# ESCUELA POLITÉCNICA NACIONAL

## FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

## IMPLEMENTACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD Y REDES (NSOC) USANDO HERRAMIENTAS OPEN SOURCE PARA LA INFRAESTRUCTURA INDUSTRIAL DE LA EMPRESA ELÉCTRICA QUITO.

**TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE LA INFORMACIÓN**

**LUIS ALBERTO HERRERA LARA**

**DIRECTOR: ING. XAVIER ALEXANDER CALDERÓN HINOJOSA**

**Quito, marzo 2022**

# AVAL

Certifico que el presente trabajo fue desarrollado por Luis Alberto Herrera Lara, bajo mi supervisión.

**ING. XAVIER ALEXANDER CALDERÓN HINOJOSA**
**DIRECTOR DEL TRABAJO DE TITULACIÓN**

# DECLARACIÓN DE AUTORÍA

Yo, Luis Alberto Herrera Lara, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional, y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración dejo constancia de que la Escuela Politécnica Nacional podrá hacer uso del presente trabajo según los términos estipulados en la Ley, Reglamentos y Normas vigentes.

---

**LUIS ALBERTO HERRERA LARA**

# DEDICATORIA

A mis padres, Anita y Luis por ser mi apoyo.

# AGRADECIMIENTOS

A mi hermano Roberto, por estar siempre presente, por sus consejos y apoyo absoluto.
Al MSc. Xavier Calderón por la acertada dirección en el desarrollo de este trabajo de titulación.

# CONTENIDO

ANEXO A: VISITAS - LEVANTAMIENTO DE INFORMACIÓN

ANEXO B: INVENTARIO DE EQUIPOS A INTEGRAR EN LA SOLUCIÓN NSOC

ANEXO C: DIAGRAMAS DE RED

ANEXO D: DETALLE CONFIGURACIÓN SERVIDORES

ANEXO E: HOJAS DE DATOS - EQUIPOS TERMINALES

# ÍNDICE DE FIGURAS

# ÍNDICE DE CÓDIGOS FUENTE

# RESUMEN

El presente trabajo de titulación se sitúa en el ámbito de servicios de red y resuelve una necesidad inherente de la Empresa Eléctrica Quito E.E.Q. a fin de contar con una solución tecnológica que le permita monitorear y gestionar la infraestructura industrial de redes de datos entre equipos activos incluyendo la seguridad de los mismos.

En este trabajo de titulación se desarrolló un análisis de las características fundamentales de los NOC, SOC, NSOC, las herramientas informáticas utilizadas en su implementación, las normas, estándares Y buenas prácticas de gestión de las redes de datos y seguridad en empresas eléctricas.

Luego de haber realizado un primer estudio sobre la forma de gestión y estándares vigentes en las empresas eléctricas se diseñó una solución para la implementación de un Centro de Operaciones de Seguridad y Redes (NSOC) usando herramientas de código abierto considerando los requerimientos solicitados por el personal técnico de la E.E.Q.

La solución implementada permite efectuar el monitoreo de los equipos activos de red y equipos terminales a través de los protocolos SNMP e ICMP, análisis de registro de eventos a través del protocolo SYSLOG, pruebas de acceso y gestión de vulnerabilidades, generación de reportes y envío de alertas tempranas.

La solución implementada fue desplegada y probada en la infraestructura de la E.E.Q., los resultados de estas pruebas se muestran en el capítulo de fase de pruebas. Finalmente, se anexan las conclusiones derivadas del desarrollo de este trabajo.

***Palabras clave—*** NOC, SOC, NSOC, SYSLOG, Norma, Estándar.

# ABSTRACT

This work focuses on the field of network services to solve an inherent need of the Electricity Company of Quito EEQ, to find a technological solution that allows monitoring the industrial infrastructure of data networks at the level of active equipment and thus, manage its security. This degree work analyzed the main features of the NOC, SOC, NSOC, the computer tools used in their implementation, regulations, standards and good practices for the management of data and security networks in electricity companies.

After having carried out a first study on the management and standards in force in electricity companies, a solution was designed for the implementation of a Network and Security Operations Center- NSOC using open-source tools considering the requirements requested by EEQ's technicians.

The implemented solution allows monitoring of active network equipment and terminal equipment through the SNMP and ICMP protocols, event log analysis through the SYSLOG protocol, access tests and vulnerability management, report generation of early warnings.

The implemented solution was deployed and tested in the infrastructure of E.E.Q., the results of these tests are shown in the testing phase chapter of this study. Finally, the conclusions are attached to the end of this work.

***Keywords—*** NOC, SOC, NSOC, SYSLOG, Regulations, Standards.

# 1. INTRODUCCIÓN

El presente capítulo tiene como objetivo realizar un estudio de las principales funcionalidades de los Centro de Operaciones de Red (NOC), Centro de Operaciones de Seguridad (SOC) y las ventajas de los Centro de Operaciones de Seguridad en Redes (NSOC) frente a los NOC y SOC, las herramientas informáticas utilizadas en su implementación y las normativas, estándares y buenas prácticas de gestión de las redes de datos y seguridad en empresas eléctricas.

## 1.1. OBJETIVOS

### 1.1.1. OBJETIVO GENERAL

- ❒ Implementar un Centro de Operaciones de Seguridad y Redes (NSOC) usando herramientas Open Source para la Infraestructura Industrial de la Empresa Eléctrica Quito E.E.Q.

### 1.1.2. OBJETIVOS ESPECÍFICOS

- ❒ Analizar las características de los conceptos de NOC, SOC, NSOC y las normas: NIST 802-82, ITU-T X.805 y NERC CIP.
- ❒ Diseñar una solución para un Centro de Operaciones de Seguridad y Redes (NSOC) usando herramientas Open Source en función de los requerimientos de la Empresa Eléctrica Quito.
- ❒ Desplegar la solución diseñada en la infraestructura de servidores del Centro de Datos de la E.E.Q..
- ❒ Realizar pruebas de funcionamiento de la solución implementada.

## 1.2. ALCANCE

El desarrollo del presente proyecto de titulación esta divido en cuatro fases: fase teórica, fase de diseño, fase de implementación y fase de pruebas de funcionamiento. Cada una de estas fases define los siguientes alcances:

En la fase teórica se realizará un estudio de las principales funcionalidades de un Centro de Operaciones de Red (NOC), de un Centro de Operaciones de Seguridad (SOC), y de un Centro de Operaciones de Seguridad y Redes (NSOC). Se realizará una comparación a fin de identificar de manera detallada las ventajas de un NSOC versus un NOC o un SOC.

Luego se realizará una revisión introductoria a las principales herramientas utilizadas en las implementaciones de NOC y SOC a fin de establecer sus principales funcionalidades y ventajas. Se realizará también una revisión de los procesos, estándares y buenas prácticas de gestión de las redes y seguridad de redes en empresas eléctricas. Se utilizarán como base las normas NIST 802-82, ITU-T X.805 y NERC CIP.

Esta fase iniciará documentando el estado actual y las limitaciones de gestión de los equipos de redes y de la automatización eléctrica instalados. Se incluirá toda la información referente al impacto de no gestionar adecuadamente la plataforma de datos y su relación directa con los indicadores de gestión de la calidad del suministro eléctrico. Se explicará como el sistema de control y automatización eléctrica depende directamente de las redes de datos y lo importante que es para la E.E.Q. contar con un *CENTRO DE OPERACIONES DE SEGURIDAD Y REDES (*NSOC*)* para la gestión de la Infraestructura Industrial de la Empresa Eléctrica Quito.

Luego se harán visitas en el sitio para elaborar diagramas de conectividad a nivel interno y en la capa de transporte en las subestaciones, centrales de generación, cámaras de soterramiento, acceso a la red de campo en distribución, centro de control y servidores SCADA. Adicionalmente, se consolidará toda la información disponible e histórica de la implementación de equipos y fibra óptica actual. Una vez hechas las visitas en sitio, el siguiente paso será el comprobar el acceso a todo el inventario de equipos levantados mediante accesos usando las credenciales proporcionadas por el personal técnico de la E.E.Q.. En este acceso se documentará la disponibilidad de protocolos de gestión SNMP y de generación de información SYSLOG en todos los equipos activos.

Con la información documentada en los accesos a los equipos se procederá a definir las herramientas a utilizar en concordancia a los requerimientos definidos y a la disponibilidad de protocolos de gestión de los equipos instalados. Se definirán parámetros iniciales de configuración de los protocolos de gestión, versiones de SNMP, habilitación de SYSLOGy reglas de acceso para ICMP. Toda esta información será utilizada para desarrollar los procedimientos de gestión que al momento no se dispone. A continuación, se elaborará el listado de requerimientos, los cuales serán definidos en conjunto con el personal técnico de la E.E.Q.. También se elaborará un procedimiento referencial de evaluación de la seguridad de la red de datos y de equipos terminales en función de los requerimientos técnicos definidos por el personal técnico de la E.E.Q..

De manera conjunta a partir de los requerimientos de criticidad definidos por el personal de la E.E.Q. se establecerán umbrales de alarmas para la generación de alertas tempranas vía correo electrónico. Una vez documentados los requerimientos, equipos y protocolos de gestión y de registro de eventos, se procederá con el dimensionamiento de los servidores de manera que su funcionamiento sea óptimo. Los principales parámetros por dimensionar son: capacidad de almacenamiento, número de núcleos de procesamiento, capacidad de memoria RAM y la conexión a la red de datos de los equipos a gestionar.

Finalmente, se analizarán las mejores alternativas para cumplir con los requisitos definidos por la E.E.Q. desde el punto de vista de la escalabilidad, funcionalidad y eficiencia sobre el manejo de todos los equipos implementados y su facilidad de escalamiento. Las herramientas con las que se contará para la implementación de la solución serán de código abierto y deberán funcionar en ambientes virtualizados a fin de poder garantizar el aspecto de escalabilidad. Todos los aspectos de seguridad sobre la plataforma de datos serán estructurados teniendo en cuenta los equipos de control de acceso de la E.E.Q..

Al final de esta fase se escogerá el sistema operativo y conjunto de herramientas a instalar que cumplan con los requerimientos de la solución tecnológica a implementar, se definirán también las interfaces gráficas a utilizar en función de las herramientas escogidas. En esta etapa se dará forma al concepto NSOC base de este trabajo de titulación, sobre el cual se definirán las capas de fuente de información (routers, switches, firewalls, reconectadores, RTU, IED, medidores, etc.), la capa de gestión de la infraestructura y la información generada por la infraestructura instalada.

En esta fase se instalarán y configurarán de manera virtualizada los servidores definidos en la fase de diseño para los servidores. Sobre este despliegue se procederá con la instalación de las herramientas definidas en la fase de diseño, luego de la instalación se realizará la configuración e integración de todas estas herramientas preparando el entorno para la integración de los equipos definidos en la etapa de diseño. En esta fase de integración usando las herramientas seleccionadas se realizarán los esquemas de red levantados en las visitas en el sitio por cada una de las localizaciones visitadas en la etapa de diseño.

En esta etapa se procederá con la instalación de un primer prototipo con base en la información desarrollada en las fases anteriores, para esto será necesario realizar una reconfiguración global de todos los equipos de redes, switches, routers, firewalls y equipos terminales para la transmisión y recepción de datos SNMP, ICMP, SYSLOG y políticas de seguridad en firewalls hacia la solución prototipo implementada. En esta fase se deberán ajustar todos los aspectos de configuración y rendimiento computacional (niveles de uso de procesadores, almacenamiento, memoria RAM) para que la solución implementada pueda garantizar un rendimiento adecuado a la plataforma a implementar.

La implementación de la solución se basará en herramientas de software ya desarrolladas, las mismas que se configuraran de manera que puedan cumplir los requerimientos de la fase de diseño. Los últimos pasos para realizar serán la configuración de la solución implementada para la generación de alarmas tempranas a cuentas de correo electrónico usando SMTP, definición de umbrales de funcionamiento para la generación de alarmas de alerta temprana en la solución implementada. Con estos parámetros definidos y configurados se desplegarán pruebas de la generación de alarmas de alerta temprana y de la generación de reportes en la solución implementada.

En la fase de pruebas se definirán procesos a seguir para comprobar el correcto funcionamiento de la implementación de la solución diseñada. La fase de pruebas incluirá escenarios controlados de cambios en las métricas de gestión definidas (procesamiento, tráfico, memoria de los equipos, etc.). Dichos escenarios incluirán también fallos controlados sobre la infraestructura para poner a prueba la generación de alarmas en la solución tecnológica desplegada, ataques de red sobre los equipos activos y equipos terminales y finalmente la generación de reportes y emisión de alertas tempranas vía correo electrónico. En caso de ser necesario y con base a los resultados obtenidos en esta fase, se realizarán correcciones menores a la solución implementada con el objetivo de garantizar su correcto funcionamiento.

## 1.3. MARCO TEÓRICO

En la actualidad la Empresa Eléctrica Quito (E.E.Q.) ha desarrollado varios procesos de modernización alineados a los principios de transformación digital industrial[1] necesarios para alcanzar el paradigma de las Redes Eléctricas Inteligentes (Smart Grids[2]).

Entre los primeros pasos de modernización desarrollados por la Empresa Eléctrica Quito estuvo la implementación de un Sistema SCADA (Supervisory Control And Data Acquisition (SCADA)), el cual generó la necesidad del despliegue de redes de datos a lo largo del área de concesión de la Empresa Eléctrica Quito.

El Sistema SCADA desplegado en conjunto a los primeros equipos de automatización

[1] **Transformación Digital Industrial:** Se define como la adopción en las empresas de las Tecnologías de la Información y de las Comunicaciones (TIC) a fin de mejorar su rendimiento y agregarle valor a su giro del negocio[1], [2]. Para el caso de las empresas eléctricas de distribución, la transformación digital industrial está enfocada en la implementación de Sistemas electrónicos de control industrial que permiten monitorear y ejecutar remotamente operaciones de apertura, cierre y transferencia sobre la Red eléctrica.

[2] **Smart Grid:** También conocidas como redes eléctricas inteligentes, se define como la integración completa de la cadena de valor del sector eléctrico partiendo desde la fase de generación, transmisión y distribución hasta llegar al cliente final la cual debe estar controlada por sistemas electrónicos de automatización industrial y monitoreada a travez de las Tecnologías de la Información y de las Comunicaciones[3]

eléctrica conformaron los primeros hitos dentro de la modernización digital necesaria para transformar la red eléctrica tradicional en la red eléctrica inteligente.

La red eléctrica inteligente está conformada por varios sistemas y equipos los cuales estructurados en capas dan como resultado el modelo de arquitectura base mostrado en la Figura 1.1, en donde a nivel tecnológico destacan las capas de comunicaciones e información.

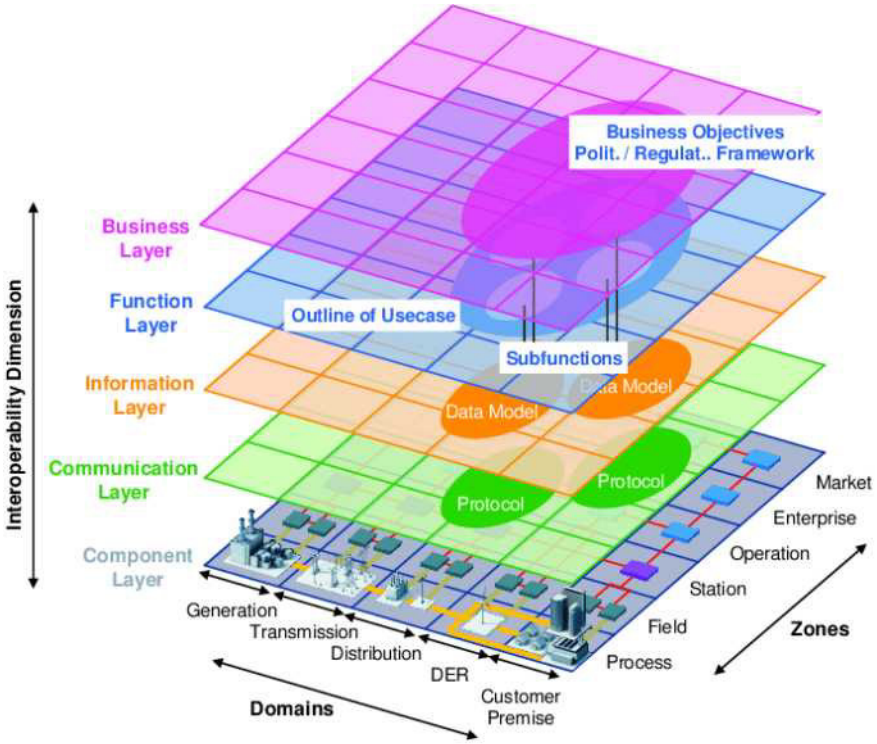



**Figura 1.1:** Arquitectura Modelo de las Redes Eléctricas Inteligentes[4]

Las capas de comunicaciones e información definidas dentro del modelo *Smart Grid Architecture Model (*SGAM*)* de la Figura 1.1 están conformadas por sistemas informáticos de gestión, servidores, equipos de redes de datos y un gran conjunto de equipos electrónicos de automatización eléctrica los cuales funcionan con sistemas operativos de propósito específico (sistemas embebidos). Todos estos equipos deben interconectarse y dependiendo de cuanto se haya avanzado en el despliegue de las redes eléctricas inteligentes, más compleja será la red de datos, servidores y equipos electrónicos de automatización eléctrica.

En la Empresa Eléctrica Quito se disponía de una red de datos para interconectar los servicios y sistemas informáticos necesarios para el funcionamiento y gestión remota de los sistemas de automatización industrial de la red eléctrica. Esta red de datos no estaba siendo gestionada adecuadamente, no se disponía de herramientas que permitan realizar tareas de descubrimiento de dispositivos de red y equipos conectados, monitorización de los equipos conectados, análisis del rendimiento, gestión y notificaciones inteligentes o alertas personalizables sobre fallos de la infraestructura instalada.

El servicio eléctrico (infraestructuras críticas[3]) está catalogado como parte de las infraestructuras críticas para la sociedad, por tal motivo es necesario se incluyan también las tareas de aseguramiento de la red de datos, a fin de mitigar posibles amenazas en la seguridad de la infraestructura tecnológica instalada.

En este trabajo de titulación se propone la implementación de una solución que permita monitorear y gestionar toda la infraestructura tecnológica de redes de datos instalada para el acceso, gestión y funcionamiento de los sistemas electrónicos de automatización de la Red eléctrica.

Al no disponer de una solución para la gestión de la red de datos, la continuidad del servicio de suministro eléctrico para los clientes de la empresa corre el riesgo de verse afectado a causa tiempos de indisponibilidad en la red de datos, y como estos tiempos inciden directamente en el rendimiento de los sistemas electrónicos de automatización.

El no administrar adecuadamente una red de datos compleja, como las implementadas en las empresas eléctricas puede llegar a inutilizar los sistemas de automatización industrial, sistemas de gestión empresarial y demás facilidades tecnológicas de las redes eléctricas inteligentes forzando que en estas situaciones críticas, la gestión de la empresa se ollados con el objetivo de garantizar la continuidad del servicio eléctrico [6], [7]. En lo que respecta a la gestión de los activos tecnológicos, redes de datos, equipos electrónicos de automatización de la red eléctrica se cuentan con los siguientes estándares y normas: North American Electric Reliability Corporation - Critical Infrastructure Protection (NERC-CIP) [8], National Institute of Standards and Technology NIST (NIST) 802-82 *Guide to Industrial Control Systems (ICS) Security* [9], International Telecommunication Union (ITU) X.805 - *Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo* [10].

Adicional a lo indicado, en la E.E.Q. tampoco se han implementado procesos de gestión para ninguno de estos estándares, incurriendo en procedimientos de atención no optimizados, no se cuenta con registros históricos del equipamiento, respaldos de configuración, procesos de aseguramiento de la infraestructura tecnológica, entre otros aspectos que dificultan una respuesta rápida y soluciones precisas en escenarios de fallas de la red de datos.

En lo que respecta al crecimiento de la complejidad de la red eléctrica, el estado actual muestra que la hiperconectividad exigida por la implementación de sistemas como el ADMS (*Advanced Distribution Management System*) o exigentes de los recursos de la red de datos como el CCTV (*Circuito Cerrado de Televisión*) vuelven mucho más importante contar con

[3] **Infraestructuras críticas:** El concepto de infraestructuras críticas está definido como todos aquellos sistemas físicos o virtuales qué son esenciales para apoyar los sistemas más básicos de la sociedad, ciento de estos de tipo social, económicos, medioambiental, o políticos[5].

herramientas para la gestión de la red de datos, mediante los cuales se pueda monitorear el rendimiento y asignación de recursos destinados a estos servicios.

En este contexto en el presente trabajo de titulación se desarrolló e implementó una solución tecnológica integral para la gestión de esta infraestructura a través de un Centro de Operaciones de Seguridad en Redes (NSOC), el cual fue desplegado usando herramientas de código abierto (open source). Esta solución permite la gestión de la red y evaluación de los niveles de seguridad de la infraestructura instalada.

La red de datos de la E.E.Q. y toda la infraestructura tecnológica de los sistemas de automatización industrial de la red eléctrica consta principalmente de los siguientes equipos:

- ❒ **Equipos de redes de datos:** Firewalls, *routers*, *switches*, y puntos de acceso inalámbricos, equipos de sincronización.
- ❒ **Equipos de automatización industrial:** Unidades Remotas de Control (RTU), Equipos Electrónicos Inteligentes (IED), reconectadores, medidores de calidad de energía, sensores de transformadores.
- ❒ **Sistemas y Servidores:** Sistemas SCADA, ADMS y CCTV.

Una de las características diferenciadoras de la infraestructura que monitoreara el sistema desarrollado en este trabajo de titulación es que se trata de equipamiento de tipo industrial, definido de manera global como equipamiento de tecnologías de la operación[4].

Los equipos de naturaleza industrial que forman parte de las tecnologías de la operación de la E.E.Q. tienen un tiempo de vida útil de alrededor de 15 a 20 años, el sistema operativo instalado en estos equipos casi no cuenta con actualizaciones[5], muchos de estos sistemas operativos no cuentan con una interoperabilidad plena entre estándares abiertos[6], y finalmente su monitoreo y gestión remota se ve limitada a un conjunto mínimo de protocolos tales como SNMP, ICMP y SYSLOG, quedando por fuera soluciones avanzadas de gestión de infraestructura. Adicional a los problemas de monitoreo y gestión remota Están los problemas de vulnerabilidad los generados por el funcionamiento propio de los

---

[4] **Tecnologías de la operación:** las tecnologías de la operación están definidas como las componentes de hardware y software que detectan o causan cambios a través del monitor el control remoto en sistemas de automatización industrial. Para el caso de las empresas eléctricas se hace referencia a todos los equipos forman parte de la automatización de las redes eléctricas, esto incluye a los equipos activos de las redes de datos.

[5] Las actualizaciones de sistemas operativos en sistemas industriales, suelen afectar la cadena de producción, por lo que son realizadas en ventanas de mantenimiento previo análisis y aprobaciones que garanticen no afectar la cadena de producción. Para el caso de las empresas eléctricas en donde se intervengan sistemas de automatización industrial se debe garantizar que estas actualizaciones no afecten la integridad de los sistemas implementados, es decir si uno o varios de ellos son actualizados, el funcionamiento del sistema de automatización no debe verse afectado.

[6] En mercado existen equipos que garantizan su pleno funcionamiento siempre y cuando se cuente con todas las herramientas de software propietarios de la marca

sistemas tecnológicos implementados en entornos industriales. La gestión de la seguridad informática y de redes de datos es otra característica implementada en el sistema de este trabajo de titulación.

Los Sistemas de Gestión de Redes (NSM) tienen como finalidad proveer los recursos necesarios para que los administradores de estas infraestructuras puedan garantizar que los parámetros de ancho de banda, tasa de transferencia efectiva (en inglés *throughput*), latencia y *jitter* sean adecuados para que las aplicaciones que hagan uso de dichos recursos funcionen correctamente, adicionalmente permiten visualizar el comportamiento de los equipos que forman parte de la red de datos, identificar comportamiento anormales, probables fallos de hardware o software, configuraciones equivocadas, etcétera.

Al principio, dichos sistemas estuvieron limitados a las consolas de gestión de servidores centrales, las cuales contaban terminales de comando desde donde se podía gestionar los recursos, administrar archivos de configuración y monitorear el rendimiento de los sistemas instalados, no obstante, pese a disponer de dichos sistemas de administración, la interoperabilidad de dichos sistemas era mínima o en algunas ocasiones nula, siendo imposible conseguir que trabajen en grupo y menos todavía poder hacer administración de sistemas complejos de diferentes marcas [11].

El desarrollo de las tecnologías de redes de datos y estándares abiertos permitió que equipos de diferentes marcas logren conectarse entre abriendo el camino para que implementen grandes redes de datos, escenario en el que entra en escena el protocolo de administración Simple Network Management Protocol (SNMP) y las Management Information Base (MIB), lo que disminuyó de manera significativa la dificultad de la incorporación de los equipos a los sistemas de gestión [11].

De manera general se espera que el gestor de red a través de la plataforma de software proporcione las tareas de administración a los agentes en cada uno de los dispositivos gestionados, y los agentes a su vez provean toda la información necesaria para desarrollar las tareas de administración[11]-[14].

Los Sistema de Gestión de Red son la piedra angular de los Centro de Operaciones de Red (NOC), dichos sistemas tienen como principales funciones monitorizar los niveles de disponibilidad, continuidad y rendimiento de la red de datos, gestión de alarmas y actividades de mantenimiento, supervisión de fallos de alimentación y activación de los sistemas de respaldo, entre otras[15], [16]. Adicionalmente en un NOC se manejan sistemas de manejo de tickets, manejo de incidentes, manejo de cartera de clientes y reportería, etc[17], [18].

Para el monitoreo de gestión de la seguridad informática y de redes de datos de manera similar a las herramientas presentes en los NOC existen herramientas informáticas que permiten manejar estas actividades de manera centralizada, permitiendo gestionar en tiempo

real infraestructuras complejas. Las dependencias desde las cuales se realizan estas tareas se definen de manera análoga a los NOC, como Centro de Operaciones de Seguridad (SOC). Las principales funciones de las herramientas informáticas utilizadas en los SOC son: mantenimiento de las herramientas de supervisión de la seguridad, investigación de actividades sospechosas, clasificación de las alertas, priorización de las alertas, procedimientos de remediación y recuperación ante desastres, y elaboración de informes [19], [20]. Las herramientas utilizadas en SOC permiten que las acciones sobre la infraestructura sean reactiva, proactiva, preventiva, y correctiva, todo ataque, amenaza incidente de seguridad tras ser identificado y detectada deberá ser analizada y corregido con prioridad y una vez que este se haya subsanado, hay que evitar que se repita, aplicando las acciones correctivas pertinentes[21]-[23].

