UNIVERSIDAD POLITÉCNICA SALESIANA SEDE GUAYAQUIL

CARRERA DE INGENIERÍA ELECTRÓNICA

DISEÑO E IMPLEMENTACIÓN DE UN BANCO DE PRUEBAS DE LABORATORIO PARA EL CONTROL DE RED Y ANCHO DE BANDA UTILIZANDO PROTOCOLO SNMP Y HERRAMIENTAS OPENSOURCE COMO PANDORA FMS Y GRAFANA

Trabajo de titulación previo a la obtención del

Título de Ingeniera Electrónica

AUTOR: MENDOZA AVILÉS DENNYS PAOLA

TUTOR: ING. DIEGO FREIRE QUIROGA

Guayaquil - Ecuador

2023

CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DETITULACIÓN

Yo, Mendoza Avilés Dennys Paola con documento de identificación N° 0924851967, manifiesto que:

Soy el autor y responsable del presente trabajo; y, autorizo a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Guayaquil, 25 de agosto de 2023

Atentamente,

Mendoza Avilés Dennys Paola

0924851967

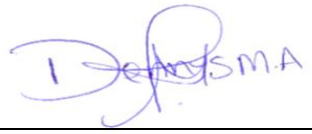
CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DETITULACIÓNA LA UNIVERSIDAD POLITÉCNICA SALESIANA

Yo, MENDOZA AVILÉS DENNYS PAOLA con documento de identificación No. 0924851967, expreso mi voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que soy autor del proyecto técnico: DISEÑO E IMPLEMENTACIÓN DE UN BANCO DE PRUEBAS DE LABORATORIO PARA EL CONTROL DE RED Y ANCHO DE BANDA UTILIZANDO PROTOCOLO SNMP Y HERRAMIENTAS OPENSOURCE COMO PANDORA FMS Y GRAFANA, el cual ha sido desarrollado para optar por el título de: Ingeniera Electrónica en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Guayaquil, 25 de agosto de 2023

Atentamente,



Mendoza Avilés Dennys Paola
0924851967

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Diego Freire Quiroga con documento de identificación N° 0917208084, docente de la Universidad Politécnica Salesiana declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: técnico DISEÑO E IMPLEMENTACIÓN DE UN BANCO DE PRUEBAS DE LABORATORIO PARA EL CONTROL DE RED Y ANCHO DE BANDA UTILIZANDO PROTOCOLO SNMP Y HERRAMIENTAS OPENSOURCE COMO PANDORA FMS Y GRAFANA, realizado por MENDOZA AVILÉS DENNYS PAOLA con documento de identificación N° 0924851967, obteniendo como resultado final el trabajo de titulación bajo la opción de proyecto técnico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, 25 de agosto de 2023

Atentamente,

Ing. Diego Freire Quiroga
0917208084

DEDICATORIA

Esta tesis se la dedico a mi Dios, quien supo guiarme por el buen camino, darme fuerzas para seguir adelante y no dejarme renunciar a mis sueños, aconsejándome en cada uno de los tropiezos en mi vida y sobre todo no dejándome sola.

A mi familia quienes por su esfuerzo llegué hasta aquí. Para mis padres Eber y Paola por su apoyo, consejos, compresión amor, ayuda en los momentos difíciles y por ayudarme con los recursos necesarios para todo este camino. Me han dado todo lo que soy como persona, mis valores, mis principios, mi empeño, mi perseverancia, mi coraje para conseguir y cumplir mis metas.

A mis grandes compañeros y amigos los llevaré en mi corazón.

Mendoza Avilés Dennys Paola.

AGRADECIMIENTO

Agradezco a la Universidad Politécnica Salesiana por haberme permitido formarme como una buena profesional, llena de valores, donde indudablemente no sólo adquieres buenos conocimientos, sino que conoces a muchas personas de las cuales cada una te da muchas enseñanzas.

A mis amigos: John, María y Maite, quienes transformaron los momentos de tensión en sonrisas con cada una de sus ocurrencias y sin olvidarme de un gran amigo Jonathan Choez, quien ahora se encuentra en el cielo, quien deseaba esto tanto como nosotros pero que estamos seguros que desde allá él celebra con nosotros este logro.

Mendoza Avilés Dennys Paola.

RESUMEN

El Protocolo Simple de Administración de Red, también conocido como SNMP, es un protocolo bastante popular entre programadores e informáticos, por su simpleza al momento de permitir la monitorización de variables de distintos dispositivos conectados a una red. En esta tesis se discutirá la implementación de un banco de pruebas para gestión de sistemas de software con este protocolo para la monitorización de redes utilizando herramientas de gestión de eventos en diferentes equipos que pertenecen a una red LAN, incluyendo, por ejemplo, teléfonos móviles, ordenadores, puntos de acceso, enrutadores, conmutadores y servidores.

La implementación de un sistema de monitorización ayudó a incrementar la eficiencia dentro de una red LAN permitiendo al alumno conocer diferentes formas de gestionar y desarrollar soluciones ayudando a detectar de forma anticipada anomalías informáticas con el resultado de realizar un diagnóstico y reducir el tiempo de detección de posibles incidencias en los servicios que se utilizarán. La herramienta Pandora FMS permitió tener un acercamiento al monitoreo de una red LAN por parte de una máquina virtual como servidor yuna Raspberry Pi como agente. Luego el montaje realizado en Node-RED y sus librerías de SNMP permitió tener un mayor acercamiento a la monitorización de red, especificando los equipos y servicios a monitorizar, determinando el tiempo en el que se debe realizar la notificación del estado de su conexión, permitiendo además la adquisición de datos sobre flujos IP.

El objetivo de implementar un banco de pruebas de monitoreo de red y control de ancho de banda utilizando el protocolo SNMP es fortalecer el conocimiento de estudiantes de Ingeniería en Electrónica y Telecomunicaciones, proponiendo un servidor centralizado virtualizado con Node-RED y GRAFANA para su monitoreo en tiempo real. Se crearon cuatro prácticas de laboratorio con actividades pedagógicas que permitieron el acercamiento y conocimiento del protocolo y las herramientas que lo ejecutan.

Palabras claves: Pandora FMS, Grafana, SNMP, Monitoreo de red, LAN

ABSTRACT

The Simple Network Management Protocol, also known as SNMP, is a very popular protocol among programmers and computer scientists, due to its simplicity when it comes to allowing the monitoring of variables of different devices connected to a network. This thesis will discuss the implementation of a software system management test bench with this protocol for network monitoring using event management tools on different equipment belonging to a LAN network, including, for example, mobile phones, computers, access points, routers, switches and servers.

The implementation of a monitoring system helped us to increase efficiency within a LAN network, allowing the student to learn about different ways of managing and developing solutions, helping to detect computer anomalies in advance with the result of making a diagnosis and reducing detection time. of possible incidents in the services that will be used. The Pandora FMS tool allowed to have an approach to the monitoring of a LAN network by a virtual machine as a server and a Raspberry Pi as an agent. Then, the assembly carried out in Node-RED and its SNMP libraries allowed for a closer approach to network monitoring, specifying the equipment and services to be monitored, determining the time in which the notification of the status of your connection should be made, allowing in addition to the acquisition of data on IP flows.

The objective of implementing a network monitoring and bandwidth control test bench using the SNMP protocol is to strengthen the knowledge of Electronic and Telecommunications Engineering students, proposing a virtualized centralized server with Node-RED and GRAFANA for its monitoring in real times. Four laboratory practices were created with pedagogical activities that allowed the approach and knowledge of the protocol and the tools that execute it.

Keywords: Pandora FMS, Grafana, SNMP, Network monitoring, LAN

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

INTRODUCCIÓN

El protocolo SNMP (Simple Network Management Protocol) por su sencillez y versatilidad es parte de la normativa para gestión de redes de computadora desde hace ya varias décadas. Dada la importancia de saber lo que ocurre con los dispositivos de la red: entiéndase siestán o no conectados, cuánto flujo de datos maneja, en qué horarios ocupan un mayor anchode banda, o cuánta velocidad de internet está siendo proveída a cada uno.

En este sentido, se cuenta con herramientas de software. Pandora, Node-Red y Grafana, de uso libre y gratuito, con alta utilidad y amplia funcionalidad. Pandora es útil para configurar un servidor SNMP y conectar los diferentes agentes SNMP como agentes, para poder consultar los datos de consumo de ancho de banda de cada dispositivo conectado en red. Grafana muestra los datos tomados por este servidor, para una visualización detallada del comportamiento de los mismos, y Node-Red mediante scripts hace la captura de los datos de funcionamiento en la computadora y mediante SNMP envía también a un servidor para su visualización.

El presente trabajo de titulación consta de cuatro partes. El Capítulo 1 habla del problema, su planteamiento, estudios relacionados, objetivos y justificación del estudio. El Capítulo 2 contiene la documentación teórica que respalda el desarrollo, incluida la debida referencia a la bibliografía que cita a los autores correspondientes. El capítulo 3 explica cómo se procedió con el desarrollo del trabajo de titulación, incluida la metodología y qué tipo de investigación se utilizó para proceder de manera adecuada. El capítulo 0 tiene los datos y métricas que resultaron del desarrollo investigativo y experimental

1. EL PROBLEMA

1.1. Descripción del problema

En el entorno de las redes de comunicación, donde el uso de ancho de banda y control de red son aspectos críticos para mantener los sistemas en parámetros funcionales y seguros; es necesario conocer las distintas herramientas para poder estar a la vanguardia de la tecnología, y de este modo poder evitar o mitigar oportunamente fallas que puedan afectar su correcto funcionamiento.

Las empresas, colegios, industrias y universidades van experimentando cambios con las nuevas tecnologías de red que surgen día a día, actualizándose con el objetivo de abastecer al constante incremento de dispositivos nuevos que acceden, generando tráfico y provocando muchas veces la saturación de la red, lo cual da como resultado la congestión de las redes, o lo que se conoce comúnmente como “internet lento”.

Los estudiantes de la carrera de Ingeniería en Telecomunicaciones de la Universidad Politécnica Salesiana sede Guayaquil, no cuentan con un banco de pruebas para realizar prácticas de monitoreo y control de red a través de software libre, donde deben estar preparados para los diferentes problemas que se presentan en la industria de las telecomunicaciones.

El laboratorio de Telecomunicaciones no está provisto de un servidor virtualizado con software de monitorización para realizar prácticas con el protocolo SNMP, por lo que el conocimiento que se tiene sobre el tema es únicamente lo revisado en la clase teórica. Esto vuelve necesario el refuerzo de la parte práctica para la experimentación y desarrollo de diferentes formas de efectuar un control de red en tiempo real detectando precipitadamente fallas de conexiones en dispositivos.

1.2. Antecedentes

En los últimos años muchos estudios han abarcado la importancia de la monitorización de redes, para control de su rendimiento y asegurar una velocidad adecuada de navegación para todos los dispositivos conectados. Algunos de estos trabajos de investigación brindan el marco de estudio en el que se sustenta el presente proyecto de titulación.

La herramienta Pandora FMS proporciona una solución completa para monitorizar el rendimiento y disponibilidad de las máquinas de los laboratorios a fin de garantizar que todas

estas están funcionando bajo los criterios de operación establecidos. Por otro lado, Integria IMS permite la gestión de tickets para llevar el control de incidencias, además de un completo sistema de inventario y capacidad interna de auditoría. Integria es un derivado parcial de Pandora FMS (Gutiérrez, Gómez, & Méndez, 2017).

Fueron identificados en un estudio dos protocolos comúnmente utilizados para la gestión de red, con amplia difusión y disponibilidad en los dispositivos propios de una red avanzada; con el objetivo de determinar la mejor alternativa de configuración en un entorno emulado de la gestión de una red avanzada considerando la configuración de los protocolos en los equipos, el uso de recursos, la seguridad que presentan y los servicios disponibles (Ramírez, 2019)

La importancia de contar con un sistema de monitoreo para toda la infraestructura del Data Center en la empresa Netsecure Perú, se da debido a que al transcurrir los años la empresa ha ido incrementando sus servicios y equipos tecnológicos. Un esquema de monitorización propuesto pretende informar la correcta actuación de la red, los servidores y servicios, el cual se halla orientado a desplegarse en una de la compañía más prestigiosa en el ambiente de la tecnología de la informática Netsecure Perú (Oré, 2019).

Se logran resultados útiles juntando los protocolos SNMP y NETFLOW para monitorizar en tiempo real una red LAN de 4 sedes de una empresa de Lima, Perú. Este estudio brinda amplio contexto en el que se basa la importancia de la gestión de redes informáticas, pues los resultados obtenidos incluyen mejora en la accesibilidad de los servicios de internet, control del ancho de banda, monitorización en tiempo real de dispositivos, mejora en el rendimiento de la LAN y prevención de eventos que puedan dañar la red o disminuir su calidad (Dett & Vega, 2020).

Aunque la plataforma Pandora es bastante versátil, puede ser un poco exclusivo su uso, al ser de pago- Por lo que también existen herramientas hechas a medida para poder hacer un monitoreo de redes, en este caso implementada con Python, y Node-Red.

El software de uso libre Grafana puede ser utilizado para generar gráficos, este estudio la encontró altamente personalizable y eficiente, lo que permitió optimizar recursos y a la vez lograr gran impacto en el monitoreo de manera periódica. Combinando las funcionalidades de Grafana y PNP4Nagios se logra la obtención de datos y su monitoreo de manera exitosa (López, 2021).

1.3. Delimitación del Problema

1.3.1. Delimitación Académica

El proyecto “Diseño e implementación de un banco de pruebas de laboratorio para el control de red y ancho de banda utilizando protocolo SNMP y herramientas código libre como Pandora FMS y Grafana”, consiste en un conjunto de prácticas que permitieron conocer a profundidad herramientas de administración de redes con base en la implementación del protocolo SNMP. En este proyecto se integraron de manera efectiva conocimientos adquiridos en las materias: Redes de Computadoras I y II, Comunicaciones Inalámbricas, Comunicaciones Ópticas y Fundamentos de Telecomunicaciones.

1.3.2. Delimitación Temporal

La implementación de este proyecto se realizó en un período de seis meses a partir de la aprobación del mismo, dentro del período académico 2023.

1.3.3. Delimitación Espacial

La implementación del proyecto de titulación se realizó en dos etapas, la primera en el domicilio de la autora, y una segunda en los laboratorios de Telecomunicaciones, ubicado en el bloque E, en la sede Guayaquil de la Universidad Politécnica Salesiana.

1.4. Objetivos

1.4.1. Objetivo General

Diseñar e implementar un banco de pruebas de laboratorio para el control de red y anchode banda utilizando protocolo SNMP y herramientas Open Source como Pandora FMS y Grafana.

1.4.2. Objetivos Específicos

- Instalar software de monitoreo Pandora FMS y Grafana en el servidor del laboratorio de Telecomunicaciones.
- Diseñar e implementar cuatro prácticas de monitorización de equipos de red LAN creada en el Laboratorio de Telecomunicaciones de la Universidad Politécnica Salesianasede Guayaquil.
- Se demuestran los resultados obtenidos con los agentes de monitoreo de red basados en Open Source.

1.5. Beneficiarios de la Propuesta

Los beneficiarios de este proyecto técnico son los estudiantes de la carrera de Ingeniería en Telecomunicaciones que conocerán las diversas maneras de monitorear una red IP.

1.6. Justificación

El motivo principal de la realización de este estudio es la importancia de la gestión de redes en un mundo globalizado, donde día a día el internet llega a cada rincón del mundo, no solamente a nivel virtual, sino en lo físico, como por ejemplo en el campo de la domótica, inmótica y el internet de las cosas (IoT) tanto en el área residencial y empresarial, como en industria 4.0.

