UNIVERSIDAD NACIONAL DE CAJAMARCA

FACULTAD DE INGENIERÍA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS

SISTEMA DE SOPORTE A LA SEGURIDAD DE LA INFORMACIÓN USANDO BIG DATA PARA MEJORAR LA GESTIÓN DE LA INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE CAJAMARCA

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTORA:

BR. EDITH ESTHER CÁCERES TAFUR

ASESOR:

DR. ING. EDWIN VALENCIA CASTILLO

CAJAMARCA- PERÚ

2021

AGRADECIMIENTO

Agradezco a Dios y su fidelidad, por siempre mostrar su amor y ricas bendiciones a mi persona, por permitirme tener una familia y personas que siempre me confortan. “Dijo Jehová: con amor eterno te he amado; por tanto, te prolongué mi misericordia". Jeremías 31:3

DEDICATORIA

Esta Investigación está dedicada a cada una de las personas que me apoyó incondicionalmente en el proceso de ser una mejor profesional y siempre me impulsó a crecer como persona.

CONTENIDO

ÍNDICE DE IMÁGENES

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

RESUMEN

La presente investigación tuvo como objetivo principal proponer un Sistema de soporte a la seguridad de la información usando big data para mejorar la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca, ya que sólo se contaba con buenas prácticas y lineamientos respecto a la seguridad de la información y uso de TI, motivo por el cual se mostraba una necesidad de medir e identificar los incidentes, ataques o riesgos que se dejaban pasar por alto; se encontró también la falta de alertas o soluciones ante los casos mencionados que se mostraban de forma reiterada. Para el desarrollo de este trabajo se usó la herramienta Nagios Core, importante herramienta que no solo permite identificar problemas sino reparar y disminuir efectos secundarios en situaciones futuras que puedan afectar al usuario final, en el transcurso del proyecto nagios permitió monitorear las diferentes áreas críticas seleccionadas en la infraestructura de TI de la oficina general de sistemas informáticos y plataformas virtuales de la institución, se logró obtener resultados confortantes ya que el 100% de usuarios calificaron como satisfactorio el uso de la herramienta, el uso de la herramienta no solo significó un manejo de grandes datos, sino una visión general y especifica de la funcionalidad de cada área evaluada y sus servicios vulnerables, así también logró identificar 2918 (7579% más de lo habitual) incidentes y controlar 403 de ellos en tiempos récord.

Palabras clave: Soporte, Seguridad, Gestión de TI, Infraestructura de TI, Incidentes, Big Data, Monitoreo.

ABSTRACT

The main objective of this research was to propose an information security support system using big data to improve the management of the information technology infrastructure of the National University of Cajamarca, since there were only good practices and guidelines regarding to information security and IT use, which is why there is a need to measure and identify incidents, attacks or risks that were overlooked; It was also found the lack of alerts or solutions in the cases mentioned that were shown repeatedly. For the development of this work, the Nagios Core tool was used, an important tool that not only allows to identify problems but also to repair and reduce secondary effects in future situations that may affect the end user. In the course of the nagios project, eventually monitor the different selected critical areas. In the IT infrastructure of the general office of computer systems and virtual platforms of the institution, it was possible to obtain comforting results since 100% of users described the use of the tool as satisfactory, the use of the tool not only meant a management of big data, but a general and specific vision of the function of each maintenance area and its vulnerable services, thus it also managed to identify 2,918 (7579% more than usual) incidents and control 403 of them in record time.

Keywords: Support, Security, IT Management, IT Infrastructure, Incidents, Big Data, Monitoring.

CAPÍTULO I. INTRODUCCIÓN

A diario aparecen nuevas amenazas que ponen en jaque a los sistemas de seguridad, en la gran mayoría de los casos corporativos se identifica al empleado como el denominador común quien produce estas vulnerabilidades, es decir el desconocimiento y desactualización de los temas de seguridad de información en las personas del equipo termina perjudicando a las empresas; según los datos de Cisco se identifica el manejo de seguridad de la información y gestión de TI en que el 65% de las compañías basan su defensa en el Firewall, un 56% en la prevención de pérdida de información, 53% en las autentificaciones y otro 53% en el cifrado de información [1], existen diferentes servicios vitales con infraestructuras físicas originalmente aisladas, que cada vez con mayor asiduidad se están interconectando a redes informáticas compartidas o públicas generando un mayor perímetro de ataque que facilitan diferentes formas para una intrusión, incluso algunas infraestructuras críticas se encuentran conectadas a Internet para su administración y monitoreo [2].

En el Perú el nivel de madurez de la gestión de la seguridad de la información aún es bajo, según la encuesta de seguridad de información de 2010 elaborada por el reconocido portal en seguridad de la información “SegurInfo”, el cual cuenta con el respaldo de prestigiosas instituciones de este rubro como ISACA, obtuvo como resultado que el principal obstáculo para desarrollar una adecuada seguridad dentro de las empresas es el poco entendimiento del tema [3].

De la misma forma es importante mencionar que en las empresas es habitual contar con distintas aplicaciones, herramientas y fuentes de datos, las cuales no permiten utilizar la información realizando combinaciones, cruces o cualquier tipo de procesado de datos, siendo este un inconveniente para que el equipo pueda determinar correctamente las causas de los incidentes, en estos casos el procesamiento de big data en tiempo real permite a las empresas usar los datos para mejorar la toma de decisiones, no solo en las decisiones futuras sino también en las decisiones presentes.

El problema de la Universidad Nacional de Cajamarca es que no cuenta con un sistema formalizado de monitoreo o control automatizado de incidentes y al mismo tiempo se muestra la necesidad de una herramienta de soporte a la

seguridad de la información, basada en el uso de big data y gestión de TI, siendo esta la mayor justificación para contar con un sistema de soporte claro y sencillo, que sea entendible sin generar mayor confusiones para los encargados, de tal forma que el uso sea con mayor confianza y sin dificultades, permitiendo medir y controlar incidentes detectados, por tanto, gestionar riesgos y el nivel de seguridad de la información de la institución de acuerdo a la estrategia del negocio (UNC) y a las regulaciones vigentes, siguiendo las buenas prácticas y estándares internacionales correspondientes que permitan realizar una adecuada gestión de la información, deseando saber en qué medida un sistema de soporte a la seguridad de la información usando big data puede mejorar la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca, llegando así al planteamiento de la hipótesis ¿Un sistema de soporte a la seguridad de la Información usando Big Data podrá mejorar la Gestión de Infraestructura de Tecnologías de Información en la Universidad Nacional de Cajamarca?.

El presente informe propone el uso de un sistema de soporte a la seguridad de la información de la Universidad Nacional de Cajamarca como medida preventiva y de mejora a las áreas críticas de TI fomentando la correcta gestión de TI y protección de información, lo que busca apoyar la operatividad institucional, mejorando la seguridad en la Infraestructura de TI, monitoreo de riesgos, incidentes e inventarios; por ser de importancia dicha herramienta implementada será a medida.

El sistema de soporte debe abarcar los requerimientos de principal importancia para las áreas críticas de la Infraestructura de TI, el uso big data en el proceso, además de verificar la factibilidad de ser implementado. La estructura visual y características del sistema se dan en función de la herramienta de desarrollo (consideraciones indicadas por la Oficina de Sistemas Informáticos y plataformas virtuales). El objetivo principal es proponer un sistema de soporte a la seguridad de la información usando big data para mejorar la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca. De forma secundaria, determinar las características de un sistema de soporte a la seguridad de la información usando big data, caracterizar los dominios de protección en la gestión de la Infraestructura de TI de la Universidad Nacional de Cajamarca, desplegar el sistema de soporte a la seguridad de los

dominios identificados, evaluar y analizar la influencia del sistema de soporte de seguridad en la gestión de la infraestructura de TI, permitiendo validar la hipótesis.

En el capítulo I se presenta el problema, hipótesis, alcances y objetivos de la investigación. En el capítulo II se habla del marco teórico: antecedentes, bases teóricas y términos básicos; necesarios para comprender el proyecto. El capítulo III muestra los materiales y métodos usados en el desarrollo del proyecto de investigación, de igual forma se detalla el tratamiento de datos. En el capítulo IV la descripción, explicación y discusión de los resultados Obtenidos. Finalmente, en el capítulo V se muestran las conclusiones según los objetivos planteados y las recomendaciones que se consideran necesarias para una mejora posterior contribuyendo al tema de investigación.

CAPÍTULO II. MARCO TEÓRICO

1. ANTECEDENTES TEÓRICOS DE LA INVESTIGACIÓN

2.1.1 ANTECEDENTES INTERNACIONALES

2.1.1.1. Gutierrez [4] en su informe “Lo que representa BIGDATA para la seguridad de la información” en Welivesecurity nos habla que la cantidad de información a la cual debemos acceder para realizar nuestras actividades diarias es cada vez mayor: Twitter, LinkedIn, blogs especializados, sistemas internos, etc; además de la creciente cantidad multimedia, metodologías, herramientas y tecnologías hacen parte del reto que plantea Big Data, que en el ambiente empresarial se adopta una tendencia, los cambios que implica se suelen hacer pensando en la tecnología. Si bien es lo más importante, hay otra serie de factores que deben considerarse para garantizar la seguridad de la información por lo cual es necesario entender cuáles son las implicaciones de estas nuevas tendencias [5]. La adopción de la tecnología que permita manejar Big Data debe ser pensada específicamente. Estructuras de cómputo distribuido, en los cuales intervienen múltiples plataformas y sistemas deben tener consideraciones especiales de seguridad, pues tanta diversidad puede dar a lugar a que queden agujeros de seguridad explotables por ciberdelincuentes, el almacenamiento y el procesamiento en la nube es una alternativa muy interesante, pero es necesario contar con las garantías necesarias para que se mantenga la confidencialidad de la información [5]. Como cualquier esquema de seguridad la educación de los empleados es necesario para que se incorporen hábitos seguros en el manejo de la información, apoyados en soluciones que aseguren el acceso y manipulación de los datos. Todos los cambios deben articularse desde las políticas de seguridad de la información, por lo cual se hace necesaria una revisión completa que permita identificar aquello de debe ajustarse al nivel de riesgo aceptado por la empresa. Lograr analizar de forma oportuna los altos volúmenes de información para minimizar la ocurrencia de los riesgos

en las empresas y maximizar las oportunidades propias del negocio es sin lugar a dudas el siguiente paso en el análisis de datos. Ya muchas empresas han dado ese paso, el reto está en implementarlo de forma segura [5].

2.1.1.2. Otarán y Perera [6] es su tesina de licenciatura “Propuesta de una solución de monitoreo para sistemas del CeSPI” plantean alcanzar una solución de monitoreo que permita entender a la infraestructura no como piezas separadas, sino como un conjunto de componentes correlacionados. Parte importante de la implementación y mantenimiento de los proyectos de la oficina es la recolección y análisis de datos de su funcionamiento. Este análisis es importante para conocer la salud de los servidores y el rendimiento de los equipos, detectar fallas en el hardware y software, descubrir comportamientos que afecten la funcionalidad de las aplicaciones y tomar decisiones que mejoren la productividad y calidad de los servicios brindados. En la actualidad existen una gran variedad de herramientas que pueden ser usadas para tener un seguimiento de métricas sobre servicios de software, y es posible integrar estas herramientas para crear un sistema que permita obtener, almacenar y visualizar los resultados. El objetivo que tiene la investigación de esta tesis es plasmar el resultado de comparar y proponer una estrategia de recolección, análisis y utilización de información de la infraestructura y aplicaciones del CeSPI (Centro Superior para el Procesamiento de la Información), que permita simplificar y enriquecer su análisis posterior y resulte en un monitoreo eficiente.

2.1.1.3. Aguirre [2] en su tesis “Ciberseguridad en Infraestructuras Críticas de Información” en la Universidad Nacional de Buenos aires para obtener la Maestría en Seguridad de la Información menciona la importancia de la ciberseguridad en las infraestructuras críticas de información, las actividades se desarrollaron en este sentido de manera general en algunos países con el apoyo de las organizaciones internacionales que colaboran en el área de la ciberseguridad. Sobre esta base, propone un modelo para la identificación de los sectores y servicios críticos de una economía y una serie de controles mínimos para su

protección. En efecto concluye, que las tecnologías de la información se han esparcido rápidamente en todos los sectores de la sociedad y prácticamente no existen servicios críticos que no dependan de aplicaciones, bases de datos, servidores, redes de comunicaciones, centros de datos, etc. La falta de controles de ciberseguridad ha ocasionado que algunos servicios se vean afectados a nivel mundial, como lo demuestran los incidentes de ciberseguridad que se describen en el trabajo y que impactaron en el funcionamiento de diferentes servicios críticos de tres países.

2.1.1.4. Santander [7] en su trabajo de maestría “Análisis y Propuesta de Arquitectura para garantizar Seguridad en entornos Big Data” menciona que su objetivo fundamental consiste en estudiar, comparar y analizar un determinado conjunto de tecnologías acerca de seguridad en sistemas, y aplicarlas en una arquitectura común a modo de propuesta de diseño, que supla los requisitos mínimos de seguridad en un entorno Big Data, dando el soporte faltante. Además, se quiere enfocar este proyecto en aplicaciones/implantaciones para el mundo empresarial, se pretende analizar una metodología efectiva capaz de gestionar los datos de los clientes de una empresa sin comprometer su privacidad; a pesar del crecimiento tan veloz que el Big Data está experimentado, tiene aún necesidades que suplir en cuestiones de seguridad. Existen diferentes razones por las cuales el Big Data no se encuentra tan actualizado en esta materia. La causa principal se debe a la gran carga computacional que supone encriptar determinados tamaños de datos, es difícil encontrar una solución óptima que permita ejecutar las funcionalidades de analítica y procesamiento de datos en un periodo razonable de tiempo. En definitiva, se precisa proteger un sistema que cumpla con las características básicas que presenta el Big Data, en cuanto a volumen y velocidad se refiere, de ahí a una necesidad de protección completa para sus almacenes de datos.

2.1.2 ANTECEDENTES NACIONALES

2.1.2.1. Aquije y Jave [3] en su tesis “Metodología De Gestión De Seguridad De La Información para el Sector Financiero Peruano” en la Universidad Nacional de Ingeniería plantean la necesidad de una metodológica para realizar una implementación exitosa del Sistema de Gestión de Seguridad de la Información (SGSI) en las empresas del Sector Financiero Peruano y de este modo dar cumplimiento a la regulación vigente que, de acuerdo a la Circular G-140 de la SBS (Superintendencia de Banca, Seguros y AFP), exige la implementación del SGSI. El problema abordado es la dificultad de las empresas de este sector para implementar el SGSI, es por ello que, el mencionado ente regulador ha venido aplazando las fechas límites de implementación al constatar que no ha sido posible que las empresas logren implementar el SGSI en el plazo previsto. Según se plantea en la tesis y de acuerdo a estudios internacionales, uno de los factores más importantes que no permiten una implementación exitosa del SGSI es el poco entendimiento que aún tienen las empresas sobre la Seguridad de la Información. Con la finalidad de dar solución al problema identificado, es que en la mencionada tesisse muestra una serie de pasos, herramientas, formatos que ayudarán y facilitarán la gestión de la seguridad de la información considerando las etapas del ciclo Deming: Establecimiento, Implementación, Monitoreo y Mejora Continua.

2.1.2.2. Quispe [8] menciona en la tesis “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” en la Universidad Nacional del Altiplano, muestra el monitoreo de la red del canal de televisión WILLAX TV en el Área de Tecnología y Soporte [8], el cual no contaba con ninguna herramienta de ese tipo, se hizo uso de la herramienta de monitoreo NAGIOS y logrando una comprobación efectiva y constante dsistena de monitoreoe los servicios y dispositivos (host, procesador, memoria RAM, Router, Fibra Óptica, Access Point, servidor) del canal de televisión; asegurando una reacción oportuna para solucionar los fallos que se

presenten en estos, los cuales proporciona mejora en la administración de los servicios y dispositivos de la red, para el personal [8]. Según detalla en informe "… El sistema de monitoreo NAGIOS permite a las organizaciones identificar y resolver problemas de infraestructura de TI antes que ellos afecten los procesos de negocios críticos. Diseñado con escalabilidad y flexibilidad, es una herramienta potente que permite detectar y reparar problemas, mitigar eventos futuros antes que afecten al usuario final y clientes [8]". Finalmente, en el estudio muestra pruebas de funcionamiento para verificar la efectividad del tráfico de red, administración de dispositivos y servicios, dando una respuesta positiva [8].

2. BASES TEÓRICAS

En este ítem se describen los principales conceptos relacionados a la investigación, se hace referencia a: sistema de soporte, seguridad de la información, gestión de TI, gestión de riesgos, incidentes e inventarios, big data, infraestructura de TI, etc.; con el objetivo de establecer un panorama claro y entendible de las bases teórica que serán usadas para el desarrollo de la investigación.

2.2.1 SEGURIDAD DE LA INFORMACIÓN

Es el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información, dicho de otro modo, son todas aquellas políticas de uso y medidas que afectan al tratamiento de los datos que se utilizan en una organización [9]. Se puede definir como la preservación de la confidencialidad, integridad y disponibilidad de la información juntamente con otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad [10].

- Disponibilidad: Acceso a la información cuando se requiere, teniendo en cuenta la privacidad. Evitar "caídas" del sistema que permitan accesos ilegítimos, que impidan el acceso al correo [9].
- Confidencialidad: Información accesible solo para personal autorizado. La información no debe llegar a personas o entidades que no estén autorizados [9].

- Integridad: Información correcta sin modificaciones no autorizadas ni errores. Se protege frente a vulnerabilidades externas o posibles errores humanos [9].
- Autenticación: Información procedente de un usuario que es quien dice ser. Se verifica y se debe garantizar que el origen de los datos es correcto [9].

Conocer y aplicar los cuatro pilares de la seguridad de la información es la base para una actitud ciber-resiliente [9].

2.2.2 CIBER – RESILIENCIA

Es la capacidad de una organización de gestionar el riesgo existente y superarlo con un mínimo impacto para la organización. Por lo tanto, es importante disponer de soluciones tecnológicas que aseguren la protección, conocer en todo momento el estado de protección de nuestra infraestructura y contar con las herramientas adecuadas para una gestión eficiente que garantice la continuidad en caso de ciberataque [9].

2.2.3 GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN

Es el proceso de supervisión de todos los asuntos relacionados con las operaciones y recursos de tecnología de la información dentro de una organización de TI. La gestión de TI asegura que todos los recursos tecnológicos y los empleados asociados son utilizados correctamente y de una manera que proporciona valor para la organización. La gestión de TI efectiva permite a una organización optimizar los recursos y la dotación de personal, mejorar los procesos de negocio y de comunicación y aplicar las mejores prácticas [11].

2.2.4 GESTIÓN DE INCIDENTES

La gestión de incidentes es un área de procesos perteneciente a la gestión de servicios de tecnologías de la información. El primer objetivo de la gestión de incidentes es recuperar el nivel habitual de funcionamiento del servicio y minimizar en todo lo posible el impacto negativo en la organización de forma que la calidad del servicio y la disponibilidad se mantengan [12].

Se considera incidente a un evento indeterminado ni planificado dentro del flujo normal de un servicio, el cual puede generar el mal funcionamiento o interrupción del mismo. El objetivo de ITIL es reiniciar el funcionamiento normal tan rápido como sea posible con el menor impacto para el negocio y el usuario con el menor coste posible" [13].

2.2.5 GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La gestión del riesgo en la seguridad de la información es un proceso continuo. Tal proceso debería establecer el contexto, evaluar los riesgos, tratar los riesgos utilizando un plan de tratamiento para implementar las recomendaciones y decisiones. La gestión del riesgo analiza lo que puede suceder y cuáles pueden ser las posibles consecuencias, antes de decidir lo que se debería hacer y cuando hacerlo, con el fin de reducir el riesgo hasta un nivel aceptable [3].

2.2.6 INFRAESTRUCTURA CRÍTICA DE TI

Una infraestructura crítica de Información (en adelante "infraestructuras críticas") es el conjunto de activos tecnológicos indispensables, que interactúan entre sí para brindar servicios vitales a los habitantes de un país. Los activos pueden ser instalaciones físicas o virtuales, redes de datos, redes industriales, sistemas de información, bases de datos, sistemas de control industrial, procesos automatizados o cualquier otro componente tecnológico que permite la prestación o el monitoreo de un servicio esencial para el bienestar de la población y el sostenimiento de la economía de un país. La falta de controles de ciberseguridad para proteger estos activos origina un grave riesgo para una nación. La realidad es que los activos no están exentos de sufrir un incidente de ciberseguridad debido al importante número de amenazas que existen en el ciberespacio. El impacto de un incidente puede afectar a diferentes sectores de un país como por ejemplo, el de la salud, la administración pública, el financiero, el de las telecomunicaciones o los proveedores de energía, entre 8 otros. En este contexto se debe tener en cuenta que los servicios vitales o críticos de un país están respaldados por infraestructuras críticas y que estas infraestructuras críticas están formadas por activos críticos que deben ser

protegidos. Las infraestructuras críticas pueden clasificarse de la siguiente manera, de acuerdo a su prestación [14].

De servicio.- Las infraestructuras críticas de servicio proveen servicios vitales a un país y para ellas, la disponibilidad constituye la condición especial. La falta de disponibilidad genera un gran impacto en los ciudadanos. Las mayores amenazas que tienen este tipo de infraestructuras son: los ataques de denegación de servicio distribuidos y el malware que tiene por objetivo alterar el funcionamiento de los sistemas principales [2].

De información.- Las infraestructuras críticas de información almacenan, procesan o transfieren información de tipo confidencial o sensible para su propietario. El propietario de la información puede ser una organización proveedora de servicios vitales, instituciones públicas o privadas o un ciudadano. La información es el activo crítico de estas infraestructuras y por lo tanto, se debe garantizar su confidencialidad, integridad y disponibilidad. Las mayores amenazas que tienen estas infraestructuras son: fraudes, robo de información confidencial y malware dedicado a secuestrar la información sensible [2].

2.2.7 AMENAZAS EN LAS INFRAESTRUCTURAS CRÍTICAS

La adopción de nuevas tecnologías sin considerar los debidos controles de ciberseguridad en las infraestructuras críticas, genera potencialmente nuevos vectores de amenazas, especialmente en los ambientes industriales porque se conectan redes seguras con entornos no seguros como Internet. Las amenazas buscan aprovechar una debilidad o ausencia de controles en los sistemas para explotar una vulnerabilidad. A continuación podemos identificar algunas fuentes de amenazas: - Estados extranjeros - Crimen organizado - Hacktivistas - Delincuentes - Organizaciones terroristas Estas fuentes pueden originar, entre otros, los siguientes tipos de amenazas: - Espionaje industrial - Sabotaje - Robo de datos - Indisponibilidad del servicio - Explotación de código malicioso [15].

2.2.8 CIBERSEGURIDAD EN LAS INFRAESTRUCTURAS CRÍTICAS

Las infraestructuras críticas están evolucionando con el avance de la tecnología. En efecto, la mayoría está usando redes de datos de gran cobertura, sistemas de información y sistemas de control industrial por sus grandes beneficios, especialmente por sus menores costos, rápida implementación, flexibilidad frente a los cambios y por la posibilidad de su administración y monitoreo de manera remota. Incluso algunos administradores monitorean las infraestructuras críticas directamente a través de Internet. La conexión de las redes de datos industriales con redes de datos extendidas y públicas, genera un vector de ataque para la proliferación de amenazas. La conexión de sistemas industriales con sistemas corporativos hace que la información y los sistemas necesariamente deban ser protegidos, ya que las redes de datos públicas como Internet, ampliamente utilizadas en las áreas corporativas, facilitan la intrusión y difusión de agentes externos potencialmente destructivos. Los ciberataques que sufren hoy en día las infraestructuras críticas son cada vez más sofisticados y se han convertido en una gran preocupación para sus responsables y proveedores. Debido a esto, los países a través de instituciones públicas y privadas deben estar preparados para enfrentar a estos ciberataques. Además, se necesita trabajar coordinadamente entre países y entre diferentes sectores, para evitar la interrupción de los servicios imprescindibles o críticos para los ciudadanos. La ciberseguridad aplicada en las infraestructuras críticas permite reducir los riesgos sobre los activos críticos de una nación, mediante la aplicación de políticas, normas, procedimientos, herramientas y/o buenas prácticas de seguridad en el ciberespacio. De acuerdo a la ITU (Unión Internacional de las Telecomunicaciones), el término ciberespacio se utiliza para describir sistemas y servicios conectados directa o indirectamente a Internet o a redes de telecomunicaciones y datos [6]. En este contexto, es posible afirmar que el proceso de adopción de nuevas tecnologías en infraestructuras críticas es irreversible. Por ello, se debe trabajar sobre el campo de la ciberseguridad para minimizar los riesgos a los que se exponen. Los gobiernos deben promover la creación de una estrategia de

ciberseguridad para proteger la información y los servicios vitales de un país, y reconocer la importancia de la protección de las infraestructuras críticas de información [16].

2.2.9 NAGIOS

Nagios es un poderoso sistema de monitoreo que permite a las organizaciones identificar y resolver problemas de infraestructura de TI antes de que afecten los procesos comerciales críticos [17]. Diseñado teniendo en cuenta la escalabilidad y la flexibilidad, Nagios le brinda la tranquilidad de saber que los procesos comerciales de su organización no se verán afectados por interrupciones desconocidas, Nagios es una herramienta poderosa que le brinda conocimiento instantáneo de la infraestructura de TI de misión crítica de su organización [17]. Nagios va a permitir que pueda detectar y reparar problemas, con la intención de reducir problemas futuros que puedan causar daños a los usuarios finales.

Al usar Nagios, puedes planificar las actualizaciones de infraestructura antes de que los sistemas obsoletos causen fallases decir, dar solución de forma inmediata a los problemas que se presenten, con previa coordinación con el equipo técnico, asegurando que se cumplan los SLA de su organización, que las interrupciones de la infraestructura de TI tengan un efecto mínimo en los resultados de su organización y un monitoreo toda su infraestructura y procesos comerciales.

Nagios permite monitorear los componentes críticos de la infraestructura de TI, incluidos las métricas del sistema, los protocolos de red, las aplicaciones, los servicios, los servidores y la infraestructura de red. Que sus usuarios reconozcan las alertas su resolución de interrupciones, del mismo modo pretende investigar si existe un nuevo caso de alerta. Las alertas de derivan a diferentes grupos en caso no se reconozcan de manera oportuna. El tiempo de inactividad programado evita alertas durante el mantenimiento programado y las ventanas de actualización. Nagios envía alertas cuando los componentes críticos de la infraestructura fallan y se recuperan, proporcionando a los administradores avisos de eventos importantes, las alertas se pueden enviar por correo electrónico, SMS o script personalizado [18]. Los informes proporcionan un registro histórico

de interrupciones, eventos, notificaciones y respuestas de alerta para su posterior revisión. Los informes de disponibilidad ayudan a garantizar que se cumplan sus SLA Los gráficos e informes de planificación de tendencias y capacidad le permiten identificar las actualizaciones de infraestructura necesarias antes de que ocurran fallas [19].

2.2.9.1 NAGIOS CORE

Nagios Core es el motor de monitoreo y alerta que sirve como la aplicación principal alrededor de la cual se construyen cientos de proyectos. Nagios Core sirve como el planificador de eventos básico, el procesador de eventos y el administrador de alertas para los elementos que se monitorean. Cuenta con varias API que se utilizan para ampliar sus capacidades para realizar tareas adicionales, se implementa como un demonio escrito en C por razones de rendimiento y está diseñado para ejecutarse de forma nativa en sistemas Linux / * nix. Ha sido diseñado con una arquitectura enfocada y extensible diseñada para flexibilidad y escalabilidad. Proporciona varias API para permitir que su conjunto de características se extienda fácilmente a través de complementos adicionales. Esta arquitectura ha demostrado ser exitosa y ha generado la creación de miles de proyectos adicionales que extienden su conjunto de características principales [20].

El Alcance general de Nagios Core se centra principalmente en las tareas de programación, ejecución, procesamiento, manejo de eventos y alertas. Nos permite realizar comprobaciones, enviar notificaciones, procesar datos de rendimiento y muchas otras tareas, existe una gran variedad de complementos que proporcionan funciones adicionales que están fuera del alcance del propio Nagios Core, incluidas interfaces de configuración , gráficos de rendimiento , autodescubrimiento y monitoreo distribuido , entre otros. Estas características se implementan en diferentes proyectos de Nagios, que se desarrollan de forma independiente y se pueden encontrar en Nagios Exchang [20].

2.2.9.2 PNP4NAGIOS

PNP4Nagios es un complemento para Nagios que analiza los datos de rendimiento obtenidos por los plugins y los almacena automáticamente en bases de datos RDD (Round Robin Databases) [21], PNP4Nagios sirve para mostrar gráficos de estado para servicios que lo soportan [22].

2.2.9.3 ÁREAS MONITOREADAS POR NAGIOS

Son extensas las ares monitoreadas por nagios, pero es resaltable la supervisión de red de Windows y una supervisión completa de los sistemas operativos de escritorio y servidor de Microsoft Windows, incluidas las métricas del sistema, los estados de servicio, los estados de proceso, los contadores de rendimiento, los registros de eventos, las aplicaciones (IIS, Exchange, etc.), los servicios (Active Directory, DHCP , etc.) y más [23]. La implementación de herramientas eficaces de monitoreo de Linux con Nagios ofrece mayor disponibilidad de servidores, servicios y aplicaciones, detección rápida de cortes de red y fallas de protocolo [24].

Nagios es reconocido como la mejor solución para monitorear servidores en una variedad de formas diferentes. La supervisión del servidor se facilita debido a la flexibilidad para supervisar sus servidores con y sin agentes. Con más de 3500 complementos diferentes disponibles para monitorear. Nagios es totalmente capaz de monitorear servidores Windows, servidores Linux, servidores Unix, Solaris, AIX, HP-UX y Mac OS / X y más. La implementación de una supervisión efectiva del servidor con Nagios permite deteccion rápida de interrupciones de red, de servidores, servicios, procesos y trabajos por lotes fallidos [25]. A demás proporciona una supervisión completa de las aplicaciones y el estado de las aplicaciones, incluidas las aplicaciones de Windows, las aplicaciones de Linux, las aplicaciones UNIX y las aplicaciones web [26].

Nagios permite un monitoreo completo de SNMP (Protocolo simple de administración de redes). SNMP es un método "sin agente" para monitorear dispositivos y servidores de red, y a menudo es preferible

a instalar agentes dedicados en las máquinas de destino. Miles de dispositivos de red y sistemas operativos diferentes de diferentes proveedores admiten SNMP para entregar información crítica sobre el estado y las métricas de uso, el estado del servicio y más. La implementación de un monitoreo SNMP efectivo con Nagios facilita el monitoreo sin agente mayor disponibilidad de servidores, servicios y aplicaciones. Detección rápida de cortes de red y fallas de protocolo [27].

El completo monitoreo y administración de registros de aplicaciones, archivos de registro, registros de eventos, registros de servicios y registros del sistema en servidores Windows, servidores Linux y servidores Unix. Nagios es capaz de monitorear registros del sistema, registros de aplicaciones, archivos de registro y datos de syslog, y alertarlo cuando se detecta un patrón de registro. Implementar un monitoreo de registro efectivo da seguridad incrementada, mayor conciencia de los problemas de infraestructura de red. Mayor disponibilidad de servidores, servicios y aplicaciones. Detección rápida de cortes de red y fallas de protocolo Detección rápida de procesos fallidos, servicios, trabajos cron y trabajos por lotes Auditoría de cumplimiento y cumplimiento normativo [28].

2.2.10 GRAFANA

Grafana es una herramienta para visualizar datos de series temporales, a partir de un grupo de datos recolectados se obtendrá un panorama gráfico de la situación de una empresa u organización [29], esta herramienta permite una mejor monitorización de información ya que trabaja con la recolección de logs, grafana es una herramienta hecha en software libre [29].

2.2.11 TELEGRAM

Telegram es una plataforma de mensajería y VOIP, la aplicación está enfocada en la mensajería instantánea, el envío de varios archivos y la comunicación en masa, este servicio ofrece funcionalidades enfocadas en realizar charlas entre usuarios, salvo excepciones, los mensajes son

almacenados, o archivados en caso de que se desee ocultarlos, en la nube con opción de reenvío, borrado temporizado, acciones de búsqueda, realizar llamadas y adjuntos varios. Desde 2014 se añaden los adjuntos de archivos de todo tipo, ya sean documentos, multimedia o animaciones gráficas, con un límite de subida de 2 GB cada uno. Además, para facilitar en compartir contenido colectivamente se emplean los canales de difusión para boletines y los grupos para discusiones, con ajustes de privacidad, públicos o privados, la posibilidad de compartir encuestas y la formación de chats de voz sin límite de oyentes. La lista de contactos y permisos son gestionados en sus respectivas secciones [30].

La información es cifrada mediante la tecnología MTProto en dos mecanismos; por defecto, las conversaciones, borradores, publicaciones de grupos y canales y la lista de contactos se cifran íntegra e independientemente vía servidor, el formato varía por el tipo de información, antes de sincronizar o respaldar en la nube personal; posteriormente, las claves son desgranadas y separadas por seguridad. Por otro lado, están las llamadas, el servicio de auto rellenado Passport y los chats secretos, exclusivos para conversaciones entre emisor y receptor, que aplican codificación local entre dispositivos clientes: extremo a extremo. La última función, promocionada por primera vez en el Criptoanálisis de 2014, recibió críticas de algunos criptógrafos y activistas y ha sido conocida por ser usada por el Estado Islámico como herramienta para comunicar sus acciones. Como respuesta, los desarrolladores realizaron actualizaciones en la tecnología para “proveer mayor privacidad y seguridad”, lema del servicio [31].

Adicionalmente, Telegram ofrece utilitarios para uso personal y colectivo. Entre ellos está el apartado “mensajes guardados”, donde se pueden almacenar conversaciones, apuntes personales y recordatorios. Para la automatización de tareas masivas se desarrollan bots, que realizan actividades y servicios extras como pagos, juegos, moderación de grupos o asignación de otras tareas bajo inteligencia artificial. Los bots se aplican también en el ámbito empresarial y social [32].

2.2.12 METODOLOGÍAS DE DESARROLLO DE SOFTWARE

En el desarrollo de software existen numerosas propuestas metodológicas que inciden en distintas dimensiones del proceso de desarrollo. Por una parte, tenemos aquellas propuestas más tradicionales que se centran especialmente en el control del proceso, estableciendo rigurosamente las actividades involucradas, los artefactos que se deben producir, y las herramientas y notaciones que se usarán. Otra aproximación es centrarse en otras dimensiones, como por ejemplo el factor humano o el producto software. Esta es la filosofía de las metodologías ágiles, las cuales dan mayor valor al individuo, a la colaboración con el cliente y al desarrollo incremental del software con iteraciones muy cortas. Este enfoque está mostrando su efectividad en proyectos con requisitos muy cambiantes y cuando se exige reducir drásticamente los tiempos de desarrollo, pero manteniendo una alta calidad. Las metodologías ágiles están revolucionando la manera de producir software, y a la vez generando un amplio debate entre sus seguidores y quienes por escepticismo o convencimiento no las ven como alternativa para las metodologías tradicionales. [11]

2.2.12.1 Ventajas del uso de una metodología

Son muchas las ventajas que puede aportar el uso de una metodología, a continuación, se van a exponer algunas de ellas, clasificadas desde distintos puntos de vista. [11]

Desde el punto de vista de gestión:

- ✓ Facilitar la tarea de planificación
- ✓ Facilitar la tarea del control y seguimiento de un proyecto
- ✓ Mejorar la relación coste/beneficio
- ✓ Optimizar el uso de recursos disponibles
- ✓ Facilitar la evaluación de resultados y cumplimiento de los objetivos
- ✓ Facilitar la comunicación efectiva entre usuarios y desarrolladores

Desde el punto de vista de los ingenieros del software:

- ✓ Ayudar a la comprensión del problema

- ✓ Optimizar el conjunto y cada una de las fases del proceso de desarrollo
- ✓ Facilitar el mantenimiento del producto final
- ✓ Permitir la reutilización de partes del producto

Desde el punto de vista del cliente o usuario:

- ✓ Garantía de un determinado nivel de calidad en el producto final
- ✓ Confianza en los plazos de tiempo fijados en la definición del proyecto
- ✓ Definir el ciclo de vida que más se adecue a las condiciones y características del desarrollo.

2.2.12.2 Metodologías tradicionales y ágiles

Según la filosofía de desarrollo se pueden clasificar las metodologías en dos grupos. Las metodologías tradicionales, que se basan en una fuerte planificación durante todo el desarrollo, y las metodologías ágiles, en las que el desarrollo de software es incremental, cooperativo, sencillo y adaptado [11].

2.2.12.3 Metodologías tradicionales

Las metodologías tradicionales son denominadas, a veces de forma peyorativa, como metodologías pesadas, centran su atención en llevar una documentación exhaustiva de todo el proyecto y en cumplir con un plan de proyecto, definido todo esto, en la fase inicial del desarrollo del proyecto. Otra de las características importantes dentro de este enfoque, son los altos costes al implementar un cambio y la falta de flexibilidad en proyectos donde el entorno es volátil. Las metodologías tradicionales (formales) se focalizan en la documentación, planificación y procesos (plantillas, técnicas de administración, revisiones, etc.) [11]

2.2.12.4 Metodologías ágiles

Este enfoque nace como respuesta a los problemas que puedan ocasionar las metodologías tradicionales y se basa en dos aspectos fundamentales, retrasar las decisiones y la planificación adaptativa. Basan su fundamento en la adaptabilidad de los procesos de desarrollo. Estas metodologías ponen de relevancia que la capacidad

de respuesta a un cambio es más importante que el seguimiento estricto de un plan. [10]

2.2.12.5 Comparativa entre metodologías ágiles y tradicionales

En la Ilustración 1, que se muestra a continuación, aparece una comparativa entre estos dos grupos de metodologías. [11]

Metodologías Ágiles	Metodologías Tradicionales
Basadas en heurísticas provenientes de prácticas de producción de código	Basadas en normas provenientes de estándares seguidos por el entorno de desarrollo
Preparado para cambios durante el proyecto	Cierta resistencia a cambios
Procesos menos controlados, con pocos principios	Procesos controlados con más políticas y normas
El cliente es parte del equipo	El cliente interactúa mediante reuniones con el equipo
Grupos pequeños trabajando en el mismo grupo	Equipos grandes mayormente distribuidos
Pocos Artefactos y roles	Mas artefactos y roles
Comunicación horizontal	Comunicación vertical

Ilustración 1 Diferencias entre Metodologías ágiles y Tradicionales

Fuente: Elaboración propia

3. DEFINICIÓN DE TÉRMINOS BÁSICOS

2.3.1 INCIDENTE

Una ocurrencia identificada en el estado de un sistema, servicio o red, indicando una posible violación de la seguridad de la información, política o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad. Puede considerarse a la falla de medidas de seguridad o una situación previamente desconocida que pueda ser relevante para la seguridad (Evento de seguridad según la Norma ISO 27035) [33].

2.3.2 MONITOREO

Monitoreo es un término no incluido en el diccionario de la Real Academia Española (RAE), su origen se encuentra en monitor, un aparato que toma imágenes de instalaciones filmadoras o sensores y que permite visualizar algo en una pantalla [34]. El monitor, por lo tanto, ayuda a controlar o supervisar una situación [34].

2.3.3 BIG DATA

Big Data es un término que describe el gran volumen de datos, tanto estructurados como no estructurados, que inundan los negocios cada día. Pero no es la cantidad de datos lo que es importante. Lo que importa con el Big Data es lo que las organizaciones hacen con los datos. Big Data se puede analizar para obtener ideas que conduzcan a mejores decisiones y movimientos de negocios estratégicos [35].

2.3.4 ÁREA CRÍTICA DE TI

Conjunto de activos tecnológicos indispensables, que interactúan entre sí para brindar servicios vitales a los habitantes de un país. Los activos pueden ser instalaciones físicas o virtuales, redes de datos, redes industriales, sistemas de información, bases de datos, sistemas de control industrial, procesos automatizados o cualquier otro componente tecnológico que permite la prestación o el monitoreo de un servicio esencial para el bienestar de la población [14].

2.3.5 SISTEMA DE SOPORTE

Es una herramienta enfocada al análisis de los datos de una organización, que permite agrupar a los problemas y niveles de forma estructurada, así como implementar reglas o procesos específicos, para una mejor toma de decisiones [36].

2.3.6 GESTIÓN DE INFRAESTRUCTURA DE TI

La gestión de infraestructura de TI es la coordinación de todos los recursos, los sistemas, las plataformas, el personal y los entornos de TI. Los entornos modernos y dinámicos necesitan un nuevo enfoque de gestión que pueda mejorar la velocidad, ayudarlo a expandirse y proporcionar estabilidad en todos sus entornos de TI empresarial [37].

El término Infraestructura de TI es definido en ITIL V3 como el conjunto de hardware, software, redes, instalaciones, etc. (incluyendo todo el equipo relacionado con la información tecnológica) usado para desarrollar, probar, entregar, monitorear, controlar y dar soporte a los servicios de TI. Las personas asociadas, procesos y documentación no son parte de la Infraestructura de TI [38].

A continuación, todos los elementos que la conforman:

2.3.6.1 Swiching

Un switch de red es el dispositivo que provee conectividad entre equipos de la red en una LAN (Local Area Network). Un switch contiene varios puertos que se conectan físicamente a otros dispositivos, incluidos otros switches, routers y servidores. Las redes más viejas usaban puentes, en los cuales cada dispositivo “veía” el tráfico de todos los demás en la red. Los switches permiten a dos de ellos comunicarse en esta sin tener que enviar el tráfico a los demás [38].

2.3.6.2 Routers

Los routers mueven paquetes de datos. Estos permiten a los dispositivos en diferentes LAN poder comunicarse al determinar el siguiente “salto” que dejará al paquete llegar a su destino. Si la dirección IP de una estación de trabajo fue configurado manualmente, el valor de la puerta de enlace ingresado era la dirección del router [38].

2.3.6.3 Firewalls

Los firewalls son dispositivos de seguridad en el borde de la red. Se puede pensar en ella como una especie de guardián. Unos conjuntos de reglas definen qué tipos de tráfico podrán pasar por ella y cuáles serán bloqueados. En sus versiones más simples, la configuración permite especificar un puerto o protocolo para el tráfico de un dispositivo a dispositivo o a un grupo de estos. La fuente es el dispositivo que la origina. El destino es la dirección de IP específica en el servidor interno. El puerto define el tipo de tráfico. El asunto con un firewall puede complicarse rápidamente. Existen muchos tipos de ellas y con distintas formas de manejar el tráfico [38].

2.3.6.4 Servidores

Un servidor de red es otra computadora más grande en términos de recursos. Este permite a los usuarios acceder y compartir información. Hay varios tipos: quizá el más conocido es el servidor de archivos, el cual provee a los usuarios con una ubicación centralizada para guardar archivos. Configurado correctamente, un servidor de archivos puede impedir el acceso a cualquier persona, el servidor de directorios también es muy común. Este provee una base de datos central con las cuentas de los usuarios que pueden ser usadas en distintas computadoras. Esto implica la existencia de una administración centralizada de cuentas que pueden disponer de los recursos del servidor, el servidor web es el último tipo. Estos utilizan el HTTP (Hyper Text Transfer Protocol) para dejar que los usuarios vean un archivo a través de un explorador, también hay servidores de aplicaciones, bases de datos, impresoras, etc [38].

2.3.6.5 Planta física

La planta física es el cableado de red en el edificio y el cuarto donde están los servidores. Este suele ser una parte descuidada por la Infraestructura de TI, ya que se permite su debilitamiento, lo que trae como consecuencia fallas en la red. El cableado suele ser de dos tipos: -CAT 5/6/7 y fibra óptica. Cada uno tiene otros tipos que dependen de la velocidad y distancia para conectar dispositivos [38].

2.3.6.6 Personal

Por estricta definición de ITIL, la gente no es considerada parte de la Infraestructura de TI. De cualquier manera, sin personal calificado para mantenerla se limitan enormemente las capacidades de la organización. En las más grandes, hay posiciones especiales para cada una de las áreas mencionadas en este artículo. En las pequeñas, el encargo de todo es el administrador de sistemas [38].

2.3.6.7 Data Center

El Data Center es el núcleo de la red. Se trata de la ubicación en la que están los servidores, el centro de la red [38], es una instalación, construcción o inmueble de gran tamaño donde se albergan y mantienen numerosos equipos electrónicos como servidores, ventiladores, conexiones y otros recursos necesarios que se utilizan para mantener una red o un sistema de computadoras, información, conexiones y datos de una o varias empresas [39].

2.3.6.8 Software de Infraestructura

Se pueden considerar también a los sistemas operativos de los servidores y servicios de directorio como parte de la Infraestructura de TI. Sin estos sistemas multiusuario, el hardware no puede llevar a cabo sus funciones [38].

CAPÍTULO III. MATERIALES Y MÉTODOS

La presente investigación se desarrolló en la oficina general de sistemas informáticos y plataformas virtuales de la Universidad Nacional de Cajamarca, junto con el apoyo de encargados, el desarrollo de la investigación se hizo de manera presencial y remota; para el control remoto se usó la herramienta TeamViewer, el monitoreo se efectuó mediante la herramienta Nagios, para la elaboración de dashboard se usó pnp4nagios y Grafana, finalmente para comunicar los mensajes de alerta se realizó mediante Telegram.

Por el tipo de la investigación de acuerdo al fin que se persigue, se realizó una investigación de tipo aplicativa sobre las variables "*Gestión de Infraestructura de TI"* y "*Sistema de Soporte a la seguridad de la Información"* ya que implica todos los conocimientos posibles, el método experimental se fundamenta en el método científico y se utiliza como procesos lógicos la inducción y la deducción, en otras palabras, se vio el efecto de la segunda variable sobre la primera.

Es importante mencionar que la investigación exploratoria se encargó de generar hipótesis que impulsen el desarrollo de un estudio más profundo del cual se obtuvo resultados y conclusiones, la investigación exploratoria tiene múltiples características que le dan ventaja sobre otros métodos [40]. Como al definir sus conceptos, prioriza los puntos de vista de las personas y está enfocada en el conocimiento que se tiene de un tema, por lo que el significado es único e innovador [40], al hacerse uso del diseño longitudinal, se tomó una muestra del objeto de investigación, la misma que fue evaluada en distintos momentos en el tiempo y por períodos [40].

Según lo establecido, se instaló y configuró Nagios core (**"***Sistema de soporte a la seguridad de la información"*) en la oficina general de sistemas informáticos y plataformas virtuales de la Universidad Nacional de Cajamarca, para monitorear las áreas determinadas, que se especifican a continuación, basándonos en el método experimental – longitudinal, se obtuvo indicadores claves, tomados en diferentes fechas, así se obtuvo datos en diferentes tiempos para hacer comparación de los cambios en la "*Gestión de Infraestructura de TI"*, fue una investigación exploratoria y pionera, ya que el tema del presente estudio no se

ha encontrado en investigaciones anteriores en repositorios de tesis de la Universidad Nacional de Cajamarca.

INFORMACIÓN DE LA EMPRESA

La Universidad Nacional de Cajamarca promueve el desarrollo humano, el bienestar universitario y el cuidado del medio ambiente; pero, nuestro indeclinable esfuerzo se dirige, en primera instancia, a brindar una educación de excelencia académica, que fomente en nuestros estudiantes un espíritu emprendedor y les permita competir con éxito en un mundo sin fronteras y que sea capaz de generar cambios y progreso en nuestro país [41].

La actividad universitaria se rige por el Plan de Desarrollo Institucional que viene priorizando e impulsando la modernización de la gestión universitaria con la incorporación de un currículo por competencias y por medio de la implementación de una red informática y de un proceso de autoevaluación que se orienta a consolidar nuestra participación en redes nacionales y extranjeras [41].

A través de sus 59 años de funcionamiento, la Institución se ha orientado a producir el capital humano que requiere el desarrollo regional y nacional y ha liderado y viene liderando la educación superior en el norte del país, garantizando a nuestros estudiantes una formación educativa y profesional que les permitirá ejercer sus respectivas profesiones con capacidad competitiva y moral [41].

Ubicación

Se encuentra Ubicada en Avenida Atahualpa 1050 (Km3), Cajamarca – Perú (Ilustración 3).

Ilustración 2 Ubicación de la Universidad Nacional de Cajamarca

Fuente: Google Maps

Misión

- Universidad dedicada a la formación integral de profesionales, gestores de conocimiento, a través de la investigación científica, tecnológica y humanística, comprometidos con los procesos sociales, económicos, ambientales y culturales con responsabilidad social [42].

Visión

- Universidad, acreditada e internacionalizada en la formación de profesionales íntegros de alta calidad. Realiza investigación científica y tecnológica interdisciplinar, orientada al desarrollo sostenible, con énfasis en tema socio-ambiental. Involucrada en los procesos de desarrollo social, regional y nacional [42].

Organización

La Universidad Nacional del Cajamarca cuenta con el siguiente Organigrama (Ilustración 4) estipulado por el ROF (Reglamento de Organización y Funciones).

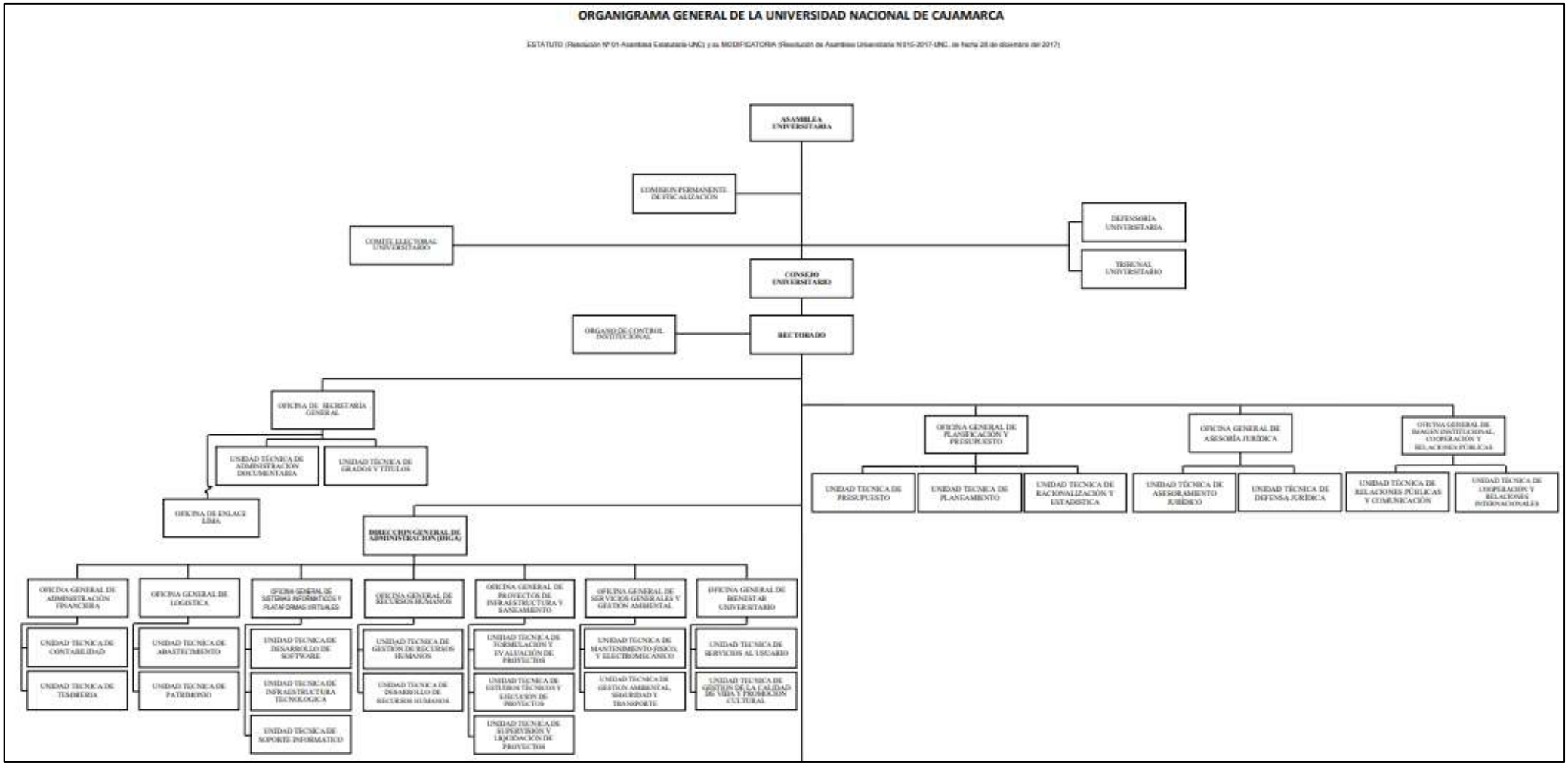


Ilustración 3 Organigrama de UNC

Fuente: Reglamento de organización y funciones de la UNC

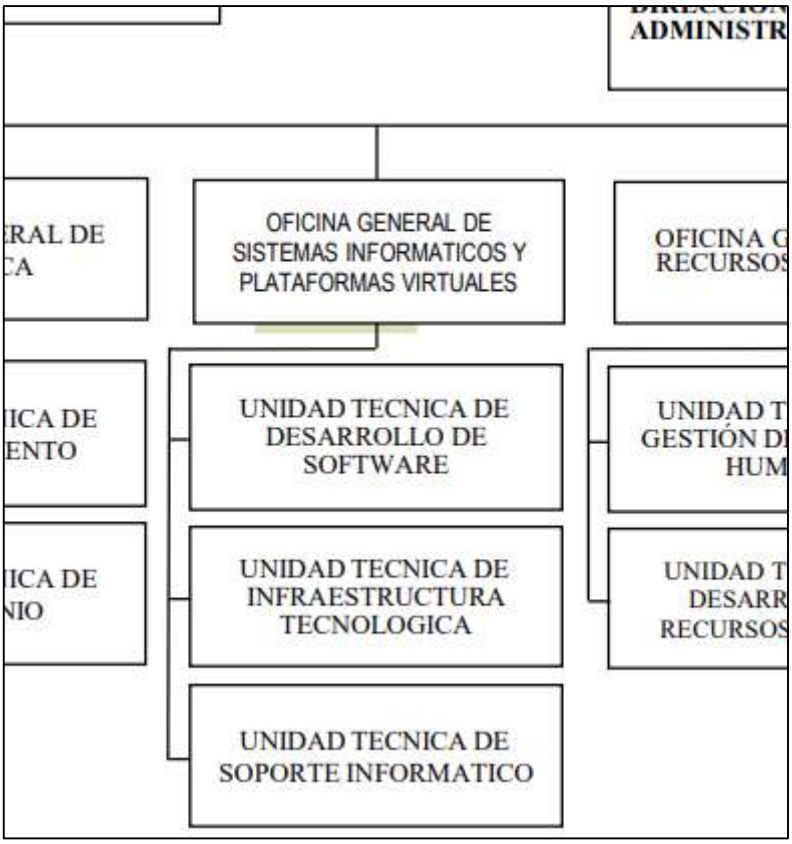


Ilustración 4 Organigrama - Oficina General de Sistemas Informáticos y Plataformas Virtuales

Fuente: Reglamento de organización y funciones de la UNC

3.1. PROCEDIMIENTO

Para el desarrollo de la investigación se usó la metodología Kanban, metodología ágil que permitió formar el grupo de trabajo y sus roles, también se identificó las prácticas en el área de TI, los procesos críticos y responsables; para el proceso y monitoreo personal se usó la herramienta VMware creando una máquina virtual donde se realizó la instalación y configuración de Nagios Core, finalmente se identificó y controlaron los incidentes determinados por el equipo. Se inició el proceso con las siguientes acciones:

- ✓ Se observó e identificó las prácticas correspondientes a seguridad y monitoreo en la oficina general de sistemas informáticos y plataformas virtuales de la Universidad Nacional de Cajamarca.
- ✓ Se logró definir los procesos críticos y responsables en la oficina general de sistemas informáticos y plataformas virtuales de la Universidad Nacional de Cajamarca

3.1.2. GRUPO DE TRABAJO

Tomando en cuenta la muestra, los responsables del proyecto y las prácticas de la oficina, se asignó el grupo de trabajo según lo mencionado (tabla 1).

Tabla 1 Grupo de Trabajo

Ing. Walter Pérez Estrada	• Jefe de la Oficina General de Sistemas Informáticos y Plataformas Virtuales de la Universidad Nacional de Cajamarca • Usuario Supervisor
Personal de la Oficina	• Oficina General de Sistemas Informáticos y Plataformas Virtuales de la Universidad Nacional de Cajamarca • Usuario
Ing. Edwin Valencia Castillo	• Director de la Escuela Academico Profesional de Ingenieria de Sistemas • Asesor de tesis
Edith Esther Cáceres Tafur	• Responsable del Proyecto

Fuente: Elaboración propia

Adicionalmente se asignó responsabilidades a cada participante del proyecto (tabla 2).

Tabla 2 Responsabilidades de Participantes

Usuario	• Define las funcionalidades requeridas del producto. • Identifica las funcionalidades con mayor importancia. • Hace uso de la herramienta. • Identifica Observaciones • Brinda opinión de la herramienta y recomendaciones
Usuario Supervisor	• Brinda opinión favorable de la herramienta. • Observaciones • Hace uso de la Herramienta • Brinda recomendaciones
Asesor de tesis	• Orienta en la investigación y brinda aternativas de desarrollo. • Verifica el correcto analisis, ejecucióny documentación de la investigación. • Supervisa la elaboración de la investigación
Responsable del proyecto	• Implemeta la herramienta Nagios y asegura su funcionamiento, de igual manera busca el entendimiento y presentacion amigable de la misma. • Realiza pruebas y monitorea la correcta comunicación de incidencias. • Documenta la Investigación. • Formula conclusiones y recomentadaciones según hipótesis y evaluación de satisfacción.

Fuente: Elaboración propia

3.1.3. VARIABLES Y ÁREAS CRÍTICAS DE TI – PRÁCTICAS IDENTIFICADAS

3.1.3.1. Buenas y malas prácticas identificadas

Según el cuestionario realizado (Anexo 1), se logró identificar las siguientes prácticas descritas en la tabla 3:

Tabla 3 Tabla "Buenas y malas Prácticas"

Prácticas identificadas en la Oficina	
Buenas Prácticas	Malas prácticas
• Se realizaba monitoreo de equipos para identificar incidentes en equipos DELL . • Las incidencias se comunicaba de forma personal, entre el usuario con el personal del área.	• El monitoreo en equipos "DELL" se daba una sola vez al día y de forma manual • La información de incidentes podía ser comunicada por algún 3° involucrado. • Las incidencias usualmente se reportaban por la constante incomodidad del usuario. • Las incidencias no eran absueltas en el tiempo acorde. • No se encontró un registro de reporte de incidentes donde llevar un historial. • No existe un protocolo de solución de incidentes. • No se aseguraba la Integridad de la información en cada reporte de incidente.

Fuente: Elaboración propia

3.1.3.2. Problema y variables

De la misma forma los problemas que planteó la investigación se define de la siguiente forma:

Tabla 4 Definición del Problemas

Problema	No se cuenta con un sistema de soporte a la seguridad de la información usando big data que mejore la gestión de infraestructura de tecnologías de información en la Universidad Nacional de Cajamarca
Grupo Afectado	Usuarios de equipos del área de TI de la UNC

Variable dependiente	**Gestión de Infraestructura de TI** Indicadores: Cantidad de incidentes identificados Incidentes o ataques controlados
Variable Independiente	**Sistema de Soporte a la seguridad de la información** Indicador: nivel de satisfacción en el usuario

Fuente: Elaboración propia

3.1.3.3. Áreas a evaluar

Según el análisis realizado por los involucrados, se determinaron las siguientes áreas a evaluar (tabla 5):

Tabla 5 Áreas evaluadas

ÁREA	Aspectos a monitorear	IP
Base de Datos	Base de datos	10.1.2.16
Redes	Se monitoreará dos switch	10.1.2.102 10.1.2.110
Sistemas operativos	El mismo Servidor al cual se dio acceso	Linux 10.1.3.16
Monitoreo de Aplicaciones	Una aplicación determinada en el Servidor	admision.unc
Servidores	Un servidor especifico	Localhost

Fuente: Elaboración propia

3.1.4. TABLERO DE TRABAJO

La presente investigación se desarrolló bajo la metodología Kanban, con la cual se definió los ítems a distribuirse en diferentes fases del tablero, complementariamente se usó la herramienta Jira Software, la cual cuenta con una plantilla de trabajo según esta metodología, se realizó dicho proceso, el desarrollo de la investigación se dividió en las fases (Ilustración 5): “Backlog”, haciendo referencia a los ítems pendientes de trabajar, “Next”, ítems priorizados para su ejecución, “Doing” ítems que están siendo

trabajados en ese momento y finalmente “Completados” los cuales ya han sido finalizados según lo propuesto en la primera fase.

Ilustración 5 División del tablero de trabajo según metodología Kanban (4 fases)

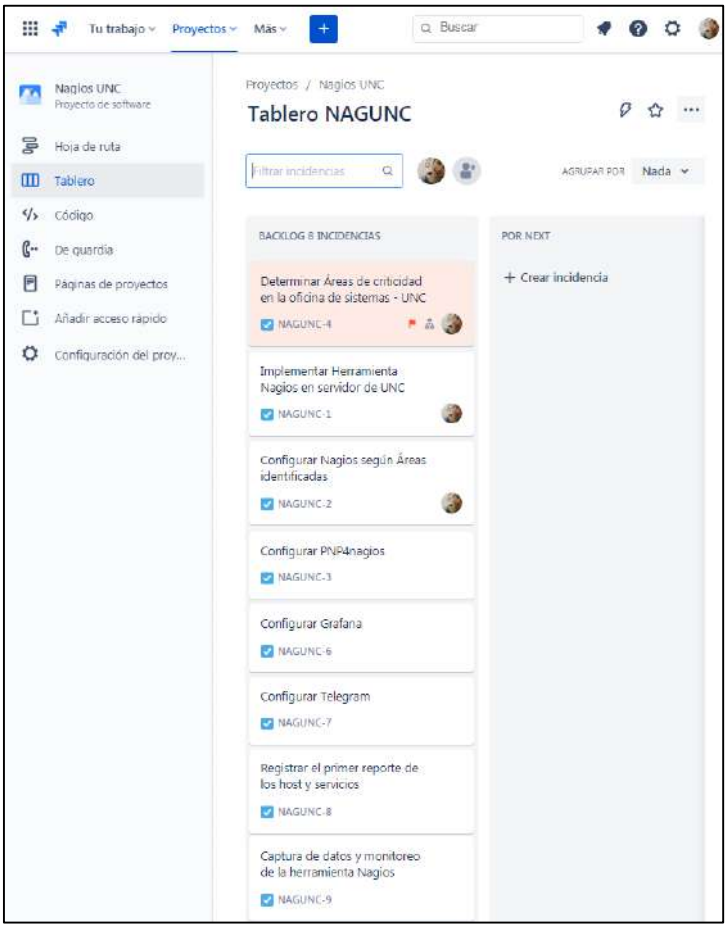


Ilustración 6 Estado inicial de Backlog (definir ítems)

Se priorizó la implementación de la Herramienta nagios en el servidor de la UNC, como se puede observar en la siguiente imagen, los ítems NAGUNC-1y NAGUNC-4 se ubican en la fase “COMPLETADOS” del tablero de trabajo, es decir, se estas tares estuvieron ubicadas anteriormente en la fase next y doing.

Ilustración 7 Proceso de desarrollo de ítems en fases

Jira software, permitió que se añada incidencias secundarias y se asigne responsables e informadores de las tareas a realizar (Ilustración 6), en esta investigación fue la misma persona, cada tarea fue titulada y detallada, permitiendo tener un trabajo mucho más ordenado, dentro del proceso de tesis el más complejo fue estabilizar la herramienta y el monitoreo a las diferentes áreas.

Ilustración 8 Tarea finalizada con incidencia secundaria

Una vez finalizado cada ítem, se adjuntó una imagen como evidencia o entregable de la culminación del proceso realizado.

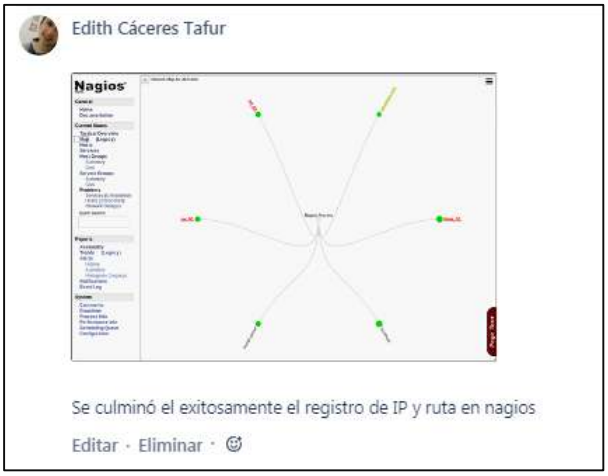


Ilustración 9 Evidencia de culminar el ítem propuesto

De la forma se desarrollaron las tareas siguientes y se adjuntó entregables (evidencia) de culminar lo propuesto.

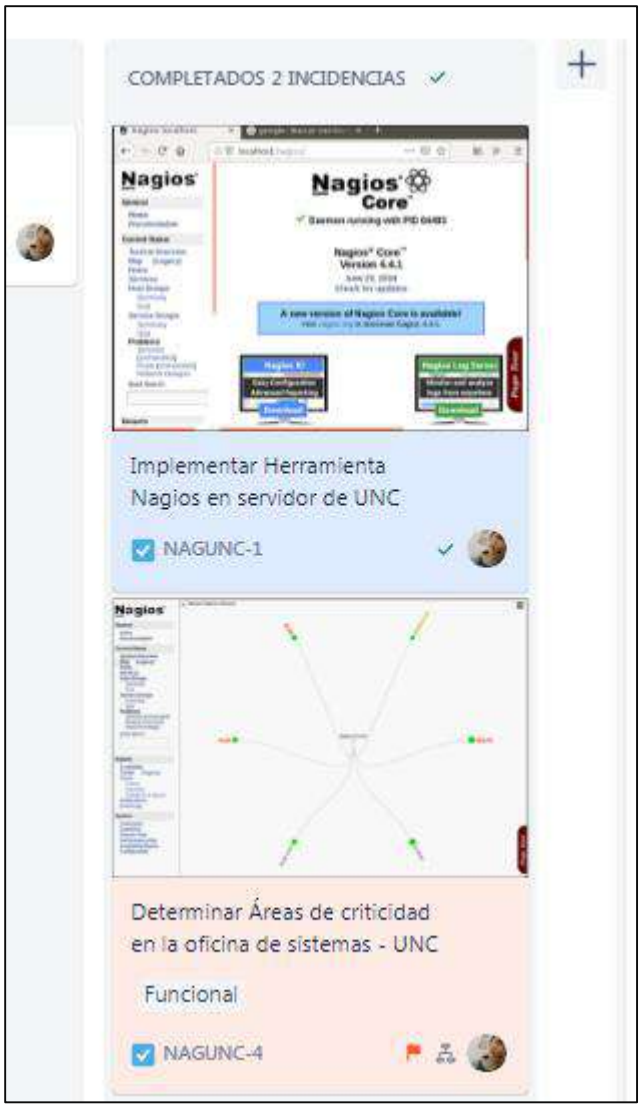


Ilustración 10 Fase "Completado" con entregables adjuntos

3.1.5. VIABILIDAD ECONÓMICA DE LA INVESTIGACIÓN

La presente investigación, fue realizada básicamente con herramientas open source, las cuales se detallan en la siguiente tabla, es importante mencionar este proceso, ya que muchas entidades de bajos recursos pueden usar este método para iniciar un monitoreo de forma correcta y a la vanguardia de la tecnología; de igual forma las grandes empresas pueden hacer uso de las herramientas open source buscando ahorrar increíbles montos en compras de licencias y asegurando la seguridad de información de la empresa.

Tabla 6 Viabilidad económica del proyecto

Herramienta	Descripción	Costo
Nagios Core	Licenciada bajo los términos de software libre GPL, permite el monitoreo de diferentes host.	s/.0 soles
Grafana	Software libre basado en licencia de Apache 2.0, que permite la visualización y el formato de datos métricos	s/.0 soles
Telegram	Plataforma de mensajería y VOIP, aplicación de código abierto.	s/.0 soles
Jira Software	Software para la gestión de proyectos, administración de tareas y seguimiento de errores.	s/.0 soles

Así también, se puede escoger versiones pagadas de las herramientas anteriormente mencionadas, las cuales pueden mejorar ciertas funciones. Es importante mencionar que para un mejor entendimiento se pueden llevar o adquirir cursos en plataformas como Udemy o Platzi de forma cómoda.