En las empresas cuyo giro del negocio no está muy relacionado con el manejo de tecnología es común que exista poco control sobre lo que sucede dentro de infraestructura de sus redes de datos. En su gran mayoría estas organizaciones funcionan en modo de extinción de incendios, lo que hace que los recursos se apliquen solo cuando los problemas están a punto de ser críticos, o si ya lo han sido. Según lo indicado en [24] los sectores más atacados son el de finanzas, manufactura y el sector energético.

Una de las medidas innovadoras para solucionar esto y que ha tenido acogida es la implementación de un modelo hibrido entre el Centro de Operaciones de Red NOC y el Centro de Operaciones de Seguridad SOC para aumentar la visibilidad, centralizar la gestión y mejorar el control. Esta intersección entre las operaciones de red y la seguridad será clave para establecer el tipo de postura defensiva flexible y la estrategia de gestión de riesgos adaptable que se requiere para proteger los entornos dinámicos y las operaciones empresariales de hoy en día[25], [26].

La gestión eficaz de la red no debe limitarse nunca a una perspectiva exclusivamente operativa o de seguridad. En el complejo ecosistema actual de redes digitales hiperconectadas, las técnicas de únicamente NOC o SOC son insuficientes. Por el contrario, un enfoque unificado de las operaciones de red seguras mitiga eficazmente las limitaciones de recursos, El término El Centro de Operaciones de Seguridad y Redes (NSOC) fue creado de forma de consolidar las funciones del Centro de Operaciones de Red (NOC) y él Centro de Operaciones de Seguridad (SOC), con el propósito de reducir el tiempo de respuesta frente a incidentes de seguridad [26].

En las siguientes secciones se describen y analizan normas y procedimientos para la gestión de las redes de datos y seguridad informática, los cuales son aplicados a las empresas eléctricas.

### 1.3.1. GESTIÓN DE REDES DE DATOS

#### 1.3.1.1. La Norma M.3100: Principios para una red de gestión de las telecomunicaciones

En esta norma técnica se presentan recomendaciones para la gestión de las redes de datos desde la perspectiva de disponer de una infraestructura independiente desde la cual se pueda gestionar los equipos activos de la red, dónde han sido identificadas 5 áreas funcionales de gestión, siendo estás las siguientes: gestión de la calidad de funcionamiento, gestión de fallos, gestión de la configuración, gestión de la contabilidad(si la red no es facturada, este término cambia por la gestión de la administración) y gestión de la seguridad[27].

La correcta aplicación de los principios para una red de gestión de las telecomunicaciones descritos en la norma M.3100 permiten alcanzar los siguientes objetivos:

- ❒ Disminuir los tiempos de respuesta de reparaciones ante eventos de fallos en las redes de datos
- ❒ Proporcionar mecanismos de segmentación de la red de datos a fin de minimizar los riesgos de seguridad ante posibles ataques a la infraestructura
- ❒ Identificar y solventar problemas por fallos de la red de datos a través de mecanismos de aislamiento
- ❒ Mejorar la calidad del servicio y el soporte ante los clientes y usuarios de la red de datos.

#### 1.3.1.2. La Norma M.3400: Funciones de gestión de la red de gestión de las telecomunicaciones

Luego de la introducción de la norma M.3010 en 1996 entra en escena la norma M.3400 que fue presentada en 1997. La norma M.3400 describe el detalle de los procesos de gestión de la calidad del funcionamiento, gestión de averías o de mantenimiento, gestión de la configuración, gestión de la contabilidad o de la administración dependiendo si la red facturada o no, y la gestión de la seguridad, dichos procesos dan inicio al modelo de gestión *Falla, Configuración, Contabilidad, Desempeño, Seguridad*.

#### 1.3.1.3. Modelo de Gestión de redes FCAPS

El modelo de gestión Falla, Configuración, Contabilidad, Desempeño, Seguridad (FCAPS) es una de las primeras normas generadas para la gestión de redes de datos y tiene su origen en 1980. Este modelo de gestión está basado en los siguientes puntos: gestión de errores, gestión de la configuración, administración, gestión del rendimiento y gestión de la seguridad[28]. A continuación se describen cada uno de estos aspectos:

1. **Gestión de errores:** Este procedimiento se lo realiza a través del uso de herramientas informáticas que permitan acceder y usar la información generada por los equipos terminales mediante protocolos de gestión de infraestructura tecnológica como son SNMP y syslog. La información generada en los equipos terminales es recibida en servidores de gestión, donde es catalogada, analizara y puede ser enviada a los administradores de la infraestructura mediante métodos como correo electrónico, mensajes de texto o plataformas mensajería instantánea como telegram, signal o WhatsApp. SNMP y syslog de manera general generan información acerca del estado de los equipos, porcentaje de uso de los recursos de hardware, procesamiento, memoria RAM, almacenamiento, para los equipos de redes de datos informan el volumen de tráfico que está ingresando y saliendo a través de sus interfaces de red, además puede alertar sobre fallos de hardware en los equipos, accesos y accesos no autorizados, detalles adicionales dependen de los equipos, modelos y marcas de equipos instalados.

2. **Gestión de la configuración:** En este procedimiento se coordinan todos los cambios de hardware y de software que se realizarán sobre la infraestructura instalada y se basa en las siguientes actividades: recolectar información de la infraestructura instalada, cambios sobre la configuración de la infraestructura instalada, generación de reportes y los procesos de gestión de cambios.

3. **Administración:** En la versión inglesa FCAPS la administración aparece representada a través del término *Accounting*, el cual está orientado a redes de datos tarifadas es decir este proceso trata en esos casos de la gestión de la tarifación. Para redes de datos no tarifadas el término *Accounting* se reemplaza por administración y en este caso tiene como objetivo gestionar el conjunto de usuarios autorizados definiendo nombres de usuario, contraseñas, permisos a asignar y también se encarga de administrar las operaciones sobre los equipos de la infraestructura instalada, esto es asignar roles y funciones a sus administradores.

4. **Gestión del rendimiento:** La gestión del rendimiento permite determinar los valores de *throughput*, el porcentaje de utilización, las tasas de error y los tiempos de

respuesta de la red de datos instalada, dicha información habilita la línea base para el despliegue posibles mejoras tecnológicas de considerarse necesarias a fin de garantizar un servicio adecuado en el transporte de datos.

5. **Gestión de la seguridad:** Este proceso realiza el control de acceso a los recursos de la red de datos, generalmente se lo realiza a través del proceso de autenticación, cifrado y autorización configurada en los equipos de red o también se pueden usar mecanismos de control de acceso centralizados como Remote Authentication Dial In User Service (RADIUS), Terminal Access Controller Access Control System (TACACS), Lightweight Directory Access Protocol (LDAP), directorios activos, etc.

### 1.3.2. GESTIÓN DE LA SEGURIDAD INFORMÁTICA EN SISTEMAS DE CONTROL INDUSTRIAL

#### 1.3.2.1. El Modelo Purdue

En el diseño y despliegue de redes de datos corporativas, la arquitectura de red según Debe estar definida de tal manera que se permitan diferenciar los distintos segmentos de red en consideración de sus funciones y objetivos a fin de poder aplicar de mejor manera las medidas de seguridad y evitar el flujo de información de manera innecesaria. está segmentación de red se aplica también al despliegue de redes de datos para sistemas de control industrial, en dónde resulta muy importante contar con zonas diferenciadas y mecanismos de control de tráfico, lo cual representa un primer paso en la implementación de controles de seguridad de la red de datos.

El modelo Purdue definidos en la norma Integración de los Sistemas de Control Empresarial (ISA-95) como *Purdue Enterprise Reference Architecture* describe una arquitectura de red como modelo de referencia en la que se establecen 5 niveles lógicos bajo los cuales se agruparán en segmentos de red elementos de la arquitectura con funciones claramente diferenciadas[29]. La estructura del modelo Purdue se conforma de manera descendente desde el nivel 4 hasta el nivel 0, los cuales se describen a continuación:

**Nivel 4 - Red Corporativa:** Las actividades del nivel 4 se ocupan de la gestión de las actividades relacionadas con el giro del negocio(es decir a que se dedica la empresa), en este nivel también se realiza la gestión de las operaciones y de los procesos industriales del negocio (giro del negocio, generación de bienes, servicios, fabricación de productos, etc.).

**Nivel 3 - Control de Procesos:** Las actividades de nivel 3 gestionan el flujo de trabajo de producción relacionado con el giro del negocio empresarial. Los sistemas que

suelen utilizarse para realizar las actividades del nivel 3 son los sistemas de gestión de lotes, los sistemas de ejecución de la fabricación (MES) y los sistemas de gestión de las operaciones de fabricación (MOM). Además, los sistemas de gestión de laboratorio, mantenimiento y rendimiento de la planta y los históricos de datos.

**Nivel 2 - Dispositivos de Monitorización:** En el nivel 2, se produce la supervisión, el seguimiento y el control de los procesos físicos. Mediante el uso de equipos de control en tiempo real, equipos industriales, como los sistemas de control distribuido (DCS), las interfaces hombre-máquina (HMI) y el control de supervisión y adquisición de datos (SCADA), se controla y dirige el proceso físico.

**Nivel 1 - Dispositivos, sensores, actuadores y analizadores:** Las actividades de nivel 1 implican la detección y manipulación de los procesos físicos. Un ejemplo sería todos los sensores, analizadores, actuadores e instrumentos relacionados necesarios para dar continuidad al giro del negocio.

**Nivel 0 - Proceso:** Define los procesos reales utilizados para crear o apoyar la creación del producto, bien o servicio generado que la empresa vende.

#### 1.3.2.2. La Norma NIST 800-82

La norma NIST SP 800-82 forma parte de un grupo de normas, recomendaciones y guías técnicas publicadas por él National Institute of Standards and Technology NIST (NIST). El grupo de las NIST SP hace referencia a guías, definiciones técnicos, recomendaciones y materiales adicionales sobre *Computer security (SP 800)*, prácticas de seguridad (SP 1800) y tecnologías de información (SP 500).

NIST SP 800-82 es una guía de seguridad para Sistema de Control y Automatización Industrial (IACS), también conocidos como Sistemas de Control Industrial (ICS). Esta norma proporciona una visión conceptual de los ICS, topologías típicas recomendadas para implementación, procedimientos para la identificación de amenazas y vulnerabilidades en la infraestructura, contramedidas de seguridad recomendadas y controles de seguridad sugeridos. En este documento se intenta englobar los requerimientos mínimos que toda empresa industrial debe tener en cuenta tales como la gestión de riesgos descritos en la serie de normas que abordan la ciberseguridad de la tecnología operativa en los sistemas de automatización y control (IEC 62433) o la selección de controles de seguridad descritos en el catálogo de controles de seguridad y privacidad para todos los sistemas de información federales de Estados Unidos (NIST 800-53). Se definen los protocolos de arquitecturas de red en infraestructuras destinadas a entornos industriales y las configuraciones sugeridas en los equipos de control de acceso para tecnologías operativas [30]-[32].

#### 1.3.2.3. La Norma NERC CIP

La Norma NERC CIP hace referencia a una serie de guías con controles de obligatorio cumplimiento para la protección de infraestructuras críticas[32], las mismas que son definidas y actualizadas por él North American Electric Reliability Corporation (NERC), organismo regulador de la energía en los Estados Unidos. En esta norma se definen los diferentes roles empresariales en la operación del sistema eléctrico, la criticidad y las vulnerabilidades de los activos que lo componen así como también los riesgos a los que estos activos están expuestos. Actualmente, están en vigor los siguientes controles[7]:

1. CIP-002-5.1a Categorización del sistema cibernético BES (red del sistema eléctrico - bulk electric system, clasificación de criticidad de los equipos).
2. CIP-003-8 Controles de gestión de la seguridad.
3. CIP-004-6 Personal y formación.
4. CIP-005-6 Perímetro(s) de seguridad electrónica.
5. CIP-006-6 Seguridad física de los cibersistemas BES.
6. CIP-007-6 Gestión de la seguridad del sistema.
7. CIP-008-6 Planificación de la notificación y respuesta a incidentes.
8. CIP-009-6 Planes de recuperación de los cibersistemas BES.
9. CIP-010-3 Gestión de los cambios de configuración y evaluación de la vulnerabilidad.
10. CIP-011-2 Protección de la información.
11. CIP-013-1 Gestión de riesgos en la cadena de suministro.
12. CIP-014-2 Seguridad física.

#### 1.3.2.4. La Norma ITU-T X.805

La norma ITU-T X.805 : Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo presenta recomendaciones para la definición de una arquitectura de seguridad de red que garantice la seguridad en las comunicaciones de extremo a extremo.

[7] El último dígito del código corresponde a la revisión

estas definiciones pueden aplicarse a distintas clases de redes en las que uno de los objetivos esenciales sea garantizar la seguridad entre equipos de la infraestructura instalada. En esta norma se abordan los siguientes conceptos: control de acceso, disponibilidad, autenticación, confidencialidad, integridad de los datos, no repudio, y privacidad. Al contar con definiciones más exhaustivas en cuanto a la seguridad de la información, esta norma es generalmente aplicada en la definición de políticas y arquitecturas de redes de datos para infraestructuras críticas como ejemplo de esto está el sector de las empresas eléctricas.

### 1.3.3. DIFERENCIAS ENTRE LA GESTIÓN DE REDES DE DATOS TRADICIONALES Y REDES DE DATOS INDUSTRIALES

Según las revisiones conceptuales realizadas hasta el momento en la sección de marco teórico existen definiciones que caracterizan de manera puntual los sistemas de control industrial tanto en normativa como en principios de gestión y administración de las redes de datos de las que estos sistemas hacen uso. Por este motivo y en consideración de que en la E.E.Q. existen una gran cantidad de sistemas implementados con tecnología legada es importante definir los conceptos de las tecnologías operativas a nivel empresarial. Según el Ministerio de Telecomunicaciones y de la Sociedad de la Información el término de tecnología operativa se define de la siguiente manera: *la tecnología operativa se refiere al hardware y software que se utiliza para detectar o causar cambios en procesos físicos a través del monitoreo o ejecución de dispositivos que forman parte de sistemas de control industrial* [33]. Para gestionar redes de datos de tecnología operativa se debe considerar las siguientes diferencias:

- **Gestión de equipamiento de servicios legados (legacy services):** Una de las principales características del equipamiento de naturaleza industrial es su extenso tiempo de vida útil que generalmente sobrepasa los 15 años por este motivo suelen tender a estar atrasados en cuanto a la tecnología manejada en equipamientos similares utilizados en ambientes no industriales, ejemplos de esto son los enrutadores y switches industriales versus los enrutadores y switches no industriales. Este desfase en acompañamiento a que muchos de los servicios industriales y equipos instalados no cuentan aún con la disponibilidad de la tecnología IP para su conectividad limitan mucho implementar procesos de gestión adecuados por lo cual estos deben adaptarse a la medida de la infraestructura instalada[34].

- **Arquitectura implementada y tráfico de datos:** las redes operativas están caracterizadas por ser de gran tamaño en consideración de los sitios que deben interconectar como en el caso de las empresas eléctricas las subestaciones, en cuanto al tráfico

este no suele ser abundante sino que más bien requiere consideraciones adicionales a las que normalmente se toman en las redes de datos tradicionales. estas consideraciones hacen referencia a la calidad del servicio aplicada por flujo de datos, resiliencia y disponibilidad de la red, estas tres características generalmente están dirigidas a garantizar que el proceso del giro de negocio no se vea afectado frente a fallos en la red de datos. Por el contrario, las redes de datos tradicionales conectan un número reducido de sitios entre los cuales generalmente se está transportando grandes volúmenes de tráfico, haciendo referencia a las empresas eléctricas este escenario aborda los nodos de red en donde están ubicadas las oficinas administrativas[34].

- **Aplicación de calidad de servicio (QoS):** este requerimiento nace en consideración de que los flujos de datos de los sistemas industriales suelen ser sensibles a los efectos del retardo en la red de datos, Adicionalmente las redes de datos industriales requieren altos niveles de disponibilidad tolerancia a fallos y autonomía de suministro eléctrico. En contraste a las redes tradicionales donde la prioridad es el rendimiento de la red, la flexibilidad y abundantes recursos de ancho de banda[34].

- **Arquitecturas de red deterministas:** en las redes de datos industriales se tiende a tener arquitecturas de red preestablecidas y normalmente fijas, como ejemplo para las empresas eléctricas están las subestaciones hacia su centro de control, esta arquitectura suele conocerse como de tipo maestro - esclavo. Para el caso de las redes de datos tradicionales esta es de arquitecturas suelen contar con mucha más flexibilidad funcionando de manera similar a una arquitectura de tipo estrella[34].

- **Ciclos de vida de las redes:** En las redes de datos operativas no es muy común el cambio en su funcionamiento y arquitectura, en estos entornos es importante garantizar la continuidad de los servicios del transporte de datos. Las actualizaciones y cambios en la red de datos operativas suele estar orquestada por las aplicaciones de los sistemas industriales involucrados. en el caso de las redes corporativas las actualizaciones son frecuentes y estén dirigidos por los nuevos paradigmas tecnológicos en cuanto a la tecnología implementada en las infraestructuras tecnológicas instaladas[34].

- **Procesos de administración de las redes de datos:** las redes de datos operativas requieren disponer de métodos de restablecimiento de fallos rápidos y efectivos los cuales deben ser continuamente monitoreados. Los procesos de gestión de las redes operativas están definidas por los tiempos de respuesta ante las posibles problemas reportados como al contrario de lo que suele suceder en las redes de datos tradicionales donde los procesos de gestión suelen ser mucho más formales requiriendo así más tiempo en ser resueltos. En las redes de datos operativas es fundamental disminuir los tiempos de restablecimiento del servicio[34].

- ❒ **Arrendamiento de redes a proveedores externos:** En los entornos de redes tradicionales este escenario suele ser común, ya que el interconectar las localizaciones empresariales puede ser mucho más barato a través de un prestador de servicios de transporte de datos (carrier). En el caso de las redes de datos operativas las veces suelen disponer de redes completamente privadas a fin de poder controlar los niveles de servicio sin que los fallos de la red de datos afecten al giro del negocio, evitando así multas o posibles sanciones de los organismos reguladores[34].

- ❒ **Administración de la seguridad:** la gestión de la seguridad presenta características radicalmente diferenciadoras entre las redes de datos operativas y las redes de datos tradicionales. Las redes de datos operativas tienen como principal prioridad garantizar la disponibilidad de los servicios mientras que las redes de datos corporativas manejan como principales prioridades garantizar la integridad y confidencialidad de la información[34].

### 1.3.4. NETWORK OPERATIONS CENTER (NOC)

Un *Centro de Operaciones de Red (*NOC*)* hace referencia a un grupo de trabajo de especialistas en la administración de redes de datos y a la infraestructura disponible para estas tareas, como infraestructura se incluye tanto las herramientas de hardware y software. Este grupo de trabajo se encarga de controlar y administrar toda la infraestructura de la red, lo cual incluye equipamiento como servidores, conmutadores, enrutadores, cortafuegos, sistemas de almacenamiento, sistemas de bases de datos, sistemas inalámbricos, sistemas de telecomunicaciones, dispositivos terminales como cámaras de circuitos cerrados de televisión y cualquier otro equipo terminal que cuente con una dirección IP.

Desde el punto de la gestión de incidencias el NOC es la componente de la organización que realiza los procesos de detección, acción, documentación y análisis de la red, generación de reportes de uso de ancho de banda, *throughput*, latencia, jitter y tasas de errores, garantizando cumplir con los niveles de servicio adecuados para la empresa.

#### 1.3.4.1. Funcionalidades del Network Operations Center (NOC)

Los *Centro de Operaciones de Red* tienen las siguientes funcionalidades:

1. Supervisión y mantenimiento de las infraestructuras de redes de datos.

2. Monitorización de alertas generadas por los equipos de redes de datos.

3. Actualizaciones de hardware y software tanto por obsolescencia tecnológica como por consideraciones de seguridad (parches de seguridad) en el firmware instalado en los equipos de redes.

4. Monitorización del tráfico de datos y porcentaje de uso del ancho de banda disponible para velar por el buen funcionamiento de los servicios (aplicaciones instaladas en los servidores y clientes) que atraviesan la red de datos.

5. Gestión de la solución a fallos y tareas de mantenimiento.

6. Gestión de la administración, copias de seguridad de configuraciones y control de acceso a los equipos de red.

7. Monitorización del suministro eléctrico de los equipos de redes de datos.

8. Generación de informes sobre los niveles de servicio de la red de datos e implementación de mejoras continuas sobre la infraestructura instalada.

#### 1.3.4.2. Facilidades técnicas del Network Operations Center (NOC)

Los *Centro de Operaciones de Red* deben contar con las siguientes facilidades técnicas:

1. Contar con un grupo de trabajo de especialistas en la administración de redes de datos asignados al NOC.

2. Disponer de infraestructura de hardware(servidores) y equipos de control de acceso a la red (firewalls) para el despliegue de herramientas informáticas que permitan realizar desplegar las funcionalidades de los NOC.

3. El área de trabajo del NOC deberá incluir además de todas las estaciones de trabajo, videowalls que permitan hacer un trabajo en conjunto por los especialistas asignados, facilitando así la conciencia situacional de los problemas.

4. Contar con herramientas de gestión de redes de datos (Sistema de Gestión de Red (NSM)) que permitan realizar tareas como las siguientes: monitorear, fiscalizar (descubrimiento automático), y realizar mantenimiento.

5. Contar con herramientas informáticas para la gestión de tickets con la asignación de labores, tiempos de respuesta, asignación de recursos, etc.

6. Contar con la capacidad de asistencia remota en casos excepcionales donde no se pueda ingresar a las instalaciones empresariales, la asistencia y actividades de respuesta podrá realizarse mediante conexiones de tipo Virtual Private Network (VPN).

7. Contar con herramientas informáticas para la emisión de informes sobre la administración de las incidencias trazándolas debidamente, solventándolas rápidamente, llegando a la raíz de los errores, fallos, e incidentes a fin de garantizar un adecuado nivel de servicio en el transporte de datos.

### 1.3.5. SECURITY OPERATIONS CENTER (SOC)

Un *Centro de Operaciones de Seguridad (*SOC*)* hace referencia a un grupo de trabajo de especialistas en la gestión de seguridad de infraestructuras tecnológicas en las cuales se deben detectar, analizar, responder, informar y prevenir incidentes de seguridad en la infraestructura tecnológica empresarial.

#### 1.3.5.1. Funcionalidades de los Security Operations Center (SOC)

Los *Centro de Operaciones de Seguridad* tienen las siguientes funcionalidades:

1. Monitorización de las infraestructuras de redes de comunicaciones, equipos de control de acceso de seguridad perimetral (firewalls), servidores, estaciones de trabajo y demás equipos terminales que forman parte de la infraestructura tecnológica instalada a nivel empresarial.

2. Monitorización avanzada de la red de datos y equipos de seguridad (firewalls) con procesos de análisis de información en tiempo real y de manera histórica.

3. Detección de riesgos y vulnerabilidades en seguridad de la infraestructura tecnológica instalada, análisis, mitigación y prevención de los mismos.

4. Procesamiento de alarmas desde los equipos instalados, así como la recopilación pasiva de registros de eventos (logs).

5. Mitigación de ataques o control de impacto de los mismos sobre la infraestructura empresarial instalada.

6. Proponer mejoras sobre la seguridad de la infraestructura tecnológica empresarial a través de la implementación de soluciones tecnológicas y de la optimización de los controles de acceso instalados.

7. Velar por el cumplimiento de las normativas de seguridad establecidas de acuerdo al giro del negocio empresarial.

8. En caso de que la empresa sufra vulneraciones en su infraestructura, él SOC será el encargado del análisis forense sobre el evento reportado y de la generación de los respectivos informes sobre el evento.

#### 1.3.5.2. Facilidades técnicas del Security Operations Center (SOC)

Los *Centro de Operaciones de Seguridad* deben contar con las siguientes facilidades técnicas:

1. Contar con un grupo de trabajo de especialistas en la gestión de la seguridad de la infraestructura tecnológica asignados al SOC.
2. Disponer de infraestructura de hardware(servidores) y equipos de control de acceso a la red (firewalls) para el despliegue de herramientas informáticas que permitan realizar desplegar las funcionalidades de los SOC.
3. El área de trabajo del SOC deberá incluir además de todas las estaciones de trabajo, videowalls que permitan hacer un trabajo en conjunto por los especialistas asignados, facilitando así la conciencia situacional de los problemas.
4. Contar con herramientas informáticas que permiten realizar la evaluación de vulnerabilidades (escáner de vulnerabilidades) sobre la infraestructura tecnológica instalada así como la información del registro de eventos (analizador de logs) procedente de este equipamiento. Implementaciones avanzadas de herramientas para Centro de Operaciones de Seguridad (SOC) suelen disponer también de soluciones de tipo Security Information and Event Management (SIEM) o Security Orchestration Automation and Response (SOAR).
5. Contar con herramientas informáticas para la gestión de tickets con la asignación de labores, tiempos de respuesta, asignación de recursos, etc.
6. Las herramientas tecnológicas instaladas en él SOC deberán contar con la capacidad de la actualización continua frente a nuevas amenazas cibernéticas.
7. Contar con la capacidad de asistencia remota en casos excepcionales donde no se pueda ingresar a las instalaciones empresariales, la asistencia y actividades de respuesta podrá realizarse mediante conexiones de tipo Virtual Private Network (VPN).
8. Contar con herramientas informáticas para la emisión de informes sobre incidencias en la seguridad de la infraestructura tecnológica, trazándolas debidamente, solventándolas rápidamente, llegando a la raíz de los errores, fallos, e incidentes a fin de garantizar las políticas de seguridad empresariales.

### 1.3.6. NETWORK SECURITY OPERATIONS CENTER (NSOC)

El Centro de Operaciones de Seguridad en Redes (NSOC), protege, gestiona y supervisa el estado operativo de la red de datos y la seguridad de la infraestructura tecnológica de la organización.