La gestión de redes implica monitorización y control, en este sentido, es posible para el personal de sistemas supervisar permanentemente el flujo de datos, lo que permite anticipar posibles fallas provocadas por la saturación de la red, así como planificar de manera más eficiente, por ejemplo, la apertura de nuevas líneas de producción en una planta, incremento en el número de equipos dentro de una oficina, o la implementación de mejoras que requieran mayor ancho de banda.

1.7. Hipótesis

Es posible crear un servidor SNMP en una máquina virtual, que pueda recopilar datos de al menos dos dispositivos que funcionen como agentes SNMP, y mostrar información de la monitorización en un dashboard en GRAFANA. También se puede hacer gestión de redes con Node-Red, y visualizar el comportamiento de las conexiones existentes.

2. MARCO TEÓRICO

2.1. Gestión y Monitoreo de Red

La literatura define la gestión de red como la integración exitosa de hardware, software y sus usuarios, para pruebas, configuración, análisis, evaluación y monitorización de elementos y recursos de la red. Las partes principales que intervienen en la gestión de red son el servidor de gestión, que es donde se realiza el procesamiento, análisis y visualización de la gestión; y el dispositivo gestionado, que será cualquier dispositivo que sea parte de la red, entre los que se puede mencionar host, routers, switches o módems (Kurose & Ross, 2017).

2.2. Simple Network Management Protocol versión 3 (SNMPv3)

SNMP es un protocolo que forma parte del conjunto de protocolos TCP/IP, más específicamente de la capa de información, y es el encargado de servir como canal de comunicación entre dos dispositivos de red, con la finalidad de intercambiar mensajes necesarios para un proceso de gestión de red. Estos dispositivos en general son un servidor de gestión y un agente del servidor para la gestión. Por su facilidad de uso es considerado el estándar para encontrar y solucionar problemas, así como para planificar el crecimiento de la red (Millán, 2003).

2.2.1. Arquitectura de red de SNMPv3

En síntesis, el protocolo SNMPv3 tiene una arquitectura cliente-servidor. El servidor es unsoftware gestor que sondea constantemente a los agentes SNMP en búsqueda de la información requerida. El cliente consta de un software agente y una base de datos o MIB que tiene información para la gestión. La figura 1 muestra la arquitectura descrita en líneas anteriores. El funcionamiento consiste básicamenteen el intercambio de información de gestión entre nodos gestores y nodos gestionados.

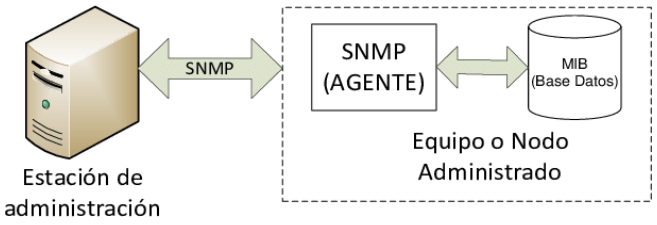


Figura 1: Arquitectura del protocolo SNMP (Hernández, 2015)

2.2.2. Ventajas frente a Protocolos similares y otras versiones de SNMP

El protocolo SNMP contiene algunas ventajas frente a otros métodos de monitoreo de redes, por ejemplo:

Simplicidad de gestión: SNMP se destaca por un enfoque sencillo y eficiente para gestionar redes. Su estructura de datos jerárquica basada en el Modelo de Información de Administración de Red (MIB) permite una fácil configuración y supervisión de los dispositivos de red. Esto simplifica las tareas de gestión y facilita la administración de la red en comparación con otros protocolos más complejos.

Amplia compatibilidad: SNMP ha sido ampliamente adoptado y está respaldado por una amplia gama de dispositivos de red y sistemas operativos. Esta compatibilidad generalizada permite que las soluciones basadas en SNMP se integren fácilmente en entornos existentes sin requerir cambios significativos en la infraestructura de red.

Flexibilidad y escalabilidad: SNMP ofrece una arquitectura flexible y escalable que se adapta a diferentes entornos de red. Permite la gestión de una amplia variedad de dispositivos y servicios de red, lo que lo convierte en una solución versátil para el control de red y el ancho de banda.

También tiene algunas desventajas frente a otros métodos, por ejemplo:

Falta de autenticación: Una desventaja importante de SNMP es la falta de autenticación incorporada en su versión original (SNMPv1). Esto significa que los mensajes SNMP pueden ser interceptados o manipulados por personas no autorizadas, lo que representa un riesgo para la seguridad de la red. Sin embargo, versiones posteriores de SNMP (como SNMPv3) abordan esta limitación al proporcionar mecanismos sólidos de autenticación y seguridad.

Consumo de ancho de banda: En comparación con algunos protocolos similares, SNMP puede consumir un mayor ancho de banda al operar en modo conectado. Esto se debe a que

cada transacción SNMP requiere una serie de intercambios de mensajes entre el dispositivo de gestión y los agentes SNMP. Sin embargo, este aumento en el consumo de ancho de banda generalmente se considera aceptable en redes modernas con capacidades de red adecuadas.

2.2.3. MIBs y OIDs

Los identificadores de objetos son conocidos como OID por el inglés “object identifier”. Se conforman como cadenas de números, de tamaño variable, separados por punto y que corresponden a una jerarquía similar a la de DNS. Esta cadena de números indica una ruta para llegar a un objeto en particular dentro del dispositivo, de manera que constituye una llave única de dicho objeto (DPSTelecom, 2022).

La colección de todos los objetos organizados en esta topología de tipo árbol conforma una base de datos conocida como Base de Datos Gestionados o MIB por el inglés “Management Information Database”. La importancia de esta MIB en SNMP radica en que permite traducir los eventos ocurridos en el dispositivo a un lenguaje que puede entender el administrador de la red. En la figura 2 se observa la estructura del árbol MIB de SNMP y sus OIDs.

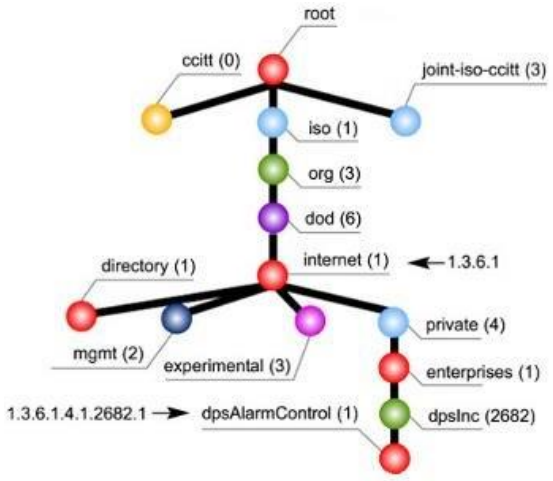


Figura 2: Estructura del árbol MIB de SNMP y sus OIDS (DPSTelecom, 2022)

2.3. Grafana

Es una plataforma de análisis para métricas de amplia funcionalidad, que permite presentar datos a través de tableros de instrumentos personalizables. Estos tableros constan de

herramientas especializadas que pueden extraer datos desde cualquier base que los contenga, y permite su visualización y consulta, para posterior análisis y manipulación. La figura 3 muestra el desarrollo y la altacompatibilidad que presenta Grafana el cual permite trabajar muy bien con soluciones en la nube y con servidores locales. (Aplyca,2018)

Figura 3: Dashboard desarrollado en Grafana.(Grafana, 2022)

2.4. Pandora FMS

Pandora FMS tiene un Servidor de Red que ejecuta de forma sistemática tareas asignadas, utilizando un sistema de colas multiproceso. De esta manera se vuelve posible la gestión de una red conectada de varios agentes SNMP. La figura 4 muestra el desarrollo y el estado de las interfaces, el consumo de ancho de banda de cada dispositivo (PandoraFMS, 2021). La plataforma es Software de uso libre, aunque tiene versión de pago con mayores funcionalidades y versatilidad.

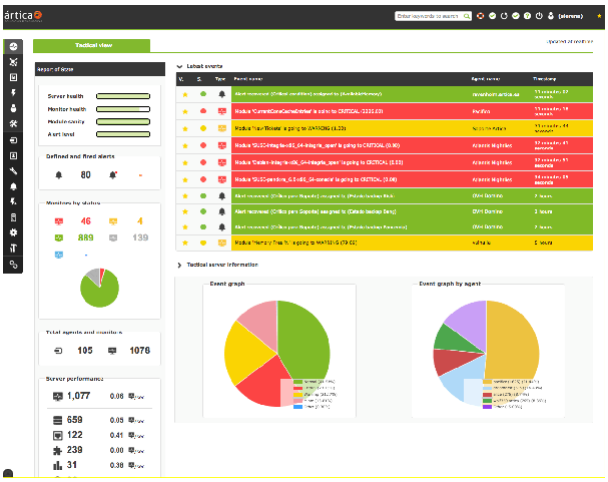


Figura 4: Dashboard desarrollado en Pandora. (PandoraFMS, 2021)

2.5. Node-RED

Node-RED es un software para desarrollo de programas que vinculen dispositivos electrónicos con interfaces virtuales, aplicaciones y servicios en línea. Utiliza diagramas de flujo a través de un editor al que se puede acceder por diversas plataformas dado que funciona con protocolo HTTP en el puerto 1883 (Node-RED, 2022). Para facilidad del cumplimiento de los objetivos, se instaló Node-RED en la Raspberry Pi Servidor SNMP, y se accedió al editor desde una ventana de navegador en una computadora portátil.

Las librerías con las que funciona Node-RED son flujos y nodos pre configurados y se basan en desarrollo comunitario debido a que constituye software de fuente abierta. Las librerías que fueron llamadas para el desarrollo de este proyecto son Big-Timer, SNMP Node-RED, InfluxDB, y Telegram Bot. La librería Big-Timer, o como su nombre oficial indica, node-red-contrib-bigtimer versión 2.8.3, es un nodo que ofrece determinadas utilidades referentes al tiempo, lo que permite manejo y gestión de tareas repetitivas en un lapso deseado (Node-RED, 2022). De esta manera, fue utilizada para que el servidor SNMP pueda consultar cada minuto, datos de valores de navegación que son de gran utilidad.

La librería SNMP Node-RED es un nodo que asigna valores OID, soporta las tres versiones existentes del protocolo SNMP. De la misma manera es posible utilizarla para extraer valores de los servidores. Los nodos disponibles de esta librería se pueden observar en la **¡Error! No se encuentra el origen de la referencia.**. La figura 5 muestra los nodos snmp que permite extraer OIDs o una lista de OIDs separados por coma, accionados por una entrada. El nodo snmp-set asigna valores a uno o más OIDs. El nodo snmp-walker realiza la lectura desde un OID específico hasta el finalde la tabla.

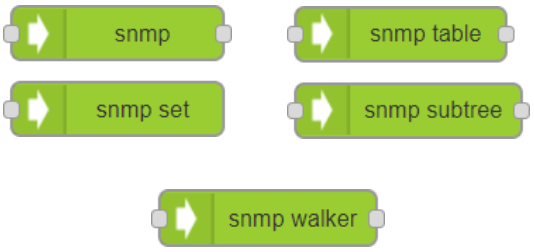


Figura 5: Nodos de la librería SNMP (Node-RED, 2022)

La librería node-red-contrib-influxdb o influxdb de Node-RED, permite escribir y consultar datos de una base en influxdb mediante los nodos input y output, respectivamente. Una funcionalidad adicional de esta librería permite consultar objetos por lotes, mediante el nodo

output tipo batch (Node-RED, 2022). La figura 6 muestra los nodos de la librería Telegram Bot para Node-RED permite utilizar un token de botfather de Telegram, para vincular Node-RED con Telegram, permitiendo de esta manera el envío y recepción de mensajes a esta aplicación de mensajeríainstantánea.

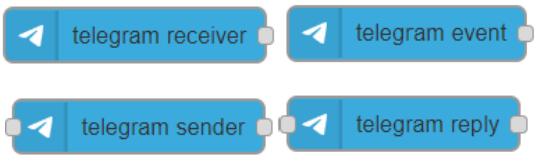


Figura 6: Nodos de la librería Telegram Bot Node-RED (Node-RED, 2022)

2.6. Python

Python se conforma como un lenguaje de programación y se caracteriza por ser fácil de aprender y eficiente en la creación de estructuras de datos de alto nivel. La facilidad en la escritura y simpleza de su estructura lo hacen fácil de aprender. Python se constituye como un lenguaje interpretado, lo que significa que no requiere compilación, sino que se ejecuta línea a línea y de manera permanente se encuentra convirtiendo lo programado en lenguaje que puede entender la computadora (Swaroop, 2022).

Las utilidades de Python son diversas, más aún por cuanto existen comunidades que desarrollan y comparten paquetes con fuente abierta para que cualquier programador tenga utilidad de ellas. Una de estas utilidades es Speedtest, que vincula la interfaz con la página web speedtest.net y permite conocer la capacidad del ancho de banda de la red en la que se trabaja. La figura 7 muestra otra librería mencionada en el presente proyecto es psutil, que recopila información del sistema, como memoria disponible, capacidad y procesamiento, sensores, entre otros, utilizada muy frecuentemente para monitoreo de sistemas (Python ORG, 2022).

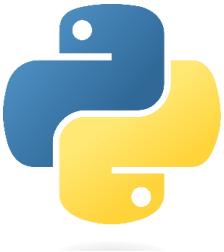


Figura 7: Logo Python (Python ORG, 2022)

2.7. Raspberry Pi

Raspberry Pi Foundation se constituye como una organización sin fines de lucro y su principal meta es llevar una computadora a cada hogar del mundo, por lo que se dedica de lleno al desarrollo de tarjetas electrónicas para sistemas embebidos. La Raspberry Pi 4 salió a la venta en el 2019. Consta de un procesador tetra core Broadcom BCM 2711 de 64 bits con una velocidad de procesamiento de 1.5 GHz. La tecnología WLAN y Bluetooth integrado permiten la comunicación en red y con otros dispositivos. Además, tiene un puerto Ethernet y GPIO de 40 pines, 4 puertos USB, salida estéreo y puerto HDMI. La tarjeta Raspberry Pi es capaz de dar acceso a sus usuarios por varias interfaces, entre las más populares se pueden mencionar VNC y SSH (Raspberry Pi, 2022).

Como sistema operativo, Raspberry Pi ofrece diversas opciones para satisfacer las necesidades y preferencias de sus usuarios. Se utilizará Raspbian, que es el sistemaoperativo oficial y más utilizado para Raspberry Pi. Está basado en el sistema operativo Debian y cuenta con una interfaz de usuario amigable y optimizada para el uso en estos dispositivos. La figura 8 muestra la Raspberry Pi OS el cual viene preinstalado con una serie de herramientas y programasesenciales, lo que lo convierte en una excelente opción.

Figura 8: Tarjeta electrónica Raspberry Pi 3B (Node-RED, 2022)

2.8. Virtualbox

La figura 9 muestra el software de virtualización de código abierto desarrollado por Oracle Corporation. Se utiliza para crear y ejecutar máquinas virtuales en un sistema operativo anfitrión. Esta herramienta permite que los usuarios instalen y ejecuten múltiples sistemas operativos en unamisma computadora, como si fueran máquinas independientes.

Ofrece una interfaz gráfica fácil de usar que facilita la configuración y administración de las máquinas virtuales. Además, es compatible con una amplia variedad de sistemas operativos invitados, incluyendo diversas versiones de Windows, Linux, macOS, Solaris y más.