4.1.2. INSTALACIÓN Y CONFIGURACIÓN DE NAGIOS CORE 4.41

Para la instalación de Nagios Core versión 4.4.1, se creó una máquina virtual Ubuntu en su versión 16.04, ambas usadas fueron software libre, luego de la verificación de conectividad a la red e internet, se continuó con la configuración de nagios, cuyo modelo de trabajo (ilustración 12), se basa en active y passive check, es decir nagios tiene lanza alertas generadas automáticamente (active check) y generadas de manera manual (passive check) a cada una de las áreas programadas y brinda un status casi de forma inmediata.

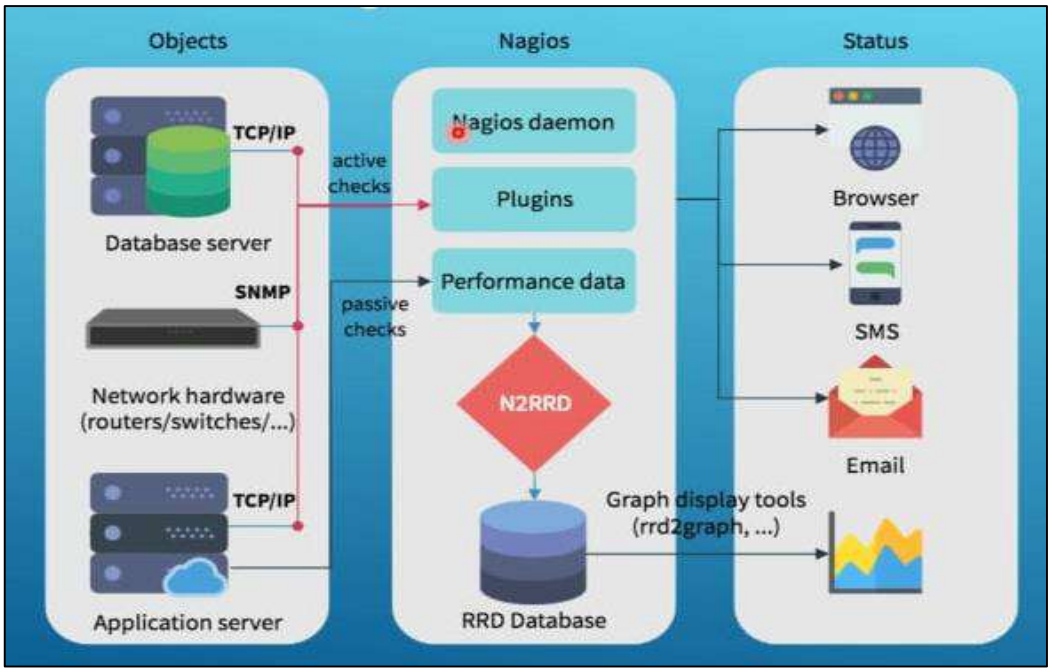


Ilustración 11 Modelo de trabajo de Nagios Core 4

La investigación usó el siguiente código para la instalación de Nagios, a continuación, se detalla y adjunta evidencia en el anexo 6 (ilustración 126 a 159).

```
sudo apt-get update
sudo apt-get upgrade
```

Se instaló las dependencias y servicios que Nagios requirió

```
sudo apt-get install wget build-essential apache2 php apache2-
mod-php7.2 php-gd libgd-dev unzip sendmail [43].
```

Se editó el fichero hosts para añadir el nombre de servidor que se utilizó a la hora de enviar correos de notificación

```
sudo vi /etc/hosts
```

Se descargó el instalador de Nagios Core y sus plugins

```
cd /tmp
sudo wget https://assets.nagios.com/downloads/nagioscore/relea
ses/nagios-4.4.1.tar.gz
sudo wget https://nagios-plugins.org/download/nagios-plugins-
2.2.1.tar.gz [44]
```

Se procedió a descomprimir los ficheros descargados

```
sudo tar zxvf nagios-4.4.1.tar.gz
```

```
sudo tar zxvf  nagios-plugins-2.2.1.tar.gz
sudo cp /etc/apache2/nagios.conf /etc/
```

Se crearon los usuarios y permisos necesarios para Nagios.

```
sudo useradd nagios
```

Adicionalmente se creó el grupo “nagcmd”

```
sudo groupadd nagcmd
```

Se agregó el usuario “nagios” al grupo “nagcmd”

```
sudo usermod -a -G nagcmd nagios
```

Se agregó el usuario “nagios” y el grupo “nagcmd” al grupo www-data utilizado por apache2

```
sudo usermod -a -G nagios,nagcmd www-data
```

Se creó el fichero de configuración

```
cd /tmp/
cd nagios-4.4.1/
sudo ./configure --with-command-group=nagcmd --with-
mail=/usr/sbin/sendmail --with-httpd-conf=/etc/apache2
```

Para la correcta instalación se ejecutó las siguientes líneas de comando

```
sudo make all
sudo make install
sudo make install-init
sudo make install-config
sudo make install-commandmode
sudo make install-webconf
sudo cp -R contrib/eventhandlers/ /usr/local/nagios/libexec/
sudo chown -R nagios:nagios /usr/local/nagios/libexec/
eventhandlers [45]
```

Se comprobó los ficheros de configuración de Nagios y se inició el servicio

```
/usr/local/nagios/bin/nagios-v/usr/local/nagios/etc/nagios.cfg
sudo service nagios start
```

Se realizó la activación del site en apache:

```
/etc/apache2/sites-available apache2/sites-available/nagios.conf
```

Se creó el vínculo permanente en sites-enabled

```
sudo ln –s /etc/apache2/sites-available/nagios.conf
/etc/apache2/sites-enabled/nagios.conf
```

Se reinició el servicio apache2

```
sudo service apache2 restart
```

Se activó el site

```
sudo a2ensite nagios
sudo a2enmod rewrite cgi
```

Nuevamente se reinició apache2

```
sudo service apache2 restart
```

Se creó del password para el usuario nagiosadmin que se utilizó en el portal Nagios

```
htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

Se instalaron los plugins ejecutando cada línea individualmente

```
cd /tmp/nagios-plugins-2.2.1
sudo ./configure --with-nagios-user=nagios --with-nagios-
group=nagios
sudo make all
sudo make install
```

Se configuró el servicio nagios para que arranque automáticamente.

```
sudo systemctl enable nagios
```

Finalmente se validó mediante la dirección

"http://ip_configurado/nagios", ver nuestra instalación de Nagios Core.

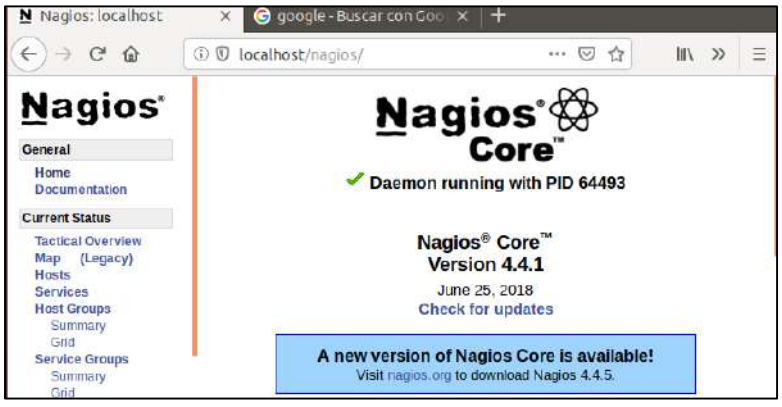


Ilustración 12 Inicialización de Nagios Core

4.1.3. INTERFAZ DE LA HERRAMIENTA

A continuación se muestran imágenes de las diferentes interfaces de Nagios en esta investigación, se puede observar cómo se dividió en áreas (host) y al mismo tiempo cada área se sub dividió en servicios, de los cuales se identificó los estados respectivos, Nagios permitió observar en diferentes formas lo monitoreado, se pudo observar de forma general y detallada el área, los tiempos de monitoreo, los logs, el tiempo de revisión, los problemas latentes, información de procesos realizados, información detallada del estado, rendimiento de la herramienta, configuración y reportes, en el pie de imagen se detalla lo que mostró la herramienta (desde ilustración 14 a 41).

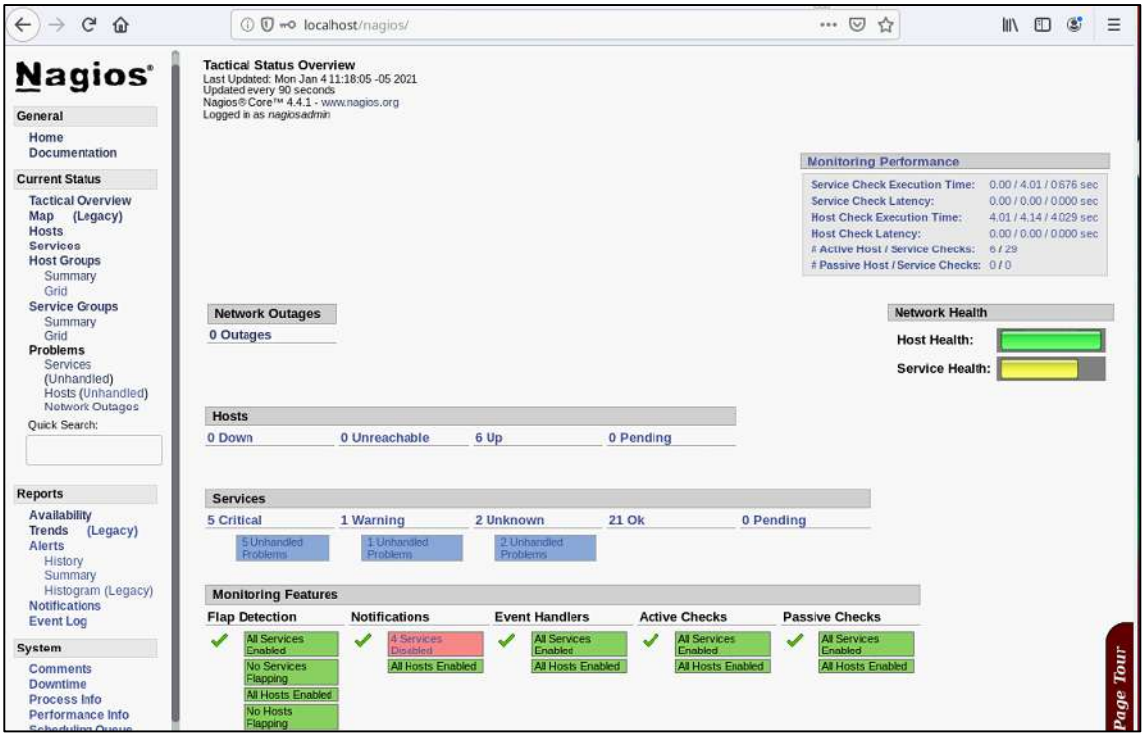


Ilustración 13 Vista "Descripción Táctica" - Máquina UNC

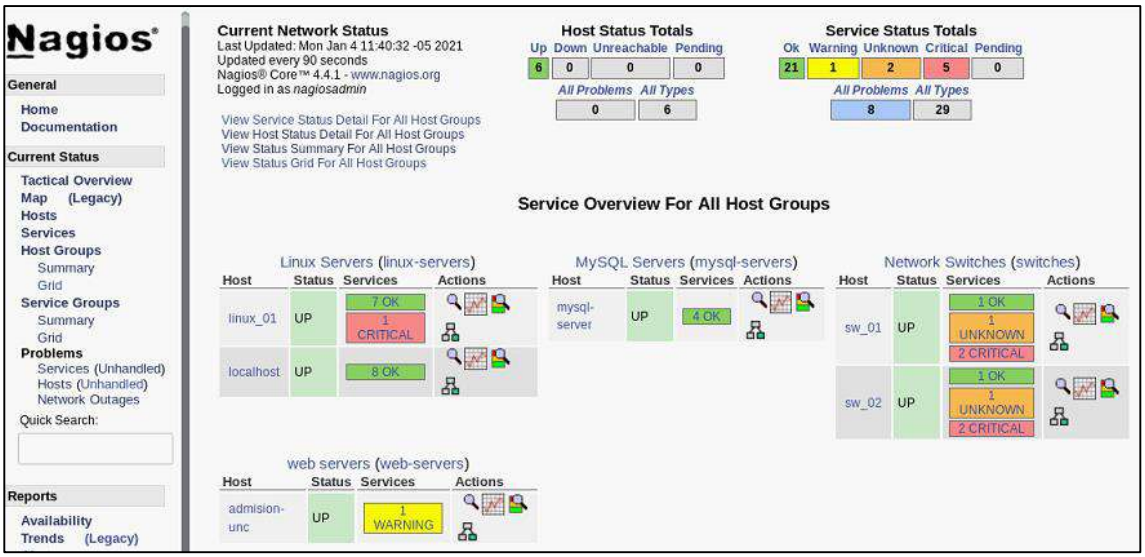


Ilustración 140 Vista "descripción general del servicio para todo el grupo de host" - Máquina UNC

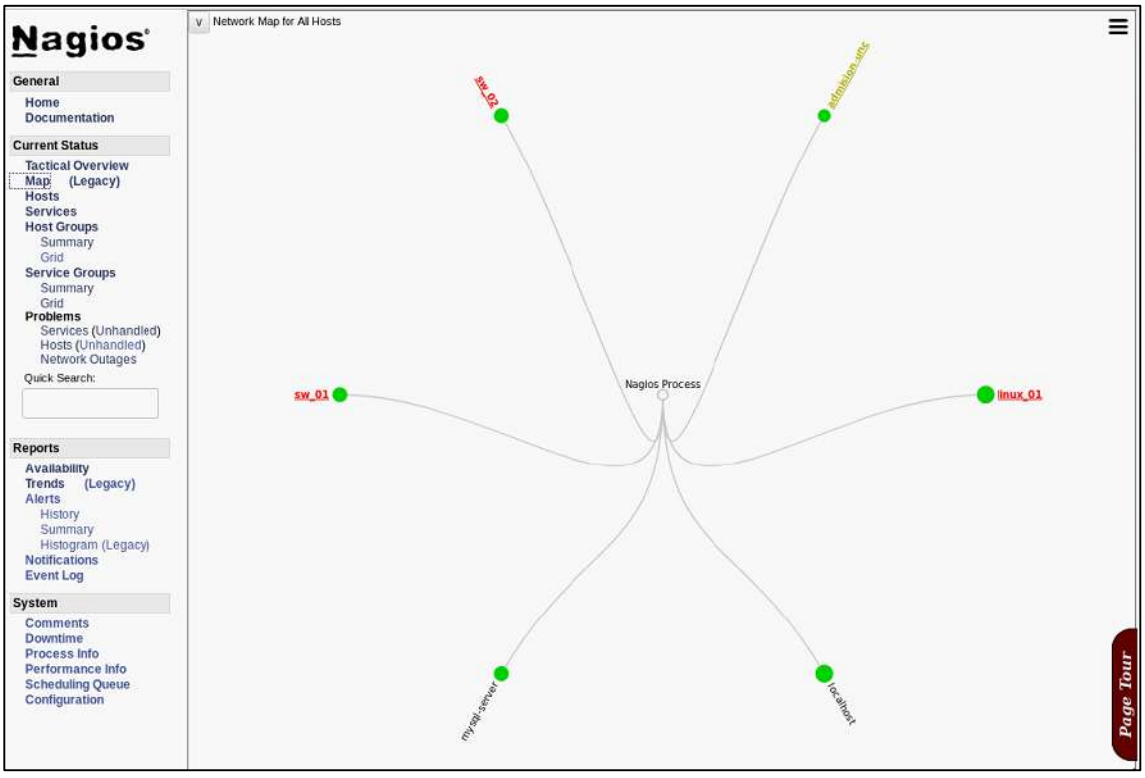


Ilustración 151 Vista "Mapa"- Máquina UNC

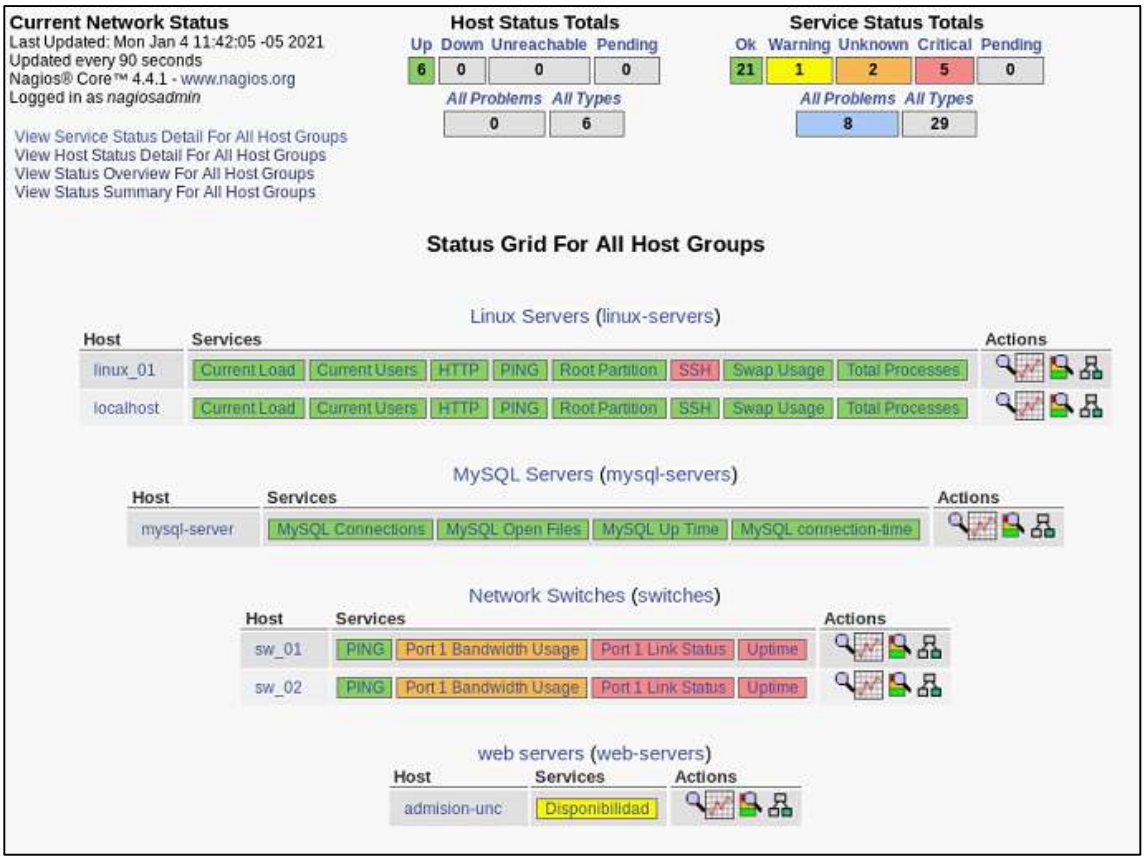


Ilustración 16 Vista "Cuadro de Estado" - Máquina UNC

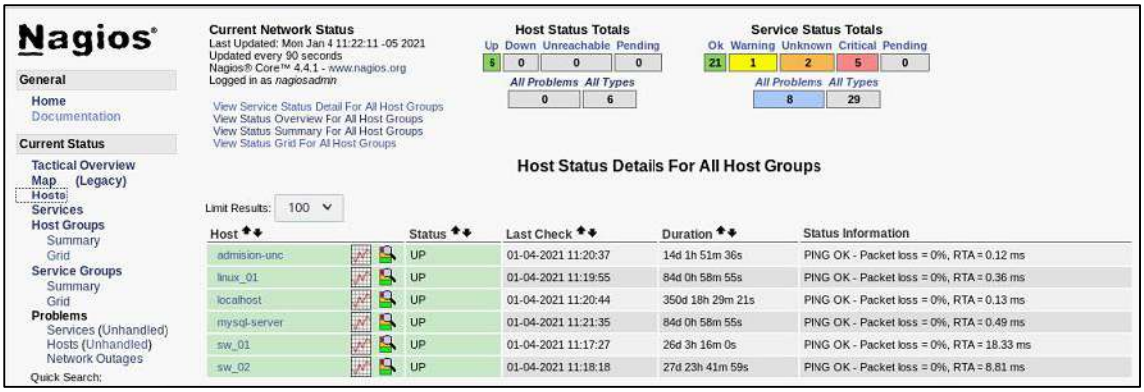


Ilustración 17 Vista "Detalle de cada Estado" - Máquina UNC

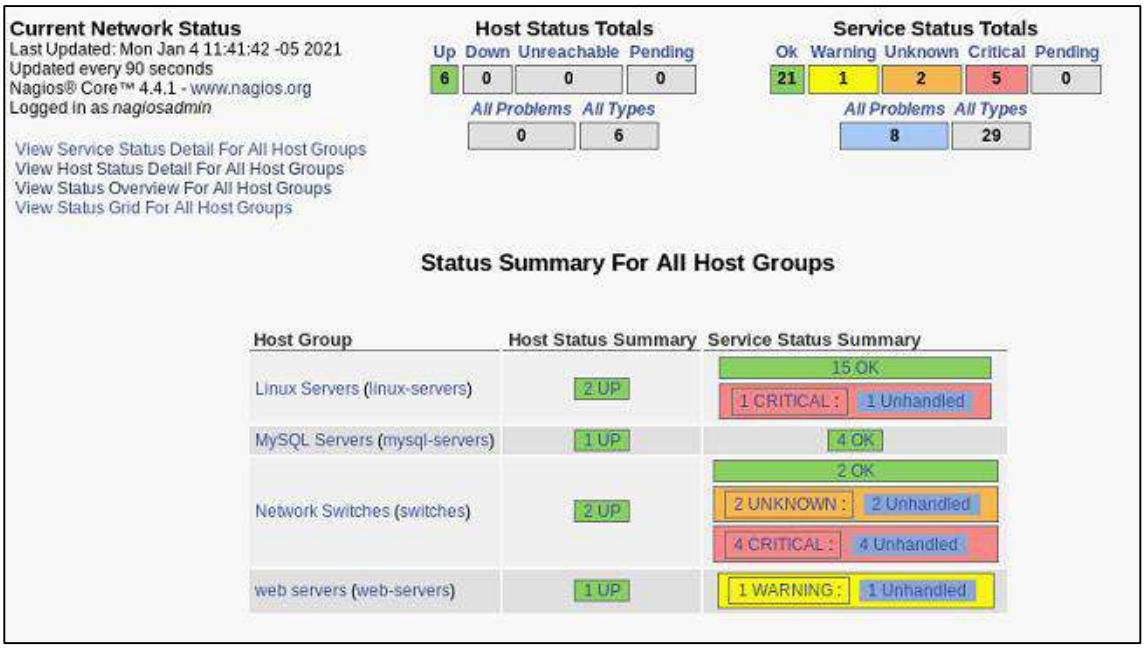


Ilustración 18 Vista "Resumen de Estado" - Máquina UNC

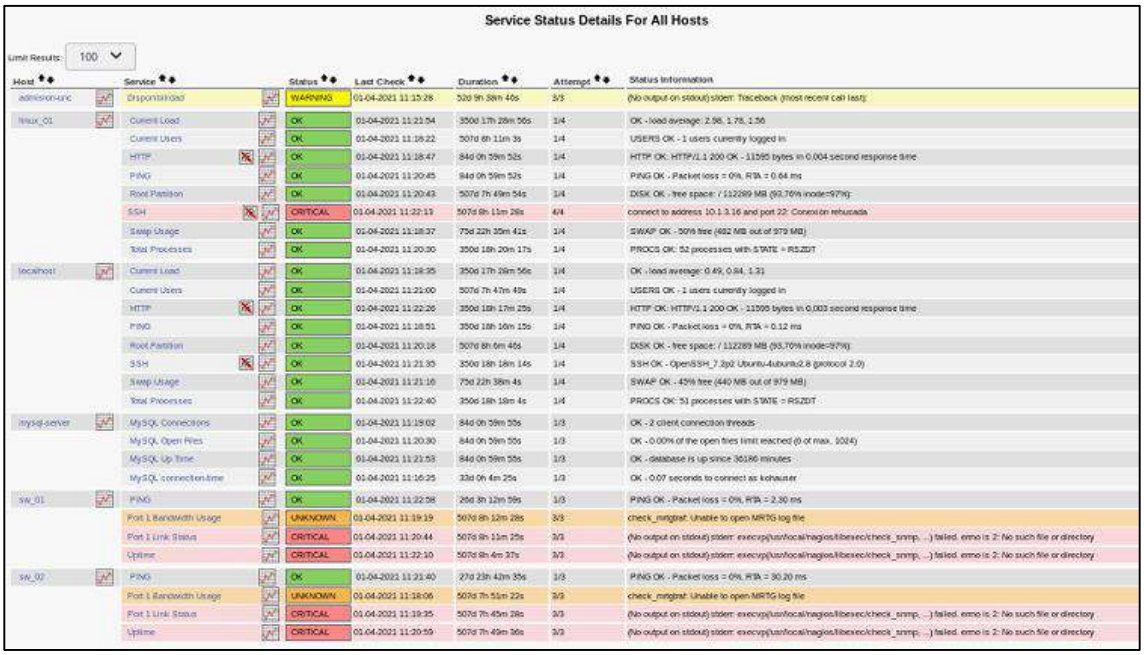


Ilustración 19 Vista "Estados General" - Máquina UNC

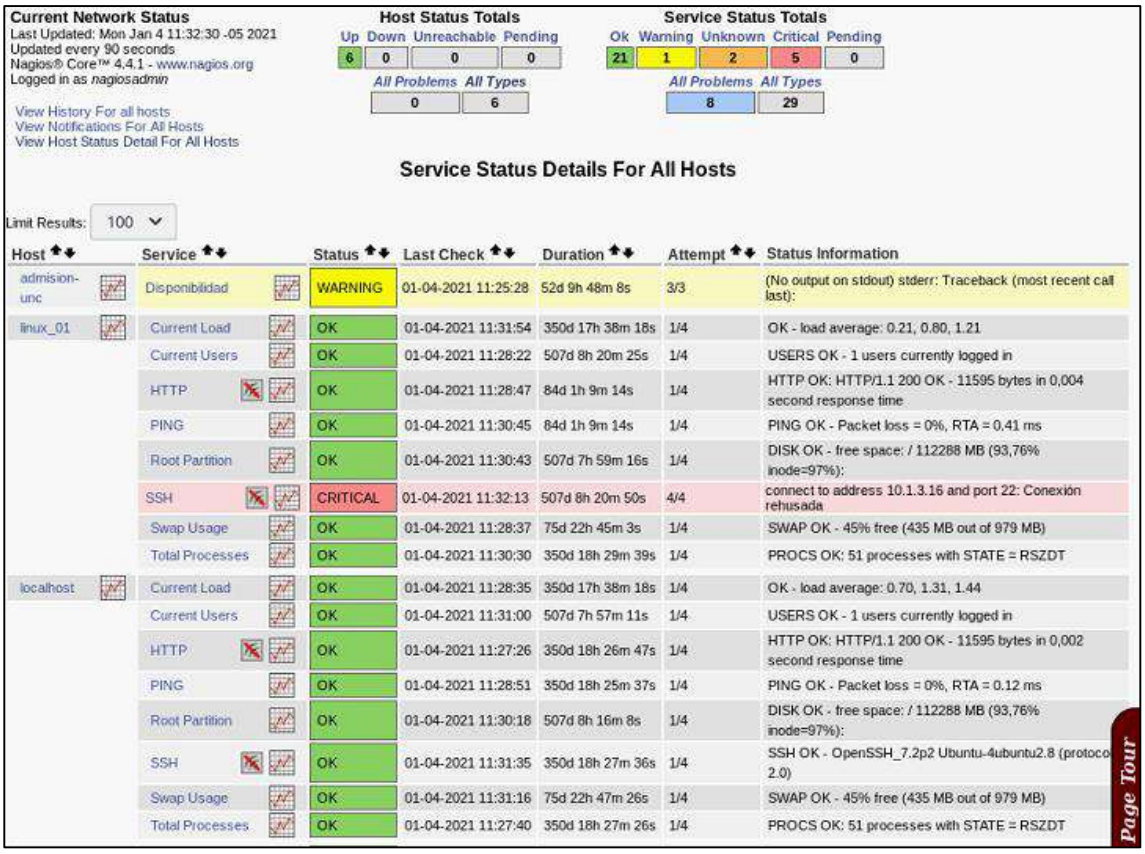


Ilustración 20 Vista "Estado General 1" - Máquina UNC

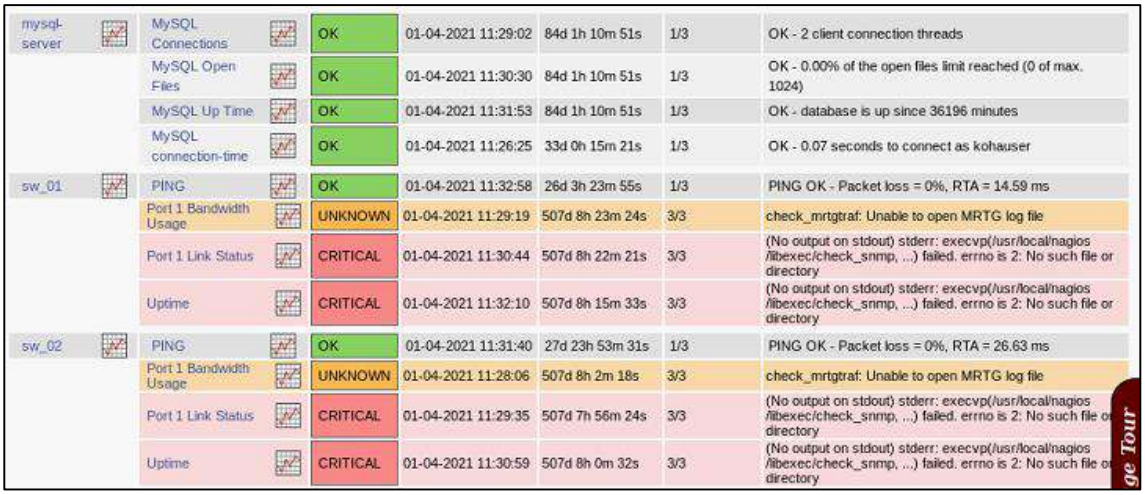


Ilustración 21 Vista "Estado General 2" - Máquina UNC

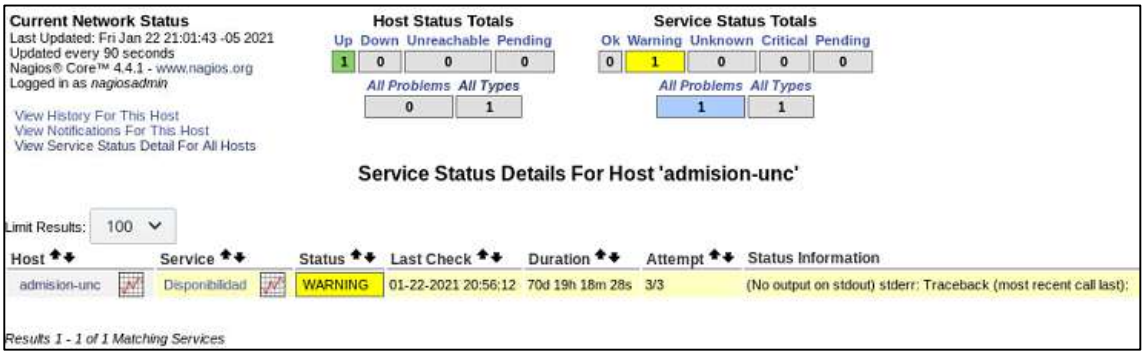
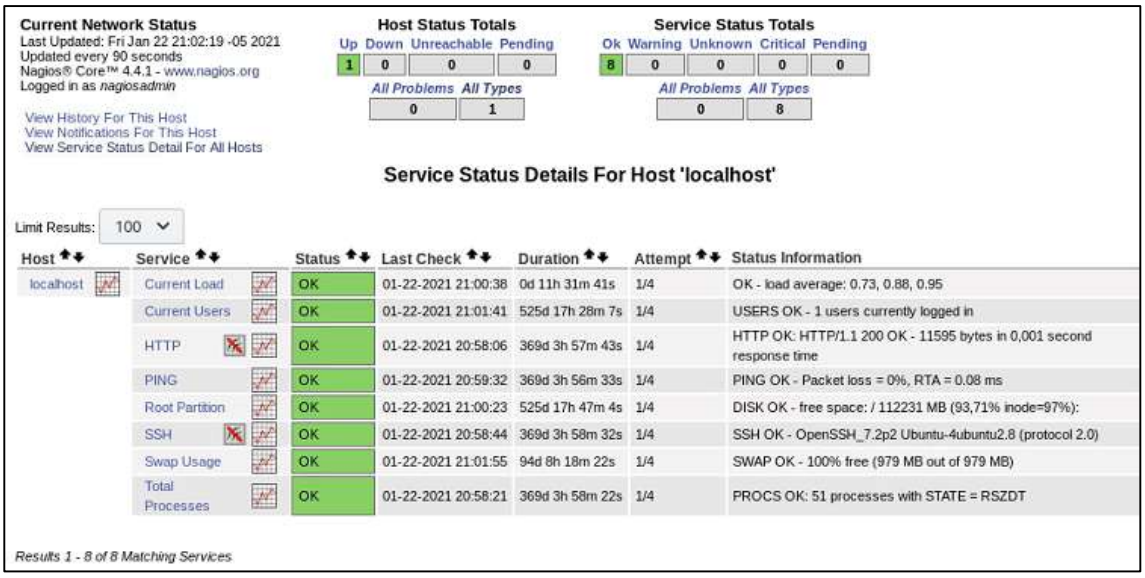


Ilustración 22 Vista "Estado admisión -unc " -Máquina UNC



Current Network Status
Last Updated: Fri Jan 22 21:02:19 -05 2021
Updated every 90 seconds
Nagios® Core™ 4.4.1 - www.nagios.org
Logged in as *nagiosadmin*

View History For This Host
View Notifications For This Host
View Service Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
1	0	0	0

All Problems	All Types
0	1

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
8	0	0	0	0

All Problems	All Types
0	8

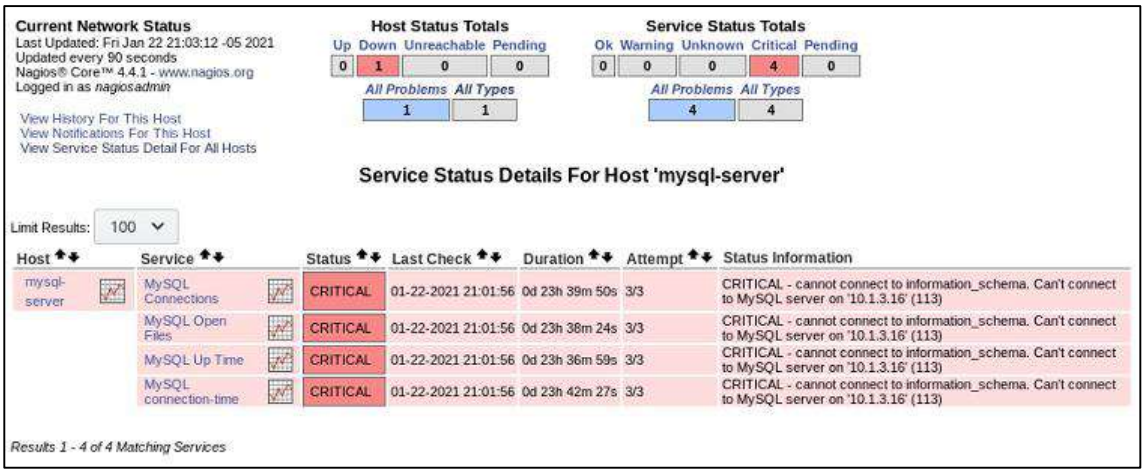
Service Status Details For Host 'localhost'

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Load	OK	01-22-2021 21:00:38	0d 11h 31m 41s	1/4	OK - load average: 0.73, 0.88, 0.95
	Current Users	OK	01-22-2021 21:01:41	525d 17h 28m 7s	1/4	USERS OK - 1 users currently logged in
	HTTP	OK	01-22-2021 20:58:06	369d 3h 57m 43s	1/4	HTTP OK: HTTP/1.1 200 OK - 11595 bytes in 0,001 second response time
	PING	OK	01-22-2021 20:59:32	369d 3h 56m 33s	1/4	PING OK - Packet loss = 0%, RTA = 0.08 ms
	Root Partition	OK	01-22-2021 21:00:23	525d 17h 47m 4s	1/4	DISK OK - free space: / 112231 MB (93,71% inode=97%):
	SSH	OK	01-22-2021 20:58:44	369d 3h 58m 32s	1/4	SSH OK - OpenSSH_7.2p2 Ubuntu-4ubuntu2.8 (protocol 2.0)
	Swap Usage	OK	01-22-2021 21:01:55	94d 8h 18m 22s	1/4	SWAP OK - 100% free (979 MB out of 979 MB)
	Total Processes	OK	01-22-2021 20:58:21	369d 3h 58m 22s	1/4	PROCS OK: 51 processes with STATE = RSZDT

Results 1 - 8 of 8 Matching Services

Ilustración 23 Vista "Estado localhost" - Máquina UNC



Current Network Status
Last Updated: Fri Jan 22 21:03:12 -05 2021
Updated every 90 seconds
Nagios® Core™ 4.4.1 - www.nagios.org
Logged in as *nagiosadmin*

View History For This Host
View Notifications For This Host
View Service Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
0	1	0	0

All Problems	All Types
1	1

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
0	0	0	4	0

All Problems	All Types
4	4

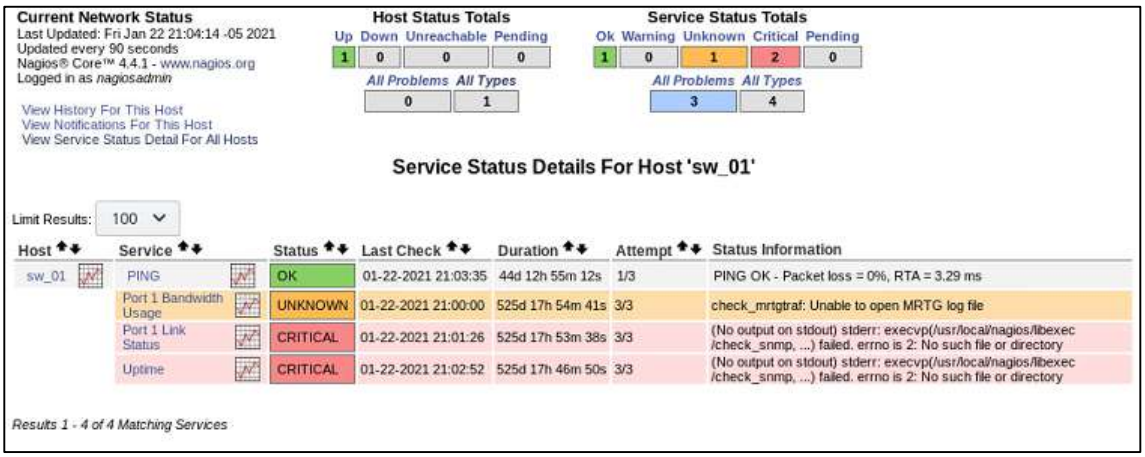
Service Status Details For Host 'mysql-server'

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
mysql-server	MySQL Connections	CRITICAL	01-22-2021 21:01:56	0d 23h 39m 50s	3/3	CRITICAL - cannot connect to information_schema. Can't connect to MySQL server on '10.1.3.16' (113)
	MySQL Open Files	CRITICAL	01-22-2021 21:01:56	0d 23h 38m 24s	3/3	CRITICAL - cannot connect to information_schema. Can't connect to MySQL server on '10.1.3.16' (113)
	MySQL Up Time	CRITICAL	01-22-2021 21:01:56	0d 23h 36m 59s	3/3	CRITICAL - cannot connect to information_schema. Can't connect to MySQL server on '10.1.3.16' (113)
	MySQL connection-time	CRITICAL	01-22-2021 21:01:56	0d 23h 42m 27s	3/3	CRITICAL - cannot connect to information_schema. Can't connect to MySQL server on '10.1.3.16' (113)

Results 1 - 4 of 4 Matching Services

Ilustración 24 Vista "Estado mysql-server" - Maquina UNC



Current Network Status
Last Updated: Fri Jan 22 21:04:14 -05 2021
Updated every 90 seconds
Nagios® Core™ 4.4.1 - www.nagios.org
Logged in as *nagiosadmin*

View History For This Host
View Notifications For This Host
View Service Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
1	0	0	0

All Problems	All Types
0	1

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
1	0	1	2	0

All Problems	All Types
3	4

Service Status Details For Host 'sw_01'

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
sw_01	PING	OK	01-22-2021 21:03:35	44d 12h 55m 12s	1/3	PING OK - Packet loss = 0%, RTA = 3.29 ms
	Port 1 Bandwidth Usage	UNKNOWN	01-22-2021 21:00:00	525d 17h 54m 41s	3/3	check_mrtgtraf: Unable to open MRTG log file
	Port 1 Link Status	CRITICAL	01-22-2021 21:01:26	525d 17h 53m 38s	3/3	(No output on stdout) stderr: execvp(/usr/local/nagios/libexec/check_snmp, ...) failed. errno is 2: No such file or directory
	Uptime	CRITICAL	01-22-2021 21:02:52	525d 17h 46m 50s	3/3	(No output on stdout) stderr: execvp(/usr/local/nagios/libexec/check_snmp, ...) failed. errno is 2: No such file or directory

Results 1 - 4 of 4 Matching Services

Ilustración 25 Vista "Estado Red - sw_01" -Máquina UNC

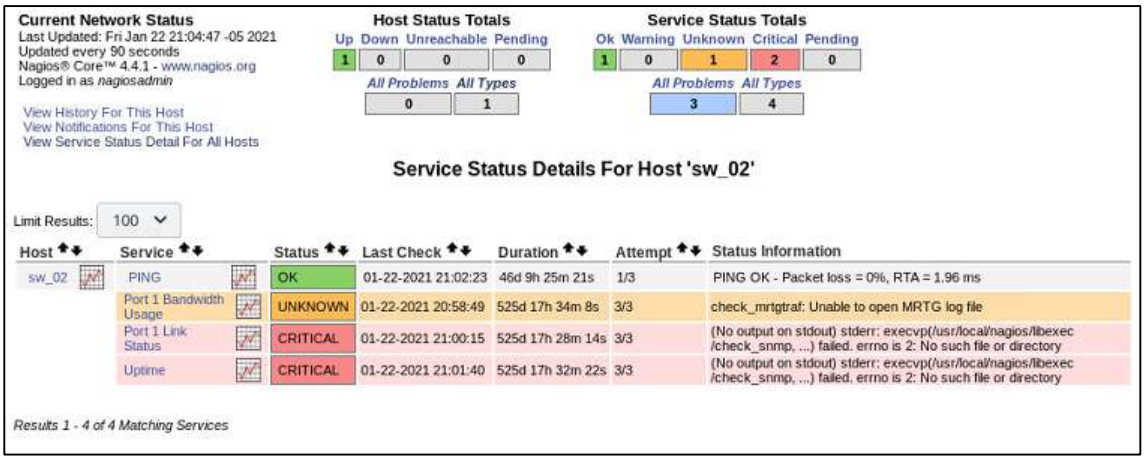


Ilustración 26 Vista "Estado Red - sw_02" - Máquina UNC

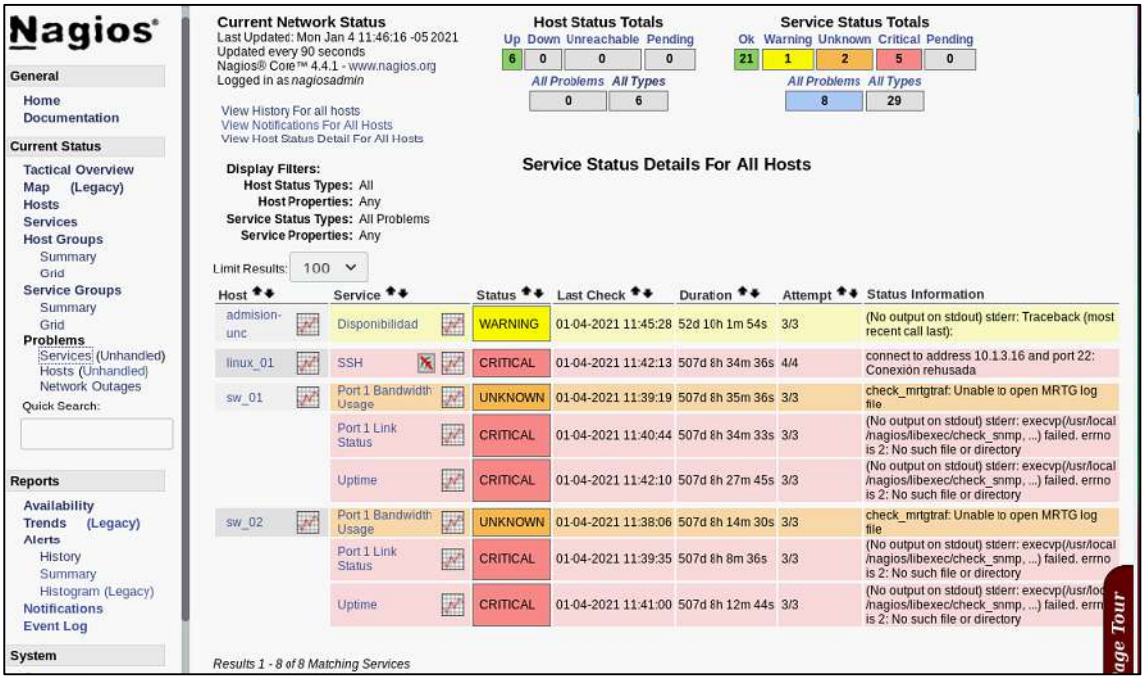


Ilustración 27 Vista "Detalle de Servicios - Problema" - Máquina UNC

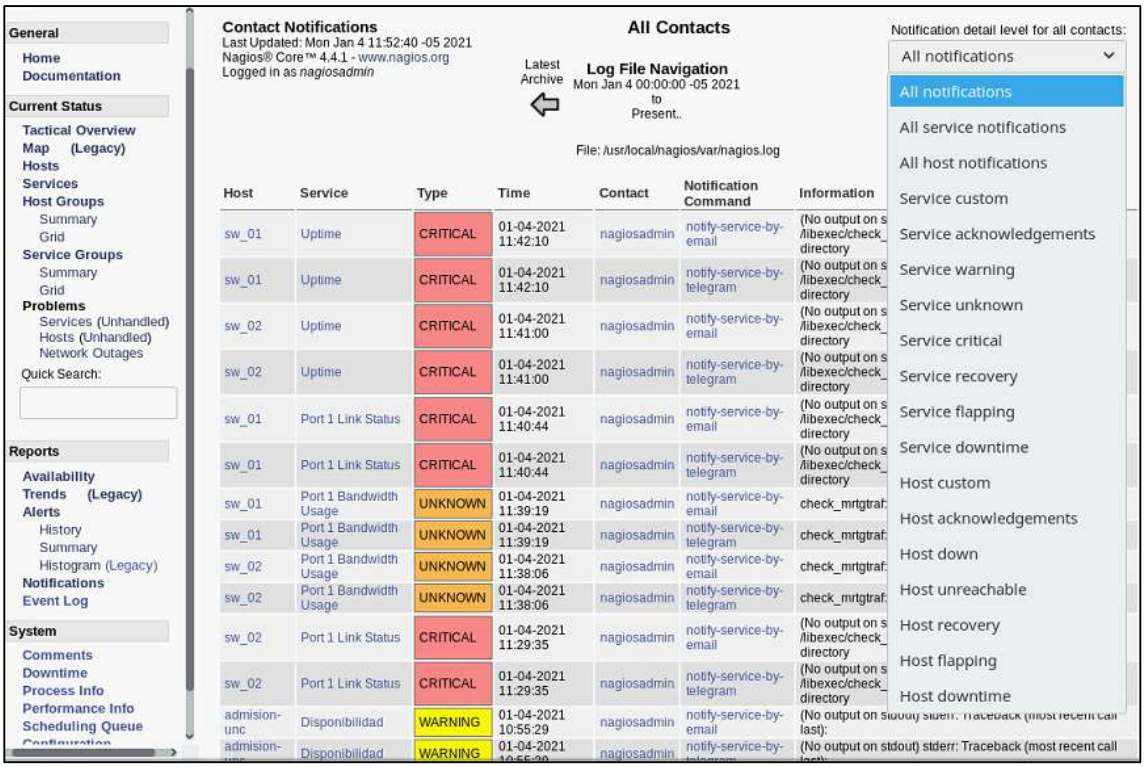


Ilustración 28 Reporte de Notificaciones - Máquina UNC

Ilustración 29 Vista "Archivo Log" - Máquinas UNC

Nagios Process Information
Last Updated: Mon Jan 4 12:09:32 -05 2021
Updated every 90 seconds
Nagios® Core™ 4.4.1 - www.nagios.org
Logged in as *nagiosadmin*

Process Information

Program Version:	4.4.1
Program Start Time:	12-21-2020 09:24:03
Total Running Time:	14d 2h 45m 29s
Last Log File Rotation:	01-04-2021 00:00:00
Nagios PID	1432
Notifications Enabled?	YES
Service Checks Being Executed?	YES
Passive Service Checks Being Accepted?	YES
Host Checks Being Executed?	YES
Passive Host Checks Being Accepted?	YES
Event Handlers Enabled?	Yes
Obsessing Over Services?	No
Obsessing Over Hosts?	No
Flap Detection Enabled?	Yes
Performance Data Being Processed?	Yes

Process Commands

- Shutdown the Nagios process
- Restart the Nagios process
- Disable notifications
- Stop executing service checks
- Stop accepting passive service checks
- Stop executing host checks
- Stop accepting passive host checks
- Disable event handlers
- Start obsessing over services
- Start obsessing over hosts
- Disable flap detection
- Disable performance data

Ilustración 30 Vista "Información Procesos Nagios" - Máquina UNC

Entries sorted by **next check time** (ascending)

Host	Service	Last Check	Next Check	Type	Active Checks	Actions
localhost	Swap Usage	01-04-2021 12:06:16	01-04-2021 12:11:16	Normal	ENABLED	
mysql-server		01-04-2021 12:06:35	01-04-2021 12:11:35	Normal	ENABLED	
localhost	SSH	01-04-2021 12:06:35	01-04-2021 12:11:35	Normal	ENABLED	
sw_02	PING	01-04-2021 12:06:40	01-04-2021 12:11:40	Normal	ENABLED	
mysql-server	MySQL Up Time	01-04-2021 12:01:53	01-04-2021 12:11:53	Normal	ENABLED	
linux_01	Current Load	01-04-2021 12:06:54	01-04-2021 12:11:54	Normal	ENABLED	
sw_01	Uptime	01-04-2021 12:02:10	01-04-2021 12:12:10	Normal	ENABLED	
linux_01	SSH	01-04-2021 12:07:13	01-04-2021 12:12:13	Normal	ENABLED	
localhost	HTTP	01-04-2021 12:07:26	01-04-2021 12:12:26	Normal	ENABLED	
sw_01		01-04-2021 12:07:27	01-04-2021 12:12:27	Normal	ENABLED	
localhost	Total Processes	01-04-2021 12:07:40	01-04-2021 12:12:40	Normal	ENABLED	
sw_01	PING	01-04-2021 12:07:58	01-04-2021 12:12:58	Normal	ENABLED	
sw_02		01-04-2021 12:08:18	01-04-2021 12:13:18	Normal	ENABLED	
linux_01	Current Users	01-04-2021 12:08:22	01-04-2021 12:13:22	Normal	ENABLED	
localhost	Current Load	01-04-2021 12:08:35	01-04-2021 12:13:35	Normal	ENABLED	
linux_01	Swap Usage	01-04-2021 12:08:37	01-04-2021 12:13:37	Normal	ENABLED	
linux_01	HTTP	01-04-2021 12:08:47	01-04-2021 12:13:47	Normal	ENABLED	
localhost	PING	01-04-2021 12:08:51	01-04-2021 12:13:51	Normal	ENABLED	
linux_01		01-04-2021 12:09:55	01-04-2021 12:14:55	Normal	ENABLED	
localhost	Root Partition	01-04-2021 12:10:18	01-04-2021 12:15:18	Normal	ENABLED	
admision-unc	Disponibilidad	01-04-2021 12:05:28	01-04-2021 12:15:28	Normal	ENABLED	
linux_01	Total Processes	01-04-2021 12:10:30	01-04-2021 12:15:30	Normal	ENABLED	
admision-unc		01-04-2021 12:10:37	01-04-2021 12:15:37	Normal	ENABLED	
linux_01	Root Partition	01-04-2021 12:10:43	01-04-2021 12:15:43	Normal	ENABLED	

Ilustración 31 Vista "Registro horas de Verificación 1" - Máquina UNC

sw_01		01-04-2021 12:07:27	01-04-2021 12:12:27	Normal	ENABLED	
localhost	Total Processes	01-04-2021 12:07:40	01-04-2021 12:12:40	Normal	ENABLED	
sw_01	PING	01-04-2021 12:07:58	01-04-2021 12:12:58	Normal	ENABLED	
sw_02		01-04-2021 12:08:18	01-04-2021 12:13:18	Normal	ENABLED	
linux_01	Current Users	01-04-2021 12:08:22	01-04-2021 12:13:22	Normal	ENABLED	
localhost	Current Load	01-04-2021 12:08:35	01-04-2021 12:13:35	Normal	ENABLED	
linux_01	Swap Usage	01-04-2021 12:08:37	01-04-2021 12:13:37	Normal	ENABLED	
linux_01	HTTP	01-04-2021 12:08:47	01-04-2021 12:13:47	Normal	ENABLED	
localhost	PING	01-04-2021 12:08:51	01-04-2021 12:13:51	Normal	ENABLED	
linux_01		01-04-2021 12:09:55	01-04-2021 12:14:55	Normal	ENABLED	
localhost	Root Partition	01-04-2021 12:10:18	01-04-2021 12:15:18	Normal	ENABLED	
admision-unc	Disponibilidad	01-04-2021 12:05:28	01-04-2021 12:15:28	Normal	ENABLED	
linux_01	Total Processes	01-04-2021 12:10:30	01-04-2021 12:15:30	Normal	ENABLED	
admision-unc		01-04-2021 12:10:37	01-04-2021 12:15:37	Normal	ENABLED	
linux_01	Root Partition	01-04-2021 12:10:43	01-04-2021 12:15:43	Normal	ENABLED	
localhost		01-04-2021 12:10:44	01-04-2021 12:15:44	Normal	ENABLED	
linux_01	PING	01-04-2021 12:10:45	01-04-2021 12:15:45	Normal	ENABLED	
localhost	Current Users	01-04-2021 12:11:00	01-04-2021 12:16:00	Normal	ENABLED	
mysql-server	MySQL connection-time	01-04-2021 12:06:25	01-04-2021 12:16:25	Normal	ENABLED	
sw_02	Port 1 Bandwidth Usage	01-04-2021 12:08:06	01-04-2021 12:18:06	Normal	ENABLED	
mysql-server	MySQL Connections	01-04-2021 12:09:02	01-04-2021 12:19:02	Normal	ENABLED	
sw_01	Port 1 Bandwidth Usage	01-04-2021 12:09:19	01-04-2021 12:19:19	Normal	ENABLED	
sw_02	Port 1 Link Status	01-04-2021 12:09:35	01-04-2021 12:19:35	Normal	ENABLED	
mysql-server	MySQL Open Files	01-04-2021 12:10:30	01-04-2021 12:20:30	Normal	ENABLED	
sw_01	Port 1 Link Status	01-04-2021 12:10:44	01-04-2021 12:20:44	Normal	ENABLED	

Ilustración 32 Vista "Registro horas de Verificación 2" - Máquina UNC

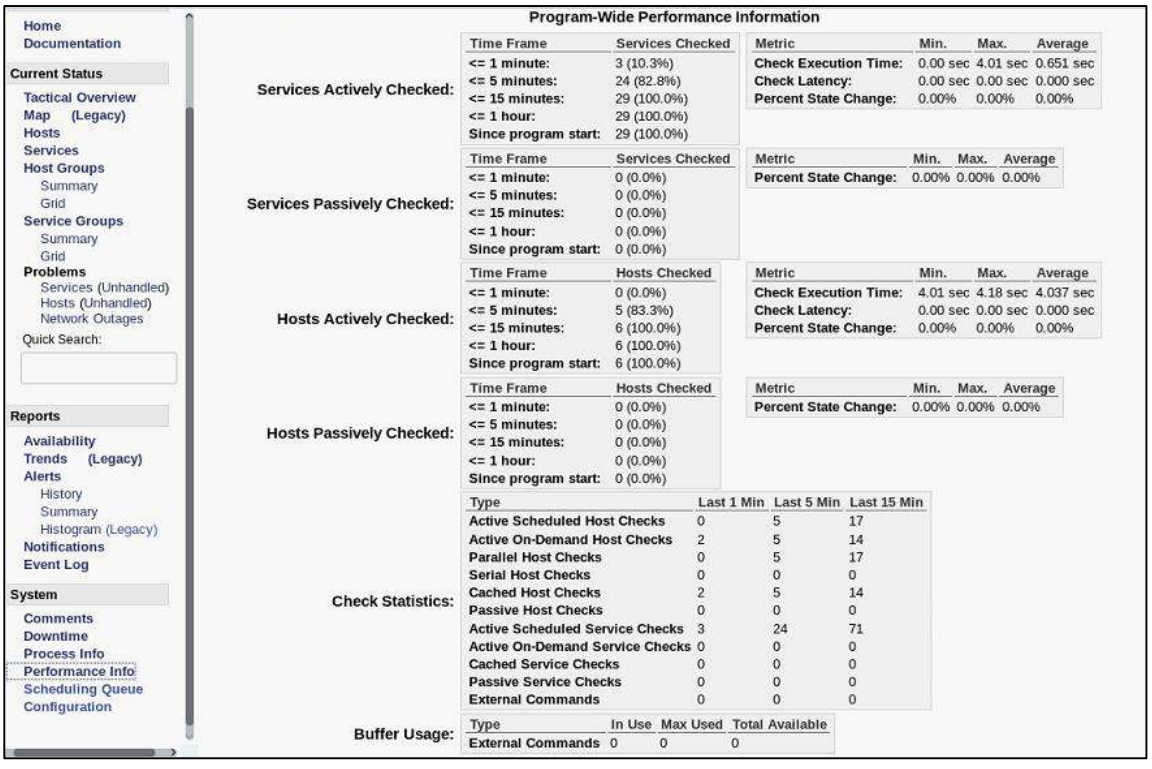


Ilustración 33 Vista "Información del rendimiento del Programa" - Máquina UNC

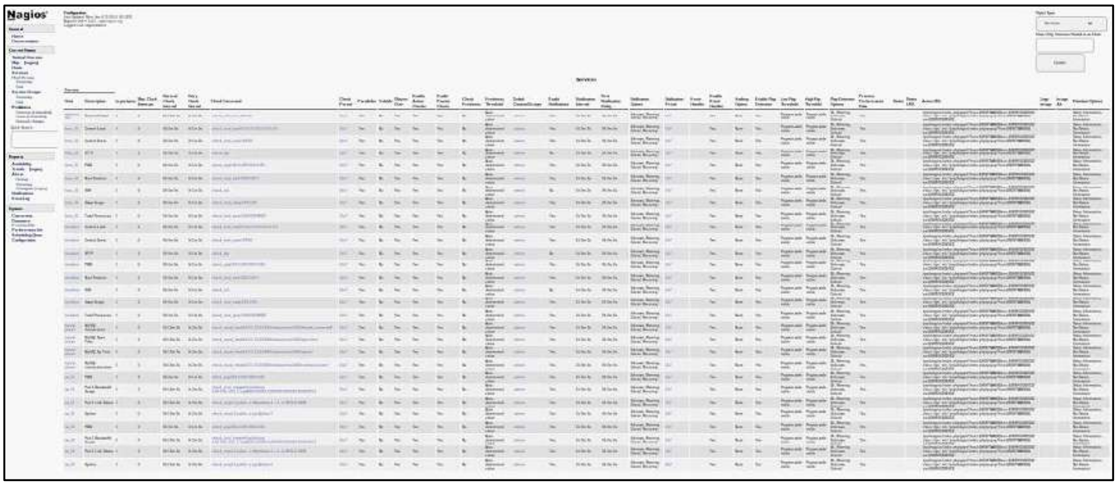


Ilustración 34 Vista "Configuración General" - Máquina UNC

Host Name	Alias/Description	Address	Importance (Host)	Importance (Host + Services)	Parent Hosts	Max. Check Attempts	Check Interval	Retry Interval	Host Check Command	Check Period	Obsess Over	Enable Active Checks	Enable Passive Checks	Check Freshness
admision-unc	admision-unc	127.0.0.1	0	0		10	0h 5m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No
linux_01	linux_01	10.1.3.16	0	0		10	0h 5m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No
localhost	localhost	127.0.0.1	0	0		10	0h 5m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No
mysql-server	MySQL Server	10.1.3.16	0	0		10	0h 5m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No
sw_01	Sw_01	10.1.2.102	0	0		10	0h 5m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No
sw_02	Sw_02	10.1.2.110	0	0		10	0h 5m 0s	0h 1m 0s	check-host-alive	24x7	Yes	Yes	Yes	No

Ilustración 35 Vista "Configuración 1" - Máquina UNC

Default Contacts/Groups	Notification Interval	First Notification Delay	Notification Options	Notification Period	Event Handler	Enable Event Handler	Stalking Options	Enable Flap Detection	Low Flap Threshold	High Flap Threshold	Flap Detection Options	Process Performance Data
admins	2h 0m 0s	0h 0m 0s	Down, Unreachable, Recovery	workhours		Yes	None	Yes	Program-wide value	Program-wide value	Up, Down, Unreachable	Yes
admins	2h 0m 0s	0h 0m 0s	Down, Unreachable, Recovery	workhours		Yes	None	Yes	Program-wide value	Program-wide value	Up, Down, Unreachable	Yes
admins	2h 0m 0s	0h 0m 0s	Down, Unreachable, Recovery	workhours		Yes	None	Yes	Program-wide value	Program-wide value	Up, Down, Unreachable	Yes
admins	2h 0m 0s	0h 0m 0s	Down, Unreachable, Recovery	workhours		Yes	None	Yes	Program-wide value	Program-wide value	Up, Down, Unreachable	Yes
admins	0h 30m 0s	0h 0m 0s	Down, Recovery	24x7		Yes	None	Yes	Program-wide value	Program-wide value	Up, Down, Unreachable	Yes
admins	0h 30m 0s	0h 0m 0s	Down, Recovery	24x7		Yes	None	Yes	Program-wide value	Program-wide value	Up, Down, Unreachable	Yes

Ilustración 36 Vista "Configuración 2" - Máquina UNC

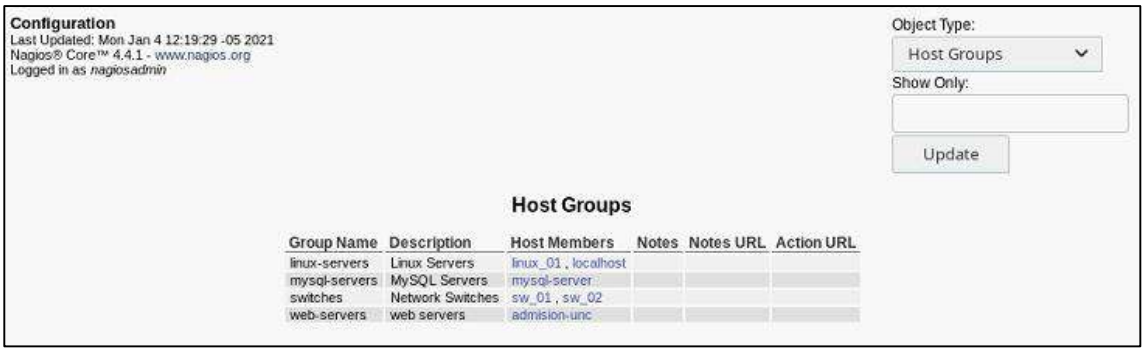


Ilustración 37 Vista "Configuración según grupo " - Máquina UNC

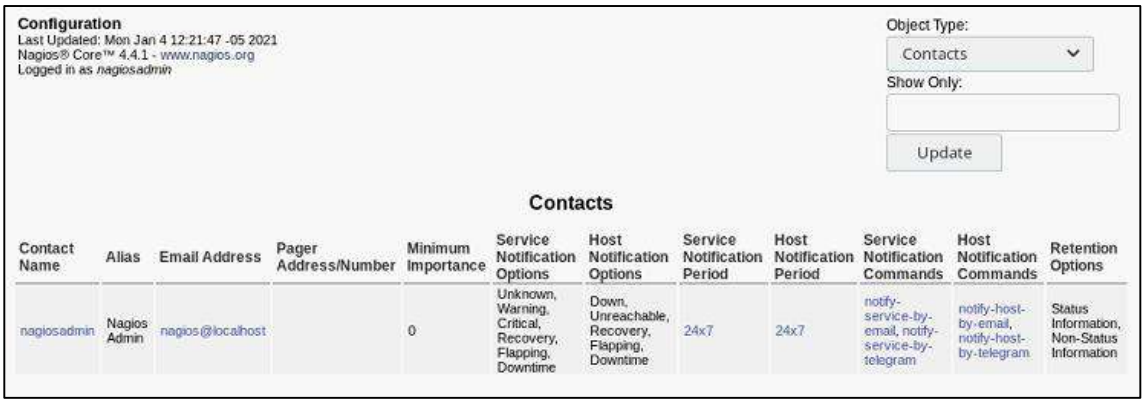


Ilustración 38 Vista "Configuración según Contacto " - Máquina UNC

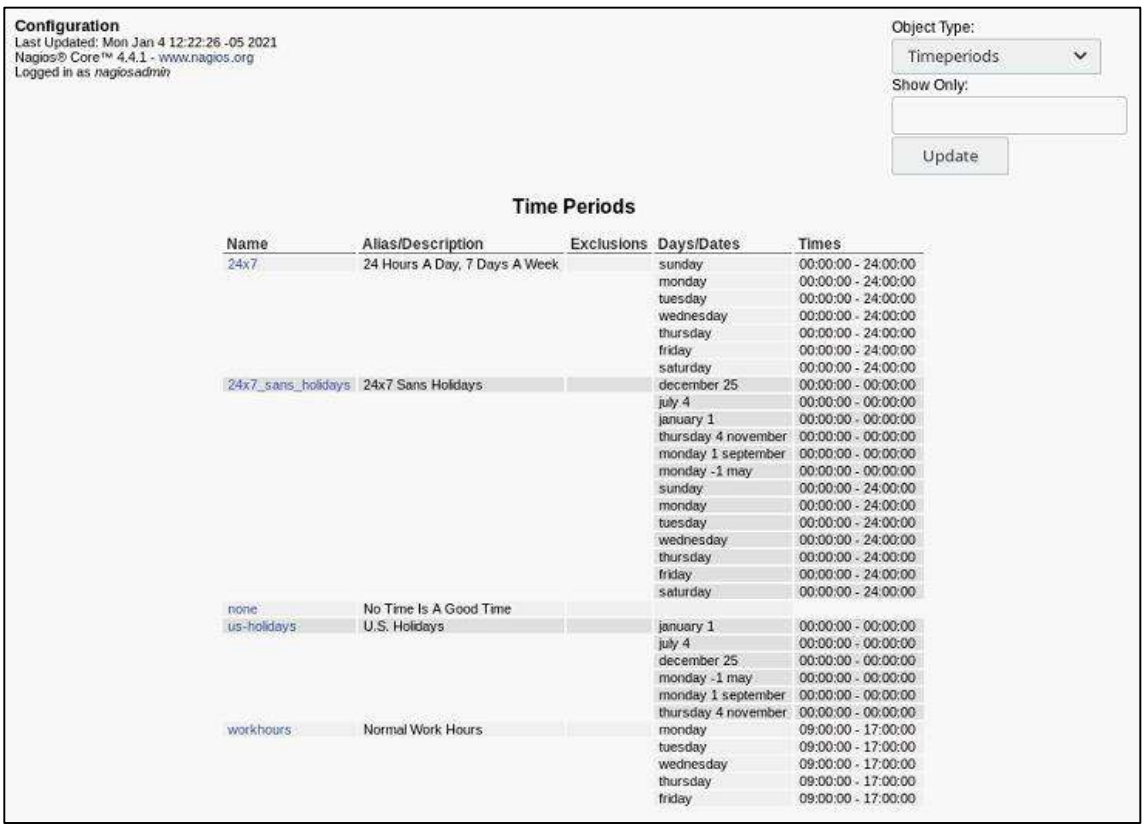


Ilustración 39 Vista "Configuración según Periodo " - Máquina UNC

Configuration
Last Updated: Mon Jan 4 12:23:10 -05 2021
Nagios® Core™ 4.4.1 - www.nagios.org
Logged in as *nagiosadmin*

Object Type: Commands
Show Only:
Update

Commands

Command Name	Command Line
check-host-alive	$USER1$/check_ping -H $HOSTADDRESS$ -w 3000.0,80% -c 5000.0,100% -p 5
check_admision_website	/usr/local/nagios/libexec/check_service_sd --id 5df959f5b03e8546378b4567 --token a5f658ea4a81a06c73456a82d78d8979 --slow 0.5 --locations 1 --allowed-status 200 301 30
check_dhcp	$USER1$/check_dhcp $ARG1$
check_ftp	$USER1$/check_ftp -H $HOSTADDRESS$ $ARG1$
check_hpjd	$USER1$/check_hpjd -H $HOSTADDRESS$ $ARG1$
check_http	$USER1$/check_http -I $HOSTADDRESS$ $ARG1$
check_imap	$USER1$/check_imap -H $HOSTADDRESS$ $ARG1$
check_local_disk	$USER1$/check_disk -w $ARG1$ -c $ARG2$ -p $ARG3$
check_local_load	$USER1$/check_load -w $ARG1$ -c $ARG2$
check_local_mrtgtraf	$USER1$/check_mrtgtraf -F $ARG1$ -a $ARG2$ -w $ARG3$ -c $ARG4$ -e $ARG5$
check_local_procs	$USER1$/check_procs -w $ARG1$ -c $ARG2$ -s $ARG3$
check_local_swap	$USER1$/check_swap -w $ARG1$ -c $ARG2$
check_local_users	$USER1$/check_users -w $ARG1$ -c $ARG2$
check_mysql_health	$USER1$/check_mysql_health -H $ARG1$ --port $ARG2$ --username $ARG3$ --password $ARG4$ --mode $ARG5$
check_nt	$USER1$/check_nt -H $HOSTADDRESS$ -p 12489 -v $ARG1$ $ARG2$
check_ping	$USER1$/check_ping -H $HOSTADDRESS$ -w $ARG1$ -c $ARG2$ -p 5
check_pop	$USER1$/check_pop -H $HOSTADDRESS$ $ARG1$
check_smtp	$USER1$/check_smtp -H $HOSTADDRESS$ $ARG1$
check_snmp	$USER1$/check_snmp -H $HOSTADDRESS$ $ARG1$
check_ssh	$USER1$/check_ssh $ARG1$ $HOSTADDRESS$
check_tcp	$USER1$/check_tcp -H $HOSTADDRESS$ -p $ARG1$ $ARG2$
check_udp	$USER1$/check_udp -H $HOSTADDRESS$ -p $ARG1$ $ARG2$
notify-host-by-email	/usr/bin/printf "%b" "***** Nagios *****\n\nNotification Type: $NOTIFICATIONTYPE$\nHost: $HOSTNAME$\nState: $HOSTSTATE$\nAddress: $HOSTADDRESS$\nInfo: $HOSTOU /sendmail -s "** $NOTIFICATIONTYPE$ Host Alert: $HOSTNAME$ is $HOSTSTATE$ **" $CONTACTEMAIL$
notify-host-by-telegram	curl -k -L --data chat_id=-499696385 --data-urlencode "text=***** Nagios ***** Notification Type: $NOTIFICATIONTYPE$ Host: $HOSTNAME$ State: $HOSTSTATE$ Address: $H $LONGDATETIME$" "https://api.telegram.org/bot1172955481:AAG3EH9hFkL7pol6leJCPku7Oc7p1Wm-iB8/sendMessage"
notify-service-by-email	/usr/bin/printf "%b" "***** Nagios *****\n\nNotification Type: $NOTIFICATIONTYPE$\n\nService: $SERVICEDESC$\nHost: $HOSTALIAS$\nAddress: $HOSTADDRESS$\nState: $S \nAdditional Info:\n\n$SERVICEOUTPUT$\n" | /usr/sbin/sendmail -s "** $NOTIFICATIONTYPE$ Service Alert: $HOSTALIAS$/$SERVICEDESC$ is $SERVICESTATE$ **" $CONTA
notify-service-by-telegram	curl -k -L --data chat_id=-499696385 --data-urlencode "text=***** Nagios ***** Notification Type: $NOTIFICATIONTYPE$ Service: $SERVICEDESC$ Host: $HOSTALIAS$ Address $LONGDATETIME$ Additional Info: $SERVICEOUTPUT$" "https://api.telegram.org/bot1172955481:AAG3EH9hFkL7pol6leJCPku7Oc7p1Wm-iB8/sendMessage"
process-host-perfdata	/usr/bin/printf "%b" "$LASTHOSTCHECK$\t$HOSTNAME$\t$HOSTSTATE$\t$HOSTATTEMPT$\t$HOSTSTATETYPE$\t$HOSTEXECUTIONTIME$\t$HOSTOUTPUT$\t$HOSTPER
process-host-perfdata-file	/bin/mv /usr/local/pnp4nagios/var/host-perfdata /usr/local/pnp4nagios/var/spool/host-perfdata.$TIMET$
process-service-perfdata	/usr/bin/printf "%b" "$LASTSERVICECHECK$\t$HOSTNAME$\t$SERVICEDESC$\t$SERVICESTATE$\t$SERVICEATTEMPT$\t$SERVICESTATETYPE$\t$SERVICEEXECUTIONTIME$\t$SERVICEL >> /usr/local/nagios/var/service-perfdata.out
process-service-perfdata-file	/bin/mv /usr/local/pnp4nagios/var/service-perfdata /usr/local/pnp4nagios/var/spool/service-perfdata.$TIMET$

Ilustración 40 Vista "Comandos" – Máquina UNC

4.1.4. HERRAMIENTAS COMPLEMENTARIAS

4.1.4.1. PNP4nagios

Es un complemento de Nagios utilizado en la investigación que analizó los datos de rendimiento obtenidos por los plugins y los almacenó automáticamente en la base de datos, RDDtool se encargó de brindar la información para los gráficos, la evidencia de la instalación en las maquina UNC se encuentra en el Anexo 7 (Imagen 160 a 184) a continuación se detalla el código usado [21].

Código prerrequisitos que se usaron para la instalación.

