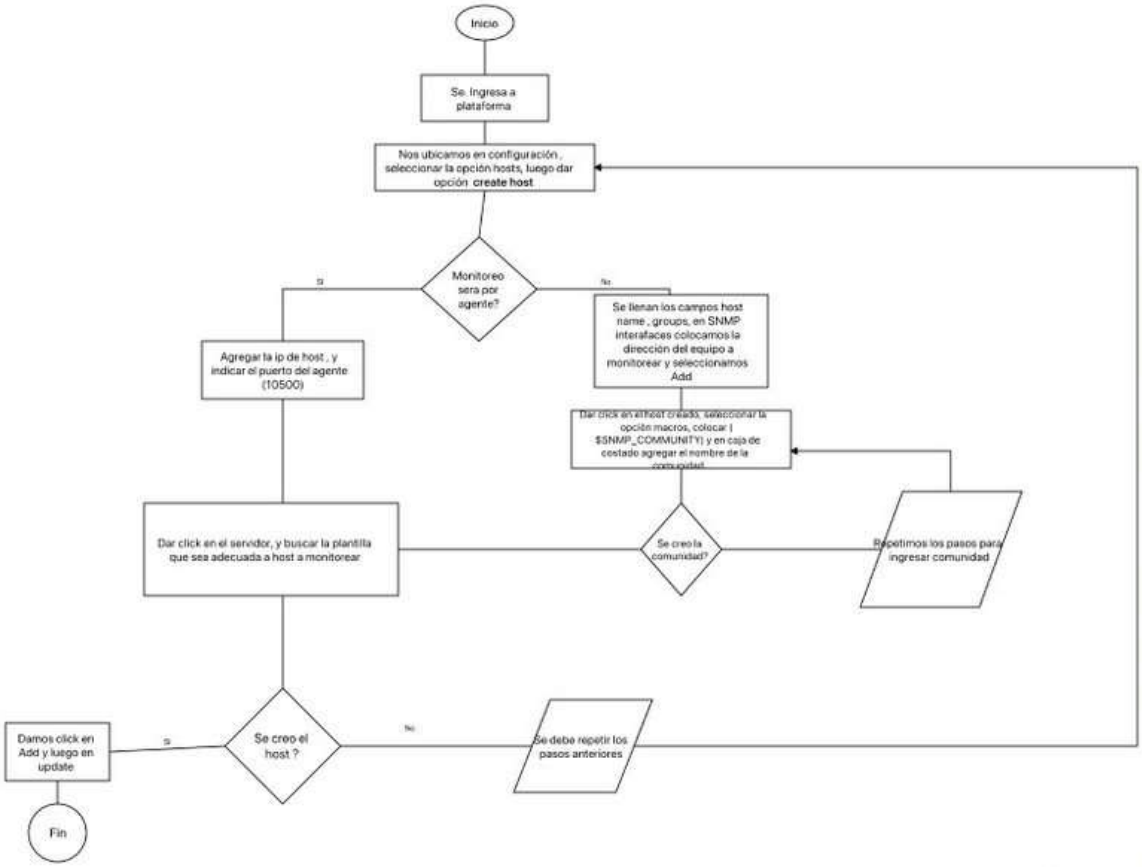


Ha esto se tendrá que escribir los siguientes comandos para la identificación del idgroup para enviar las notificaciones