Figura 9: Logo VirtualBox (Oracle, 2023)

2.9. Sistema operativo Centos

Es una distribución de sistema operativo Linux de tipo Enterprise, de código abierto y basada en el código fuente de Red Hat Enterprise Linux (RHEL) mostrada en la figura 10. Su nombre proviene de "CommunityEnterprise Operating System". Se caracteriza por ofrecer un sistema operativo robusto, estable y seguro, orientado principalmente a entornos empresariales y servidores.

Es desarrollado y mantenido por una comunidad de voluntarios que trabajan en conjunto para asegurar que la distribución sea totalmente compatible con RHEL y, por lo tanto, pueda beneficiarse de las actualizaciones y parches de seguridad proporcionados por Red Hat. Esto hace que CentOS sea una excelente opción para aquellos que buscan una alternativa gratuita y fiable a RHEL, sin perder la estabilidad y el soporte a largo plazo.

Figura 10: Logo Centos (Oracle, 2023)

2.10. InfluxDb

Es una base de datos de series temporales de código abierto diseñada para almacenar, consultar y visualizar datos temporales con alta disponibilidad y rendimiento. Se ha convertido en una herramienta popular en el ámbito de la monitorización y recopilación de datos de tiempo real.

La característica más destacada de InfluxDB es su capacidad para gestionar grandes volúmenes de datos que cambian con el tiempo, como datos de sensores, métricas de rendimiento, registros de eventos y cualquier información que se genere o actualice en intervalos regulares. Su arquitectura optimizada para series temporales permite una escritura y lectura eficiente de datos, lo que la hace ideal para aplicaciones que generan flujos continuos de información.

La figura 11 muestra la base de datos que utiliza el lenguaje de consulta InfluxQL, el cual facilita la realización de consultas y agregaciones temporales para analizar y visualizar los datos almacenados. Además, InfluxDB es compatible con múltiples interfaces y protocolos, como HTTP, line protocol, SNMP, entre otros, lo que facilita la integración con diversas aplicaciones y sistemas.

Figura 11: Logo Indluxfdb (Influx Db, 2023)

3. MARCO METODOLÓGICO

Dentro de la investigación científica como desarrolladores de conocimiento comprometidos a la producción de material científico confiable se respalda este trabajo investigativo dentro deun marco metodológico delimitado y definido. En los siguientes títulos hablara sobre el método utilizado, además de los tipos de investigación que serán de ayuda para llevar a cabo este proyecto.

3.1. Método Analítico – Sintético

El método analítico – sintético consiste en el desglose del objeto de estudio en sus partes más básicas, para después estudiar al objeto como un todo. Estudiar individualmente cada sección ayuda a especializarse dentro del conocimiento, y la conjunción que se realiza luego ayuda a entender el objeto como un todo y a la vez como la suma de cada parte. Es necesario explorar cómo se relacionan estas partes para saber cómo esta relación influirá en las demás.

3.2. Investigación Descriptiva y Aplicada

Se utiliza la investigación descriptiva para sistematizar el proceso por el cual se elabora un banco de prácticas donde intervienen variables tanto cualitativas como cuantitativas, esto quiere decir considerar características medibles y los parámetros en que se tomaron dichas medidas. También será útil la investigación aplicada, ya que el objetivo luego de estudiar, es producir conocimiento y convertirlo en un producto orientado a satisfacer necesidades de un grupo beneficiario.

4. IMPLEMENTACIÓN DE LA PROPUESTA

4.1. Arquitectura del Sistema

Se proponen dos arquitecturas de sistema, donde cada una en su implementación tienen su alcance y facilidad de despliegue. La figura 12 muestra la primera implementación de un servidor virtualen VirtualBox con el sistema Pandora, con el envío de datos a Grafana y notificaciones de alertas por medio de Telegram. En este caso, los agentes serían dos tarjetas Raspberry Pi que configuradas como agentes SNMP, envían datos de su funcionamiento.

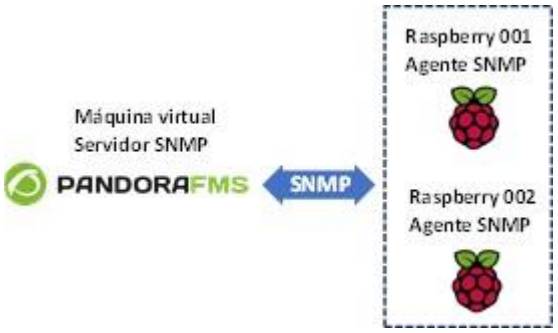


Figura 12: Arquitectura de red en Pandora para la solución propuesta
(Pandora, 2023)

La segunda sería la configuración de una Raspberry Pi como servidor SNMP, que supervisa la acción de otros dos dispositivos Raspberry Pi que funcionan como agentes SNMP. En la figura 12 se observa la jerarquía descrita anteriormente, con la Raspberry Pi principal como servidor y las otras dos Raspberry Pi como agentes, vinculadas cada una a su respectiva MIB.

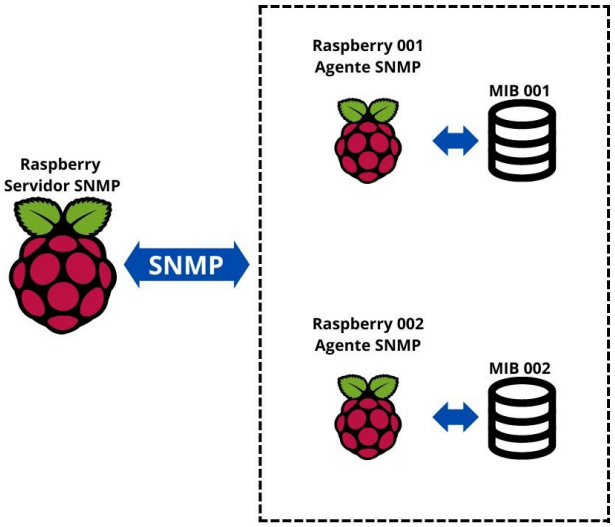


Figura 12: Arquitectura de red para la solución propuesta (Pandora, 2023)

El servidor SNMP es una tarjeta Raspberry Pi 3 b+ con sistema operativo Raspbian, en la cual se instalaron las utilidades de Node-RED y Grafana. Con la librería SNMP de Node-RED en lenguaje de diagrama de flujo fue creada la lógica que condiciona el funcionamiento de esta Raspberry Pi como servidor SNMP. Al mismo tiempo brinda la utilidad de un Dashboard que presenta en forma de gráficas, los datos consultados de los demás dispositivos, agentes SNMP, conectados a la red. De igual manera se instaló Grafana en el servidor SNMP, para la ejecución de gráficas con los datos disponibles en las MIBs de los agentes SNMP.

En la figura 13 se observa un diagrama del funcionamiento del prototipo implementado. En este caso la relación del servidor con los agentes es bidireccional, ya que el servidor puede tanto consultar datos como ordenar acciones a los agentes. En el servidor funcionan Node-Red y Grafana, brindando una interfaz gráfica que se transmite a través de servidor web.

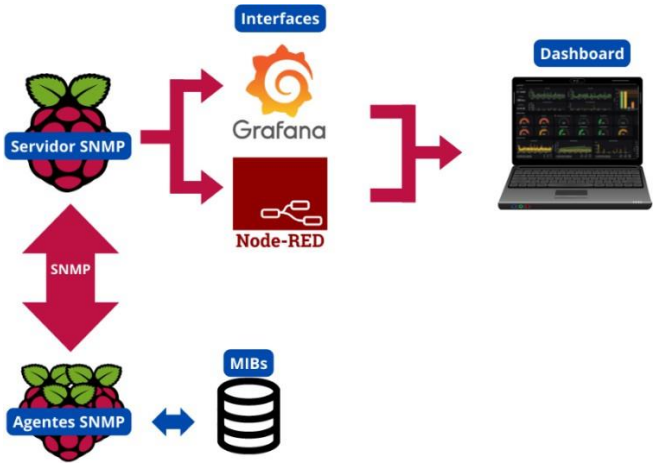


Figura 13: Diagrama de Flujo de la Propuesta (Los autores, 2023)

La comunicación entre Node-RED y Grafana para la generación de las gráficas se da mediante InfluxDB, donde el Servidor envía los datos al instante que son consultados en los Agentes. Al tiempo, Grafana interpreta estos datos en InfluxDB y genera las gráficas de acuerdo al desarrollo elaborado por el autor.

4.2. Instalación de Pandora FMS en el Servidor SNMP

Para la creación del servidor SNMP se creó una máquina virtual con el sistema operativo CentOS de Linux, en la versión gratuita de la plataforma de virtualización llamada Virtualbox. Una vez descargado e instalado, se creó la máquina virtual, para lo que fue necesario descargar la imagen ISO del sistema operativo CentOS 7 en la página web de Pandora FMS.

La creación de la máquina virtual no se dificultó utilizando el asistente de VirtualBox. Lo único que se cambió fue al momento de configurar la personalización del hardware, para otorgar 4 GB de memoria RAM, 2 núcleos de procesamiento y un adaptador de red en puente. Estas características dan funcionalidad a la máquina virtual sin restar en exceso recursos del sistema. Las credenciales para acceder al fichero raíz son *"root"* en usuario y *"Tesis22$"* en contraseña.

Los pasos que se siguió para la instalación de Pandora FMS se describen a detalle en el manual de prácticas al final de este documento.

4.3. Creando un Agente SNMP en Raspberry Pi

Una vez descargado el sistema operativo de la página oficial de Raspberry se procede a quemar la imagen en una memoria micro SD que se insertó en el espacio libre de la tarjeta Raspberry Pi. Luego se procede con la configuración de la red conectando la tarjeta a un monitor y periféricos. En este caso se escoge una IP fija, deshabilitando el protocolo DHCP que asigna la dirección de manera automática.

La IP seleccionada para esta raspberry se verifica con el comando ifconfig, la cual es muy importante dado que es la que funciona como servidor SNMP dentro del proyecto. Adicionalmente se conecta la tarjeta a internet mediante wi-fi y se activa la interfaz VNC para facilitar el acceso desde cualquier computador conectado a la red.

4.4. Habilitación de Servidor SNMP

El protocolo SNMP proporciona una gran cantidad de información de los dispositivos al servidor SNMP. Pero antes este debe estar habilitado en todos los dispositivos que intervienen en este intercambio. Como primer paso del desarrollo del prototipo se habilitó el protocolo SNMP en la Raspberry Servidor.

Este proceso se repitió de igual forma para las Raspberry Agentes. Consiste en líneas de código que actualizan el sistema operativo de Raspberry Pi, instala los servicios del protocolo

y finalmente lo habilita, procedimiento que se describe en la práctica 3. En este punto se considera importante mencionar que las Raspberry Pi como tal no constituyen Servidores o Agentes SNMP, sino dispositivos conectados a la red, que luego de la configuración descrita en este apartado se convierten en Servidores o Agentes SNMP respectivamente.

Es posible comprobar el funcionamiento del protocolo con la línea de código *systemctl status snmpd*, cuya ejecución devuelve el estado del protocolo como activo o deshabilitado. Otro comando útil para la implementación es *systemctl restart snmpd*, que reinicia el servicio cuando el archivo de configuración de SNMP ha sido modificado y se requiere que el servicio reconozca los cambios realizados.

A continuación, en la figura 14 se procede con la instalación de utilidades de Node-RED, InfluxDB y Grafanaen la Raspberry Pi, que se encuentran en los Anexos **¡Error! No se encuentra el origen de la referencia.**, **¡Error! No se encuentra el origen de la referencia.** y **¡Error! No se encuentra el origen de la referencia.** respectivamente. Una vez instalado Node-RED es posible acceder mediante el puerto 1883 en la IP de la Raspberry Servidor, y se continúa conla instalación de las librerías big-timer, node-snmp, influxdb y telegrambot.

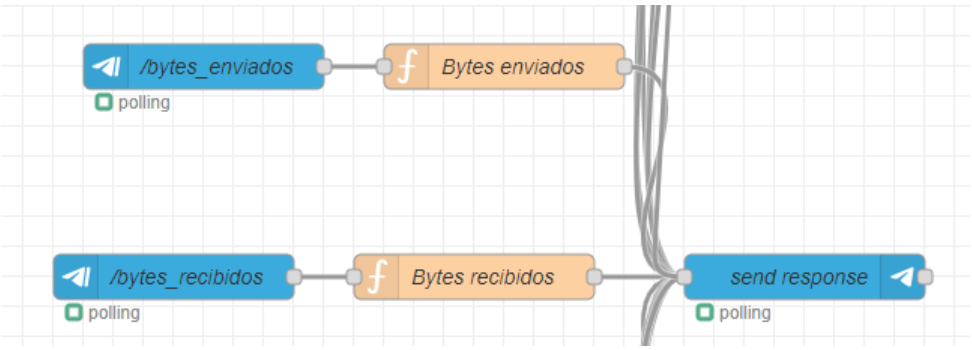


Figura 14: Primer Diagrama de bloques en Node-RED

(Node-RED, 2022)

Las librerías trabajando en conjunto convierten la Raspberry Pi en servidor SNMP. Big-Timer se encarga de repetir minuto a minuto la activación de cada nodo SNMP-get, el cual luego de un arreglo de datos escribe este valor en una dirección específica (OID) en InfluxDB, lo cual crea la MIB de cada uno de los agentes.

Los nodos SNMP-get en este caso funcionan como las variables a consultar de cada dispositivo conectado a la red. Entre estas variables se mencionan velocidad de internet para carga, velocidad de internet para descarga, espacio total de almacenamiento, espacio de almacenamiento utilizado, cantidad de bytes enviados y cantidad de bytes recibidos.

4.5. Asignación de valores en MIBs

Se configura un script en Python para obtener los distintos valores necesarios para la verificación del estado de los agentes y almacenarlos en sus respectivas MIBs. En este caso, editándolas asignando cada dato a una dirección que será llamada desde el servidor SNMP.

4.6. Consulta de OIDs desde Node-Red

En el editor de Node-RED, se genera una consulta de datos desde los agentes SNMP como se muestra en la figura 15, luegoesos valores asignándoles una conversión a la unidad que se desea ser visualizada. Luego ese valor es guardado en un bloque de InfluxDb asignando en que tabla sería guardado parapoder ser visualizado desde Grafana.

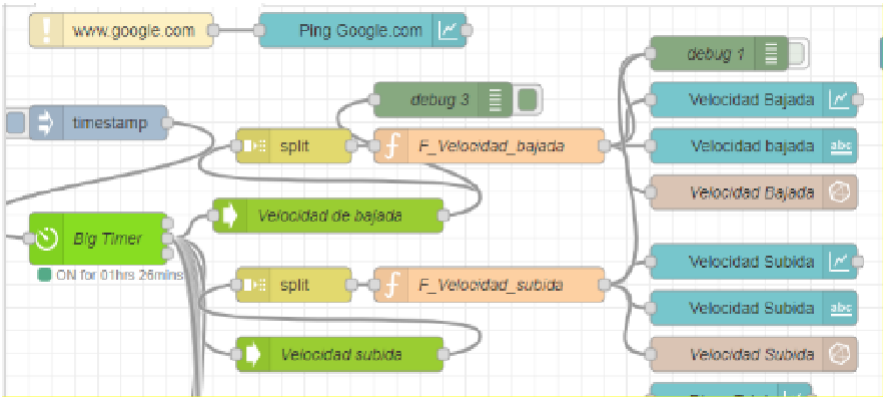


Figura 15: Segundo Diagrama de bloques de manejo SNMP en Node-RED

(Node-RED, 2022)

4.7. Dashboard SNMP en Grafana

Desde ambas arquitecturas se hace una visualización de datos a través de Grafana como se muestra en la figura 16. En Pandora, se configura directamente como un plugin que es llamado por medio deuna conexión http, y se van configurando cada uno de los datos recopilados, mientrasen la arquitectura usada en Node-Red se hace una conexión con influxDb, y así mismo se llama cada uno de los valores para ser visualizados.