```
sudo apt-get update
sudo apt-get install -y rrdtool librrd-simple-perl php-gd
```

Se descargó la fuente

```
cd / tmp
wget -O pnp4nagios.tar.gz
https://github.com/lingej/pnp4nagios/archive/0.6.26.tar.gz
tar xzf pnp4nagios.tar.gz
```

Se compiló e instaló

```
cd pnp4nagios-0.6.26
sudo ./configure --with-httpd-conf = / etc / apache2 / sites-
enabled
sudo make all
sudo make install
sudo make install-webconf
sudo make install-config
sudo make install-init
```

Se inició el servicio *npcd* el cual se configuró para iniciar el arranque al igual que el servicio apache2 también se reinició.

```
sudo update-rc.d npcd defaults
sudo service npcd start
sudo service apache2 restart
```

Se configuró Nagios Core para enviar los datos de rendimiento a PNP4Nagios.

```
/ usr / local / nagios / etc / nagios.cfg
process_performance_data = 1
host_perfdata_file = / usr / local / pnp4nagios / var / host-
perfdata
host_perfdata_file_template = DATATYPE :: HOSTPERFDATA \ tTIMET
:: $ TIMET $ \ tHOSTNAME :: $ HOSTNAME $ \ tHOSTPERFDATA $ $ \
tHOSTSTATE :: $ HOSTSTATE $ \ tHOSTSTATETYPE :: $ HOSTSTATETYPE
$
host_perfdata_file_mode = a
host_perfdata_file_processing_interval = 15
host_perfdata_file_processing_command = process-host-local-
perfdata_file_processing_command = process-host-local-
perfdata_file-
service-var_perfdata_file_processing_interval
service_perfdata_file_template = DATATYPE :: SERVICEPERFDATA \
```

```
tTIMET :: $ TIMET $ \ tHOSTNAME :: $ HOSTNAME $ \ tSERVICEDESC
:: $ SERVICEDESC $ \ tSERVICEPERFDATA :: $ SERVICEPERFDATA $ \
tSERVATE $ tHOSTCHECKCOSTS :: $ HOSTSTATETYPE $ \ tSERVICESTATE
:: $ SERVICESTATE $ \ tSERVICESTATETYPE :: $ SERVICESTATETYPE $
service_perfdata_file_mode = a
service_perfdata_file_processing_interval = 15
service_perfdata_file_processing_command-process -cd
```

sudo sh -c "sed -i 's / process_performance_data = 0 / process_performance_data = 1 / g' /usr/local/nagios/etc/nagios.cfg"

sudo sh -c "sed -i 's / # host_perfdata_file = / host_perfdata_file = / g '/usr/local/nagios/etc/nagios.cfg "

sudo sh -c" sed -i' s / ^ host_perfdata_file =. * / host_perfdata_file = \ / usr \ / local \ / pnp4nagios \ / var \ / service-perfdata / g '/usr/local/nagios/etc/nagios.cfg "

sudo sh -c" sed -i' s / ^ # host_perfdata_file_template =. * / '/usr/local/nagios/etc/nagios.cfg "

sudo sh -c "sed -i 's / ^ # service_perfdata_file_template =. * / service_perfdata_file_template = DATATYPE :: SERVICEPERFDATA \\\\ tTIMET :: \ $ TIMET \ $ \\\\ tHOSTNAME :: \ $ HOSTNAME \ $ \\ \\ tSERVICEDESC :: \ $ SERVICEDESC \ $ \\\\ tSERVICEPERFDATA :: \ $ SERVICEPERFDATA \ $ \\\\ tSERVICECHECKCOMMAND :: \ $ SERVICECHECKCOMMAND \ $ \\\\ tHOSTSTATE :: \ $ HOSTSTATE \ $ \\ tHOSTSTATETYPE :: \ $ HOSTSTATETYPE \ $ \\\\ tSERVICESTATE :: \ $ SERVICESTATE \ $ \\\\ tSERVICESTATETYPE :: \ $ SERVICESTATETYPE \ $ / g '/usr/local/nagios/etc/nagios.cfg "

sudo sh -c "sed -i 's / # service_perfdata_file_mode = / service_perfdata_file_mode = / g' /usr/local/nagios/etc/nagios.cfg"

sudo sh -c "sed -i 's / ^ # service_perfdata_fileval_processing_interval_f. * / service_fileval_processing_interval_f. * / = 15 / g '/usr/local/nagios/etc/nagios.cfg "

sudo sh -c "sed -i 's / ^ # service_perfdata_file_processing_command =. * / service_perfdata_file_processing_command = process-service-perfdata-file-bulk-npcd / g' /usr/local/nagios/etc/nagios.cfg" [22].

Se definió el comando “**commands.cfg** ” ubicado en la siguiente carpeta: / usr / local / nagios / etc / objects /

```
define el comando {
    command_name process-service-perfdata-file-bulk-npcd
command_line
    / bin / mv / usr / local / pnp4nagios / var / service-
perfdata /usr/local/pnp4nagios/var/spool/service-
perfdata.$TIMET$
    }
definir comando {
    command_name process-host-perfdata-file-bulk-npcd
command_line
    / bin / mv / usr / local / pnp4nagios / var / host-perfdata
/usr/local/pnp4nagios/var/spool/host-perfdata.$TIMET $
    } [22].
```

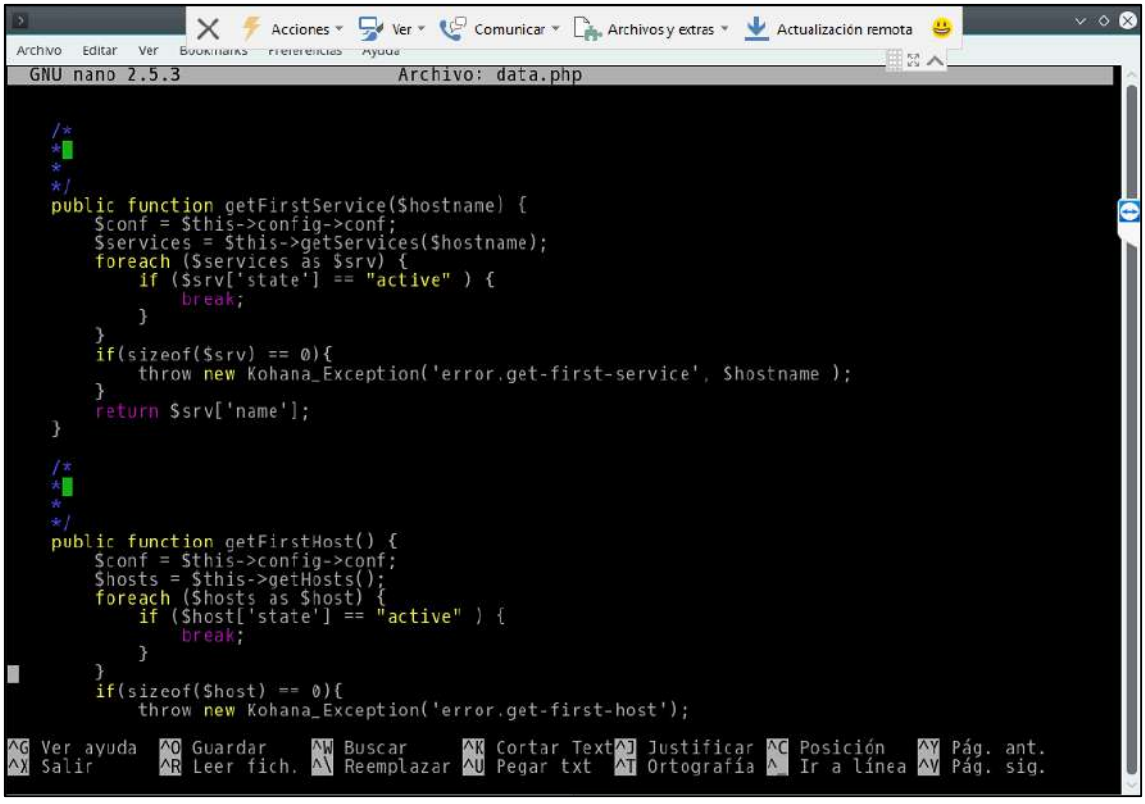


Ilustración 41 Configuración PNP4nagios - Máquina UNC

VeriSe verificó la configuración de Nagios Core con el siguiente comando:

```
sudo / usr / local / nagios / bin / nagios -v
/usr/local/nagios/etc/nagios.cfg
```

Para confirmar que PNP4Nagios está funcionando se buscó en los archivos RRD y al mismo tiempo se buscó en / usr / local / pnp4nagios / var / perfdata / la existencia de diferentes carpetas para cada host de Nagios, por ejemplo la siguiente ruta mostró el host local y sus servicios:

```
ls -la / usr / local / pnp4nagios / var / perfdata / localhost /
```

Para acceder a la interfaz weby ver datos de PNP4Nagios, se buscó en el navegador la URL: http: // 10.1.3.195 / pnp4nagios / y se verificó los indicadores en verde (ilustración 43-44)

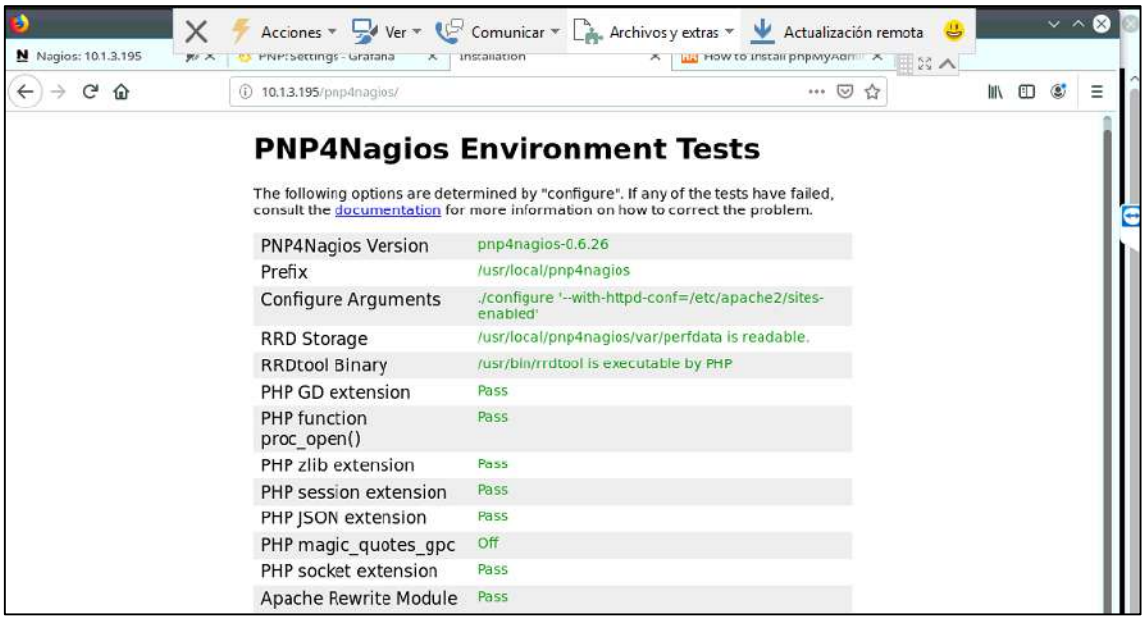


Ilustración 42 Cuadro Instalación PNP4nagios – Máquina UNC

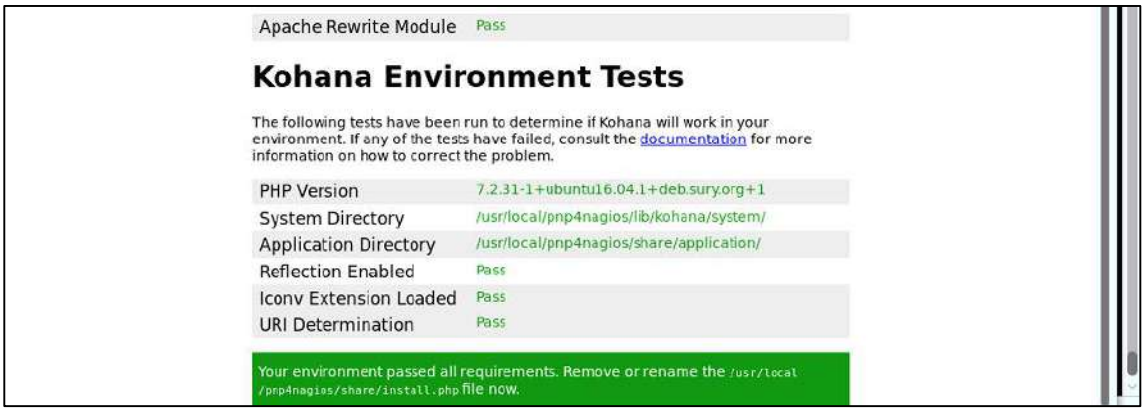


Ilustración 43 Confirmación de Instalación correcta - Máquina UNC

Finalmente se actualizó el navegador web con la dirección de nagios y se comenzó a ver los gráficos de Nagios en la interfaz principal (Ilustración 45 y 46) y de la misma forma se logró observar los gráficos (Ilustración 47).

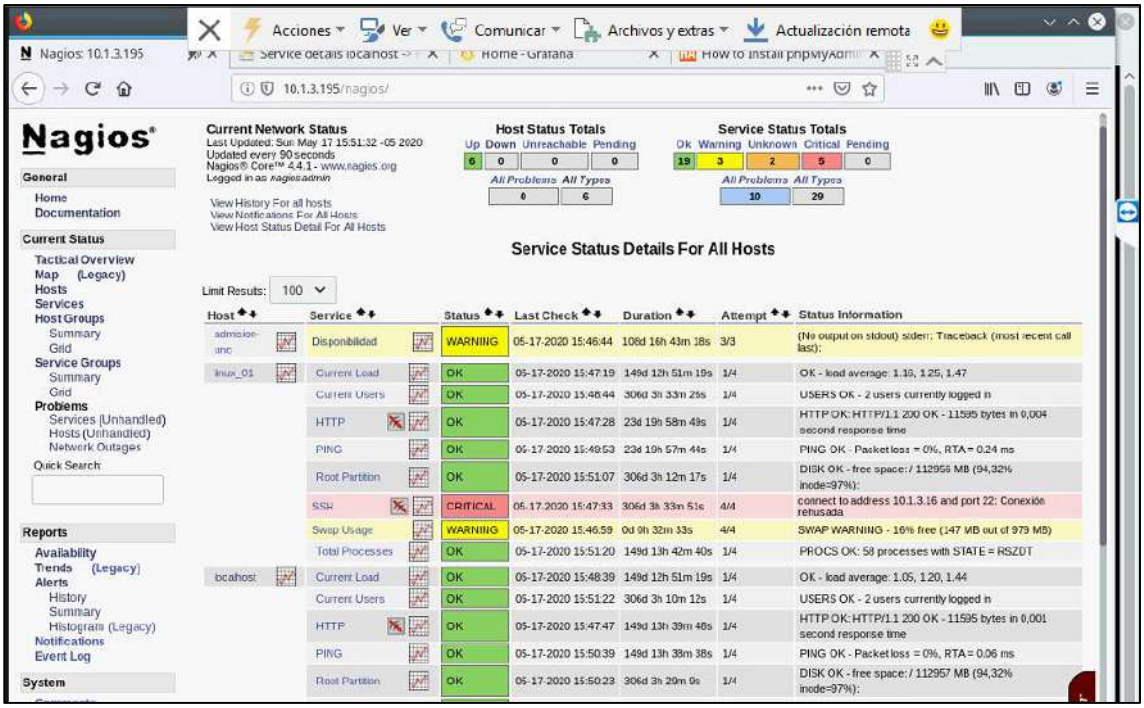


Ilustración 44 Proyecto Nagios con acceso PNP4nagios- Máquina UNC

Ilustración 45Proyecto Nagios con acceso PNP4nagios- Máquina UNC

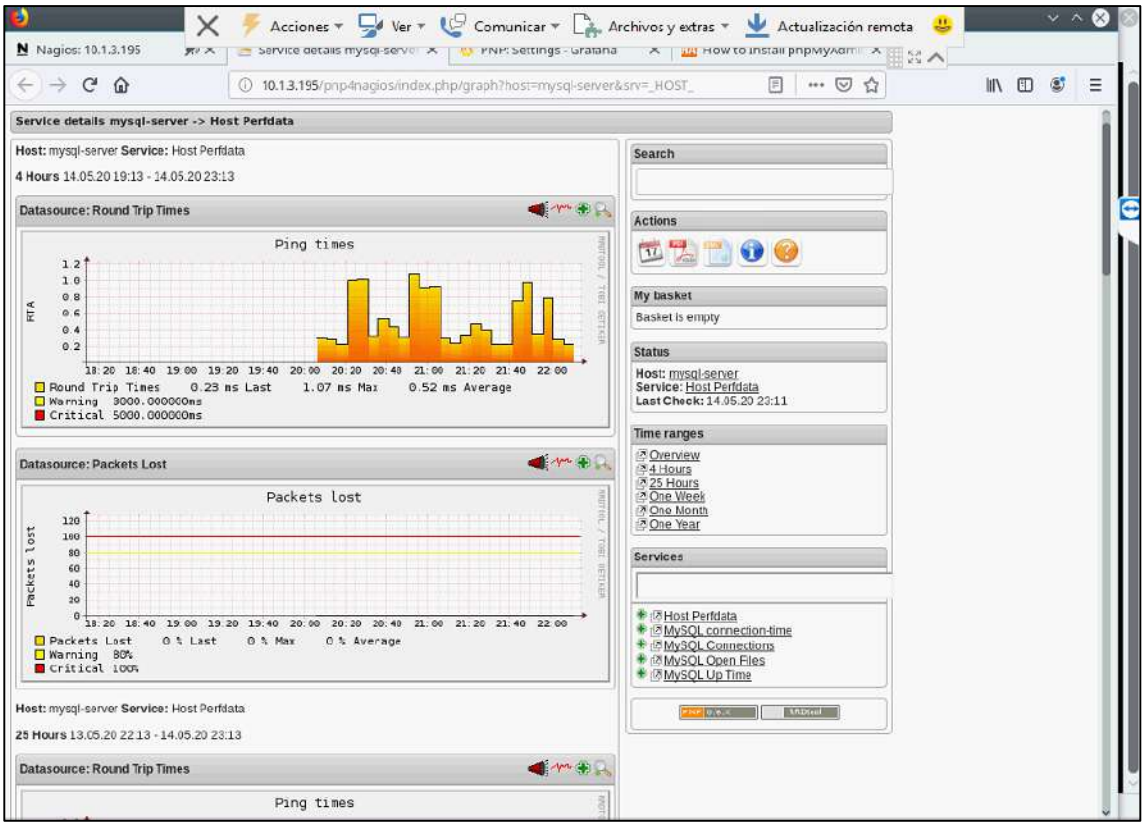


Ilustración 46 Primer gráfico proporcionado por PNP4nagios - Máquina UNC

4.1.4.2. Grafana

Grafana fue otra herramienta usada en la investigación que, mediante la interfaz web, permitió crear paneles de Grafana con las métricas a lo largo del tiempo, en otras palabras, permitió crear dashboard más interactivos y dinámicos para el usuario, la evidencia de Instalación se muestra en el Anexo 8 (Ilustración 185 a 195), el código descrito a continuación se utilizó para realizar la instalación del servicio.

Para instalar e iniciar el servicio de grafana se usaron los siguientes comandos:

```
sudo systemctl enable grafana-server.service
sudo systemctl start grafana-server.service
```

Para el tráfico de datos se habilitó el puerto 3000 en el firewall local para poder acceder a la interfaz web de Grafana.

```
sudo ufw permitir 3000 / tcp
sudo ufw reload
```

Se instaló los componentes PNP4Nagios para que Grafana pueda hiciere uso de la data almacenada:

```
sudo grafana-cli plugins instalar sni-pnp-datasource
sudo systemctl reiniciar grafana-server.service
cd / usr / local / pnp4nagios / share / application /
controllers /
sudo wget -O api.php "https://github.com/lingej /pnp-metrics-
api/raw/master/application/controller/api.php "
```

Grafana llamó a la API de PNP4Nagios y solicitó permiso de la siguiente forma:

```
sudo sh -c "sed -i '/ Require valid-user / a \ Require ip
127.0.0.1 :: 1' /etc/apache2/sites-enabled/pnp4nagios.conf"
```

El servicio *Apache* apache2 se reinició para que este cambio surta efecto:

```
sudo systemctl reiniciar apache2.service
```

Mediante la URL: http: // 10.1.3.195:3000, se accedió al inicio de sesión, como muestra la ilustración 48.

Ilustración 47 Puerto 3000 Grafana - Máquina UNC

Se configuró y añadió la fuente de datos para grafana, usando el API de PNP4Nagios (Ilustración 49), para la información HTTP que solicitó la creación del datasource se usó la url http: // localhost / pnp4nagios, y el usuario y password registrados en configuración (Ilustración 50 y 51).

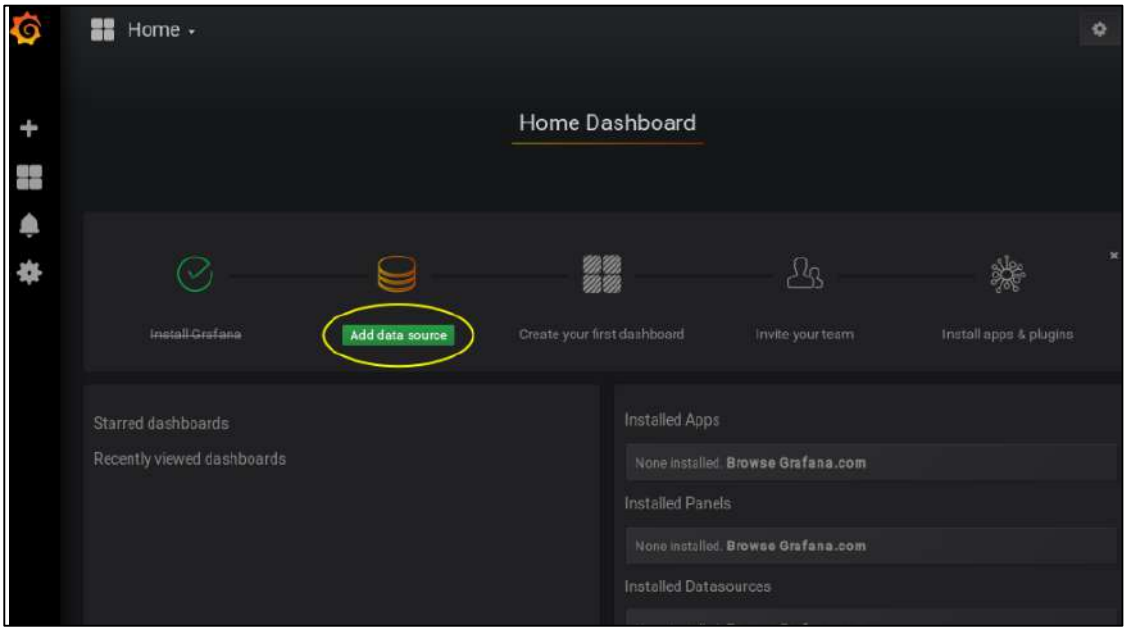


Ilustración 48 Agregar fuente de datos -Máquina UNC

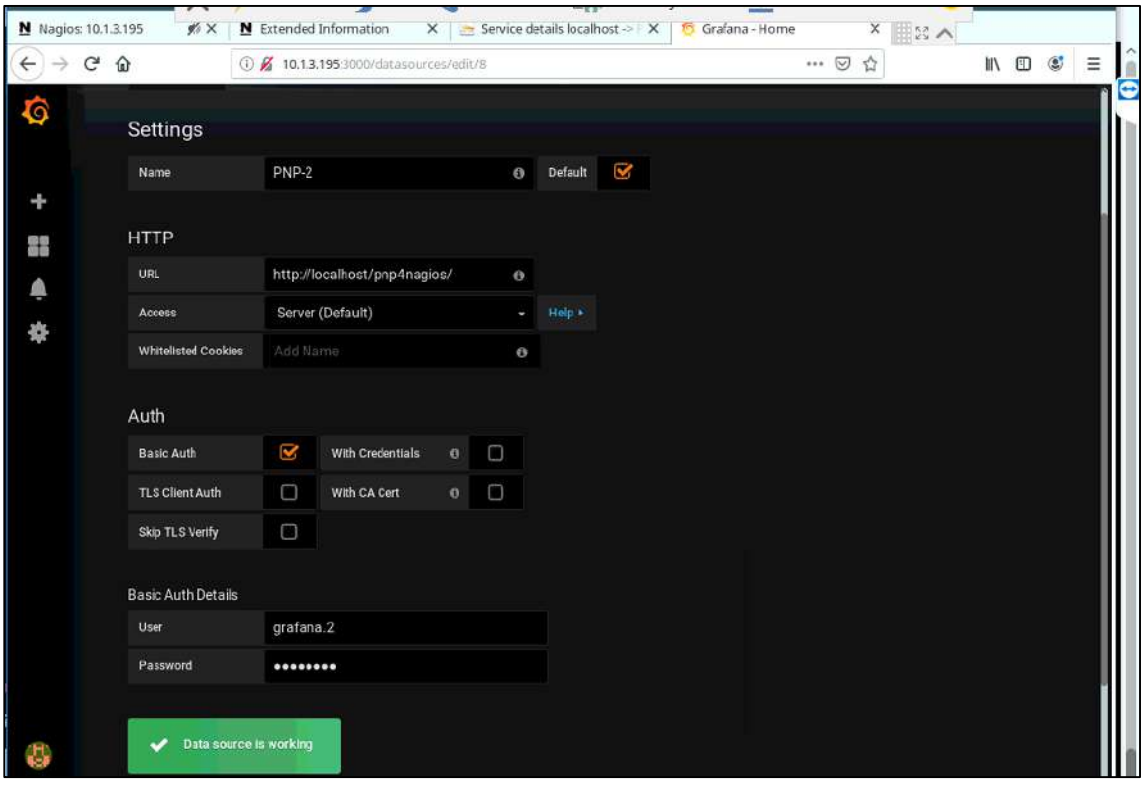


Ilustración 49 Configurar Data - Máquina UNC

Se creó el datasource PNP v1.0.5 como muestra la ilustración 46.

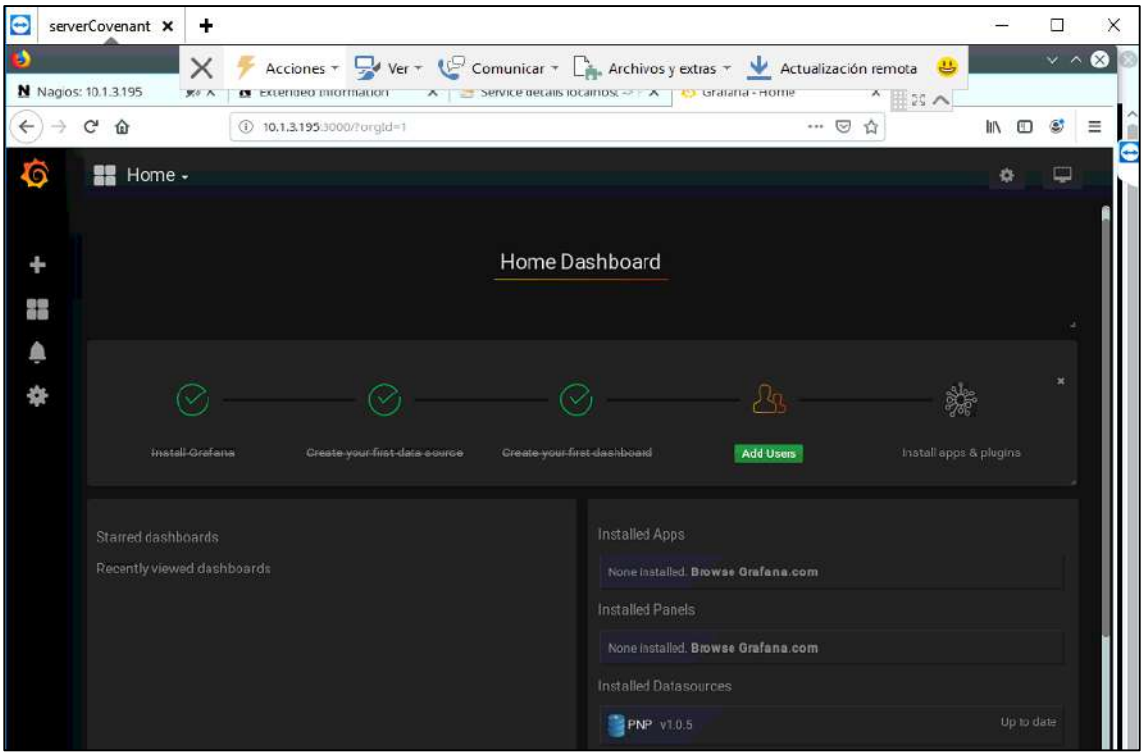


Ilustración 50 Grafana habilitada para crear dashboard -Máquina UNC

Al tener una fuente de datos (PNP v1.0.5) se accedió al menú para crear el primer gráfico, según como muestra la ilustración 52.

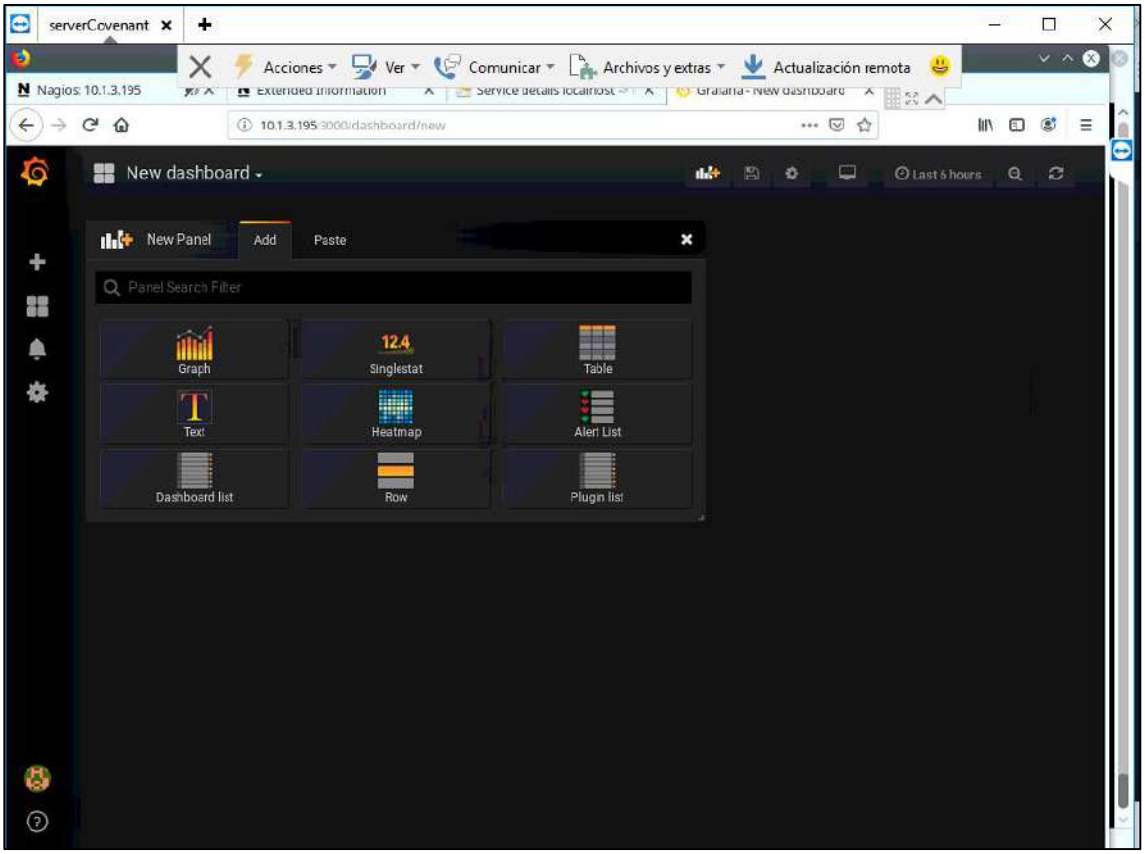


Ilustración 51 Menú crear Gráfico - Máquina UNC

Las ilustraciones 53 y 54 muestran cómo se pudo ingresar datos y filtros según los requerimientos solicitados, los resultados fueron amigables y de fácil entendimiento, adicionalmente como se observa en la ilustración 54 fue posible añadir otra consulta sobre la realizada mejorando el aspecto y resultados del gráfico.

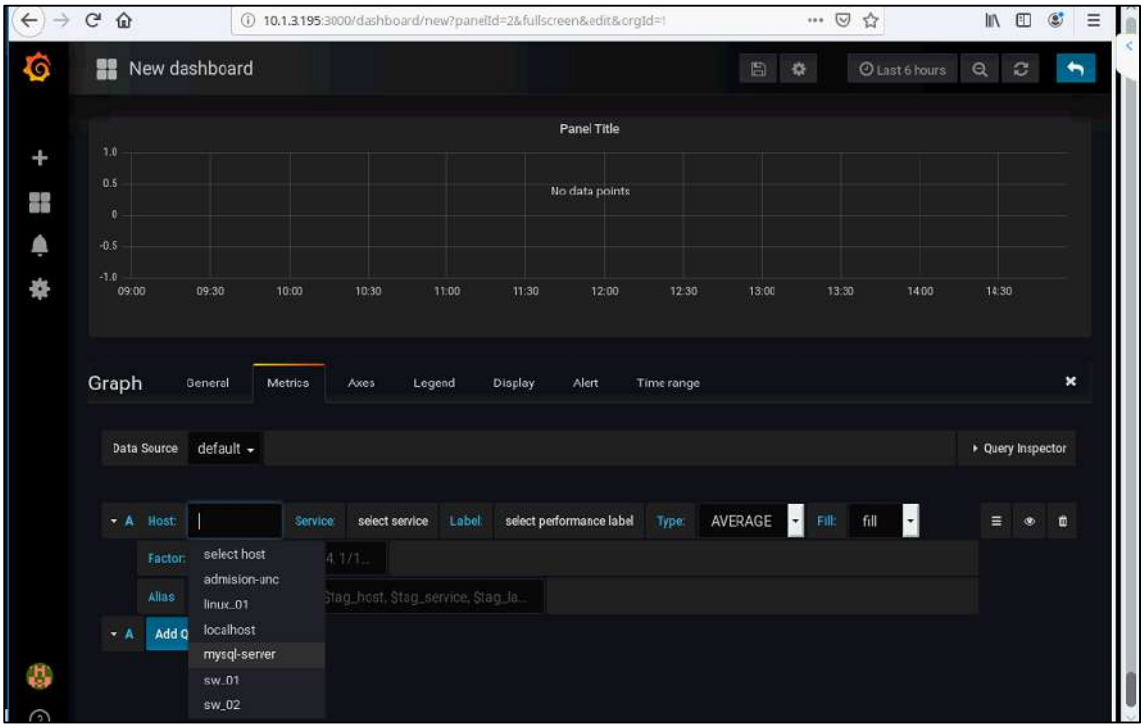


Ilustración 52 Primera configuración de Gráficos -Máquina UNC

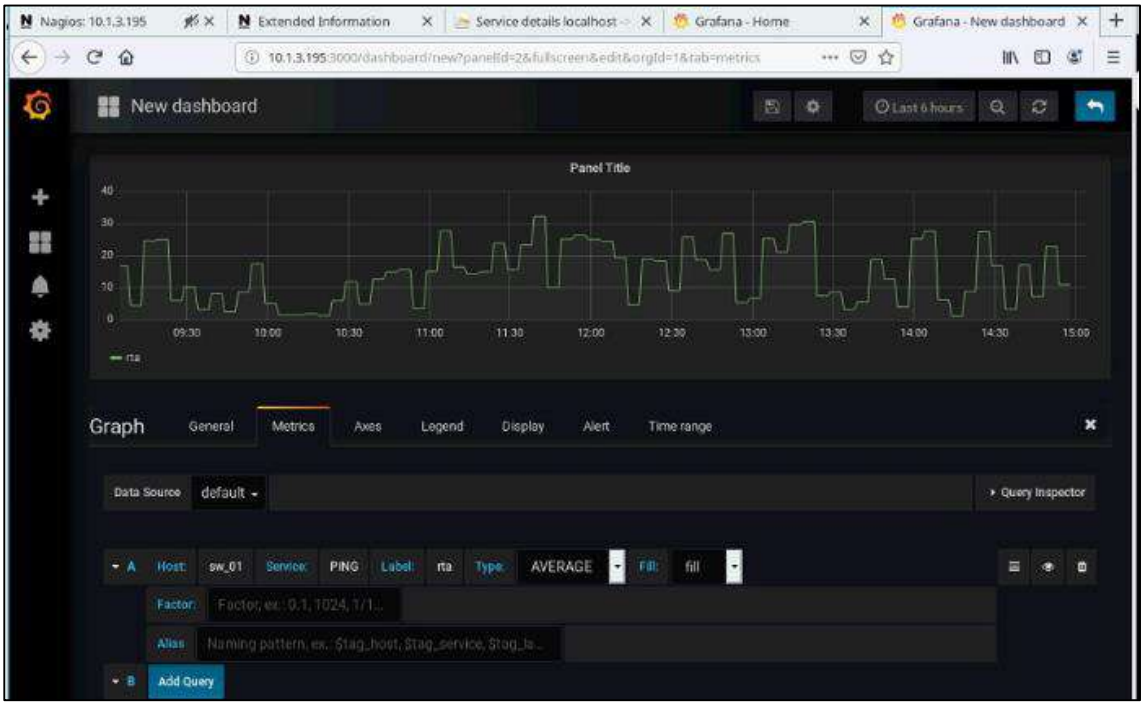


Ilustración 53 Primer gráfico sw_01 - Máquina UNC

4.1.4.3. Telegram

Telgram facilitó la comunicación y reporte de incidentes en gran manera y lo más importante de forma segura ya que esta herramienta cuenta con políticas de seguridad en el transporte de información, el procedimiento usado para lograr las notificaciones se hizo mediante bots y grupos.

Inicialmente se buscó @BotFather en Telegram (Ilustración 55 – 56).

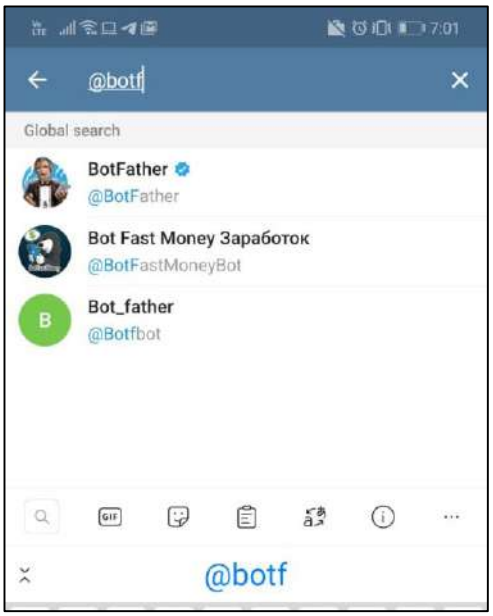


Ilustración 54Buscar @BotFather

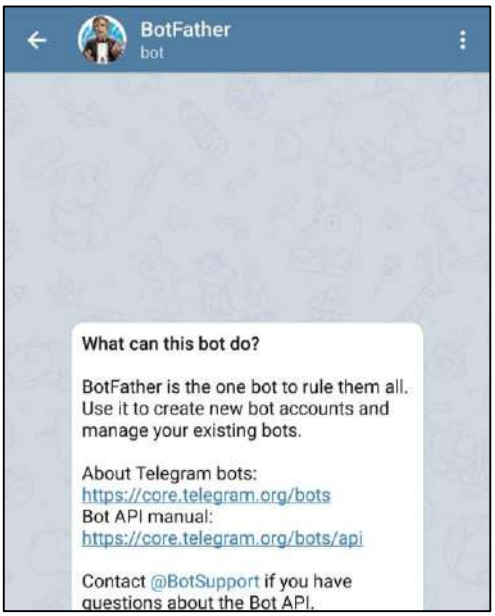


Ilustración 55 Iniciar Bot

Se creó el bot y con el comnado newbot se creó el bot nagiosUNC_bot (Ilustración 57 a 59).

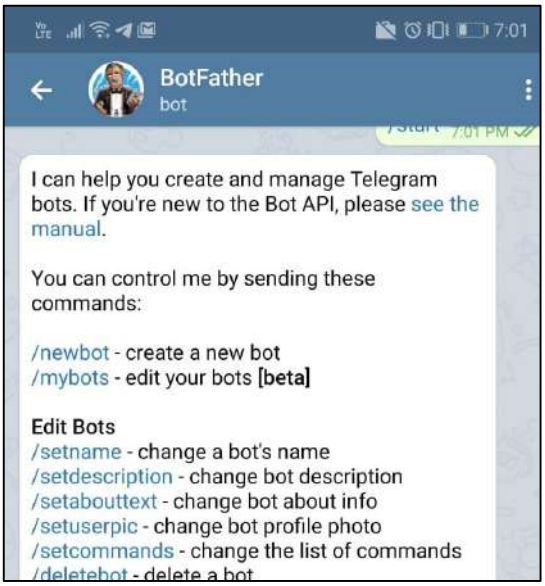


Ilustración 56Crear bot

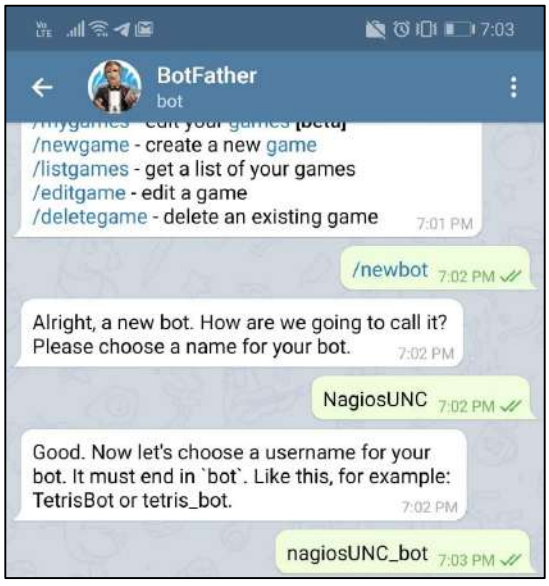


Ilustración 57nagiosUNC_bot

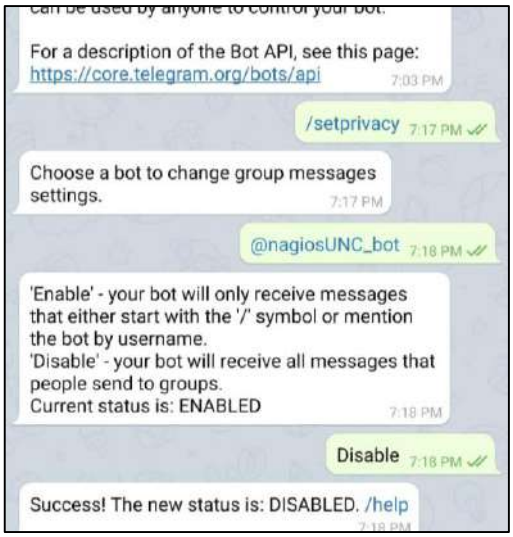


Ilustración 58 Bot nagiosUNC_bot habilitado

Culminada la creación del bot, se creó un grupo de trabajo, con el bot anterior, para reportar las incidencias que se hallaron (Ilustración 60 a 65).

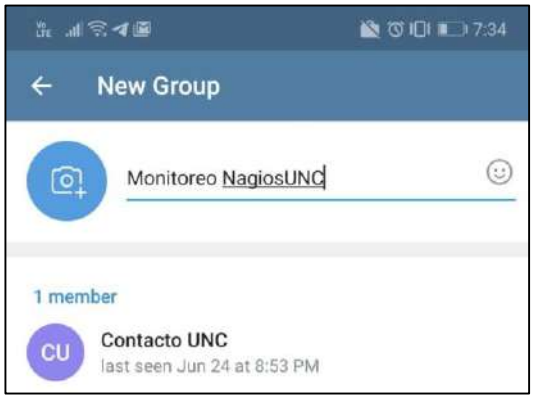


Ilustración 59 Crear grupo de Monitoreo

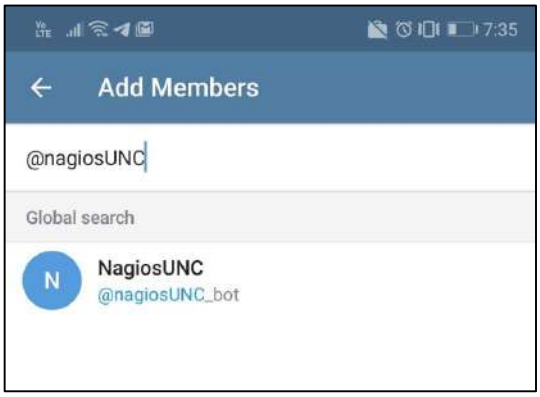


Ilustración 60 Añadir bot nagiosUNC_bot

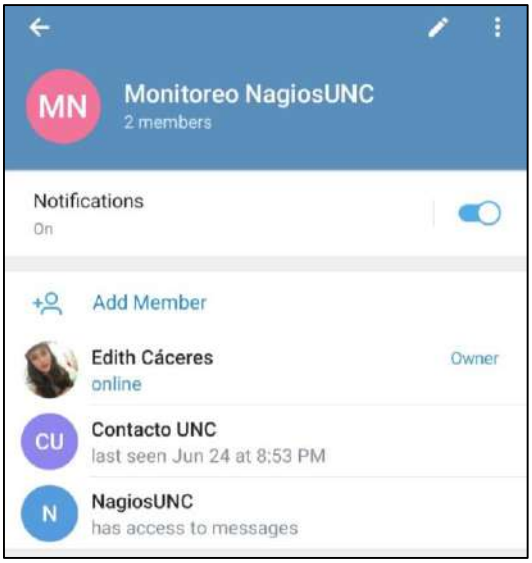
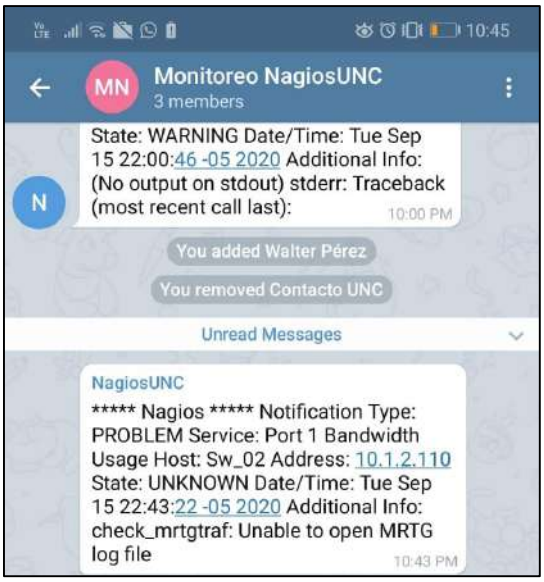


Ilustración 61 Añadir miembros de Área

Ilustración 62 Comunicación de Grupo



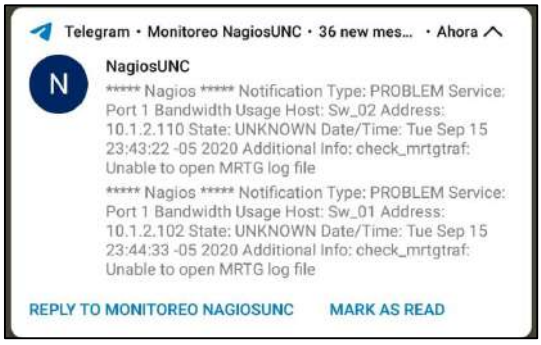


Ilustración 63 Primeras notificaciones

Ilustración 64 Constantes notificaciones

La configuración de Telegram en Nagios, se dió descargando telegram-notify.zip, evidencia de configuración en la Máquina UNC en el Anexo 9 (Ilustración 196 a 201).

```
/ usr / local / nagios / sbin. telegram-notify.zip.
```

Se dio permisos de escritura a la carpeta "log" para el usuario de nagios

```
chown nagios: nagios -R / usr / local / nagios / sbin /
telegram-notificar / log /
chmod 775 -R / usr / local / nagios / sbin / telegram-notificar
/ log /
chown root: root / usr / local / nagios /sbin/telegram-
notify/log/.htaccess
chmod 644 /usr/local/nagios/sbin/telegram-notify/log/.htaccess
define comando {
command_name notificar-servicio-telegrama
command_line / usr / bin / php /usr/local/nagios/sbin/telegram-
notify/telegram-bot.php "$ _CONTACTTELEGRAM $" "83633434:
kewkekekekdkkfiirrjriririjr" $ _SERVICESENDTELEGRAM $NOSTX $
"Notificar: 0XzXZ0 Servicio: $ SERVICEDESC $ 0XzXZ0 Fecha: $
SHORTDATETIME $ 0XzXZ0 Información: $ SERVICEOUTPUT $ "
}
```