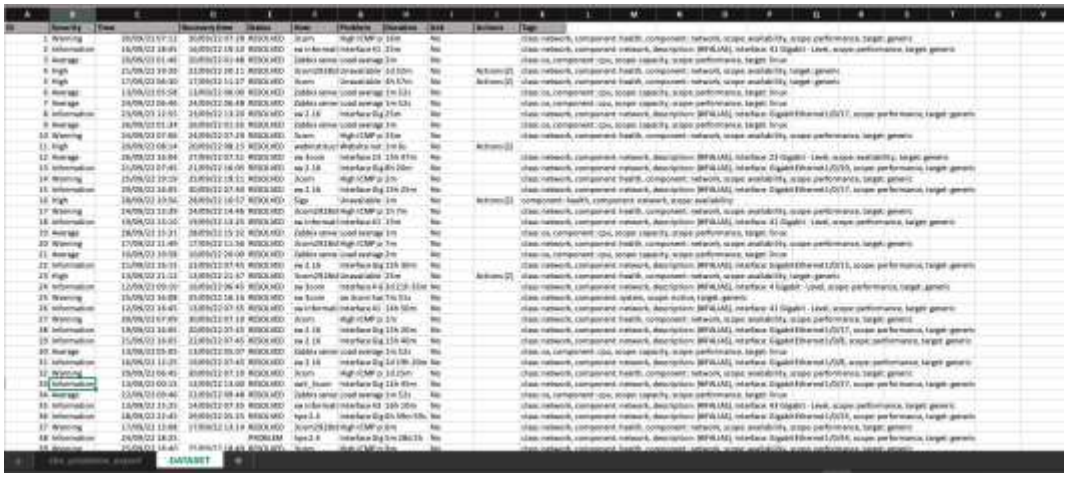
-614405832

ANEXO 5 MANUAL OPERACIONES

Diagrama de flujo de configuración host en Zabbix



ANEXO 6 MUESTRA ALEATORIA DE REGISTRO DE NOTIFICACIONES DEL SISTEMA DE MONITOREO DE INFRAESTRUCTURA DE TI IRENSUR



ANEXO 7 CUESTIONARIO DE ACTIVIDADES DE PERSONAL DE TI

1. ¿Cuáles son las principales responsabilidades de su rol en el departamento de TI?
2. ¿Cuáles son los principales procesos y actividades que se realizan en el departamento de TI actualmente?
3. ¿Cómo se realiza actualmente el monitoreo de la infraestructura de TI? ¿Qué herramientas y sistemas se utilizan para este fin?
4. ¿Cuáles son los principales desafíos o problemas que se han enfrentado en el monitoreo de la infraestructura de TI?
5. ¿Qué información se considera crítica para el monitoreo de la infraestructura de TI?
6. ¿Qué mejoras se podrían implementar con un nuevo sistema de monitoreo de TI? ¿Cómo se espera que este nuevo sistema mejore el monitoreo de la infraestructura de TI?
7. ¿Qué características o funcionalidades son importantes para el nuevo sistema de monitoreo de TI?
8. ¿Cómo se espera que el nuevo sistema de monitoreo de TI impacte en la eficiencia y eficacia del departamento de TI?
9. ¿Qué recursos serían necesarios para implementar el nuevo sistema de monitoreo de TI?

ANEXO 8 CODIGO DE PROCESAMIENTO DE DATA DE SISTEMA DE MONITOREO

```
import pandas as pd
import matplotlib.pyplot as plt
from datetime import datetime, timedelta

# Leer el archivo CSV y crear un DataFrame
df = pd.read_csv('data.csv', delimiter=';')

# Convertir las columnas de fecha/hora a formato datetime
df['Time'] = pd.to_datetime(df['Time'], format='%d/%m/%y %H:%M')
df['Recovery time'] = pd.to_datetime(df['Recovery time'], format='%d/%m/%y %H:%M')

# Calcular el tiempo de resolución de cada problema
df['Resolution time'] = df['Recovery time'] - df['Time']

# Calcular el porcentaje de problemas resueltos satisfactoriamente
resolved_problems = df[df['Status'] == 'RESOLVED']
problems_resolved_percentage = len(resolved_problems) / len(df) * 100

# Calcular el tiempo promedio de recuperación de problemas
avg_recovery_time = resolved_problems['Resolution time'].mean()

# Calcular la frecuencia de problemas
freq_problems = df['Severity'].value_counts()

# Generar histograma del tiempo de resolución de problemas
plt.hist(df['Resolution time'] / timedelta(minutes=1), bins=30)
plt.xlabel('Tiempo de resolución (minutos)')
plt.ylabel('Frecuencia')
plt.title('Histograma del tiempo de resolución de problemas')
```

```
plt.show()

# Generar gráfico de barras del porcentaje de problemas resueltos
plt.bar(['Problemas resueltos', 'Problemas sin resolver'], [problems_resolved_percentage, 100 - problems_resolved_percentage])
plt.ylim(0, 100)
plt.ylabel('Porcentaje')
plt.title('Porcentaje de problemas resueltos')
plt.show()

# Generar gráfico de línea del tiempo promedio de recuperación
resolved_problems = resolved_problems.set_index('Recovery time').sort_index()
resolution_times = resolved_problems['Resolution time'].resample('D').mean()
plt.plot(resolution_times / timedelta(hours=1))
plt.xlabel('Fecha')
plt.ylabel('Tiempo promedio de recuperación (horas)')
plt.title('Tiempo promedio de recuperación de problemas')
plt.show()
```

ANEXO 9 CONSTANCIA DE APROBACION DE INVESTIGACION

UNIVERSIDAD AUTÓNOMA DEICA

CONSTANCIA DE APROBACIÓN DE INVESTIGACIÓN

Dra. Mariana Alejandra Campos Sobrino
Decana de la Facultad de Ingeniería, Ciencias y Administración
Universidad Autónoma de Ica.

Presente. -

De mi especial consideración:

Sirva la presente para saludarla e informar que, **Karol Jhusep Nuñez Parra,** estudiante de la **Facultad de Ingeniería, Ciencias y Administración**, del programa Académico de **Ingeniería de Sistemas,** han cumplido con elaborar su:

PLAN DE TESIS		TESIS	X

TITULADA:

"IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO PARA LA INFRAESTRUCTURA DE TI EN EL INSTITUTO DE ENFERMEDADES NEOPLASICAS DEL SUR-IRENSUR"

Por lo tanto, quedan expeditos para continuar con el procedimiento correspondiente para solicitar la sustentación de su investigación ante el jurado evaluador que designe la Universidad, remito la presente constancia adjuntando mi firma en señal de conformidad.

Agradezco por anticipado la atención a la presente, aprovecho la ocasión para expresar los sentimientos de mi especial consideración y deferencia personal.

Cordialmente,

Dr. Elio Javier Huamán Flores
DNI: 42627418
CODIGO ORCID: 0000-0002-8461-5082