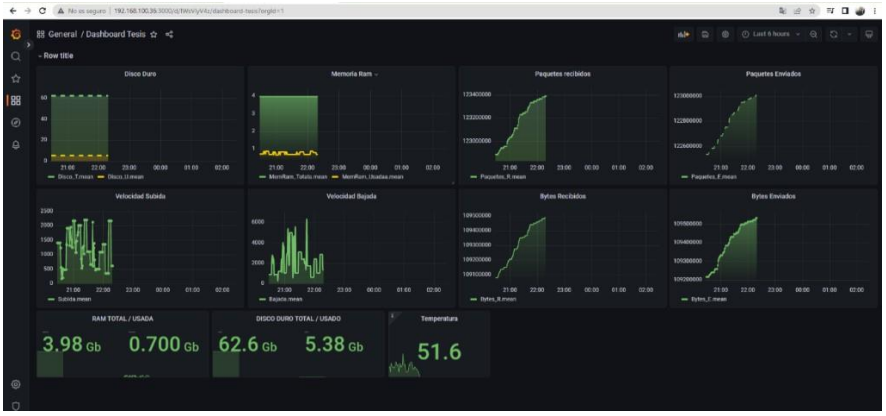


Figura 16: Tercer Diagrama de bloques de manejo SNMP en Node-RED

(Node-RED, 2022)

5. RESULTADOS

5.1. PRÁCTICA I

<table>
<tr><td colspan="3">FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO / TALLERES / CENTROS DE SIMULACIÓN – PARA DOCENTES</td></tr>
<tr><td colspan="2">CARRERA: Ingeniería Electrónica</td><td>ASIGNATURA: Redes de computadoras</td></tr>
<tr><td>NRO. PRÁCTICA:</td><td>1</td><td>TÍTULO PRÁCTICA: Control de dispositivos de Red por medio de Pandora FMS y Grafana</td></tr>
<tr><td colspan="3">OBJETIVO:
• OBJETIVO GENERAL.
Crear una máquina virtual con el sistema operativo CentOS 7 de Linux, que soporte la plataforma de Pandora FMS, configurar a las tarjetas Raspberry Pi que serían usadas como agentes monitoreados, y mostrar datos por plataforma Grafana.
• OBJETIVOS ESPECÍFICOS:
- Conectar la máquina virtual a la red de internet.
- Conectar Pandora FMS con dispositivos que tienen el agente instalado para gestión de red.
- Acceder a la consola virtual de Pandora FMS desde navegador.
- Visualizar variables de agentes en dashboard en plataforma Grafana.</td></tr>
<tr><td colspan="2" rowspan="2">INSTRUCCIONES:</td><td>1. Descargar desde el AVAC procedimientos de la práctica.</td></tr>
<tr><td>2. Responder la tarea a través del AVAC, adjuntando un archivo PDF con capturas paso a paso de lo desarrollado. Cambie el nombre del archivo con sus datos (NOMBRE_APELLIDO.pdf), y adjuntar como respuesta al taller.</td></tr>
<tr><td colspan="3">ACTIVIDADES POR DESARROLLAR</td></tr>
<tr><td colspan="3">1. Descargar la imagen de CentOS 7 compatible, donde se encuentra preinstalado el software de Pandora, desde la página web oficial de Pandora FMS.</td></tr>
</table>

Figura 17 : Logo de sistema operativo Centos

(Centos, 2023)

2. Una vez inicializado el sistema operativo en Virtualbox, se encuentran las siguientes pantallas, dónde se realiza la configuración de entorno de red, dirección de instalación en disco duro, además, como el idioma, la zona horaria y el método de entrada por teclado.

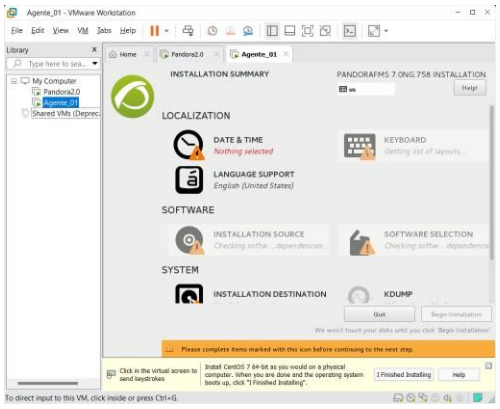


Figura 18: Primeras Pantallas de Wizard de instalación de Pandora.

(Los autores, 2023)

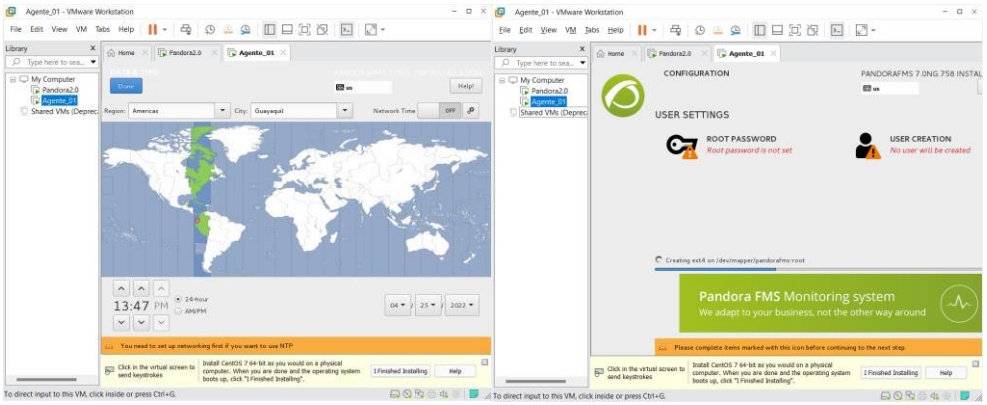


Figura 19: Segundas Pantallas de Wizard de instalación de Pandora .

(Los autores, 2023)

Dando click en *Installation Destination* se elige el dispositivo donde se instala CentOS 7, dado el caso de la máquina virtual que se crea, hay un único dispositivo de almacenamiento. Al dar click en *Done* cambia

a una pantalla donde se selecciona la casilla *click here to create them automatically*, lo que creará puntos de montaje del sistema operativo. En la siguiente pantalla se aceptan los cambios.

Finalmente se configura *Network and Host name* y se enciende la conexión Ethernet para brindar acceso a la red.

3. Se inicia la instalación de Pandora FMS, lo cual tomará algunos minutos. Mientras tanto se puede editar usuarios y contraseñas de acceso al local host. Al terminar se accede con las credenciales elegidas.

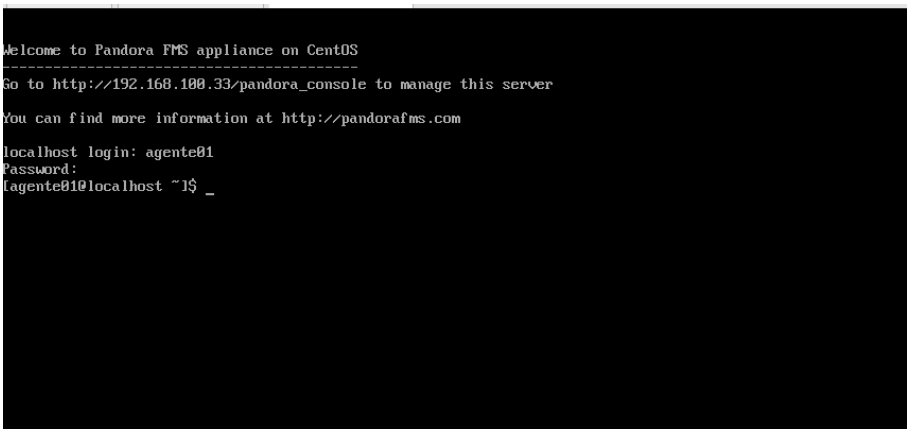


Figura 20: Pantallas de inicialización de comandos en Centos.

(Los autores, 2023)

4. Una vez listo el servidor, en una de las tarjetas Raspberry se instala el servidor de Grafana a través de los siguientes comandos.

Primero se agrega la llave específica para autentificar los paquetes

wget -q -O - https://packages.grafana.com/gpg.key | sudo apt-key add -

Luego se agrega el repositorio APT de Grafana, y se instala por medio de:

apt-get
echo "deb https://packages.grafana.com/oss/deb stable main" | sudo tee -a /etc/apt/sources.list.d/grafana.list
sudo apt-get update
sudo apt-get install -y grafana

Grafana se encuentra instalado, pero hay que inicializarlo, además de la activación cada vez que se reinicie la tarjeta.

sudo /bin/systemctl enable grafana-server

sudo /bin/systemctl start grafana-server

A partir de este momento, se encuentra activo el servido con la dirección http://<ip address>:3000, se puede verificar la IP con el comando *ifconfig*.

5. A continuación, se instala el paquete para convertir la Raspberry en un agente de Pandora, haciendo la descarga desde el siguiente link:

wget https://sourceforge.net/projects/pandora/files/Pandora%20FMS%207.0NG/752/Tarball/pandorafms_agent_unix-7.0NG.752.tar.gz

Se descomprime el archivo con el siguiente comando.

Tar -zxvf pandorafms_agent_unix-7.0NG.752.tar.gz

Luego se inicializa el instalador.

/unix/pandora_agent_installer –install

Generando las carpetas necesarias para el funcionamiento del agente, se edita un archivo para gestionar en qué dirección se encuentra el servidor.

nano /etc/pandora/pandora_agent.conf

Editando la línea server_ip con la dirección del servidor, cómo también remote_config asignándole un valor de 1.

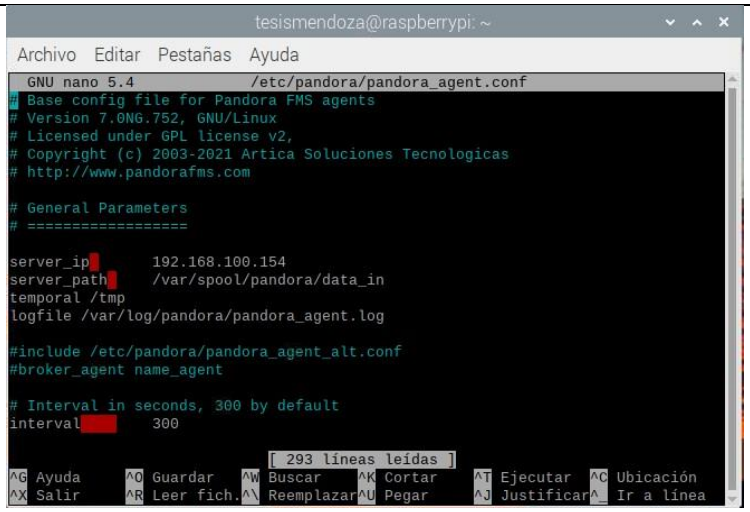


Figura 21: Pantallas de línea de comandos en Raspberry.

(Los autores, 2023)

Se inicializa el agente una vez configurado para que envíe los datos al servidor.

sudo /etc/init.d/pandora_agent_daemon start

A partir de ahí, se configura la tarjeta Raspberry dentro del software Pandora, buscándola en la lista entre los dispositivos conectados.

Figura 22: Pantalla de control en Pandora.

(Los autores, 2023)

Entre los servicios que incluye el monitoreo de la tarjeta, se incluyen algunos que no se encuentran instalados por default, tales como el servidor web, la gestión de bases de datos, entre otros. Por lo cual, para no tener la alerta constante de error, se procede a desactivarlos.

6. Consecuentemente se configuran los servidores de Pandora y Grafana para poder ver los agentesa través del dashboard en Grafana.

Primero, hay que descargar del siguiente link https://pandorafms.com/library/grafana-datasource-extension/ los dos archivos necesarios. En este caso, como cada servidor se encuentra en computadores diferentes, se dispone en cada uno en el correspondiente.

Para habilitar la extensión en Pandora, se sube el archivo “Pandora FMS extension.zip” en el cargador de extensiones en el servidor web.

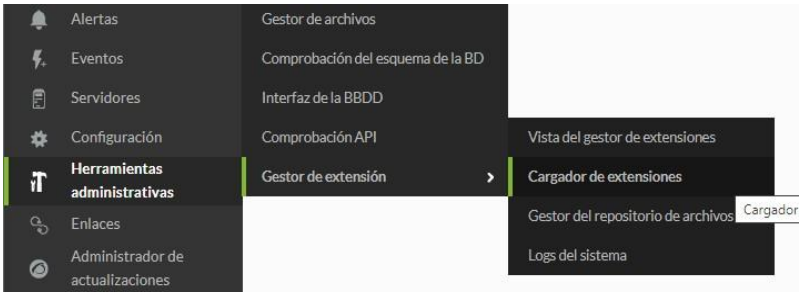


Figura 23: Menú de control en Pandora.(Los autores, 2023)

Se edita el archivo de configuración http con el siguiente código:

nano /etc/httpd/conf/httpd.conf

Donde dice “*AllowOverride none”,* se cambia a “*AllowOverride All*”

```
# Relax access to content within /var/www.
#
<Directory "/var/www">
    #AllowOverride none_
    AllowOverride all
    # Allow open access:
    Require all granted
</Directory>

# Further relax access to the default document root:
<Directory "/var/www/html">
```

Figura 24: Primera Pantalla de configuración PHP en Raspberry.

(Los autores, 2023)

También se edita el configurador de PHP con el siguiente código:

nano /etc/php.ini

Se agrega la línea "*serialize_presicion =-1*" en caso que no se encuentre.

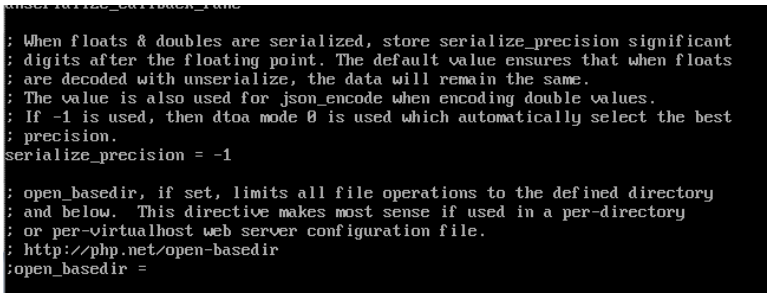


Figura 25: Segunda Pantalla de configuración PHP en Raspberry.

(Los autores, 2023)

Se guarda el archivo, y se reinicia el servicio de Apache.

systemctl restart httpd

Con eso, se encuentra lista la parte de conexión por el lado de Pandora.

En el servidor donde se va a instalar el Grafana, hay que entrar a la capeta de plugins, ubicado en la dirección */var/lib/grafana/plugins*, y se baja el plugin para que haga la conexión con el comando wget.