```
# 'notificar-host-telegram' definición de
comando definir comando {
command_name notify-host-telegram
command_line / usr / bin / php / usr / local
/nagios/sbin/telegram-notify/telegram-bot.php "$
_CONTACTTELEGRAM" "83633434: kewkekekekdkkfiirrjririrjr" $
_HOSTSENDTELEGRAM $ "Notificar: $ NOTIFICATIONTYPE $ 0XzXZ0 $
HOSTX $ HOSTX $ Fecha: $ 0XZPZUTX "
}
```

3.2. ANÁLISIS Y PRESENTACIÓN DE DATOS

3.2.1. COMPARATIVA NAGIOS – VS. ANTES Y DESPUÉS DE LA HERRAMIENTA

En la presente investigación se logró identificar cuadros generales en comparativa del ipso facto y con el uso de herramienta, para lo cual fue necesario identificar y conocer el significado de los colores que mostraban los estados de servicios y áreas, la siguiente tabla (tabla 6) muestra de los colores de la alerta y la descripción que se usó en la investigación.

Tabla 7 Tipo de Alerta y descripción

ALERTA	DESCRIPCIÓN
Down	No se cuenta con conectividad a la red.
Critical	El servicio tiene valores iguales o superiores al valor establecido como crítico.
Warning	El servicio tiene valores superiores al valor percibido como aceptable.
Unknown	El servicio está oscilando entre estados.
Ok	El servicio monitoreado ha recuperado la conectividad.
Up	El servicio monitoreado tiene conectividad a la red.

Fuente: Elaboración propia

A continuación, se detalla los cambios significativos que se dieron usando la herramienta Nagios, en cada imagen se verá una comparativa de los resultados mostrados por Nagios en el ipso facto (recuadro rojo) de configurada la herramienta y luego del tiempo de prueba (recuadro gris).

- La siguiente imagen (Ilustración 66) la agrupación de áreas y los servicios monitoreados respectivamente, la principal diferencia que se encontró fue, como lo muestra el cuadro rojo, que inicialmente los servicios de Linux y MySql se encontraban en un estado “Down” con 7 servicios en estado crítico, luego de atender los incidentes y gracias al reporte oportuno de los mismos, el cuadro gris muestra las 5 áreas en estado “Up”, y solo con un servicio crítico en Linux, la similitud en ambos cuadros se dio en las áreas de Network switches, ya que según se evaluó con el Usuario, se determinó que existen ciertas fallas de hardware que se relacionan a estos incidentes, sin embargo en el estado general se mostró como UP ya que se mantuvo una correcta conectividad con el ping de los switchs.

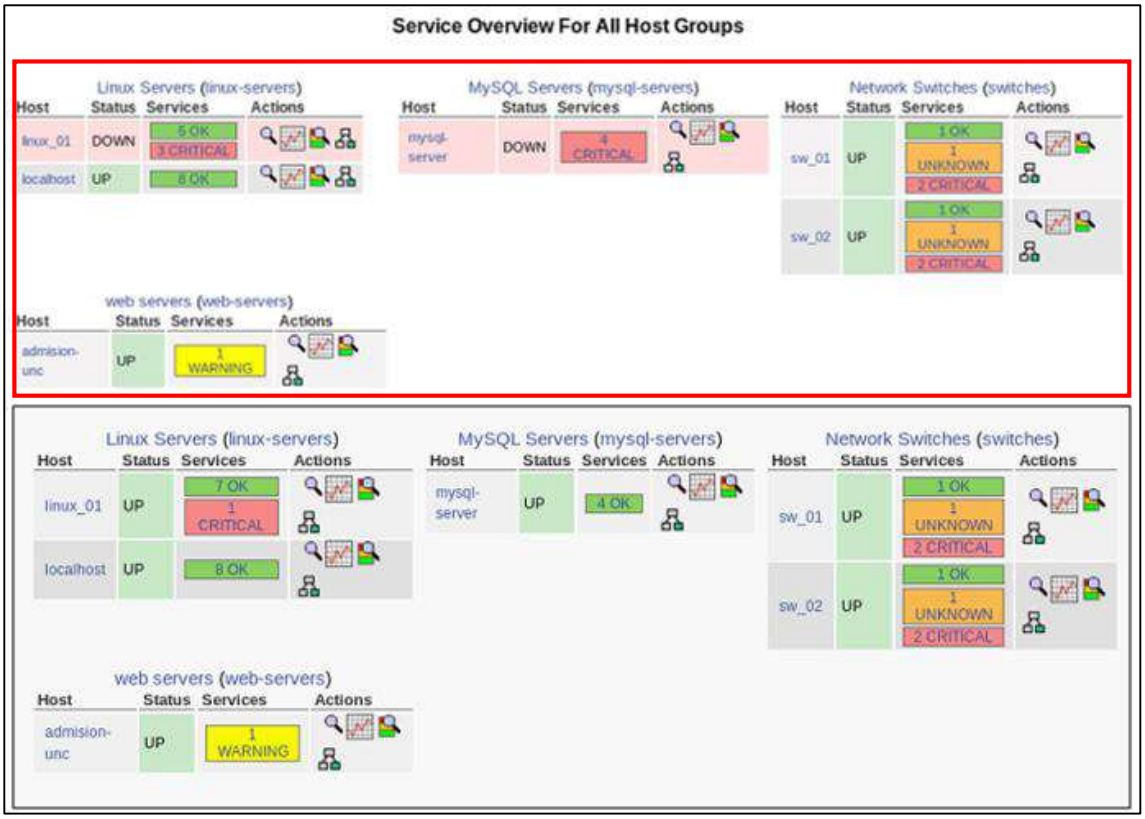


Ilustración 65 Versus " Estados detallados según área " - Máquina UNC

- En la ilustración 67 se presenta una comparativa de áreas y servicios, el cuadro rojo (registro ipso facto) mostró que en el resumen “Estados totales de host” se identificó 2 áreas en estado “Down” considerados como 2 problemas y en el resumen “Estado total de servicios” hubo 11 servicios en estado crítico, 2 desconocidos y 1 servicio en estado warning, siendo estos a la vez ubicados como 14 problemas de los servicios en total, a diferencia del cuadro gris (registro después de control de incidentes) que mostró todas la áreas en estado “Up” sin ningún problema y 5 servicios en estado crítico, 2 desconocidos y 1 warning, reduciéndose en 6 problemas a los 14 encontrados inicialmente.

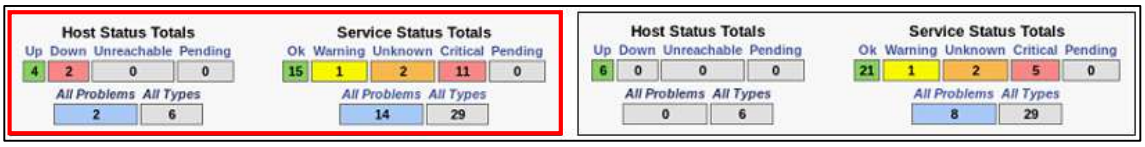


Ilustración 66 Versus “Estados detallados según riesgo total” – Máquina UNC

- Al igual que la ilustración anterior, la ilustración 68 muestra una comparación en los estados de los host o áreas evaluadas, el cuadro rojo muestra que hubieron 2 áreas en estado “DOWN” sin ser atendidas, a su derecha el cuadro gris refleja que las incidencias reportadas o encontradas en el primer monitoreo fueron resueltas, ya que los resultados que se registraron muestra a todas las áreas en estado “UP”, siendo prueba de que la herramienta resultó efectiva en la gestión de infraestructura de TI.

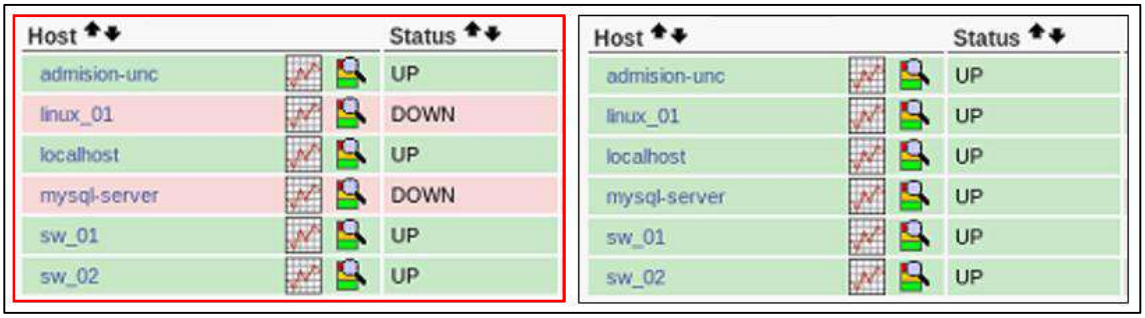


Ilustración 67 Versus “Estado de Áreas” – Máquinas UNC

3.2.1.1. Resumen estadístico PNP4nagios

PNP4Nagios, en esta investigación, permitió crear gráficos con diferentes parámetros de servicios en cada área o host, no fue necesario configurar los tiempos de monitoreo ya que nagios realizó esta acción de forma automáticamente a los servicios, la información se acumuló de gran manera

generando con el tiempo una data grande, PNP4Nagios permitió acceder con mayor rapidez y exactitud a dicha información.

3.2.1.1.1. Datos acumulados Área admisión

La data de admisión muestra a detalle la continuidad en el tiempo, los servicios, rangos de tiempo y los diferentes picos de visitas en el tiempo, que se realizaron al sitio web (Ilustración 69).

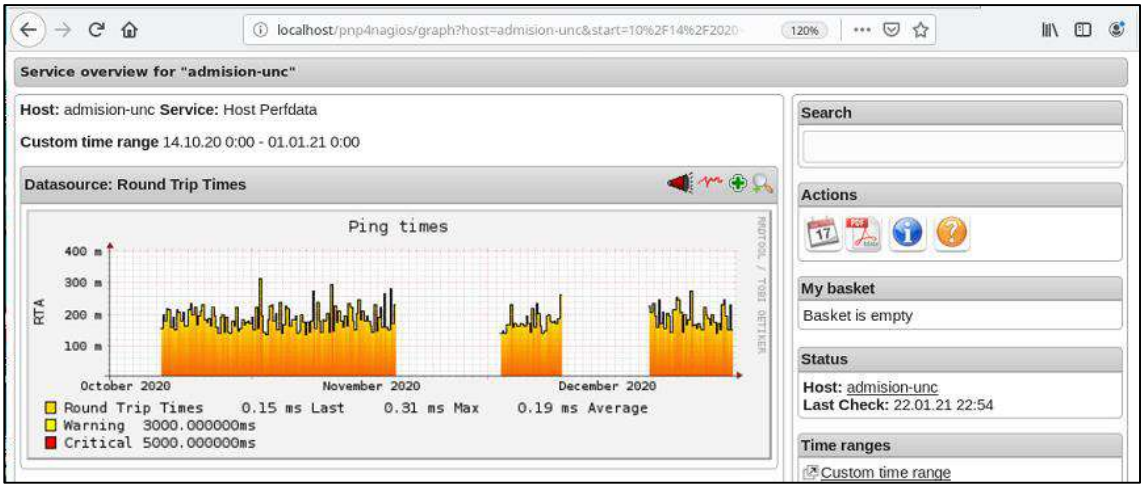


Ilustración 68 Gráfico resumen "ADMISIÓN" - Máquina UNC

- Nagios permite ver a detalle la disponibilidad que mostró el host evaluado y sus servicios, podemos observar los tiempos de respuesta (recuadro rojo) y como se clasificaron sobre los valores establecidos (Ilustración 65).

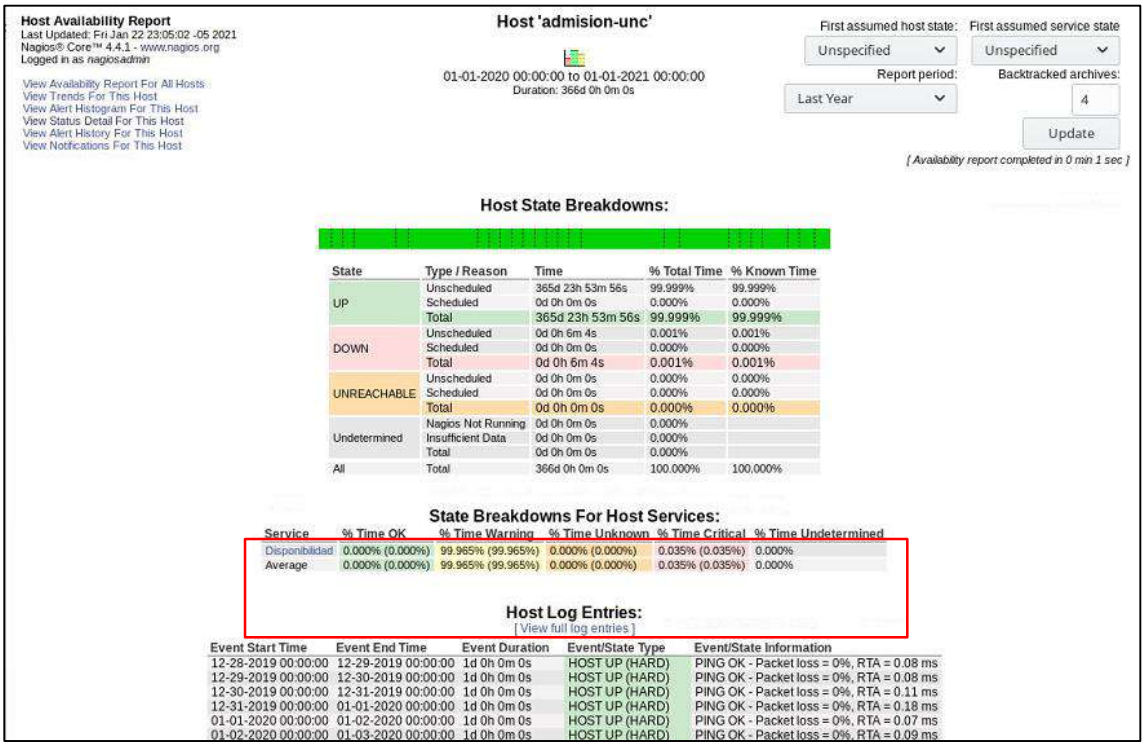


Ilustración 69 Reporte de disponibilidad "ADMISION" - Máquina UNC

- En el proceso de monitoreo, el almacenamiento se dio mediante archivos log (Ilustración 71), se permitió un rastreo diario de actividades y estado general del mismo, lo que ayudó a poder identificar con mayor exactitud cuándo fuese necesario localizar algún incidente o se deseó revisar el registro de actividades. El Archivo log está disponible de forma diaria o inmediata según la necesidad del usuario, cada registro se realiza de forma independiente por host monitoreado, y todo son almacenado mediante RRD data base, herramienta hecha sobre el concepto de Round- Robin, una base de datos orientada al almacenamiento de datos basado en series temporales.

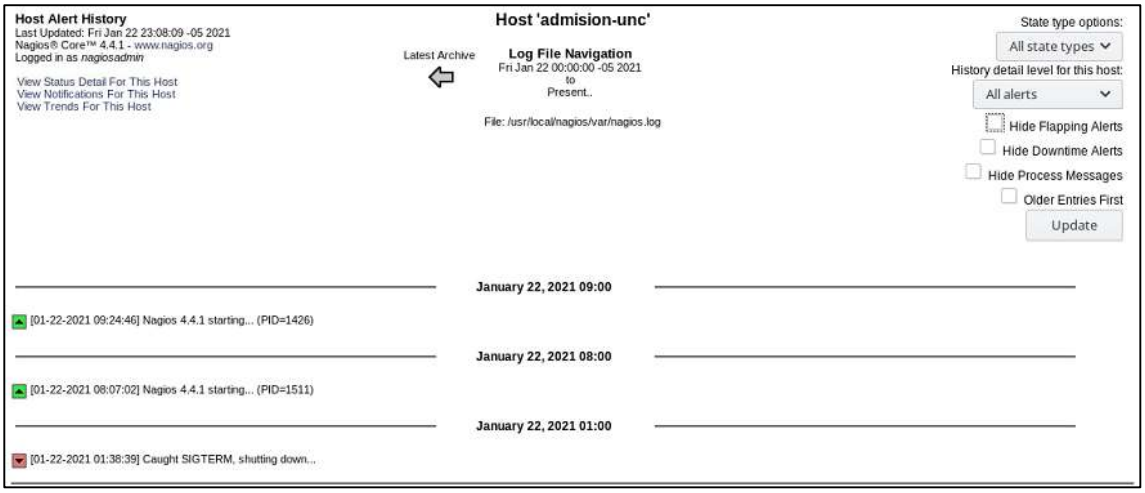


Ilustración 70 Archivo Log "ADMISIÓN" - Máquina UNC

- Finalmente se puedo observar (Ilustración 72) que los datos anteriores se resumen con la clasificación de los servicios del área admisión en warning, adicionalmente se mostró la última revisión del host y el tiempo de total de monitoreo con la información detallada del estado.

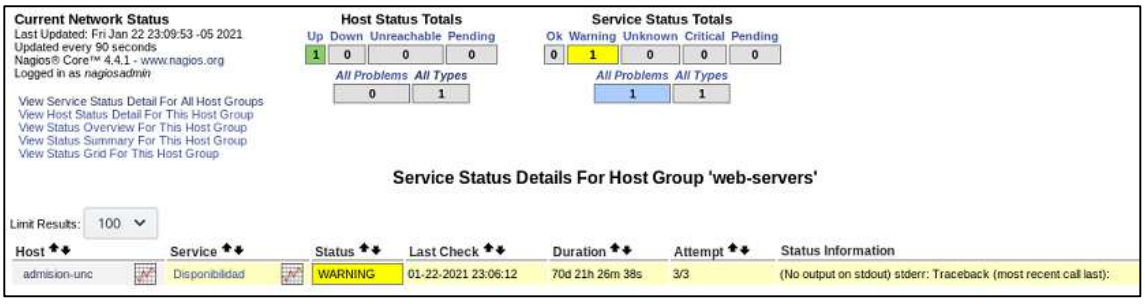


Ilustración 71 Estado Detallado "ADMISIÓN" - Máquina UNC

- PNP4Nagios permitió generar gráficos con filtros de tiempo establecidos, la Ilustración 73 muestra 5 gráficos de 4 horas, 25 horas, una semana, un mes y un año respectivamente, como se puede observar existen periodos donde

los picos son más altos como en el gráfico anual, también se pudo observar que a finales del mes de mayo de 2020 se tuvo una mayor visita de la web, al mismo tiempo se puede determinar que existió un manejo grande de información.

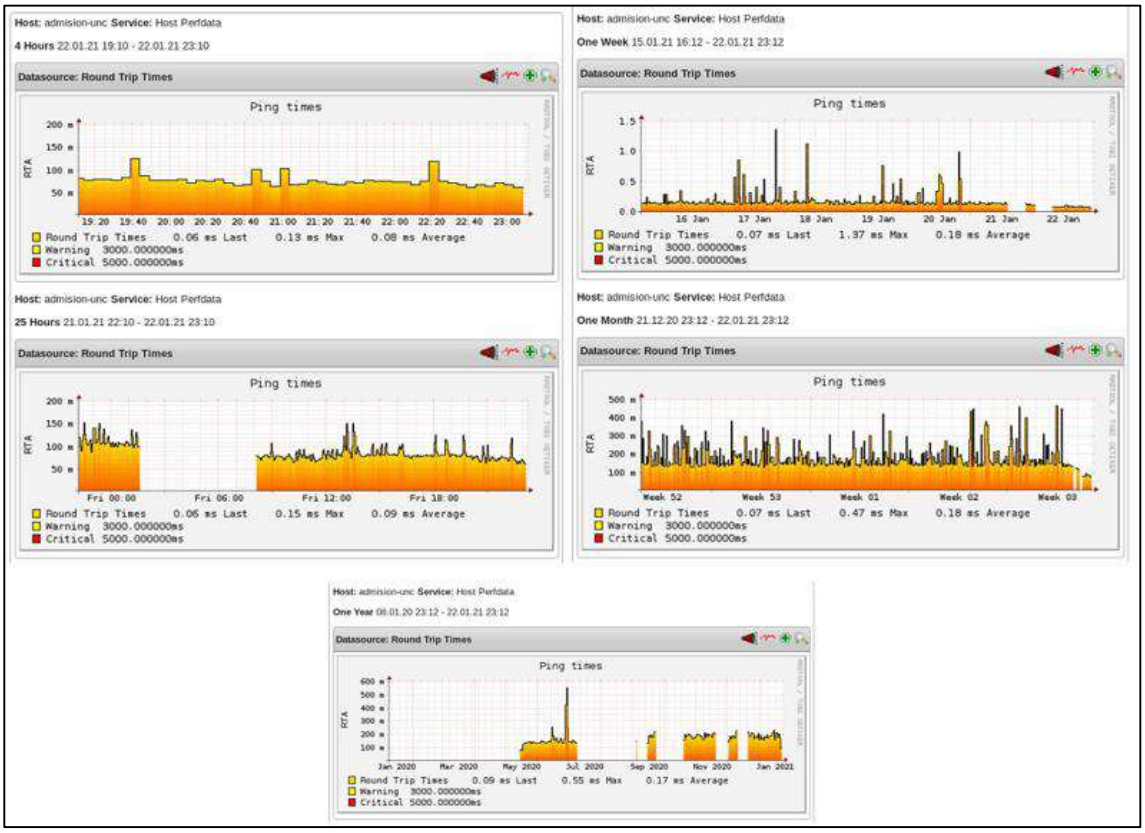


Ilustración 72 Reporte "ADMISIÓN" NP4Nagios en: 4 horas, 25 horas, una semana, un mes, un año.

3.2.1.1.2. Linux

La data de linux mostró a detalle la continuidad en el tiempo, los servicios a monitorear (Ilustración 74), rangos de tiempo y los diferentes picos de visitas que se realizaron al host de Linux.

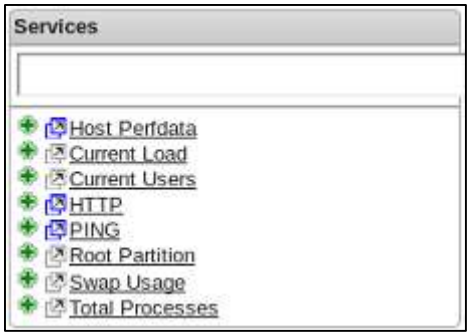


Ilustración 73 Servicios medibles de LINUX en PNP4Nagios

- Nagios permitió ver a detalle la disponibilidad del host evaluado y sus servicios, se pudo observar los tiempos de respuesta (recuadro rojo) y como se clasificaron sobre los valores establecidos (Ilustración 75).

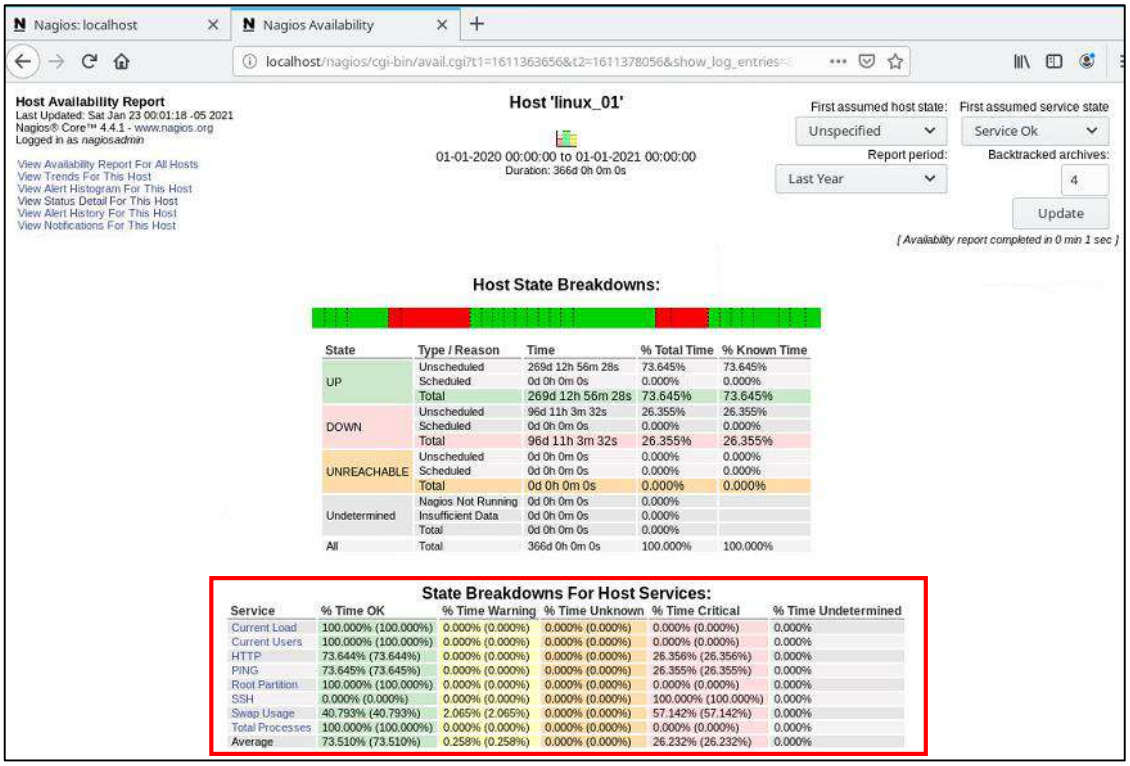


Ilustración 74 Reporte de disponibilidad "LINUX" - Máquina UNC

- PNP4Nagios permitió generar gráficos según filtros de tiempo, las ilustraciones 76 y 77 muestran 5 gráficos de 2 meses, 25 horas, una semana, un mes y un año respectivamente, como se puede observar existen periodos donde no hubo actividad (gráfico de 25 horas) y los otros gráficos muestran que existió picos muy elevados registrados a fines de junio de 2020, al mismo tiempo se puede determinar que existió un manejo grande de información.

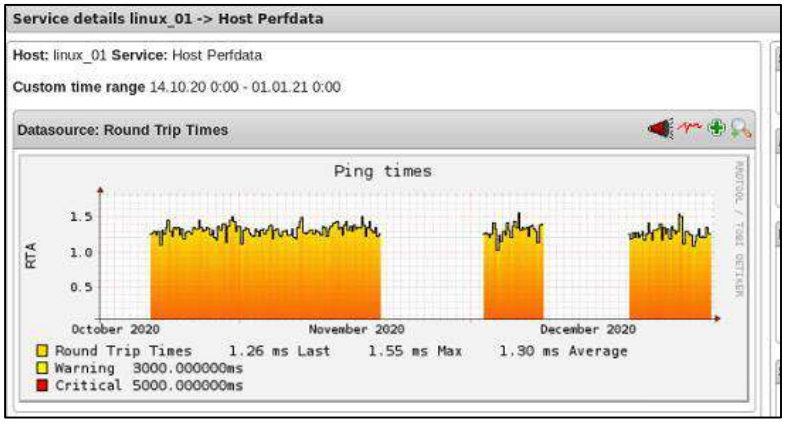


Ilustración 75 Gráfico 1 resumen "LINUX" - Máquina UNC

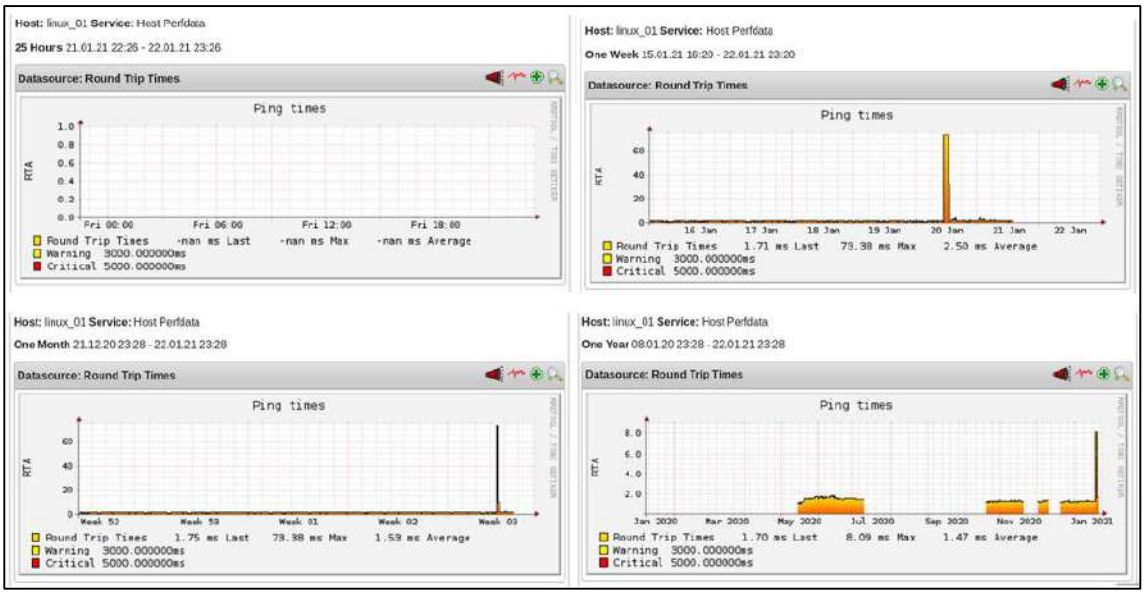


Ilustración 76 Reporte "LINUX" NP4Nagios en: 25 horas, una semana, un mes, un año.

- En las ilustraciones 78 y 79 se muestran 6 gráficos de 2 meses, 4 horas, 25 horas, una semana, un mes y un año respectivamente, en los cuales se observa que hubo periodos interrumpidos de data y al mismo tiempo se registraron de forma pareja la información, es decir sin picos elevados o resaltantes.

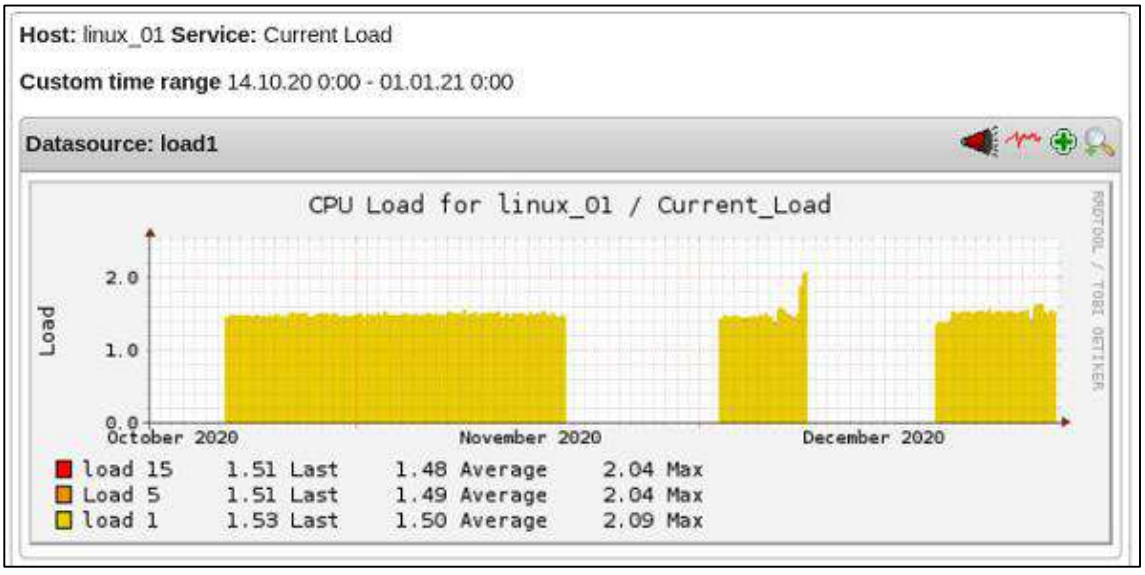


Ilustración 77 Gráfico "Carga Actual" resumen "LINUX" - Máquina UNC

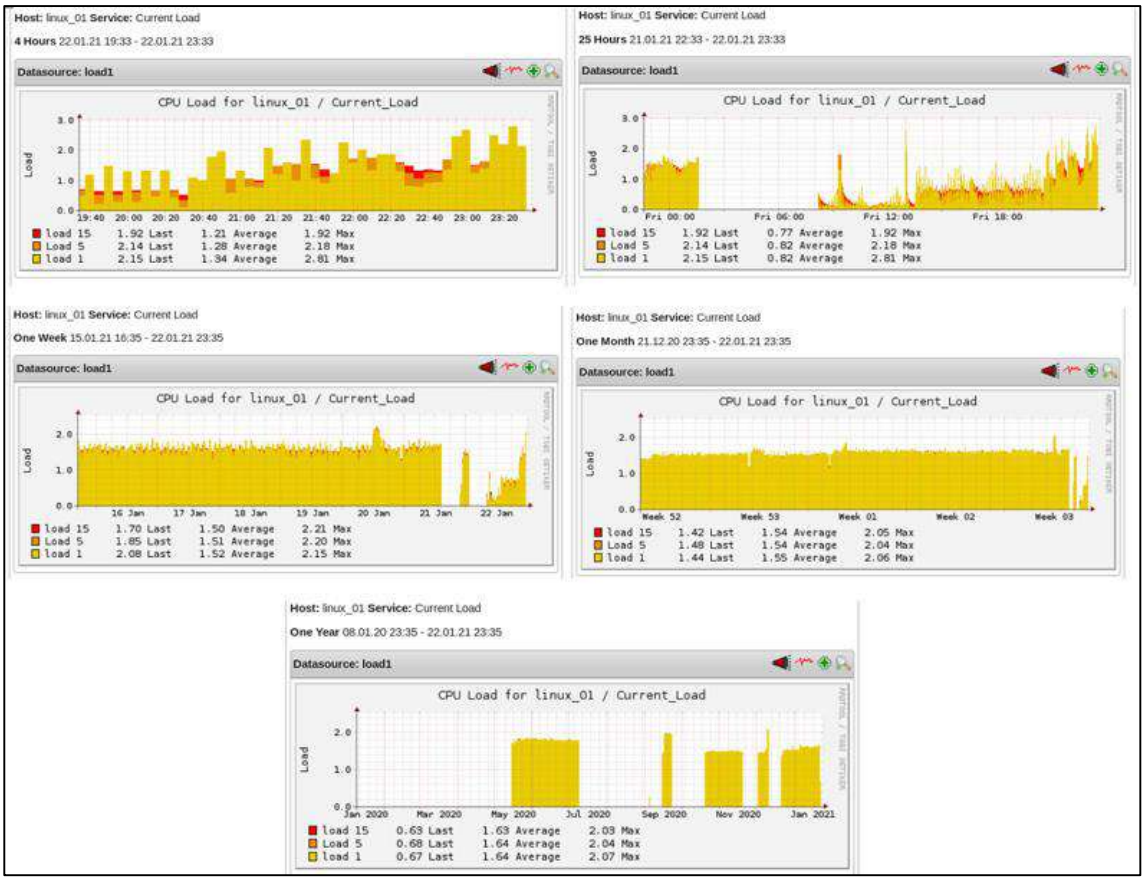


Ilustración 78 Reporte "LINUX – Carga Actual" NP4Nagios en: 25 horas, una semana, un mes, un año.

- En las ilustraciones 80 y 81 se muestran 6 gráficos de 2 meses, 4 horas, 25 horas, una semana, un mes y un año respectivamente, existieron periodos interrumpidos de data y al mismo tiempo registros parejos de usuarios hasta setiembre de 2020 y a continuación disminuyó el nivel en comparativa a meses anteriores, pero igual se mostró estable.

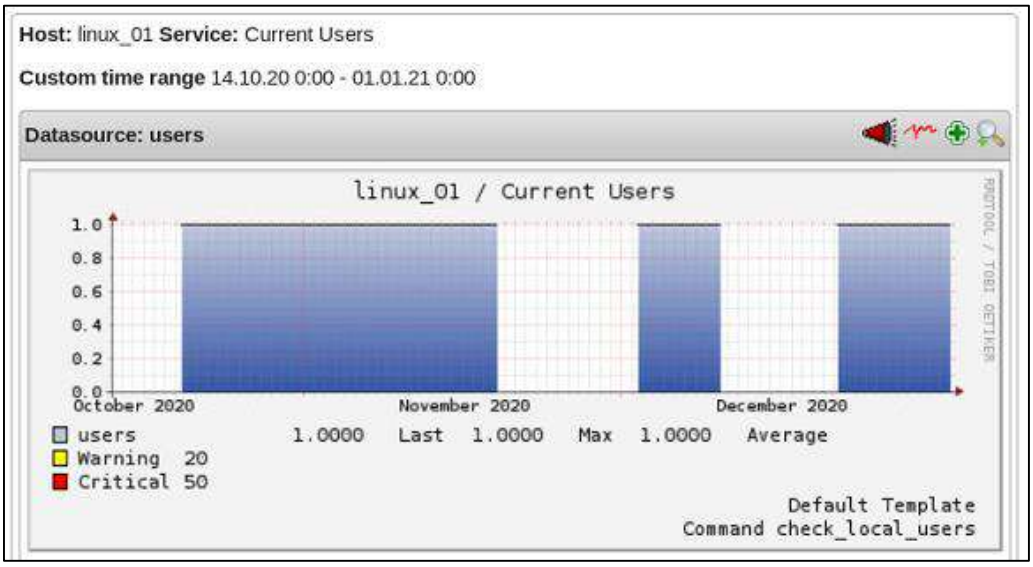


Ilustración 79 Gráfico "Usuarios" resumen "LINUX" - Máquina UNC

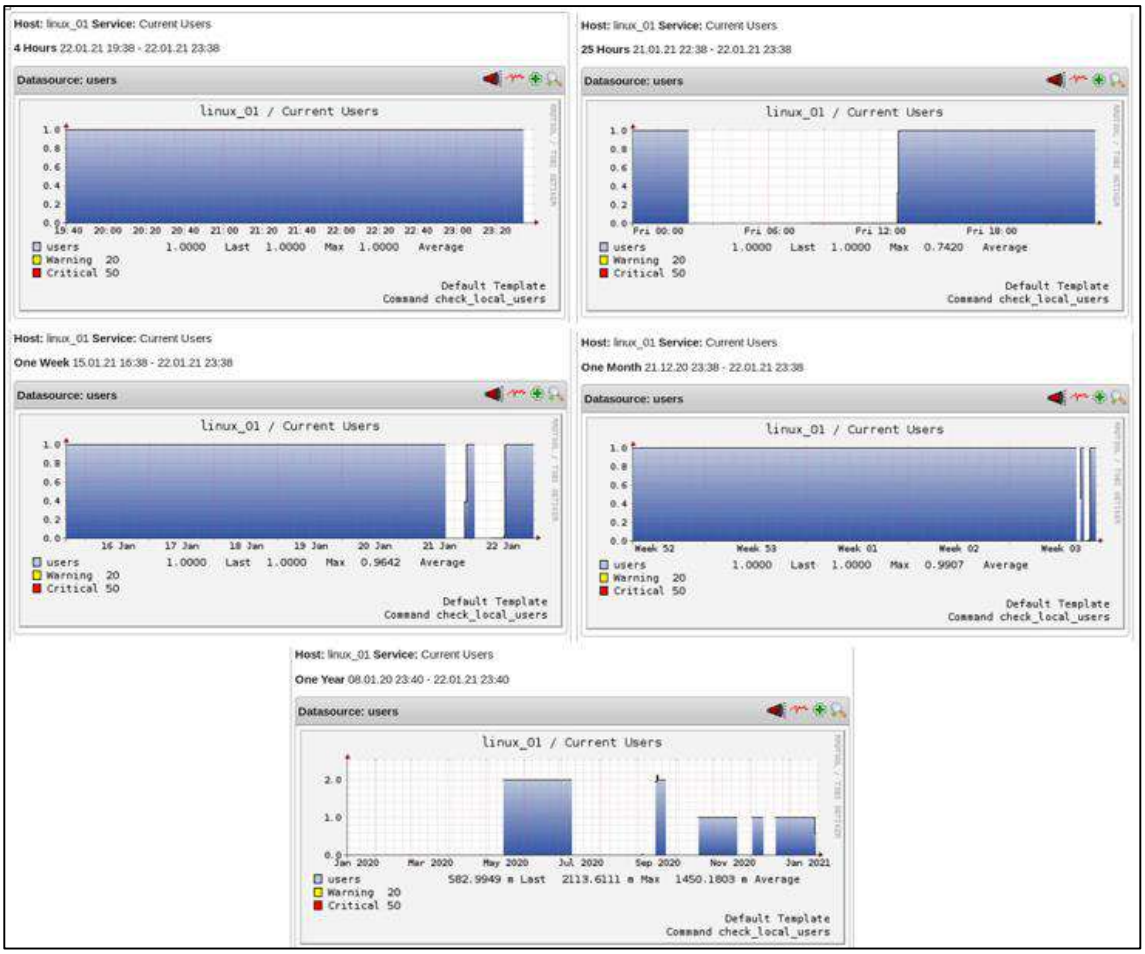


Ilustración 80 Reporte "LINUX – Usuarios" NP4Nagios en: 25 horas, una semana, un mes, un año.

- En las ilustraciones 82 y 83 se muestran 4 gráficos de 2 meses, una semana, un mes y un año respectivamente, se evidencia que existieron periodos interrumpidos de data y al mismo tiempo registros parejo de usuarios en los periodos de continuidad, significando que el monitoreo a la conexión http se mantuvo estable.

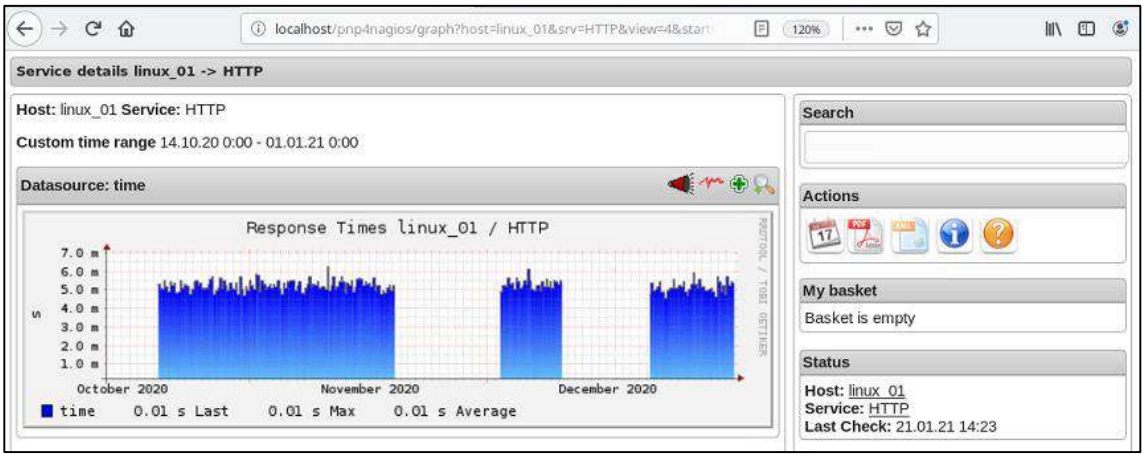


Ilustración 81 Gráfico "HTTP" resumen "LINUX" - Máquina UNC

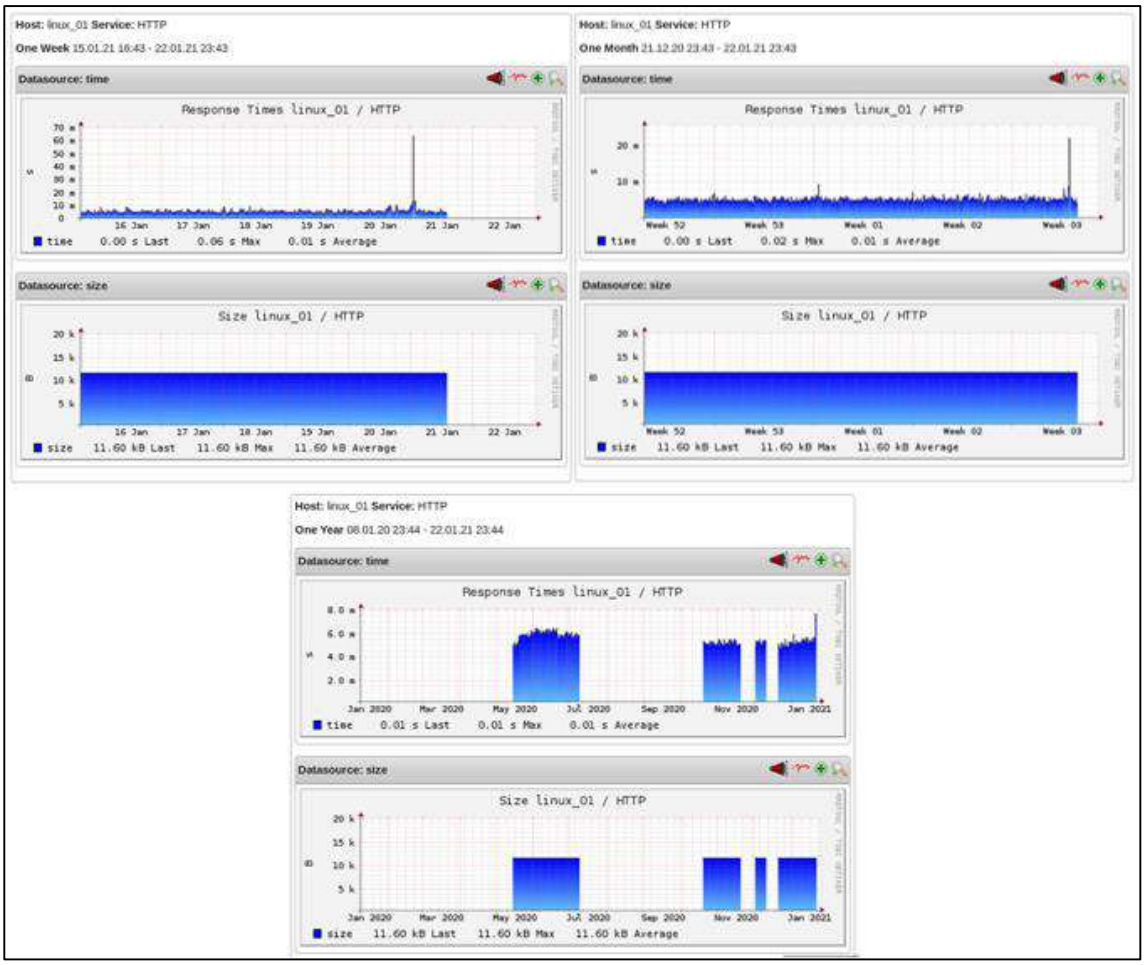


Ilustración 82 Reporte "LINUX – HTTP" NP4Nagios en: una semana, un mes, un año.

- En las ilustraciones 84 y 85 se muestran 5 gráficos de 2 meses, 25 horas, una semana, un mes y un año respectivamente, se evidencia que hubo periodos interrumpidos de data y al mismo tiempo muestra un registro parejo de usuarios en los periodos de continuidad, significando que el monitoreo a la conexión http se mantuvo estable en los tiempos activos.

Ilustración 83 Gráfico "PING" resumen "LINUX" - Máquina UNC

Ilustración 84 Reporte "LINUX – PING" NP4Nagios en: 4 horas, una semana, un mes, un año.

- En las ilustraciones 86 y 87 se muestran 6 gráficos de 2 meses, 4horas, 25 horas, una semana, un mes y un año respectivamente, como se puede observar existieron periodos continuos de monitoreo a la partición raíz, las líneas verde, amarilla y roja muestran la constante evaluación que hubo del size, warning y critical, según detalla la leyenda.

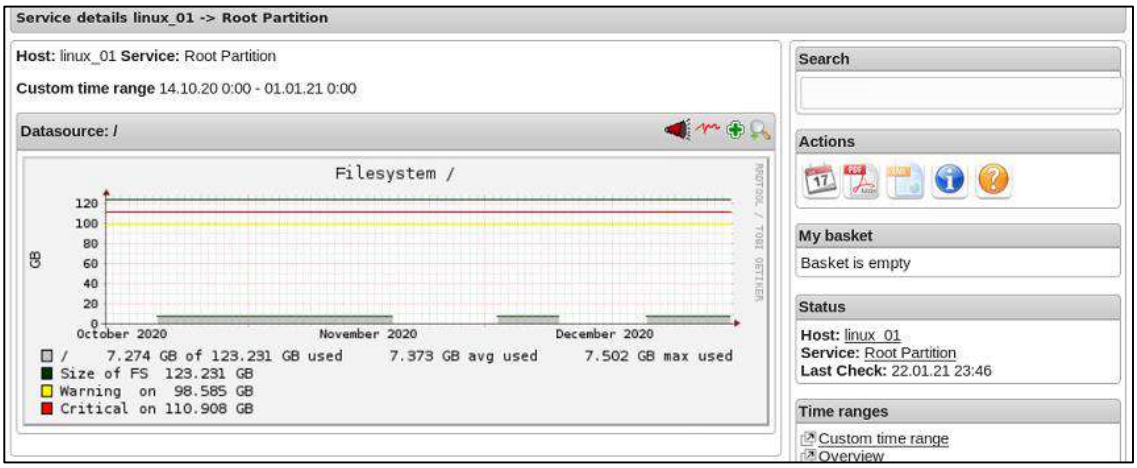


Ilustración 85 Gráfico "Partición" resumen "LINUX" - Máquina UNC

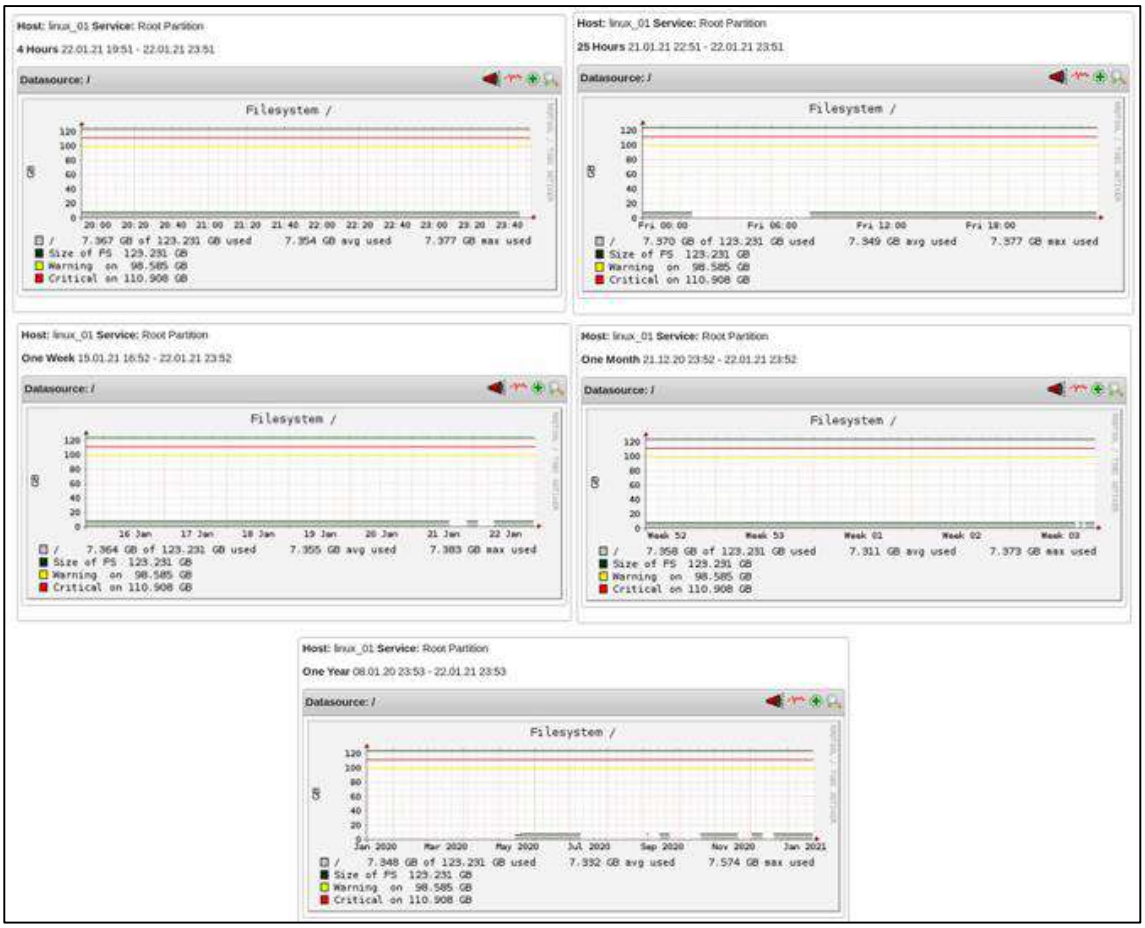


Ilustración 86 Reporte "LINUX – Partición" NP4Nagios en: 4 horas, 25 horas, una semana, un mes, un año.

- En las ilustraciones 88 y 89 se muestran 6 gráficos de 2 meses, 4horas, 25 horas, una semana, un mes y un año respectivamente, se observa que hubo periodos interrumpidos de acciones de intercambio y también que los registros del size, Warning y critical se mantuvieron activos constantemente, se hace referencia a las líneas verde, amarilla y roja detalladas en la leyenda inferior del gráfico.

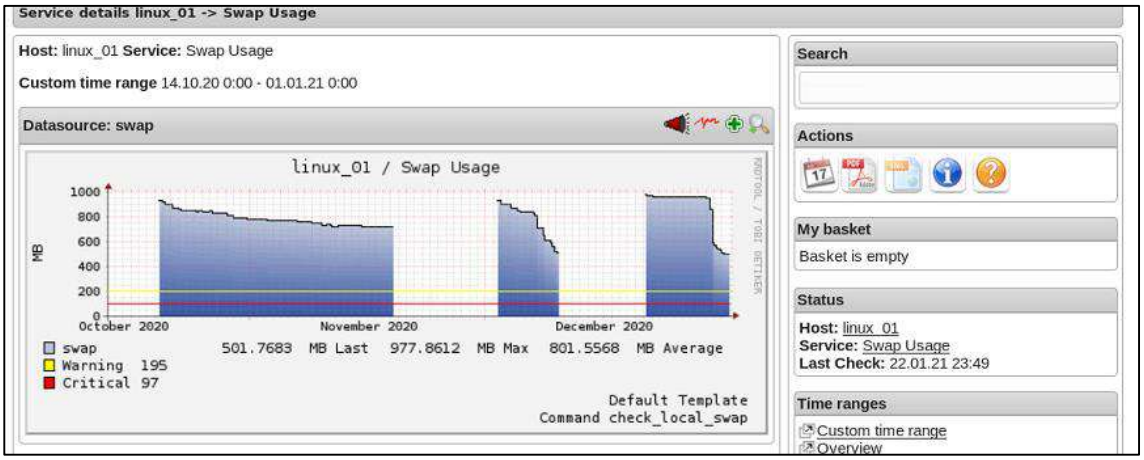


Ilustración 87 Gráfico "Swap Usage" resumen "LINUX" - Máquina UNC

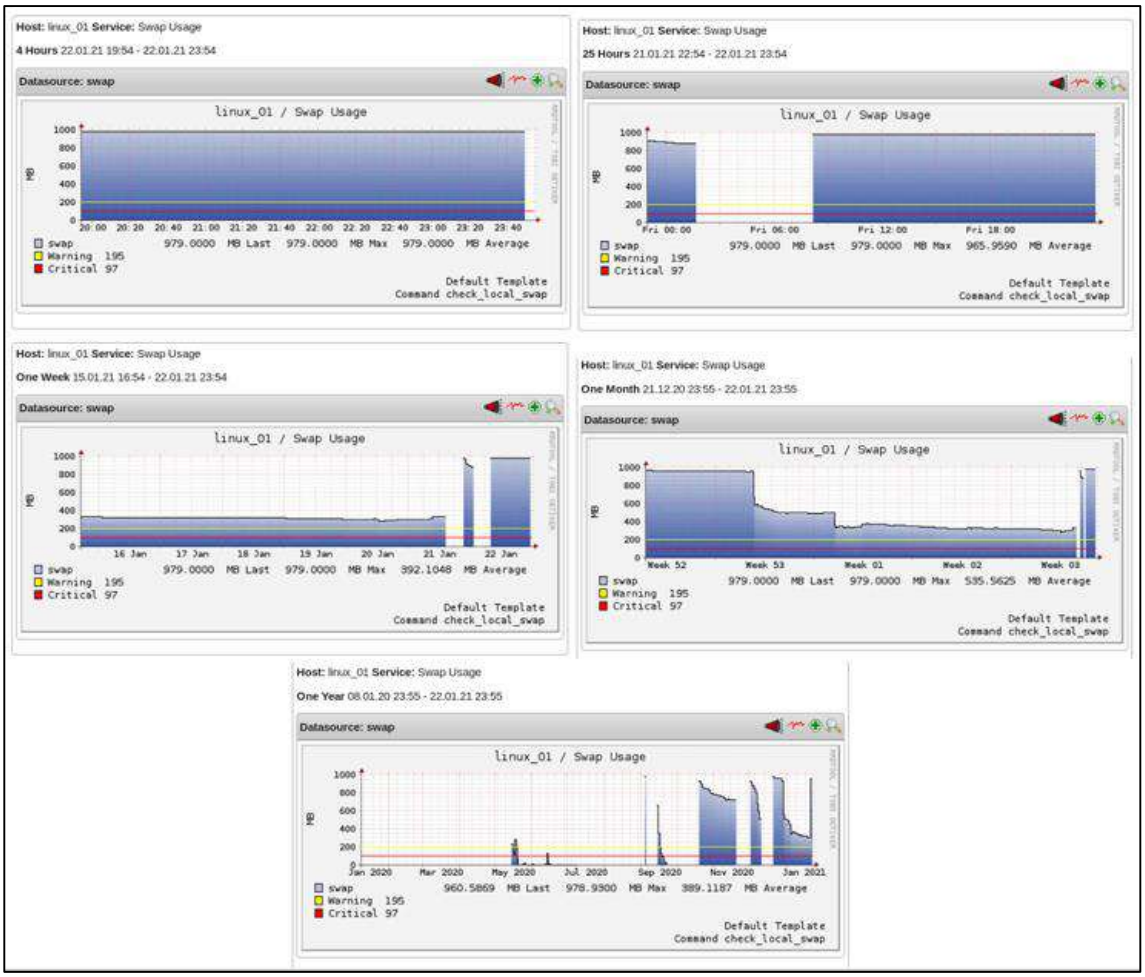


Ilustración 88 Reporte "LINUX – Swap Usage" NP4Nagios en: 4 horas, 25 horas, una semana, un mes, un año.

- En las ilustraciones 90 y 91 se muestra evidencia que hubo registros interrumpidos de los procesos totales en todo el proceso, según las 6 gráficas de 2 meses, 4horas, 25 horas, una semana, un mes y un año respectivamente.

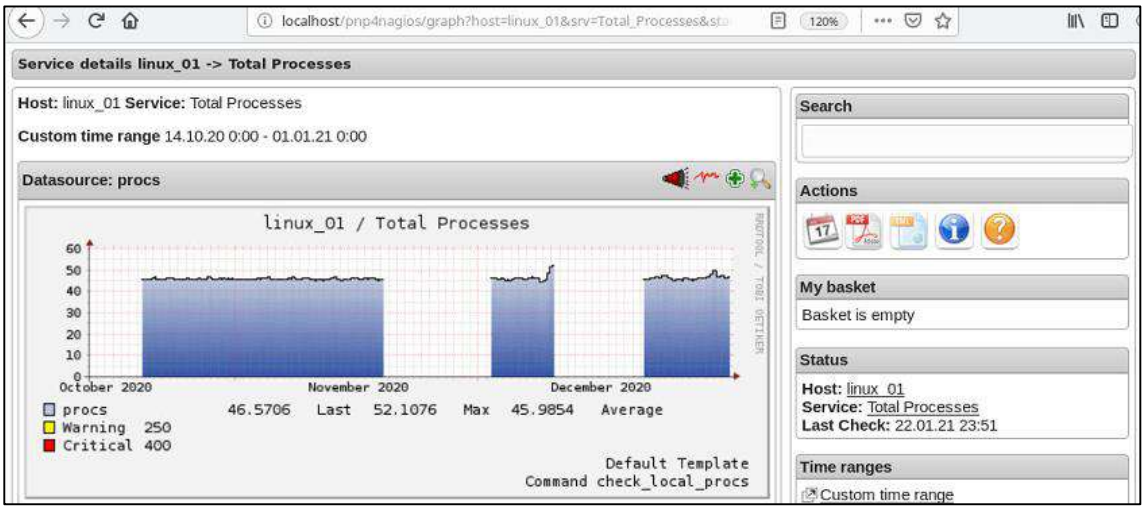


Ilustración 89Gráfico "Procesos Totales" resumen "LINUX" - Máquina UNC

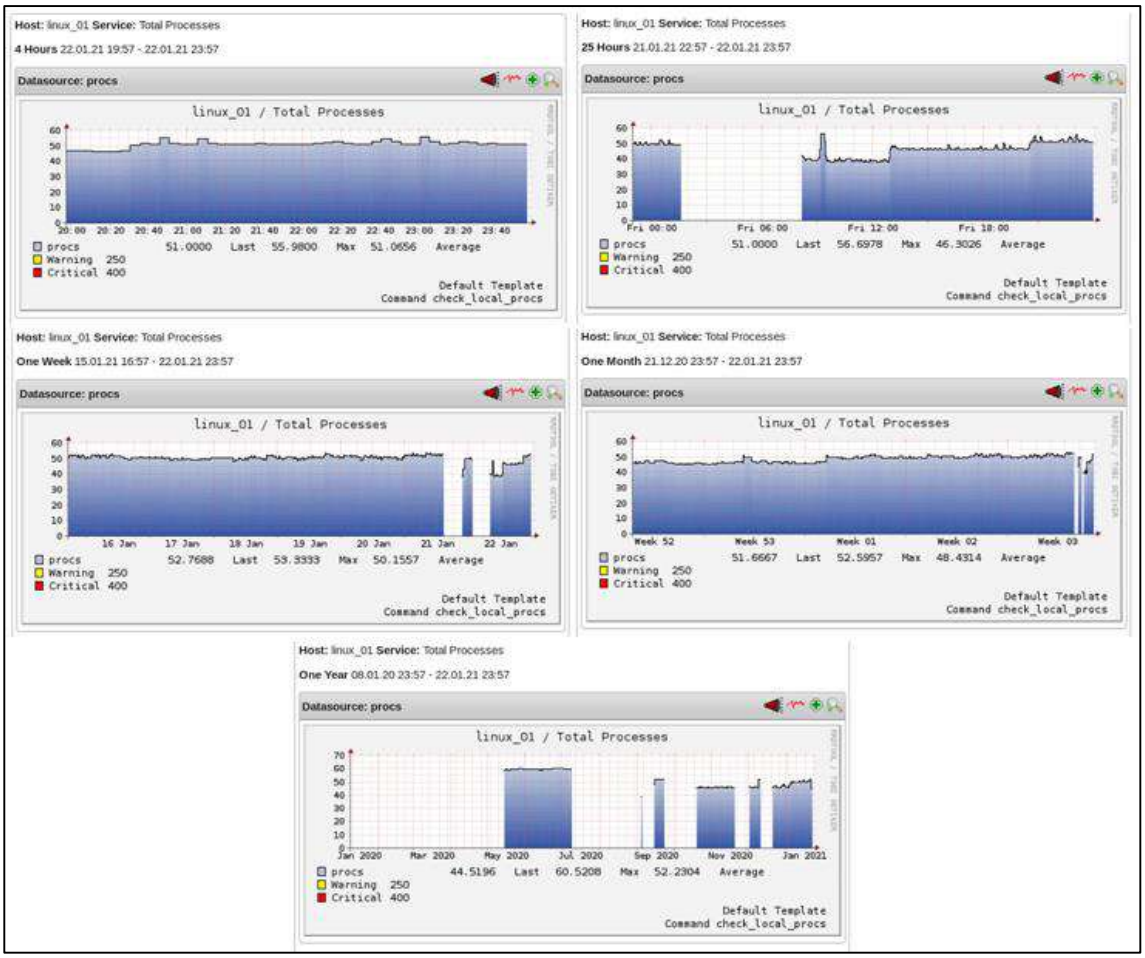


Ilustración 90 Reporte "LINUX – Procesos Totales" NP4Nagios en: 4 horas, 25 horas, una semana, un mes, un año.

4.1.4.3.1. Local Host

- En el monitoreo de local host se obtuvo 6 gráficos de 2 meses, 4horas, 25 horas, una semana, un mes y un año respectivamente, con evidencia de que se dieron picos altos de frecuencia del servicio con tiempos interrumpidos (Ilustración 92 y 93).

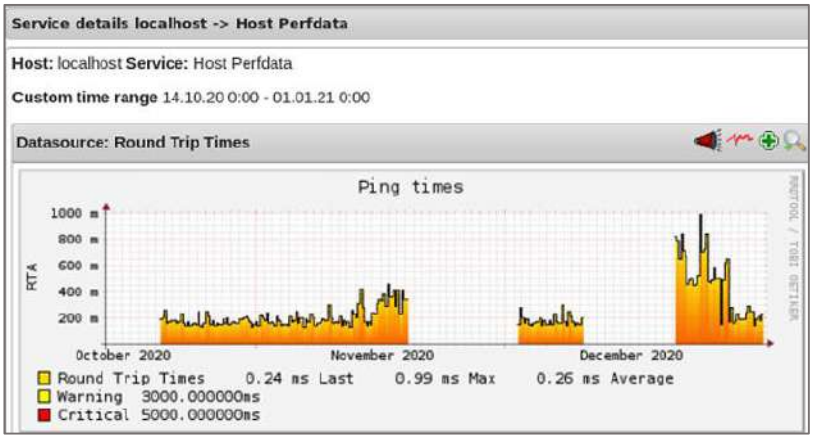


Ilustración 91 Gráfico resumen "Localhost" - Máquina UNC

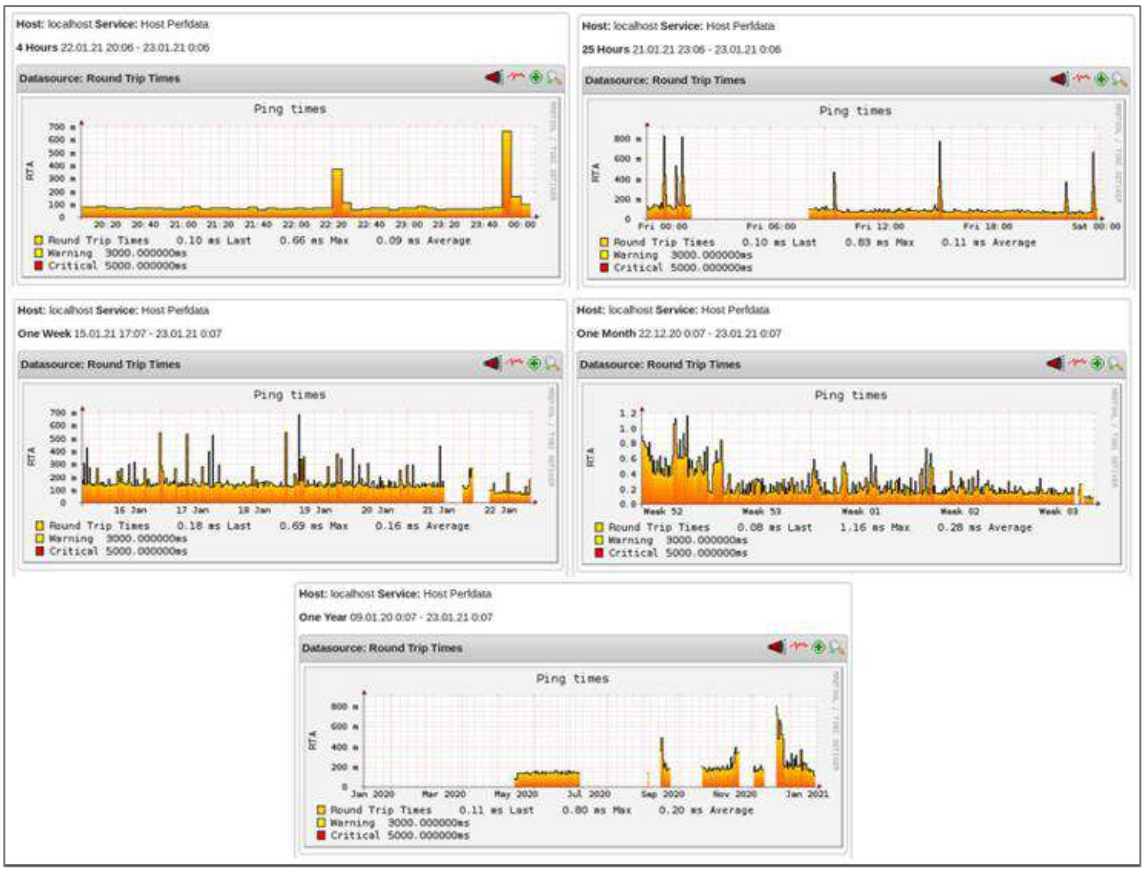


Ilustración 92 Reporte "Localhost" NP4Nagios en: 4 horas, 25 horas, una semana, un mes, un año.

- En las ilustraciones 94 y 95 se muestran 6 gráficos de 2 meses, 4horas, 25 horas, una semana, un mes y un año respectivamente, en las cuales muestra que hubo tiempos interrumpidos de data y al mismo tiempo una data homogénea de registros en los tiempos de continua actividad de carga actual (current load).

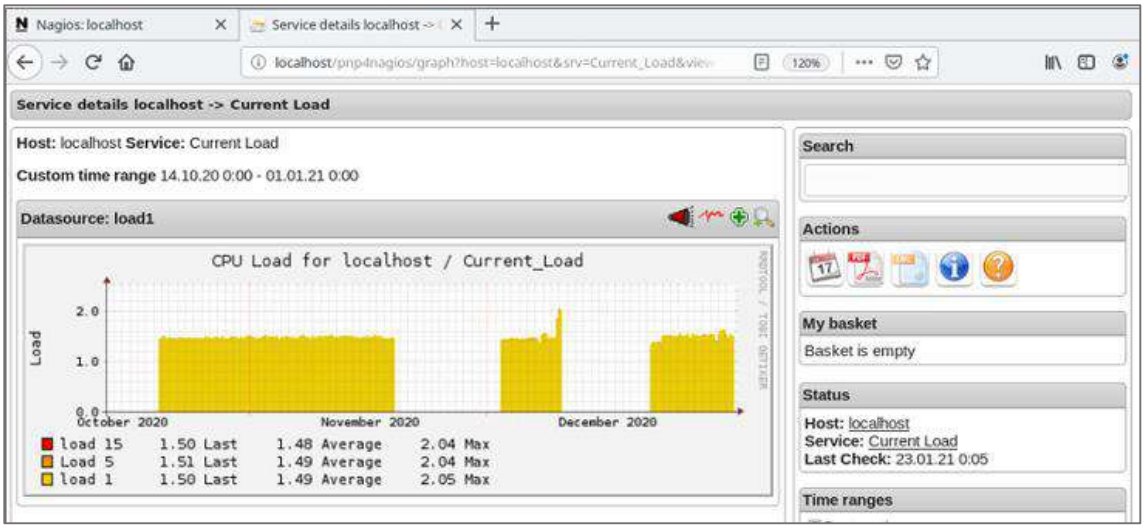


Ilustración 93 Gráfico "Carga Actual" resumen "Localhost"- Máquina UNC

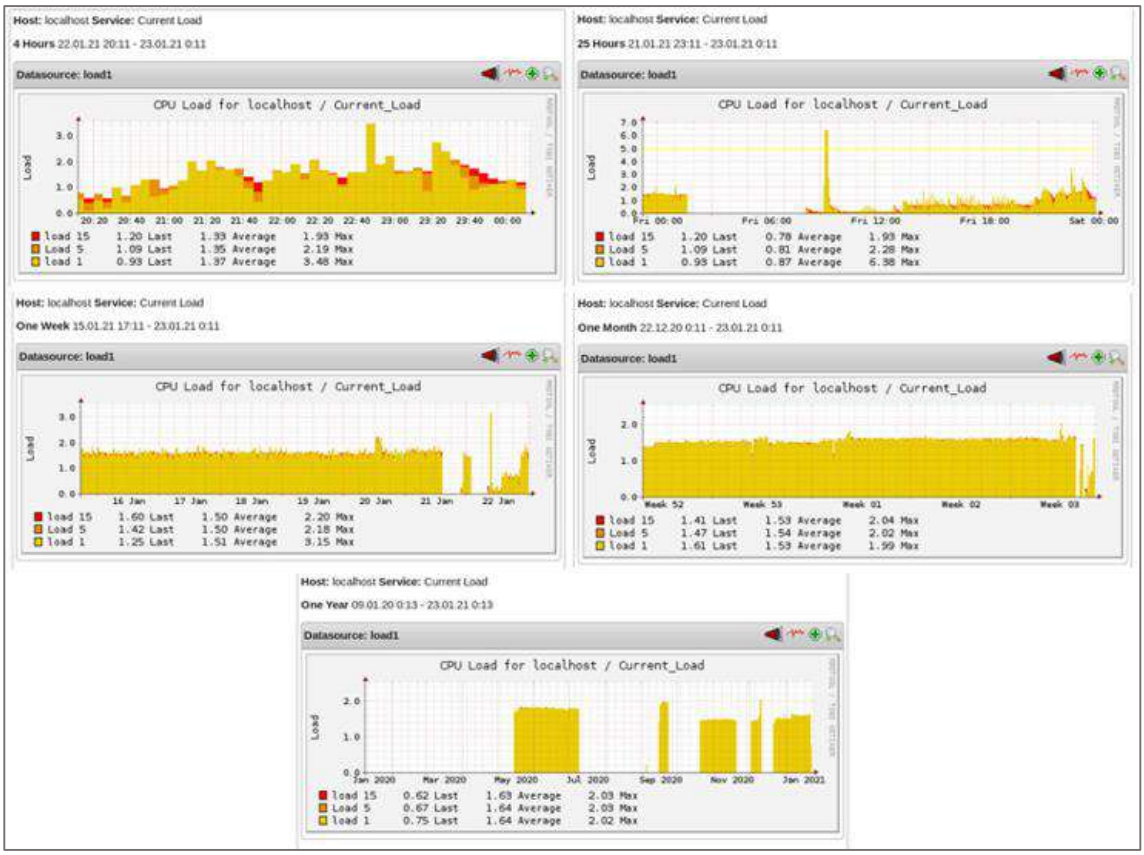


Ilustración 94 Reporte "Localhost - Carga Actual " NP4Nagios en: 4 horas, 25 horas, una semana, un mes, un año.

- En las ilustraciones 96 y 97 se muestran 6 gráficos de 2 meses, 4horas, 25 horas, una semana, un mes y un año respectivamente, se muestra que existió frecuente actividad de los usuarios, muestra que se dieron tiempos interrumpidos con un registro constante hasta setiembre de 2020, disminuyendo proporcionalmente en adelante.

Ilustración 95 Gráfico "Usuarios" resumen "Localhost"- Máquina UNC

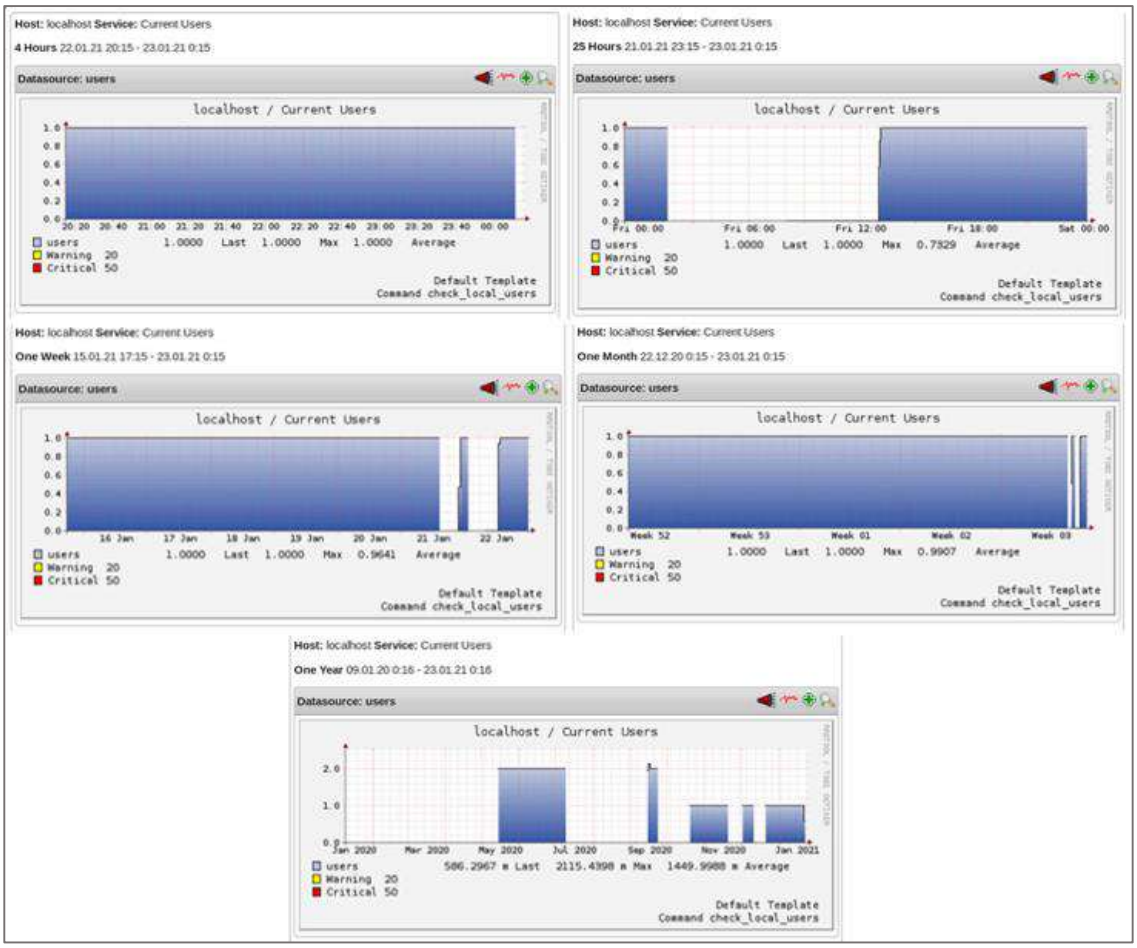


Ilustración 96 Reporte "Localhost - Usuarios " NP4Nagios en: 4 horas, 25 horas, una semana, un mes, un año.

- En las ilustraciones 98 y 99 se muestran 4 gráficos de 2 meses, una semana, un mes y un año respectivamente, se observan que en el tiempo de prueba se dieron periodos interrumpidos de data y al mismo tiempo muestra picos altos en los periodos de continuidad.

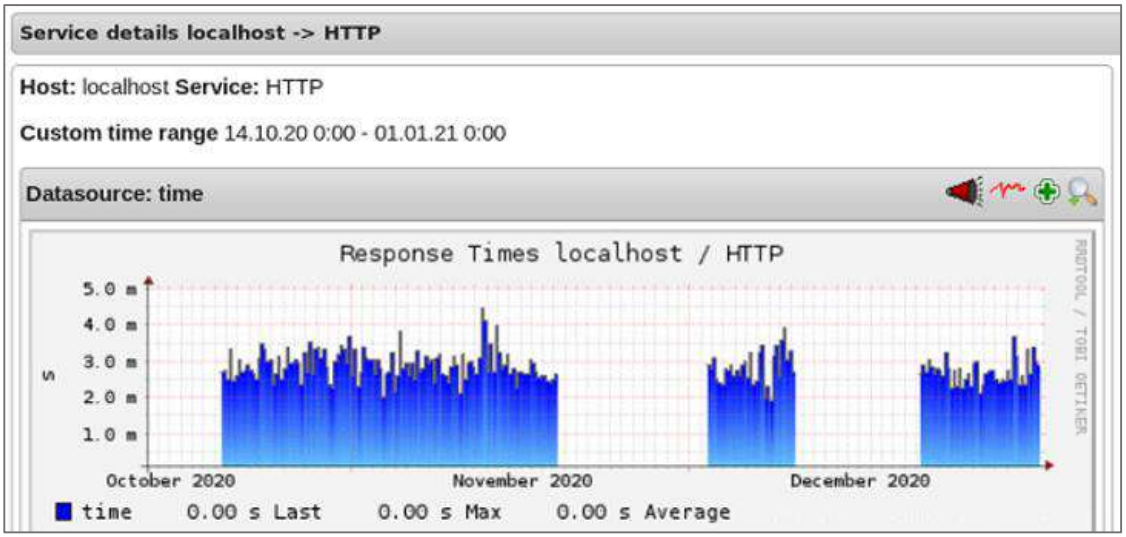


Ilustración 97 Gráfico "HTTP" resumen "Localhost"- Máquina UNC

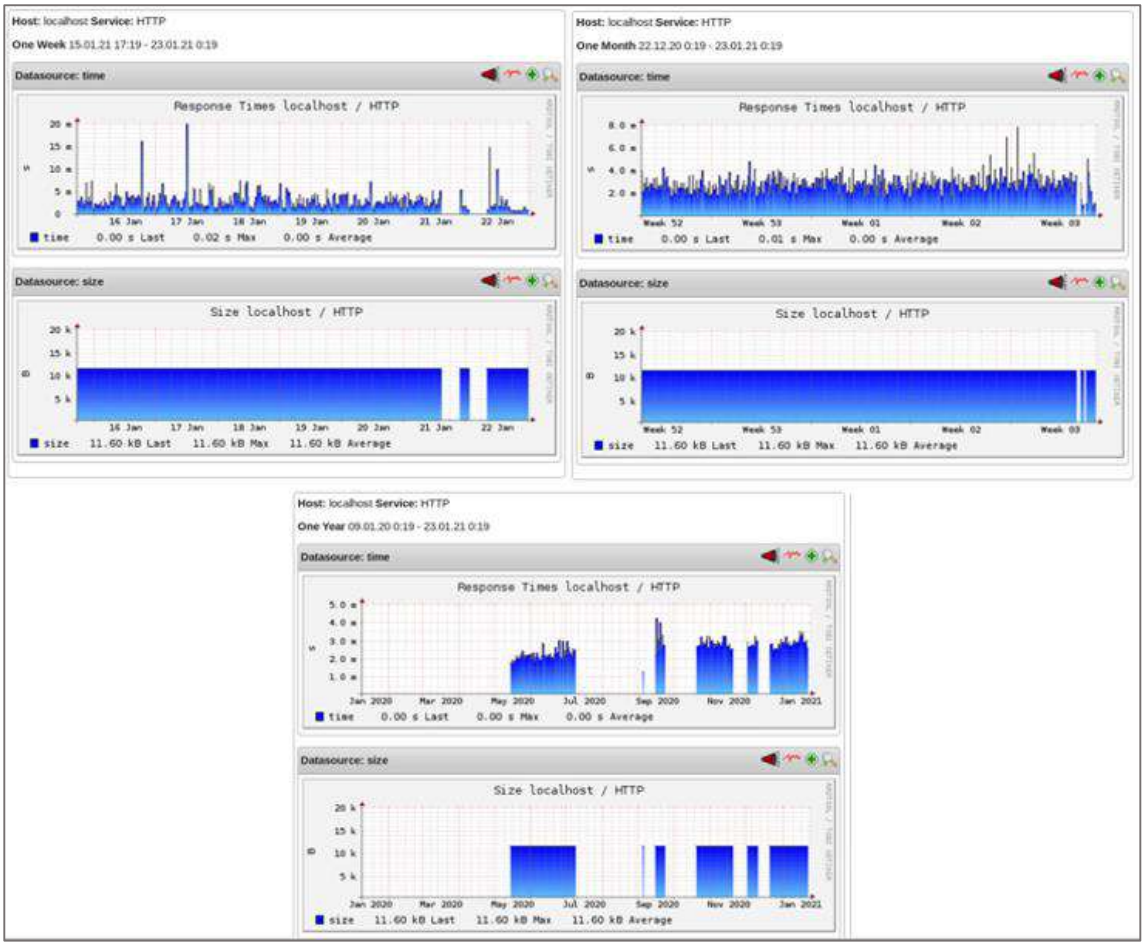


Ilustración 98 Reporte "Localhost - HTTP" NP4Nagios en: una semana, un mes, un año.

- En las ilustraciones 100 y 101 se muestran 6 gráficos de 2 meses, 4 horas, 25 horas, una semana, un mes y un año respectivamente, hay una data muy variable con diferentes picos registrados del ping hacia el local host, de la misma forma hay discontinuidad en los registros que se obtuvieron.

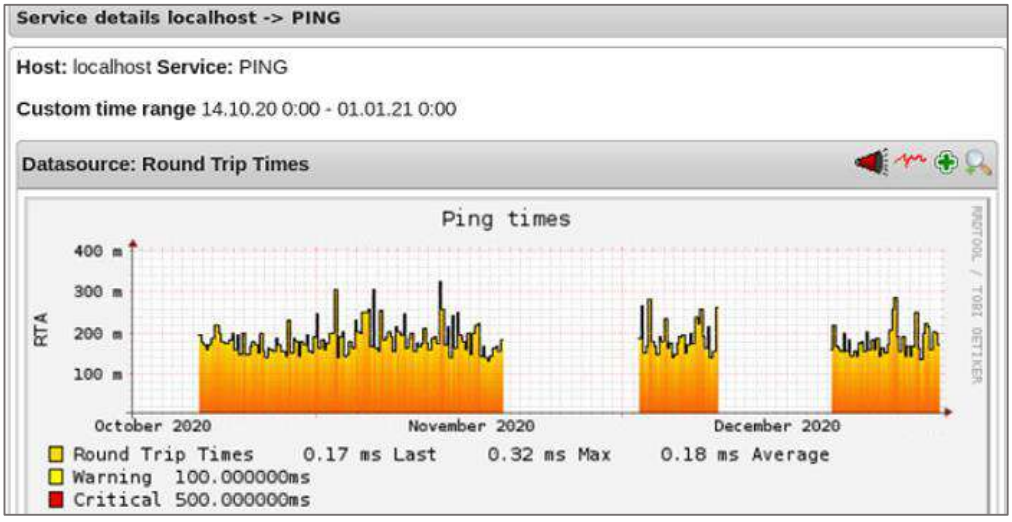


Ilustración 99 Gráfico "PING" resumen "Localhost"- Máquina UNC

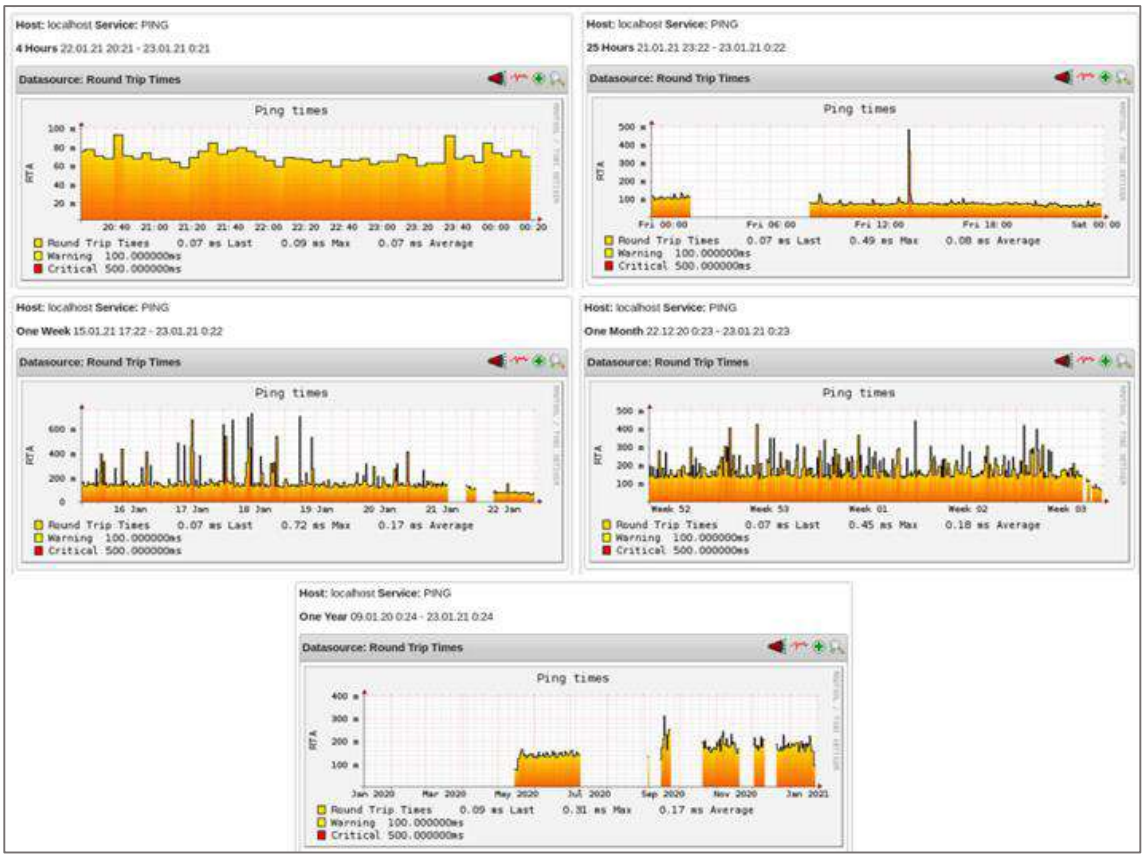


Ilustración 100 Reporte "Localhost - Ping" NP4Nagios en: 4 horas, 25 horas, una semana, un mes, un año.

- En las ilustraciones 102 y 103 se muestran 6 gráficos de 2 meses, 4horas, 25 horas, una semana, un mes y un año respectivamente, como se puede observar se dieron periodos continuos de monitoreo a la partición raíz, las líneas verde, amarilla y roja muestran la constante evaluación del size, warning y critical, en el tiempo de prueba, según detalla la leyenda.

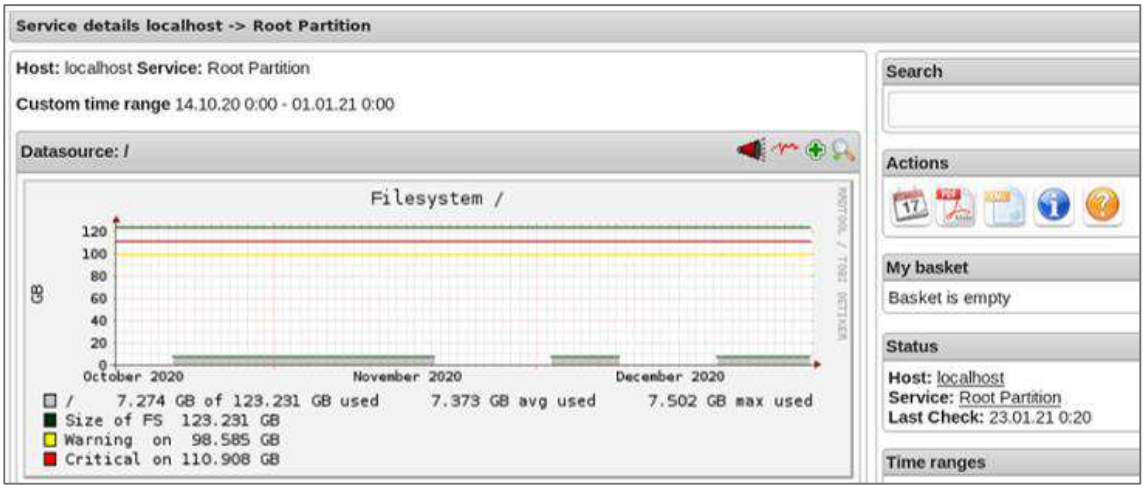


Ilustración 101 Gráfico "Partición" resumen "Localhost"- Máquina UNC

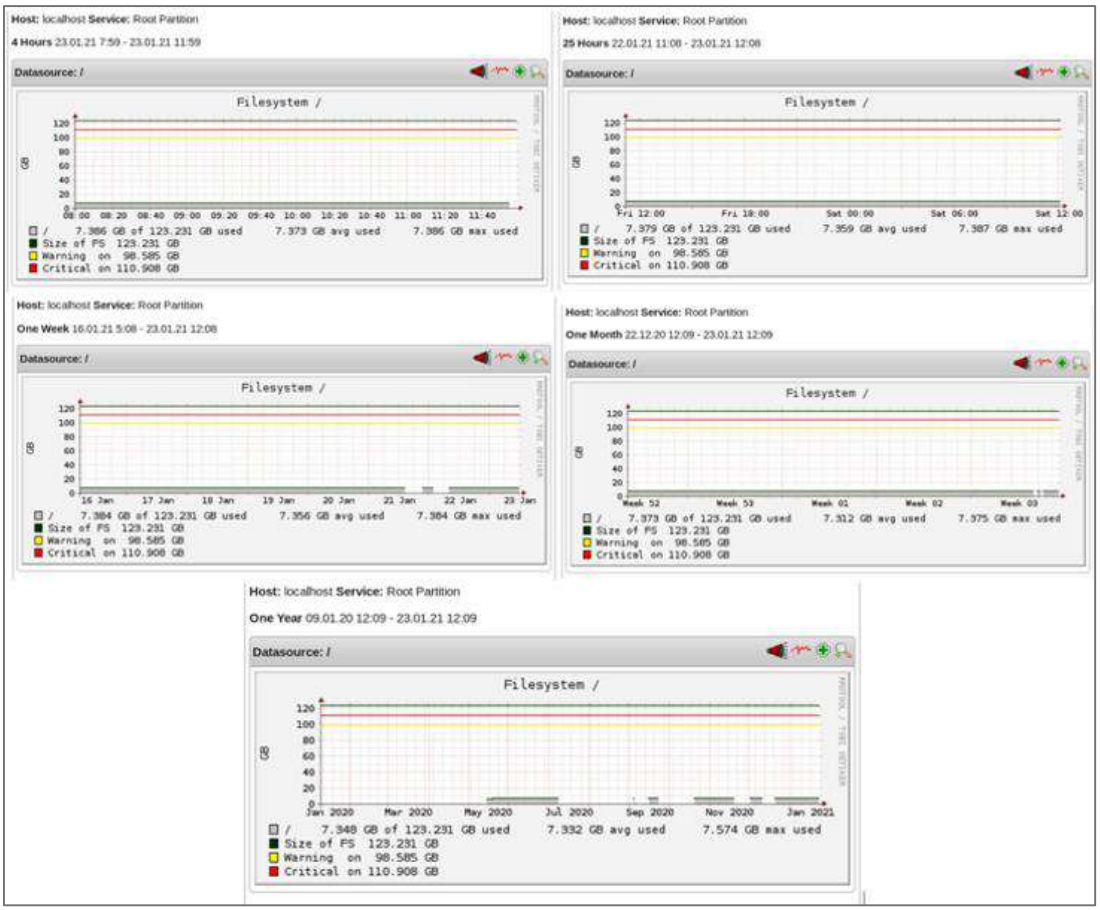


Ilustración 102 Reporte "Localhost - Particiones" NP4Nagios en: 4 horas, 25 horas, una semana, un mes, un año.

4.1.5. RESULTADOS GRAFANA

La herramienta Grafana permitió graficar de forma más amigable la información que almacenaba PNP4Nagios en el servicio ping del Swith 01 siendo constante y regular el monitoreo (ilustración 104).

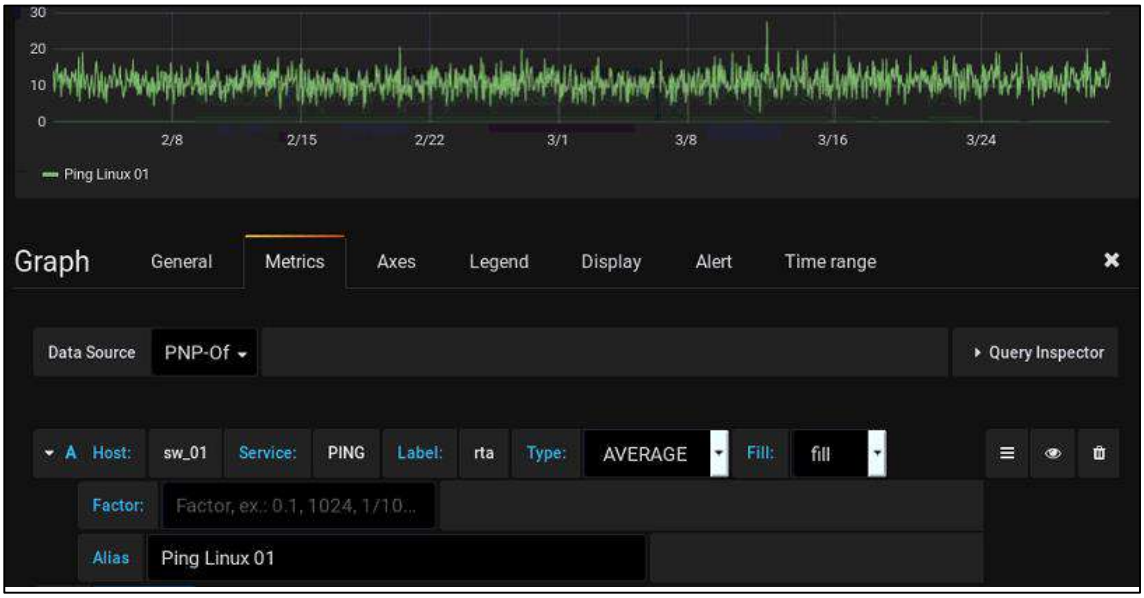


Ilustración 103 DashBoard – PING – Swich 1

- La ilustración 105 muestra como el servicio “Ping” fue lanzado constantemente en el swith 02 y al igual que en el caso anterior, el swich 02 da una respuesta de forma regular sin interrupciones en el tiempo de prueba.

Ilustración 104 Dashboard – PING – Switch 2

3.3. TRATAMIENTO, ANÁLISIS DE DATOS Y PRESENTACIÓN DE RESULTADOS

La presente investigación utilizó el tipo de investigación aplicada, ya que se buscó dar importancia a la resolución de problemas y su aplicación futura, al mismo tiempo esta investigación es exploratoria pues se usó todo el material disponible para el estudio de nuevos temas; la investigación buscó comprobar, demostrar o reproducir ciertos fenómenos hechos o principios en forma natural o artificial usando el método experimental, pero en mayor detalle la toma de datos se diseñó de forma longitudinal, es decir se observó y registró data del objeto de investigación de forma previa al uso de la herramienta y de la misma forma se hizo cuando el objeto de investigación uso la herramienta:

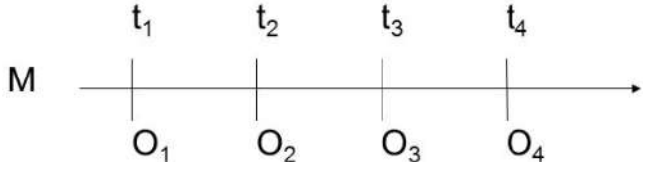


Ilustración 105 Diseño de la investigación

M: Muestra del estudio

t1 a t2: Momentos en que se hacen las observaciones

O1 a O4: Observación o mediciones de las variables de estudio.

La investigación se desarrolló en torno a dos variables, las cuales de detallan a continuación en la siguiente tabla (Tabla 8):

Tabla 8 Operacionalización de variables

VARIABLE	DIMENSIÓN – INDICADOR	SUB - DIMENSIONES
Dependiente: Gestión de la Infraestructura de TI	Número de incidentes identificados (tasas)	Incidentes registrados según el host Incidentes reportados y recibidos en el tiempo de estudio Incidentes atendidos por el usuario
	Número de incidentes controlados (tasas)	
Independiente: Sistema de soporte a la seguridad de la información	Satisfacción del usuario (Nivel)	Efectividad Tiempo Confidencialidad Disponibilidad Integridad Accesibilidad

3.3.1. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Para el registro de información, el presente trabajo de investigación hizo uso de dos técnicas de recolección de datos: la encuesta y la observación, con el fin de tener suficiente data que ayude a la comprobación de la hipótesis; para asegurar que la información tomada sea aún más verídica, en el caso de la encuesta se utilizó el cuestionario como instrumento, el cual fue medido en la escala de Likert y en el caso de la observación se utilizó la ficha de observación, elaborada en base a los indicadores de variables, la importancia en el uso de estos fue que logró almacenar la información de forma correcta.

3.3.1.1. Ficha de Observación

Para la construcción de las fichas de observación se utilizaron hojas de cálculo de la herramienta Excel, los registros debían ser considerados bajo las dimensiones a evaluar según el indicador y variable a evaluar, en este caso "Gestión de infraestructura de TI".

3.3.1.2. Cuestionario

Al igual que en el anterior instrumento, esta investigación uso los indicadores y dimensiones de la variable correspondiente, "Sistema de soporte a la seguridad de la información", para la elaboración del instrumento cuestionario, en el cual se redactaron preguntas que serían evaluadas según la escala de Likert.

3.3.2. VALIDACIÓN DE INSTRUMENTOS

Con el fin de asegurar la confiabilidad y validez de los instrumentos de recolección de datos, la Ing. Rocío Huamán Ramos revisó y aprobó la validación de los instrumentos que se usaron en la investigación y de la misma forma avaló la aplicación del coeficiente de Alpha de crombach para medir la confiabilidad de instrumentos.

Los resultados de las acciones ya mencionadas se pueden revisar en el Anexo 3 –CONFIABILIDAD DEL INSTRUMENTO, Anexo 4 VALIDACIÓN DEL INSTRUMENTO CUESTIONARIO y Anexo 5 VALIDACIÓN DEL INSTRUMENTO FICHA DE OBSERVACIONES.

3.3.3. PRUEBA ESTADISTICA

En los dos primeros indicadores se utilizó como método de análisis de datos, la distribución T-student se encontró la diferencia entre las medias de los dos grupos y se dividió por el error estándar, es decir la desviación de estándar de la distribución de las diferencias, agrupando los datos en 20 días tanto en la pre-prueba (sin el uso de la herramienta nagios) y post-prueba (usando la herramienta), sumando la información registrada según el área determinada, a continuación la fórmula que se siguió:

$$T = \frac{\bar{d} - D}{S_d / \sqrt{n}}$$

Se usó las mismas fórmulas en cada caso promedio de la diferencia de las medias de la investigación:

La media aritmética de las diferencias, obtenida usando al siguiente formula:

$$\bar{d} = \frac{\sum d_i}{n}$$

Varianza de la diferencia de las medias del post test y pre test:

$$S_d^2 = \frac{\sum (d_i - \bar{d})^2}{n-1}$$

Desviación estándar de la deferencia de las medidas del pre y post test:

$$S_d = S_d^2$$

$$D = U_{POST} - U_{PRE}$$

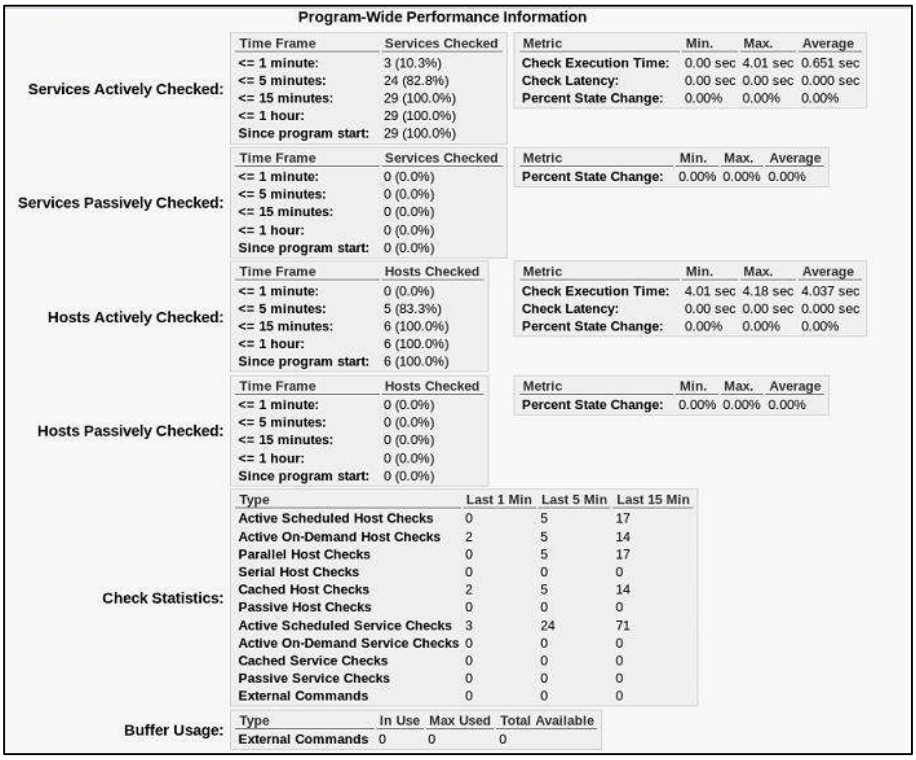
3.3.4. RESULTADOS DE LA VARIABLE DEPENDIENTE – GESTIÓN DE LA INFRAESTRUCTURA DE TI

3.3.4.1. Incidentes identificados

Nagios realizó una constante prueba de status de sus áreas monitoreadas, al momento inmediato de identificarse algún indicie que se ubicó según el siguiente cuadro en un rango de preocupación, se envió una notificación mediante telegram con el detalle del estado del servicio observado, estas notificaciones se contaron personalmente y fueron registradas de forma diaria, de igual forma se puede verificar en el rrd los registros de envió de notificaciones (Ilustración 107-108), pero se optó por la primera manera.

Current Load	OK	01-04-2021 11:31:54	350d 17h 38m 18s	1/4	OK - load average: 0.21, 0.80, 1.21
Current Users	OK	01-04-2021 11:28:22	507d 8h 20m 25s	1/4	USERS OK - 1 users currently logged in
HTTP	OK	01-04-2021 11:28:47	84d 1h 9m 14s	1/4	HTTP OK: HTTP/1.1 200 OK - 11595 bytes in 0,004 second response time
PING	OK	01-04-2021 11:30:45	84d 1h 9m 14s	1/4	PING OK - Packet loss = 0%, RTA = 0.41 ms
Root Partition	OK	01-04-2021 11:30:43	507d 7h 59m 16s	1/4	DISK OK - free space: / 112288 MB (93,76% inode=97%):
SSH	CRITICAL	01-04-2021 11:32:13	507d 8h 20m 50s	4/4	connect to address 10.1.3.16 and port 22: Conexión rehusada
Swap Usage	OK	01-04-2021 11:28:37	75d 22h 45m 3s	1/4	SWAP OK - 45% free (435 MB out of 979 MB)
Total Processes	OK	01-04-2021 11:30:30	350d 18h 29m 39s	1/4	PROCS OK: 51 processes with STATE = RSZDT
Current Load	OK	01-04-2021 11:28:35	350d 17h 38m 18s	1/4	OK - load average: 0.70, 1.31, 1.44
Current Users	OK	01-04-2021 11:31:00	507d 7h 57m 11s	1/4	USERS OK - 1 users currently logged in
HTTP	OK	01-04-2021 11:27:26	350d 18h 26m 47s	1/4	HTTP OK: HTTP/1.1 200 OK - 11595 bytes in 0,002 second response time
PING	OK	01-04-2021 11:28:51	350d 18h 25m 37s	1/4	PING OK - Packet loss = 0%, RTA = 0.12 ms

Ilustración 106 Evidencia de los tiempos que Nagios monitorea .automaticamente



Program-Wide Performance Information

Services Actively Checked:

Time Frame	Services Checked
<= 1 minute:	3 (10.3%)
<= 5 minutes:	24 (82.8%)
<= 15 minutes:	29 (100.0%)
<= 1 hour:	29 (100.0%)
Since program start:	29 (100.0%)

Metric	Min.	Max.	Average
Check Execution Time:	0.00 sec	4.01 sec	0.651 sec
Check Latency:	0.00 sec	0.00 sec	0.000 sec
Percent State Change:	0.00%	0.00%	0.00%

Services Passively Checked:

Time Frame	Services Checked
<= 1 minute:	0 (0.0%)
<= 5 minutes:	0 (0.0%)
<= 15 minutes:	0 (0.0%)
<= 1 hour:	0 (0.0%)
Since program start:	0 (0.0%)

Metric	Min.	Max.	Average
Percent State Change:	0.00%	0.00%	0.00%

Hosts Actively Checked:

Time Frame	Hosts Checked
<= 1 minute:	0 (0.0%)
<= 5 minutes:	5 (83.3%)
<= 15 minutes:	6 (100.0%)
<= 1 hour:	6 (100.0%)
Since program start:	6 (100.0%)

Metric	Min.	Max.	Average
Check Execution Time:	4.01 sec	4.18 sec	4.037 sec
Check Latency:	0.00 sec	0.00 sec	0.000 sec
Percent State Change:	0.00%	0.00%	0.00%

Hosts Passively Checked:

Time Frame	Hosts Checked
<= 1 minute:	0 (0.0%)
<= 5 minutes:	0 (0.0%)
<= 15 minutes:	0 (0.0%)
<= 1 hour:	0 (0.0%)
Since program start:	0 (0.0%)

Metric	Min.	Max.	Average
Percent State Change:	0.00%	0.00%	0.00%

Check Statistics:

Type	Last 1 Min	Last 5 Min	Last 15 Min
Active Scheduled Host Checks	0	5	17
Active On-Demand Host Checks	2	5	14
Parallel Host Checks	0	5	17
Serial Host Checks	0	0	0
Cached Host Checks	2	5	14
Passive Host Checks	0	0	0
Active Scheduled Service Checks	3	24	71
Active On-Demand Service Checks	0	0	0
Cached Service Checks	0	0	0
Passive Service Checks	0	0	0
External Commands	0	0	0

Buffer Usage:

Type	In Use	Max Used	Total Available
External Commands	0	0	0

Ilustración 107 Información de Rendimiento

- Pre - Prueba

Según el cuestionario realizado al personal de la oficina general de sistemas informáticos y plataformas virtuales, en los equipos Dell se identificaban los incidentes de forma manual y diaria, en una sola revisión al día, hecha por el personal encargado y en otros caso los incidentes fueron reportados por el público usuario de los servicios, todos fueron registrados manualmente (tabla 9), así se obtuvo la siguiente data correspondiente a incidentes registrados de forma diaria en las 6 áreas determinadas:

Tabla 9 Registro de Incidencias sin Herramienta Nagios

Resultados - Antes de la Herramienta																					
ÁREA	**Indicador**	**SEMANA 01**					**SEMANA 02**					**SEMANA 03**					**SEMANA 04**				
		L	**M**	**M**	**J**	**V**	**L**	**M**	**M**	**J**	**V**	**L**	**M**	**M**	**J**	**V**	**L**	**M**	**M**	**J**	**V**
Local host	Número de Incidentes por día																				
sw 01																					
sw 02						1	2		2		1	1			2	2	2	3	1	1	
Linux																					
admisión			1	2	1				1	1				2	2	3	1		1	1	
Mysql		1					1	2													

Fuente: Elaboración propia

- Post - Prueba

Los datos que se obtuvieron en la investigación, para post-prueba se registraron manualmente y de forma diaria, según los mensajes recibidos en telegram (Ilustración 109) y se clasificaron según el área y detalle que indicaba el mensaje, se tomó la data (tabla 10) por un mes en días laborables como se puede observar

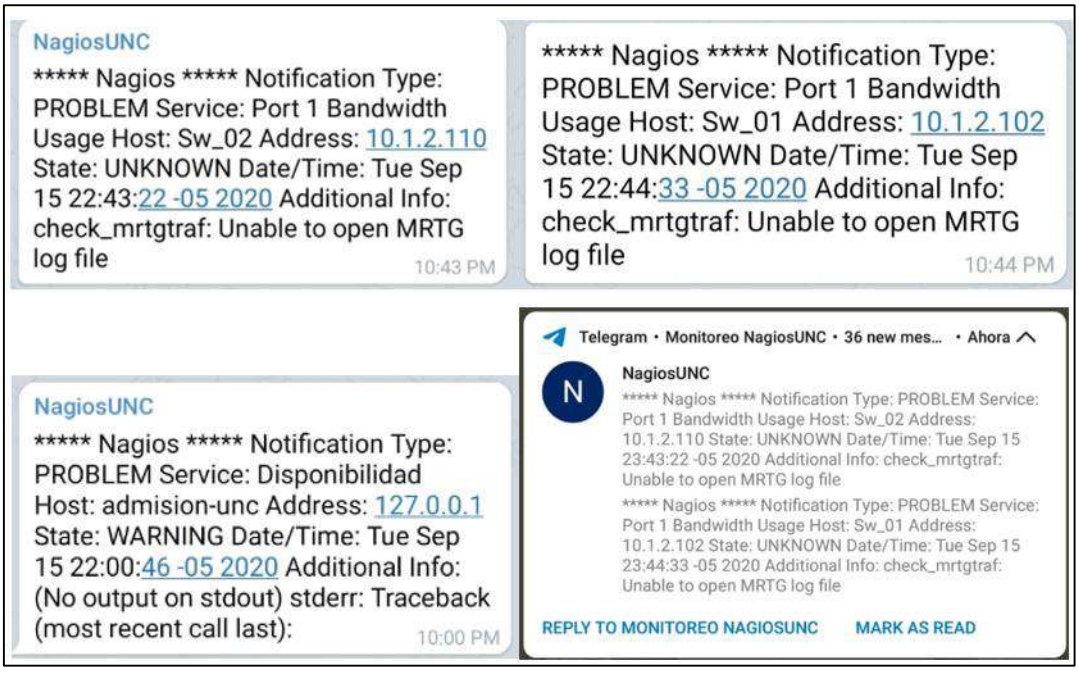


Ilustración 108 Mensajes vía telegram reportando incidentes reistrados en Nagios

Tabla 10 Registro de Incidencias post Herramienta Nagios

Resultados - Al usar la Herramienta																					
		SEMANA 01					**SEMANA 02**					**SEMANA 03**					**SEMANA 04**				
		L	**M**	**M**	**J**	**V**	**L**	**M**	**M**	**J**	**V**	**L**	**M**	**M**	**J**	**V**	**L**	**M**	**M**	**J**	**V**
Local host	Número de Incidentes por día							5	5	7	3										
sw 01		48	65	64	58	58	65	66	63	60	65	64	65	64	58	66	64	60	63	60	61
sw 02		50	60	60	59	60	66	66	64	61	64	66	66	66	59	66	64	60	64	62	63
Linux															3			3	3		4
admisión		18	17	18	18	17	18	18	16	18	16	18	18	17	18	18	18	18	18	18	18
Mysql				3	4	4									3		6	8	6	6	9

Fuente: Elaboración propia

- Contrastación de la hipótesis

Incidentes identificados en Local Host

A. Formulación de la Hipótesis

- Hipótesis Nula

  Los incidentes identificados en local host con el sistema de soporte a la seguridad de la información usando big data no mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca. $H_O : D = 0$

- Hipótesis Alterna

  Los incidentes identificados en local host con el sistema de soporte a la seguridad de la información usando big data mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca. $H_1 : D > 0$

B. Nivel de significancia

El nivel de significancia o margen de error (α) escogido para la prueba de la hipótesis fue del 5%. Siendo α = 0.05. Por lo tanto, el nivel de confianza (1 - α = 0.95) fue del 95%.

C. Estadística de Prueba:

Mediante t-student se trató 20 datos de la muestra dependiente.

$$T = \frac{\bar{d} - D}{S_d / \sqrt{n}} = \frac{1 - 0}{2.15 / \sqrt{20}} = 2.08$$

Considerando que el grado de libertad es n-2=20-2=18, se obtiene la Ttabla=1.734 equivale al 5% de n-2, es decir, el nivel de significancia fue el 5%.

D. Datos de la Hipótesis estadística

Tabla 11 Prueba t Número de Incidentes identificados - Local Host

Prueba t-student / medias de 2 muestras (local host)		
	Post Test	*Pres Test*
Media	1	0
Varianza	4.63157895	0
Observaciones	20	20
Diferencia hipotética de las medias	0	
Grados de libertad	19	
Estadístico t	2.07802354	
P(T<=t) una cola	0.02575178	
Valor crítico de t (una cola)	1.72913279	
P(T<=t) dos colas	0.05150356	
Valor crítico de t (dos colas)	2.09302405	

Fuente: Elaboración propia

E. Valor crítico

Ilustración 109 Región de Aceptación y Rechazo

Fuente: Elaboración propia

F. Decisión

Ho se rechaza, por lo tanto, los incidentes identificados en local host con el sistema de soporte a la seguridad de la información usando big data mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca, con p=0.02575178

Incidentes identificados en Network (sw_01)

A. Formulación de la Hipótesis

- Hipótesis Nula

  Los incidentes identificados en sw_01 con el sistema de soporte a la seguridad de la información usando big data no mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca. $H_O : D = 0$

- Hipótesis Alterna

  Los incidentes identificados en sw_01 con el sistema de soporte a la seguridad de la información usando big data mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca. $H_1 : D > 0$

B. Nivel de significancia

   El nivel de significancia o margen de error (α) escogido para la prueba de la hipótesis fue del 5%. Siendo α = 0.05. Por lo tanto, el nivel de confianza (1 - α = 0.95) fue del 95%.

C. Estadística de Prueba:

   Mediante t-student se trató 20 datos de la muestra dependiente.

$$T = \frac{\bar{d} - D}{S_d / \sqrt{n}} = \frac{61.85 - 0}{4.25 / \sqrt{20}} = 65.0827$$

   Considerando que el grado de libertad es n-2=20-2=18, se obtiene la Ttabla =1.734 equivale al 5% de n-2, es decir, el nivel de significancia fue el 5%.

D. Datos de la Hipótesis estadística

Tabla 12 Prueba T Número de Incidentes identificados - sw_01

Prueba t-student / medias de 2 muestras (Sw_01)		
	Post Test	*Pres Test*
Media	61.85	0
Varianza	18.0289474	0
Observaciones	20	20
Diferencia hipotética de las medias	0	
Grados de libertad	19	
Estadístico t	65.1432642	
P(T<=t) una cola	4.1967E-24	
Valor crítico de t (una cola)	1.72913279	
P(T<=t) dos colas	8.3934E-24	
Valor crítico de t (dos colas)	61.85	

Fuente: Elaboración propia

E. Valor crítico

Ilustración 110 Región de Aceptación y Rechazo

Fuente: Elaboración propia

F. Decisión

Ho se rechaza, por lo tanto, los incidentes identificados en sw_01 con el sistema de soporte a la seguridad de la información usando big data mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca, con p=4.1967E-24

Incidentes identificados en Network (sw_02)

A. Formulación de la Hipótesis

- Hipótesis Nula

  Los incidentes identificados en sw_02 con el sistema de soporte a la seguridad de la información usando big data no mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca. $H_O : D = 0$

- Hipótesis Alterna

  Los incidentes identificados en sw_02 con el sistema de soporte a la seguridad de la información usando big data mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca. $H_1 : D > 0$

B. Nivel de significancia

El nivel de significancia o margen de error (α) escogido para la prueba de la hipótesis fue del 5%. Siendo α = 0.05. Por lo tanto, el nivel de confianza (1 - α = 0.95) fue del 95%.

C. Estadística de Prueba:

Mediante t-student se trató 20 datos de la muestra dependiente.

$$T = \frac{\bar{d} - D}{S_d / \sqrt{n}} = \frac{61.40 - 0}{3.86 / \sqrt{20}} = 71.14$$

Considerando que el grado de libertad es n-2=20-2=18, se obtiene la Ttabla=1.734 equivale al 5% de n-2, es decir, el nivel de significancia fue el 5%.

D. Datos de la Hipótesis estadística

Tabla 13 Prueba T Número de Incidentes identificados – sw_02

Prueba t-student / medias de 2 muestras (Sw_02)		
	Post Test	*Pres Test*
Media	62.3	0.9
Varianza	15.2736842	0.93684211
Observaciones	20	20
Diferencia hipotética de las medias	0	
Grados de libertad	19	
Estadístico t	71.1738513	
P(T<=t) una cola	7.8556E-25	
Valor crítico de t (una cola)	1.72913279	
P(T<=t) dos colas	1.5711E-24	
Valor crítico de t (dos colas)	2.09302405	

Fuente: Elaboración propia

E. Valor crítico

Ilustración 111 Región de Aceptación y Rechazo

Fuente: Elaboración propia

F. Decisión

Ho se rechaza, por lo tanto, los incidentes identificados en sw_02 con el sistema de soporte a la seguridad de la información usando big data

mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca, con p=7.8556E-25

Incidentes identificados en Linux

A. Formulación de la Hipótesis

- Hipótesis Nula

  Los incidentes identificados en linux con el sistema de soporte a la seguridad de la información usando big data no mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca. $H_O : D = 0$

- Hipótesis Alterna

  Los incidentes identificados en linux con el sistema de soporte a la seguridad de la información usando big data mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca. $H_1 : D > 0$

B. Nivel de significancia

El nivel de significancia o margen de error (α) escogido para la prueba de la hipótesis fue del 5%. Siendo α = 0.05. Por lo tanto, el nivel de confianza (1 - α = 0.95) fue del 95%.

C. Estadística de Prueba:

Mediante t-student se trató 20 datos de la muestra dependiente.

$$T = \frac{\bar{d} - D}{S_d / \sqrt{n}} = \frac{0.65 - 0}{1.35 / \sqrt{20}} = 2.1533$$

Considerando que el grado de libertad es n-2=20-2=18, se obtiene la Ttabla=1.734 equivale al 5% de n-2, es decir, el nivel de significancia fue el 5%.

D. Datos de la Hipótesis estadística

Tabla 14 Prueba T Número de Incidentes identificados - Linux

Prueba t-student / medias de 2 muestras (Linux)		
	Post Test	*Pres Test*
Media	1	0
Varianza	4.63157895	0
Observaciones	20	20
Diferencia hipotética de las medias	0	
Grados de libertad	19	
Estadístico t	2.1556643	
P(T<=t) una cola	0.02207092	
Valor crítico de t (una cola)	1.72913279	
P(T<=t) dos colas	0.04414183	
Valor crítico de t (dos colas)	2.09302405	

Fuente: Elaboración propia

E. Valor crítico

Ilustración 112 Región de Aceptación y Rechazo

Fuente: Elaboración propia

F. Decisión

Ho se rechaza, por lo tanto, los incidentes identificados en linux con el sistema de soporte a la seguridad de la información usando big data mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca, con p=0.02207092

Incidentes identificados en admisión.unc

A. Formulación de la Hipótesis

- Hipótesis Nula

  Los incidentes identificados en admisión con el sistema de soporte a la seguridad de la información usando big data no mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca. $H_O : D = 0$

- Hipótesis Alterna

  Los incidentes identificados en admisión con el sistema de soporte a la seguridad de la información usando big data mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca. $H_1 : D > 0$

B. Nivel de significancia

El nivel de significancia o margen de error (α) escogido para la prueba de la hipótesis fue del 5%. Siendo α = 0.05. Por lo tanto, el nivel de confianza (1 - α = 0.95) fue del 95%.

C. Estadística de Prueba:

Mediante t-student se trató 20 datos de la muestra dependiente.

$$T = \frac{\bar{d} - D}{S_d / \sqrt{n}} = \frac{16.85 - 0}{1.09 / \sqrt{20}} = 69.1335$$

Considerando que el grado de libertad es n-2=20-2=18, se obtiene la Ttabla=1.734 equivale al 5% de n-2, es decir, el nivel de significancia fue el 5%.

D. Datos de la Hipótesis estadística

Tabla 15 Prueba T Número de Incidentes identificados – admisión.unc

Prueba t-student / medias de 2 muestras (Admisión)		
	Post Test	*Pres Test*
Media	17.65	0.8
Varianza	0.45	0.8
Observaciones	20	20
Diferencia hipotética de las medias	0	
Grados de libertad	19	
Estadístico t	69.1701043	
P(T<=t) una cola	1.3488E-24	
Valor crítico de t (una cola)	1.72913279	
P(T<=t) dos colas	2.6977E-24	
Valor crítico de t (dos colas)	2.09302405	

Fuente: Elaboración propia

E. Valor crítico

Ilustración 113 Región de Aceptación y Rechazo

Fuente: Elaboración propia

F. Decisión

Ho se rechaza, por lo tanto, los incidentes identificados en admisión con el sistema de soporte a la seguridad de la información usando big data mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca, con p=1.3488E-24

Incidentes identificados en MySql

A. Formulación de la Hipótesis

- Hipótesis Nula

  Los incidentes identificados en mysql con el sistema de soporte a la seguridad de la información usando big data no mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca. $H_O : D = 0$

- Hipótesis Alterna

  Los incidentes identificados en mysql con el sistema de soporte a la seguridad de la información usando big data mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca. $H_1 : D > 0$

B. Nivel de significancia

El nivel de significancia o margen de error (α) escogido para la prueba de la hipótesis fue del 5%. Siendo α = 0.05. Por lo tanto, el nivel de confianza (1 - α = 0.95) fue del 95%.

C. Estadística de Prueba:

Mediante t-student se trató 20 datos de la muestra dependiente.

$$T = \frac{\bar{d} - D}{S_d / \sqrt{n}} = \frac{2.25 - 0}{3.31 / \sqrt{20}} = 3.040$$

Considerando que el grado de libertad es n-2=20-2=18, se obtiene la Ttabla=1.734 equivale al 5% de n-2, es decir, el nivel de significancia fue el 5%.

D. Datos de la Hipótesis estadística

Tabla 16 Prueba T Número de Incidentes identificados – MySql

Prueba t-student / media de 2 muestras(MySql)		
	Post Test	*Pres Test*
Media	2.45	0.2
Varianza	9.62894737	0.27368421
Observaciones	20	20
Diferencia hipotética de las medias	0	
Grados de libertad	19	
Estadístico t	3.04301295	
P(T<=t) una cola	0.00334601	
Valor crítico de t (una cola)	1.72913279	
P(T<=t) dos colas	0.00669201	
Valor crítico de t (dos colas)	2.09302405	

Fuente: Elaboración propia

E. Valor crítico

Ilustración 114 Región de Aceptación y Rechazo

Fuente: Elaboración propia

F. Decisión

Ho se rechaza, por lo tanto, los incidentes identificados en mysql con el sistema de soporte a la seguridad de la información usando big data mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca, con p=0.00334601

3.3.4.2. Incidentes controlados

Luego de identificarse los incidentes se clasificaron según el criterio del personal de la oficina general de sistemas informáticos y plataformas virtuales y se determinó cuáles serían los controlados de forma inmediata o los que no recibirían atención, de la misma forma que la anterior se registró la información de manera manual y diaria.

- Pre- Prueba

Al culminar cada día se revisaron los equipos Dell y se efectuaron subsanación de incidentes según lo cotidiano (tabla 17), se detalla a continuación:

Tabla 17 Registro de Incidencias resueltas sin Herramienta Nagios

Resultados - Antes de la Herramienta																					
Área	**Indicador**	**SEMANA 01**					**SEMANA 02**					**SEMANA 03**					**SEMANA 04**				
		L	**M**	**M**	**J**	**V**	**L**	**M**	**M**	**J**	**V**	**L**	**M**	**M**	**J**	**V**	**L**	**M**	**M**	**J**	**V**
Local host	Número de Incidentes resueltos por día																				
sw 01																					
sw 02						1	2		2		1	1			2	2	1	3	1	1	
Linux																					
admisión			1	1					1	1				2	2	1	1		1	1	
mysql		1					1	2													

Fuente: Elaboración propia

- Post – Prueba

Al recibir un mensaje mediante Telegram y según prioridad y criterio el personal, se resolvió o controló la incidencia y se registró manualmente (tabla 18) de la siguiente forma:

Tabla 18 Registro de Incidencias resueltas con Herramienta Nagios

Resultados - Usando la Herramienta																					
Área	**Indicador**	**SEMANA 01**					**SEMANA 02**					**SEMANA 03**					**SEMANA 04**				
		L	**M**	**M**	**J**	**V**	**L**	**M**	**M**	**J**	**V**	**L**	**M**	**M**	**J**	**V**	**L**	**M**	**M**	**J**	**V**
Local host	Número de Incidentes resueltos por día							2	2	2	3										
sw 01		5	5	6	4	5	4	6	4	5	5	5	7	4	6	8	4	5	6	8	7
sw 02		4	6	8	6	4	5	5	8	6	6	7	8	8	9	7	9	8	8	7	9
Linux															1			1	1		2
admisión		6	6	5	4	8	6	9	8	4	6	8	3	8	6	4	5	8	4	3	4
mysql				3	2	1									1		6	4	5	2	3

Fuente: Elaboración propia

- CONTRASTACIÓN DE RESULTADOS: INCIDENTES CONTROLADOS

Incidentes controlados en Local Host

A. Formulación de la Hipótesis

- Hipótesis Nula

  Los incidentes controlados en local host con el sistema de soporte a la seguridad de la información usando big data no mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca. $H_O : D = 0$

- Hipótesis Alterna

  Los incidentes controlados en local host con el sistema de soporte a la seguridad de la información usando big data mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca. $H_1 : D > 0$

B. Nivel de significancia

El nivel de significancia o margen de error (α) escogido para la prueba de la hipótesis fue del 5%. Siendo α = 0.05. Por lo tanto, el nivel de confianza (1 - α = 0.95) fue del 95%.

C. Estadística de Prueba:

Mediante t-student se trató 20 datos de la muestra dependiente.

$$T = \frac{\bar{d} - D}{S_d / \sqrt{n}} = \frac{0.45 - 0}{0.94 / \sqrt{20}} = 2.14$$

Considerando que el grado de libertad es n-2=20-2=18, se obtiene la Ttabla=1.734 equivale al 5% de n-2, es decir, el nivel de significancia fue el 5%.

D. Datos de la Hipótesis estadística

Tabla 19 Prueba T Número de Incidentes controlados - Local Host

Prueba t-student / medias de 2 muestras (Local host)		
	Post Test	*Pres Test*
Media	0.45	0
Varianza	0.892105263	0
Observaciones	20	20
Diferencia hipotética de las medias	0	

Grados de libertad	19	
Estadístico t	2.130686042	
P(T<=t) una cola	0.023199307	
Valor crítico de t (una cola)	1.729132792	
P(T<=t) dos colas	0.046398613	
Valor crítico de t (dos colas)	2.09302405	

Fuente: Elaboración propia

E. Valor crítico

Ilustración 115 Región de Aceptación y Rechazo

Fuente: Elaboración propia

F. Decisión

Ho se rechaza, por lo tanto, los incidentes controlados en local host con el sistema de soporte a la seguridad de la información usando big data mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca, con p=0.023199307

Incidentes controlados en Network (sw_01)

A. Formulación de la Hipótesis

- Hipótesis Nula

  Los incidentes controlados en sw_01 con el sistema de soporte a la seguridad de la información usando big data no mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca. $H_O : D = 0$

- Hipótesis Alterna

  Los incidentes controlados en sw_01 con el sistema de soporte a la seguridad de la información usando big data mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca. $H_1 : D > 0$

B. Nivel de significancia

El nivel de significancia o margen de error (α) escogido para la prueba de la hipótesis fue del 5%. Siendo α = 0.05. Por lo tanto, el nivel de confianza (1 - α = 0.95) fue del 95%.

C. Estadística de Prueba:

Mediante t-student se trató 20 datos de la muestra dependiente.

$$T = \frac{\bar{d} - D}{S_d / \sqrt{n}} = \frac{5.45 - 0}{1.28 / \sqrt{20}} = 19.04$$

Considerando que el grado de libertad es n-2=20-2=18, se obtiene la Ttabla=1.734 equivale al 5% de n-2, es decir, el nivel de significancia fue el 5%.

D. Datos de la Hipótesis estadística

Tabla 20 Prueba T Número de Incidentes controlados - sw_01

Prueba t-student / medias de 2 muestras (SW_01)		
	Post Test	*Pres Test*
Media	5.45	0
Varianza	1.628947368	0
Observaciones	20	20
Diferencia hipotética de las medias	0	
Grados de libertad	19	
Estadístico t	19.09668454	
P(T<=t) una cola	3.68294E-14	
Valor crítico de t (una cola)	1.729132792	