#### 1.3.6.1. Funcionalidades de los Network Security Operations Center (NSOC)

1. Monitorización de sistemas, dispositivos(equipos de redes de datos, firewalls, servidores, estaciones de trabajo, etc.) y aplicaciones empresariales a fin de garantizar el correcto funcionamiento de la infraestructura tecnológica instalada.
2. Monitorización avanzada de alertas en los equipos de la red de datos y equipos de seguridad (firewalls) con procesos de análisis de información en tiempo real y de manera histórica.
3. Actualizaciones de hardware y software tanto por obsolescencia tecnológica como por consideraciones de seguridad (parches de seguridad) en el firmware instalado en los equipos de redes y firewalls, estas actividades podrían incluir también actualizaciones en el firmware del hardware de servidores y sobre los sistemas operativos de los equipos terminales.
4. Monitorización del tráfico de datos y porcentaje de uso del ancho de banda disponible para velar por el buen funcionamiento de los servicios (aplicaciones instaladas en los servidores y clientes) que atraviesan la red de datos.
5. Gestión de la administración, copias de seguridad de configuraciones y control de acceso a los equipos de red.
6. Procesamiento de alarmas desde los equipos instalados, así como la recopilación pasiva de registros de eventos (logs).
7. Monitorización del suministro eléctrico de los equipos de redes de datos.
8. Gestión de fallos y tareas de reparación, notificación al grupo de trabajo del NSOC.
9. Detección de riesgos y vulnerabilidades en seguridad de la infraestructura tecnológica instalada, análisis, mitigación y prevención de los mismos.
10. Mitigación de ataques o control de impacto de los mismos sobre la infraestructura empresarial instalada.
11. Aplicación de actualizaciones de software, parches de seguridad y reemplazos de hardware del equipamiento instalado frente a fallos físicos.

12. Debe contar con la capacidad de gestión de la red de datos de la empresa, incluyendo inventario de activos, distribución de software, parches automatizados, despliegue de actualizaciones en sistemas operativos, acceso remoto a estaciones de trabajo y servidores.

13. Proponer mejoras sobre la seguridad de la infraestructura tecnológica empresarial a través de la implementación de soluciones tecnológicas y de la optimización de los controles de acceso instalados, velando por el cumplimiento de las normativas de seguridad establecidas de acuerdo al giro del negocio empresarial.

14. Debe proporcionar informes históricos y bajo demanda, incluyendo informes de estadísticas de rendimiento de la red (jitter, latencia, disponibilidad, entrega de paquetes, métricas de cumplimiento de los niveles de servicio) e informes de gestión de los niveles de seguridad, eventos y sobre la actividad de los usuarios finales, los cambios administrativos y las alertas de seguridad reportadas.

#### 1.3.6.2. Facilidades técnicas de los Network Security Operations Center (NSOC)

Los *Centro de Operaciones de Seguridad en Redes* deben contar con las siguientes facilidades técnicas:

1. Contar con un grupo de trabajo de especialistas en la gestión de redes y de la seguridad de la infraestructura tecnológica asignados al NSOC.

2. Disponer de infraestructura de hardware(servidores) y equipos de control de acceso a la red (firewalls) para el despliegue de herramientas informáticas que permitan realizar desplegar las funcionalidades de los NSOC.

3. El área de trabajo del NSOC deberá incluir además de todas las estaciones de trabajo, videowalls que permitan hacer un trabajo en conjunto por los especialistas asignados, facilitando así la conciencia situacional de los problemas.

4. Contar con herramientas informáticas que permitan gestión de redes de datos (Sistema de Gestión de Red (NSM)) que permitan realizar tareas como las siguientes: monitorear, fiscalizar (descubrimiento automático), y realizar mantenimiento, realizar la evaluación de vulnerabilidades (escáner de vulnerabilidades) sobre la infraestructura tecnológica instalada así como la información del registro de eventos (analizador de logs) procedente de este equipamiento, esto se puede complementar con la inclusión de herramientas como los Security Information and Event Management (SIEM) o las soluciones Security Orchestration Automation and Response (SOAR).

5. Contar con herramientas informáticas para la gestión de tickets con la asignación de labores, tiempos de respuesta, asignación de recursos, etc.

6. Las herramientas tecnológicas instaladas en él SOC deberán contar con la capacidad de la actualización continua frente a nuevas amenazas cibernéticas.

7. Contar con la capacidad de asistencia remota en casos excepcionales donde no se pueda ingresar a las instalaciones empresariales, la asistencia y actividades de respuesta podrá realizarse mediante conexiones de tipo Virtual Private Network (VPN).

8. Contar con herramientas informáticas para la emisión de informes sobre incidencias en la seguridad de la infraestructura tecnológica, trazándolas debidamente, solventándolas rápidamente, llegando a la raíz de los errores, fallos, e incidentes a fin de garantizar las políticas de seguridad empresariales.

### 1.3.7. COMPARACIÓN DE LAS FUNCIONALIDADES DE UN NOC VS. SOC VS NSOC

En la presente sección se realizará un análisis comparativo de las funcionalidades y facilidades técnicas requeridas por los NOC, SOC, NSOC. La comparación es realizarse la desarrollará teniendo en cuenta los aspectos comunes entre los tres tipos de centros de operación de infraestructura tecnológica y los aspectos especializados que los diferencian.

#### 1.3.7.1. Funcionalidades comunes entre NOC VS SOC VS NSOC

Las principales funcionalidades comunes entre los NOC, SOC versus NSOC son:

- ❒ Funcionalidades de monitoreo y supervisión de la continuidad de la infraestructura tecnológica:
  - ✧ Él NOC monitorea métricas como ancho de banda, throughput, latencia, jitter y la tasa de error, alarmas, temperatura, porcentaje de uso de memoria, procesamiento, almacenamiento en la infraestructura de redes de datos empresarial.
  - ✧ Él SOC monitorea, analiza y mitiga las vulnerabilidades de la infraestructura tecnológica empresarial, esto incluye: servidores, estaciones de trabajo, equipos de redes de datos, equipos de seguridad de red (firewalls), y demás equipos conectados a la red de datos empresarial, además de procesar la información recibida desde los equipos instalados a través de los registros de eventos.

- ✧ Él NSOC aborda las funcionalidades del NOC y del SOC de tal manera que se encarga de monitorear la red de datos a nivel de niveles de uso de ancho de banda, throughput, latencia, jitter y la tasa de error, alarmas, temperatura, porcentaje de uso de memoria, procesamiento, almacenamiento en la infraestructura de redes de datos empresarial así como también de monitorear, analizar y mitigar las vulnerabilidades de la infraestructura tecnológica empresarial, esto incluye: servidores, estaciones de trabajo, equipos de redes de datos, equipos de seguridad de red (firewalls), y demás equipos conectados a la red de datos empresarial, además de procesar la información recibida desde los equipos instalados a través de los registros de eventos.

- ❒ Funcionalidades de actualización de firmware, sistemas operativos y aplicación de parches de seguridad:

  - ✧ Él NOC se encarga de actualizar los firmware y aplicar parches de seguridad en los equipos de redes.
  - ✧ Él SOC se encarga de actualizar los firmware y aplicar parches de seguridad principalmente en firewalls, infraestructura de servidores, estaciones de trabajo, aunque también podría incluir los equipos de redes de datos, adicional a equipamiento como cámaras de videovigilancia, equipos de control y registro del personal, etc.
  - ✧ El NSOC debido a que aborda las responsabilidades del NOC y del SOC realiza la actualización de los firmware y aplica parches de seguridad principalmente en firewalls, infraestructura de servidores, estaciones de trabajo, equipos de redes de datos y demás equipos conectados a la red de datos.

- ❒ Funcionalidades de reparación y mantenimiento de la infraestructura:

  - ✧ Él NOC se encarga de la gestión del mantenimiento y reparación de los equipos de redes de datos.
  - ✧ Él SOC se encarga de la gestión del mantenimiento y reparación de los equipos de seguridad de red, pudiendo incluir hardware de servidores, estaciones de trabajo y demás equipamiento destinado a asegurar la infraestructura tecnológica frente a posibles ataques cibernéticos.
  - ✧ Él NSOC presenta entre sus responsabilidades la gestión y mantenimiento del total de la infraestructura tecnológica instalada, incluyendo tanto equipos de redes de datos como firewalls, servidores, etc.

- ❒ Emisión de reportería e informes técnicos: Tanto él NOC, SOC y NSOC deben generar reportes e informes sobre las actividades que estos realizan, así como también

sobre los eventos y soporte desarrollado en la infraestructura tecnológica empresarial.

#### 1.3.7.2. Facilidades técnicas comunes requeridas entre NOC VS SOC VS NSOC

Como facilidades técnicas comunes para poder desplegar se tienen las siguientes:

- ❒ Recursos humanos: Tanto él NOC, SOC y NSOC deben con equipos de personal técnico especializado en sus respectivas áreas, en este punto existe la posibilidad de que este personal técnico comparta funciones a nivel de la gestión de los equipos de redes de datos con la gestión de los equipos de seguridad de red, esto permite optimizar los recursos técnicos asignados, logrando así ejecutar las funciones de NOC, SOC en un solo grupo llamado NSOC. Para conseguir esto se debe contar con programas de entrenamiento que permitan diversificar las habilidades técnicas del personal asignado al NSOC.
- ❒ Recursos de hardware y herramientas especializadas de software: Tanto él NOC, SOC y NSOC deben con infraestructura de hardware de servidores y herramientas de software que les permitan desarrollar las funciones de administración y gestión de los equipos de redes de datos, seguridad de red e infraestructura tecnológica instalada. Esta infraestructura de hardware puede ser optimizada usándose de manera simultánea para instalar las herramientas de software necesarias para la gestión de las redes de datos y la seguridad de los equipos instalados.
- ❒ Infraestructura de mobiliario, estaciones de trabajo y videowall: Los espacios físicos de las estaciones de trabajo son fundamentales para el correcto desempeño de los grupos técnicos asignados al NOC, SOC y NSOC. Al optimizar los recursos humanos asignados a estos grupos de trabajo se puede optimizar también el número de las estaciones de trabajo y las instalaciones de videowall requeridas. Desde el punto de vista de la conciencia situacional contar con un solo videowall permitirá que las acciones de soporte y mantenimiento así como las actividades de respuesta frente a ataques cibernéticos puedan desarrollarse de mejor manera entre los profesionales y administradores a cargo de la infraestructura empresarial.
- ❒ Contar con herramientas informáticas para la emisión de informes técnicos: En la actualidad el mercado tecnológico de las herramientas informáticas orientadas a la gestión de la infraestructura permite la posibilidad de que se puedan gestionar de manera simultánea tantos equipos de redes de datos, firewalls, servidores, y demás equipos que cuenten con protocolos de gestión de infraestructura disponibles. Desde este punto de vista resulta factible el contar con un número menor de herramientas

informáticas para poder abordar el análisis de información y generación de informes tanto a nivel de NOC, SOC y NSOC.

#### 1.3.7.3. Funcionalidades especializadas entre NOC VS SOC VS NSOC

Las principales funcionalidades especializadas que diferencian los NOC, SOC versus NSOC son:

- ❒ El personal técnico del NOC posee habilidades especializadas en garantizar la eficiencia operativa a través de la correcta gestión de la infraestructura de la red de datos, configuración de equipos, correcta aplicación de las tecnologías de redes de datos, actividades, soporte y solución de problemas.

- ❒ El personal técnico del SOC posee habilidades especializadas en garantizar entornos seguros para la infraestructura tecnológica empresarial instalada.

- ❒ Al contrario de lo que el personal técnico del NOC o SOC realiza especializándose en cada una de sus áreas, a través del NSOC el personal técnico dispone de una visibilidad integral de la seguridad y las operaciones de las redes de datos.

#### 1.3.7.4. Facilidades técnicas requeridas especializadas entre NOC VS SOC VS NSOC

Las principales facilidades técnicas especializadas que diferencian los NOC, SOC versus NSOC son:

- ❒ Él NSOC al tener como principal de sus características el combinar diferentes fuentes de información para ser visualizada y analizada en un solo contexto puede llegar a necesitar infraestructura de hardware y software que permita combinar estas fuentes de información y su posterior publicación en paneles de control (dashboard) dedicados.

- ❒ El manejar grandes volúmenes de información en un NSOC hace necesario contar con herramientas de automatización de tareas que permiten aprovechar de mejor manera la información recibida, de esta manera se podrán definir flujos de trabajo y acciones de realizar en determinados contextos minimizando así los tiempos de respuesta frente a eventos reportados.

### 1.3.8. HERRAMIENTAS INFORMÁTICAS UTILIZADAS PARA LA IMPLEMENTACIÓN DE NOCs Y SOCs

Para la implementación de los Centro de Operaciones de Red (NOC) y Centro de Operaciones de Seguridad (SOC) se utilizan varias herramientas en función de las necesidades definidas en el diseño de su implementación. En las siguientes secciones se detallan las funcionalidades y ventajas de un conjunto de herramientas utilizadas en la implementación de estos centros de control de redes y seguridad.

#### 1.3.8.1. Herramientas para la implementación de NOCs

**1.3.8.1.1.** ***Nagios:*** Esta herramienta permite la monitorización de redes de datos a nivel de hardware y software de equipos de redes e infraestructura de servidores.

1. Es un software de monitorización popular con abundante información de los usuarios de código libre.
2. Es un software que tiene versiones de prueba por 60 días y versiones de pago.
3. Nagios está escrito en C, las redes evolucionan rápidamente hoy en día, C al ser un lenguaje antiguo es difícil de adaptar a esta rápida evolución.
4. Nagios cuenta con una comunidad activa, existe una gran variedad de complementos que han sido desarrollados por la comunidad.
5. Permite la monitorización con o sin agente.
6. Monitorización de disponibilidad de nodos (pcs, servidores, enrutadores, switches, etc.).
7. Monitorización de servicios (HTTP, SSH, FTP, pop, etc.).
8. Puede soportar la monitorización de miles de dispositivos y servicios.
9. Posee un portal web para la visualización del estado de dispositivos y servicios, log's, etc.
10. Generación de reportes sustentados basándose en los datos almacenados, estos reportes sirven para sustentar necesidades de la red, posibles actualizaciones.
11. Análisis del tráfico en tiempo real.
12. Envió de alertas al personal por email, SMS, etc.

**1.3.8.1.2.** ***Zabbix:*** Es un sistema de monitorización de redes diseñado para monitorizar y registrar el estado de varios servicios de red, Servidores, y hardware de red.

1. Zabbix es una herramienta gratuita, de código abierto.
2. Permite la monitorización con o sin agente.
3. Zabbix está disponible en muchos idiomas, entre ellos el español, siendo más fácil el manejo ara las personas nativas.
4. Permite la recopilación de métricas de varias fuentes (dispositivos de red, bases de datos, aplicaciones, servicios, etc.)
5. Es posible definir umbrales inteligentes para alertar de los problemas, estos umbrales son muy flexibles, pueden ir desde condiciones tan simples como "mayor que.ª usar toda la amplia gama de operadores admitidos.
6. Permite clasificar los problemas en niveles de gravedad.
7. Detección de incidencias en tiempo real.
8. Predicción de incidencias basada en tendencias.
9. Envió de alertas a las personas responsables a través de correo electrónico, SMS, Telegram, etc.
10. Visualización gráfica de datos recopilados, zabbix ofrece la funcionalidad de multi-page dashboards, que permite la unificación de pantallas y dashboards para la visualización de todos los datos.
11. Integración sencilla con la infraestructura existente, Zabbix está listo para monitorear el software y hardware de los principales distribuidores.
12. Gran capacidad de escalabilidad.
13. Generación de reportes en PDF, el periodo de generación y envió delos reportes se puede establecer.
14. Constante creación de nuevos templates para la monitorización de aplicaciones y servicios.

**1.3.8.1.3.** ***OpenNMS:*** OpenNMS está escrito en Java, por lo que puede ejecutarse en cualquier plataforma con soporte para un SDK de Java versión 8 o superior. Cuenca con binarios precompilados disponibles para la mayoría de las distribuciones de Linux, Windows, Solaris y OS X.

1. Es un software de código abierto.
2. Está orientado al uso de un agente en los clientes.
3. Gestión de Eventos y Notificaciones
4. Descubrimiento y Aprovisionamiento
5. Monitoreo de Servicios
6. Recolección de Datos, Características Adicionales.
7. Está escrito en Java, esto otorga la ventaja de que se pueda ejecutar en todas las plataformas existentes.
8. Gran escalabilidad.
9. Recolección de incidencias, puede recoger todo tipo de incidencias ocurridas.
10. OpenNMS está listo para usar, es de fácil integración con la infraestructura existente, lleva implementado MIBS, que soportan la mayoría de distribuidores.
11. Presentación de los datos recolectados en forma de gráficos.
12. Generación de informes de rendimiento.
13. Definición de umbrales para el disparo de alarmas.
14. Gestión de los acuerdos de nivel de servicio, cuando estos acuerdos de nivel de servicio son incumplidos se disparan alarmas.
15. Descubrimiento de elementos en la red, dado un segmento de direcciones.
16. Utilización de mapas para visualizar la topología de la red.

**1.3.8.1.4.** ***LibreNMS:*** Es una herramienta de monitoreo de redes de datos de código abierto instalable distribuciones del sistema operativo Linux.

1. Sistema de monitorización de red escrito en PHP.
2. Es posible el autodescubrimiento de la red mediante SNMP.
3. Es fácilmente integrable con la infraestructura actual de la empresa, viene por defecto con soporte para una amplia gama de fabricantes de hardware (cisco, linux, juniper, etc.).
4. Puede recolectar gran cantidad de métricas, por ejemplo: uso de CPU, memoria, almacenamiento, tráfico de interfaz, estadísticas detalladas de paquetes, etc.

5. Posee paneles de control (dashboards) desde donde el usuario puede administrar el software.

6. Integración con otras herramientas por ejemplo: smokeping, syslog (registros de dispositivos), etc.

7. Se enfoca en la rápida configuración del monitoreo de la red.

8. Una de las grandes limitaciones de LibreNMS es que se limita a la monitorización solo siempre y cuando SNMP este habilitado.

9. Usa los protocolos Cisco Discovery Protocol (CDP) y Link Layer Discovery Protocol (LLDP) para el autodescubrimiento y la autoagregación.

#### 1.3.8.2. HERRAMIENTAS PARA LA EVALUACIÓN DE VULNERABILIDADES.

**1.3.8.2.1.** ***OpenVAS:*** Es una conjunto de herramientas especializadas integradas que permiten realizar actividades de escaneo y gestión de vulnerabilidades de seguridad de sistemas informáticos incluyendo equipos de redes de datos.

1. Es un gestor de vulnerabilidades de código abierto, totalmente de código abierto.

2. Proporciona un gran conjunto de características para el escaneo de vulnerabilidades, presenta esta información en informes detallados por host (dirección IP, puertos abiertos, nivel de severidad, soluciones sugeridas, el impacto negativo, etc.).

3. Control a través de un portal web (interfaz gráfica).

4. Varios modelos de reportes.

5. Establecimiento de horarios para el escaneo automático de vulnerabilidades.

6. Otorga ciber-resiliencia a la empresa, esto es que su proceso comercial pueda continuar en circunstancias cibernéticas adversas, greenbone ayuda a adquirir este estado con la identificación temprana de vulnerabilidades.

7. Greenbone tiene carácter proactivo, tiene como objeto cerrar vulnerabilidades que pueden ser explotadas por atacantes.

8. Comúnmente se implementa en conjunto con un firewall.

9. Tiene actualizaciones constantes y proporciona más de cien mil pruebas de vulnerabilidades y políticas de seguridad.

**1.3.8.2.2.** ***Nessus:*** Es una herramienta de escaneo de vulnerabilidades en diversos sistemas operativos.

1. Software extremadamente limitado en su versión gratuita, solamente permite el escaneo de 16 host.
2. Valoración y reparación automática de las vulnerabilidades (configuración errónea, programas maliciosos, actualizaciones, etc.)
3. Tiene un muy bajo índice de falsos positivos, apenas de 0,32 entre un millón de escaneos.
4. Tiene un gran número de clientes, alrededor de 30 mil organizaciones lo usan como gestor de vulnerabilidades.
5. Trabaja proactivamente con su comunidad, tiene constantes actualizaciones de nuevas vulnerabilidades y en los últimos tres años ha descubierto cien vulnerabilidades de día cero.
6. Es fácilmente desplegable en las organizaciones, debido a que ofrece cobertura para las principales marcas fabricantes de dispositivos de red, sistemas operativos, dispositivos móviles, aplicaciones, etc.

**1.3.8.2.3.** ***Nexpose:*** Es una herramienta de escaneo de vulnerabilidades comercial producida por Rapid7 y cuenta con las siguientes funcionalidades:

1. Calificación real de riesgos con base en la información de indicadores Common Vulnerability Scoring (CVSS) siendo posible caracterizar infraestructuras críticas.
2. Monitoreo continuo y la capacidad de realizar evaluaciones adaptativas de la infraestructura de manera pasiva mitigando así los efectos de vulnerabilidades de día cero[8].
3. Definición de políticas de aseguramiento con base en estándares como él National Institute of Standards and Technology NIST (NIST) o él Center for Internet Security (CIS).
4. Generación de reportes técnicos que permiten establecer acciones de aseguramiento y remedición de las vulnerabilidades detectadas, estos reportes condensan información de varias fuentes simplificando las acciones a realizar y los tiempos implicados.

[8] Las vulnerabilidades de día cero son aquellas para los cuales no existe parche de seguridad disponible, se las denomina de día cero, ya que indican que han pasado cero días desde que pudieron ser mitigadas.

#### 1.3.8.3. HERRAMIENTAS PARA LA SEGURIDAD DE RED

**1.3.8.3.1.** ***Suricata:*** Es un sistema de detección de intrusiones (IDS) y un sistema de prevención de intrusiones (IPS) de código abierto.

1. Es una herramienta de seguridad de red gratuita y código abierto.
2. Proporciona un sistema de detección de intrusos y un sistema de prevención de intrusos.
3. Es escalable.
4. Esta herramienta de seguridad balancea la carga, esta herramienta puede usar funciones multi-hilo, esto es que distribuye toda su carga de trabajo en el número de procesadores disponibles, gracias a esta característica puede procesar un ancho de banda de hasta 10 gigabits.
5. Gracias a poder manejar un gran ancho de banda puede controlar en tiempo real cualquier posible amenaza de programa malicioso.
6. Puede controlar el tráfico de internet, realiza una comprobación MD5 para comprobar que los archivos no hayan tenido cambios en su integridad.
7. Puede analizar los archivos en busca de programa malicioso escondido.

**1.3.8.3.2.** ***Snort:*** Es un sistema de detección de intrusos en red, libre y gratuito, que cuenta con la capacidad de almacenamiento de bitácoras en archivos de texto y en bases de datos abiertas, además de permitir detección de ataques y escaneo de puertos que permite registrar, alertar y responder anomalías previamente definidas.

1. Es una de las herramientas de seguridad de red de código abierto, más importantes del mundo.
2. A pesar de que es una herramienta gratuita, posee dos conjuntos de reglas, un conjunto de reglas de la comunidad completamente gratis, y un conjunto de reglas de subscriptor que son de pago.
3. Provee a la organización un sistema de prevención de intrusos, se basa en un conjunto de reglas que definen la actividad maliciosa en una red.
4. Es una herramienta en tiempo real, posee una gran cantidad de reglas predefinidas que detectan patrones de ataque, aprovechamientos de vulnerabilidades.

5. Snort puede vigilar, paquetes entrantes, paquetes salientes, atrás del firewall, afuera del firewall, en cualquier área critica que necesitemos.

6. Posee la funcionalidad de FlexResp, esto es que se comporta de manera similar a un firewall, cuando se detecta tráfico malicioso desde una conexión, Snort corta la conexión.

**1.3.8.3.3.** ***Zeek:*** Se trata de un monitor de seguridad de red (NSM), pero también puede utilizarse como sistema de detección de intrusiones en la red (NIDS) junto con un análisis adicional en vivo de los eventos de la red.

1. Zeek es una herramienta para la seguridad de red que provee un sistema de detección de intrusos IDS.

2. Monitorea y analiza todo el tráfico capturado por ejemplo: inicios de sesión, conexión a un número de puerto, etc.

3. Es un software de Código abierto.

4. Es altamente adaptable, es posible el establecimiento de políticas de monitorización de manera específica a través de scripts.

5. Es efectivo en redes de alto rendimiento.

6. Es muy flexible, puede cambiar de enfoque rápidamente para la detección de amenazas.

7. Se puede usar para el análisis forense, registra todo lo que analiza en archivos de registro.

8. Es capaz de realizar análisis en profundidad, tiene una gran pila de protocolos por defecto.

**1.3.8.3.4.** ***Security Onion:*** Es una distribución de Linux que viene con varias herramientas forenses, IDS y NSM preinstaladas.

1. Es una distribución de Linux que proporciona a la organización un sistema de detección de intrusos, monitoriza la seguridad de la red también realiza la gestión de archivos de registro.

2. Es una compilación de las herramientas anteriormente tratadas por ejemplo: snort, suricata, zeek, etc., herramientas de análisis de paquetes por ejemplo: wireshark,

networkminer, herramientas de gestión de archivos de registro por ejemplo: logstash, Kibana, etc.

3. Security Onion tiene como propósito la disposición de todo este conjunto de herramientas rápidamente, ya que la instalación e implementación son tareas bastante complicadas.

#### 1.3.8.4. HERRAMIENTAS PARA EL ANÁLISIS DE REGISTRO DE EVENTOS.

**1.3.8.4.1.** ***Splunk:*** Es una herramienta que captura, indexa y correlaciona los datos en tiempo real de registros de eventos en un repositorio con capacidad de búsqueda, a partir del cual puede generar gráficos, informes, alertas, cuadros de mando y visualizaciones.

1. Es un capturador en tiempo real de los datos que se generan en una infraestructura tecnológica, incluyendo los historiales de registro de aplicaciones, servidores, portales web, máquinas virtuales, redes, sensores, equipos de telecomunicaciones, sistemas operativos, etc.

2. Splunk tiene un gran número de funcionalidades, más de 500, con las que se puede realizar el procesamiento y el análisis de los archivos de registro de eventos en la mayoría de los casos.