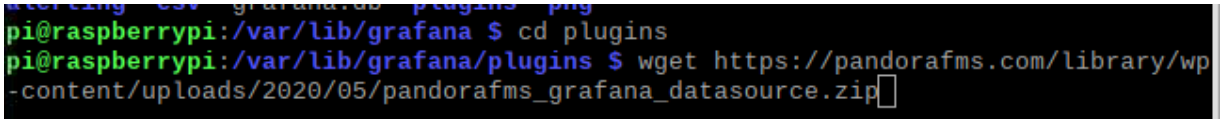


Figura 26: Captura de descarga de archivo de configuración en Raspberry.

(Los autores, 2023)

Luego se descomprime el archivo con el comando unzip, y se reinicia el servicio de grafana.

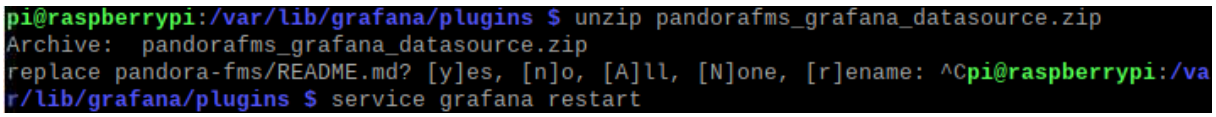


Figura 27: Inicialización de servicio de Pandora en Raspberry.

(Los autores, 2023)

Luego hay que dirigirse a la pestaña de Configuraciones, Data-Sources, y se ponen los datos básicos para conexión con el servidor de Pandora.

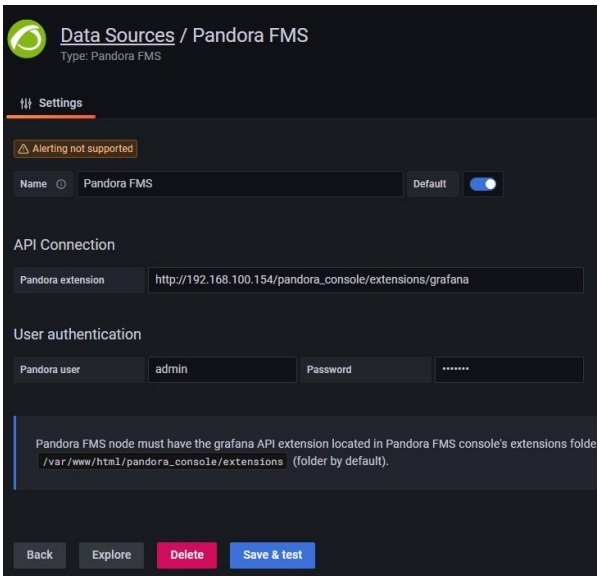


Figura 28: Configuración de conexión de Pandora con Grafana.

(Los autores, 2023)

Por último, se llaman cada una de las variables que se desean revisar, además de su verificación en los tiempos deseados.

Figura 29: Configuración de Dashboard de datos adquiridos desde Pandora en Grafana.

(Los autores, 2023)

RESULTADO(S) OBTENIDO(S): Se comprueba que una máquina virtual con CentOS 7 y los requerimientos básicos soporta la interfaz de Pandora FMS, y es posible acceder a la consola desde un navegador web.
CONCLUSIONES: Los estudiantes estarán en capacidad de crear una máquina virtual con el sistema operativo CentOS 7 de Linux, que soporte la plataforma de Pandora FMS.
RECOMENDACIONES: Asegurarse de otorgar los valores de memoria recomendados para el correcto funcionamiento de la consola.

Docente: _____

Firma: _____

5.2. PRÁCTICA II

<table>
<tr><td colspan="3">FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO / TALLERES / CENTROS DE SIMULACIÓN – PARA DOCENTES</td></tr>
<tr><td colspan="2">CARRERA: Ingeniería Electrónica</td><td>ASIGNATURA: Redes de computadoras</td></tr>
<tr><td>NRO. PRÁCTICA:</td><td>2</td><td>TÍTULO PRÁCTICA: Habilitación de alertas en agentes de Pandora y envío de alertas a través de Telegram.</td></tr>
<tr><td colspan="3">OBJETIVO:
• OBJETIVO GENERAL.
Crear alertas personalizadas en los agentes monitoreados, y gestionar alertas si existen valores fuera de parámetros establecidos.
• OBJETIVOS ESPECÍFICOS:
- Crear bot en Telegram para poder tener comunicación con el servidor.
- Instalar plugin de Telegram en Pandora.
- Configurar alertas con parámetros establecidos para al momento de salir de rango, hacer envío de mensaje a través de Telegram.</td></tr>
<tr><td colspan="2" rowspan="2">INSTRUCCIONES:</td><td>1. Descargar desde el AVAC procedimientos de la práctica.</td></tr>
<tr><td>2. Responder la tarea a través del AVAC, adjuntando unarchivo PDF con capturas paso a paso de lo desarrollado. Cambie el nombre del archivo con sus datos (NOMBRE_APELLIDO.pdf), y adjuntar como respuesta al taller.</td></tr>
<tr><td colspan="3">ACTIVIDADES POR DESARROLLAR</td></tr>
<tr><td colspan="3">1. Se configura un nuevo bot a través del BotFather en la cuenta de Telegram del usuario que requiera tener los datos de los equipos, además se copia el token del bot que será usado para su conexión,
 
</td></tr>
</table>

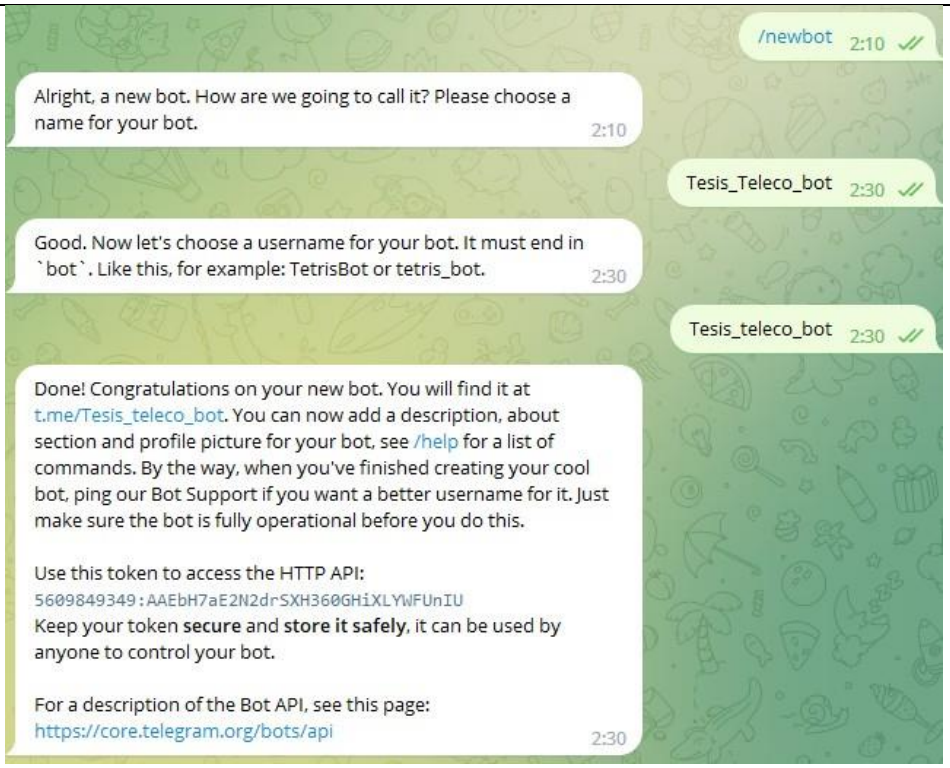


Figura 30: Configuración de BotFather en Telegram.

(Los autores, 2023)

2. Determinar el número identificador del usuario, que sería donde el bot envíe el mensaje. Escribiendo en el buscador de usuarios @getmyidbot, y escribiéndole “/start” responderá con el identificador del chat.

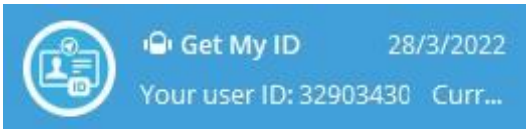


Figura 31: Usuario robot que envía mensaje de identificación.

(Los autores, 2023)

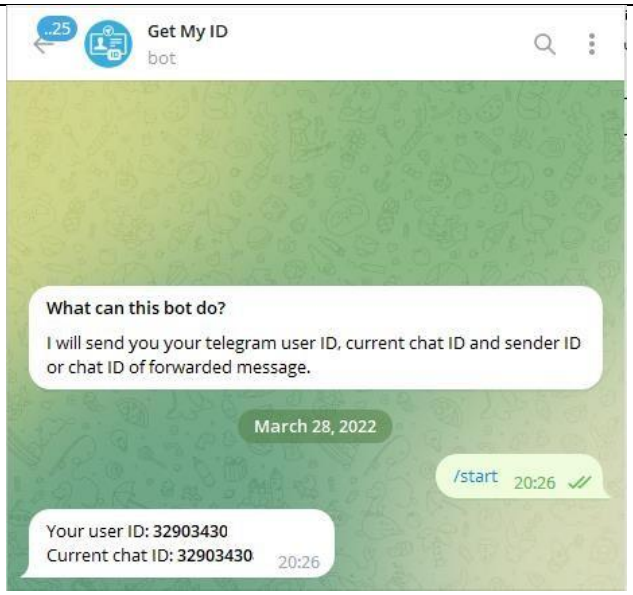


Figura 32: Adquisición de ID por medio de robot en Telegram.

(Los autores, 2023)

3. Se instala Python, y PIP por medio de Yum que gestionará el programa del bot que va a ser descargado.

```
[root@localhost ~]# yum install --nogpgcheck python3-pip
[root@localhost ~]# yum install --nogpgcheck python3_
```

Figura 33: Instalación de Python en Centos.

(Los autores, 2023)

4. De la siguiente página https://pandorafms.com/library/telegram-bot-cli/ se descarga el archive zip, y se descomprime en la carpeta /usr/share/pandora_server/util/pandora donde quedarán dos archivos.

```
[root@localhost util]# pip3 install -r requirements.txt
```

Figura 34: Instalación de parámetros necesarios para uso de comunicación de Pandora por Telegram.

(Los autores, 2023)

5. Para verificar que se encuentre todo instalado se corre el programa en Python con el sigueinte código, junto co el Token, el Id de usuario y un mensaje.

python pandora-telegram-cli.py -t <bot_token> -c <chat_id> -m "Prueba de Telegram"

6. En la pestaña de “Alerta”, se escoge “Comandos” y se hace click en “Crear”, dónde se agregarán los parámetros para los mensajes.

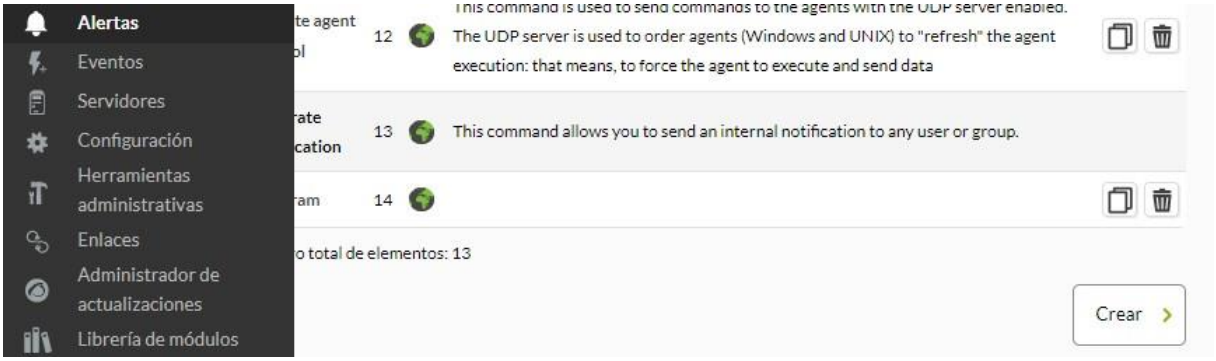


Figura 35: Configuración de comandos en Pandora para comunicación con Telegram

(Los autores, 2023)

7. Se agregan los parámetros en el comando, como también en los campos del Token, Id y mensaje.

python3 /usr/share/pandora_server/util/pandora_telegram_cli.py -t _field1_ -c _field2_ -m "_field3_"

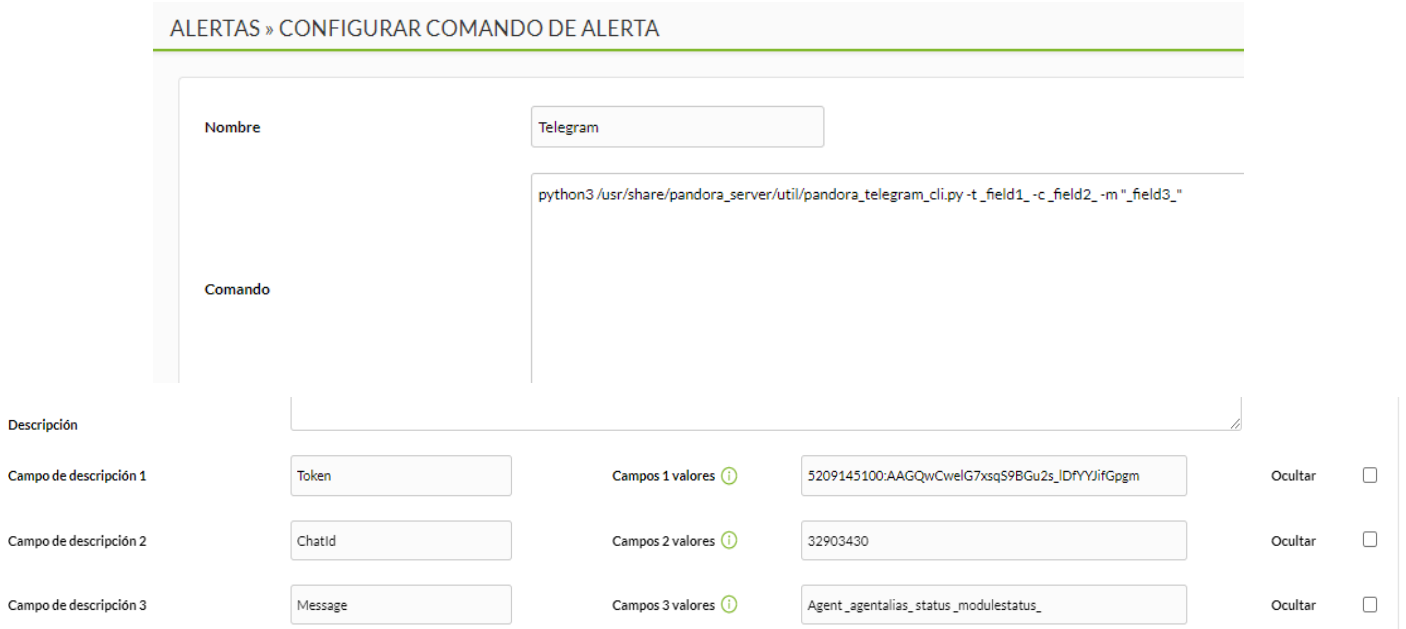


Figura 36: Parámetros para comunicación de Pandora con Telegram.