P(T<=t) dos colas	7.36588E-14	
Valor crítico de t (dos colas)	2.09302405	

Fuente: Elaboración propia

E. Valor crítico

Ilustración 116 Región de Aceptación y Rechazo

Fuente: Elaboración propia

F. Decisión

Ho se rechaza, por lo tanto, los incidentes controlados en sw_01 con el sistema de soporte a la seguridad de la información usando big data mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca, con p=3.68294E-14

Incidentes identificados en Network (sw_02)

A. Formulación de la Hipótesis

- Hipótesis Nula

  Los incidentes controlados en sw_02 con el sistema de soporte a la seguridad de la información usando big data no mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca. $H_O : D = 0$

- Hipótesis Alterna

  Los incidentes controlados en sw_02 con el sistema de soporte a la seguridad de la información usando big data mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca. $H_1 : D > 0$

B. Nivel de significancia

El nivel de significancia o margen de error (α) escogido para la prueba de la hipótesis fue del 5%. Siendo α = 0.05. Por lo tanto, el nivel de confianza (1 - α = 0.95) fue del 95%.

C. Estadística de Prueba:

Mediante t-student se trató 20 datos de la muestra dependiente.

$$T = \frac{\bar{d} - D}{S_d / \sqrt{n}} = \frac{6.05 - 0}{1.67 / \sqrt{20}} = 16.20$$

D. Considerando que el grado de libertad es n-2=20-2=18, se obtiene la Ttabla=1.734 equivale al 5% de n-2, es decir, el nivel de significancia fue el 5%.

E. Datos de la Hipótesis estadística

Tabla 21 Prueba T Número de Incidentes controladas – sw_02

Prueba t-student / medias de 2muestras (Sw_02)		
	Post Test	*Pres Test*
Media	6.9	0.85
Varianza	2.515789474	0.871052632
Observaciones	20	20
Diferencia hipotética de las medias	0	
Grados de libertad	19	
Estadístico t	16.20743135	
P(T<=t) una cola	6.99788E-13	
Valor crítico de t (una cola)	1.729132792	
P(T<=t) dos colas	1.39958E-12	
Valor crítico de t (dos colas)	2.09302405	

Fuente: Elaboración propia

F. Valor crítico

Ilustración 117 Región de Aceptación y Rechazo

Fuente: Elaboración propia

G. Decisión

Ho se rechaza, por lo tanto, los incidentes controlados en sw_02 con el sistema de soporte a la seguridad de la información usando big data mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca, con p=6.99788E-13

Incidentes controlados en Linux

A. Formulación de la Hipótesis

- Hipótesis Nula

  Los incidentes controlados en linux con el sistema de soporte a la seguridad de la información usando big data no mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca. $H_O : D = 0$

- Hipótesis Alterna

  Los incidentes controlados en linux con el sistema de soporte a la seguridad de la información usando big data mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca. $H_1 : D > 0$

B. Nivel de significancia

El nivel de significancia o margen de error (α) escogido para la prueba de la hipótesis fue del 5%. Siendo α = 0.05. Por lo tanto, el nivel de confianza (1 - α = 0.95) fue del 95%.

C. Estadística de Prueba:

Mediante t-student se trató 20 datos de la muestra dependiente.

$$T = \frac{\bar{d} - D}{S_d / \sqrt{n}} = \frac{0.25 - 0}{0.55 / \sqrt{20}} = 2.03$$

Considerando que el grado de libertad es n-2=20-2=18, se obtiene la Ttabla=1.734 equivale al 5% de n-2, es decir, el nivel de significancia fue el 5%.

D. Datos de la Hipótesis estadística

Tabla 22 Prueba T Número de Incidentes controlados - Linux

Prueba t-student / medias de 2 muestras (Linux)		
	Post Test	*Pres Test*
Media	0.25	0
Varianza	0.302631579	0
Observaciones	20	20
Diferencia hipotética de las medias	0	
Grados de libertad	19	
Estadístico t	2.032347112	
P(T<=t) una cola	0.02816832	
Valor crítico de t (una cola)	1.729132792	
P(T<=t) dos colas	0.056336641	
Valor crítico de t (dos colas)	2.09302405	

Fuente: Elaboración propia

E. Valor crítico

Ilustración 118 Región de Aceptación y Rechazo

Fuente: Elaboración propia

F. Decisión

Ho se rechaza, por lo tanto, los incidentes controlados en linux con el sistema de soporte a la seguridad de la información usando big data mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca, con p= 0.02816832

Incidentes controlados en admisión.unc

A. Formulación de la Hipótesis

- Hipótesis Nula

  Los incidentes controlados en admisión con el sistema de soporte a la seguridad de la información usando big data no mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca. $H_O : D = 0$

- Hipótesis Alterna

  Los incidentes controlados en admisión con el sistema de soporte a la seguridad de la información usando big data mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca. $H_1 : D > 0$

B. Nivel de significancia

El nivel de significancia o margen de error (α) escogido para la prueba de la hipótesis fue del 5%. Siendo α = 0.05. Por lo tanto, el nivel de confianza (1 - α = 0.95) fue del 95%.

C. Estadística de Prueba:

Mediante t-student se trató 20 datos de la muestra dependiente.

$$T = \frac{\bar{d} - D}{S_d / \sqrt{n}} = \frac{5.15 - 0}{2.06 / \sqrt{20}} = 11.18$$

Considerando que el grado de libertad es n-2=20-2=18, se obtiene la Ttabla=1.734 equivale al 5% de n-2, es decir, el nivel de significancia fue el 5%.

D. Datos de la Hipótesis estadística

Tabla 23 Prueba T Número de Incidentes controlados – admisión.unc

Prueba t-student / medias de 2 muestras (Admisión)		
	Post Test	*Pres Test*
Media	5.75	0.6
Varianza	3.565789474	0.463157895
Observaciones	20	20
Diferencia hipotética de las medias	0	
Grados de libertad	19	
Estadístico t	11.18577952	
P(T<=t) una cola	4.20397E-10	
Valor crítico de t (una cola)	1.729132792	
P(T<=t) dos colas	8.40795E-10	
Valor crítico de t (dos colas)	2.09302405	

Fuente: Elaboración propia

E. Valor crítico

Ilustración 119 Región de Aceptación y Rechazo

Fuente: Elaboración propia

F. Decisión

Ho se rechaza, por lo tanto, los incidentes controlados en admisión con el sistema de soporte a la seguridad de la información usando big data mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca, con p=4.20397E-10

Incidentes controlados en MySql

A. Formulación de la Hipótesis

- Hipótesis Nula

  Los incidentes controlados en mysql con el sistema de soporte a la seguridad de la información usando big data no mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca. $H_O : D = 0$

- Hipótesis Alterna

  Los incidentes controlados en mysql con el sistema de soporte a la seguridad de la información usando big data mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca. $H_1 : D > 0$

B. Nivel de significancia

El nivel de significancia o margen de error (α) escogido para la prueba de la hipótesis fue del 5%. Siendo α = 0.05. Por lo tanto, el nivel de confianza (1 - α = 0.95) fue del 95%.

C. Estadística de Prueba:

Mediante t-student se trató 20 datos de la muestra dependiente.

$$T = \frac{\bar{d} - D}{S_d / \sqrt{n}} = \frac{5.15 - 0}{2.11 / \sqrt{20}} = 10.92$$

Considerando que el grado de libertad es n-2=20-2=18, se obtiene la Ttabla=1.734 equivale al 5% de n-2, es decir, el nivel de significancia fue el 5%.

D. Datos de la Hipótesis estadística

Tabla 24 Prueba T Número de Incidentes controlados – MySql

Prueba t-student / medias de 2 muestras (MySql)		
	Post Test	*Pres Test*
Media	1.35	0.2
Varianza	3.607894737	0.273684211
Observaciones	20	20
Diferencia hipotética de las medias	0	

Grados de libertad	19	
Estadístico t	2.437995124	
P(T<=t) una cola	0.012381554	
Valor crítico de t (una cola)	1.729132792	
P(T<=t) dos colas	0.024763109	
Valor crítico de t (dos colas)	2.09302405	

Fuente: Elaboración propia

E. Valor crítico

Ilustración 120 Región de Aceptación y Rechazo

Fuente: Elaboración propia

F. Decisión

Ho se rechaza, por lo tanto, los incidentes controlados en mysql con el sistema de soporte a la seguridad de la información usando big data mejora la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca, con p=0.012381554

3.3.5. RESULTADOS DE LA VARIABLE INDEPENDIENTE – SISTEMA DE SOPORTE A LA SEGURIDAD DE LA INFORMACIÓN

Para recolectar los datos correspondientes al indicador nivel de satisfacción, se realizó un cuestionario a los trabajadores de la oficina general de sistemas informáticos y plataformas virtuales, a diferencia de la variable dependiente, la variable independiente no se podrá calcular antes del uso, ya que no se encontró alguna herramienta similar o parecida para comparar.

El cuestionario permitió medir los niveles de satisfacción del usuario en el uso de la herramienta de soporte a la seguridad de información en la transmisión de incidentes. Para realizar la puntuación de las preguntas aplicadas en los cuestionarios se tomó como base la escala de Likert (tabla 24) y se comprobó la confiabilidad mediante el coeficiente de alpha de crobach (Anexo 3).

Tabla 25 Escalas de Lirket - Nivel de Satisfacción, en el Uso de la herramienta de monitoreo Nagios

Escala	NIVEL DE SATISFACCIÓN	Valor
E	Excelente	5
MB	Muy Bueno	4
B	Bueno	3
R	Regular	2
M	Malo	1

Fuente: Elaboración Propia.

La investigación hizo uso del método top two box junto a la escala de Likert, logrando que el rango de valores permita obtener conclusiones más exactas de acuerdo a los puntajes obtenidos en excelente y muy bueno (4 y 5) con los resultados se pudo ver cuáles son los puntos fuertes de la herramienta y también los puntos a mejorar, la siguiente tabla (tabla 26) detalla que sus dimensiones fueron evaluadas en cada pregunta:

Tabla 26 Valores válidos para confirmar la Satisfacción

		E	MB	B	R	M
1. ¿Cómo considera la efectividad de la herramienta?	Efectividad	1	2	3	4	5
2. ¿Cómo considera el tiempo de identificación de Incidentes?	Tiempo	1	2	3	4	5
3. ¿Cómo considera la confidencialidad de la información en el uso de la herramienta?	Confidencialidad	1	2	3	4	5
4. ¿Cómo considera la disponibilidad de la información en el uso de la herramienta?	Disponibilidad	1	2	3	4	5
5. ¿Cómo considera la integridad de la información en el uso de la herramienta?	Integridad	1	2	3	4	5
6. ¿Qué tan accesible considera el uso de la herramienta?	Accesibilidad	1	2	3	4	5

Fuente: Elaboración propia

El cuestionario virtual de 6 preguntas (Anexo 2) fue aplicado a las personas pertenecientes a la oficina general de sistemas informáticos y plataformas virtuales, basándose en la siguiente tabla (tabla 27).

Tabla 27 Calificación de Satisfacción del Uso de la Herramienta Nagios – Método Top two Box

N°	Pregunta	5 E	4 MB	3 B	2 R	3 M
1	¿Cómo considera la efectividad de la herramienta?					
2	¿Cómo considera el tiempo de identificación de Incidentes?					
3	¿Cómo considera la confidencialidad de la información en el uso de la herramienta?					
4	¿Cómo considera la disponibilidad de la información en el uso de la herramienta?					
5	¿Cómo considera la integridad de la información en el uso de la herramienta?					
6	¿Qué tan accesible considera el uso de la herramienta?					

Fuente: Elaboración Propia.

- Nivel de satisfacción en el uso de la Herramienta

Para obtener los datos del uso de herramienta, se utilizó la información recopilada del cuestionario del anexo 2 y usando como referencia la tabla 25 se resumió en la información den la siguiente tabla (tabla 28).

Tabla 28 Resultados obtenidos al realizar Encuesta de Satisfacción

Usuario	Efectividad	Tiempo	Confidencialidad	Disponibilidad	Integridad	Accesibilidad
Usuario 1	4	5	4	5	4	5
Usuario 2	4	4	4	4	4	4
Usuario 3	5	4	5	4	4	3
Usuario 4	5	5	5	5	5	5

Fuente: Elaboración propia

De tal forma se continuó el cálculo estadístico de los datos de la variable independiente, usando hojas de cálculo en Excel, para obtener mediante tablas dinámicas los resultados porcentuales según la teoría de Top two Box, como se observa en la tabla 29 los resultados casi en su totalidad se encuentran en los valores 4 y 5, que implican valores de bueno y muy bueno evidenciando un nivel satisfactorio, el único valor 3 registrado, según la teoría, se asume como un valor que disminuye el porcentaje aceptable, por tal motivo es que el aspecto accesibilidad muestra sólo un 75% de satisfacción.

Tabla 29 Tablas Dinámicas de Satisfacción - Método Top two box

Etiquetas de fila	Cuenta de Efectividad
4	50%
5	50%
Total general	**100%**

Etiquetas de fila	Cuenta de Confidencialidad
4	50%
5	50%
Total general	**100%**

Etiquetas de fila	Cuenta de Tiempo
4	50%
5	50%
Total general	**100%**

Etiquetas de fila	Cuenta de Disponibilidad
4	50%
5	50%
Total general	**100%**

Etiquetas de fila	Cuenta de Tiempo
3	25%
4	25%
5	50%
Total general	**100%**
Total Contable	75%

Etiquetas de fila	Cuenta de Integridad
4	75%
5	25%
Total general	**100%**

Fuente: Elaboración propia

Tabla 30 Resultados porcentuales según aspectos evaluados criterios de Satisfacción

Efectividad	Tiempo	Confidencialidad	Disponibilidad	Integridad	Accesibilidad
100%	100%	100%	100%	100%	75%

Fuente: Elaboración propia

Finalmente, la presente investigación obtiene como resultado los niveles de satisfacción al 100% en 5 rubros y 75% en accesibilidad (tabla 30), a pesar de la diferencia en el 6° rubro los resultados obtenidos siguen siendo positivos en su totalidad.

CAPÍTULO IV. ANÁLISIS Y DISCUSIÓN DE RESULTADOS

Basándonos en los resultados obtenidos en la investigación, se acepta la hipótesis general, al decir que el uso de un sistema de soporte a la seguridad de la Información usando big data mejorará la gestión de infraestructura de tecnologías de información en la Universidad Nacional de Cajamarca, esto se puedo definir por las diferencias porcentuales en las tasas que se muestran a continuación.

4.1. ANÁLISIS DE RESULTADOS

Con el indicador de la variable sistema de soporte a la seguridad de la información, se buscó que al finalizar el tiempo de uso se compruebe que el nivel de satisfacción del usuario al usar la herramienta fue lo más aceptable posible, según se observa en el gráfico 1 la respuesta dada por los usuarios fue totalmente buena, ya que en el aspecto efectividad, tiempo, confidencialidad, disponibilidad e Integridad la puntuación fue entre 4 y 5 por todos los usuarios, es decir que el 100% de usuarios considera que el Nivel de satisfacción es total mente bueno en esos rubros, vale recalcar que dentro de estos 5 rubros, se mencionan las principales características de la seguridad de la información; sin embargo en accesibilidad, solo el 75% considera que la herramienta es buena.

Gráfico 1 Nivel de Satisfacción de Usuarios

Fuente: Elaboración propia

Esta investigación trabajó con indicadores netamente cuantitativos en la variable dependiente, por lo cual, si hubo una comparación antes y durante el uso de la herramienta, en el indicador “Incidentes identificados”, según estadísticas, se

registró que, sin el uso de la herramienta, el reporte final fue de 38 incidentes y durante el proceso de prueba 2918, es decir 7579 veces más.

Cifras que llevadas a porcentajes expresan un alto impacto, la tabla 30 muestra cómo el número de reportes se elevó en 7579% más, es decir la tasa muestra un cambio favorable que afirma nuevamente la hipótesis planteada.

Tabla 31 Comparación de % Pre y Post Prueba – "Incidentes identificados"

Sin Usar Herramienta		Usando herramienta		Incremento
Incidentes	**%**	**Incidentes**	**%**	**%**
38	100%	2918	7679%	7579%

Fuente: Elaboración propia

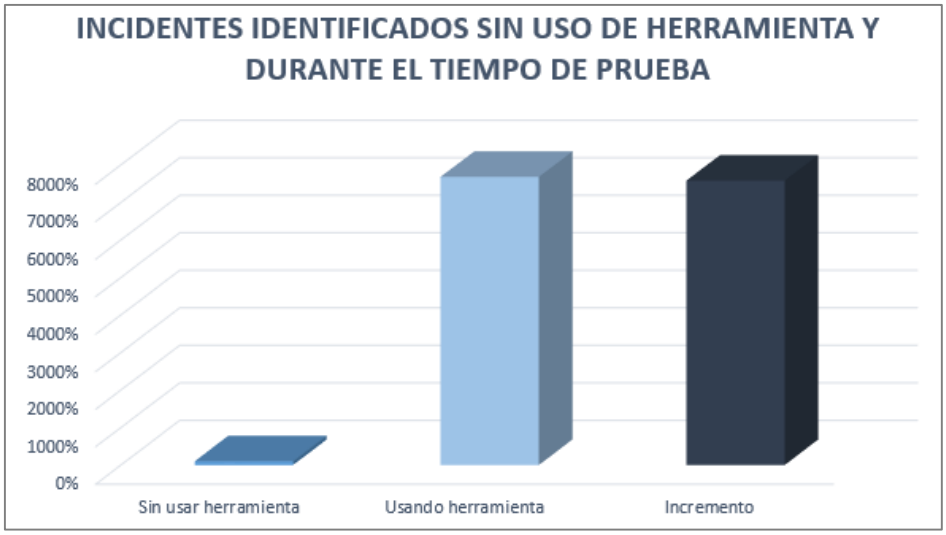


Gráfico 2 Incidentes Identificados sin Uso de herramienta vs durante el tiempo de prueba

Fuente: Elaboración propia

Po otro lado la presente investigación en el indicador "Incidentes controlados", registró que 33 incidentes fueron controlados sin el uso de la herramienta y usando la herramienta 403, es decir 1121 veces más; nuevamente la variación de la tasa es muy alta, comprobando la efectividad de la hipótesis.

Tabla 32 Comparación de % Pre y Post Prueba – "Incidentes Controlados"

Sin Usar Herramienta		Usando herramienta		Incremento
Incidentes	**%**	**Incidentes**	**%**	**%**
33	100%	403	1221%	1121%

Fuente: Elaboración propia

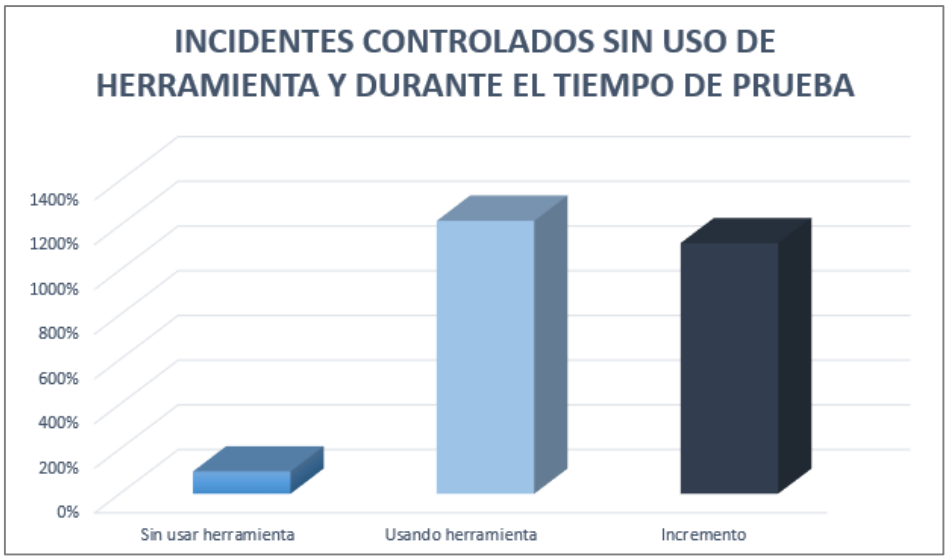


Gráfico 3 Incidentes Identificados sin Uso de herramienta vs durante el tiempo de prueba

Fuente: Elaboración propia

Tanto el indicador de incidentes controlados y reportados con el uso de la herramienta son muestra de que nagios trabaja con una gran cantidad de información, fortaleciendo y corroborando el fin del uso del big data.

4.2. DISCUSIÓN DE RESULTADOS

A partir de los resultados obtenidos, se acepta la hipotesis alternativa general que establece que existe relación de dependencia entre el uso del sistema de soporte a la seguridad de la información usando big data para y la gestión de infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca.

Estos resultados guardan relación con lo que propone Gutiérrez [4] respecto a la adopción de tecnología que permita manejar big data y la importancia de esta en la seguridad de la información a tratar, de la misma forma Otarán y Perera [5] plantean el uso de herramientas que realicen seguimientos métricos sobre servicios de software, salud de los servidores y el rendimiento de los equipos, en su tesis ellos informan sobre monitoreo de 3 aplicaciones del cuan buscaron detectar fallas en el hardware y software, en todos ellos fue recolectando los logs de las aplicaciones y descubrieron comportamientos que afecten la funcionalidad de las aplicaciones, el 100% dio una respuesta positiva al monitoreo y evidenció gran cantidad de información, lo mencionado anteriormente es acorde con lo que en el presente estudio se halla, puesto que para delimitar las áreas a evaluar se buscó conocer el negocio sus procesos críticos y necesidades primordiales, las

áreas investigadas mediante el monitoreo de la herramienta nagios fueron registrando información mediante logs, facilitando identificar donde es el manejo masivo de datos y mayor cantidad de incidencias, adicionalmente se hizo uso de herramientas de manejo de datos, siguiendo políticas de seguridad de Información en la Universidad Nacional de Cajamarca, consiguiendo que el usuario y experto rastree también el 100% de lo propuesto.

Por otro lado la propuesta que hace Santander [6] define que el crecimiento tan rápido del Big Data aún presenta necesidades que suplir en cuestiones de seguridad, se coincide y se ha mostrado en este informe que la gran carga de datos y continua generación de ellos, ya que en su investigación evidencia que el uso de big data en los proceso tecnológicos incrementan potencialmente la información a tratar, según su estudio se evidencia que el manejo de información crece a 150 veces más de lo establecido y de tal forma crecen las vulnerabilidades, en definitiva, se precisa proteger un sistema que cumpla con las características básicas que presenta el Big Data, en cuanto a volumen y velocidad se refiere, de ahí a una necesidad de protección completa para sus almacenes de datos, de la misma forma la presente investigación evidenció en los resultados la impactante variación de tasas en los registros de incidentes, de hasta más de 7000 veces, coincidiendo que los procesos tecnológicos implican mucha información a tratar.

Por otro lado Aquije y Jave [3] mencionan que es necesario implementar metodologías SGSI (Sistema de Gestión de Seguridad de la Información) para el control de Seguridad de Información y se basen en la metodologia Demming, en lo que no concuerda el presente estudio, ya que no es siempre es necesario que se use SGSI para el monitoreo o control del área de tecnologías de información, como se ha descrito en el desarrollo, se puede usar herramientas de monitoreo y sistemas de soporte para manejar de forma correcta la seguridad del área de TI, adicionalmnete cuando se inicia un análisis para la implementación del sistema, es necesaria una metodología de desarrollo, como se ha dado en este estudio, Kanban es util para que de manera ágil y eficiente se de solución a lo planificado sin la necesidad de seguir la metodología Demming que se recomienda en procesos de mejora continua.

En esta investigación los resultados referentes al uso de herramienta y satisfacción del usuario guardan relación con Quispe [8] al mencionar el logro y comprobación efectiva y constante de los servicios y dispositivos (host, procesador, memoria RAM, Router, Fibra Óptica, Access Point, servidor) [8], según los resultados mostrados en su informe precisa que el 67% de los usuarios encuestados determinan que la disponibilidad, manejo y diseño tiene un calificativo independiente de excelente y el 33% los califica como regular, asegurando una reacción optima en la intervención de la solución a los fallos evidenciados en ellos, generando una mejor administración de los servicios, adicionalmente indica que la asistencia en incidencias mejora después de la implementación del sistema en un 81% para los de alto nivel [8], se coincide en que la herramienta Nagios permite identificar y resolver problemas de infraestructura de TI antes que ellos afecten los procesos de negocios críticos [8], ya que los reportes son casi inmediatos a su identificación, el estudio de Quispe indica que la aceptación por parte del público fue dada en unanimidad, el presente informe coincide que en 100% los usuarios tienen una aceptación en el criterio “Seguridad de la Información” y un porcentaje aceptable de 75% en accesibilidad y 100% en tiempo y efectividad. Se coincide que tanto en diseñado con aceptación y seguridad de datos, es una gran herramienta que no solo permite detectar, sino también ir disminuyendo eventos próximos antes que causen efectos sobre el usuario final.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Se logró cumplir el objetivo general propuesto en la investigación, proponer un sistema de soporte a la seguridad de la información usando big data para mejorar la gestión de la infraestructura de tecnologías de información de la Universidad Nacional de Cajamarca, corroborando la influencia positiva de la variable independiente (sistema de soporte a la seguridad de la Información) sobre la variable dependiente (gestión de Infraestructura de TI), precisa mencionar que el sistema de soporte recibió y validó la investigación con una gran cantidad de datos, incrementando en 7579% el número de incidentes identificados, importante logro a concluir ya que fortalece aún más el planteamiento de la hipótesis desde el aspecto de big data.
- Se logró determinar las características de un sistema de soporte a la seguridad de la información usando big data, que permita el monitoreo automático y su comunicación inmediata al usuario, facilitando la labor al equipo delegado, entre las principales características identificadas se menciona la disponibilidad, confiabilidad e integridad de la información, las cuales fueron calificadas como excelente o muy bueno, es decir el 100% de usuarios caracterizan a la herramienta como segura.
- Se caracterizó y delimitó los dominios de protección en la gestión de la Infraestructura de TI de la Universidad Nacional de Cajamarca, identificando 5 áreas de mayor importancia o criticidad en la oficina general de sistemas informáticos y plataformas virtuales.
- Se implementó la herramienta nagios, consiguiendo desplegar el sistema de soporte a la seguridad con los dominios identificados, dentro de la oficina general de sistemas informáticos y plataformas virtuales, sin ningún inconveniente a los accesos o IP establecidos y a su vez nagios permitió identificar sus servicios respectivamente, esta herramienta permitió evaluar de forma paralela y en tiempos de milisegundos cada host.

- Culminado el análisis y tratamiento de datos se pudo evaluar y analizar la influencia del sistema de seguridad en la gestión de la infraestructura de TI, permitiendo validar la hipótesis de forma afirmativa. Se consiguió adaptar la herramienta a las necesidades encontradas, llevando consigo una mejora en la Gestión de Infraestructura de TI en la Universidad Nacional de Cajamarca.

5.2. RECOMENDACIONES

- Recomendar a la Universidad Nacional de Cajamarca que mantenga siempre de forma óptima los ambientes y herramientas tecnológicas, ya que eso se convierte en un influyente de la gestión de TI.
- La implementación de un manual o guía para saber cómo actuar cuando se reporten incidentes repetitivos, priorizando altamente la importancia de mantener el control y correcta gestión de la infraestructura de TI en la oficina general de sistemas informáticos y plataformas virtuales.
- Se debe realizar una mejora continua por parte del equipo, es decir un nuevo análisis de requerimientos para complementar el diseño y funcionalidad del sistema de soporte a la seguridad en la oficina general de sistemas informáticos y plataformas virtuales.
- Se recomienda organizar el monitoreo en toda la institución, según las áreas de criticidad, equipos e infraestructura de TI de la Universidad Nacional de Cajamarca.
- Es recomendable que en un futuro se utilice herramientas para la gestión de proyectos, reporte y resolución de incidencias, que complemente la investigación realizada en oficina general de sistemas informáticos y plataformas virtuales.
- Realizar constantes capacitaciones a usuarios del sistema de soporte de seguridad en la gestión de TI en la Universidad Nacional de Cajamarca.

BIBLIOGRAFÍA

[1] Ó. Condés, «TICbeat,» TICbeat.com - Axel Springer España S.A., 16 Enero 2016. [En línea]. Available: http://www.ticbeat.com/seguridad/el-empleado-es-el-punto-dbil-para-la-seguridad-de-las-empresas/. [Último acceso: 16 diciembre 2018].

[2] A. A. Aguirre Ponce, «Ciberseguridad en Infraestructuras Críticas,» Universidad de Buenos Aires, buenos Aires, 2017.

[3] J. G. AQUIJE QUIJANDRIA y L. L. JAVE BOBADILLA, «METODOLOGÍA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL SECTOR FINANCIERO EN EL PERU,» Universidad Nacional de Ingenieria, Lima, Peru, 2012.

[4] C. Gutierrez Amaya, «Welivesecurity by ESET,» 29 enero 2014. [En línea]. Available: https://www.welivesecurity.com/la-es/2014/01/29/que-representa-big-data-seguridad-informacion/. [Último acceso: 10 Dciembre 2018].

[5] M. B., «Welivesecurity,» 29 Enero 2014. [En línea]. Available: https://www.welivesecurity.com/la-es/2014/01/29/que-representa-big-data-seguridad-informacion/. [Último acceso: 16 abril 2020].

[6] F. Otarán y N. Perera, «Propuesta de una solución de monitoreo para sistemas del CeSPI,» Universidad Nacional de La Plata, La Plata, 2017.

[7] I. Santander, «ANALISIS Y PROPUESTA DE ARQUITECTURA PARA GARANTIZAR SEGURIDAD EN ENTORNOS BIG DATA,» Universidad Aut´onoma de Madrid, Madrid, 2017.

[8] J. Quispe Bustino, «Repositorio UNA,» 2017. [En línea]. Available: http://repositorio.unap.edu.pe/bitstream/handle/UNAP/9019/Quispe_Bustincio_Jhon_Watson.pdf?sequence=1&isAllowed=y. [Último acceso: 15 abril 2020].

[9] S. I. Tecon, «Tecon,» Copyright - Tecon, [En línea]. Available: https://www.tecon.es/la-seguridad-de-la-informacion/. [Último acceso: 10 2019].

[10] C. Silva, «Ciberseguridad,» Ministerio de la Secretaria General de la Presidencia del Gobierno de Chile, Santiago de Chile, 2018.

[11] M. Rouse, «TechTarget,» TechTarget, S.A de C.V, agosto 2014. [En línea]. Available: https://searchdatacenter.techtarget.com/es/definicion/Gestion-de-TI. [Último acceso: 15 febrero 2019].

[12] «Wikipedia,» [En línea]. Available: https://es.wikipedia.org/wiki/Gesti%C3%B3n_de_incidentes. [Último acceso: 01 marzo 2019].

[13] «Service Tonic,» [En línea]. Available: https://www.servicetonic.es/itil/itil-v3-gestion-de-incidencias/. [Último acceso: 01 marzo 2019].

[14] M. f. t. i. o. C. I. a. a. s. Infrastructure, «Ensia Europa,» [En línea]. Available: https://www.enisa.europa.eu/publications/methodologies-for-theidentification-of-ciis . [Último acceso: 08 diciembre 2018].

[15] «Nacional, Riesgos y Amenazas para la Seguridad,» [En línea]. Available: http://www.dsn.gob.es/es/sistema-seguridad-nacional/qu%C3%A9-esseguridad-nacional/riesgos-amenazas-para-seguridad-nacional (. [Último acceso: 05 diciembre 2018].

[16] « THE ITU NATIONAL CYBERSECURITY STRATEGY GUIDE,» [En línea]. Available: http://www.itu.int/ITUD/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf . [Último acceso: 05 diciembre 2018].

[17] N. Networks, «North Networks,» [En línea]. Available: https://www.north-networks.com/nagios/. [Último acceso: 21 abril 2020].

[18] E. Espinoza, D. Lorio, M. Mendoza y M. Ruiz, «Slideshare,» 29 Agosto 2013. [En línea]. Available: https://www.slideshare.net/mmendoz4/informe-nagios-proyecto-operacin-y-monitoreo-de-redes.

[19] NAGIOS, «Nagios Org,» Nagios Enterprises, [En línea]. Available: https://www.nagios.org/about/overview/. [Último acceso: 2019 08 28].

[20] NAGIOS, «Nagios Org,» Nagios Enterprises, [En línea]. Available: https://www.nagios.org/projects/nagios-core/. [Último acceso: 2019 08 20].

[21] Jorge, «Sistemas - Web de Tecnología,» Digital Ocean, 21 Noviembre 2017. [En línea]. Available: https://nksistemas.com/instalacion-de-pnp4nagios-en-nagios-con-centos/. [Último acceso: 20 mayo 2020].

[22] C. León, «Adictos al trabajo,» 17 Agosto 2011. [En línea]. Available: https://www.adictosaltrabajo.com/2011/08/17/nagios-nagiosql-pnp-4nagios/. [Último acceso: abril 2020].

[23] Nagios, «Nagios Org,» Nagios Enterprises, [En línea]. Available: https://www.nagios.com/solutions/windows-monitoring/?__hstc=118811158.6ddbb43ac4b1defd79a5c9861d86edc9.1567693372880.1567693372880.1567693372880.1&__hssc=118811158.1.1567693372881&__hsfp=2289000598. [Último acceso: 2019 08 15].

[24] Nagios, «Nagios Org,» Nagios Enterprises, [En línea]. Available: https://www.nagios.com/solutions/linux-monitoring/?__hstc=118811158.6ddbb43ac4b1defd79a5c9861d86edc9.15676933

72880.1567693372880.1567693372880.1&__hssc=118811158.1.1567693372881&__hsfp=2289000598. [Último acceso: 2019 08 15].

[25] Nagio, «Nagiso Org,» Nagios Enterprises, [En línea]. Available: https://www.nagios.com/solutions/server-monitoring/?__hstc=118811158.6ddbb43ac4b1defd79a5c9861d86edc9.1567693372880.1567693372880.1567693372880.1&__hssc=118811158.1.1567693372881&__hsfp=2289000598. [Último acceso: 2019 05 15].

[26] Nagios, «Nagios Org,» Nagios Enterprises, [En línea]. Available: https://www.nagios.com/solutions/application-monitoring/?__hstc=118811158.6ddbb43ac4b1defd79a5c9861d86edc9.1567693372880.1567693372880.1567693372880.1&__hssc=118811158.1.1567693372881&__hsfp=2289000598. [Último acceso: 2019 08 15].

[27] Nagio, «Nagios Org,» Nagios Enterprises, [En línea]. Available: https://www.nagios.com/solutions/snmp-monitoring/?__hstc=118811158.6ddbb43ac4b1defd79a5c9861d86edc9.1567693372880.1567693372880.1567693372880.1&__hssc=118811158.1.1567693372881&__hsfp=2289000598. [Último acceso: 2018 08 16].

[28] «Nagios Org,» Nagios Enterprises, [En línea]. Available: https://www.nagios.com/solutions/log-monitoring/?__hstc=118811158.6ddbb43ac4b1defd79a5c9861d86edc9.1567693372880.1567693372880.1567693372880.1&__hssc=118811158.1.1567693372881&__hsfp=2289000598. [Último acceso: 2019 08 18].

[29] J. Olano, «Pandora,» 2016. [En línea]. Available: https://pandorafms.com/blog/es/que-es-grafana/. [Último acceso: 28 Abril 2020].

[30] «Telegram Org,» 2018. [En línea]. Available: https://telegram.org/faq_channels/es. [Último acceso: 13 mayo 2020].

[31] «The Strain Times,» Asia New Network, 20 enero 2016. [En línea]. Available: https://technology.inquirer.net/46297/telegrams-secret-chats-bots-boon-for-isis. [Último acceso: 13 mayo 2020].

[32] «Archive Org,» 24 marzo 2017. [En línea]. Available: http://web.archive.org/web/20190913160159/https://www.rbc.ru/money/24/03/2017/58d52d479a7947f73ac39092. [Último acceso: 13 mayo 2020].

[33] I. 27035, «Gub Uy,» Centro Nacional de respuesta a incidentes de seguridad informatica, [En línea]. Available: https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/comunicacion/publicaciones/que-es-un-incidente. [Último acceso: 12 agosto 2021].

[34] J. Pérez Porto y A. Gardey, «Defínción,» Definición.de, mayo 2013. [En línea]. Available: https://definicion.de/monitoreo/. [Último acceso: 18 diciembre 2018].

[35] «PowerData,» [En línea]. Available: https://www.powerdata.es/big-data. [Último acceso: diciembre 2018].

[36] «Sinnexus,» Sinergia e Inteligencia de Negocio S.L., [En línea]. Available: https://www.sinnexus.com/business_intelligence/sistemas_soporte_decisiones.aspx. [Último acceso: 08 febrero 2019].

[37] «RedHat.com,» Red Hat Production, [En línea]. Available: https://www.redhat.com/es/topics/management. [Último acceso: Octubre 2019].

[38] D. Maldonado, «Icorp,» Icorp 2019, [En línea]. Available: http://www.icorp.com.mx/blog/infraestructura-de-ti-componentes/. [Último acceso: Octubre 2019].

[39] «kio Networks,» 1 Agosto 2019. [En línea]. Available: https://www.kionetworks.com/blog/data-center/qu%C3%A9-es-un-data-center. [Último acceso: mayo 2020].

[40] Y. Semerena, «QuestionPro Investigación,» [En línea]. Available: https://www.questionpro.com/blog/es/investigacion-exploratoria/. [Último acceso: 2018].

[41] A. Dávila, «Universidad Nacional de Cajamarca,» [En línea]. Available: https://www.unc.edu.pe/index.php/nuestra-universidad/. [Último acceso: 18 Enero 2020].

[42] U. N. d. Cajamarca, «Misión - Visión,» Universidad Nacional de Cajamarca, Cajamarca, 1962.

[43] Ebergementwebs, «Ebergementwebs,» 21 NOVIEMBRE 2020. [En línea]. Available: https://www.hebergementwebs.com/tutorial-de-nagios/nagios-guia-rapida. [Último acceso: 2020].

[44] R. Izumi, «Blog Moon,» [En línea]. Available: https://blog.moon.cat/instalar-configurar-nagios-opensuse/.

[45] A. Maulana, «Scribd,» Mayo 2014. [En línea]. Available: https://es.scribd.com/document/244828722/Installing-Nagios-Core-From-Source.

ANEXOS

ANEXO 1 CUESTIONARIO - PRÁCTICAS DE MONITOREO Y GESTIÓN DE TI EN UNC

N°	Pregunta
1	¿Cómo considera la gestión de TI en la UNC, en la Oficina de Sistemas Informáticos y plataformas virtuales?
2	¿Cómo realiza la identificación de Incidentes en la Oficina de Sistemas Informáticos y plataformas virtuales?
3	¿Cómo considera la confidencialidad de la información en el uso de la herramienta?
4	¿Cómo considera la disponibilidad de la información en el uso de la herramienta?
5	¿Cómo considera la integridad de la información en el uso de la herramienta?
6	¿Qué tan frecuente es el monitoreo de los equipos en el área de TI?

Ilustración 121 Cuestionario "Prácticas de monitoreo y gestión de TI"

ANEXO 2 – CUESTIONARIO NIVEL DE SATISFACCIÓN

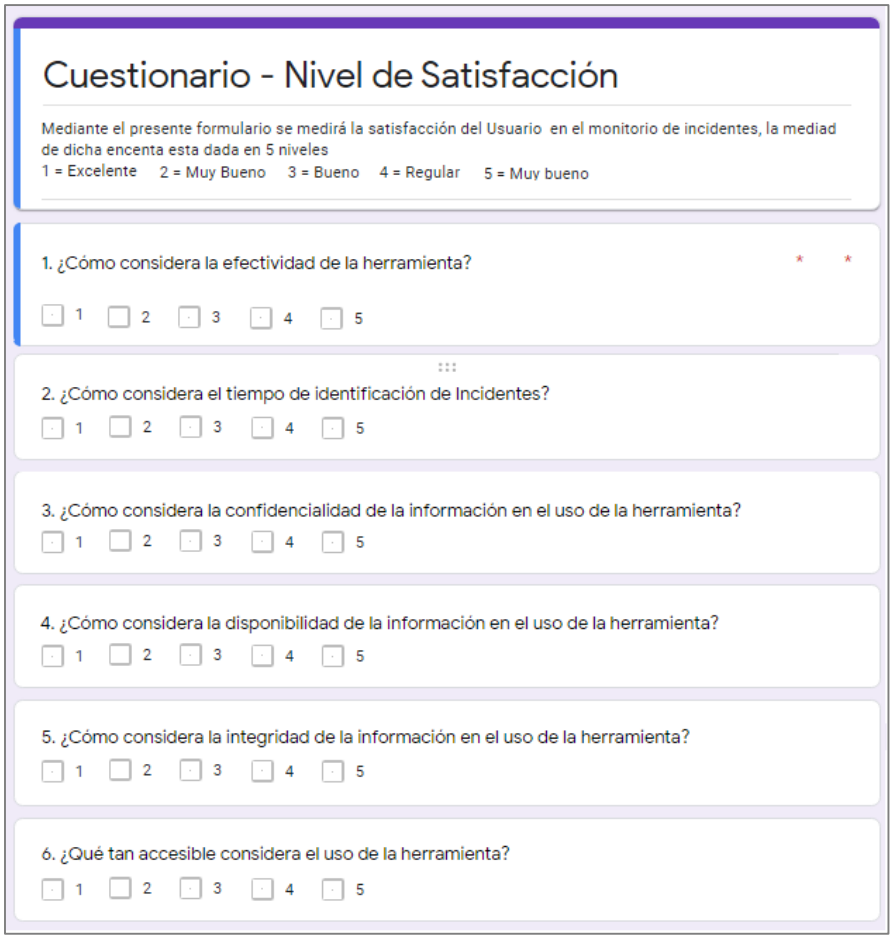


Ilustración 122 Cuestionario - Nivel de Satisfacción - tomado de forma virtual

ANEXO 3 – CONFIABILIDAD DEL INSTRUMENTO

Para la evaluación de la confiabilidad del instrumento para la recolección de datos, se utilizó hojas de cálculo Excel, considerando los siguientes ítems:

- Coeficiente alfa > 0.9: excelente

- Coeficiente alfa > 0.8 bueno

- Coeficiente alfa > 0.7: aceptable

- Coeficiente alfa < 0.6 es cuestionable

La evaluación de la ficha se realizó de la siguiente manera

Tabla 33 : Cálculo de confiabilidad del instrumento cuestionario Nivel de satisfacción

	P1	P2	P3	P4	P5	P6	Total
Usuario 1	4	5	4	5	4	5	27
Usuario 2	4	4	4	4	4	4	24
Usuario 3	5	4	5	4	4	3	25
Usuario 4	5	5	5	5	5	5	30
Varianza	0.3	0.3	0.3	0.3	0.2	0.7	5.25
∑ varianza de items	1.875						

$$\propto = \frac{n}{n-1}\left[1 - \frac{\Sigma\, Vi}{\Sigma\, Vt}\right]$$

Numero de items del instrumentos	n	4
Sumatoria de varianzas de los items	Vi	1.875
Varianza total del instrumento	Vt	5.25
Coeficiente de confiabilidad del cuestionario	α	0.857

ANEXO 4 – VALIDACIÓN DEL INSTRUMENTO CUESTINOARIO

FICHA DE VALIDACIÓN DEL INSTRUMENTO

Yo, **ROCIO HUAMÁN RAMOS**, identificada con el DNI N° 44706307, especialista en Analisis de sistemas, cuento con el grado de Ingeniera de Sistemas y ejerzo la carrera profesional en Proyecto BID en el Organismo Supervisor de las Contrataciones del Estado –OSCE.

Por medio de la presente hago constar que he revisado, únicamente con fines de validación, el instrumento "Cuestionario – Nivel de Satisfacción", a los efectos de su aplicación en la investigación "SISTEMA DE SOPORTE A LA SEGURIDAD DE LA INFORMACIÓN USANDO BIG DATA PARA MEJORAR LA GESTIÓN DE LA INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE CAJAMARCA" de la alumna Edith Esther Cáceres Tafur.

Luego del análisis y observaciones pertinentes detallo:

INDICADOR		CRITERIO	VALORACIÓN				
			D	M	R	B	MB
1	**Coherencia**	Mantiene relación lógica con la dimensión a medir					X
2	**Claridad**	Su formulación mantiene un lenguaje claro y comprensible					X
3	**Redacción**	El lenguaje usado es apropiado					X
4	**Objetividad**	Permite medir hechos empíricos y observables					X
5	**Relevancia**	La pregunta es de importancia en el cuestionario					X
6	**Congruencia**	Contribuye a la investigación y prueba de hipótesis					X
7	**Académico**	Se fundamenta en bases teóricas					X

D: deficiente - M: malo - R: regular - B: bueno - MB: muy bueno

RESULTADO DE VALORACIÓN PORCENTUAL: 100%

Fecha: 17/09/2020

Firma de la experta
DNI: 44706307
CIP: 155804

Ilustración 123 Validación del instrumento cuestionario por la experta

ANEXO 5 – VALIDACIÓN DEL INSTRUMENTO FICHA DE OBSERVACIÓN

FICHA DE VALIDACIÓN DEL INSTRUMENTO

Yo, **ROCIO HUAMÁN RAMOS**, identificada con el DNI N° 44706307, especialista en Análisis de sistemas, cuento con el grado de Ingeniera de Sistemas y ejerzo la carrera profesional en Proyecto BID en el Organismo Supervisor de las Contrataciones del Estado –OSCE.

Por medio de la presente hago constar que he revisado, únicamente con fines de validación, el instrumento "Ficha de Observación", a los efectos de su aplicación en la investigación "SISTEMA DE SOPORTE A LA SEGURIDAD DE LA INFORMACIÓN USANDO BIG DATA PARA MEJORAR LA GESTIÓN DE LA INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN DE LA UNIVERSIDAD NACIONAL DE CAJAMARCA" de la alumna Edith Esther Cáceres Tafur.

Luego del análisis y observaciones pertinentes detallo:

INDICADOR		CRITERIO	VALORACIÓN				
			D	M	R	B	MB
1	**Coherencia**	Mantiene relación lógica con la dimensión a medir					X
2	**Claridad**	Su formulación mantiene un lenguaje claro y comprensible					X
3	**Redacción**	El lenguaje usado es apropiado					X
4	**Objetividad**	Permite medir hechos empíricos y observables					X
5	**Relevancia**	La pregunta es de importancia en el cuestionario					X
6	**Congruencia**	Contribuye a la investigación y prueba de hipótesis					X
7	**Académico**	Se fundamenta en bases teóricas					X

D: deficiente - M: malo - R: regular - B: bueno - MB: muy bueno

RESULTADO DE VALORACIÓN PORCENTUAL: 100%

Fecha: 17/09/2020

Firma de la experta
DNI: 44706307
CIP: 155804

Ilustración 124 Validación del instrumento ficha de observación por la experta

ANEXO 6 - INSTALACIÓN DE NAGIOS

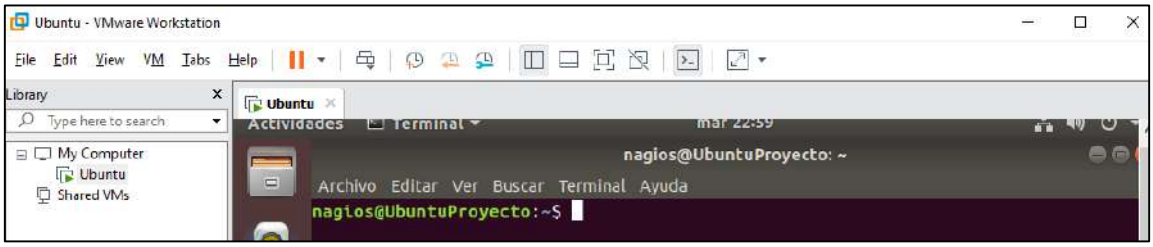


Ilustración 125 Maquina VirtualUbunto - Nagios@UbuntuProyecto

Ilustración 126 Actualización del Sistema

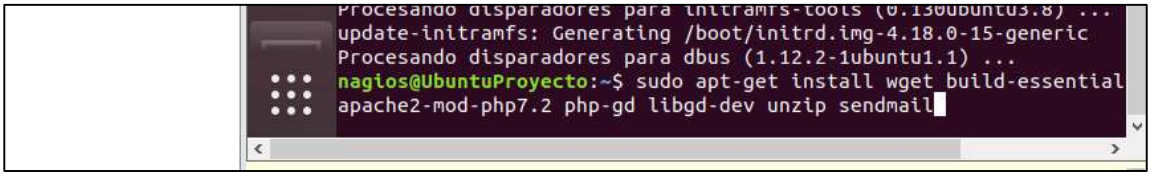


Ilustración 127 Instalación de dependencias

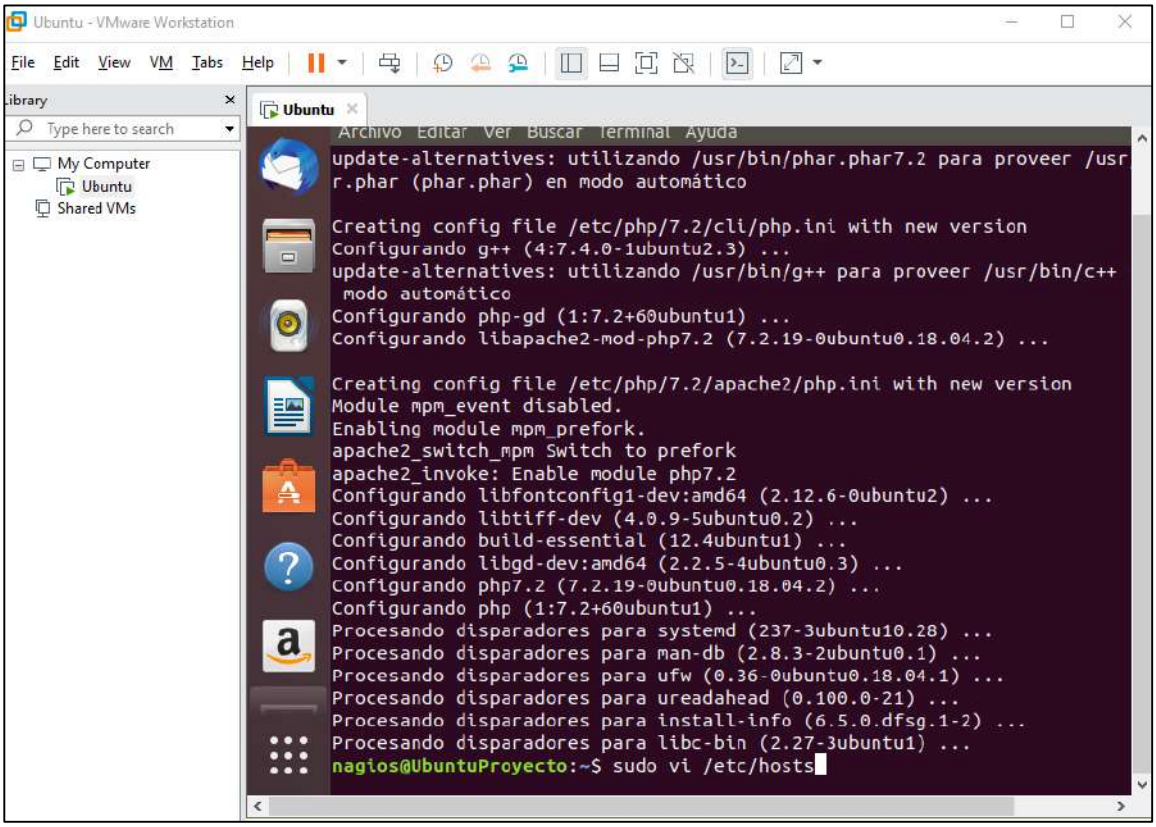


Ilustración 128 Servidor añadido

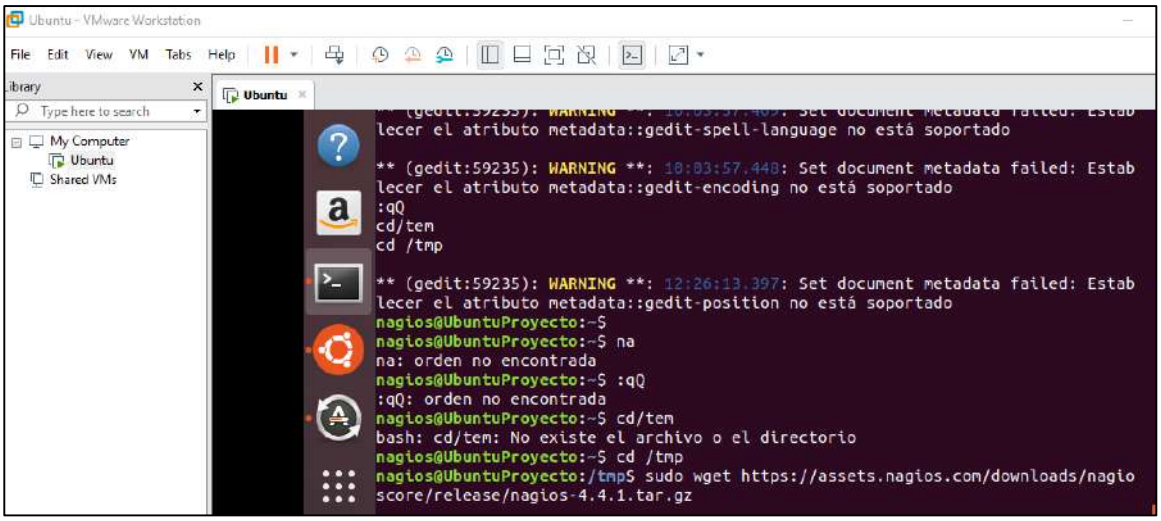


Ilustración 129 Comando descarga Nagios 4.4.1

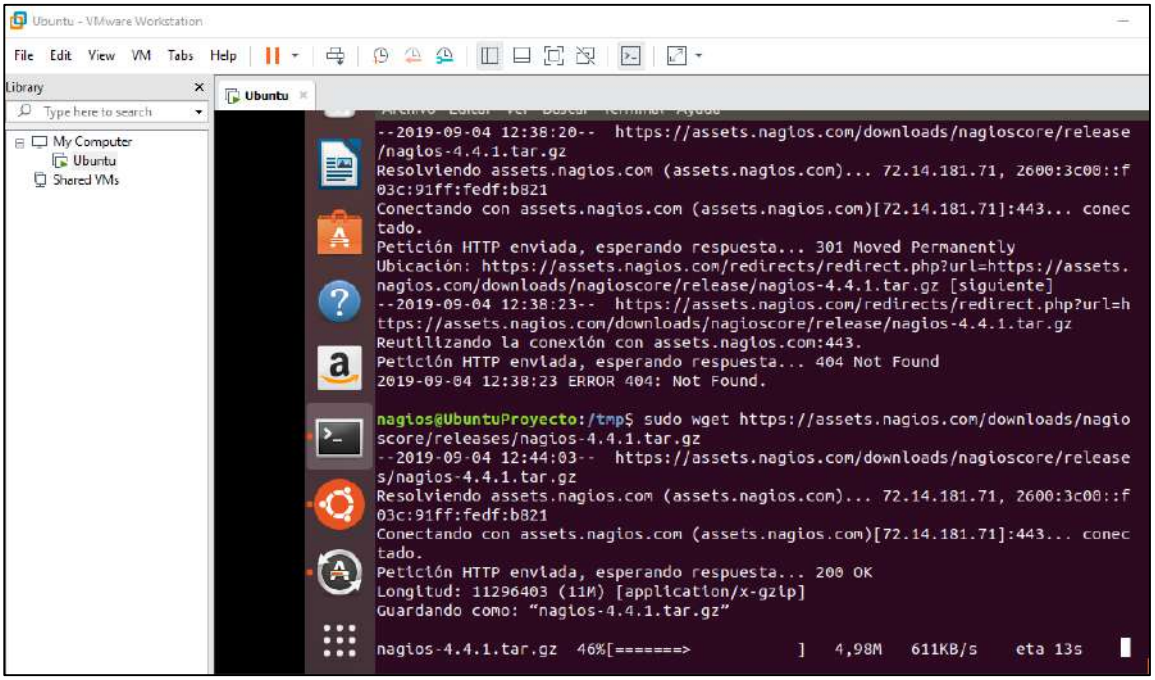


Ilustración 130 Comando descarga de plugins

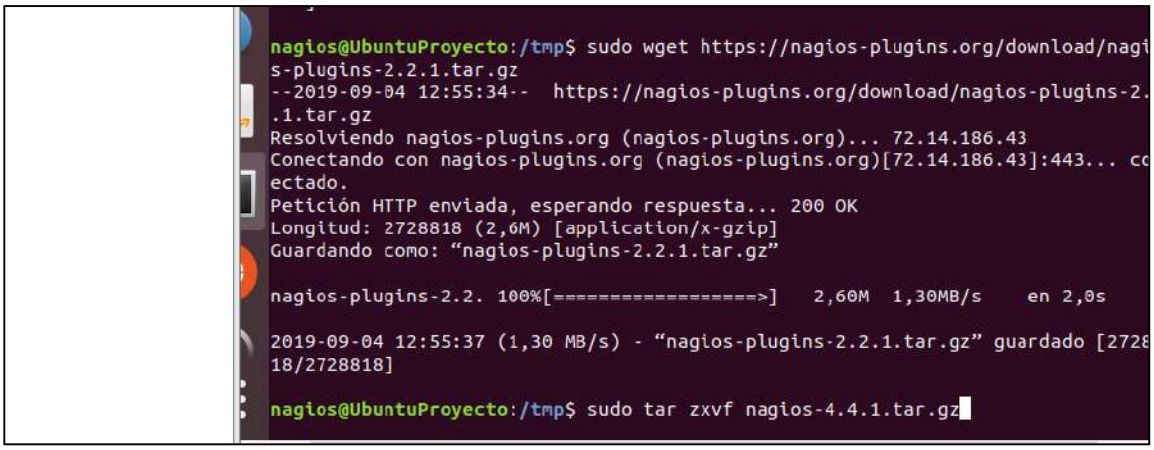


Ilustración 131 Descomprimir ficheros Nagios 4.4.1

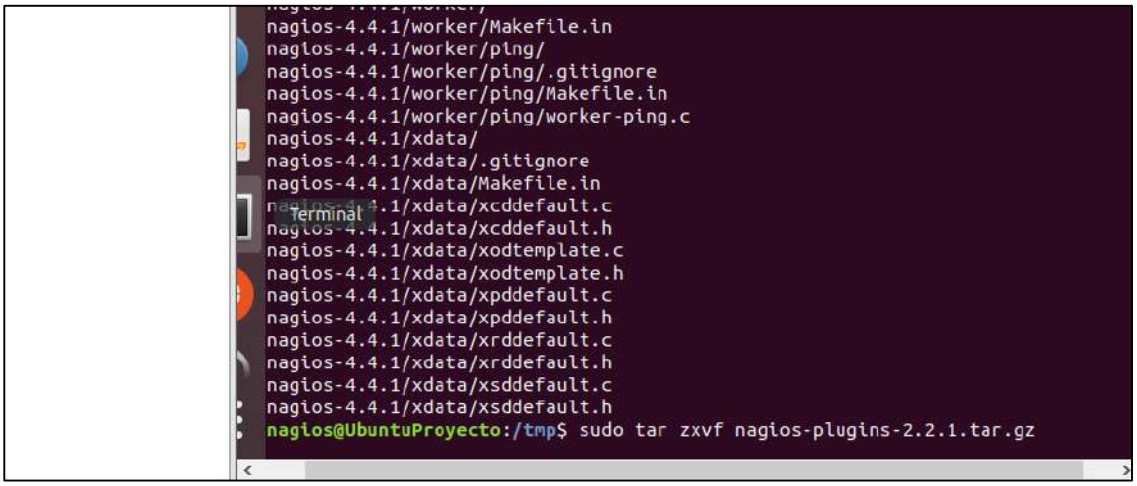


Ilustración 132 Descomprimir Plugins

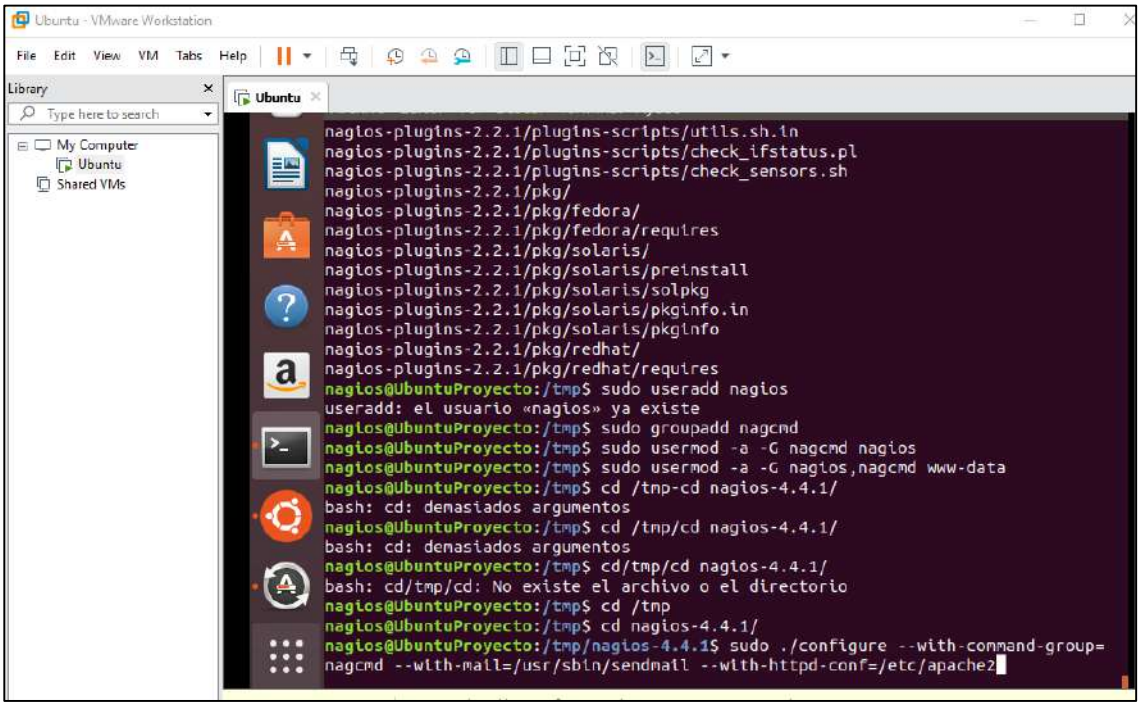


Ilustración 133 Creación de usuarios y permisos

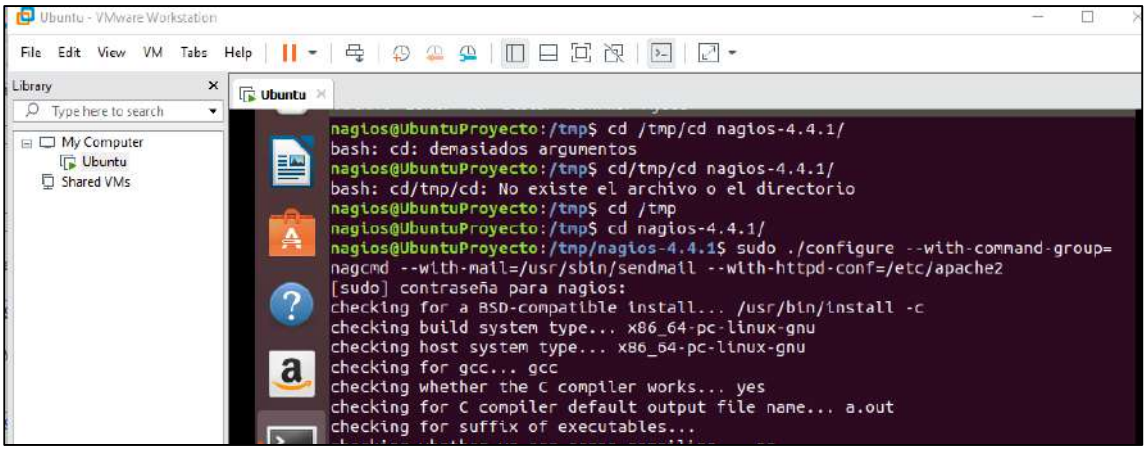


Ilustración 134 Creación de ficheros de configuración

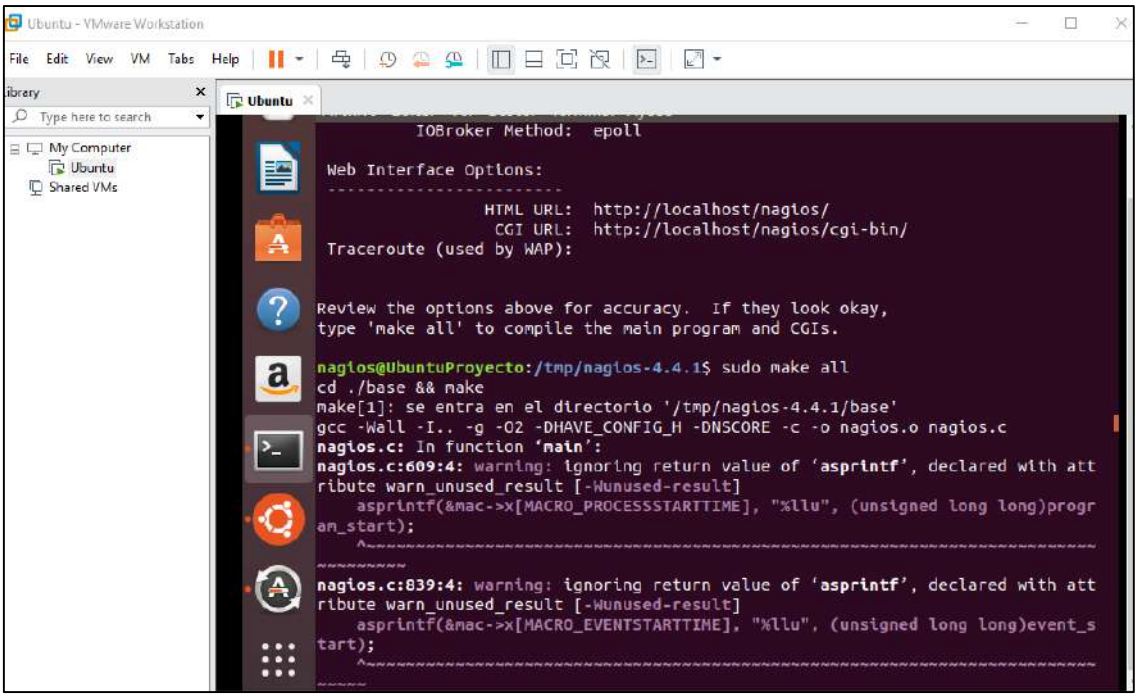


Ilustración 135 Descarga e instalación 1

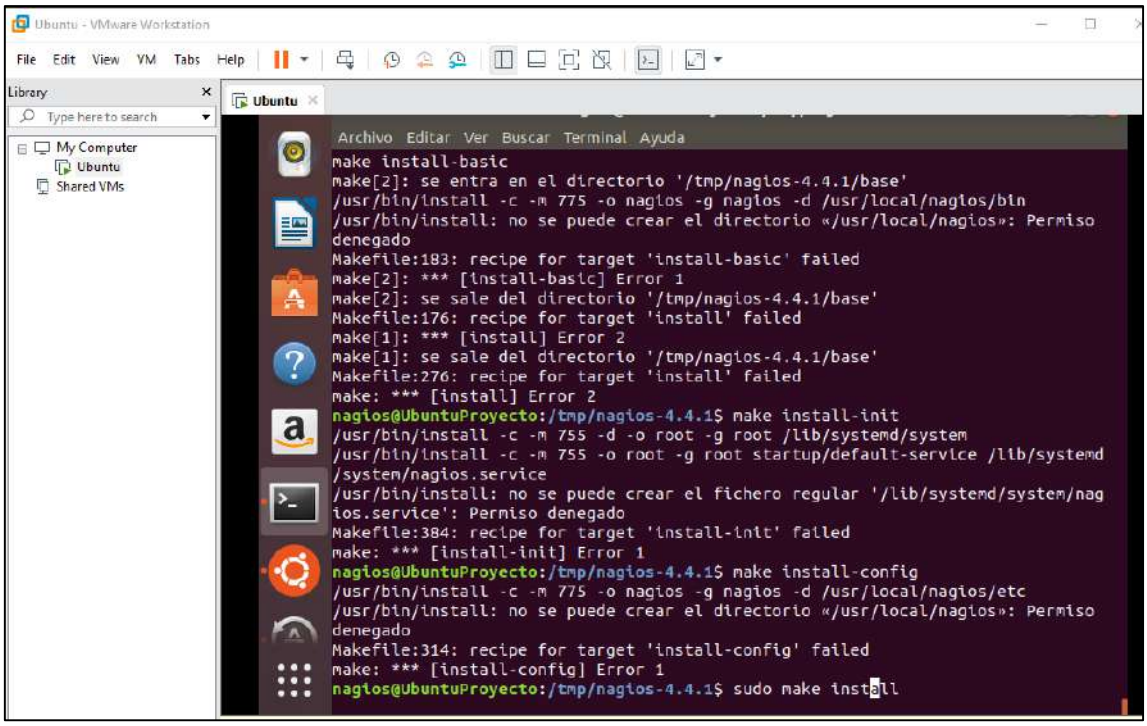


Ilustración 136 Descarga e instalación 2

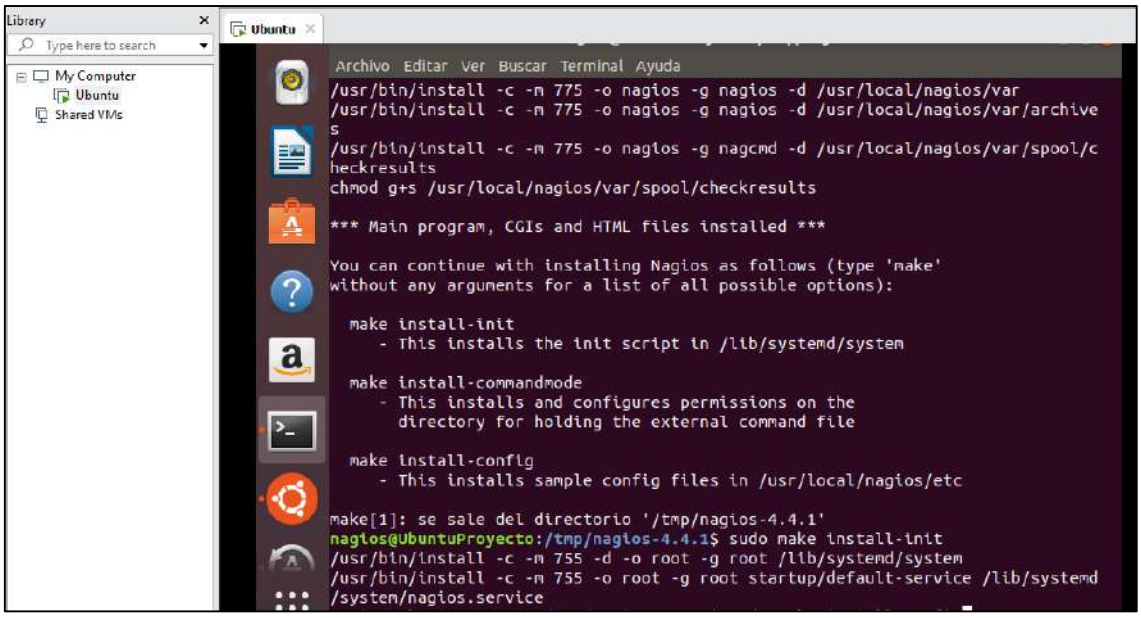


Ilustración 137 Descarga e instalación 3

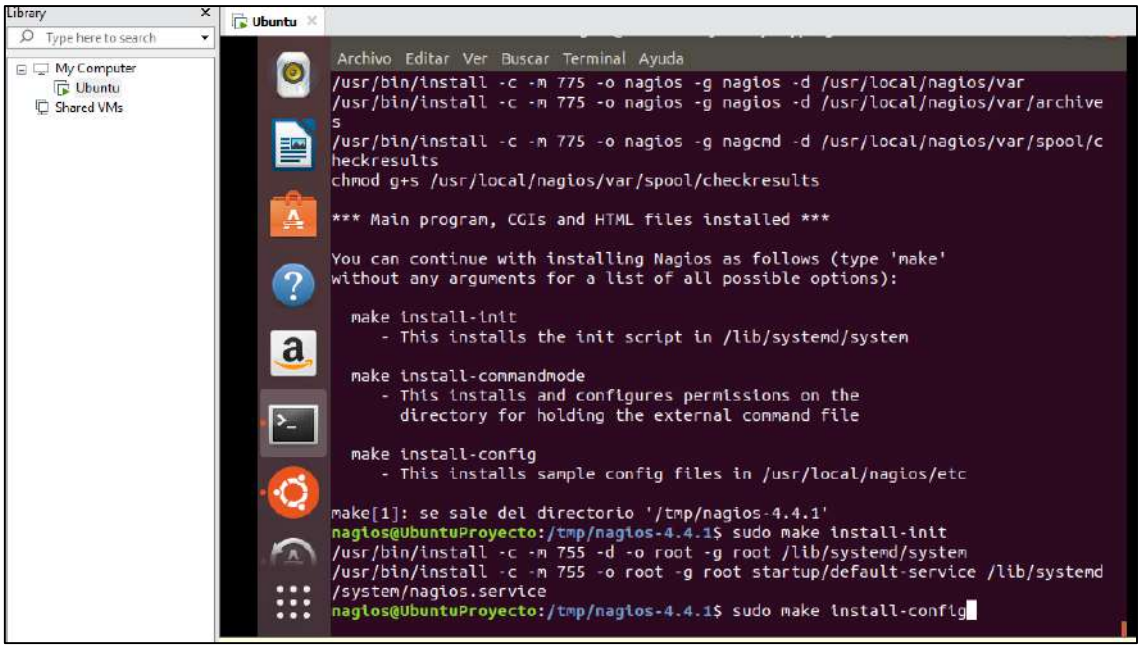


Ilustración 138 Descarga e instalación 4

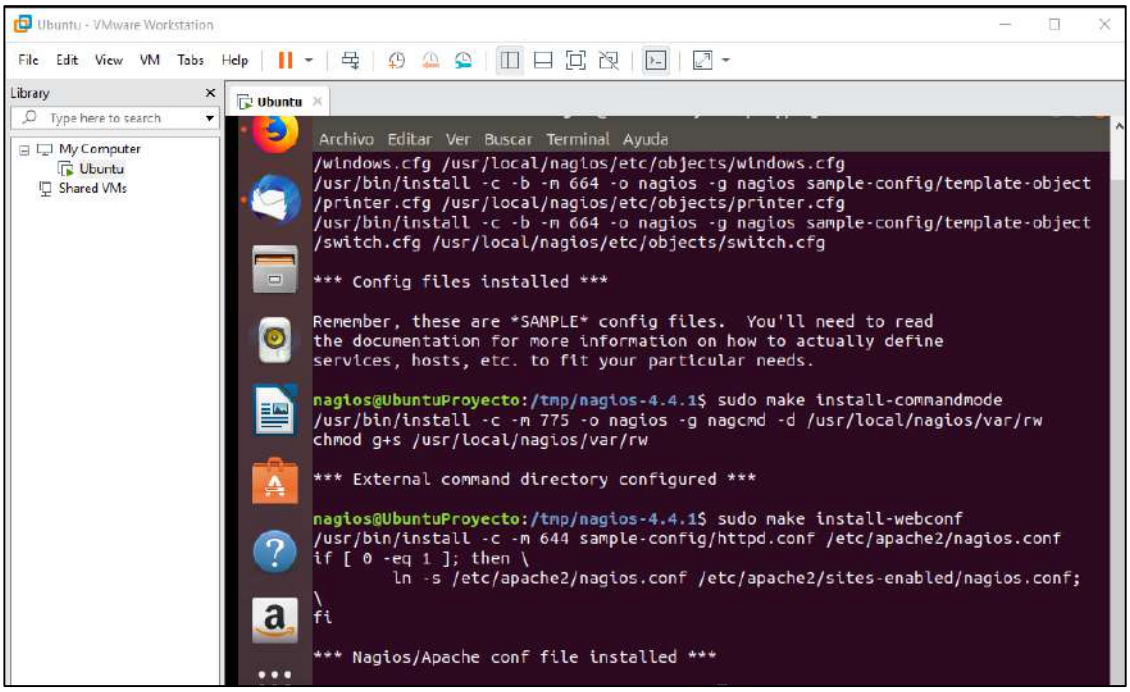


Ilustración 139 Descarga e instalación 5

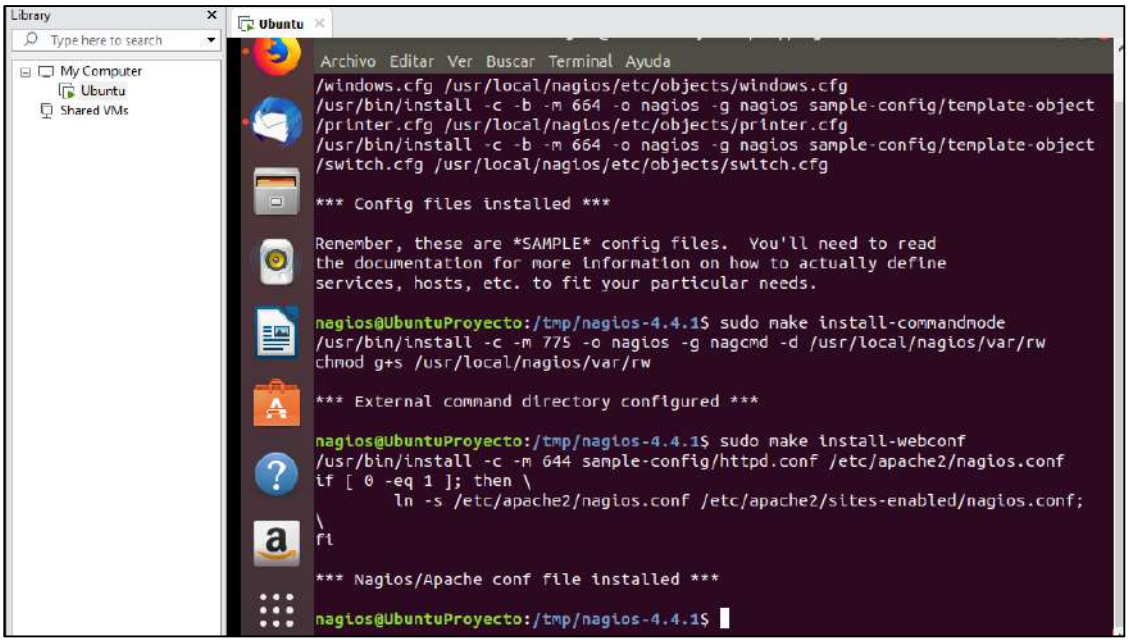


Ilustración 140 Descarga e instalación 6

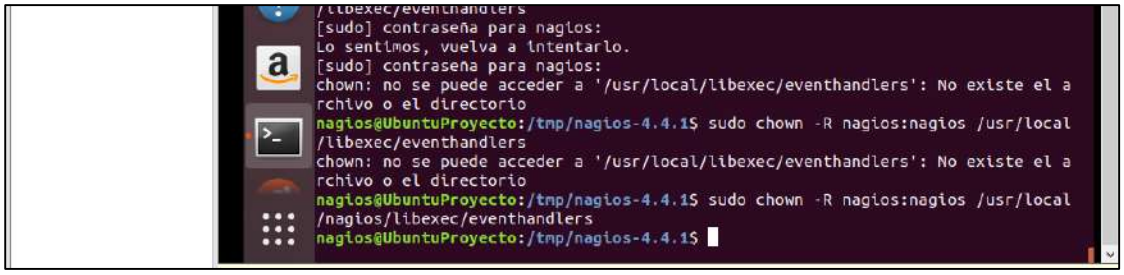


Ilustración 141 Descarga e instalación 7

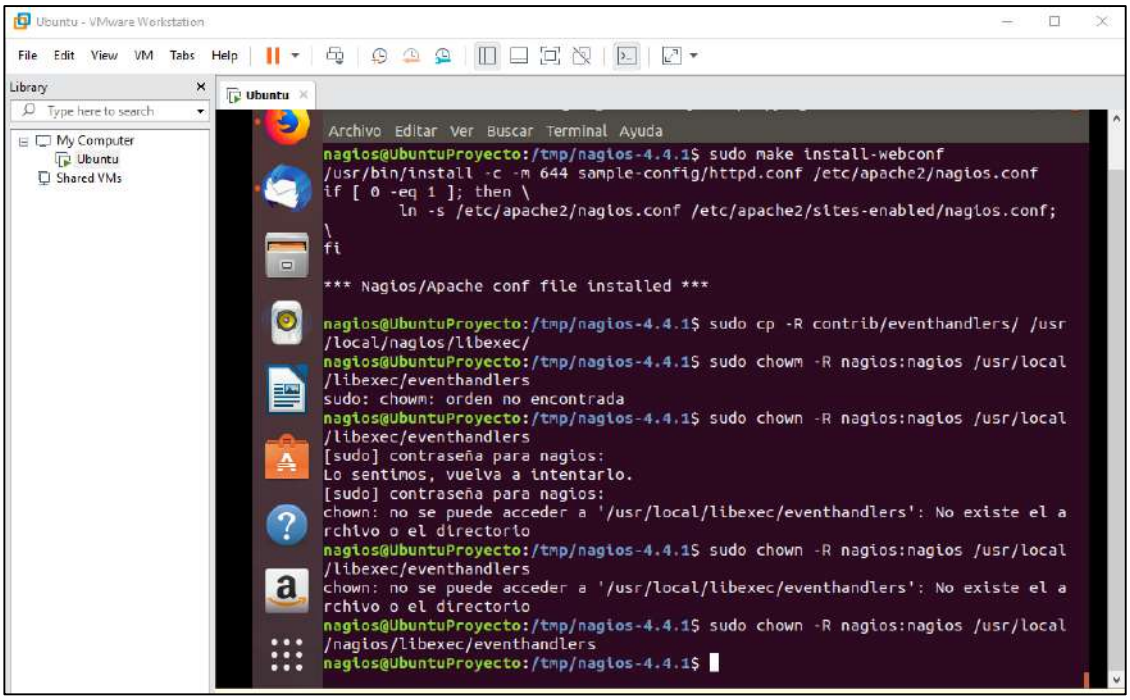


Ilustración 142 Descarga e instalación 8

Ilustración 143 Ficheros de configuración de Nagios

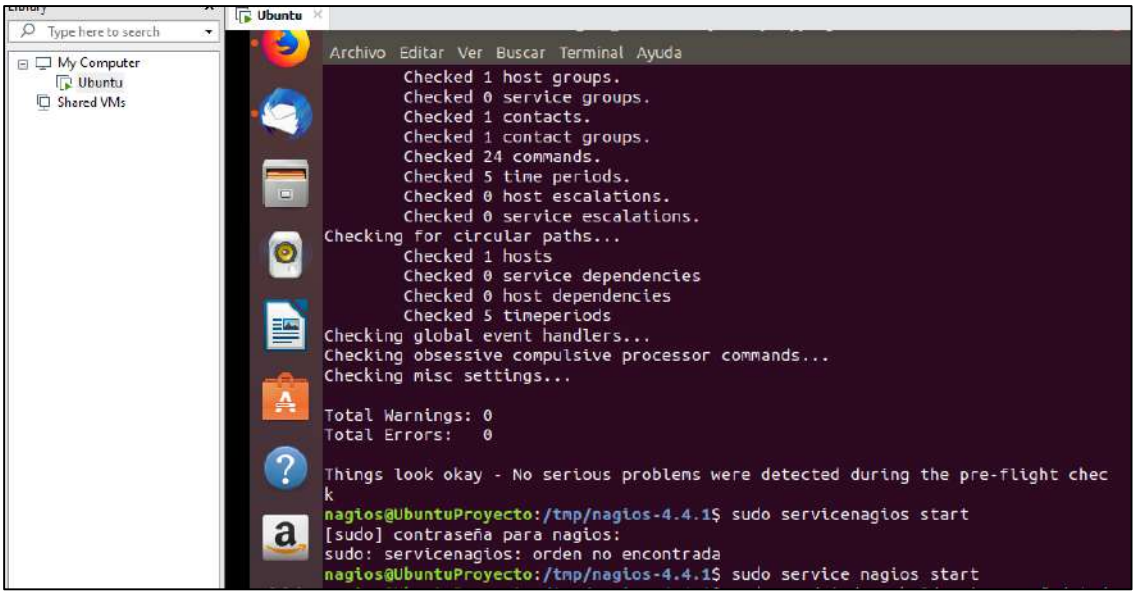


Ilustración 144 Iniciación de servicio Nagios

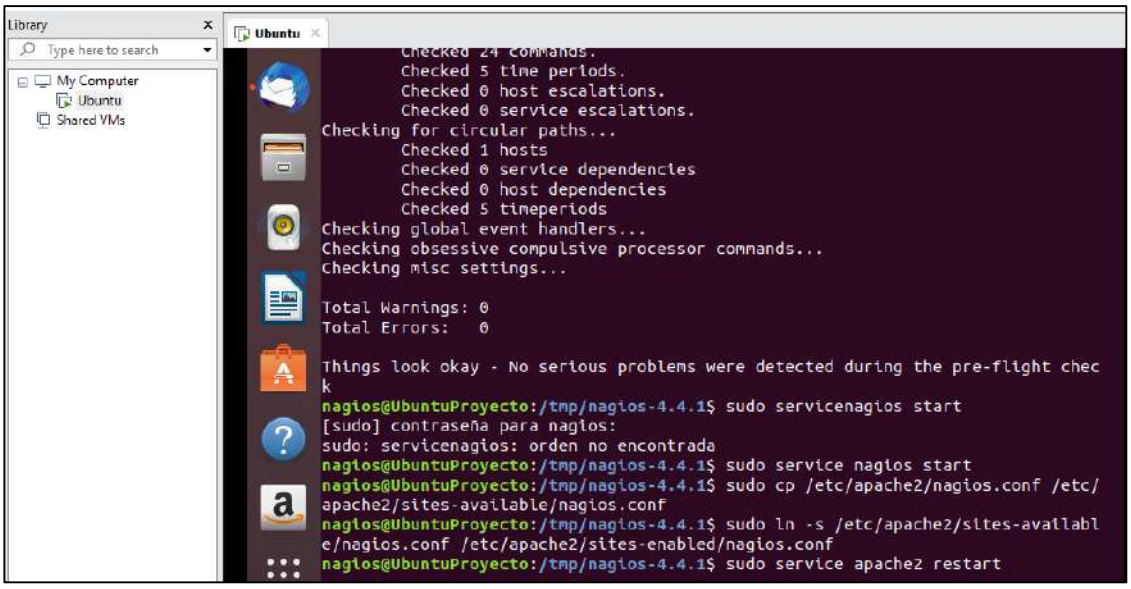


Ilustración 145 Copia de fichero de configuración

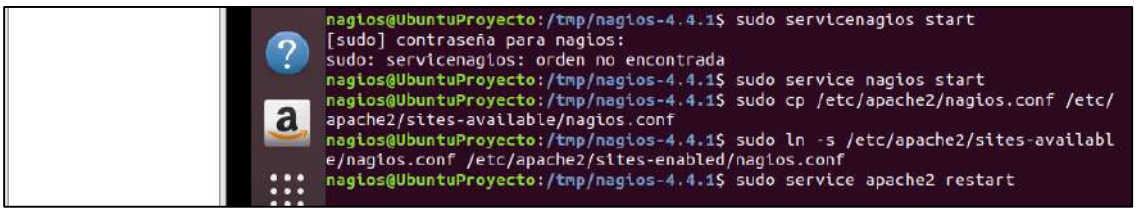


Ilustración 146 Creación de vinculo permanente y reinicio de Apache

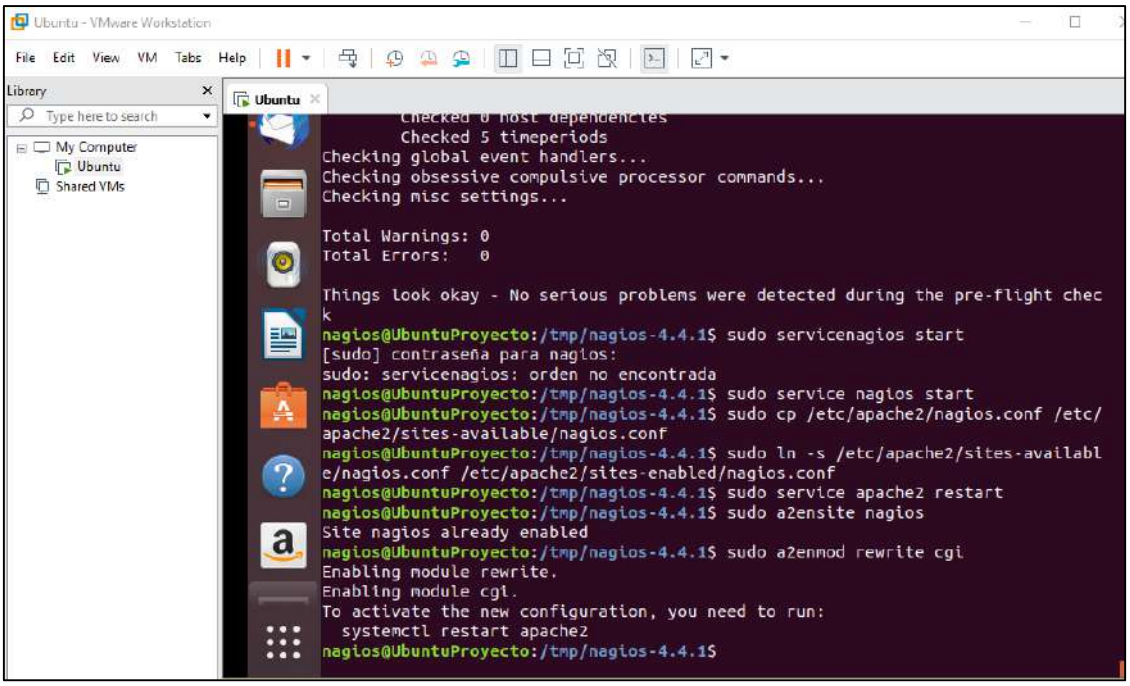


Ilustración 147 Activación del sitio

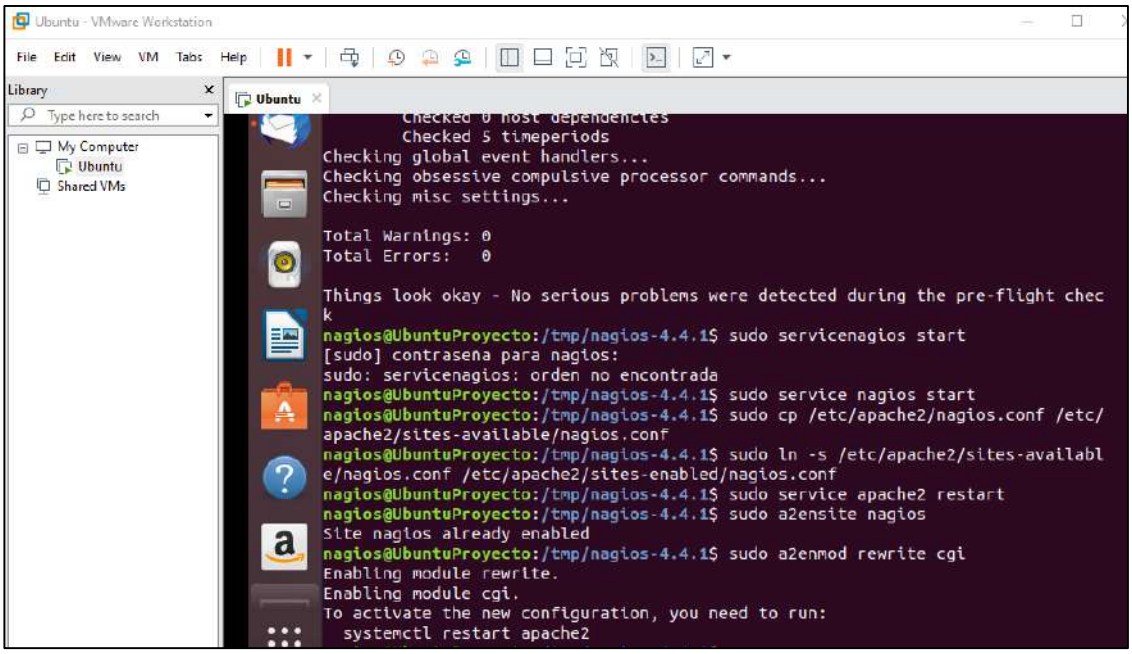


Ilustración 148 Activación del sitio

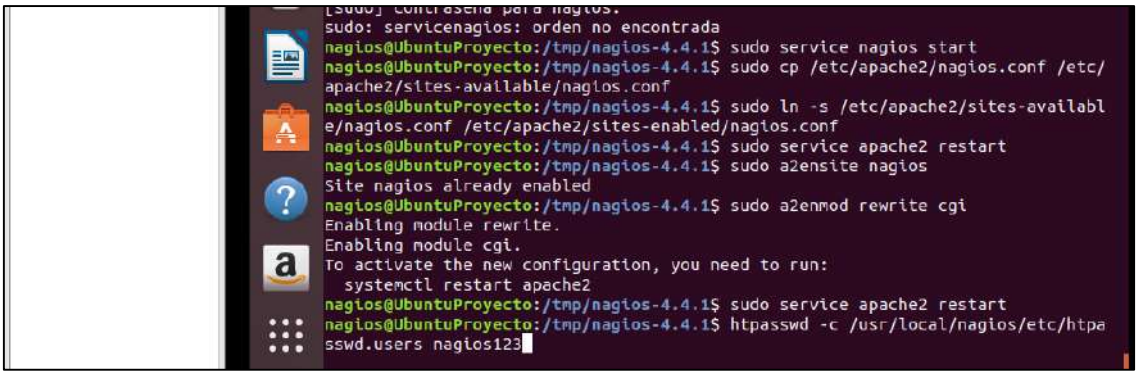


Ilustración 149 Reiniciación de Servidor

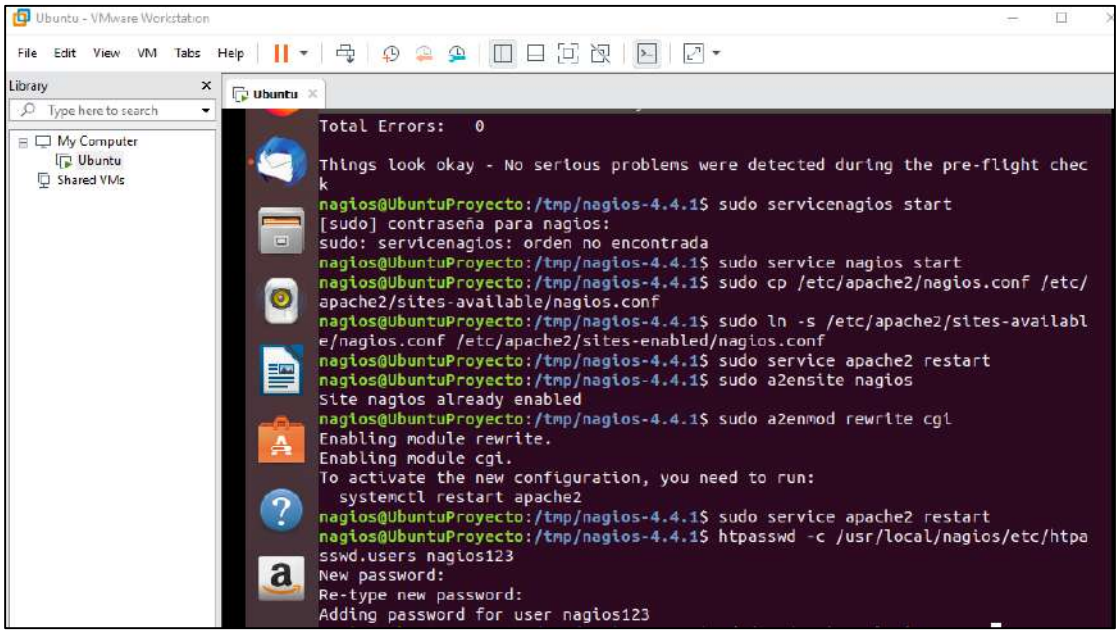


Ilustración 150 Creación de usuario y password

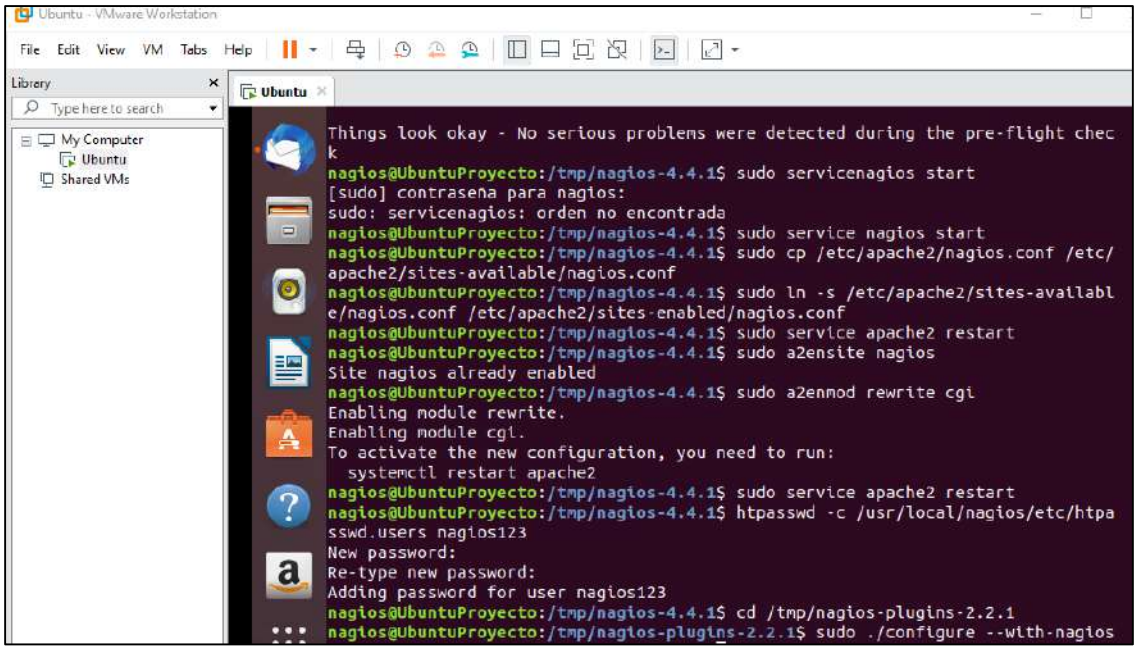


Ilustración 151 Instalación de plugins

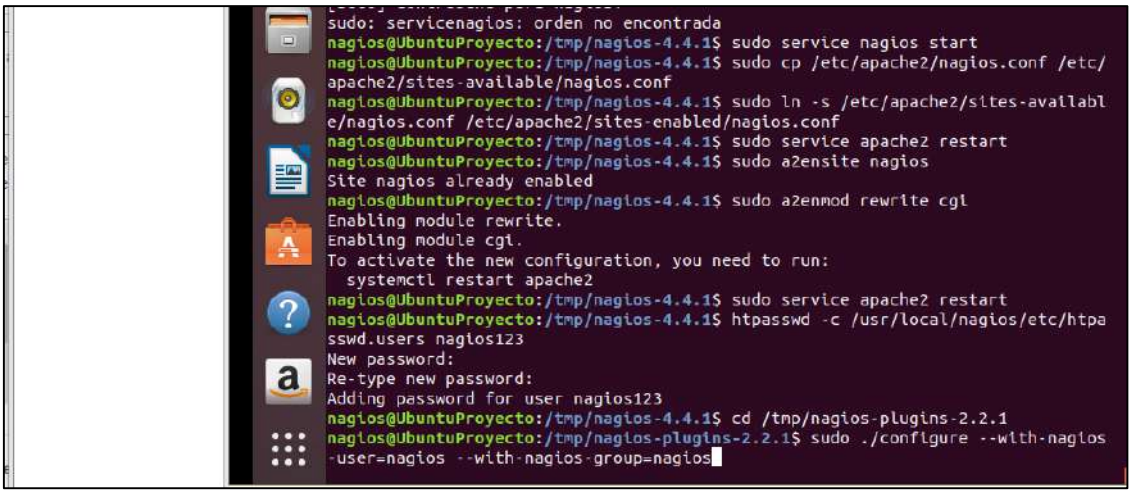


Ilustración 152 Instalación de plugins

Ilustración 153 Ejecución de todos los comandos

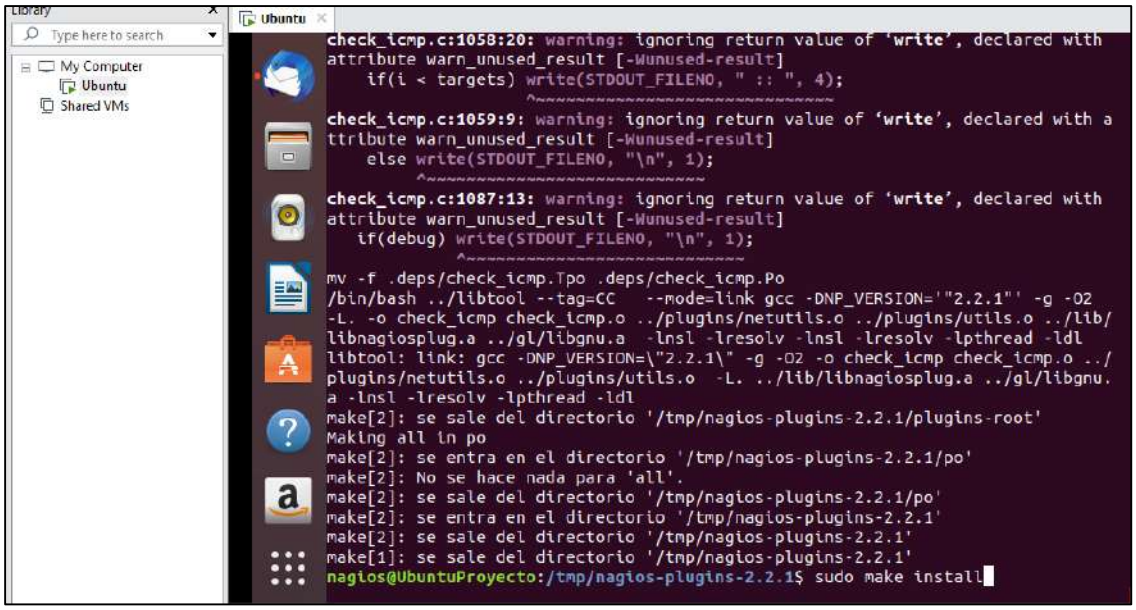


Ilustración 154 Instalación

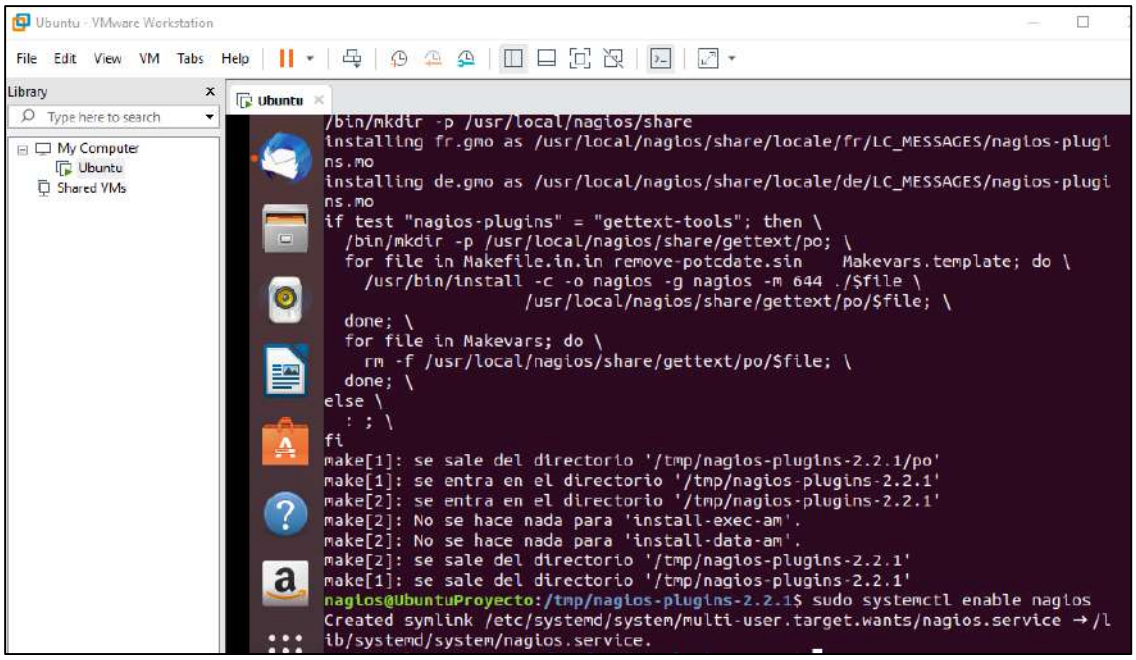


Ilustración 155 Servidor iniciado automáticamente

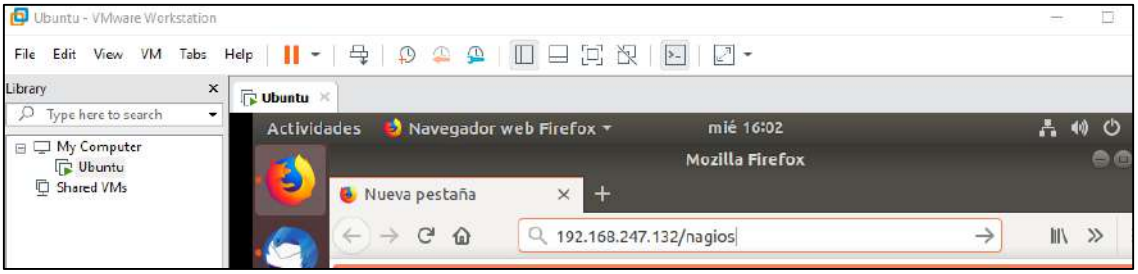


Ilustración 156 Dirección IP para acceder a Nagios Core

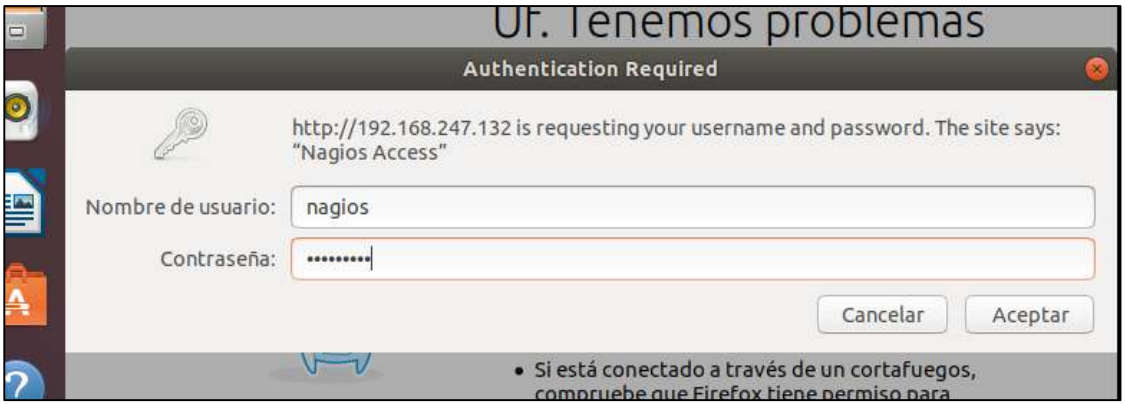


Ilustración 157 Validación de usuario y contraseña

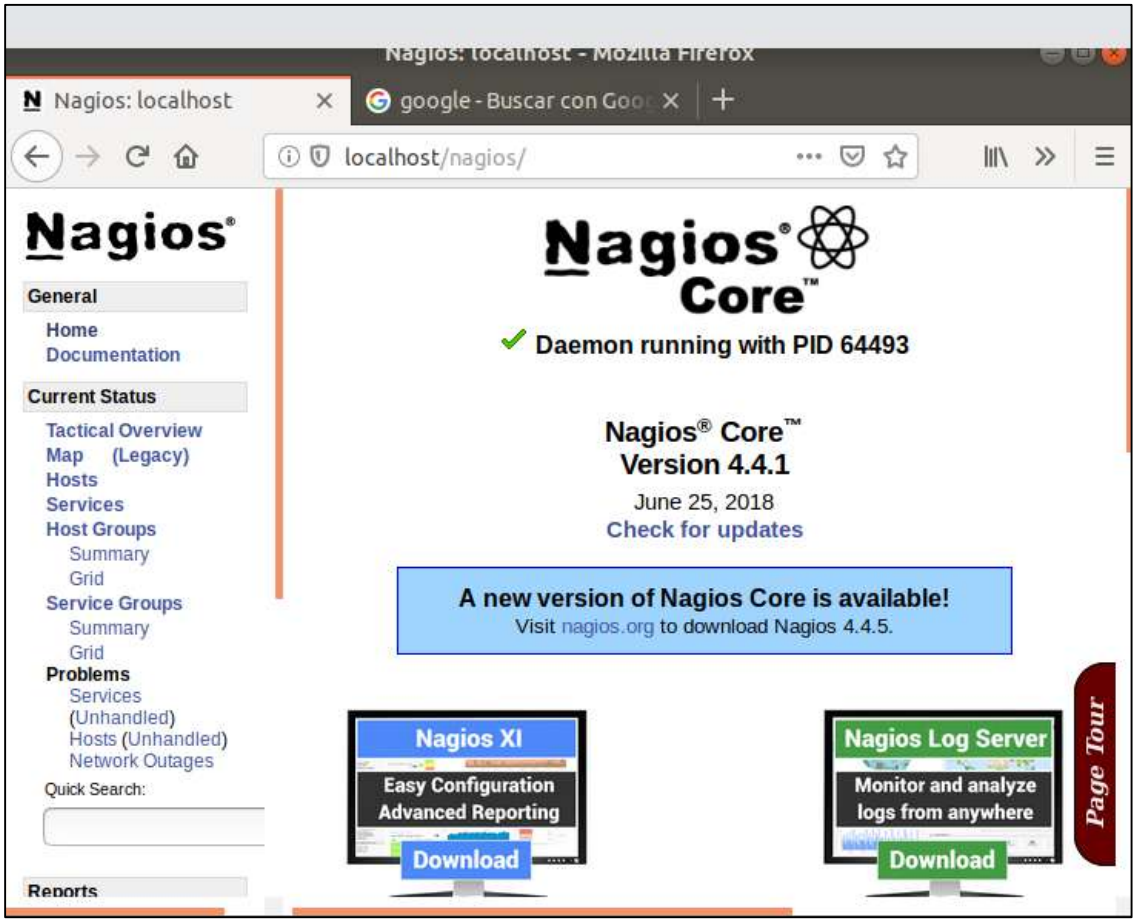


Ilustración 158 Inicialización de Nagios Core

ANEXO 7 - INSTALACIÓN PNP4Nagios

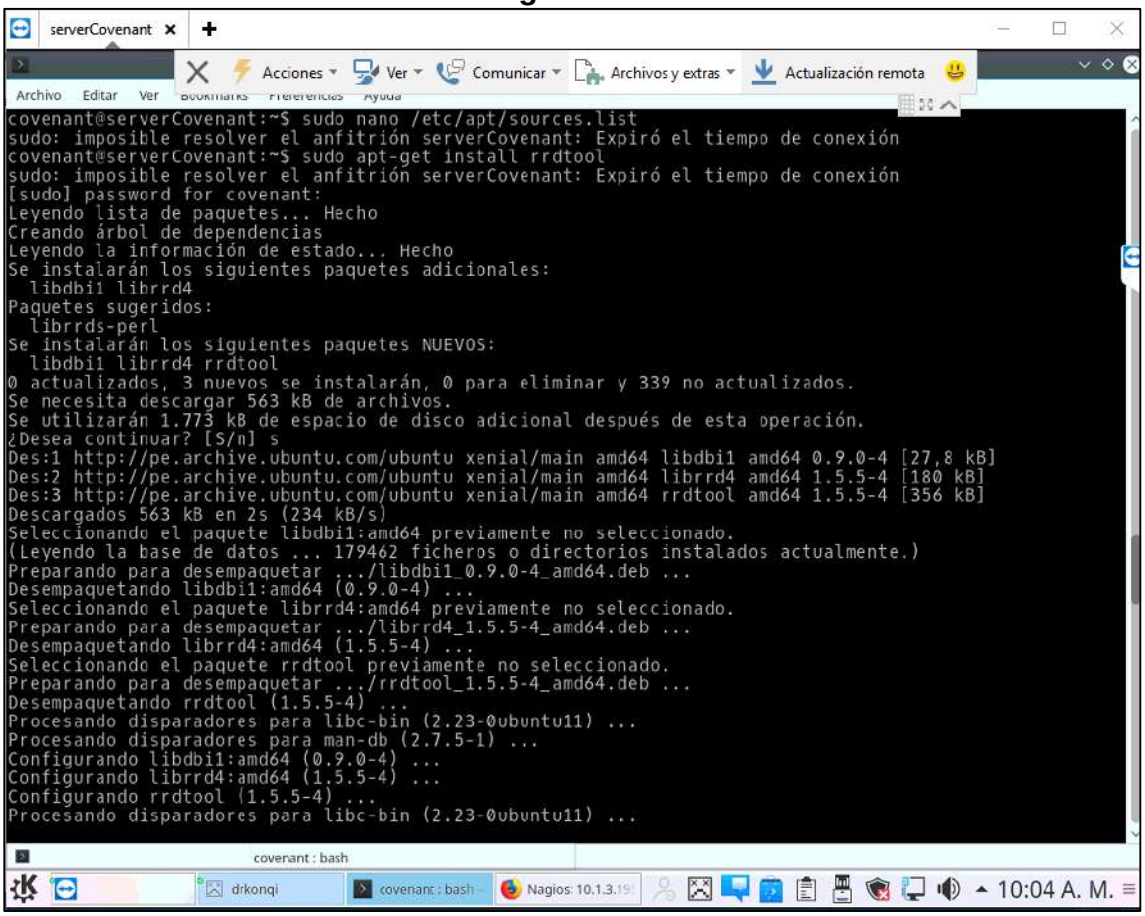


Ilustración 159 Instalación de PNP4Nagios

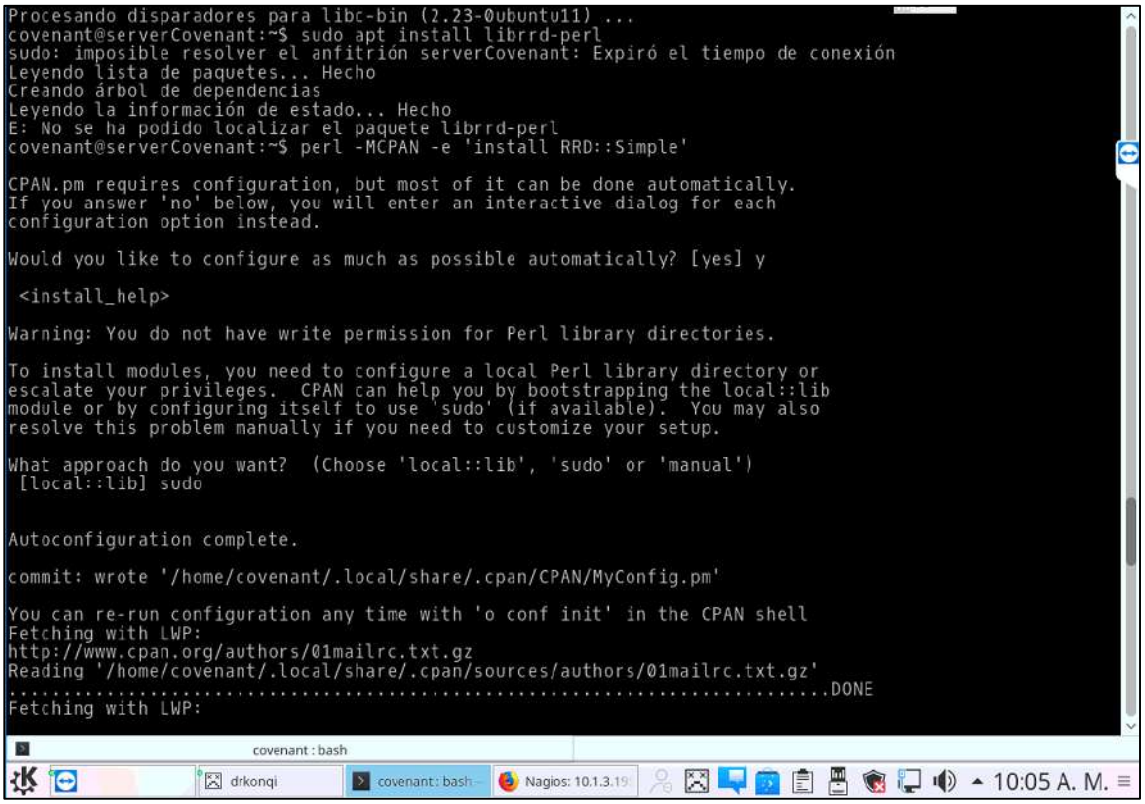


Ilustración 160 Instalación de PNP4Nagios

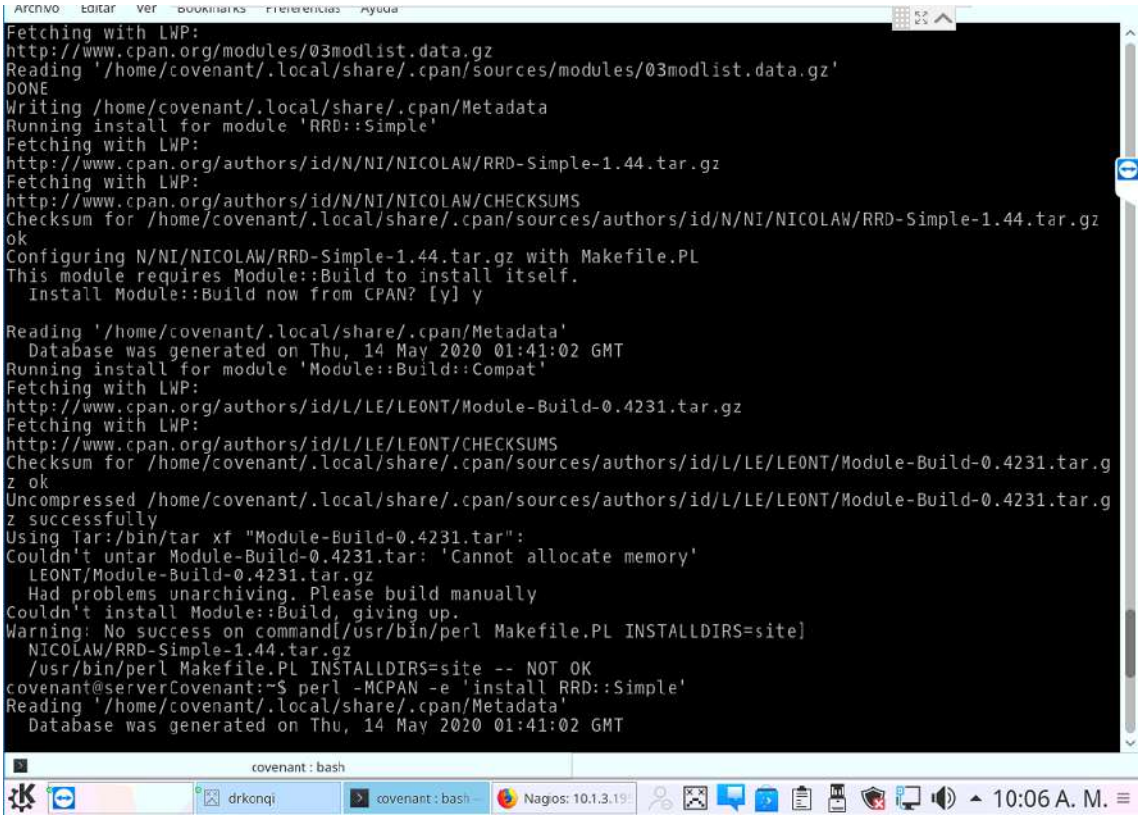


Ilustración 161 Instalación de PNP4Nagios

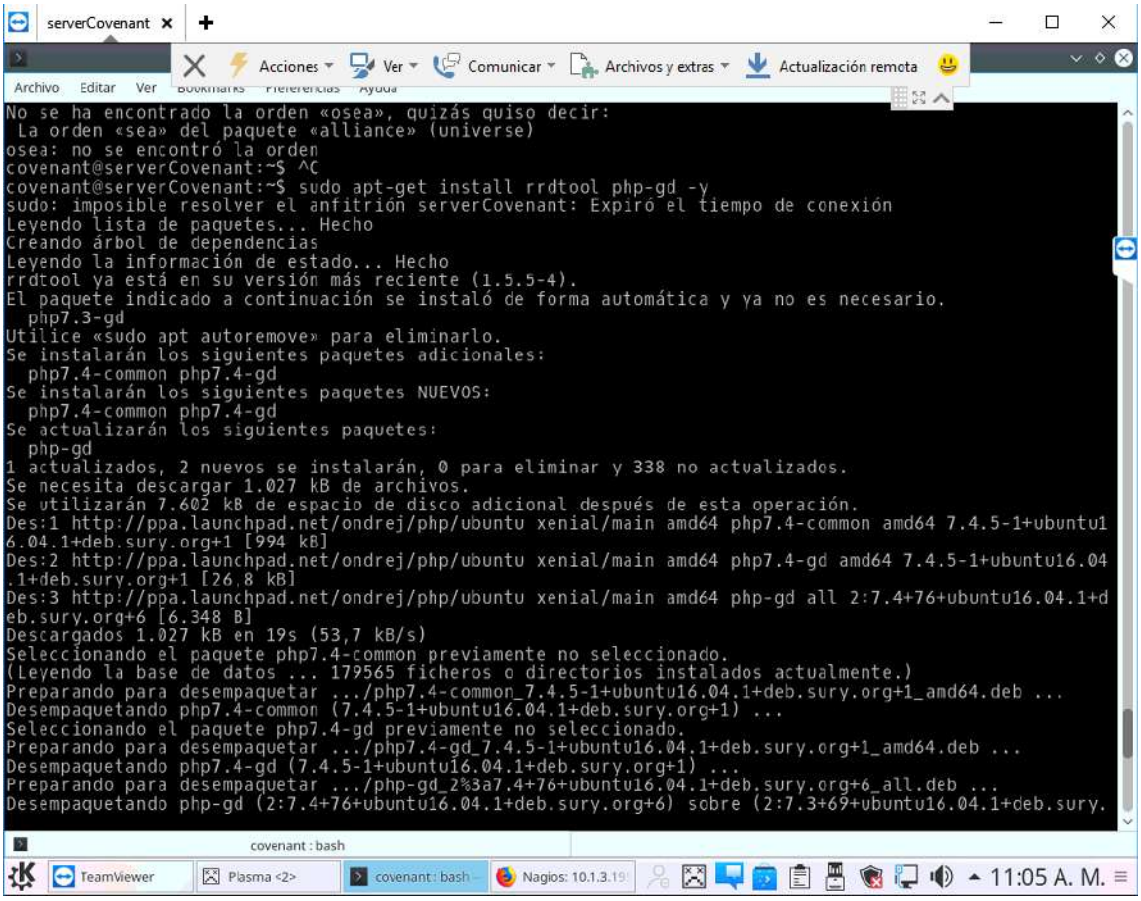


Ilustración 162 Instalación de PNP4Nagios

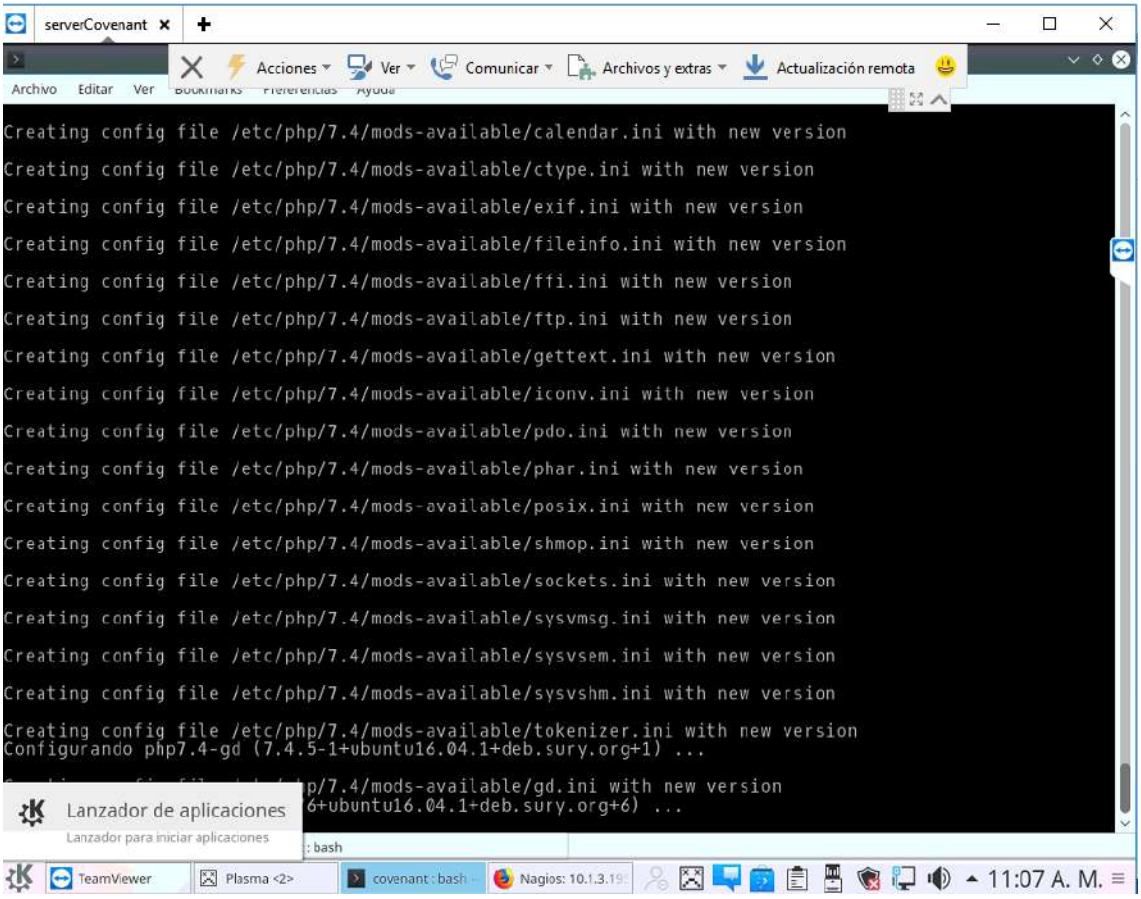


Ilustración 163 Instalación de PNP4Nagios

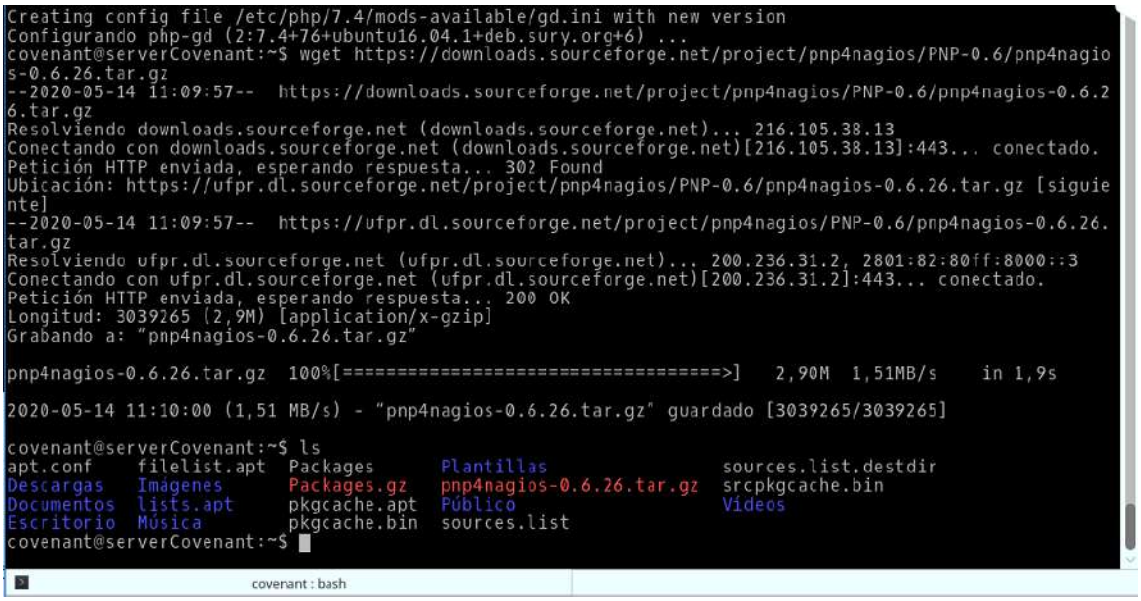


Ilustración 164 Instalación de PNP4Nagios

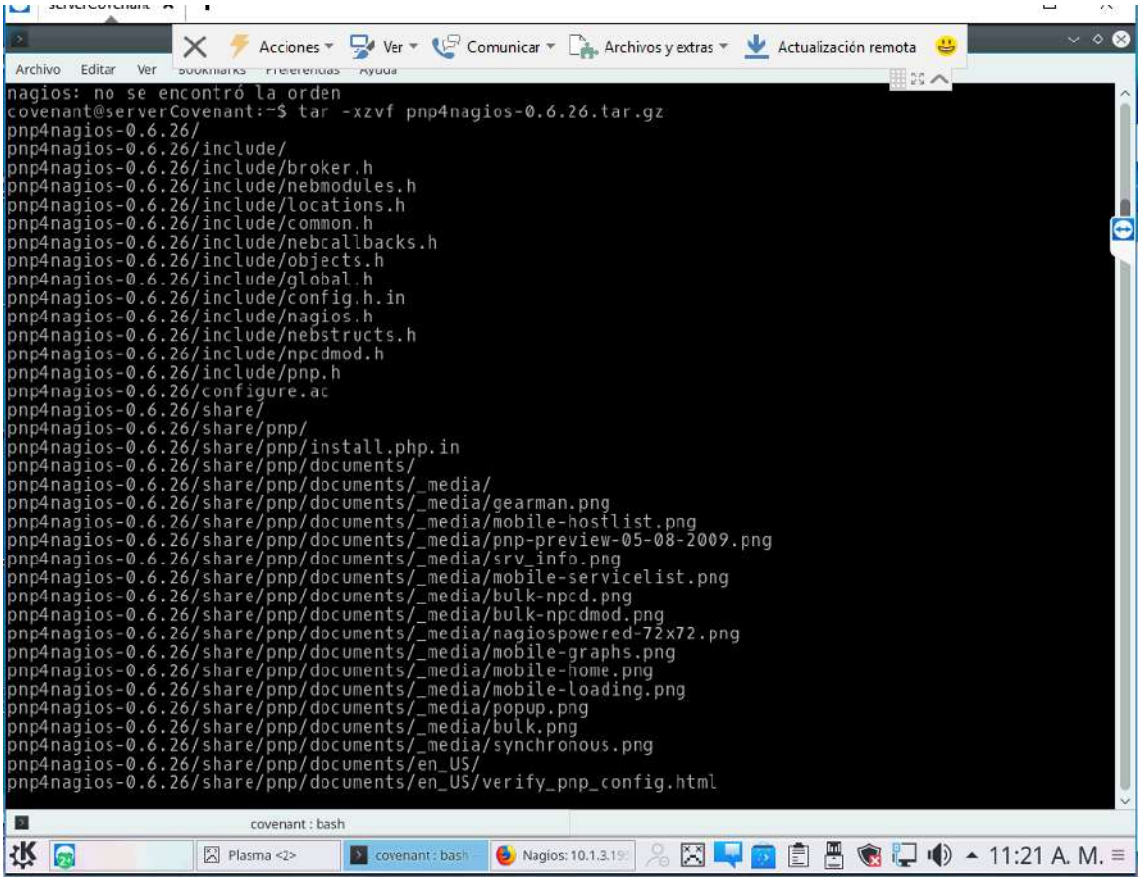


Ilustración 165 Instalación de PNP4Nagios

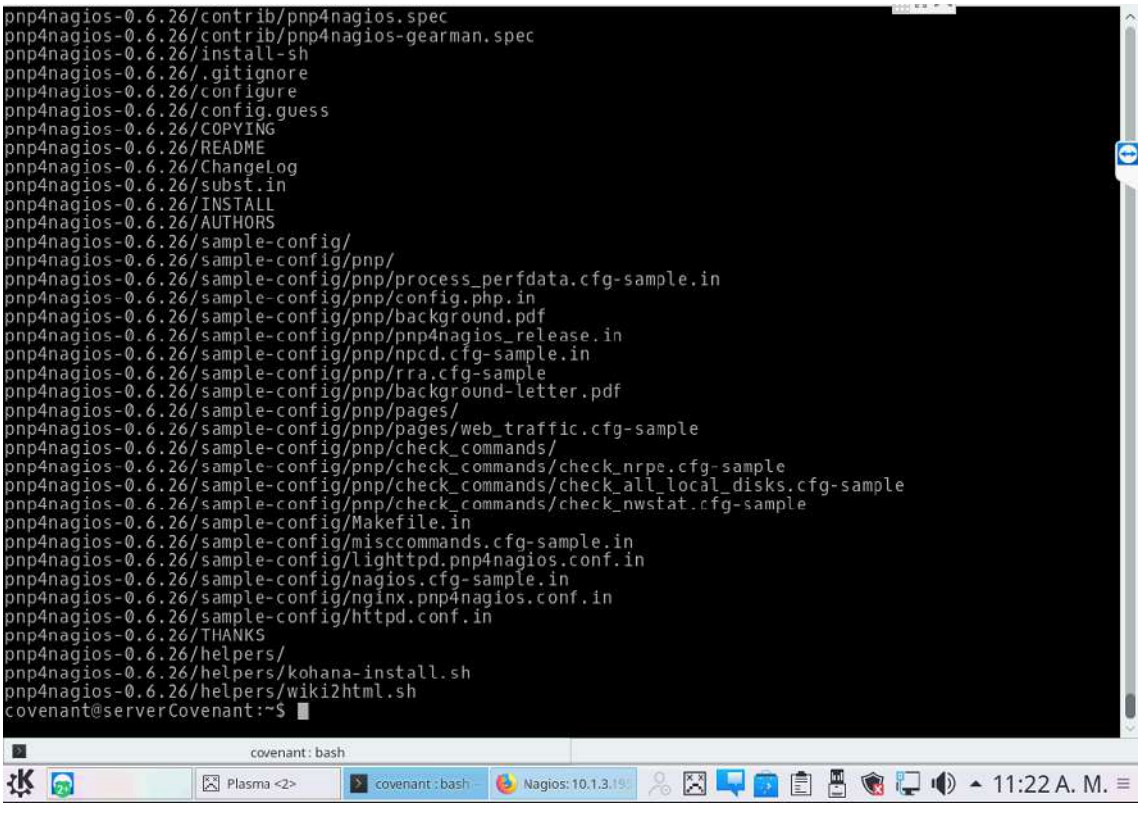


Ilustración 166 Instalación de PNP4Nagios

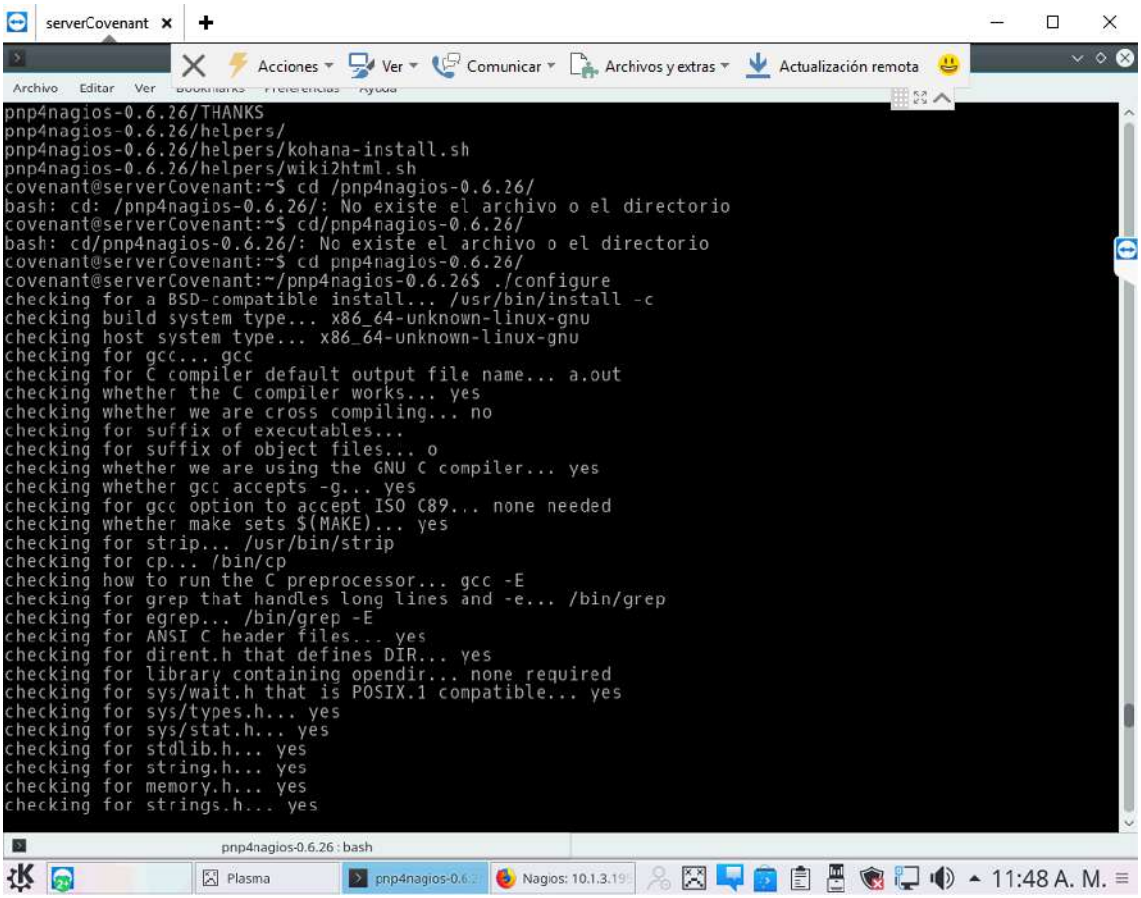


Ilustración 167 Instalación de PNP4Nagios

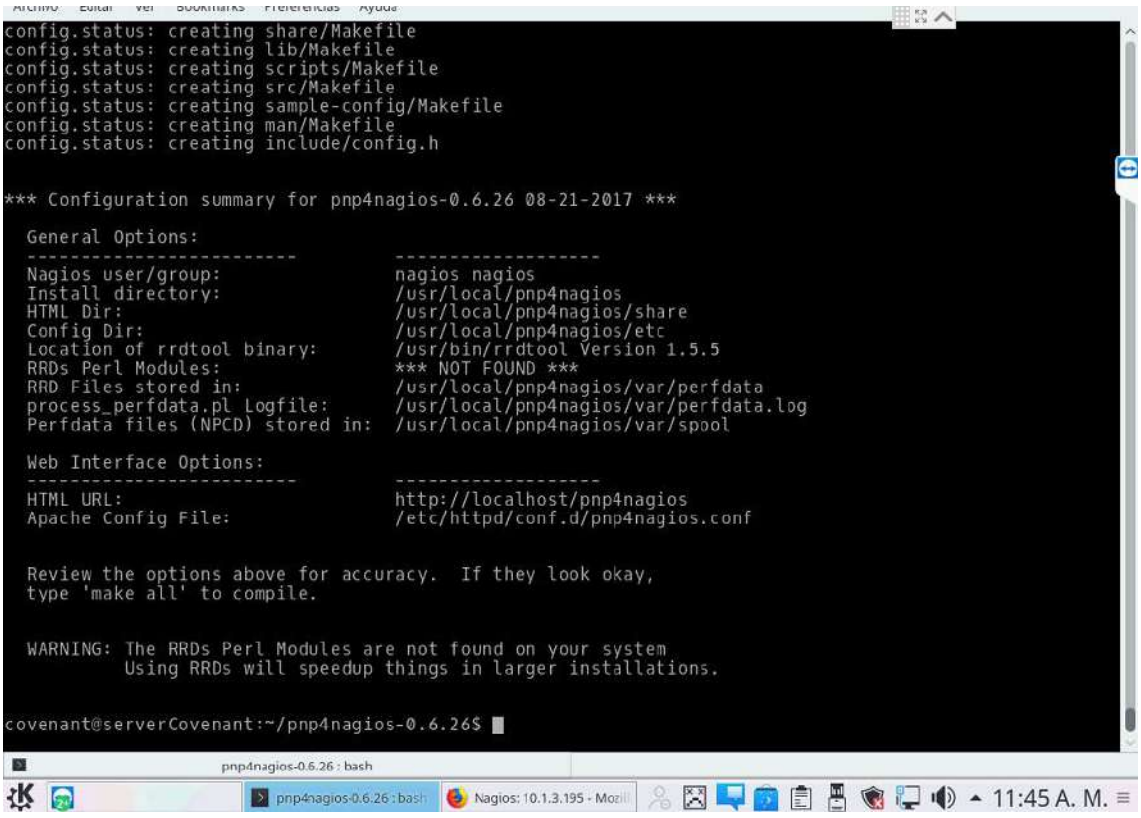


Ilustración 168 Instalación de PNP4Nagios

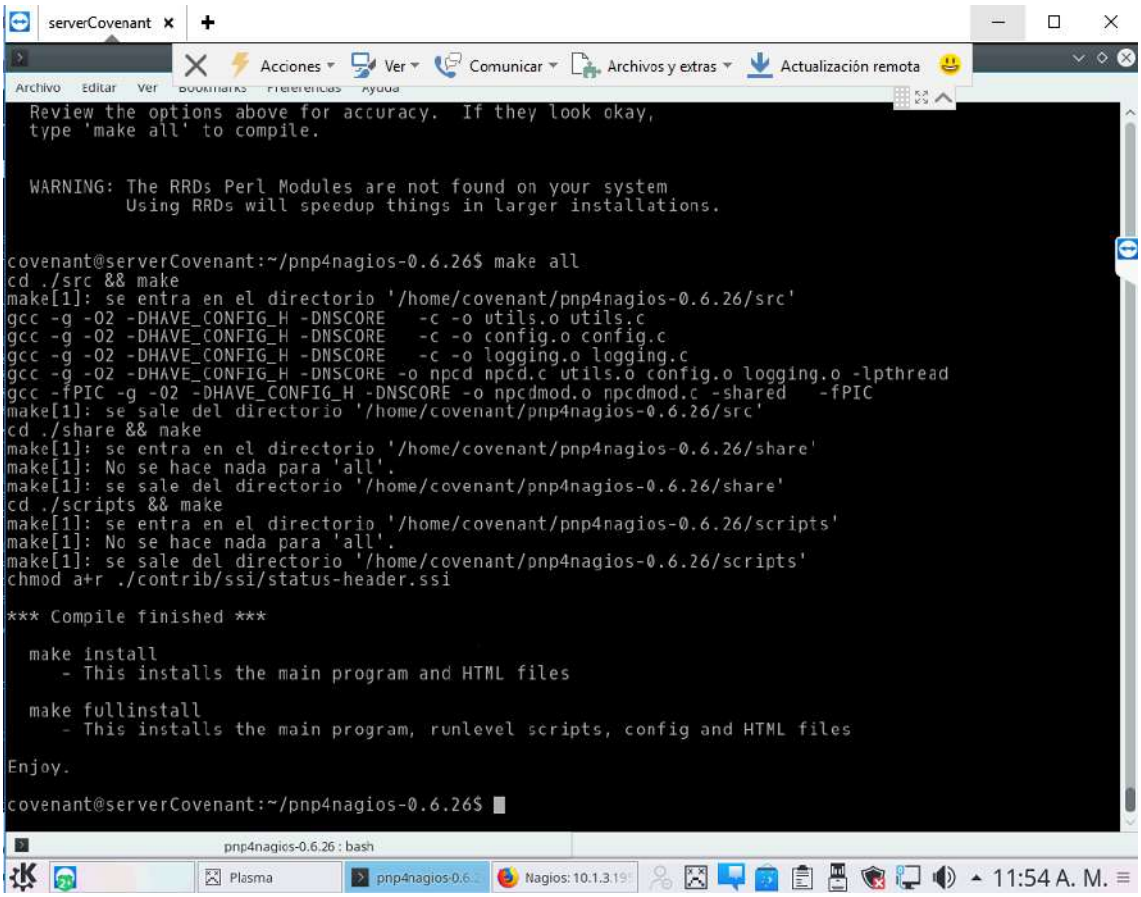


Ilustración 169 Instalación de PNP4Nagios

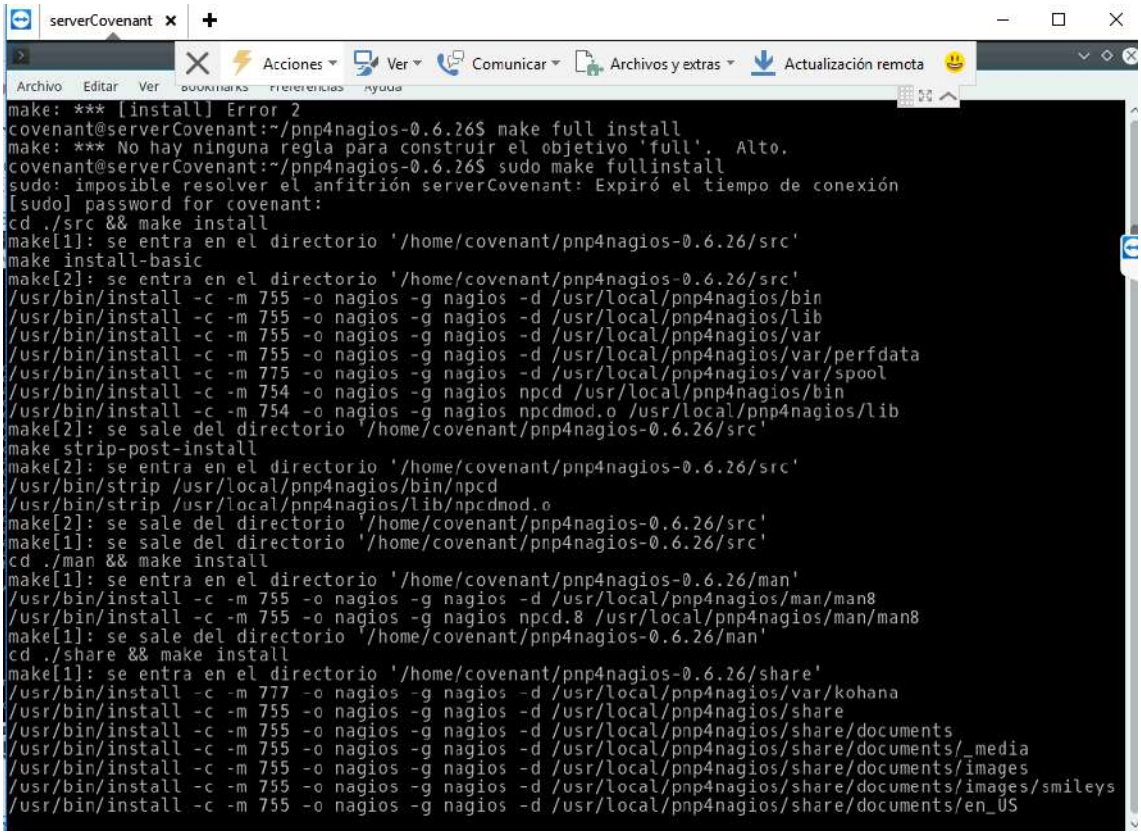


Ilustración 170 Instalación de PNP4Nagios

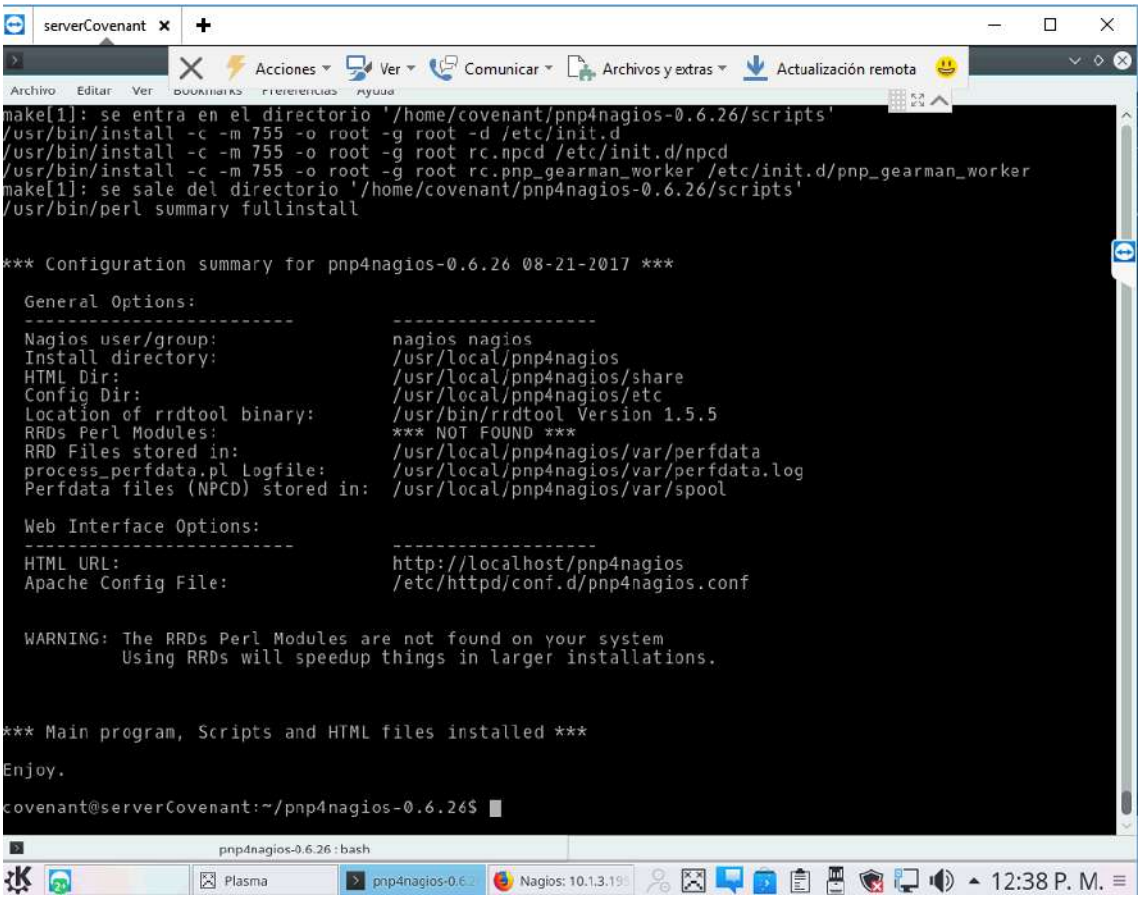


Ilustración 171 Instalación de PNP4Nagios

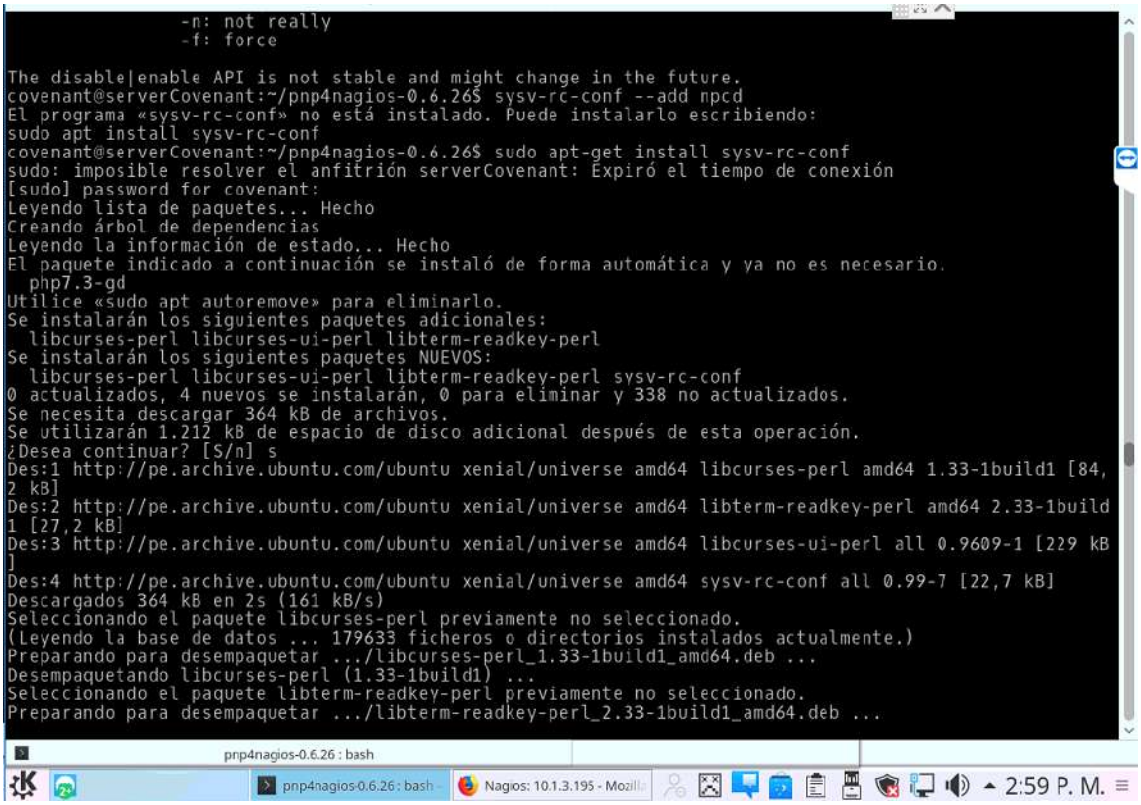


Ilustración 172 Instalación de PNP4Nagios

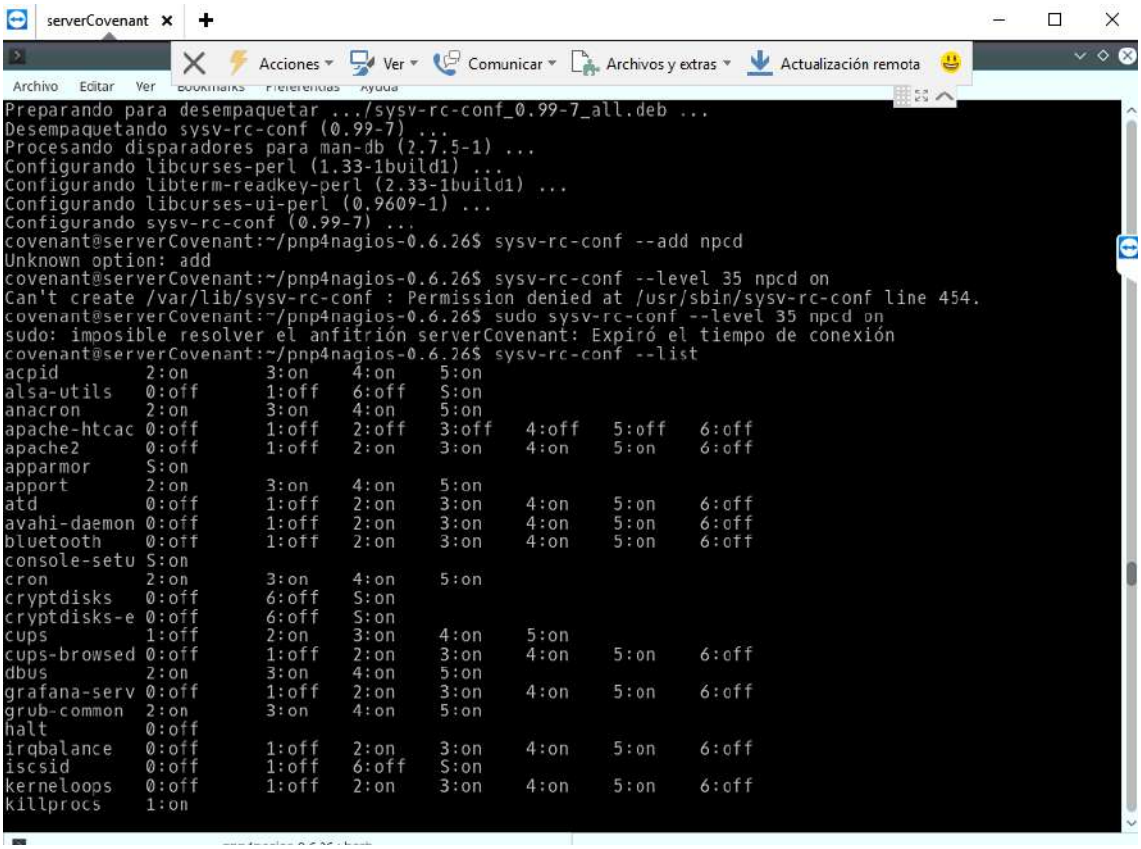


Ilustración 173 Instalación de PNP4Nagios

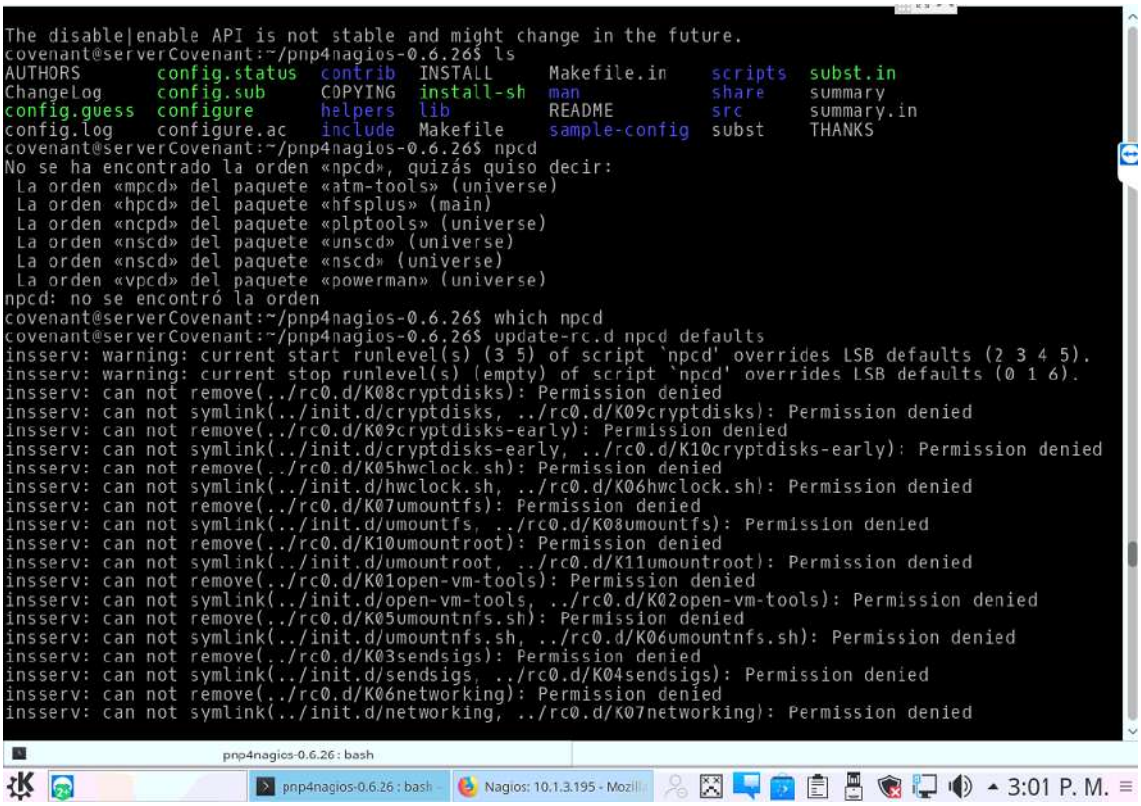


Ilustración 174 Instalación de PNP4Nagios

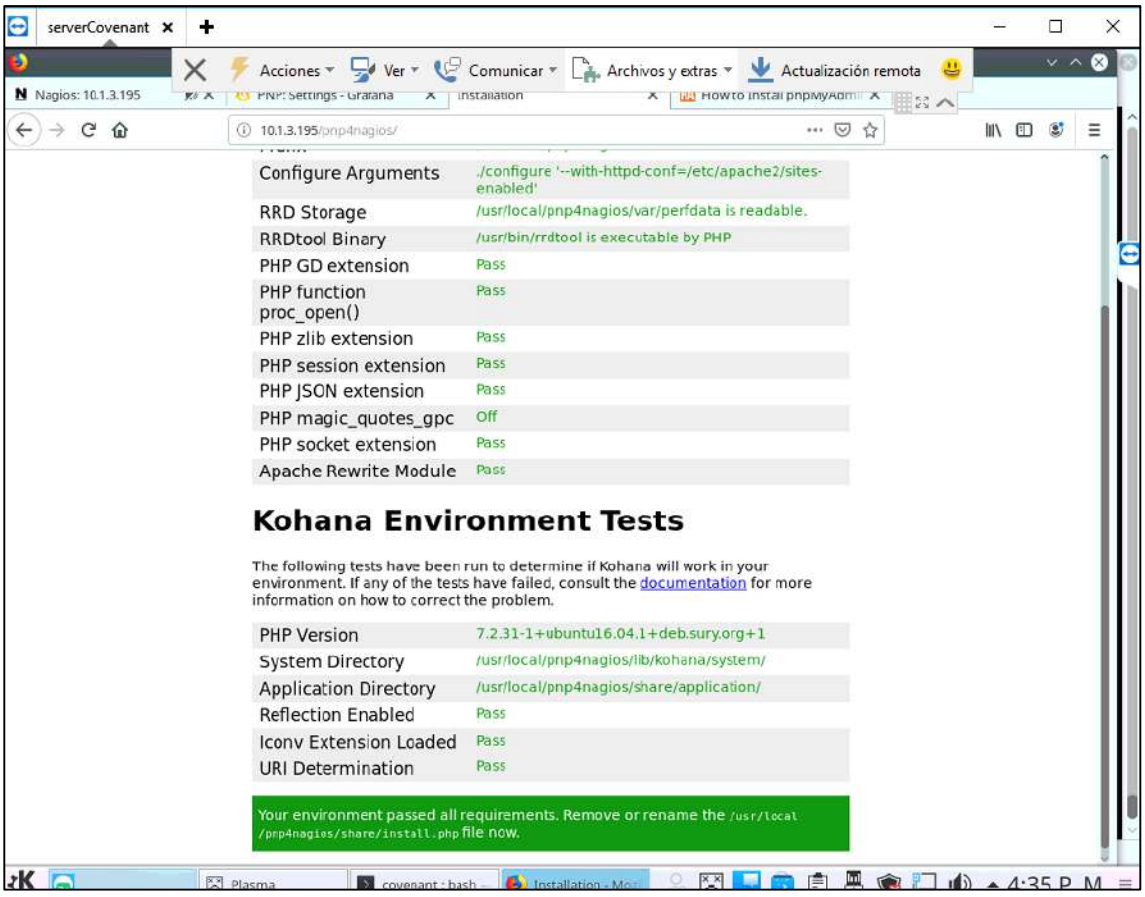


Ilustración 175 Instalación de PNP4Nagios