3. Tiene una interfaz amigable para que hasta los usuarios menos experimentados puedan ejecutar la generación de reportes y gráficos en lo que se puede ver de manera más informativa los resultados del análisis de los datos.

4. Posee alta disponibilidad y escalabilidad, se puede implementar en clústeres, también se puede hacer balanceo de carga.

5. Efectúa la correlación entre las distintas fuentes de datos.

**1.3.8.4.2.** ***Logtash:*** Es una herramienta para la administración de registros de eventos (logs) que se puede utilizar para recolectar, analizar (parsing) y guardar los logs para futuras búsquedas.

1. Es una herramienta de análisis de registro de eventos gratuita de código abierto.

2. Es parte de la solución ELK (ElasticSearch, Logstash y Kibana), ElasticSearch para la indexación de datos, Logstash para la recolección de archivos de registro y Kibana para visualizar los datos gráficamente.

3. Una de sus ventajas más apreciadas es que a pesar de ser una solución de código abierto es bastante fácil de instalar y desplegar.
4. Recibe actualizaciones constantes, tiene una comunidad muy robusta.
5. Ayuda a centralizar los archivos de registro de distintos servidores, esto lo hace una solución escalable, si hay un par de servidores cuyos archivos de registro necesitan ser gestionados se puede hacer con SSH y grep, pero si el número de servidores es mucho mayor esta manera no es sustentable.

**1.3.8.4.3.** ***Graylog:*** Es una herramienta que captura, almacena y permite la búsqueda y el análisis de registros de eventos en tiempo real contra terabytes de datos de máquina de cualquier componente en la infraestructura de TI y las aplicaciones.

1. Es una solución gratuita de código abierto para la gestión de registro de eventos.
2. Es una solución centralizada de los diferentes servicios que puede tener una organización.
3. En su análisis de datos, rastrea posibles amenazas en búsqueda de programas maliciosos, realiza un análisis en profundidad para encontrar respuestas al origen de los incidentes.
4. Tiene la capacidad de correlacionar los datos con distintas fuentes, con esto podemos llegar a localizar más rápido el origen de los problemas.
5. Es fácilmente adaptable a un SOC o NOC, con esto se conseguirá un incremento en la capacidad de aseguramiento de la solución. Graylog nos muestra la información en forma de gráficos para entender mejor las métricas y tendencias.
6. Es posible la generación de informes, en los cuales se visualizara las métricas y tendencias a lo largo del tiempo, esto permitirá asegurar el cumplimiento de las políticas de ciberseguridad de la organización.

**1.3.8.4.4.** ***Log-Analyzer:*** Es una herramienta de análisis de almacenamiento y análisis de registro de eventos de código abierto instalable en distribuciones Linux.

- ❒ Posee una interfaz web para syslog y permite realizar el análisis de los registros de eventos en la red de datos.
- ❒ Esta interfaz web no realiza la recolección de los datos, solo se enfoca en presentar los datos en una interfaz amigable para el usuario, los datos son recolectados por otro software, por ejemplo: syslogd, rsyslog, etc.

- ❒ Proporciona una navegación fácil en su interfaz, análisis de eventos de red en tiempo real, servicios de informes.

### 1.3.9. GESTIÓN DE LAS REDES DE DATOS Y SEGURIDAD EN EMPRESAS ELÉCTRICAS

El despliegue de redes de datos en el sector eléctrico está haciendo cada vez más significativo lo que ha hecho que las redes de datos que en especial importancia en el funcionamiento de estas empresas. La explotación y el mantenimiento de la infraestructura de redes de datos permitirá garantizar el aprovisionamiento del servicio de suministro eléctrico de acuerdo a estándares de calidad de servicios dispuestos por los organismos de control, por otro lado, la su utilización y por qué innovación en estos aspectos estancará el crecimiento de las redes eléctricas y degradará la provisión del servicio de suministro eléctrico afectando directamente a los indicadores de calidad.

Las nuevas redes de datos están conectadas directamente con las tecnologías operativas y vienen definidas por un amplio espectro de tecnologías y estándares adecuados al sector eléctrico, evolucionan de la mano con estos requerimientos y constituyen uno de los sistemas de apoyo esenciales en las empresas eléctricas modernas.

Para garantizar el normal funcionamiento de las redes de datos deben incluirse dentro de los procedimientos empresariales procesos de operación y mantenimiento que permiten garantizar la provisión de los servicios de transporte de datos entre los distintos datos de la Red eléctrica manteniendo rendimientos óptimos para los sistemas de control industrial. Estas actividades deben estar definidas de manera que se adecúan a los requerimientos empresariales y pueda ser medidas de acuerdo a métricas que garanticen su mejora continua. Dentro de las actividades de resaltar están la actualización de la infraestructura de los equipos de redes, actividades de aseguramiento y mitigación de vulnerabilidades, administración y gestión de activos. También se debe garantizar que la infraestructura de redes de datos pueda resistir a eventos catastróficos a fin de que en la movilización del personal técnico en estos escenarios sean mínimas sin afectar de manera considerable factores económicos en la gestión de las redes eléctricas.

### 1.3.10. ESTÁNDARES DE GESTIÓN DE LA SEGURIDAD DE REDES DE DATOS EN EMPRESAS ELÉCTRICAS

Las infraestructuras tecnológicas implicadas en los sistemas de automatización industrial de las empresas eléctricas constituyen en su conjunto infraestructuras críticas para el fun-

cionamiento de las sociedades. El aseguramiento de estas infraestructuras ha generado el desarrollo de varios estándares y procedimientos que buscan de manera continua y sistemática garantizar un nivel adecuado de seguridad para esta infraestructura crítica. Este nivel de seguridad incluye aspectos técnicos asociados a las contramedidas tecnológicas, mecanismos criptograma picos, mecanismos de autenticación e identificación, mecanismos de control de acceso y autorización o de los mismos sistemas de detección y prevención de intrusos. En la definición del nivel de seguridad también se debe incluir los aspectos directivos y organizativos, los mismos que están relacionados con las personas y los procesos empresariales, como la organización funcional, sus objetivos y su estrategia, y es en referencia a la gestión empresarial. Finalmente, se cuenta con los aspectos de gobernanza y políticas, los cuales son los aspectos en lo más alto de la gestión del aseguramiento de la infraestructura, relacionados con el desarrollo, establecimiento de aplicación de políticas de seguridad empresariales.

Dentro de los estándares técnicos destaca la normativa de la *Critical Infrastructure Protection (CIP)* de la *North American Electric Reliability Corporation (NERC)*, la cual se centra principalmente en la definición de los requerimientos obligatorios a cumplir para el aseguramiento de las infraestructuras de las empresas eléctricas. Para las infraestructuras críticas deben establecerse en las siguientes políticas de seguridad: concienciar y entrenar al personal técnico, delimitar el perímetro de seguridad, establecer controles de seguridad física, implementar políticas de gestión de la seguridad de los sistemas informáticos, generar procesos de respuesta a incidentes, generar planes de recuperación y continuidad del negocio, generar procesos de gestión de la configuración de los equipos y evaluación de vulnerabilidades establecer mecanismos de protección de la información y finalmente identificar Situaciones excepcionales sobre la infraestructura crítica.

Otra norma aplicable a la gestión de la seguridad en empresas eléctricas es la IEC 62443-2-1 *Industrial communication networks -Network and system security -Part 2-1:*, la cual busca establecer un programa de seguridad de los sistemas de control y automatización industrial, describiendo los componentes fundamentales de la gestión de la seguridad, dentro de los cuales destacan el análisis de riesgos, el tratamiento de riesgos y el seguimiento y mejor que los sistemas de gestión de la seguridad.

La NIST SP 800-82 *Guide to Industrial Control Systems (ICS) Security (Revision 2)* aborda una nueva perspectiva sobre los elementos de los sistemas de gestión de la seguridad enfocados en los sistemas de control industrial. Como base de la gestión de la seguridad se distinguen las siguientes actividades: desarrollar el giro del negocio fortaleciendo los aspectos de seguridad, crear y formar equipos inter funcionales que permitan fortalecer los frentes de acción de la seguridad empresarial, definir las hojas de ruta y alcances de las actividades para la mejora de la gestión de la seguridad, definir las políticas y procedimien-

tos específicos para los sistemas de control industrial, implementar marcos de gestión de riesgos e impartir formación a fin de sensibilizar al personal sobre la gestión e importancia de la seguridad de la infraestructura tecnológica.

La NIST íntegra una norma específica para el aseguramiento de la Red eléctrica inteligente incluyendo definiciones interfaces lógicas hacen los sistemas analizados, la identificación de los requisitos asociados, la aplicación de estos criterios en fases posteriores, y ciertas actividades entre las cuales destacan: identificar las funciones empresariales, determinar la misión y los procesos empresariales en donde intervenga la Red eléctrica inteligente, inventariar los sistemas activos críticos de las redes inteligente, asignar a los sistemas de las redes eléctricas inteligentes las características adecuadas en las interfaces lógicas, identificar los requisitos de seguridad de alto nivel y realizar una evaluación de las deficiencias del cumplimiento de los requisitos definidos de manera macro, finalmente desarrollar un plan correctivo que permitan mitigar las deficiencias del cumplimiento de los requerimientos de alto nivel definidos en los puntos anteriores, esta actividad debe ir acompañada de la supervisión y fiscalización del cumplimiento de estos requisitos de seguridad sobre la Red eléctrica inteligente.

# 2. METODOLOGÍA

## 2.1. DISEÑO

La solución tecnológica implementada en este trabajo de titulación se desplegó usando como marco de referencia para la definición del diseño a implementar se ha tomado las fases del proceso de diseño de ingeniería [35]. En el proceso de diseño de ingeniería destacan las siguientes actividades: investigar los antecedentes e información base, definir los requisitos con los que debe cumplir el diseño, analizar las posibles soluciones y escoger la que mejor se adapte a las especificaciones definidas en los requisitos.

El levantamiento de la información base se desarrolló por medio de visitas técnicas a los distintos sitios y nodos de la Red WAN. Con la información recabada en estas visitas técnicas se desarrollaron diagramas para su despliegue en las herramientas de gestión de la infraestructura. Luego de realizar esta actividad se analizaron y definieron las herramientas a instalar y utilizar para el despliegue de la solución técnica diseñada. Las herramientas escogidas fueron las que mejor se adaptaron a los requerimientos definidos por el personal técnico de la E.E.Q. Finalmente se dimensionaron los servidores donde se instalarán las herramientas de gestión y administración de los equipos de redes y se definieron protocolos de pruebas de la solución diseñada. En la sección final de este capítulo se resumen los criterios y detalles del diseño realizado previo su implementación.

### 2.1.1. DOCUMENTO DE REQUERIMIENTOS Y FUNCIONALIDADES CON EL PERSONAL TÉCNICO DE LA E.E.Q.

Una vez definida una línea base en cuanto a los equipos que formarán parte de la infraestructura tecnológica hacer gestionado y monitoreada con la solución propuesta en este trabajo de titulación, el siguiente paso es definir los requerimientos que esta solución cumplirá. Cómo requerimientos de ser considerados en la implementación de esta solución se tienen los siguientes:

1. Se deberá contar con la posibilidad de manejar accesos remotos a través de los protocolos telnet y SSH.
2. La solución deberá garantizar la capacidad de recuperar la información de los equipos que sean compatibles con el protocolo SNMP. Para aquellos equipos que cuenten con versiones antiguas de este protocolo se deberá garantizar la operatividad de los

equipos terminales sobre la integración de estos a la solución del monitoreo, es decir en caso de qué haya, inconvenientes en la integración de los equipos terminales prevalecerá la operatividad y funcionalidad de estos equipos, como alternativa a esta integración se deberá utilizar el protocolo ICMP.

3. Toda la información recuperada por medio del protocolo SNMP deberá presentarse de manera gráfica, la solución implementada deberá contar con la facilidad de desarrollar diagramas de redes de datos, dicha simbología deberá disponer de las capacidades de generar de manera gráfica alertas es decir en caso de caídas de Red o cambios de estado se deberá contar con la capacidad de visualizar estos eventos en el diagrama de Red.

4. Adicional a la información recuperada vía protocolo SNMP, los equipos que cuenten con la capacidad de emitir mensajes vía protocolo Syslog deberán ser integrados a la solución tecnológica y dicha información deberá ser presentada de manera gráfica. Los mensajes generados vía protocolo Syslog en una base de datos consolidada que permita su procesamiento y filtrado de manera gráfica.

5. Se deberán considerar como situaciones críticas la pérdida de Red de los equipos terminales. Eventos que no impliquen la pérdida de Red de los equipos terminales deberán considerarse como alarmas informativas.

6. Todos aquellos eventos en donde los equipos terminales pierdan acceso a la Red de datos deberán ser emitidos por medio de la generación de alertas tempranas. Estas alertas tempranas deberán ser enviadas por medio de correos electrónicos hacia los administradores de las redes de datos.

7. De manera conjunta en las actividades de gestión la solución desplegada deberá contar con la facilidad de analizar e identificar vulnerabilidades en la seguridad de la infraestructura instalada. Estas vulnerabilidades deberán ser presentadas a manera de reporte para su posterior análisis y mitigación.

### 2.1.2. VISITAS TÉCNICAS PARA LEVANTAMIENTO DE INFORMACIÓN

Cómo primer paso para conocer y documentar la infraestructura que se integrará a la solución tecnológica a desplegar se hicieron visitas técnicas a los distintos sitios (subestaciones, centrales de generación, centros de datos, etc.). En estas visitas se documentó el listado de equipos instalados de manera gráfica y con diagramas de Red. En los diagramas de red se identificaron de manera clara los equipos terminales y los equipos de redes de datos además de los medios de transmisión y ya sean estos de fibra óptica o cobre. Los sitios visitados fueron los siguientes:

1. Subestación Olimpico
2. Subestación Luluncoto
3. Subestación Barrionuevo
4. Subestación Chimbacalle
5. Subestación Chilibulo
6. Subestación Escuela Sucre
7. Subestación San Roque
8. Subestación La Marín
9. Subestación Miraflores
10. Subestación Diez Vieja
11. Subestación Belisario Quevedo
12. Subestación La Floresta
13. Subestación Grande Centeno
14. Subestación Gualo
15. Subestación El Bosque
16. Subestación Rio Coca
17. Subestación Andalucía
18. Subestación Cristiania
19. Subestación Cotocollao
20. Subestación Sur
21. Subestación Epiclachima
22. Subestación San Antonio
23. Subestación Conocoto
24. Subestación Carolina
25. Subestación San Pablo
26. Subestación Alangasi
27. Subestación San Rafael
28. Subestación Iñaquito
29. Subestación Cumbaya
30. Subestación Plataforma Financiera
31. Subestación Tababela
32. Subestación Diez Nueva
33. Subestación Aeropuerto
34. Subestación Machachi
35. Subestación Tumbaco
36. Subestación Santa Rosa
37. Subestación Norte
38. Subestación Vicentina
39. Subestación Selva Alegre
40. Subestación Papallacta Movil
41. Subestación Machachi Movil
42. Subestación Inga Bajo
43. Subestación Los Bancos
44. Subestación Pérez Guerrero
45. Subestación Sangolqui
46. Subestación Pomasqui
47. Subestación El Quinche
48. Subestación Eugenio Espejo
49. Subestación El Labrador
50. Subestación Movil Pifo
51. Subestación El Obraje
52. Subestación Estación Terrena

53. Subestación Guangopolo Térmica
54. Subestación Guangopolo Hidráulica
55. Subestación HCJB Pifo
56. Central de Generación Nayón
57. Central de Generación Cumbaya

Los diagramas y documentación fotográfica resultado de esta actividad se presentan en los anexos de este trabajo de titulación. Se hace hincapié en que esta documentación fue levantada la fecha previa el despliegue de las herramientas de gestión por lo que se considera como referencial. Existe la posibilidad que durante el despliegue de las herramientas de gestión y monitoreo de la infraestructura existen actualizaciones e instalaciones del nuevo equipamiento en los diferentes nodos de la E.E.Q.


**(a)** Ubicación geográfica de las subestaciones

**(b)** Ubicación geográfica de los nodos de repetición y reconectadores

**Figura 2.1:** Ubicaciones geográficas de los nodos visitados para la realización de levantamiento de información.

### 2.1.3. ELABORACIÓN DE INVENTARIO DE EQUIPOS A INTEGRAR A LA SOLUCIÓN DE GESTIÓN

Luego de las visitas realizadas adicionales a la información levantada se consolidó también la documentación de la cual se disponía al interno de la E.E.Q. En esta documentación se disponía de listados de equipos y direcciones IP asignada cuyas denominaciones estaban ligadas completamente a terminología de ingeniería eléctrica, dificultando que pueden ser identificados de manera clara en la red de datos. Con el objetivo de clarificar el tipo de equipos, denominación, ubicación, sitio de instalación, y tipo de equipos se desarrolló un inventario integral con toda esta información, el mismo que se incluye en los anexos de este trabajo de titulación.

En la denominación de los equipos se identificó de manera clara la ubicación de estos es decir a qué subestación, central de generación, centro de datos o de ser el caso cámara de soterramiento pertenece. De igual manera, en la denominación se puede identificar el

sitio de instalación y el tipo de equipo. En el inventario realizado también se incluyeron los equipos de radiocomunicaciones como parte del acceso inalámbrico de los sistemas industriales de automatización de la distribución. En la sección de anexos consta el detalle del inventario realizado, tal como se muestra en la Figura 2.2.

**ANEXO B: INVENTARIO DE EQUIPOS A INTEGRAR EN LA SOLUCIÓN NSOC**

**Tabla 5.1:** Inventario de Equipos de Redes de Datos

| SUBESTACIÓN | NOMBRE |
|---|---|
| SE 01 Norte-Olimpico | OL-01-SW-BORDE-01-COMMS |
| SE 01 Norte-Olimpico | OL-01-SW-01-COMMS |
| SE 01 Norte-Olimpico | OL-01-SW-02-COMMS |
| SE 01 Norte-Olimpico | OL-01-SW-03-COMMS |
| SE 01 Norte-Olimpico | OL-01-SW-04-COMMS |
| SE 01 Norte-Olimpico | OL-01-SW-05-COMMS |
| SE 03 Barrio Nuevo | BN-03-SW-BORDE-01-COMMS |
| SE 03 Barrio Nuevo | BN-03-SW-01-COMMS |
| SE 03 Barrio Nuevo | BN-03-SW-02-COMMS |
| SE 04 Chimbacalle | CH-04-SW-BORDE-01-COMMS |
| SE 04 Chimbacalle | CH-04-ROFW-01-COMMS |
| SE 04 Chimbacalle | CH-04-SW-01-COMMS |
| SE 04 Chimbacalle | CH-04-SW-02-COMMS |
| SE 04 Chimbacalle | CH-04-SW-03-COMMS |
| SE 05 Chilibulo | CL-05-SW-BORDE-01-COMMS |
| SE 05 Chilibulo | CL-05-ROFW-01-COMMS |
| SE 05 Chilibulo | CL-05-SW-01-COMMS |
| SE 05 Chilibulo | CL-05-SW-02-COMMS |
| SE 05 Chilibulo | CL-05-SW-03-COMMS |
| SE 05 Chilibulo | CL-05-SW-04-COMMS |
| SE 05 Chilibulo | CL-05-SW-05-COMMS |
| SE 05 Chilibulo | CL-05-SW-06-COMMS |
| SE 05 Chilibulo | CL-05-SW-07-COMMS |
| SE 05 Chilibulo | CL-05-SW-08-COMMS |
| SE 06 Escuela Sucre | ES-06-ROFW-01-COMMS |
| SE 06 Escuela Sucre | ES-06-SW-01-COMMS |
| SE 06 Escuela Sucre | ES-06-SW-02-COMMS |
| SE 06 Escuela Sucre | ES-06-SW-03-COMMS |
| SE 07 San Roque | RQ-07-ROFW-01-COMMS |
| SE 07 San Roque | RQ-07-SW-01-COMMS |
| SE 07 San Roque | RQ-07-SW-02-COMMS |
| SE 07 San Roque | RQ-07-SW-03-COMMS |
| SE 08 La Marin | LM-08-ROFW-01-COMMS |
| SE 08 La Marin | LM-08-SW-01-COMMS |
| SE 08 La Marin | LM-08-SW-02-COMMS |
| SE 08 La Marin | LM-08-SW-03-COMMS |
| SE 08 La Marin | LM-08-SW-04-COMMS |
| SE 08 La Marin | LM-08-SW-05-COMMS |

CONTINÚA EN LA PÁGINA SIGUIENTE

**Figura 2.2:** Detalle de inventario realizado, adjunto en la sección de anexos

Con el levantamiento realizado y el inventario de equipos disponible, el siguiente paso fue la elaboración de los diagramas de red que serían cargados a la herramienta de monitoreo de red. En la sección de anexos consta el detalle del inventario realizado, tal como se muestra en la Figura 2.3.

## ANEXO C: DIAGRAMAS DE RED

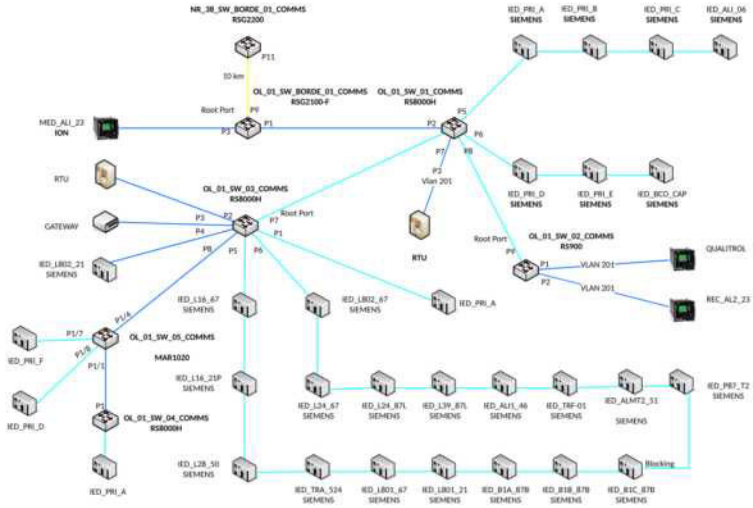


**Figura 5.42:** Subestación 01 Olímpico

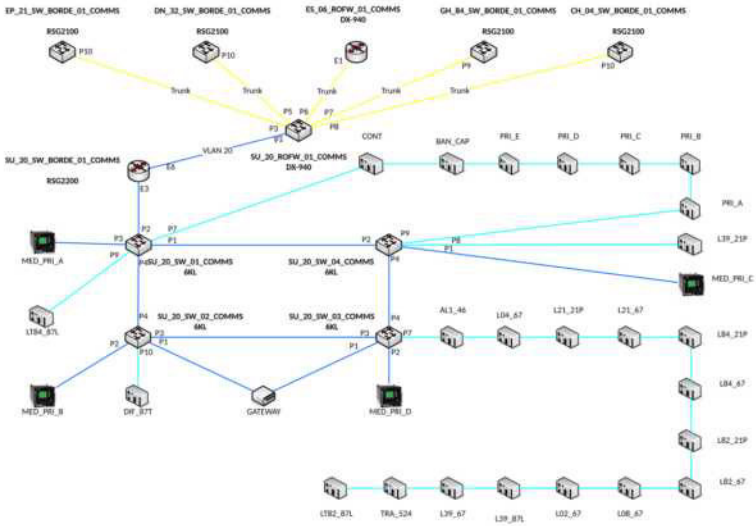


**Figura 5.43:** Subestación 02 Luluncoto

**Figura 2.3:** Detalle de diagramas de redes realizados, adjuntos en la sección de anexos

### 2.1.4. ESTUDIO DE LAS CARACTERÍSTICAS TÉCNICAS DE LOS EQUIPOS A INTEGRAR

En esta sección se presenta un estudio detallado de los protocolos de gestión disponibles en los equipos de redes y equipos terminales que se integrarán y analizarán con la solución tecnológica desarrollada en este trabajo de titulación. Este estudio abarca: routers, switches, firewalls, unidades remotas de control (RTU), equipos electrónicos inteligentes

(IED) y equipos de radioenlaces. En cada una de las siguientes secciones se adjuntan tablas resumen de las características de los equipos analizados listando los protocolos de gestión disponibles en estos equipos.

#### 2.1.4.1. Routers

En la Empresa Eléctrica Quito (E.E.Q.) se encuentran instalados los routers mostrados en la Figura 2.4 y en la Tabla 2.1 se presenta un resumen de los protocolos de gestión disponibles en estos equipos.

**(a)** Garretcom DX940e

**(b)** Ruggedcom 1500x

**(c)** Hirschmann MACH102-8TP

**(d)** Cisco 1800x

**Figura 2.4:** Routers instalados en la infraestructura industrial de la E.E.Q.

**Tabla 2.1:** Routers instalados en la Empresa Eléctrica Quito

| MARCA | MODELO | PROTOCOLOS DE GESTIÓN DISPONIBLES |
|---|---|---|
| Garretcom | DX940e | ICMP, SNMP MIB II, SNMP Traps, Web-based Graphical User Interface (GUI), SSH, TELNET |
| Ruggedcom | 1500X | Web-based, SSH, SNMP v1/v2/v3, NETCONF, Remote Syslog |
| Hirschmann | EAGLE 30 | SSH, web interface, SNMP v2/v3 |
| Cisco | 1841 | SSH, SNMP v2/v3, ICMP, syslog |

### 2.1.4.2. Switches

En la Empresa Eléctrica Quito (E.E.Q.) se encuentran instalados los switches mostrados en la Figura 2.5 y en la Tabla 2.2 se presenta un resumen de los protocolos de gestión disponibles en estos equipos.