(Los autores, 2023)

8. Luego se configura en “Alertas” las “Acciones”, donde se crea una nueva, referente al parámetro del agente.

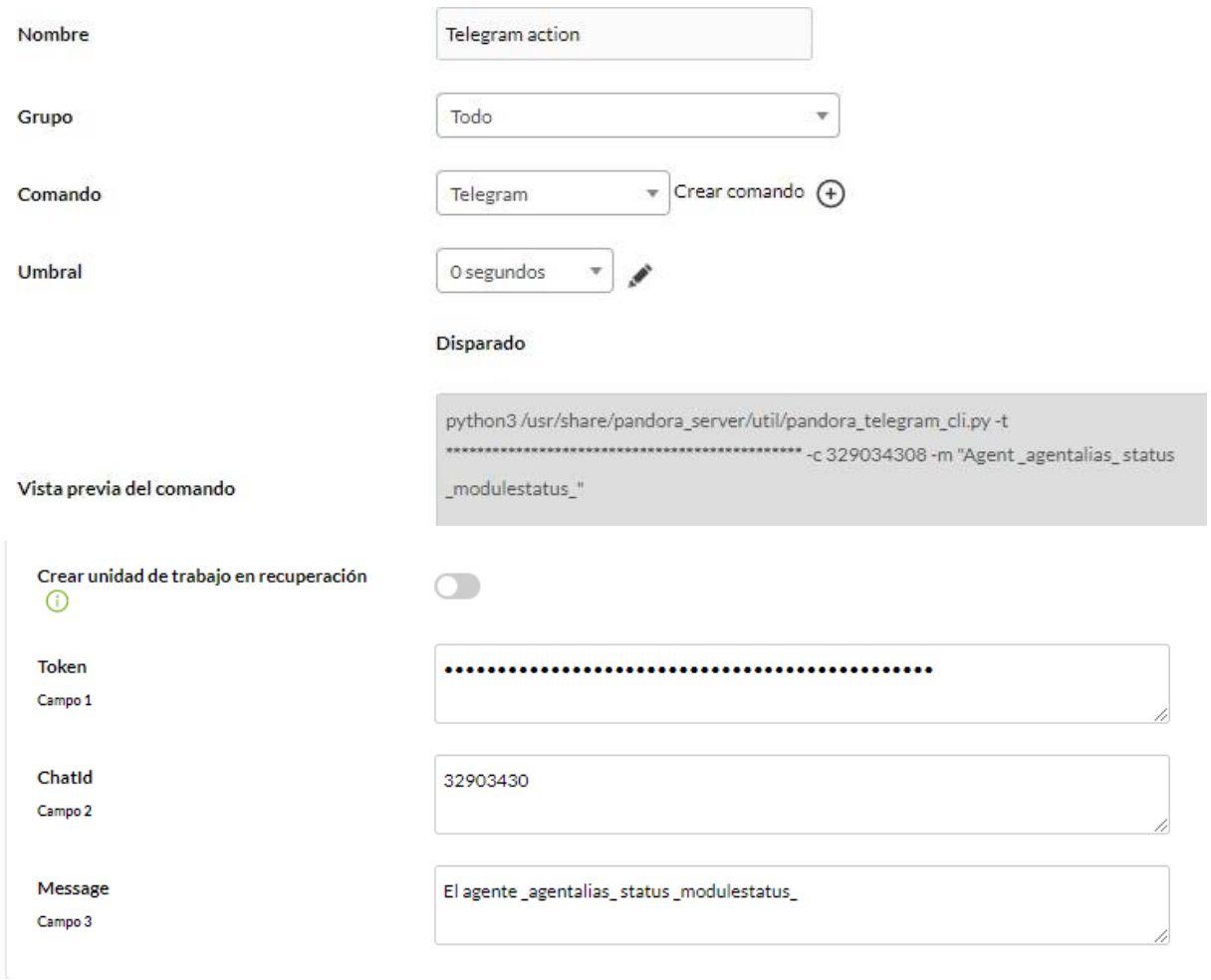


Figura 37: Configuración de parámetros para comunicación de Pandora con Telegram.

(Los autores, 2023)

9. Se crea la la alerta, agregando los parámetros previamente configurados y gestionando el valor y equipo a monitorear.

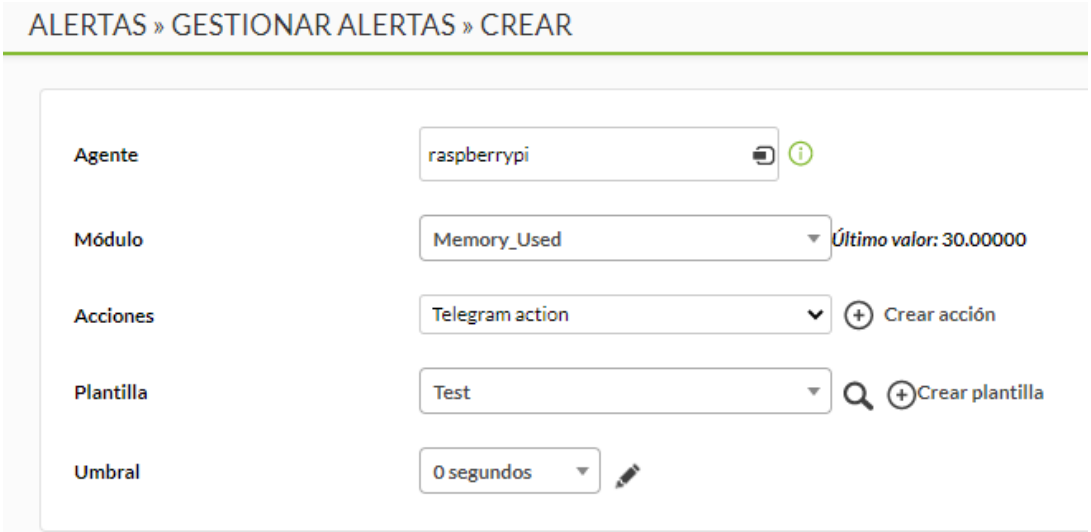


Figura 38: Creación de alerta para comunicación de Pandora con Telegram.

(Los autores, 2023)

10. Por último, se configura la plantilla de alerta, y que se dispare cuando pasa el valor mínimo del 50% de memoria usada del equipo.

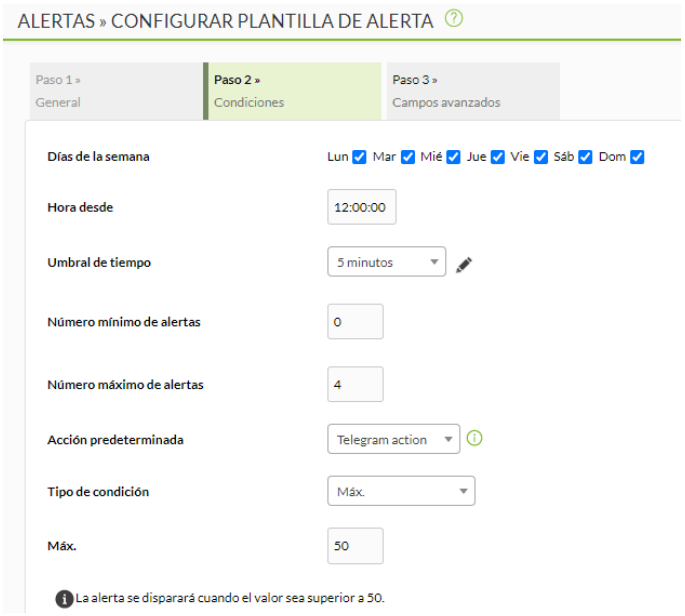


Figura 39: Configuración de plantillas de alerta.

(Los autores, 2023)

11. Se verifica que la alerta se encuentra activa al forzar una activación y que llegue al usuario el estado de funcionamiento.

Figura 40: Mensaje de llagada desde Pandora en Telegram.

(Los autores, 2023)

CONCLUSIONES:

Los estudiantes podrán tener un control del funcionamiento de los equipos remotamente, dónde según el tipo de alerta que se gestione podrán mantener los equipos en parámetros recomendados.

RECOMENDACIONES:

Asegurarse que, al momento de guardar el programa, revisar todos los caracteres se encuentren escritos tal como en el servidor, y hacer pruebas en cada una de las etapas.

Docente: _____

Firma: _____

5.3. PRÁCTICA III

<table>
<tr><td colspan="2">FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO / TALLERES / CENTROS DE SIMULACIÓN – PARA DOCENTES</td></tr>
<tr><td>CARRERA: Ingeniería Electrónica</td><td>ASIGNATURA: Redes de computadoras</td></tr>
<tr><td>NRO. PRÁCTICA: 3</td><td>TÍTULO PRÁCTICA: Configuración y visualización de datos de equipos conectados por medio del protocolo SNMP en Grafana adquiridos desde el servidor Node-Red.</td></tr>
<tr><td colspan="2">OBJETIVO:
• OBJETIVO GENERAL.
Configurar y visualizar los datos de equipos conectados por el protocolo SNMP en Grafana que fueron adquiridos desde el servidor Node-Red.
• OBJETIVOS ESPECÍFICOS:
- Habilitar el protocolo SNMP en un dispositivo Raspberry con Raspbian OS.
- Vincular la Raspberry como agente SNMP a través del script de adquisición de datos.
- Adquirir datos en cada Raspberry por medio de un script en Python y enviarlo al servidor en Node-Red a través de SNMP.
- Conexión de Node-Red con InfluxDB
- Crear base de datos según cada equipo y parámetro en InfluxDB.
- Configuración y conexión de Grafana con InfluxDB.
- Elaboración de Dashboard en Grafana con los datos SNMP del servidor.</td></tr>
<tr><td rowspan="2">INSTRUCCIONES:</td><td>1. Descargar desde el AVAC procedimientos de la práctica.</td></tr>
<tr><td>2. Responder la tarea a través del AVAC, adjuntando un archivo PDF con capturas paso a paso de lo desarrollado. Cambie el nombre del archivo con sus datos</td></tr>
</table>

	(NOMBRE_APELLIDO.pdf), y adjuntar como respuesta al taller.

ACTIVIDADES POR DESARROLLAR

1. Consultar la IP de la Raspberry abriendo una ventana de comando y escribiendo ifconfig.

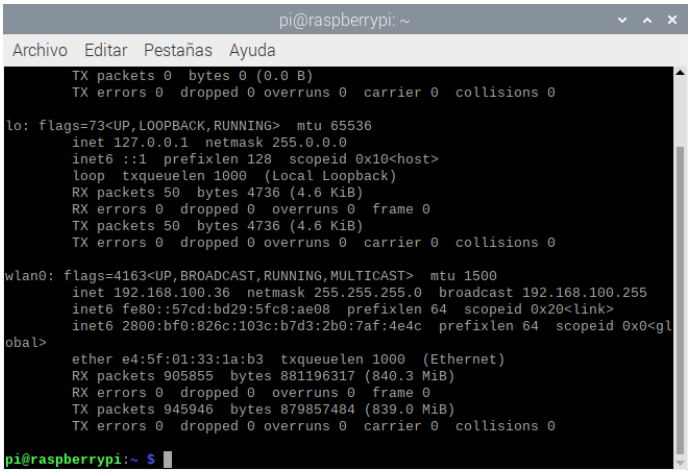


Figura 41: Pantallas de comandos en Raspberry.

(Los autores, 2023)

2. Con la información de la IP del dispositivo se accede a la Raspberry desde una computadora utilizando el software VNCViewer. Las credenciales por defecto del sistema operativo son usuario: pi y contraseña: raspberry.

3. En una terminal de comandos de Raspberry se ejecutan los siguientes códigos:

sudo apt-get update

sudo apt-getinstall snmpd

sudo apt-get install snmp

4. Una vez actualizada se ingresa la siguiente línea de comando para descargar e instalar Node-RED en la Raspberry Pi.

bash <(curl -sL https://raw.githubusercontent.com/node-red/linux-installers/master/deb/update-nodejs-and-nodered)

5. Para iniciar el servicio de Node-RED se ejecuta la siguiente línea de código.

node-red

Aunque es más recomendable habilitar la utilidad para que arranque al iniciar el sistema operativo. Esto se hace con la siguiente línea de código.

sudo systemctl enable nodered.service

6. Lo siguiente es abrir una ventana de navegador e ingresar a la IP de localhost desde el puerto 1880. A pesar que es posible ingresar en la misma Raspberry, es recomendable hacerlo desde una computadora, ya que la aplicación consume un gran volumen de memoria. La pantalla que se observa es la interfaz de desarrollo de diagramas de flujo de Node-RED.
7. Se crea un OID de ejemplo y se lo envía a la carpeta donde el protocolo snmp adquiere sus datos, luego este se actualiza mediante un script de Python con las variables deseadas a controlar, como lo son:

El archivo *scriptdatos.py* por medio de una acción repetitiva configurada por cron, actualiza cada minuto el OID llamado *exampleScript.sh* que se encuentra en la carpeta */etc/snmp/*

```
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
#*/1 * * * * python3 /home/pi/Desktop/script_datos.py >> /home/pi/Desktop/aaaba.txt
tesismendoza@raspberrypi:~ $
```

Figura 42: Configuración de CRON en Raspberry del script en Python.

(Los autores, 2023)

Tamaño y uso actual del disco, velocidad del internet actual, Memoria RAM usada , tiempo de encendido de la computadora, entre otros que pueden ser necesarios para tener un control activo del sistema. Con Python se hace un script que obtiene valores de trabajo actuales de la computadora, a través de la librería “psutil” , luego de hacer la adquisición, se maneja la trama dividiéndola en cada variable según la etiqueta que la representa.

8. Instalación de la base de datos de influxdb.

sudo apt install influxdb

9. Se Inicializa el servicio en el puerto 8086.

influx -precision rfc3339

10. S e Crea una nueva base de datos y llamada SNMP

create database SNMP

Se puede visualizar la base de datos disponibles con el código

Show databases

11. Luego en el sistema de node-red se instala la librería de la base de datos Influx Db, dónde se pueden adquirir, cómo también escribir nueva información en la base de datos desde la interfaz de bloques.

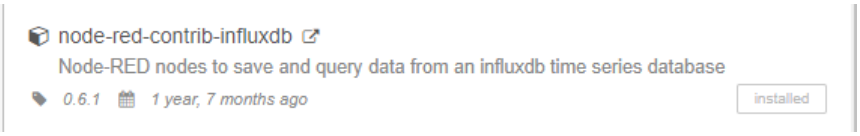


Figura 43: Instalación de librería de InfluxDb en Node-Red.

(Los autores, 2023)

En la configuración principal de la base de datos se apunta al servidor que en este caso es local, con el nombre de la base de datos a tratar.

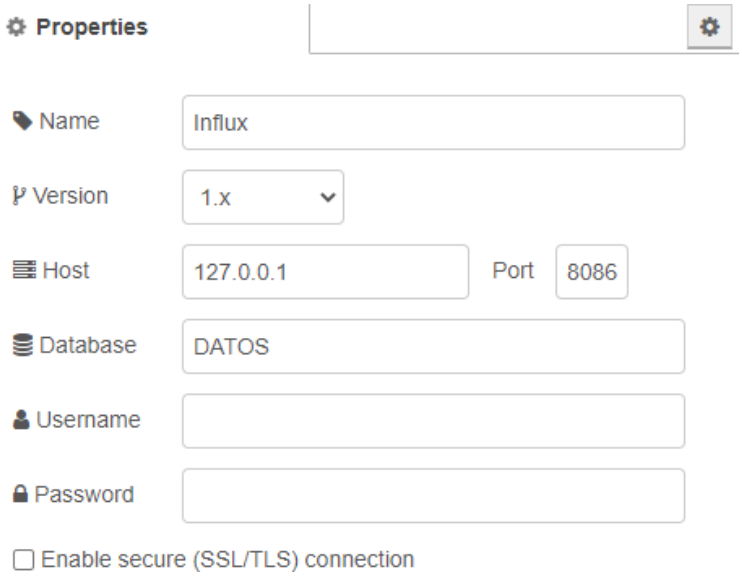


Figura 44: Configuración de parámetros de InfluxDb en Node-Red.