```
covenant@serverCovenant:~$ mv /usr/local/pnp4nagios/share/install.php /usr/local/pnp4nagios/share/inst
all.php.BKR
mv: no se puede mover '/usr/local/pnp4nagios/share/install.php' a '/usr/local/pnp4nagios/share/install
.php.BKR': Permiso denegado
covenant@serverCovenant:~$ sudo mv /usr/local/pnp4nagios/share/install.php /usr/local/pnp4nagios/share
/install.php.BKR
sudo: imposible resolver el anfitrión serverCovenant: Expiró el tiempo de conexión
covenant@serverCovenant:~$ mv /usr/local/pnp4nagios/share/install.php /usr/local/pnp4nagios/share/inst
all.php.BKP
mv: no se puede efectuar `stat' sobre '/usr/local/pnp4nagios/share/install.php': No existe el archivo
o el directorio
covenant@serverCovenant:~$ sudo mv /usr/local/pnp4nagios/share/install.php /usr/local/pnp4nagios/share
/install.php.BKP
sudo: imposible resolver el anfitrión serverCovenant: Expiró el tiempo de conexión
mv: no se puede efectuar `stat' sobre '/usr/local/pnp4nagios/share/install.php': No existe el archivo
o el directorio
covenant@serverCovenant:~$
```

Ilustración 176 Instalación de PNP4Nagios