**(a)** Cisco Nexus 9300

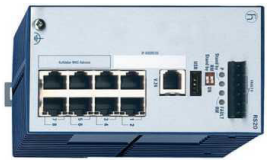
**(b)** Cisco SG30052

**(c)** Cisco 2960X

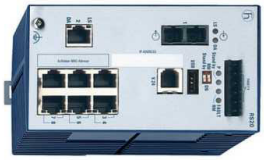

**(d)** Garretcom Magnum 6KL

**(e)** Hirschmann MACH1020

**(f)** Hirschmann MACH1028



**(g)** Hirschmann RS20



**(h)** Hirschmann RS200-800M

**(i)** Hirschmann RS3024

**(j)** Ruggedcom RS940G

**(k)** Ruggedcom RS8000H

**(l)** Ruggedcom RS900

**Figura 2.5:** Switches instalados en la infraestructura industrial de la E.E.Q.

**Tabla 2.2:** Switches instalados en la infraestructura industrial de la E.E.Q.

| MARCA | MODELO | PROTOCOLOS DE GESTIÓN DISPONIBLES |
|---|---|---|
| Cisco | Nexus 9300 | SSH, SNMP v2/v3, ICMP, syslog |
| Cisco | SG30052 | SSH, SNMP v2/v3, ICMP, syslog |
| Cisco | 2960X | SSH, SNMP v2/v3, ICMP, syslog |
| Garretcom | Magnum 6KL | ICMP, SNMP MIB II, SNMP Traps, Web-based Graphical User Interface (GUI), SSH, TELNET |
| Hirschmann | MACH1020 | SSH, web interface, SNMP v2/v3 |
| Hirschmann | MACH1028 | SSH, web interface, SNMP v2/v3 |
| Hirschmann | RS20 | SSH, web interface, SNMP v2/v3 |
| Hirschmann | RS200-800M | SSH, web interface, SNMP v2/v3 |
| Hirschmann | RS3024 | SSH, web interface, SNMP v2/v3 |
| Ruggedcom | RS940G | Web-based, SSH, SNMP v1/v2/v3, NETCONF, Syslog |
| Ruggedcom | RS800H | Web-based, SSH, SNMP v1/v2/v3, NETCONF, Syslog |
| Ruggedcom | RS900 | Web-based, SSH, SNMP v1/v2/v3, NETCONF, Syslog |

### 2.1.4.3. Firewalls

En la Empresa Eléctrica Quito (E.E.Q.) se encuentran instalados los firewalls mostrados en la Figura 2.6 y en la Tabla 2.3 se presenta un resumen de los protocolos de gestión disponibles en estos equipos.

**(a)** Fortigate 300E **(b)** Fortianalyzer 200F

**Figura 2.6:** Firewalls Fortinet instalados en la infraestructura industrial de la E.E.Q.

**Tabla 2.3:** Firewalls instalados en la Empresa Eléctrica Quito

| MARCA | MODELO | PROTOCOLOS DE GESTIÓN DISPONIBLES |
|---|---|---|
| Fortinet | Fortigate 300e | SSH, SNMP v2/v3, ICMP, syslog |
| Fortinet | Fortianalyzer 200F | SSH, SNMP v2/v3, ICMP, syslog |

### 2.1.4.4. Dispositivos Electrónicos Inteligentes

En la Empresa Eléctrica Quito (E.E.Q.) se encuentran instaladas las IED's mostradas en la Figura 2.7 y en la Tabla 2.4 se presenta un resumen de los protocolos de gestión disponibles en estos equipos.

**(a)** ABB REC650

**(b)** ABB REF615

**(c)** ABB RET670

**(d)** GE F60

**(e)** INGEPAC EF BD

**(f)** MICOM C264

**(g)** SIPROTEC 7SA

**Figura 2.7:** Switches instalados en la infraestructura industrial de la E.E.Q.

**Tabla 2.4:** IEDs instalados en la Empresa Eléctrica Quito

| MARCA | MODELO | PROTOCOLOS DE GESTIÓN DISPONIBLES |
|---|---|---|
| ABB | REC650 | WEB SERVER, ICMP |
| ABB | REF615 | WEB SERVER, ICMP |
| ABB | RET670 | WEB SERVER, ICMP |
| GE | F60 | WEB SERVER, ICMP |
| INGETEAM | EF BD | WEB SERVER, ICMP |
| SCHNEIDER | C264 | WEB SERVER, ICMP |
| SIEMENS | 7SA | WEB SERVER, ICMP |

### 2.1.4.5. Unidades Terminales Remotas

En la Empresa Eléctrica Quito (E.E.Q.) se encuentran instaladas las RTU's mostradas en la Figura 2.8 y en la Tabla 2.5 se presenta un resumen de los protocolos de gestión disponibles en estos equipos.

**(a)** Gateway Cooper

**(b)** Elliop 5000

**(c)** Kalkitech

**(d)** Novatech

**(e)** Ormazabal

**(f)** Scheneider Saitel

**(g)** Siemens SICAM

**Figura 2.8:** RTUs instaladas en la infraestructura industrial de la E.E.Q.

**Tabla 2.5:** RTU's en la infraestructura industrial de la E.E.Q.

| MARCA | MODELO | PROTOCOLOS DE GESTIÓN DISPONIBLES |
|---|---|---|
| COOPER | SG-4250 | SYSLOG UDP/IP, SYSLOG TCP/IP, ICMP, CEF TCP/I |
| ELLIOP | 5000 | SYSLOG UDP/IP, SYSLOG TCP/IP, ICMP, CEF TCP/I |
| KALKITECH | SYNC3000 | SYSLOG UDP/IP, SYSLOG TCP/IP, ICMP, CEF TCP/I |
| NOVATECH | Orion LX | AWEB SERVER, ICMP, SYSLOG |
| ORMAZABAL | EKOR UCT | WEB SERVER, ICMP, SYSLOG |
| SCHNEIDER | SAITEL DP | WEB SERVER, SNMP V2/V3, ICMP |
| SIEMENS | SICAM A8000 | SYSLOG, SNMP V3, ICMP |

### 2.1.4.6. Equipos de radioenlaces

En la Empresa Eléctrica Quito (E.E.Q.) se encuentran instalados los equipos de radioenlaces mostrados en la Figura 2.9 y en la Tabla 2.6 se presenta un resumen de los protocolos de gestión disponibles en estos equipos.

**(a)** Ubiquiti Nanostation 2

**(b)** Ubiquito Rocket M2

**(c)** Microhard IP2421B


**(d)** RedLine 5000

**Figura 2.9:** Equipos de redes inalámbricas en la infraestructura industrial de la E.E.Q.

**Tabla 2.6:** Características técnicas de los equipos de radioenlaces instalados

| MARCA | MODELO | PROTOCOLOS DE GESTIÓN DISPONIBLES |
|---|---|---|
| UBIQUITI | NANOSTATION 2 | Web Server, SNMP v1/v2, SSH Server, Telnet , Ping |
| UBIQUITI | ROCKET M2 | Web Server, SNMP v2/v3, SSH Server, Telnet , Ping |
| MICROHARD | IP2421B | Local Serial Port Console, Telnet, WebUI, SNMP |
| REDLINE | 5000 | ClearView NMS, HTTP, SNMP v2/v3, Telnet, serial |

### 2.1.5. SELECCIÓN DE PROTOCOLOS PARA EL MONITOREO Y GESTIÓN

Este trabajo de titulación aborda la gestión de equipamiento de índole industrial, estos equipos por su naturaleza presentan características que los diferencian de los equipos que tradicionalmente se manejan como parte de infraestructura tecnológica. Una de las características esenciales de estos equipos es el largo tiempo de vida útil el cual está estimado de entre 15 a 20 años. Esto dificulta la gestión de dicho equipamiento y, ya que tienden a verse discontinuados tecnológicamente. De manera general a fin de garantizar la compatibilidad en el manejo de estos equipos se consideraron como herramientas de gestión los siguientes protocolos: telnet, SSH, SNMP, ICMP, SYSLOG, dichos protocolos están disponibles según el estudio realizado en la sección anterior. En las siguientes secciones se describen brevemente las características de estos protocolos, sus funciones y principales usos.

#### 2.1.5.1. Teletype Network- Telnet

Telnet es un protocolo de terminal virtual, definido en el RFC 854, el cual permite abrir sesiones y ejecutar comandos en hosts remotos. Durante muchos años este protocolo fue el método por el que los clientes accedían a sistemas multiusuario como mainframes y minicomputadores. También fue el método de conexión preferido para los sistemas UNIX. Hoy en día, Telnet sigue siendo utilizado para acceder a los enrutadores y otros dispositivos de red administrables a través de conexiones que operan por defecto en el puerto 23/tcp.

Uno de los problemas de Telnet es que no es seguro, todo el transporte de la información se realiza de manera transparente, sin encriptación. Como mejora a esta característica surgió el protocolo Secure SHell (SSH).

#### 2.1.5.2. Secure Shell - SSH

El protocolo Secure SHell (SSH) fue creado por estudiantes de la Universidad Tecnológica de Helsinki, funciona en el puerto 22/tcp. Este protocolo surgió como una alternativa segura a Telnet. SSH mejora la seguridad de la información al cifrar los datos cuando viajan entre sistemas. Esto dificulta la labor de los piratas informáticos que utilizan rastreadores de paquetes para poder capturar la información y acceder a ella. También proporciona sistemas de autenticación más robustos que Telnet, SSH1 y SSH2, siendo SSH2 la más segura. Las dos versiones son incompatibles, por lo que no es viable conectarse a terminales que trabajen con SSH2 desde clientes que solamente puedan generar conexiones en SSH1.

Aunque SSH, al igual que Telnet, se asocia principalmente con los sistemas UNIX y Linux,

existen implementaciones de SSH para todas las plataformas informáticas de uso común, incluyendo Windows y OS X. SSH es la tecnología base del Protocolo de Transferencia Segura de Archivos (SFTP).

#### 2.1.5.3. Simple Network Management Protocol - SNMP

El protocolo Simple Network Management Protocol (SNMP) en la actualidad se ha convertido en el estándar de facto de los protocolos de gestión de redes y servidores. Originalmente, este protocolo fue creado para gestionar nodos de red(servidores de red, enrutadores, conmutadores, servidores de red)[36].SNMP cuenta con 3 versiones de su implementación, la primera versión de SNMP (SNMPv1) y la versión 2c (SNMPv2c) están definidas por los siguientes elementos:

- **Gestor SNMP:** Un gestor SNMP ejecuta una aplicación de gestión de red denominada (Network Management System (NMS)).
- **Agente SNMP:** Un agente SNMP es un pequeño software que se ejecuta en un dispositivo gestionado.
- **Base de datos de gestión (MIB):** La información sobre los recursos y la actividad de un dispositivo gestionado se define por una serie de objetos. La estructura de estos objetos de gestión está definida por la MIB de un dispositivo gestionado.

En la Figura 2.10 se esquematiza el funcionamiento del protocolo SNMP en sus versiones v1 y v2c.

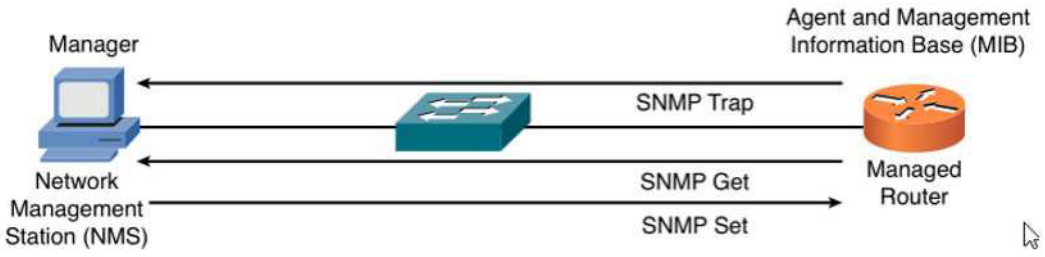



**Figura 2.10:** Componentes y mensajes de gestión de redes SNMPv1 y SNMPv2c

Las debilidades de seguridad de SNMPv1 y SNMPv2c se solucionaron con SNMPv3 con la puesta en marcha de los conceptos de modelos de seguridad y niveles de seguridad. Un modelo de seguridad define un enfoque para las autenticaciones de usuarios y grupos (por ejemplo, SNMPv1, SNMPv2c y SNMPv3). En tanto que el nivel de seguridad define el tipo de algoritmo de seguridad que se realiza sobre los paquetes SNMP en los paquetes SNMP. Existen 3 niveles de seguridad.

1. **noAuthNoPriv:** El nivel de seguridad noAuthNoPriv (sin autorización, sin privacidad) utiliza cadenas de comunidad para la autorización y no utiliza el cifrado para proporcionar privacidad.

2. **authNoPriv:** El nivel de seguridad authNoPriv (autorización, sin privacidad) proporciona autorización usando el código autenticado. El nivel de seguridad authNoPriv (autorización, sin privacidad) proporciona autorización empleando el código de autenticación de hash de mensajes (HMAC) con MD5 o el Algoritmo de Hash Seguro (SHA). No se emplea el cifrado.

3. **authPriv:** El nivel de seguridad authPriv (autorización, privacidad) proporciona HMAC MD5 o SHA y proporciona privacidad a través de la encriptación. En concreto, el cifrado emplea el estándar de cifrado de datos (DES).

Además de las mejoras de seguridad que se implementan en SNMPv3, este difiere arquitectónicamente de SNMPv1 y SNMPv2c, ya que en SNMPv3 se definen entidades SNMP, que son agrupaciones de componentes individuales de SNMP. Las aplicaciones SNMP y un gestor SNMP se combinan en una entidad SNMP NMS, mientras que un agente SNMP y una MIB se combinan en una entidad SNMP de nodo gestionado, estas interacciones se muestran en la Figura 2.11.

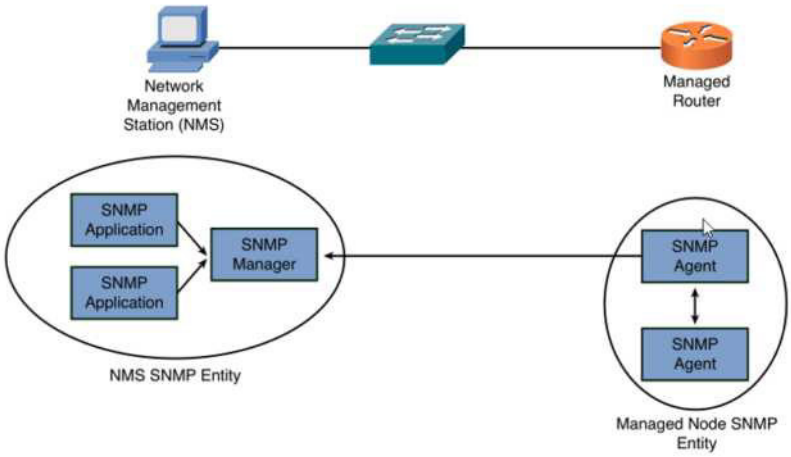



**Figura 2.11:** Entidades SNMPv3

#### 2.1.5.4. Internet Control Message Protocol - ICMP

El protocolo de mensajes de control de internet (ICMP) tiene como objetivo proporcionar la funcionalidad de comprobación e información de errores en la capa IP. Este protocolo está definido en el RFC Nro. 792[36].

El protocolo ICMP proporciona varias funciones entre las cuales están enviar un flujo de peticiones de echo ICMP a un host remoto, también conocida como la funcionalidad del ping. Si este host remoto puede responder, lo hace enviando un flujo de mensajes de respuesta echo hacia al host emisor. Mediante este sencillo proceso, ICMP permite verificar la configuración del conjunto de protocolos de los nodos emisores como de los receptores y de cualquier dispositivo de red intermedio.

Hay que destacar que la funcionalidad de ICMP no se limita al uso de la utilidad ping. ICMP también puede devolver mensajes de error como *"host de destino inalcanzable"* y *"Tiempo excedido"*. El primer mensaje se reporta cuando un host destino no puede alcanzarse y el segundo cuando se ha superado el tiempo de vida [TTL] de un datagrama.

ICMP también tiene la utilidad de *source quench*, eso ocurre cuando un host receptor no puede manejar la afluencia de datos al mismo ritmo que se envían los datos. Para reducir la velocidad del host emisor, el host receptor envía mensajes ICMP de supresión de origen, indicando al remitente que reduzca la velocidad. Esta acción evita que los paquetes se pierdan y tengan que ser reenviados[36].

#### 2.1.5.5. System Logging Protocol - SYSLOG

Syslog es un estándar que permite el registro de mensajes separando el software que genera los mensajes, el sistema que los almacena y el software que los informa y analiza. Cada mensaje generado se etiqueta con un código, que indica el tipo de sistema que generó el mensaje, al cual se le asigna un nivel de gravedad. Diversos componentes de la red (routers, switches y servidores) pueden enviar su información de registro a un servidor syslog común. Al tener información de varios dispositivos en un registro general y examinarlas a través del tiempo, los administradores de red pueden correlacionar mejor los eventos que ocurren en un dispositivo de red con los que ocurren en otro dispositivo de red. Los mensajes syslog y las traps SNMP pueden utilizarse para activar mensajes de notificación que pueden enviarse por correo electrónico o algún otro medio de notificación. Una solución de registro syslog consta de dos componentes principales:

- ❒ **Servidores syslog:** recibe y almacena los mensajes de registro enviados desde los clientes syslog.
- ❒ **Clientes syslog:** Un gran número de dispositivos de red pueden actuar como clientes syslog y enviar información de registro a un servidor syslog.

Existen ocho niveles de gravedad de los mensajes Syslog. Cuanto más alto sea el nivel de syslog más detallado es el registro, estos registros más detallados requieren mayor

almacenamiento en un servidor Syslog. En la Figura **??** se muestra una arquitectura básica cliente-servidor usando este protocolo.

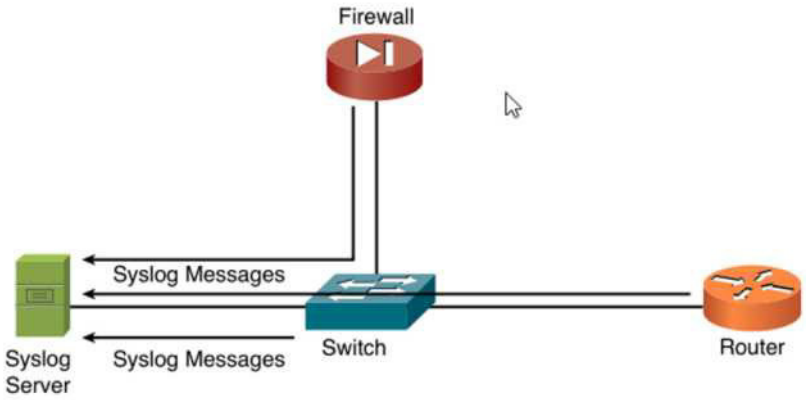



**Figura 2.12:** Arquitectura de cliente-servidor usando Syslog

### 2.1.6. DESARROLLO DE LOS PROCEDIMIENTOS DE GESTIÓN DE LA RED DE DATOS CON LOS PROTOCOLOS SELECCIONADOS

Una vez se disponga de la solución tecnológica diseñada, estas herramientas deberán permitir realizar las siguientes actividades:

- ❒ Recolectar información, ya sea a través del protocolo SNMP, Syslog o de ser el caso ICMP.
- ❒ Modificar la configuración, para esto deberán utilizarse los protocolos telnet o SSH.
- ❒ Generación de reportes, dichos reportes deberán generarse directamente desde las herramientas instaladas.
- ❒ Gestión de cambios, el histórico de cambios deberá documentarse directamente en las herramientas instaladas.

En cuanto a la gestión de la infraestructura tecnológica se deberá poder contar con las facilidades para la realización de los siguientes procesos:

- ❒ Permitir el acceso rápido a la información sobre configuraciones, incluyendo la información histórica de los cambios realizados sobre los equipos.
- ❒ Facilitar la configuración remota de los dispositivos, esto es a través del uso de los protocolos telnet o SSH.

- ❒ Proporcionar inventario actualizado de los componentes de la red, esta funcionalidad deberá ser directa y en medida de lo posible automatizada dentro de las herramientas instaladas.

Una vez descritas las actividades iniciales del proceso de gestión de la red de datos industrial y la seguridad de la infraestructura se definieron los siguientes conceptos: acuerdo de nivel de servicio, objetivos de nivel de servicio e indicadores de nivel de servicio.

- ❒ **Acuerdo de nivel de servicio:** Un acuerdo de nivel de servicio es un compromiso entre el proveedor y los clientes, donde se definen parámetros medibles como el tiempo de actividad del servicio, la capacidad de respuesta, tiempos permitidos de indisponibilidad y las responsabilidades del proveedor.
- ❒ **Objetivo del nivel de servicio:** El objetivo del nivel de servicio es un acuerdo descrito en función de los términos el acuerdo de nivel de servicio sobre una o varias métricas específicas, como por ejemplo el tiempo de indisponibilidad máximo permitido en determinados servicios.
- ❒ **Indicador del nivel de servicio:** Los indicadores de nivel de servicio son aquellas métricas que evalúan el cumplimiento de los objetivos del nivel de servicio. Para poder entender este concepto se tiene el siguiente ejemplo: el acuerdo de nivel de servicio especifica una disponibilidad de los servicios en el 99.95 % del tiempo, sobre este parámetro el objetivo del nivel de servicio indica que se buscará conseguir una disponibilidad cercana probablemente al 99.95 %, mientras que el indicador del nivel de servicio describe la medida real de la métrica, la cual podría estar entre el 99.96 % hasta un posible valor del 99.99 %. Para garantizar el cumplimiento del acuerdo de nivel de servicio el indicador de servicio deberá cumplir o superar las metas definidas en el objeto del nivel de servicio.

Para poder describir los indicadores del nivel de servicio se definieron las métricas de tiempo medio entre fallos tiempo medio de recuperación y disponibilidad según se muestra a continuación:

- ❒ **Tiempo medio entre fallos (MTBF):** El tiempo medio entre fallos es la media de tiempo entre fallos reparables de la infraestructura tecnológica que está siendo monitoreada. Para este trabajo de titulación este tiempo se medirá a través de la información adquirida en los equipos integrados a las herramientas de monitoreo por medio el protocolo ICMP o SNMP dependiendo el caso, este parámetro indica si el equipo está disponible o no (up/down).

- ❒ **Tiempo medio entre recuperación (MTTR):** Es la medida de tiempo que le toma a la red de datos tarda en recuperarse de un fallo o problemas de funcionamiento.
- ❒ **Disponibilidad:** Esta métrica mide la disponibilidad de los servicios en la red de datos considerando tiempo medio entre fallos y el tiempo medio entre recuperación ($D = (1 - (MTTR/MBTF)) \times 100\,\%$).

La disponibilidad deberá cumplir con los presupuestos de errores máximos permitidos. Según se describe en [37] se consideró un valor de disponibilidad del $99.5\,\%$ el cual corresponde a redes de datos con mecanismos de recuperación ante errores (arquitecturas redes de alta disponibilidad). Esta disponibilidad define un presupuesto de tiempos de indisponibilidad anual permitida de 4 horas, 22 minutos y 48 segundos.

Sobre los incidentes generados en el proceso de gestión de la red de datos es necesario definir también los niveles de impacto de los eventos, esta definición de acuerdo a las funcionalidades de la solución desplegada en este trabajo de titulación se describe a continuación:

- ❒ **Nivel alto:** Se considera un nivel alto de impacto a aquellos eventos que desconecten equipos terminales de control industrial, redes LAN o grandes segmentos de la red WAN de automatización industrial de la E.E.Q.
- ❒ **Nivel medio o Advertencia:** Se considera un nivel medio o de advertencia a aquellos eventos que generen intermitencias en la disponibilidad de acceso a los equipos terminales y redes LAN de los entornos industriales de la E.E.Q..
- ❒ **Nivel bajo o Información:** Se considera un nivel bajo o de información a aquellos eventos que indiquen cambios en los estados de los equipos de redes, los cuales no impacten en la continuidad del servicio de transporte de datos.

La solución tecnológica implementada en este programa proyecto de titulación interviene en el proceso de la Figura 2.13 habilitando las tareas de gestión de la red de datos con el uso de la herramienta Zabbix, recuperando la información de los equipos terminales con el uso de la herramienta LogAnalyzer y Zabbix, y finalmente evaluando el nivel de exposición y vulnerabilidades haciendo uso de la herramienta OpenVAS.

Teniendo en cuenta las actividades inicialmente descritas en esta sección y los conceptos preliminares el proceso de gestión propuesto para la red de datos de los sistemas industriales de la E.E.Q. se define en la Figura 2.13 y se describen de la siguiente manera:

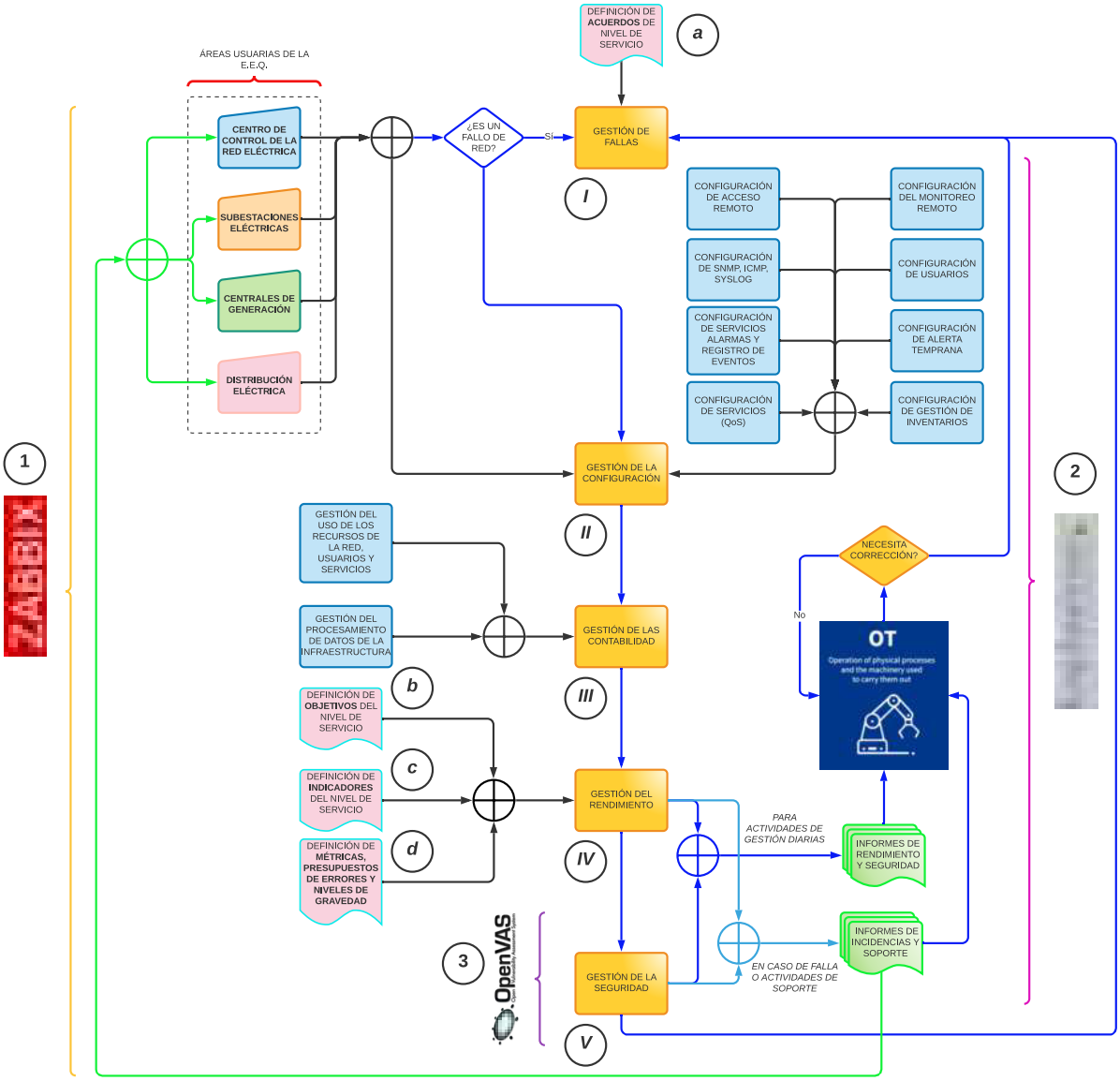



**Figura 2.13:** Proceso de gestión de redes y seguridad de la infraestructura industrial de la E.E.Q.

I El proceso de gestión inicia a través de los requerimientos de las áreas usuarias, las cuales son las siguientes: centro de control, personal técnico de subestaciones, personal técnico de centrales de generación y el personal técnico del área de distribución. Estas áreas usuarias definen los siguientes requerimientos: soporte ante fallos en la red de datos, reconfiguraciones de equipos, actualizaciones en la configuración, habilitación e integración de nuevos equipos de automatización, análisis de datos en el flujo de la información con herramientas de lectura de tráfico (sniffer de red). En situaciones en donde la red de datos no esté funcionando adecuadamente el siguiente paso dentro del proceso definido es la **gestión de fallas**. En caso de que no se trate de una falla, el siguiente paso será la **gestión de la configuración**.

a En la gestión de fallas deberán incluirse las definiciones del acuerdo de nivel

de servicio. En este acuerdo se deberán incluir las definiciones de tiempos de respuesta y responsabilidades sobre la continuidad del servicio del transporte de dato de los sistemas industriales.