(Los autores, 2023)

12. Cada dato se escribe directamente en el bloque, escribiendo la tabla donde será guardado.

Figura 45: Bloque de InfluxDb para guardado de datos.

Fuente: (Los autores, 2023)

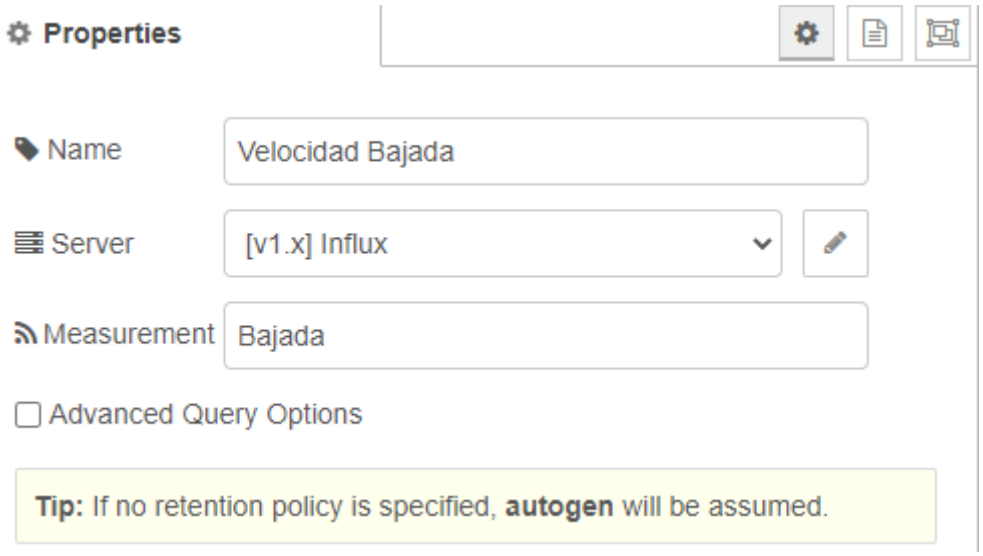


Figura 46: Configuración de bloque de entrada de InlfuxDb en Node-Red

(Los autores, 2023)

13. Instalar Grafana para poder actualizar los valores recibidos desde el script de Node-RED.

wget -q -O - https://packages.grafana.com/gpg.key | sudo apt-key add - echo "deb https://packages.grafana.com/oss/deb stable main" | sudo tee -a /etc/apt/sources.list.d/grafana.list sudo apt-get update sudo apt-get install -y grafana

El Puerto por defecto es 3000.
sudo service grafana-server start

14. En este caso, para fines prácticos el usuario es “admin” y la contraseña Clave123456, se puede poner otras credenciales para aumentar el nivel de seguridad

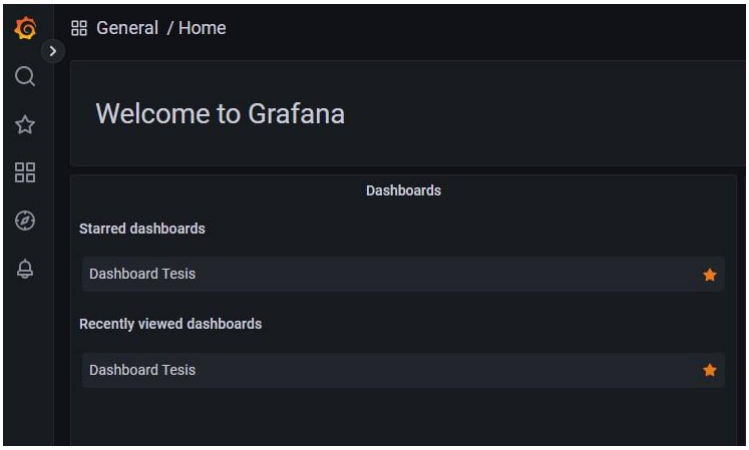


Figura 47: Pantalla inicial en Grafana.

(Los autores, 2023)

Se busca la opción Datasources que es el entorno de configuración para encontrar los diferentes medios de donde se pueden obtener datos. En este caso se escoge la opción de InfluxDb.

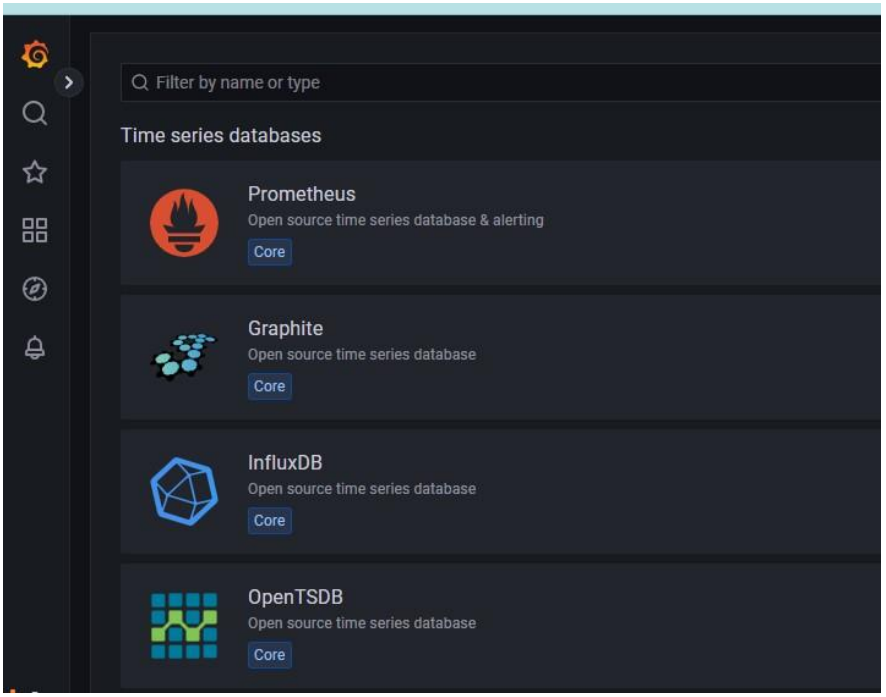


Figura 48: Selección de sistema de base de datos para adquisición de datos.

(Los autores, 2023)

15. Entre las opciones se escoge la dirección del servidor, en este caso local host con el puerto por defecto, y en las opciones de Databases, el nombre de la base que fue creada y dónde se han guardado los datos que genera el sistema.

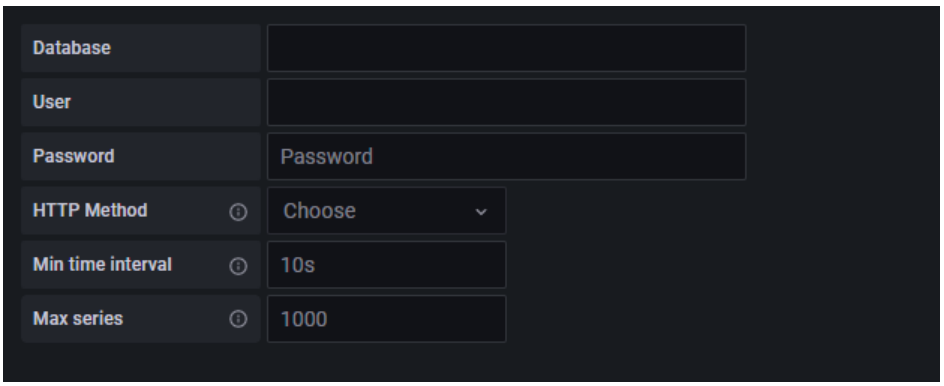


Figura 49: Configuración de parámetros de bases de datos InfluxDb.

(Los autores, 2023)

Una vez teniendo configurada la adquisición de datos se dirige a la pantalla del dashboard y se agrega un nuevo panel

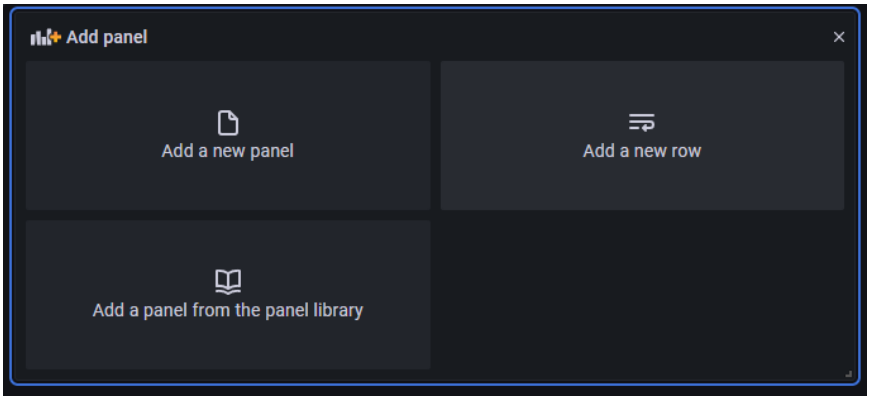


Figura 50: Configuración de panel en Grafana.

(Los autores, 2023)

Donde se escoge el Data Source como también que tabla se quiere agregar, adicional en este caso otro valor adicional para determinar el tamaño completo, y el uso actual del disco duro.

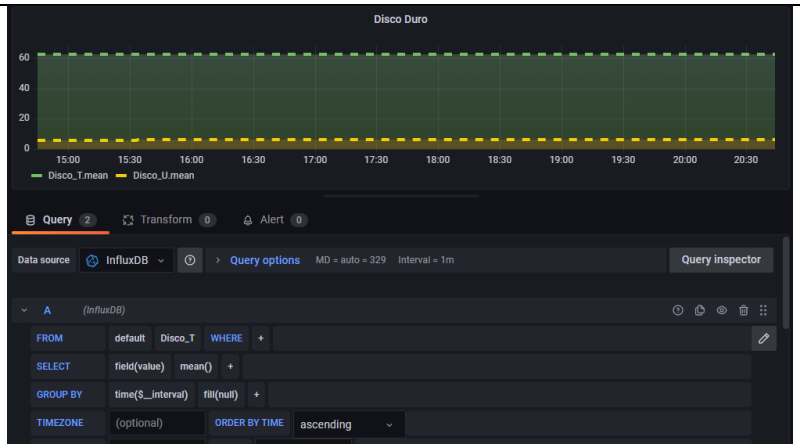


Figura 51:Configuración de adquisición de datos en Grafana.

(Los autores, 2023)

Se pueden agregar todos los datos que han sido grabados a través de las distintas prácticas, o cambiando el script de adquisición, obtener valores adicionales

RESULTADO(S) OBTENIDO(S):

Se comprueba el funcionamiento de Grafana en Node-RED

CONCLUSIONES:

Los estudiantes estarán en capacidad de hacer la generación de actualización de datos para poder ser transmitidos a un servidor SNMP, como también de crear bases de datos en influxdb y vincularlas con Node-RED.

RECOMENDACIONES:

Verificar la correcta utilización de operadores, variables y expresiones, del lenguaje utilizado, para poder llevar a cabo la implementación.

Docente: _____

Firma: _____

5.4. PRÁCTICA IV

FORMATO DE GUÍA DE PRÁCTICA DE LABORATORIO / TALLERES / CENTROS DE SIMULACIÓN – PARA DOCENTES		
CARRERA: Ingeniería Electrónica		**ASIGNATURA: Redes de computadoras**
NRO. PRÁCTICA:	4	**TÍTULO PRÁCTICA:** Verificación de datos de equipos a través de Telegram desde Node-Red

OBJETIVO:

- **OBJETIVO GENERAL.**

Poder visualizar los datos adquiridos en SNMP desde plataforma de mensajería en Telegram para toma de decisiones.

- **OBJETIVOS ESPECÍFICOS:**

- Configurar Bot en Telegram para tener conexión por medio de Webhook
- Instalar y configurar librería de Telegram en Node-Red.
- Tratar los datos y enviarlos al usuario por cada comando de solicitud.

INSTRUCCIONES:	1. Descargar desde el AVAC procedimientos de la práctica.
	2. Responder la tarea a través del AVAC, adjuntando un archivo PDF con capturas paso a paso de lo desarrollado. Cambie el nombre del archivo con sus datos (NOMBRE_APELLIDO.pdf), y adjuntar como respuesta al taller.

ACTIVIDADES POR DESARROLLAR

1. Se configura un nuevo bot a través del BotFather en la cuenta de Telegram del usuario que requiera tener los datos de los equipos.

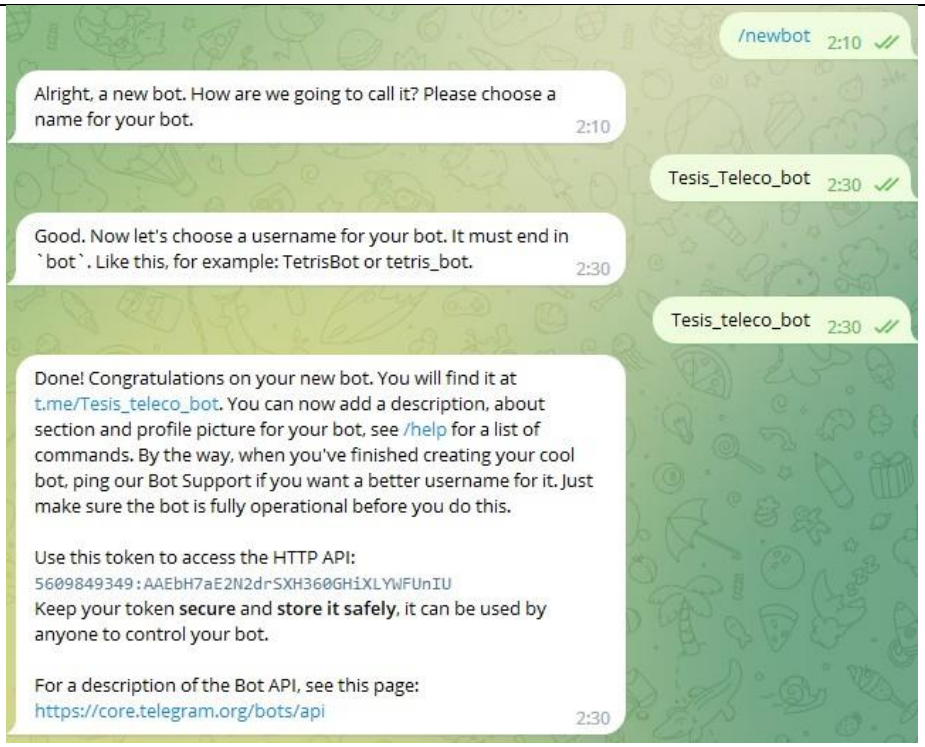


Figura 52: Configuración de Bot en Telegram.