```
covenant@serverCovenant:/usr/local/nagios/etc$ sudo nano nagios.cfg
sudo: imposible resolver el anfitrión serverCovenant: Expiró el tiempo de conexión
[sudo] password for covenant:
covenant@serverCovenant:/usr/local/nagios/etc$ sudo nano nagios.cfg
sudo: imposible resolver el anfitrión serverCovenant: Expiró el tiempo de conexión
covenant@serverCovenant:/usr/local/nagios/etc$ cd objects/
covenant@serverCovenant:/usr/local/nagios/etc/objects$
```

Ilustración 177 Instalación de PNP4Nagios

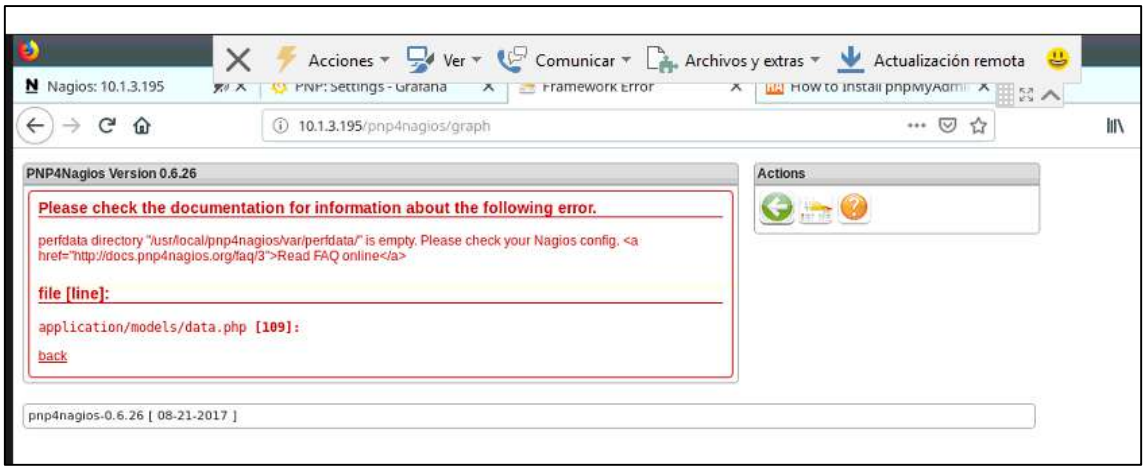


Ilustración 178 Instalación de PNP4Nagios

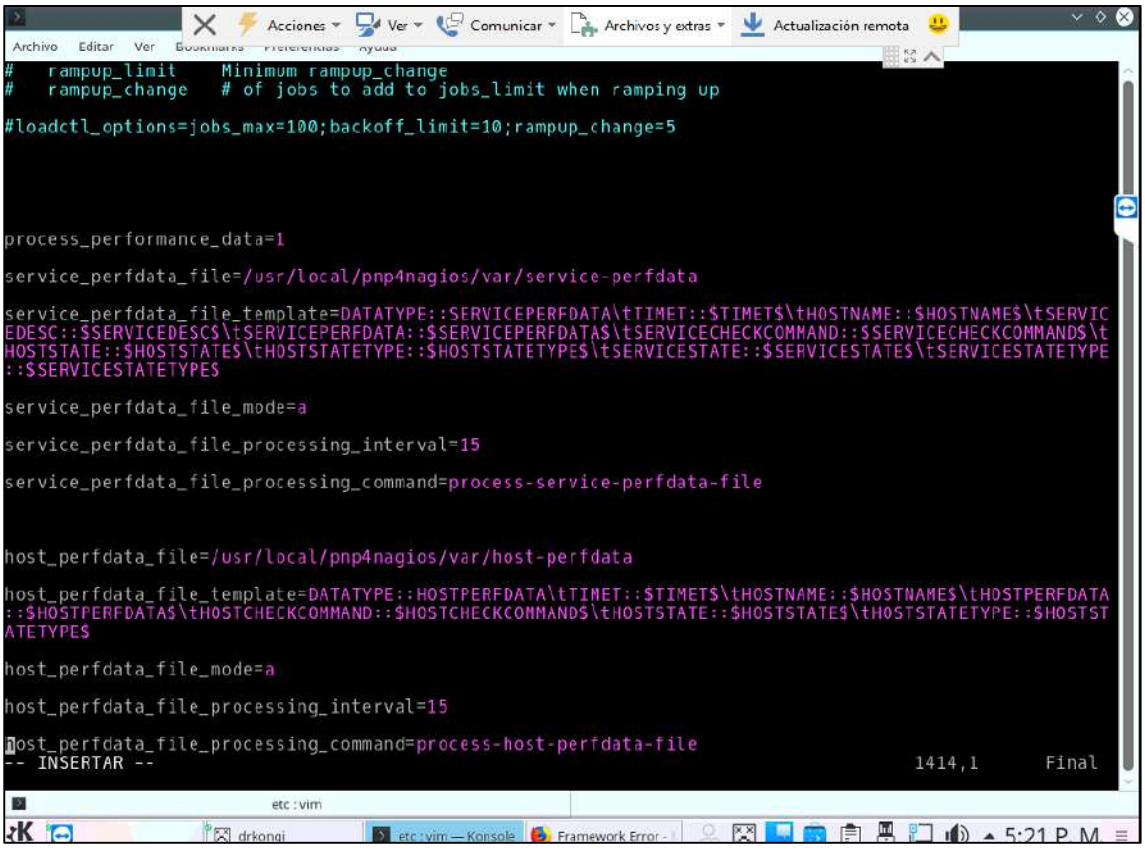


Ilustración 179 Instalación de PNP4Nagios

Ilustración 180 Instalación de PNP4Nagios

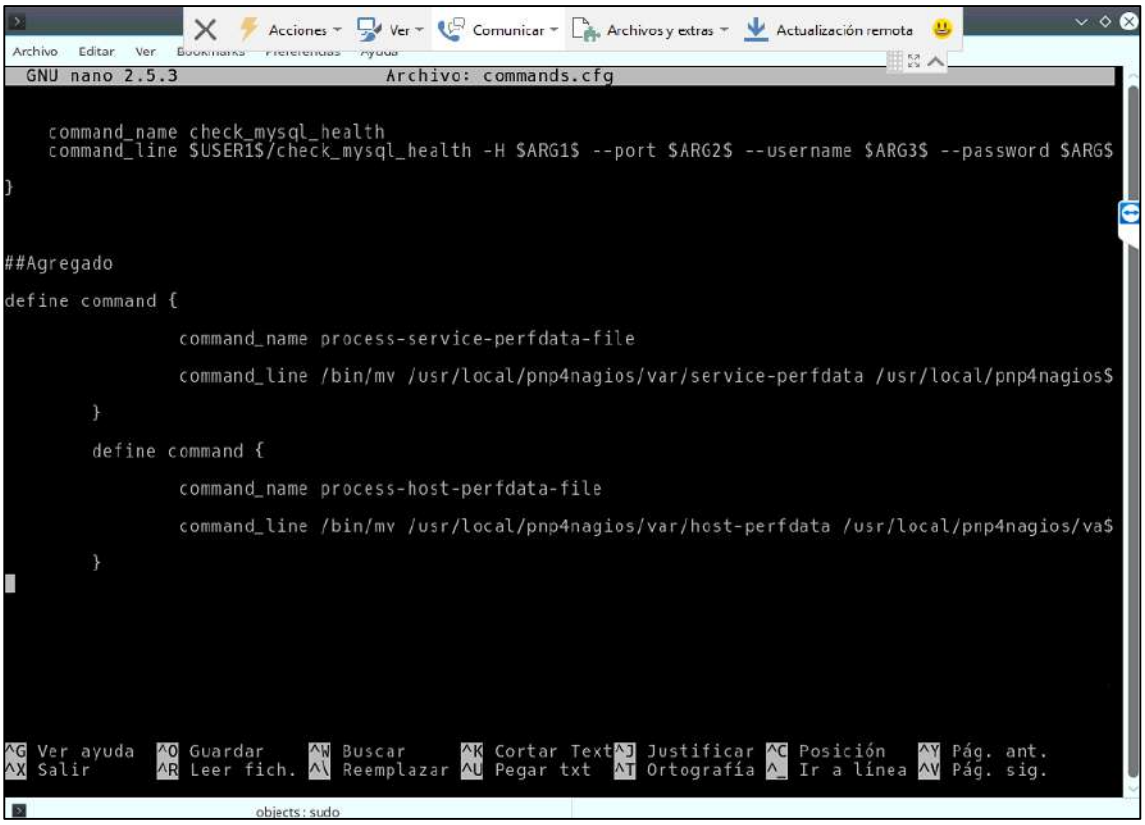


Ilustración 181 Instalación de PNP4Nagios

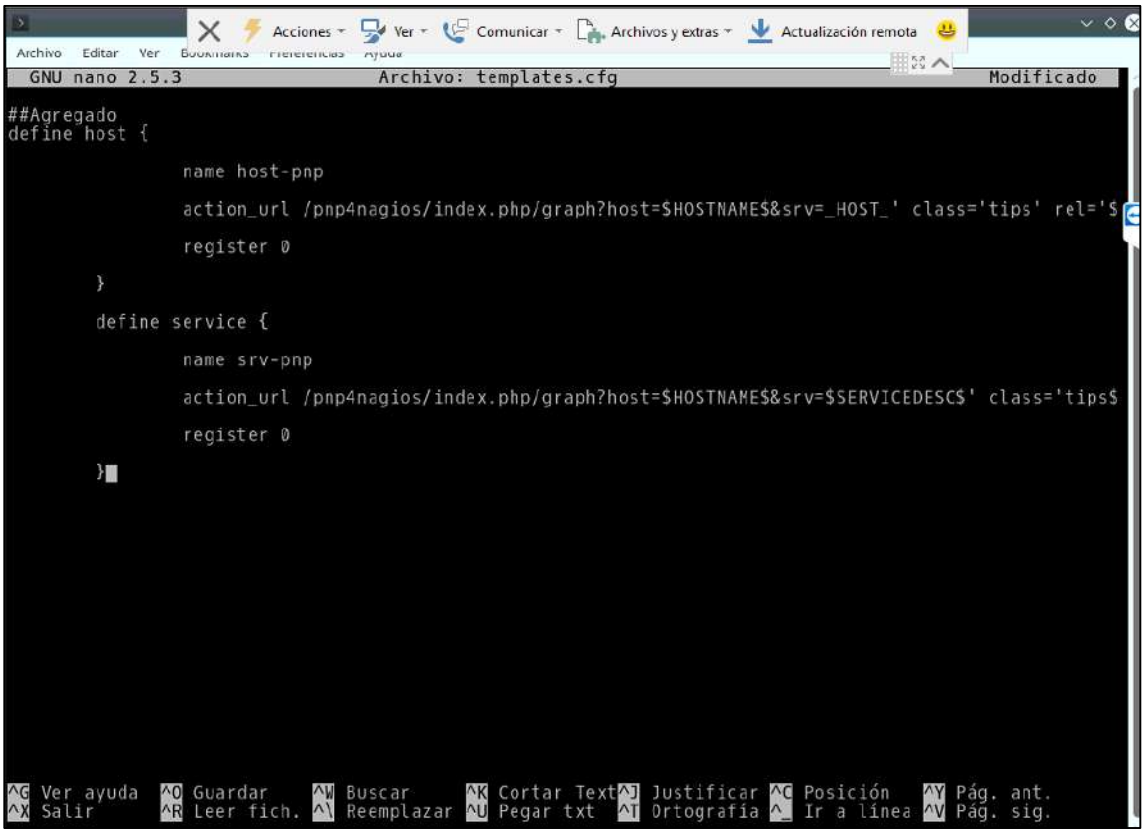


Ilustración 182 Instalación de PNP4Nagios

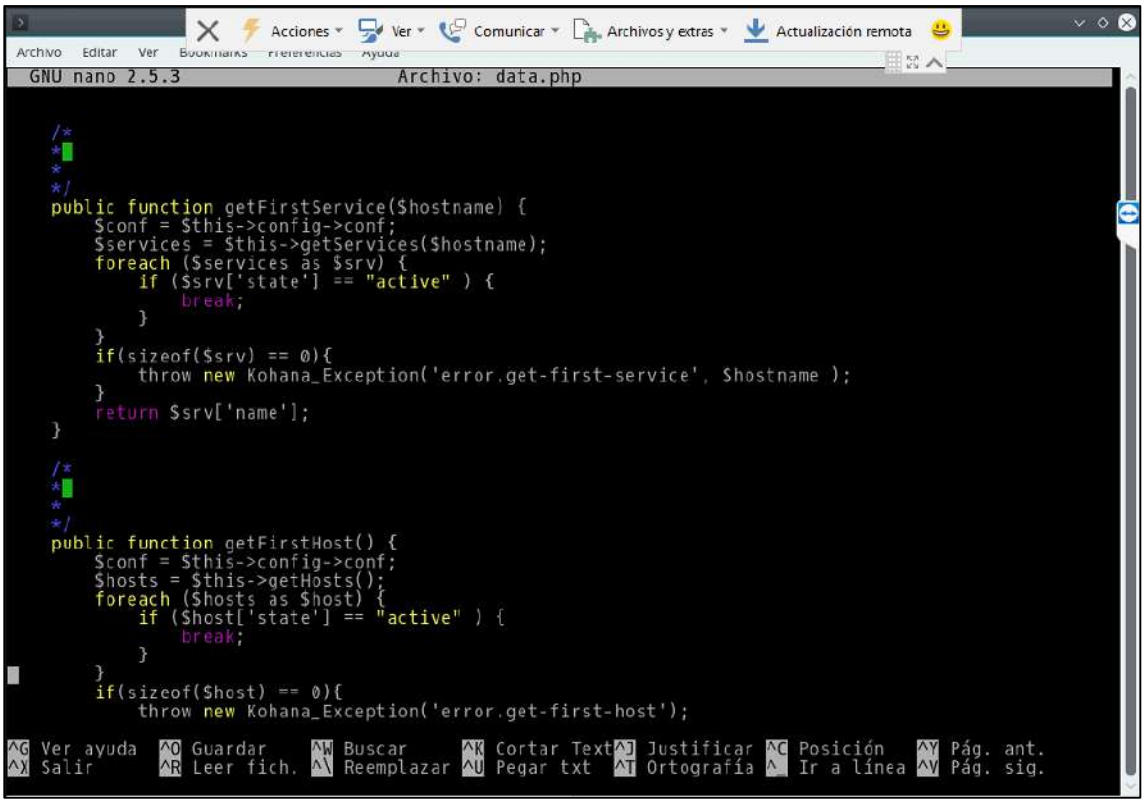


Ilustración 183 Instalación de PNP4Nagios

ANEXO 8 - INSTALACIÓN GRAFANA

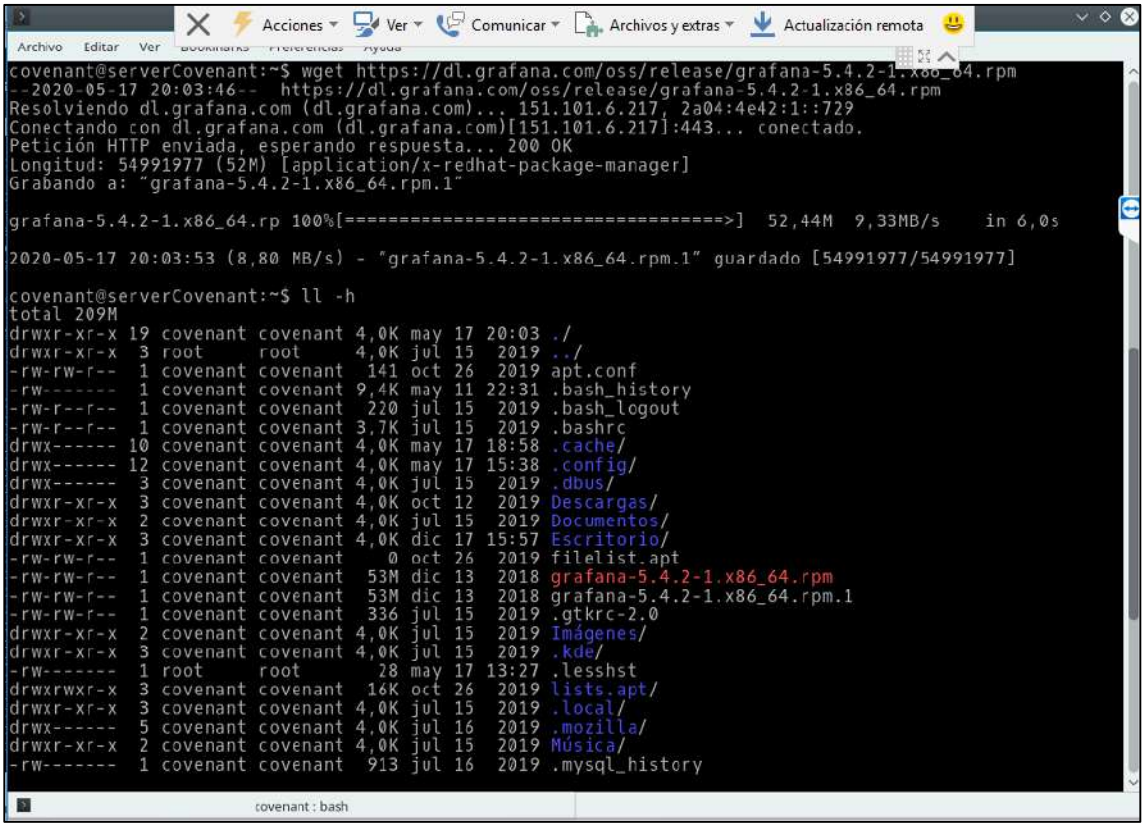


Ilustración 184 Instalación de Grafana

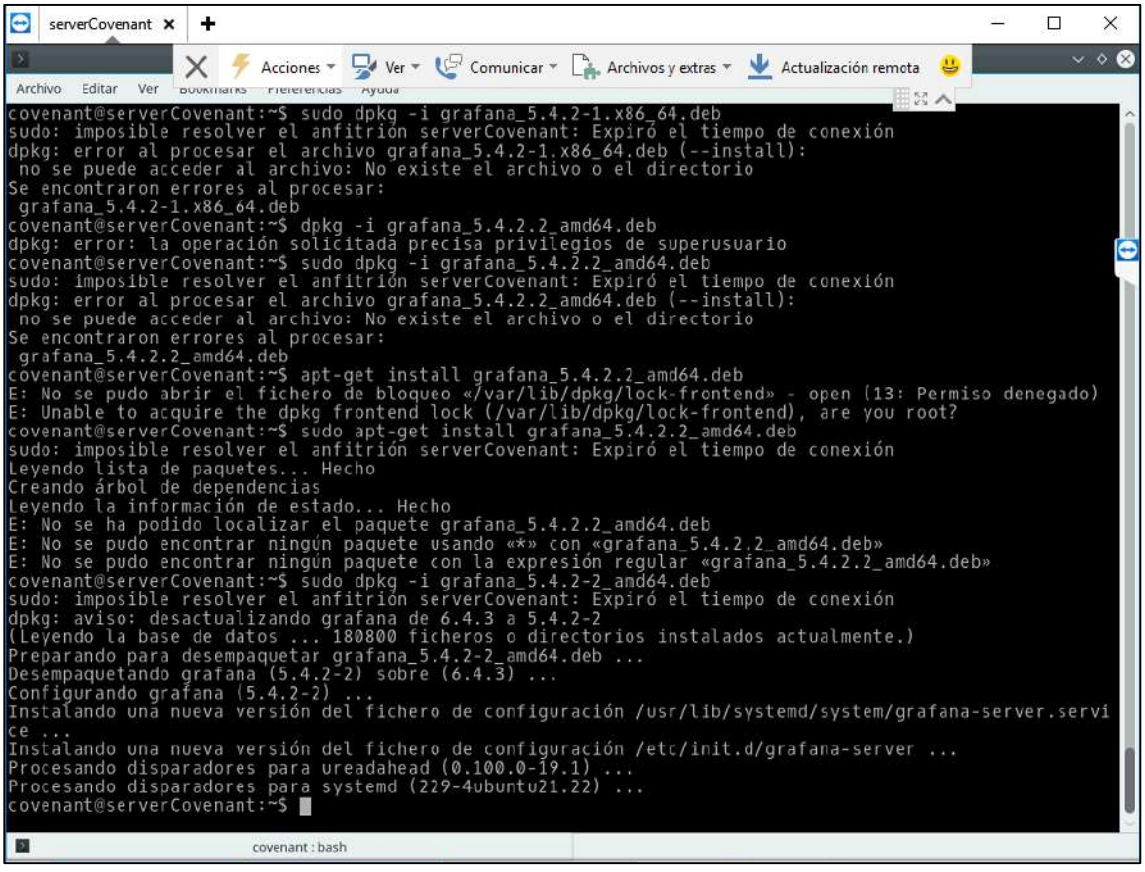


Ilustración 185 Instalación de Grafana

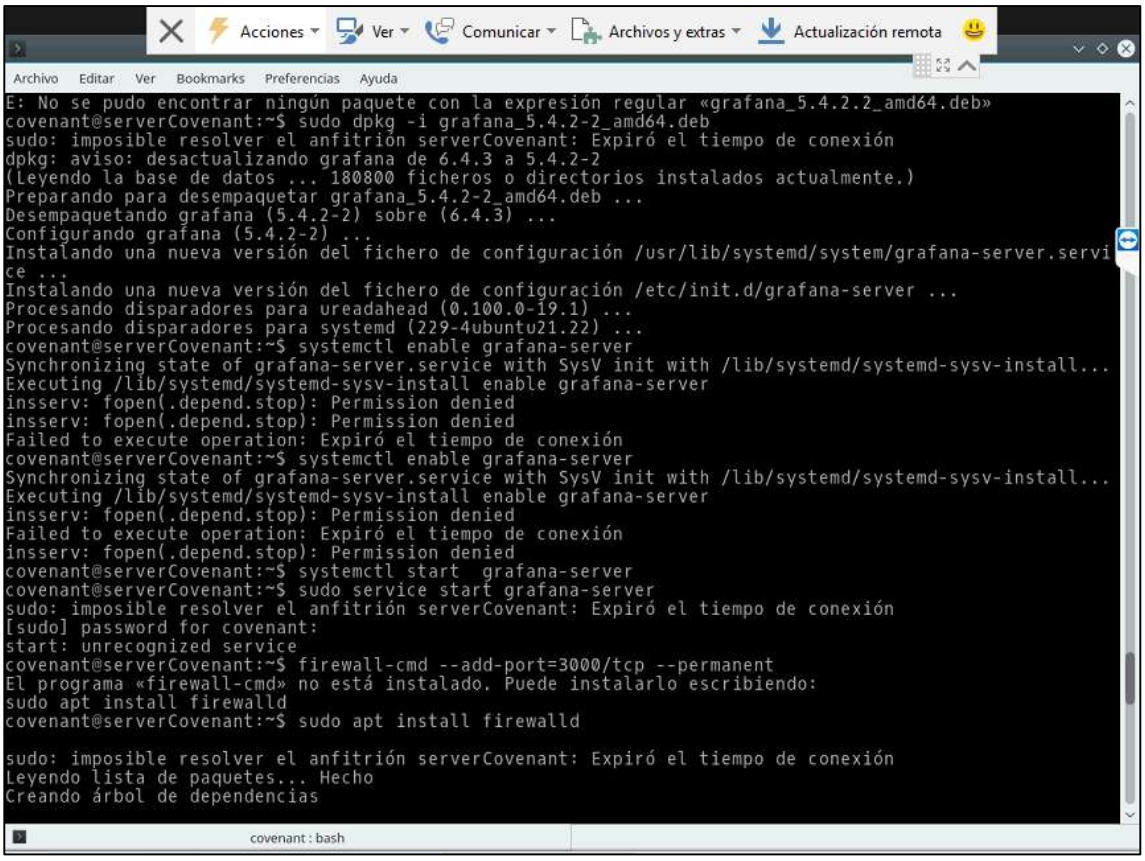


Ilustración 186 Instalación de Grafana

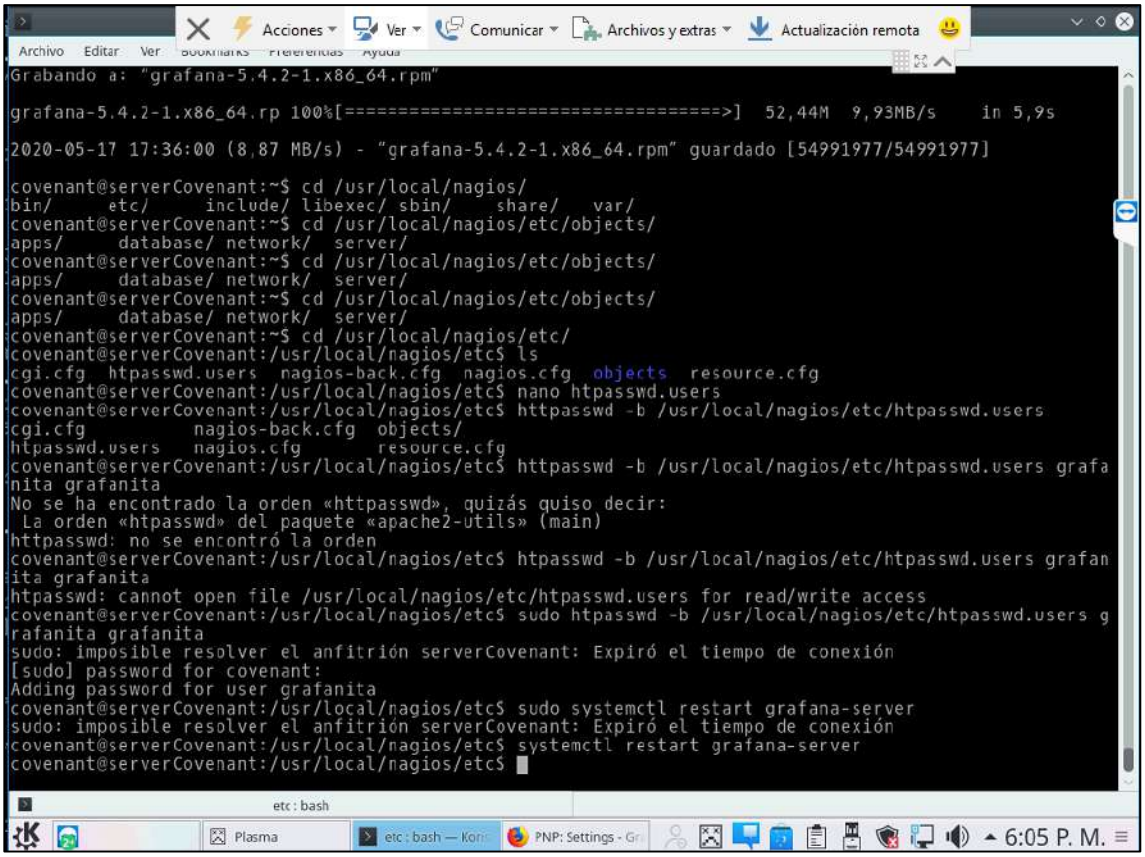


Ilustración 187 Instalación de Grafana

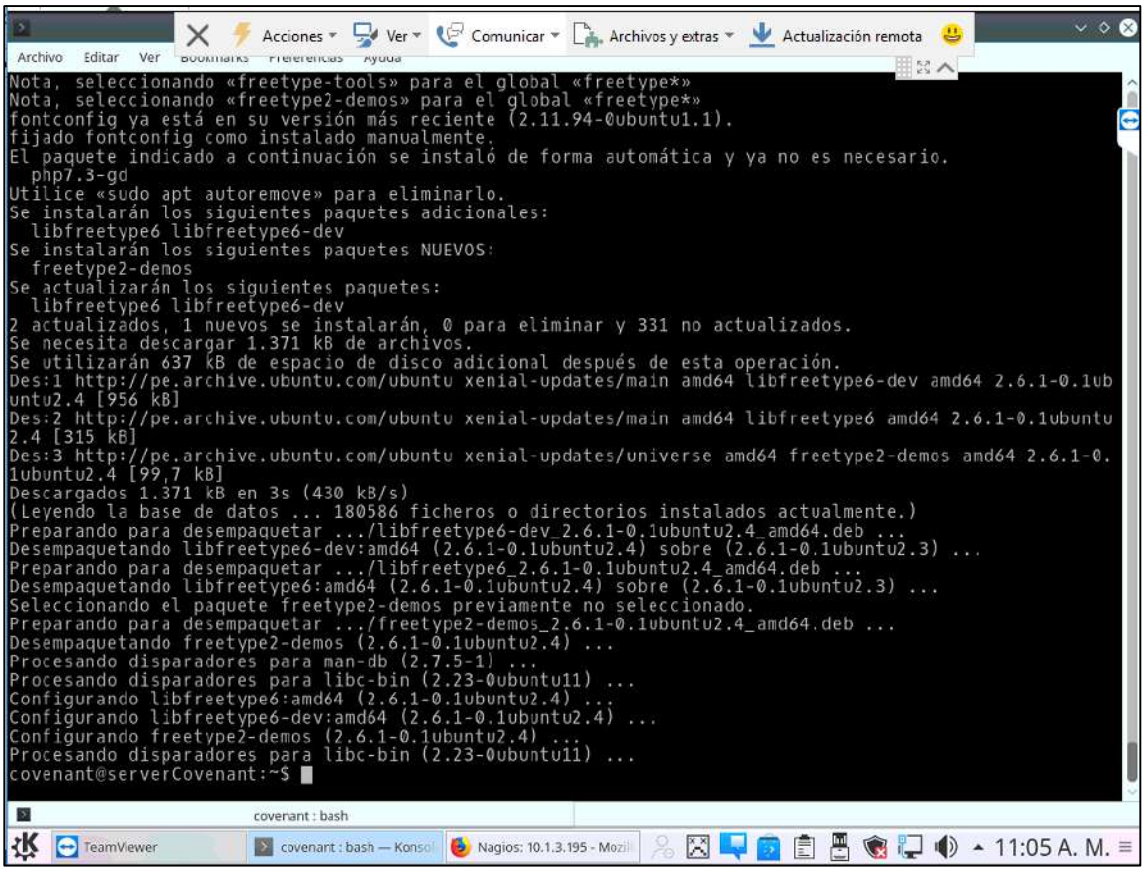


Ilustración 188 Instalación de Grafana

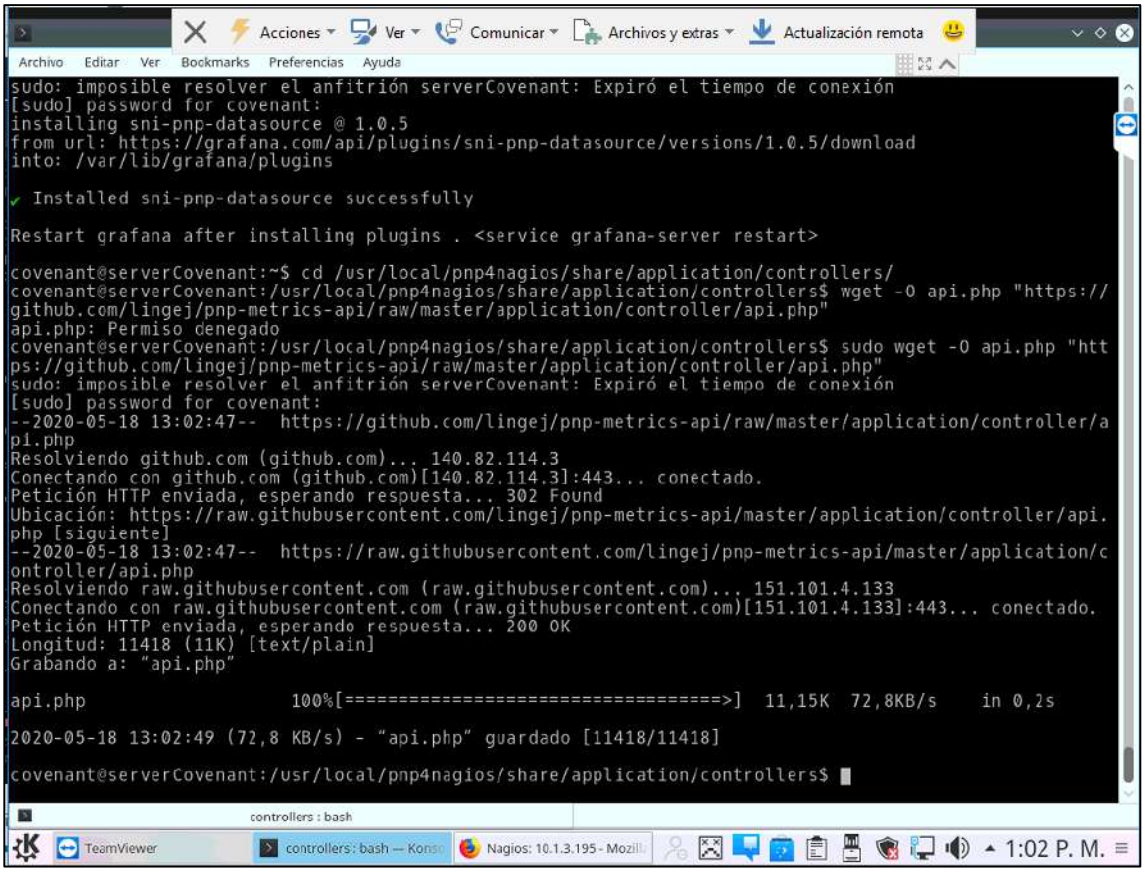


Ilustración 189 Instalación de Grafana

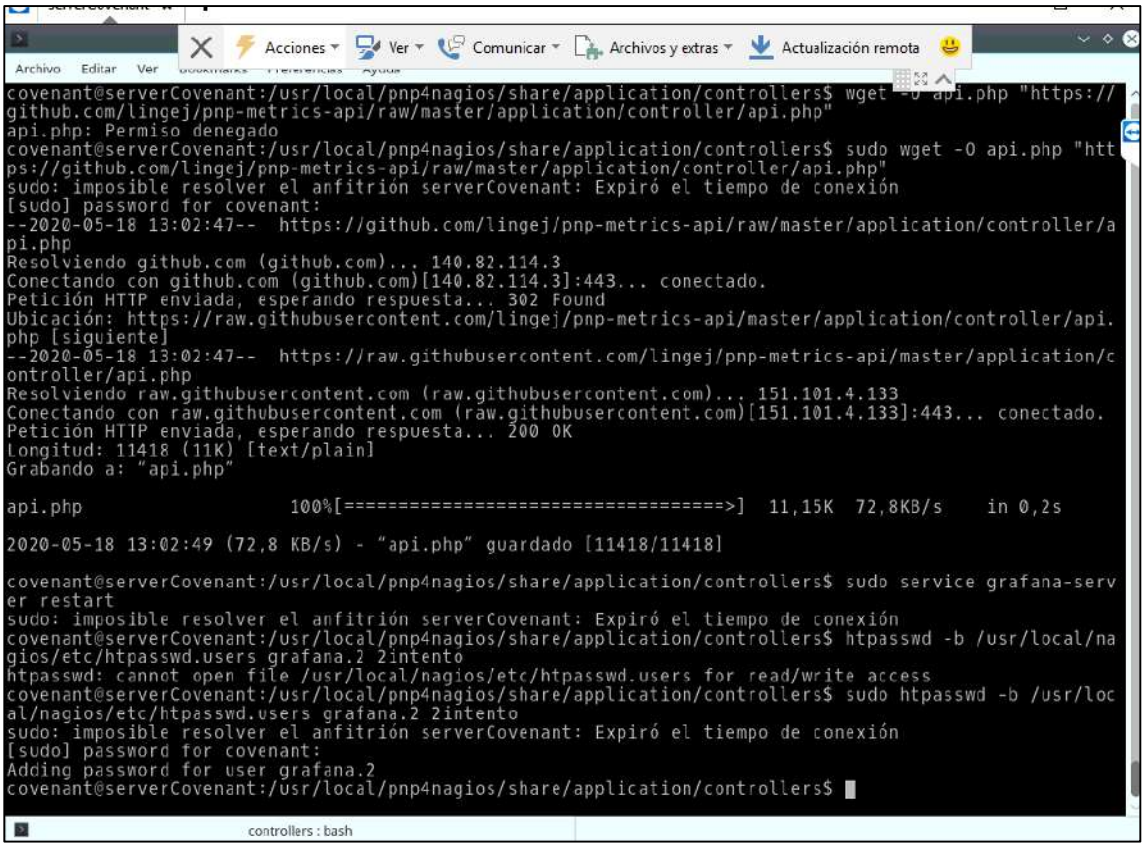


Ilustración 190 Instalación de Grafana

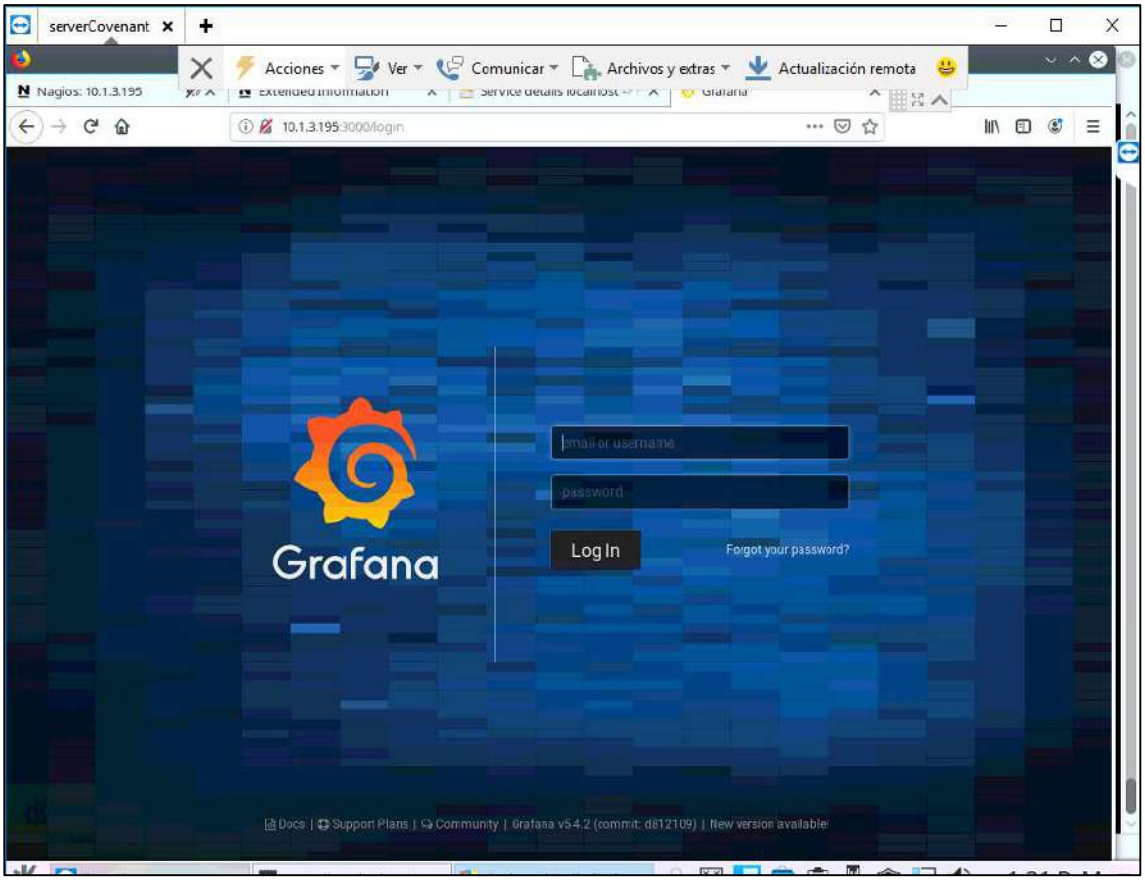


Ilustración 191 Instalación de Grafana

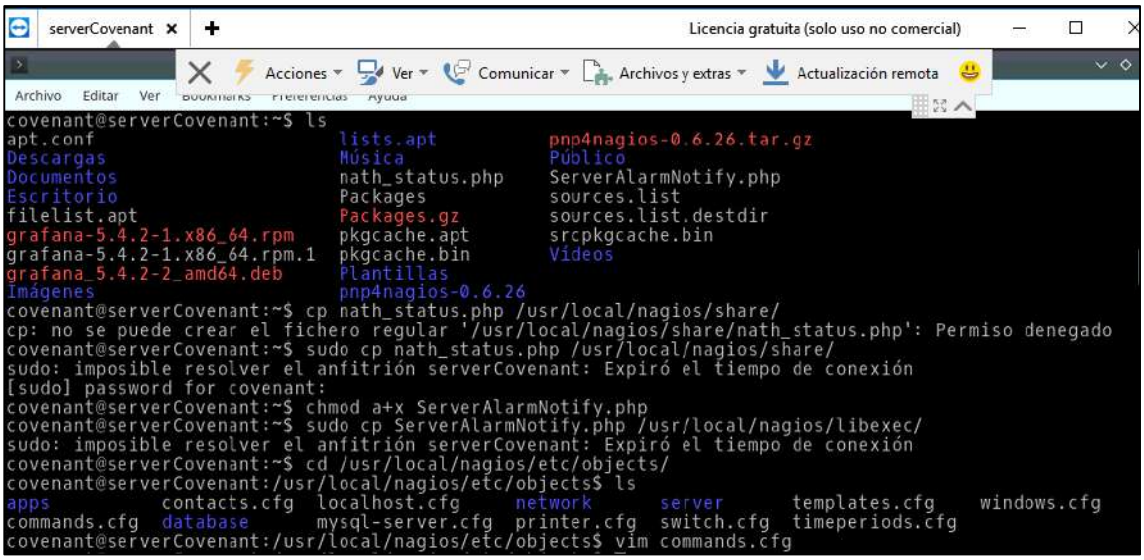


Ilustración 192 Instalación de Grafana