II En la **gestión de configuración** se atenderán los requerimientos de las áreas usuarias y se incluirán también los procesos de configuración de acceso remoto a los equipos terminales, configuración de los protocolos de gestión de infraestructura, configuración de los servicios de alarmas y registros de eventos, configuración de la calidad de servicio (QoS) y diferenciación entre servicios, configuración del monitoreo remoto, configuración de los usuarios de administración de los equipos terminales, configuración de la metodología de alerta temprana y finalmente el proceso de configuración de la gestión de inventarios.

II El proceso de **gestión de la configuración** suministra los datos necesarios para la gestión de la contabilidad. En el proceso de **gestión de la contabilidad** se realizan registros del uso de los recursos de la red de datos de acuerdo a los servicios habilitados tales como: http, ssh, telnet, https, IEC104, DNP3, modbus, entre otros.

IV La gestión del rendimiento tiene como objetivo determinar la eficiencia de la red de datos en función de ciertas métricas tales como los objetivos del nivel de servicio, los indicadores del nivel de servicio, factores de disponibilidad, niveles de throughput, el porcentaje de utilización, las tasas de error y los tiempos de respuesta.

b Para la gestión de la red de la E.E.Q. se definió un objetivo de nivel de servicio de $99.5\,\%$.

c Para la gestión de la red de la E.E.Q. se definió un objetivo de nivel de servicio de $99.6\,\% - 99.99\,\%$

d Como métricas se definieron los conceptos de disponibilidad, tiempo medio entre fallos y tiempo medio de recuperación. Adicionalmente, se incluyeron definiciones de los presupuestos de errores en un máximo de 4 horas, 22 minutos y 48 segundos. Finalmente, se definieron los niveles de impacto en alto, medio y bajo.

V En la **gestión de la seguridad** se deberán realizar tareas de aseguramiento de los equipos de redes y equipos terminales de automatización industrial, eliminación de las configuraciones por defecto o de fábrica, actualizaciones de seguridad en los equipos terminales siempre y cuando estas actualizaciones no afecten al giro del negocio y a la continuidad de los procesos industriales. Adicionalmente, se deberán realizar también evaluaciones periódicas del nivel de exposición y grado de vulnerabilidad de la infraestructura tecnológica instalada.

Otro gran soporte al proceso de gestión de la seguridad son los lineamientos descritos por el marco de referencia del NIST. En este marco de referencia se listan como

principales 5 actividades siendo esta es las siguientes: identificación protección, detección, respuesta y recuperación.

La solución diseñada contribuye al proceso de identificación, ya que permite realizar una lista de todos los equipos que están conectados a la red de datos industrial. Sobre esta lista se pueden determinar las funciones y responsabilidades de los administradores que gestionan estos equipos, así como también los pasos de seguir para proteger dicha infraestructura.

Luego de la identificación está la protección en esta fase se delinean las políticas de seguridad definiéndose de esta manera quien accede a los equipos críticos, cómo se administran, gestión de la copia de seguridad en las configuraciones, y procesos de capacitación de la cultura de la seguridad sobre estos equipos.

La solución implementada contribuye en este proceso, ya que permite visualizar de manera integral la realidad datos y su comportamiento en cuanto a criterios de seguridad. Luego de la identificación y la protección hasta la fase de detección en la cual destacan los procesos de monitoreo continuo, revisión de la red de datos e investigación de cualquier actividad anormal (análisis de comportamiento).

Luego de la fase de detección se lista la de respuesta, en la cual se definen las políticas de notificación en las áreas usuarias, procesos de reporte de ataques, procesos de investigación e implementación de medidas de contención, mecanismos de mitigación para garantizar la continuidad del negocio, si es de requerirse actualización a las políticas de seguridad, y finalmente implementación de medidas de contención frente a futuros casos de similar naturaleza.

La solución tecnológica desplegada interactúa en cada una de estas fases permitiendo evaluar de manera directa el estado actual de la infraestructura facilitando así su gestión y mejores en cuanto a los niveles de seguridad. Como última fase está la de recuperación en la cual se delinean los procesos de reparación y restauración de los equipos que resultaron afectados en el ataque cibernético recibido sobre la infraestructura empresarial, en esta fase también se indica que se debe mantener informados a todos los empleados de la empresa así como a los clientes.

Luego de que se ha terminado el proceso de gestión de seguridad descrito en la Figura 2.13 sí incluyó además la generación de documentación entregable en formato informes tanto para el rendimiento como seguridad de la infraestructura tecnológica. También se incluyó informes de soporte técnico realizado sobre las incidencias reportadas en el funcionamiento de la red de datos y equipos terminales.

Como siguiente paso en la Figura 2.13, esta documentación será analizada por el grupo de trabajo técnico del NSOC, el cual para la E.E.Q. estará conformado por los técnicos de la

Unidad OT. Si en esta documentación se detecta la presencia de fallas en la red de datos el proceso inicia nuevamente con la gestión de las fallas reportadas en el informe.

Estos informes deberán remitirse también a las áreas usuarias como respaldo ante eventualidades y la generación de informes a los organismos de control del sector eléctrico[1].

### 2.1.7. SELECCIÓN DE HERRAMIENTAS A USAR

Los requisitos solicitados para el despliegue de la herramienta utilizada en la gestión de redes y análisis de seguridad de la infraestructura industrial de la Empresa Eléctrica Quito se basan principalmente en el uso de los protocolos SNMP, ICMP y SYSLOG. Estos protocolos disponen de un gran número de herramientas de tipo comercial y de código abierto las cuales permiten trabajar con los datos que estos generan, para poder definir las herramientas que se van a utilizar se consideraron las siguientes características:

- ❒ Nivel de popularidad y casos de éxito en implementaciones de monitoreo de infraestructura de equipos a gran escala, se consideró casos en donde el número de equipos superaban Las mil unidades.
- ❒ Practicidad y simpleza en la instalación, utilización, y actualización de los componentes instalados.
- ❒ Nivel de funcionalidades de la versión de código abierto de uso libre versus la versión de carácter comercial licenciada.
- ❒ Disponibilidad de personalización y ajustes en la integración de los equipos terminales de la infraestructura instalada.

Considerando las características anteriormente mencionadas las herramientas seleccionadas para desplegar la solución de gestión de redes y seguridad de este trabajo de titulación son las siguientes:

- ❒ Zabbix - The Enterprise-Class Open Source Network
- ❒ OpenVAS - Open Vulnerability Assessment Scanner
- ❒ LogAnalyzer&Report

[1] En el Ecuador existen 2 organismos de control del sector eléctrico: la Agencia de Regulación y Control de Energía y Recursos Naturales No Renovables (ARCERNNR) y Operador Nacional de Electricidad (CENACE)

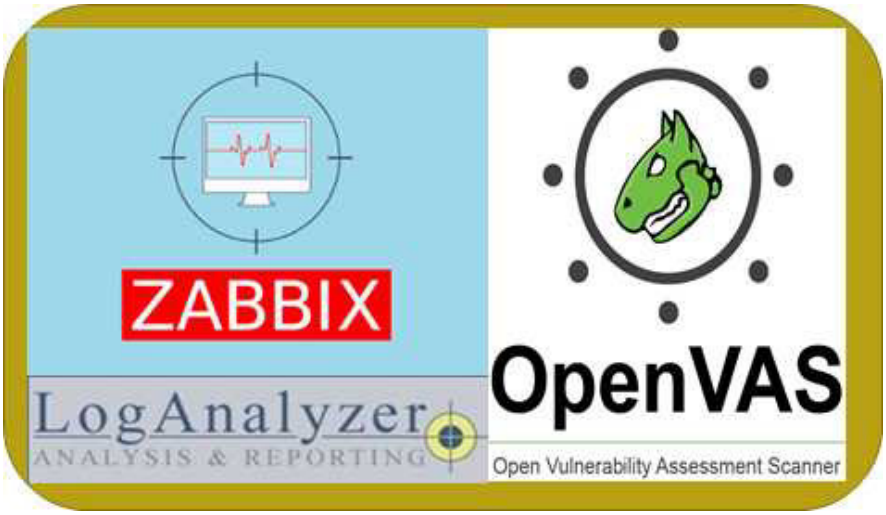



**Figura 2.14:** Solucion a implementar

### 2.1.8. PROTOCOLOS DE PRUEBAS DE LA SOLUCIÓN IMPLEMENTADA

La solución tecnológica diseñada para cubrir las necesidades de la Empresa Eléctrica Quito consta de varias herramientas de gestión de redes de datos, análisis de vulnerabilidades y registros de eventos, por tal motivo el protocolo de pruebas fue desarrollado en función de cada una de las funcionalidades disponibles en las herramientas instaladas.

#### 2.1.8.1. Prueba de funcionamiento de la solución instalada

Para probar el correcto funcionamiento de la solución instalada se realizarán los siguientes pasos:

1. Prueba de funcionamiento de la herramienta de monitoreo de redes de datos

   *a*) Chequeo del estado de archivo de logs del Servidor usando el comando: `servidor> more /var/log/syslog` con el objetivo de verificar que no existan errores de funcionamiento sobre la instalación realizada.

   *b*) Chequeo el estado del servicio del servidor Zabbix con el siguiente comando: `servidor> systemctl status zabbix-server`

   *c*) Chequeo el estado del servidor Apache con el siguiente comando: `servidor> systemctl status apache2`

   *d*) Chequeo el estado del servidor MySQL con el siguiente comando: `servidor> systemctl status mysql`

2. Prueba de funcionamiento de la herramienta de análisis de registros de eventos (logs)

*a*) Chequeo del estado de archivo de logs del Servidor usando el comando `servidor> more /var/log/syslog` con el objetivo de verificar que no existan errores de funcionamiento sobre la instalación realizada.

*b*) Chequeo del estado del servidor Apache con el siguiente comando:
`servidor> systemctl status apache2`

*c*) Chequeo del estado del servicio rsyslog con el siguiente comando:
`servidor> systemctl status rsyslog`

*d*) Chequeo del estado del servicio MySQL con el siguiente comando:
`servidor> systemctl status mysql`

*e*) Chequear que todos los prerequisitos de la herramienta estén correctamente instalados, con el siguiente comando: `servidor> dpkg -s php php-cli php-fpm php-json php-pdo php-mysql php-zip php-gd php-mbstring php-curl php-xml php-pear php-bcmath php-mysqli php-mysqli`

*f*) Chequear que el servicio PHP esté corriendo `servidor> php -v`

3. Prueba de funcionamiento de la herramienta de análisis de vulnerabilidades

   *a*) Chequeo del estado de archivo de registro de eventos (logs) del Servidor usando el comando `servidor>`
   `more /var/log/syslog` con el objetivo de verificar que no existan errores de funcionamiento sobre la instalación realizada.

   *b*) Chequeo del estado del servicio de la herramienta instalada con el siguiente comando `servidor> systemctl status greenbone-security-assistant.service`

#### 2.1.8.2. Prueba de funcionamiento de la integración de equipos a través del protocolo SNMP

Para probar el correcto funcionamiento de la integración de los equipos a la herramienta de monitoreo de redes a través del protocolo SNMP se realizarán los siguientes pasos:

1. Tomar lecturas de tráfico filtrando el puerto 161 hacia la dirección IP del servidor de la herramienta Zabbix

2. Comprobar la integración de los equipos a la herramienta Zabbix a través de la interfaz gráfica, en la configuración de integración de equipos.

3. Visualización de gráficas de las siguientes métricas:

   *a*) Disponibilidad del equipo (estado up/down)

*b*) Tiempos de repuesta en el protocolo ICMP

*c*) Porcentaje de pérdidas usando el protocolo ICMP

*d*) Curvas de valores de tráfico en las interfaces de red.

#### 2.1.8.3. Prueba de funcionamiento de la integración de equipos a través del protocolo ICMP

Para probar el correcto funcionamiento de la integración de los equipos a la herramienta de monitoreo de redes a través del protocolo ICMP se realizarán los siguientes pasos:

1. Tomar lecturas de tráfico filtrando protocolo ICMP hacia la dirección IP del servidor de la herramienta Zabbix
2. Comprobar la generación de datos en la herramienta Zabbix a través de la interfaz gráfica, en la configuración de integración de equipos a través del protocolo ICMP.
3. Visualización de gráficas de las siguientes métricas:
   *a*) Disponibilidad del equipo (estado up/down)
   *b*) Tiempos de repuesta en el protocolo ICMP
   *c*) Porcentaje de pérdidas usando el protocolo ICMP

#### 2.1.8.4. Prueba de funcionamiento de la integración de equipos a través del protocolo SYSLOG

Para probar el correcto funcionamiento de la integración de los equipos a la herramienta de monitoreo de redes a través del protocolo SYSLOG se realizarán los siguientes pasos:

1. Tomar lecturas de tráfico filtrando el puerto 512 hacia la dirección IP del servidor de la herramienta de análisis de registro de eventos (logs).
2. Comprobar la integración de los equipos a la herramienta de análisis de registro de eventos (logs), a través de la interfaz gráfica.
3. Visualización de gráficas de los mensajes recibidos, donde debe constar:
   *a*) Origen del mensaje recibido
   *b*) Nivel de severidad de la alarma recibida
   *c*) Texto descriptivo que detalle el error generado

#### 2.1.8.5. Prueba de funcionamiento de la generación de alarmas ante ataques sobre la red de datos

Para probar el correcto funcionamiento de la generación de alarmas ante posibles ataques de red se seguirá el siguiente protocolo:

1. Para la generación del ataque de red controlado se usarán las herramientas `hydra`.
2. A través del uso de la herramienta `hydra` en conjunto con los diccionarios `rockyou.txt.gz` se generarán intentos de intrusión fallos a través del uso de usuarios y contraseñas de prueba.
3. Para realizar las pruebas se usará el siguiente comando:
   *a*) Protocolo SSH: `servidor> hydra -L /usr/share/wordlists.rockyou.txt -P /usr/share/wordlists/rockyou.txt IP-SERVIDOR-ZABBIX -t 4 ssh`
   *b*) Protocolo telnet: `servidor> hydra -L /usr/share/wordlists/common-usernames -P /usr/share/wordlists/rockyou.txt IP-SERVIDOR-ZABBIX telnet`
4. Los mensajes generados serán recuperados a través del protocolo SYSLOG y visualizados en la interfaz de la herramienta instalada
5. En los mensajes recibidos se comprobará que se encuentre incluida la fecha y hora en la que fueron recibidos.

#### 2.1.8.6. Prueba de funcionamiento de las alarmas generadas en los equipos integrados

Para probar el correcto funcionamiento del monitoreo continuo del estado de los equipos de redes y automatización industrial, y de como estos generan alarmas ante posibles fallos se seguirá el siguiente protocolo:

1. El funcionamiento de la recepción y generación de alarmas se comprobará a través de las interfaces gráficas de las herramientas instaladas En el caso del protocolo SNMP, los mensajes recibidos dependerán de la marca y estructura de la MIB II, desde la cual se obtendrán los mensajes de alarma generados.
2. En este caso se analizarán únicamente las métricas de ICMP, estado, porcentaje de pérdida de paquetes, tiempos de respuesta y valores de tráfico en las interfaces de red.

3. Las alarmas deberán generar señales visuales de cambios de colores sobre los equipos monitoreados. Para casos de alarmas de nivel medio se deberán visualizar en color naranja, y para casos críticos en color rojo.

4. En el caso de la comprobación en la herramienta de análisis de logs, la comprobación se realizará a través de cambios generados en un ambiente controlado sobre la configuración del equipo, es decir, deberán generarse registros de cambios a través del protocolo SYSLOG.

#### 2.1.8.7. Prueba de funcionamiento de la generación de reportes

Para probar el correcto funcionamiento de la capacidad de la generación de reportes en las herramientas instaladas se seguirá el siguiente protocolo:

1. La generación de reportes deberá estar disponible en las herramientas instaladas.

2. En el caso de que sea posible, los reportes serán extraídos en formato PDF, de no ser así, podrán generarse en formatos alternativos como CSV o similares.

### 2.1.9. DIMENSIONAMIENTO DE SERVIDORES

Para el dimensionamiento de los servidores fueron considerados escenarios similares a los descritos en los sitios web oficiales adecuándolos a la situación actual de la infraestructura de la E.E.Q. Hay que tener en cuenta que para esta primera implementación no se disponía de información histórica que permita definir de mejor manera y con mayor precisión los recursos de hardware necesarios para el correcto funcionamiento de las herramientas a instalar. Dichas limitaciones se ven mitigadas teniendo en cuenta de qué todas las herramientas hacer desplegadas funcionarán en ambientes virtualizados, siendo posible de ser el caso posteriores actualizaciones de recursos una vez desplegadas las herramientas.

Para la definición de los requerimientos asignar en la creación de las máquinas virtuales para la instalación de las herramientas definidas dentro de la solución tecnológica a implementar ser considerado como base los requerimientos mínimos recomendados en cada uno de los sitios web oficiales. De ser el caso dependiendo de cada una de las herramientas estos requerimientos ha sido ampliados a necesidad y en referencia de levantamientos referencial de la infraestructura que fue realizado en las secciones anteriores.

#### 2.1.9.1. Herramienta Zabbix

En la página web oficial de la herramienta Zabbix[38] se indica que el parámetro principal de dimensionamiento es el número de equipos a monitorear. De levantamiento realizado usted tiene un paso por un límite de 1000 equipos terminales hacer monitoreados, para lo cual sé los siguientes recursos:

- ❒ **Procesamiento:** $4[vCPU]$
- ❒ **Memoria RAM:** $8[GB]$

De levantamiento base realizado se determinaron que existen más de 3000 hosts activos en los segmentos de red asignados a los sistemas de automatización industrial. Manteniendo las recomendaciones de la página web oficial se asignarán como recursos de procesamiento y memoria RAM los siguientes:

- ❒ **Procesamiento:** $10[vCPU]$
- ❒ **Memoria RAM:** $16[GB]$

Esta herramienta será instalada en un Sistema Operativo Linux Ubuntu, el cual necesita los siguientes recursos para funcionar:

- ❒ **Procesamiento:** $2[vCPU]$
- ❒ **Memoria RAM:** $2[GB]$
- ❒ **Almacenamiento:** $25[GB]$

De los recursos necesarios el dimensionamiento para la instalación de la herramienta Zabbix debe considerar al menos los siguientes recursos de hardware:

- ❒ **Procesamiento:** $8 + 2 = 10[vCPU]$
- ❒ **Memoria RAM:** $16 + 2 = 18[GB]$

Adicionalmente, se considera un espacio de almacenamiento de 250 GB en donde se alojará el sistema operativo, todos los prerrequisitos para el correcto funcionamiento de la herramienta y la información histórica recuperada de la infraestructura. Hay que tener en cuenta que se trata de una implementación piloto la cual deberá ser evaluada en el tiempo y readecuada en función de las necesidades y crecimiento de la Red de datos que se monitoreara.

#### 2.1.9.2. Herramienta OpenVAS

Para la herramienta OpenVAS con lo indicado en la página web oficial[39] se deben considerar como requerimientos mínimos de la solución los siguientes:

- ❒ **Procesamiento:** $10[vCPU]$
- ❒ **Memoria RAM:** $18[GB]$
- ❒ **Almacenamiento:** $16[GB]$

Para este caso en específico sea considerado como sistema operativo en anfitrión a Kali Linux, esto con el objetivo de aprovechar la compatibilidad entre el gran stock de herramientas devaluación de seguridad infraestructura tecnológica. Con esta consideración adicional los recursos asignados para la instalación de la herramienta son:

- ❒ **Procesamiento:** $4[vCPU]$
- ❒ **Memoria RAM:** $4[GB]$
- ❒ **Almacenamiento:** $200[GB]$

De los recursos necesarios el dimensionamiento para la instalación de la herramienta Zabbix debe considerar al menos los siguientes recursos de hardware:

- ❒ **Procesamiento:** $4 + 2 = 6[vCPU]$
- ❒ **Memoria RAM:** $6 + 8 = 14[GB]$

Adicionalmente, se considera un espacio de almacenamiento de 250 GB en donde se alojará el sistema operativo, todos los prerrequisitos para el correcto funcionamiento de la herramienta y la información histórica recuperada de la infraestructura. Hay que tener en cuenta que se trata de una implementación piloto la cual deberá ser evaluada en el tiempo y readecuada en función de las necesidades y crecimiento de la Red de datos que se monitoreara.

#### 2.1.9.3. Herramienta LogAnalyzer

La herramienta de análisis de registros de eventos LogAnalyzer de acuerdo lo indicado en la página web oficial[40] indica como requerimientos mínimos los siguientes:

- ❒ **Procesamiento:** 2 CPU cores
- ❒ **Memoria RAM:** 512 MB
- ❒ **Almacenamiento:** 16 GB

Esta herramienta será instalada en un Sistema Operativo Linux Ubuntu, el cual necesita los siguientes recursos para funcionar:

- ❒ **Procesamiento:** Procesador de doble núcleo de 2 GHz.
- ❒ **Memoria RAM:** 2 GB de RAM (memoria del sistema)
- ❒ **Almacenamiento:** 25 GB de espacio en el disco duro.

De los recursos necesarios el dimensionamiento para la instalación de la herramienta Zabbix debe considerar al menos los siguientes recursos de hardware:

- ❒ **Procesamiento:** $2 + 2 = 4[vCPU]$
- ❒ **Memoria RAM:** $0.512 + 2 = 2.512[GB] \approx 4[GB]$

Los requerimientos mínimos indicados para esta herramienta variará en función del uso y la información recibida de la infraestructura integrada para su monitoreo a través del protocolo Syslog. Como no se cuenta con valores referenciales en cuanto al crecimiento del almacenamiento de la información de la infraestructura que se integra en esta herramienta se asignarán al igual que las otras herramientas o un almacenamiento de 250 GB, se mantienen los Recursos de procesamiento de indicados y se amplía la Memoria RAM 4 GB.

## 2.2. IMPLEMENTACIÓN

En el presente capítulo se describe la implementación de la solución diseñada a partir de la instalación de la plataforma de hardware en donde se desplegaron los servidores de la solución tecnológica instalada. Se detalla el procedimiento de instalación de las herramientas de software y su utilización en el monitoreo y gestión de la infraestructura tecnológica industrial de la E.E.Q..

### 2.2.1. INSTALACIÓN DE LOS SERVIDORES VIRTUALIZADOS

La plataforma de hardware utilizada para la instalación de las herramientas informáticas de la solución diseñado fue ubicada en el Centro de Datos Iñaquito, su instalación se muestra en la Figura 2.15. Los recursos de hardware disponibles para la implementación fueron: un procesador AMD Ryzen 7 3800X de 8 núcleos y 16 hilos, además de 64 GB de memoria RAM según se muestra en la 2.15c.

Para el despliegue de las máquinas virtuales se utilizó Oracle VM VirtualBox, la cual se distribuye bajo licencia GPLv2[2]. Esta herramienta permite manejar infraestructuras de hasta 32 núcleos (cores), espacios de almacenamiento de hasta 2 TB, compatibilidad con hardware Intel y AMD, funciones de gestión como clonado completo de máquinas, múltiples resoluciones de pantalla para el acceso mediante escritorio remoto, soporte para dispositivos USB y es posible de instalar en sistemas operativos propietarios como Microsoft Windows, Mac OS y varias distribuciones Linux. En la Figura 2.15e se muestra una captura de la pantalla de la herramienta Virtualbox instalada y con las máquinas virtuales de los servidores instados en pleno funcionamiento, adicionalmente en la Figura 2.15f se muestra la conexión física del hardware de virtualización hacia la red de datos para acceder a los sistemas de automatización industrial de la E.E.Q.

[2] **GNU General Public License v2:** Licencia Pública General de GNU, la cual brinda el derecho de autor usado en el mundo del software libre y código abierto y garantiza a los usuarios finales la libertad de usar, estudiar, compartir (copiar) y modificar el software distribuido bajo esta licencia.