(Los autores, 2023)

2. Se instala la librería de Telegram en el servidor de Node-red, buscando en la paleta de librerías llamada “node-red-contri-telegrambot”

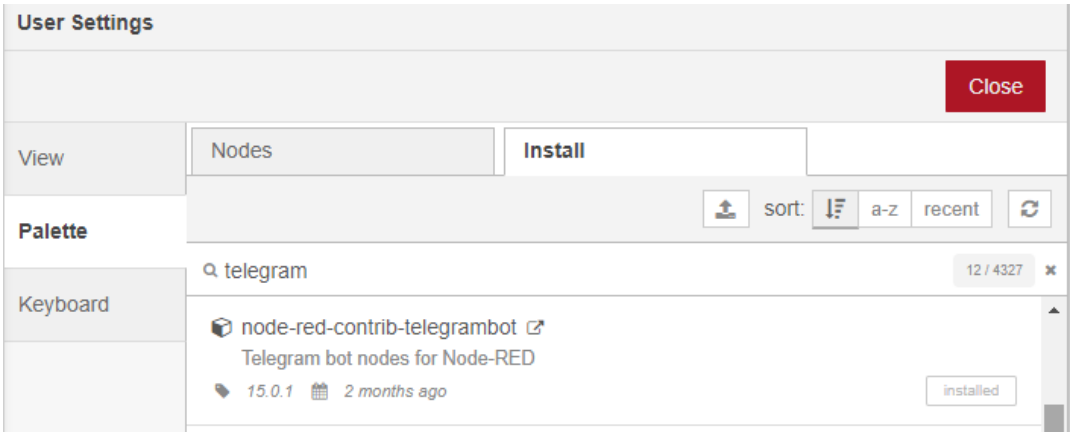


Figura 53: Instalación de Telegram en Node-Red.

(Los autores, 2023)

Luego de eso, se configura el bot en el panel de propiedades de la librería, asignando el Token que se había obtenido desde el BotFather.

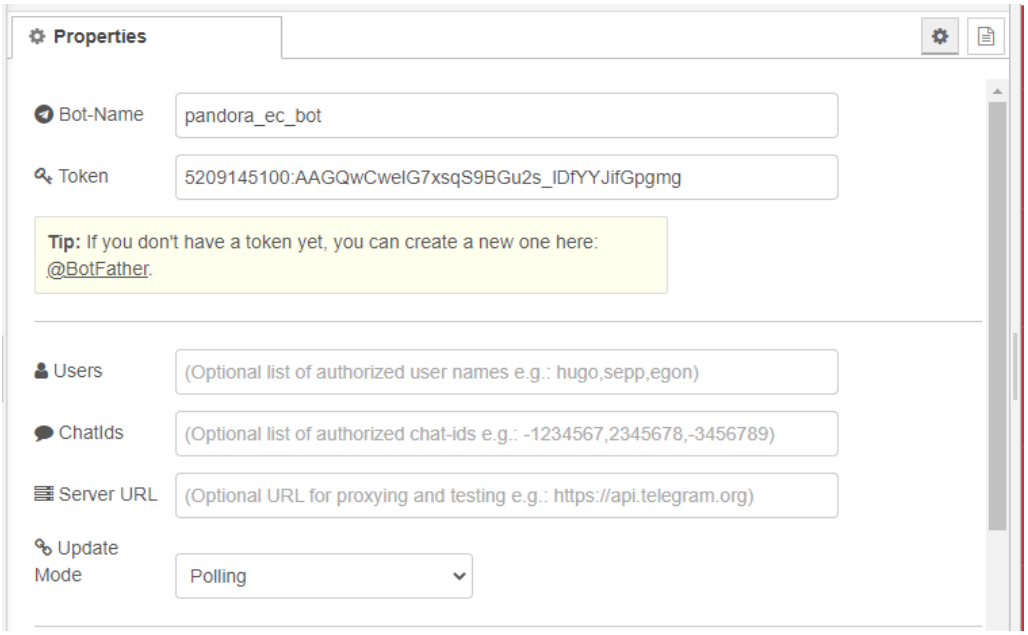


Figura 54: Pantalla de configuración en Bot de Telegram en Node-Red.

(Los autores, 2023)

3. Se asignan los comandos para que cada uno de ellos tenga una acción al ser enviados al bot de Telegram.

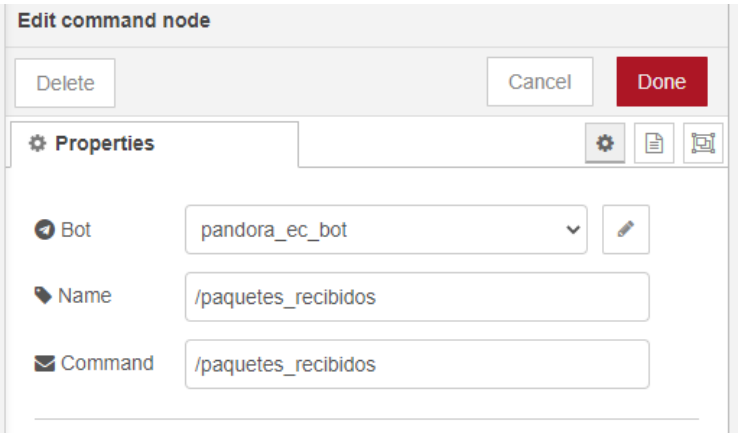


Figura 55: Configuración de comandos de Telegram en Node-Red.

(Los autores, 2023)

Luego del bloque de comando, se asigna nodo de función, para poder tratar los valores que han llegado desde SNMP, y sean enviados con los valores correctos.

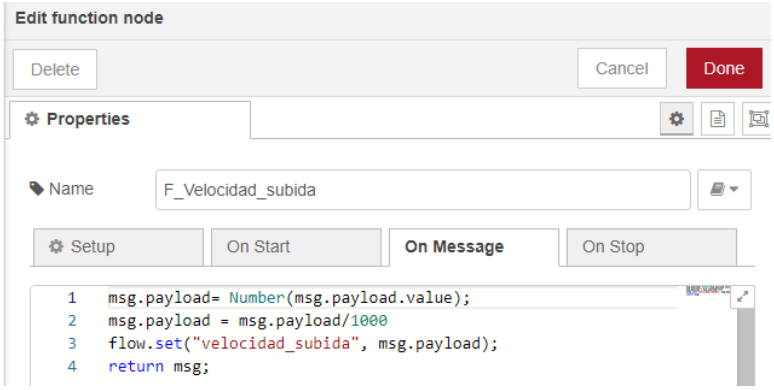


Figura 56: Configuración de conversión de datos para ser adquiridos en InfluxDb.

(Los autores, 2023)

4. Para la respuesta, se asigna el “Set Response” conectado al dato tratado para que sea reenviado al mismo número que hizo el pedido de información.

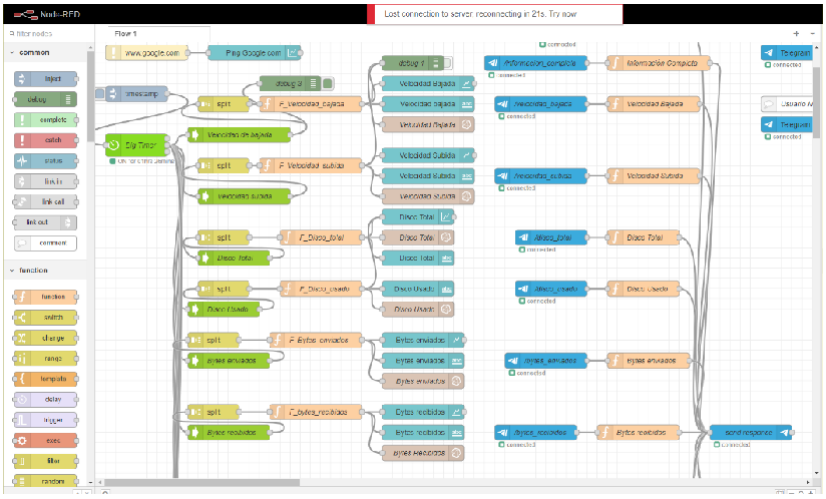


Figura 57: Nodos de adquisición de datos y envío por Telegram en Node-Red.

(Los autores, 2023)

5. Recordar que también un aspecto importante para el control de equipos, es la seguridad. Queda a discreción del usuario tomar las medidas necesarias para el acceso y control de todas las instancias con las que se va a trabajar. Por ejemplo, en el Telegram, se pueden asignar usuarios, o números identificadores a los cuales se les permite que envíen clos comandos.

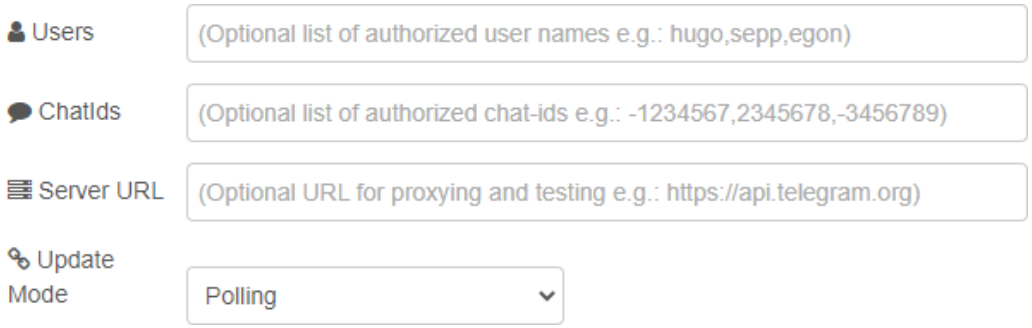


Figura 58: Configuración principal de Telegram en Node-Red .
(Los autores, 2023)

6. Por último, se verifica que los datos sean llamados correctamente desde la aplicación de Telegram, y se da por finalizada la práctica.

Figura 59: Recepción de mensajes en Telegram desde Node-Red.

(Los autores, 2023)

RESULTADO(S) OBTENIDO(S): Se comprueba el envío de datos por medio de Telegram desde el servidor de Node-Red
CONCLUSIONES: Los estudiantes estarán en capacidad de tener una comunicación a través de IoT con Node-red, pudiendo revisar el estado de los agentes desde cualquier parte del mundo.
RECOMENDACIONES: Tomar en cuenta los aspectos de seguridad de exponer servicios o equipos al internet, ya que algún usuario que no tenga buenas intenciones, puede afectar el funcionamiento correcto de estos.

Docente: _____

Firma: _____

CONCLUSIONES

1. Se logra implementar un banco de pruebas para pruebas en laboratorio orientadas al control y monitoreo de red utilizando el protocolo SNMP y Node-RED, entendiendo además el funcionamiento del protocolo mencionado en la plataforma Pandora FMS.
2. Se consigue elaborar un prototipo con tres dispositivos Raspberry Pi con Sistema Operativo Raspbian, que funcione en los laboratorios de telecomunicaciones de la Universidad Politécnica Salesiana sede Guayaquil.
3. Se crearon cuatro prácticas para el monitoreo de Red mediante protocolo SNMP, con pedagogía adecuada para estudiantes de telecomunicaciones, y llevando orden para lograr objetivos de manera ordenada.
4. Se pudo observar en los dashboard con valores actualizados recurrentemente de los agentes SNMP.

RECOMENDACIONES

1. Se debe tener en cuenta, al hacer las configuraciones iniciales, que se verifique el direccionamiento IP para tener una conexión efectiva entre los equipos en caso de que estén con una configuración predefinida.
2. Se recomienda, al hacer las instalaciones de los diversos programas utilizados, tener en cuenta la versión o fuentes de donde han sido descargados en su caso directamente en su página oficial y verificación en la documentación.
3. Una de las recomendaciones, en caso de hacer las configuraciones en la terminal de la tarjeta Raspberry, es tener en cuenta al hacer las modificaciones, que las mismas sean desde el usuario Root para poder así tener todos los permisos dentro de los directorios raíz del sistema.
4. También, es importante tener las horas de todos los equipos actualizadas para que no haya conflictos en la actualización de datos en tiempo real.

BIBLIOGRAFÍA

Aplyca. (2018). *aplyca.com*. Obtenido de Grafana y Prometheus para monitoreo de contenedores: https://www.aplyca.com/es/blog/grafana-y-prometheus-para-monitoreo-de-contenedores

Dett, B., & Vega, E. (2020). *Aplicación de protocolos SNMP y NETFLOW para operar una LAN de 4 sedes de la empresa DETCOM.* Lima: Universidad Ricardo Palma. Obtenido de http://repositorio.urp.edu.pe/bitstream/handle/URP/3448/T030_06669840_T%20%20%20%20EDWIN%20CESAR%20VEGA%20SANTIAGO.pdf?sequence=1&isAllowed=y

DPSTelecom. (2022). *What does oid network elements*. Obtenido de SNMP OID: Introduction for industry professionals: https://www.dpstele.com/snmp/what-does-oid-network-elements.php

Gutiérrez, J., Gómez, N., & Méndez, J. (2017). *Propuesta de solución para la monitorización de los laboratorios del departamento de computación de la facultad de ciencias y tecnología de la UNAN-León utilizando las herramientas Pandora FMS 6.0 e Integria IMS 5.0.* León: Universidad Nacional Autónoma de Nicaragua. Obtenido de http://riul.unanleon.edu.ni:8080/jspui/bitstream/123456789/6634/1/238135.pdf

Hernández, D. (2015). Implementación de un sistema de monitoreo remoto de una red de impresoras multi-funcionales basado en SNMP y programado con Labview.. 28. *Revista Tecnológica ESPOL - RTE, 28*(4), 78-93. Obtenido de https://www.researchgate.net/publication/322936645_Implementacion_de_un_sistema_de_monitoreo_remoto_de_una_red_de_impresoras_multi-funcionales_basado_en_SNMP_y_programado_con_Labview

Kurose, J., & Ross, K. (2017). *Redes de computadora - Un enfoque descendente* (7ma ed.). Madrid: Pearson Eduacación. Obtenido de https://www.academia.edu/40738627/Redes_de_computadoras_Un_enfoque_descendente_7a_Edici%C3%B3n

López, E. (2021). *Diseño e implemetnación de sistema de inventario y monitorización de red.* Bilbao: Universidad del País Vasco. Obtenido de https://addi.ehu.es/bitstream/handle/10810/53432/TFG_ADDI_Eder_Lopez.pdf?sequence=1&isAllowed=y

Millán, R. (2003). SNMPv3 (Simple Network Management Protocol version 3). (Unirioja, Ed.) *Bit, 139*, 45-48. doi:https://dialnet.unirioja.es/servlet/articulo?codigo=7811210

Node-RED. (2022). *Node-RED* . Obtenido de Node-RED ORG: https://nodered.org/

Node-RED. (2022). *node-red-contrib-influxdb*. Obtenido de Node-RED: https://flows.nodered.org/node/node-red-contrib-influxdb

Node-RED. (2022). *node-red-node-snmp*. Obtenido de Node-RED: https://flows.nodered.org/node/node-red-node-snmp

Oré, Á. (2019). *Implementación de un sistema de monitoreo para asegurar la continuidad de los servicios en un data center utilizando protocolo SNMP.* Lima: Universidad Tecnológica del Perú. Obtenido de https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/2016/Cristian%20Ore_Tesis_Titulo%20Profesional_2019.pdf?sequence=1&isAllowed=y

PandoraFMS. (2021). *Monitorización Remota*. Obtenido de PandoraFMS: https://pandorafms.com/manual/es/documentation/03_monitoring/03_remote_monitoring

Python ORG. (2022). *PyPi*. Obtenido de PSUTIL: https://pypi.org/project/psutil/

Ramírez, E. (2019). *Alternativas de configuración con el uso de los protocolos SYSLOG y SNMP para la gestión de red de redes avanzadas.* Perú: Tingo María. Obtenido de http://repositorio.unas.edu.pe/bitstream/handle/UNAS/1645/RDY_2019.pdf?sequence=1&isAllowed=y

Raspberry Pi. (2022). *Raspberry Pi Foundation*. Obtenido de https://www.raspberrypi.org

Swaroop, C. (2022). *About Python*. Obtenido de Python ORG: https://python.swaroopch.com/about_python.html