```
##Agregado

define command {

                command_name process-service-perfdata-file

                command_line /bin/mv /usr/local/pnp4nagios/var/service-perfdata /usr/local/pnp4nagios/
var/spool/service-perfdata.$TIMET$

        }

        define command {

                command_name process-host-perfdata-file

                command_line /bin/mv /usr/local/pnp4nagios/var/host-perfdata /usr/local/pnp4nagios/var
/spool/host-perfdata.$TIMET$

        }
## comandos evniar notificaciones host y problemas servicios

        define command{
                command_name sm-host-push-notify
                command_line $USER1$/ServerAlarmNotify.php $HOSTNAME$ ----- HOST $HOSTSATATE$
        }
        define command{
                command_name sm-service-push-notify
                command_line $USER1$/ServerAlarmNotify.php $HOSTNAME$ ----- SERVICE  $HOSTSATATE$
        }
```

Ilustración 193 Instalación de Grafana

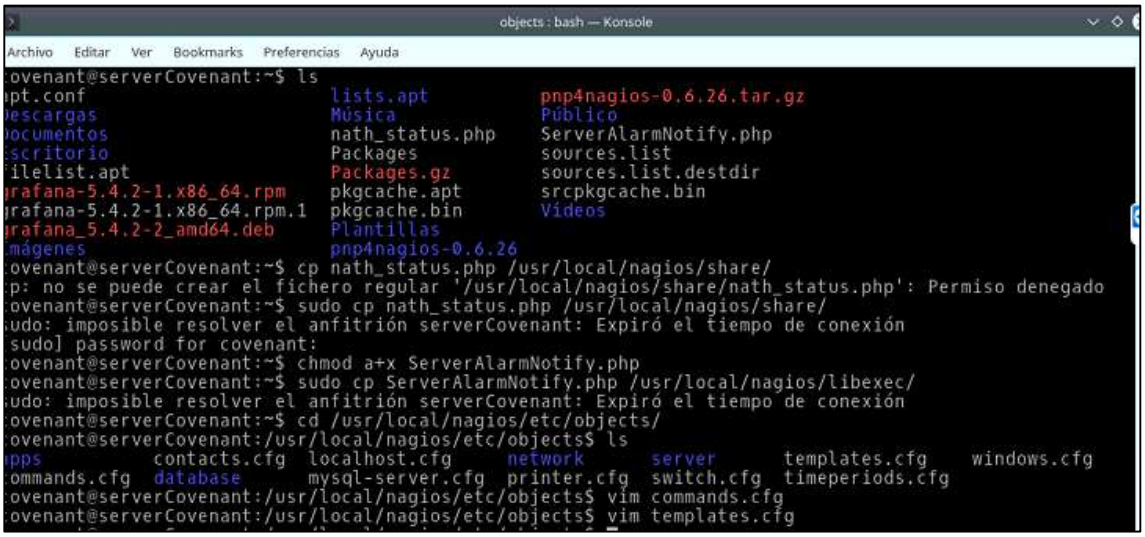


Ilustración 194 Instalación de Grafana

ANEXO 9 - CONFIGURACIÓN TELEGRAM

```
###############################################################################
#
# CONTACT TEMPLATES
#
###############################################################################

# Generic contact definition template
# This is NOT a real contact, just a template!

define contact {

    name                            generic-contact         ; The name of this contact template
    service_notification_period     24x7                    ; service notifications can be sent anytim
e
    host_notification_period        24x7                    ; host notifications can be sent anytime
    service_notification_options    w,u,c,r,f,s             ; send notifications for all service state
s, flapping events, and scheduled downtime events
    host_notification_options       d,u,r,f,s               ; send notifications for all host states,
flapping events, and scheduled downtime events
    service_notification_commands   notify-service-by-email,sm-service-push-notify ; send service noti
fications via email
    host_notification_commands      notify-host-by-email,sm-host-push-notify    ; send host notificati
ons via email
    register                        0                       ; DON'T REGISTER THIS DEFINITION - ITS NOT
 A REAL CONTACT, JUST A TEMPLATE!
}



###############################################################################
#
# HOST TEMPLATES
#
```

Ilustración 195 Instalación de Telegram

```
covenant : bash — Konsole
Archivo  Editar  Ver  Bookmarks  Preferencias  Ayuda
covenant@serverCovenant:~$ cd
covenant@serverCovenant:~$
covenant@serverCovenant:~$
covenant@serverCovenant:~$ curl -Lk -i -X GET https://api.telegram.org/bot1172955481:A
AG3EH9hFkL7pol6leJCPku7Oc7p1Wm-iB8/getUpdates
HTTP/1.1 200 OK
Server: nginx/1.16.1
Date: Wed, 16 Sep 2020 00:41:51 GMT
Content-Type: application/json
Content-Length: 23
Connection: keep-alive
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET, POST, OPTIONS
Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection

{"ok":true,"result":[]}covenant@serverCovenant:~$ curl -Lk -i -X GET https://api.teleg
AG3EH9hFkL7pol6leJCPku7Oc7p1Wm-iB8/getUpdates
HTTP/1.1 200 OK
Server: nginx/1.16.1
Date: Wed, 16 Sep 2020 00:43:15 GMT
Content-Type: application/json
Content-Length: 323
Connection: keep-alive
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET, POST, OPTIONS
Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection

{"ok":true,"result":[{"update_id":210936143,
"message":{"message_id":3,"from":{"id":1248456150,"is_bot":false,"first_name":"Edith",
"last_name":"C\u00e1ceres"},"chat":{"id":-499696385,"title":"Monitoreo NagiosUNC","typ
e":"group","all_members_are_administrators":true},"date":1600216981,"text":"confirmamo
s conexi\u00f3n"}}]}covenant@serverCovenant:~$
covenant : bash
TeamViewer  objects : bash  covenant : bash  Service overview  7:43 P. M.
```

Ilustración 196 Configuración de Telegram

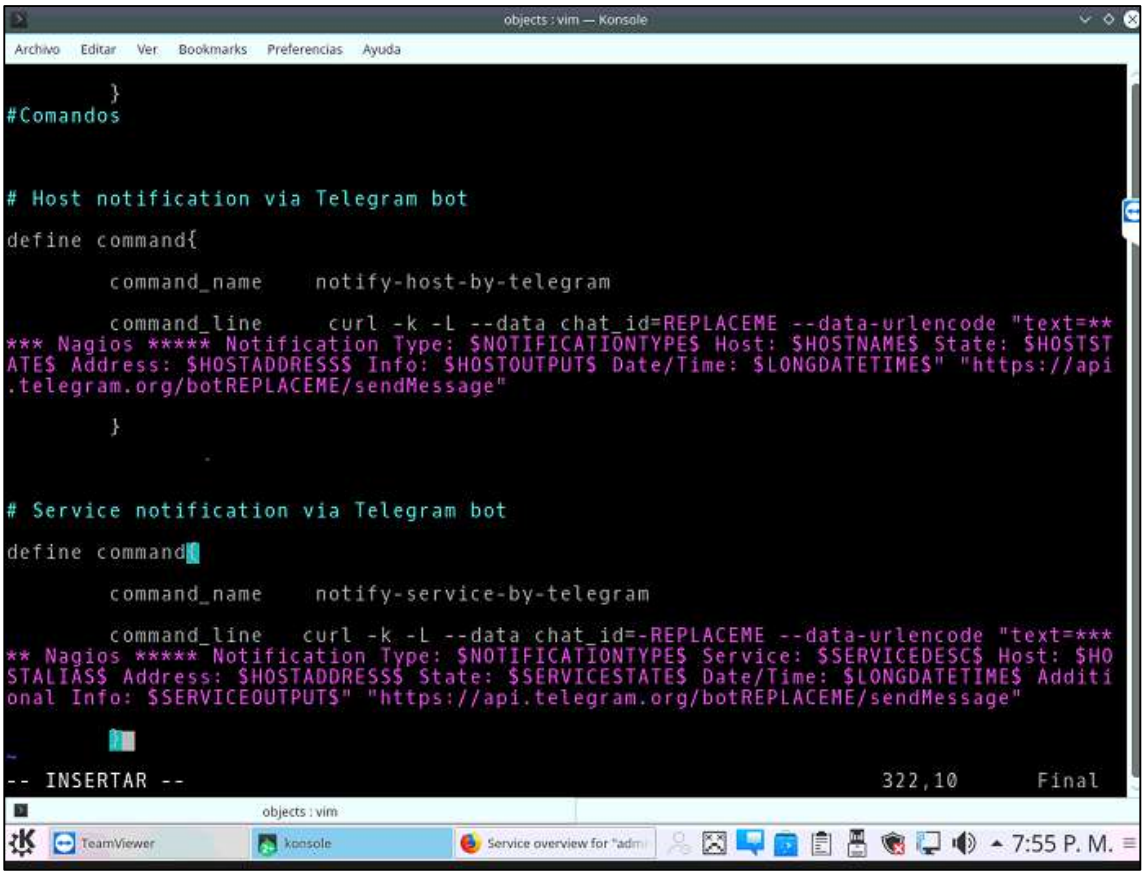


Ilustración 197 Configuración de Telegram

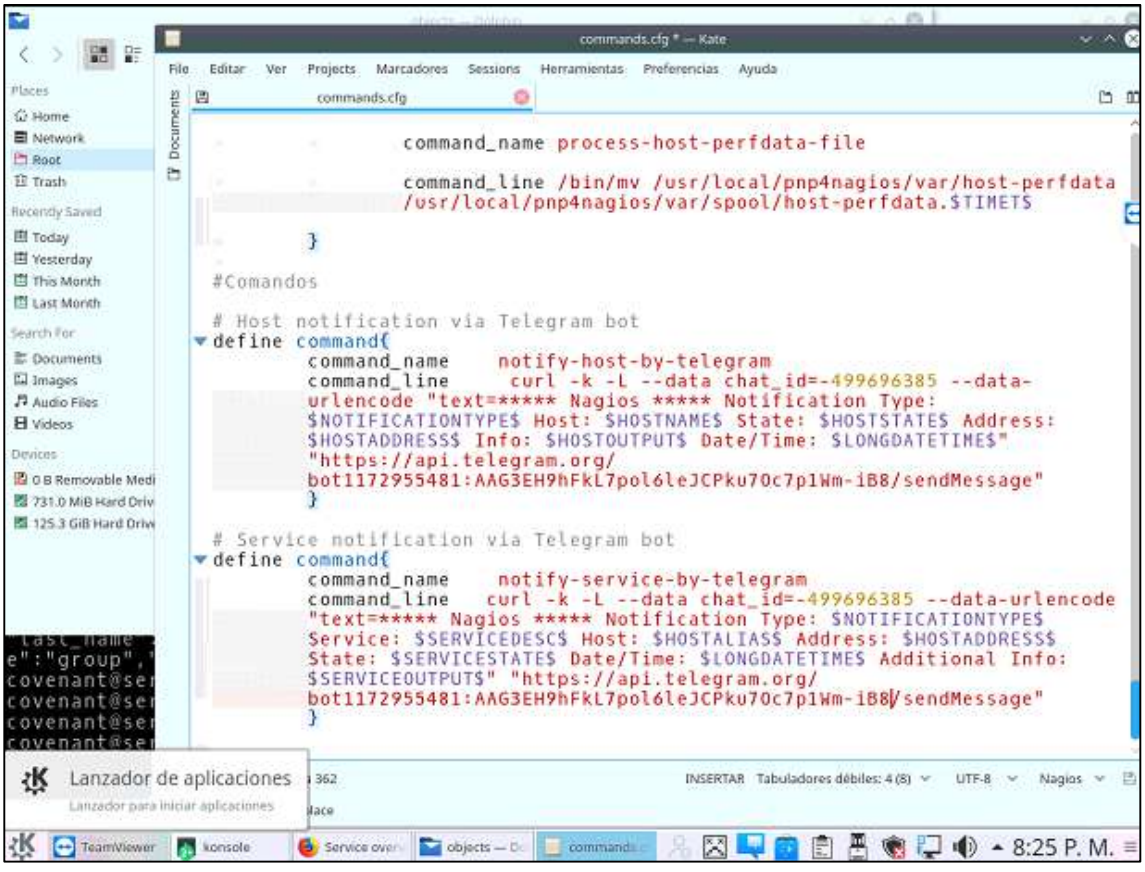


Ilustración 198 Configuración de Telegram

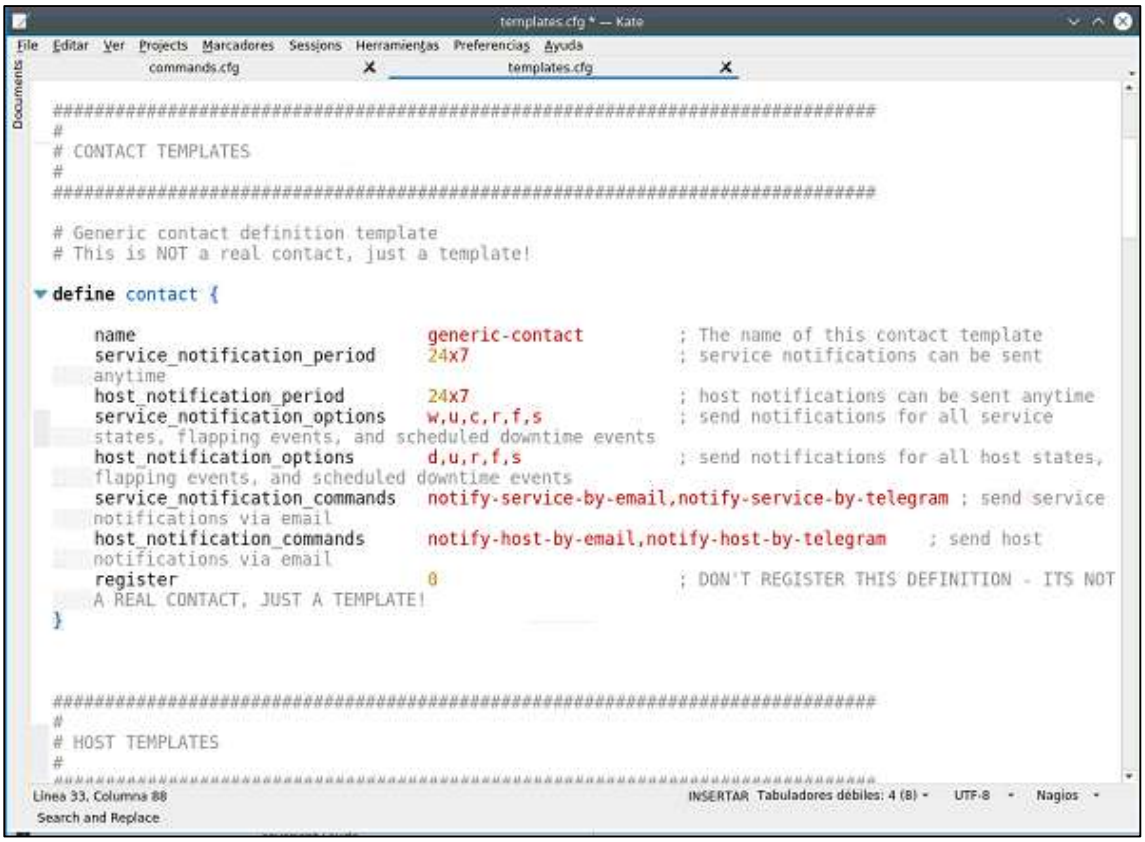


Ilustración 199 Configuración de Telegram

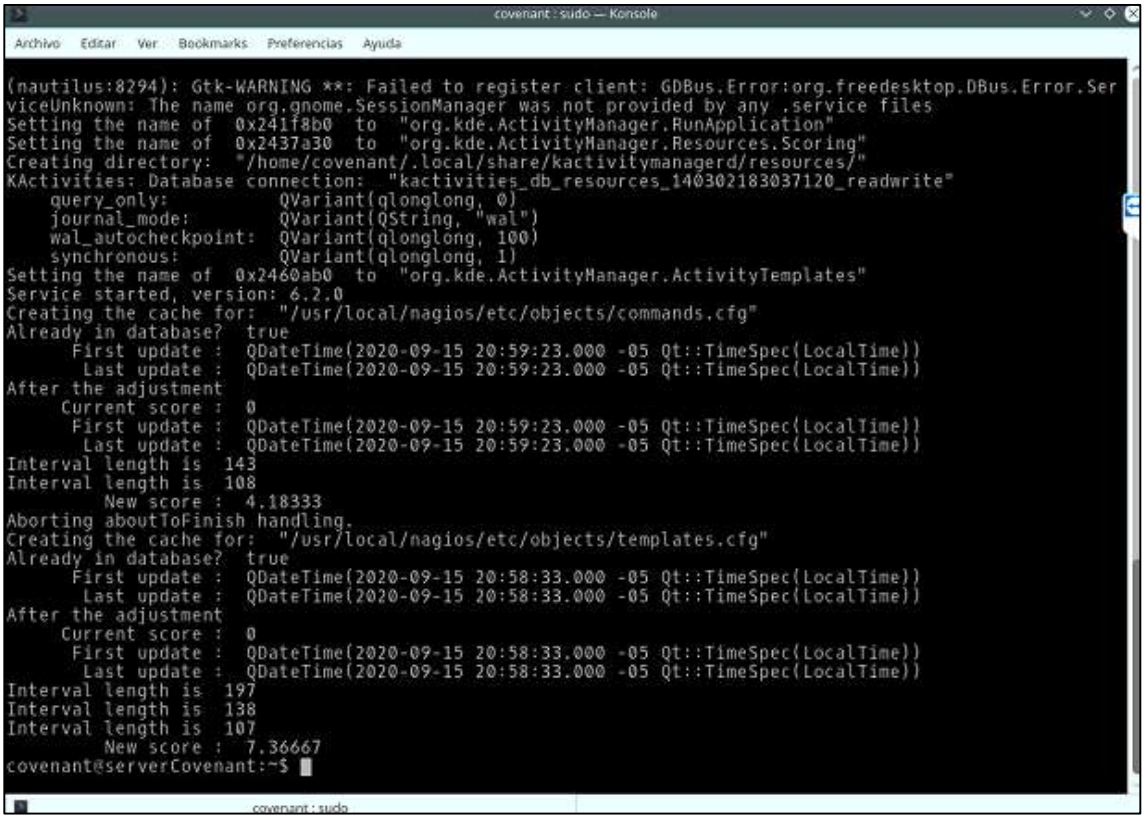


Ilustración 200 Configuración de Telegram