**(a)** CPU Vista posterior

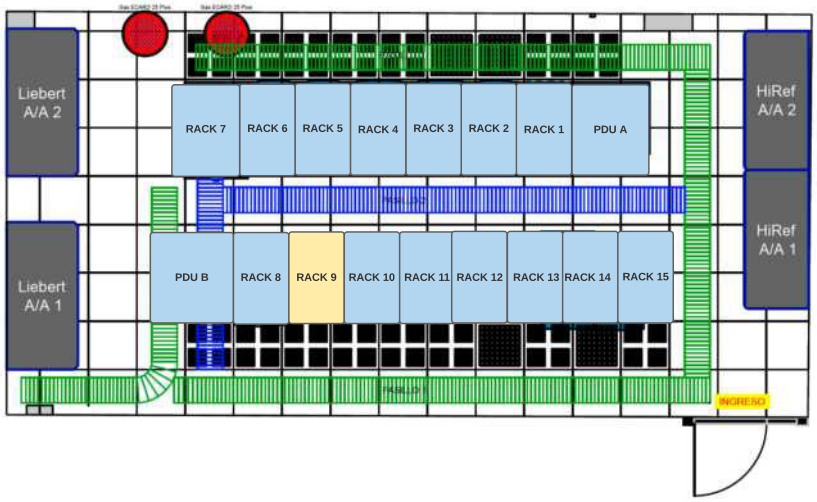
**(b)** CPU Vista frontal

Especificaciones del dispositivo

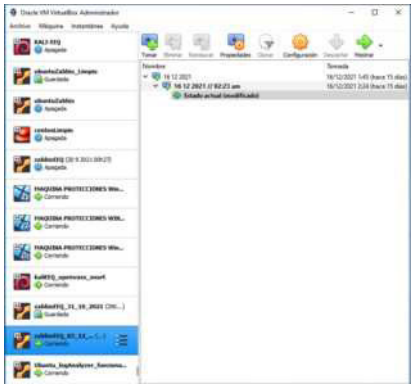
| | |
|---|---|
| Nombre del dispositivo | DESKTOP-FV8R0EI |
| Procesador | AMD Ryzen 7 3800X 8-Core Processor 3.89 GHz |
| RAM instalada | 64,0 GB |
| Id. del dispositivo | 6119CB00-AF76-4D5E-8FD2-8CF7FA4ACB37 |
| Id. del producto | 00330-81482-70959-AA451 |
| Tipo de sistema | Sistema operativo de 64 bits, procesador x64 |
| Lápiz y entrada táctil | La entrada táctil o manuscrita no está disponible para esta pantalla |

Copiar

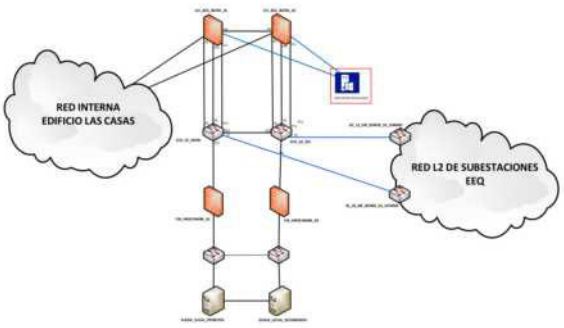
**(c)** Recursos de Hardware Disponibles




**(d)** Ubicación en el Centro de Datos Iñaquito



**(e)** Pantalla de la herramienta Oracle VM VirtualBox



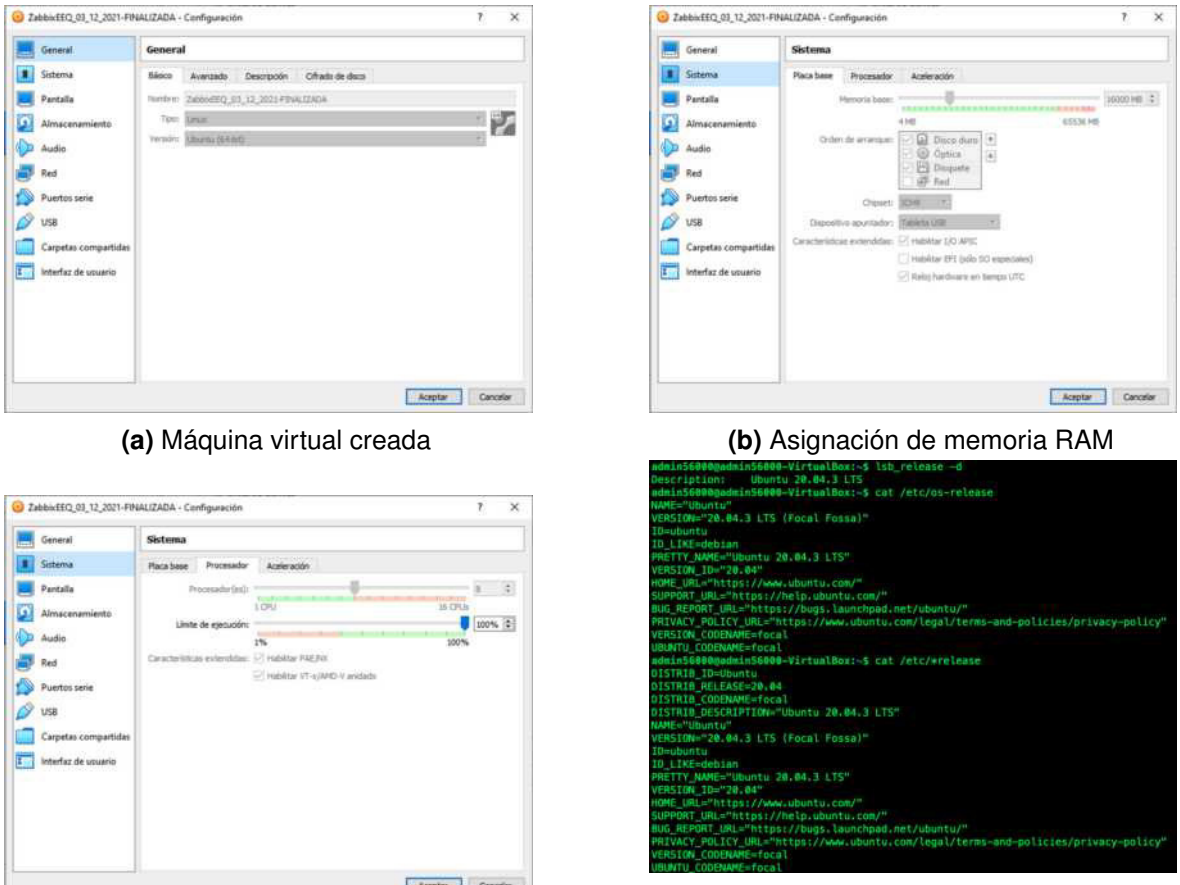

**(f)** Servidor Físico conectado a la red de datos

**Figura 2.15:** Plataforma de Hardware, instalación y conexión a la red de datos para el despliegue de las herramientas de software instaladas.

#### 2.2.1.1. Instalación de la herramienta Zabbix

En la presente sección se detalla el proceso de instalación de la herramienta Zabbix, la cual servirá de plataforma de monitoreo de la red de datos. El proceso de instalación inicia en la creación de la máquina virtual, asignación de memoria RAM, almacenamiento y los núcleos de procesamiento que se utilizarán. Esta herramienta fue instalada en el sistema operativo Ubuntu 20.04, todos estos detalles se muestran en la Figura 2.16.

1. Creación de la máquina para la instalación de la herramienta Zabbix.




**(a)** Máquina virtual creada

**(b)** Asignación de memoria RAM

**(c)** Asignación de núcleos de procesamiento

**(d)** Verificación del Sistema Operativo usado

**Figura 2.16:** Instalación de la herramienta Zabbix en una máquina virtual.

2. Descargar el instalador de la herramienta Zabbix para el sistema operativo Ubuntu 20.04.

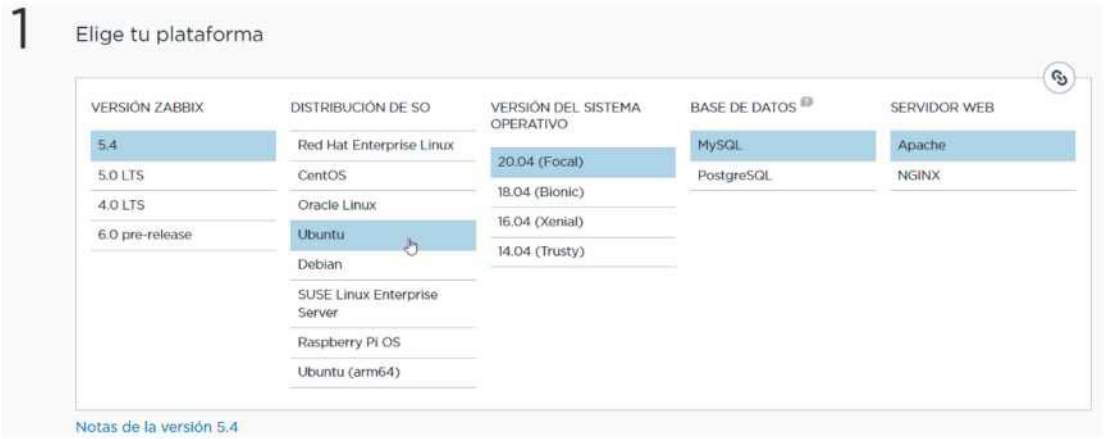



**Figura 2.17:** Descarga del instalador de la herramienta Zabbix desde el portal web oficial

3. Una vez seleccionado el instalador de acuerdo a la versión del sistema operativo, el cual se muestra en la Figura 2.17, aparecerá el listado de comandos a ejecutar en el proceso de instalación de la herramienta, dicho proceso inicia partir de la Figura 2.18 con la ejecución de los siguientes comandos:

   *a*) Descarga de archivos desde el repositorio oficial de la herramienta Zabbix.

**Código Fuente 2.1:** Descarga de repositorios de la herramienta Zabbix

```
1    wget https://repo.zabbix.com/zabbix/5.4/ubuntu/pool/main/
        z/zabbix-release/zabbix-release_5.4-1+ubuntu20.04_all.
        deb
```


**Figura 2.18:** Descarga de repositorios de la herramienta Zabbix.

   *b*) Instalación del paquete de repositorios de Zabbix.

**Código Fuente 2.2:** Instalación del paquete de repositorios de Zabbix

```
1    dpkg -i zabbix-release_5.4-1+ubuntu20.04_all.deb
```

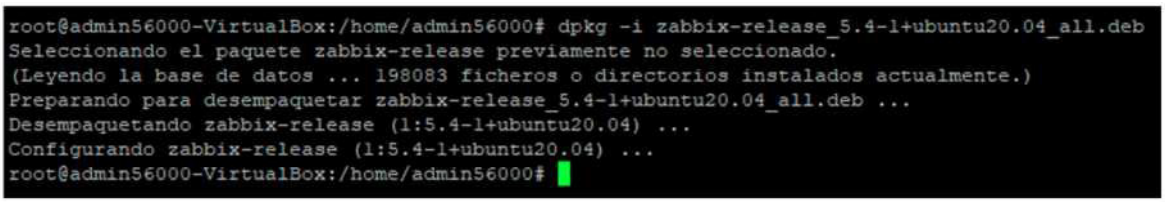



**Figura 2.19:** Instalación del paquete de repositorios de Zabbix.

*c*) Actualizar los repositorios

**Código Fuente 2.3:** Actualización de repositorios

```
1     apt update
```

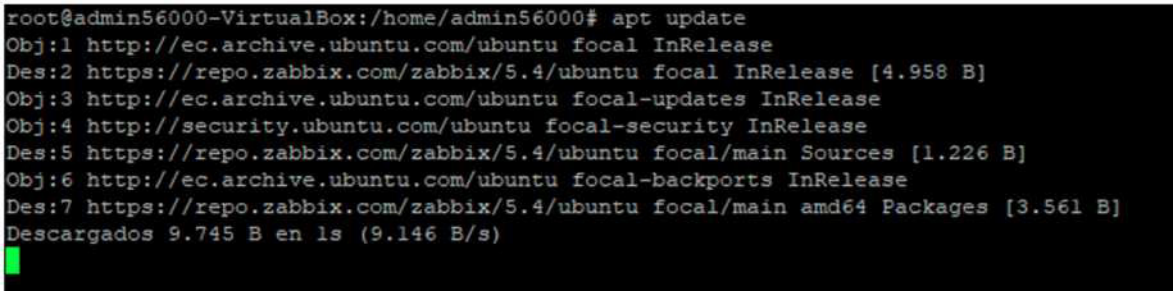



**Figura 2.20:** Actualización de repositorios.

*d*) Instalar el servidor de la herramienta, la interfaz web, el servidor web apache 2, y el agente de monitoreo.

**Código Fuente 2.4:** Instalación de prerequisitos de Zabbix

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


**Figura 2.21:** Instalación del servidor de la herramienta, la interfaz web, el servidor web apache 2, y el agente de monitoreo.

*e*) Instalar el servidor MySQL

**Código Fuente 2.5:** Instalación del servidor MySQL

```
1     sudo apt install mysql-server
```

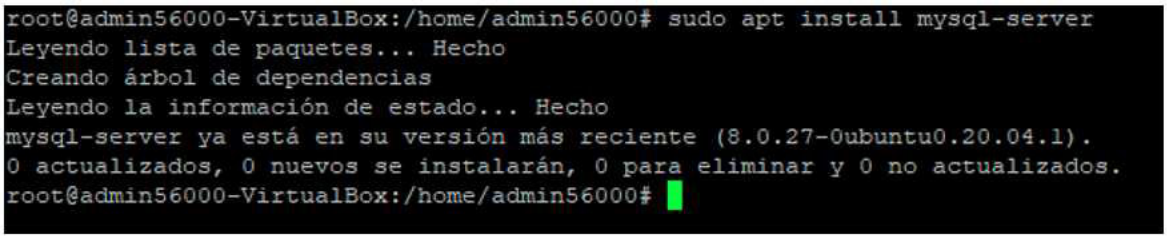



**Figura 2.22:** Instalación del servidor MySQL.

*f*) Verificar el estado del servidor MySQL.

**Código Fuente 2.6:** Verificación del estado del servidor MySQL

```
1    service mysql status
```

```
root@admin56000-VirtualBox:/home/admin56000# service mysql status
● mysql.service - MySQL Community Server
     Loaded: loaded (/lib/systemd/system/mysql.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2022-01-01 08:14:56 -05; 20min ago
   Main PID: 843 (mysqld)
     Status: "Server is operational"
      Tasks: 38 (limit: 4110)
     Memory: 566.3M
     CGroup: /system.slice/mysql.service
             └─843 /usr/sbin/mysqld

ene 01 08:14:52 admin56000-VirtualBox systemd[1]: Starting MySQL Community Server...
ene 01 08:14:56 admin56000-VirtualBox systemd[1]: Started MySQL Community Server.
root@admin56000-VirtualBox:/home/admin56000#
```

**Figura 2.23:** Verificación del estado del servidor MySQL.

*g*) Iniciar sesión en el servidor de base de datos MySQL.

**Código Fuente 2.7:** Inicio de sesión en el servidor MySQL

```
1    mysql -uroot -p
```

```
root@admin56000-VirtualBox:/home/admin56000# mysql -uroot -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 9
Server version: 8.0.27-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

**Figura 2.24:** Inicio de sesión en el servidor MySQL.

*h*) Crear la base de datos inicial, el usuario y contraseña para el servidor y otorgar los permisos necesarios

**Código Fuente 2.8:** Creación de la base de datos inicial

```
1    mysql> create database zabbix character set utf8 collate
         utf8_bin;
-    mysql> create user zabbix@localhost identified by '
         password';
-    mysql> grant all privileges on zabbix.* to
         zabbix@localhost;
-    mysql> quit;
```

```
mysql> create database zabbix character set utf8 collate utf8_bin;
Query OK, 1 row affected, 2 warnings (0,01 sec)

mysql> create user zabbix@localhost identified by 'password';
Query OK, 0 rows affected (0,01 sec)

mysql> grant all privileges on zabbix.* to zabbix@localhost;
Query OK, 0 rows affected (0,01 sec)

mysql> quit;
Bye
root@admin56000-VirtualBox:/home/admin56000#
```

**Figura 2.25:** Creación de la base de datos y asignación de permisos de usuario.

*i*) Importar al servidor MySQL el esquema inicial de la base de datos y establecer su contraseña.

**Código Fuente 2.9:** Importación de esquema y datos iniciales

```
1    zcat /usr/share/doc/zabbix-sql-scripts/mysql/create.sql.
        gz | mysql -uzabbix -p zabbix
```

```
root@admin56000-VirtualBox:/home/admin56000# zcat /usr/share/doc/zabbix-sql-scripts/mysql/create.sql.gz | mysql -uzabbix -p zabbix
Enter password:
root@admin56000-VirtualBox:/home/admin56000#
```

**Figura 2.26:** Importación de servidor MySQL y asignación de contraseña.

*j*) Colocar en el archivo de configuración del servidor, la contraseña de su base datos

**Código Fuente 2.10:** Configuración de credenciales en la base de datos

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

```
### Option: DBPassword
#       Database password.
#       Comment this line if no password is used.
#
# Mandatory: no
# Default:
DBPassword=tle2s3i4s5
```

**Figura 2.27:** Configuración de credenciales en la base de datos.

*k*) Configurar la zona horaria en el archivo de configuración PHP de apache 2.

**Código Fuente 2.11:** Configuración la zona horaria

```
1    nano /etc/zabbix/apache.conf
```

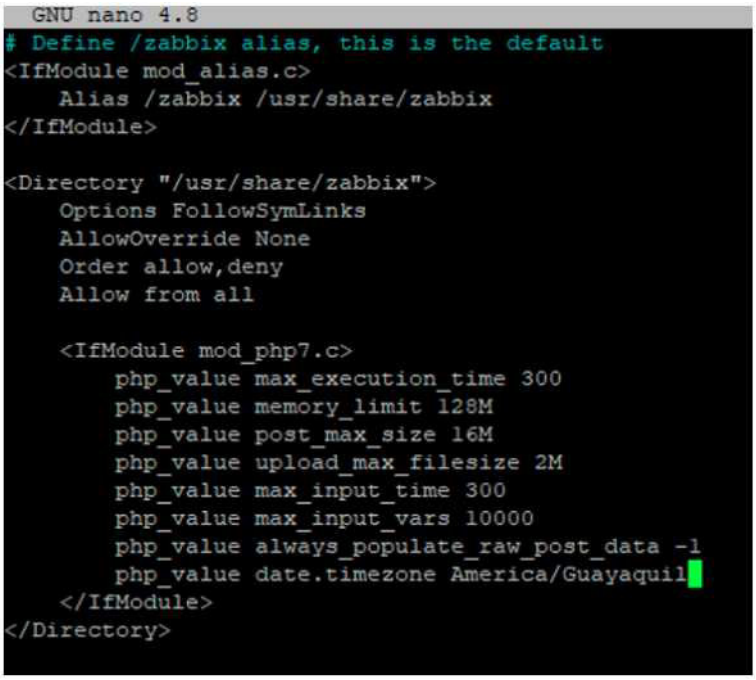



**Figura 2.28:** Configuración la zona horaria en el archivo de configuración PHP.

*l*) Reiniciar el servidor Zabbix, el agente Zabbix, el servidor apache 2 y establecer que estos tres servicios se carguen de manera automática en el inicio del sistema.

**Código Fuente 2.12:** Reinicio de servicios servidor zabbix y agente zabbix

```
1     systemctl restart zabbix-server zabbix-agent apache2
-     systemctl enable zabbix-server zabbix-agent apache2
```


**Figura 2.29:** Reinicio de servicios servidor zabbix y agente zabbix.

*m*) Definición de regla en el Firewall para el puerto 80.

**Código Fuente 2.13:** Definición de regla en el Firewall para el puerto 80

```
1     ufw allow 80/tcp
```


**Figura 2.30:** Definición de regla en el Firewall para el puerto 80.

4. Configuración inicial del servidor Zabbix desde su interfaz web.


**Figura 2.31:** Configuración inicial del servidor Zabbix desde su interfaz web.

5. Chequear el cumplimiento de los prerrequisitos.


**Figura 2.32:** Cumplimiento de los prerrequisitos.

6. Configurar la conexión a la base de datos

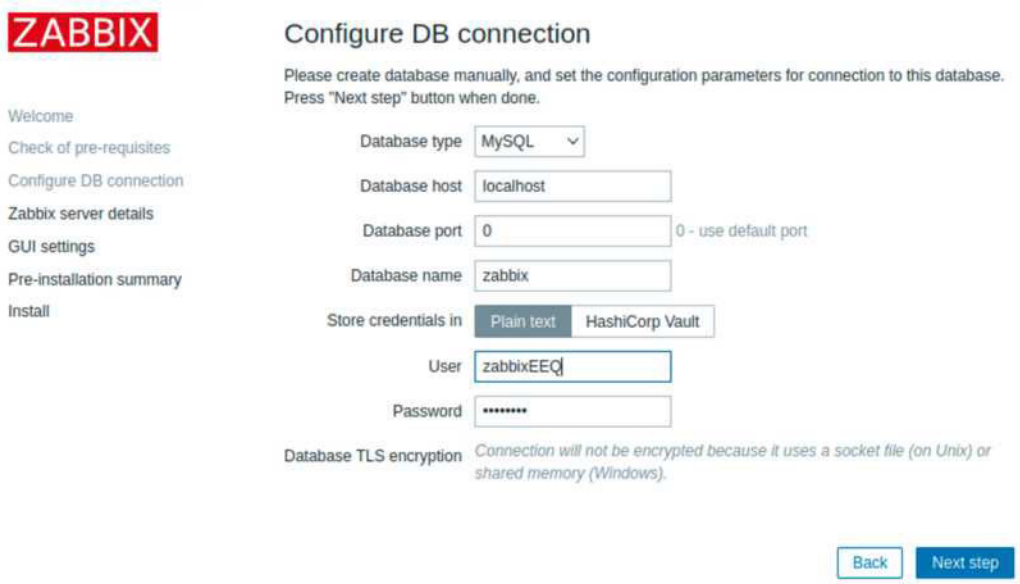



**Figura 2.33:** Configuración la conexión a la base de datos.

7. Configurar el nombre del servidor Zabbix.


**Figura 2.34:** Configuración del nombre del servidor Zabbix.

8. Definición del tema y la zona horaria en el servidor.

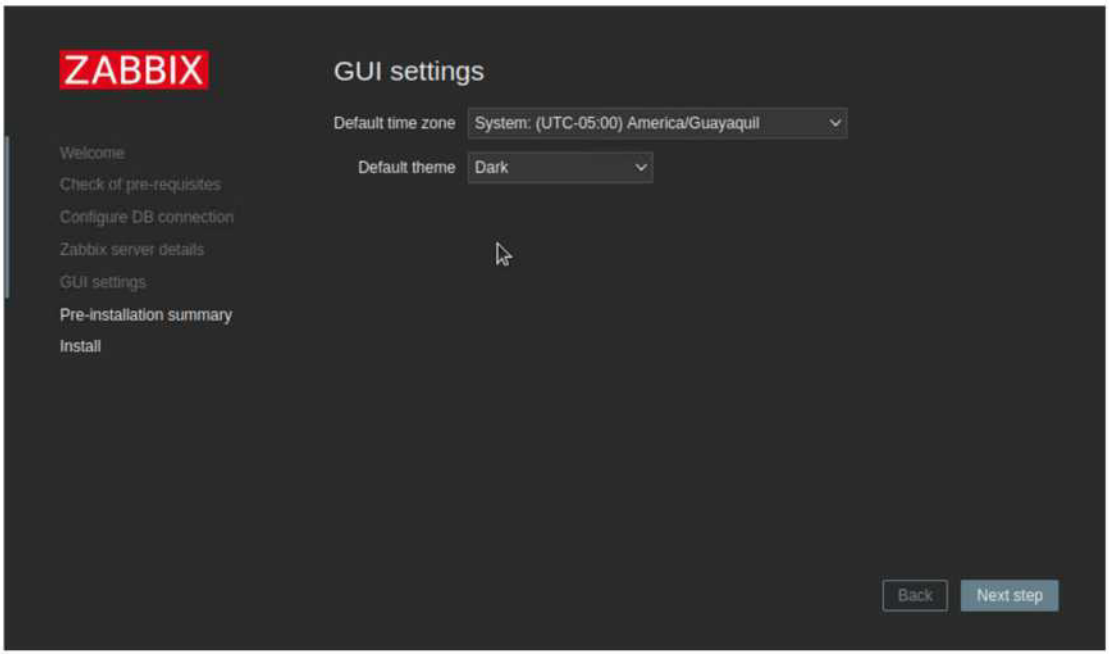



**Figura 2.35:** Definición del tema y la zona horaria en el servidor.

9. Resumen de la configuración inicial del servidor Zabbix

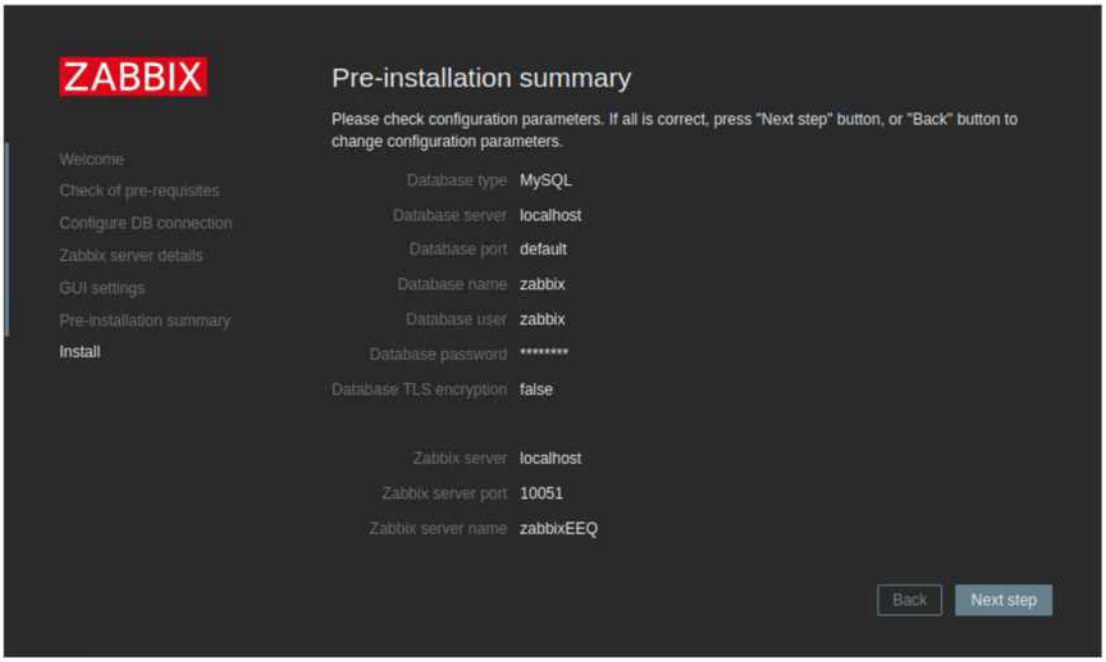



**Figura 2.36:** Ejecución `sudo apt install gvm`

10. Finalización la instalación.

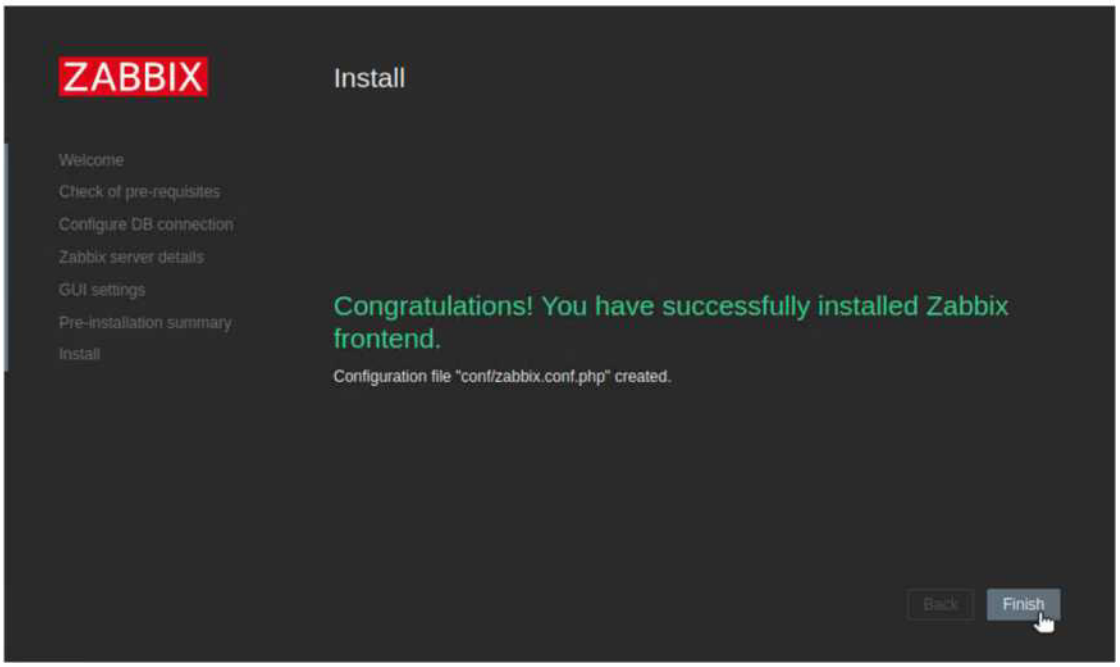



**Figura 2.37:** Finalización la instalación

11. Comprobación del ingreso al servidor Zabbix.

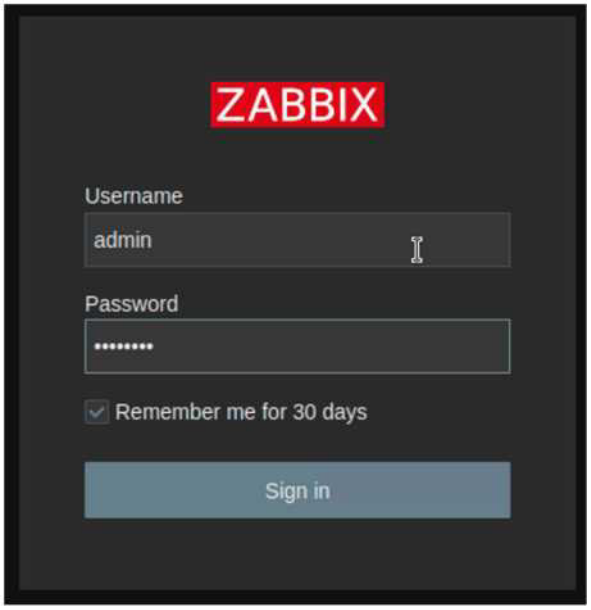



**Figura 2.38:** Ingreso al servidor Zabbix.

12. Página inicial del servidor Zabbix.

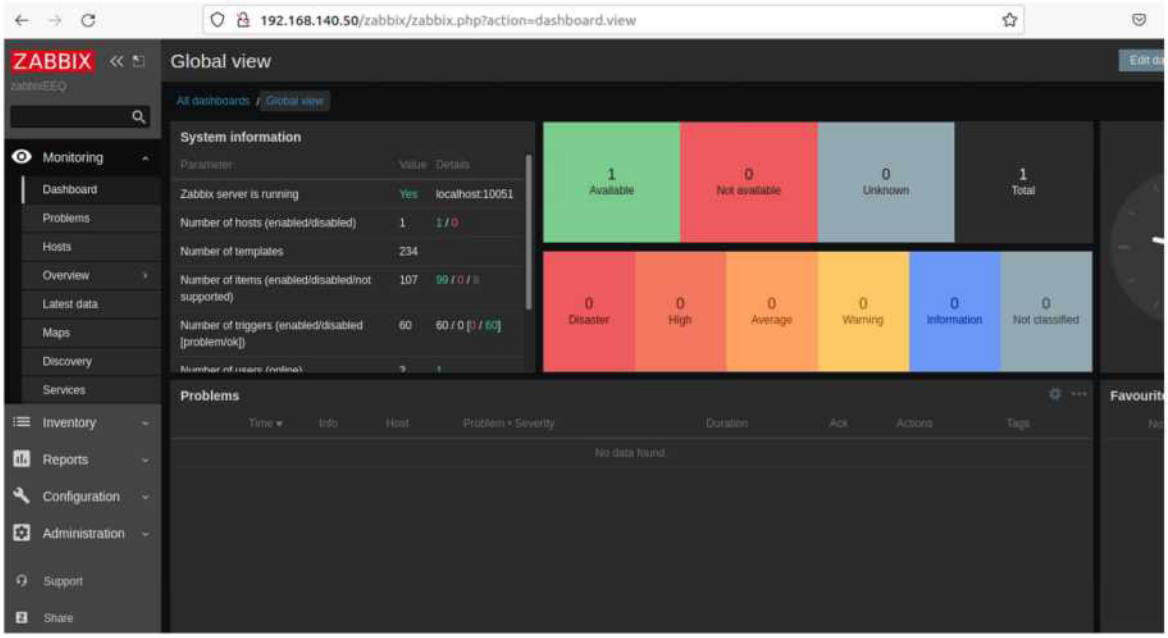
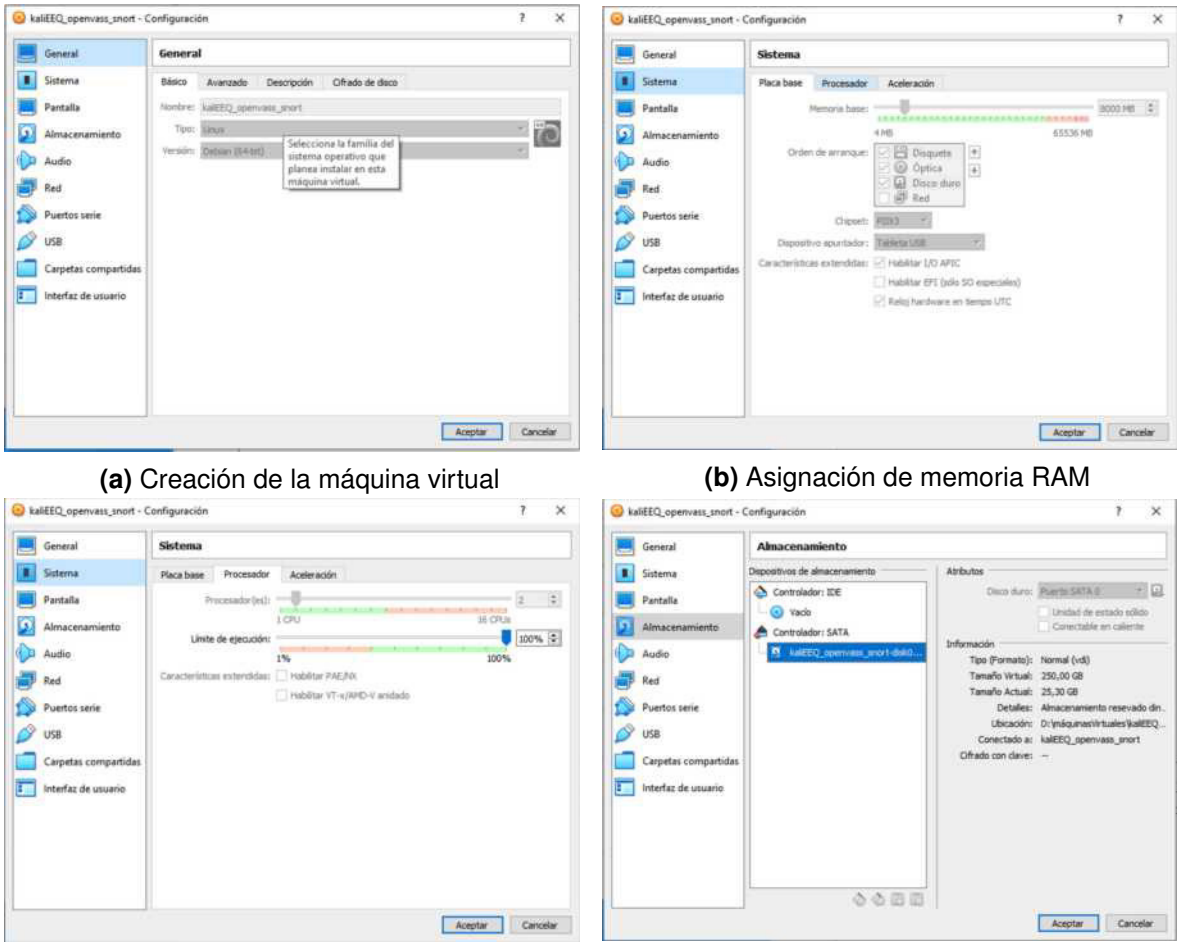



**Figura 2.39:** Página inicial del servidor Zabbix.

### 2.2.1.2. Instalación de la herramienta OpenVAS

La gestión de vulnerabilidades en la infraestructura instalada y en las redes de datos se le realizará por medio del uso de las herramientas OpenVAS y LogAnalyzer. En las siguientes secciones se describe el proceso de instalación de estas dos herramientas, se incluye también los procedimientos de integración de los equipos terminales hacia estas herramientas.

1. Creación de la máquina virtual



**(a)** Creación de la máquina virtual

**(b)** Asignación de memoria RAM

**(c)** Asignación de procesadores

**(d)** Asignación de almacenamiento

**Figura 2.40:** Máquina virtual creada para la instalación de la herramienta OpenVAS.

2. En la terminal de comandos ejecutar `sudo apt install gvm`

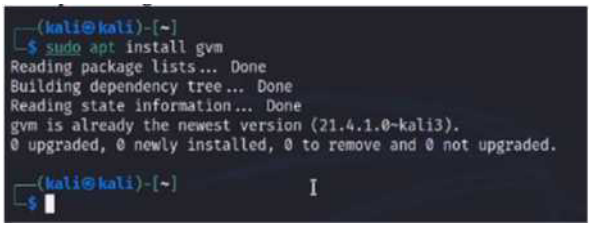



**Figura 2.41:** Ejecución `sudo apt install gvm`

3. Durante el proceso de instalación el sistema crea un usuario administrador y le otorga una contraseña segura, es importante anotar esta contraseña para poder ingresar más adelante a la interfaz web de OpenVas GVM.

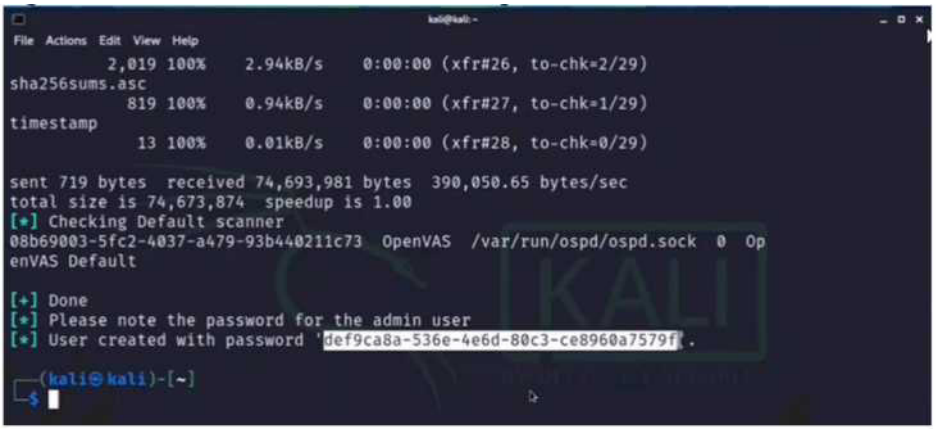



**Figura 2.42:** Proceso de creación de la cuenta de usuario administrador y su contraseña

4. Chequear que el proceso de instalación sea correcto, se chequearan todos los paquetes y librerías necesarios con el siguiente código `sudo gvm-check-setup`


**Figura 2.43:** Ejecución `sudo gvm-check-setup`

5. Para solucionar el error abrir `/usr/bin/gvm-check-setup` y cambiar Greenbone Security Assistant de 21.04 a 21.4 con el siguiente código `nano /usr/bin/gvm-check-setup`

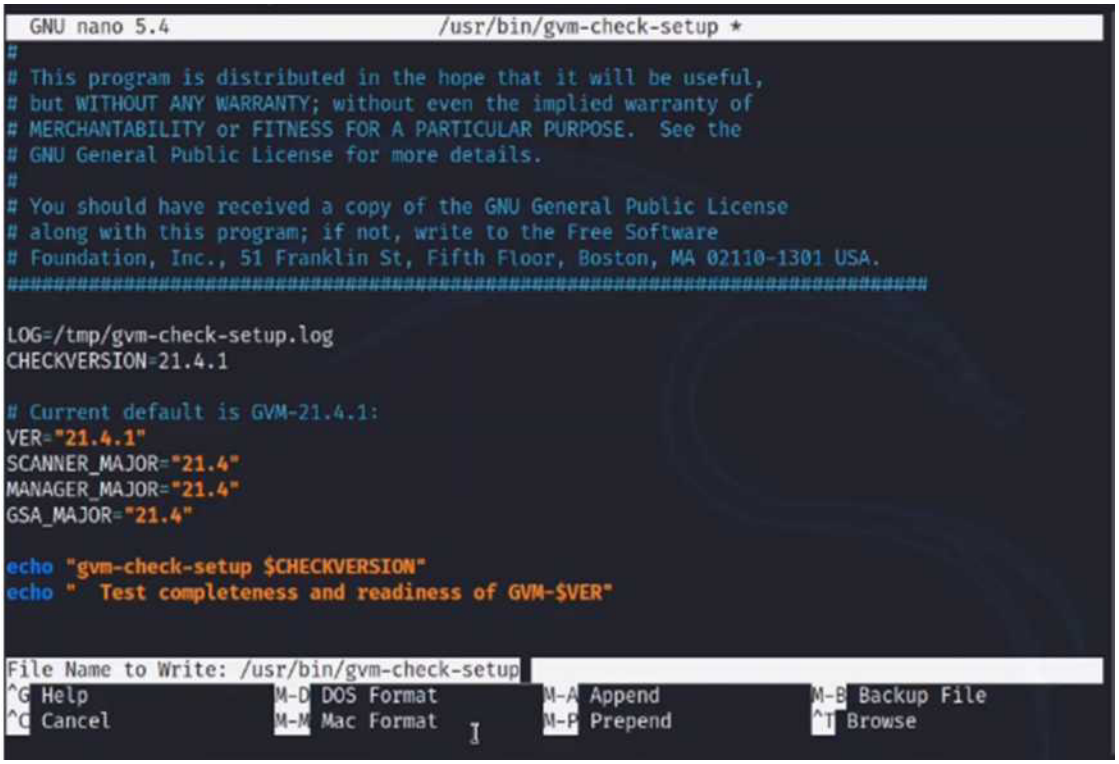



**Figura 2.44:** Ejecución `nano /usr/bin/gvm-check-setup`

6. Chequear nuevamente que el proceso de instalación sea correcto, si el problema anterior fue solucionado, la salida del comando mostrara que la instalación está completa y correcta con el siguiente código `sudo gvm-check-setup`


**Figura 2.45:** Ejecución `sudo gvm-check-setup`

7. Iniciar el gestor de vulnerabilidades OpenVas GVM con el siguiente código `sudo gvm-start`

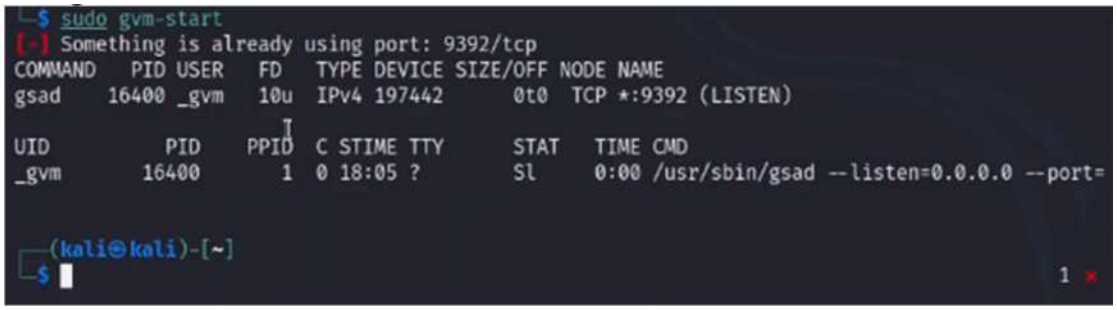



**Figura 2.46:** Ejecución `sudo gvm-start`

8. Acceder a la interfaz web de OpenVas GVM, se muestra una alerta de seguridad, esto se debe al certificado autofirmado de OpenVas GVM, seleccionar aceptar los riesgos y continuar con el siguiente enlace `https://10.16.6.122:9392/login`.

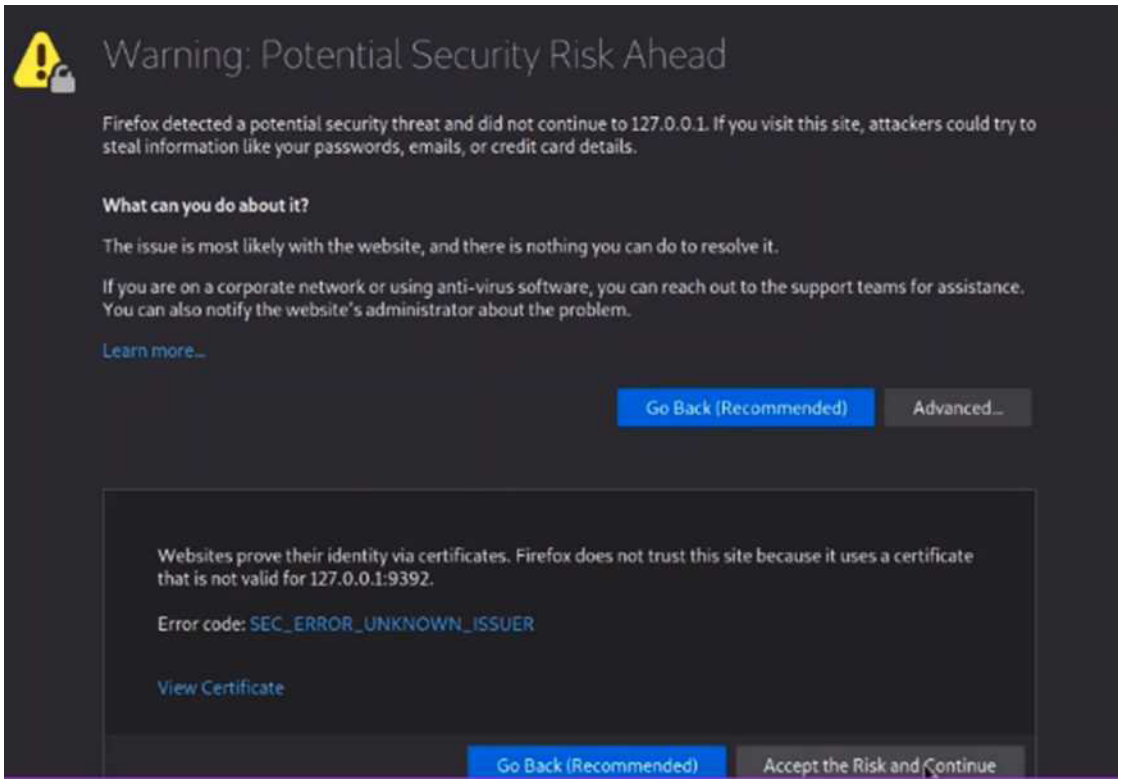



**Figura 2.47:** Ejecución `https://127.0.0.1:9392/login`

9. Ingresar con las credenciales generadas por el sistema en los pasos iniciales.


**Figura 2.48:** Ingreso de credenciales generadas al sistema OpenVas

10. Pantalla de Inicio del gestor de vulnerabilidades OpenVas GVM.


**Figura 2.49:** Pantalla de Inicio del gestor de vulnerabilidades OpenVas GVM

11. Cambio de contraseña, Ir al Panel de gestión de la cuenta y dar clic en mis ajustes.


**Figura 2.50:** Cambio de contraseña de administración.

Clic en editar mis ajustes.

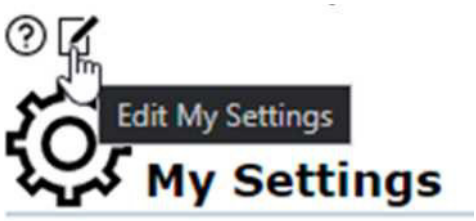



**Figura 2.51:** Edición de ajustes

En el panel de ajustes de la cuenta de usuario colocar la contraseña antigua generada por el sistema y establecer una nueva contraseña.


**Figura 2.52:** Ingreso de nueva contraseña de administración

12. Cambiar la dirección IP de loopback asignada por el sistema por la dirección IP definida en la red de la Empresa Eléctrica Quito.

13. Cambiar de directorio a `/lib/systemd/system` y abrir el archivo de configuración de OpenVas GVM.

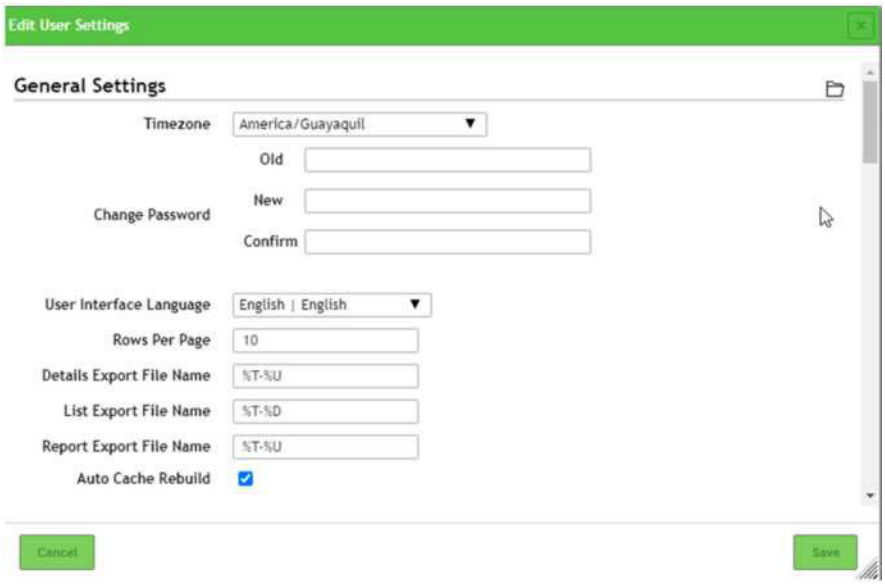



**Figura 2.53:** Cambio de directorio a `/lib/systemd/system`

14. Cambiar en la sección de servicio la IP de loopbaaack por la IP escogida en la red de la Empresa Eléctrica Quito.

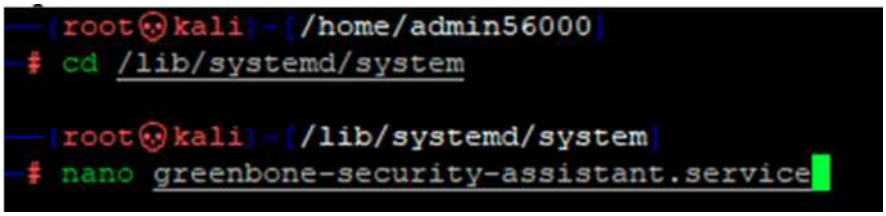



**Figura 2.54:** Cambio de la dirección IP de la loopback a la definida como implementación

15. Reiniciar OpenVas GVM con el siguiente código `systemctl daemon-reload && systemctl restart greenbone-security-assistant.service`

```
[Unit]
Description=Greenbone Security Assistant (gsad)
Documentation=man:gsad(8) https://www.greenbone.net
After=network.target gvmd.service
Wants=gvmd.service

[Service]
Type=forking
User=_gvm
Group=_gvm
ExecStart=/usr/sbin/gsad --listen=10.16.6.122 --port=9392
Restart=always
TimeoutStopSec=10

[Install]
WantedBy=multi-user.target
Alias=gsad.service
```

**Figura 2.55:** Ejecución reinició de servicios y validación de cambios

```
root@kali /lib/systemd/system
# systemctl daemon-reload && systemctl restart greenbone-security-assistant.service
```

**Figura 2.56:** Reinicio de servicios.

16. Probar si es posible ingresar a OpenVas GVM con la dirección IP establecida en el paso anterior.

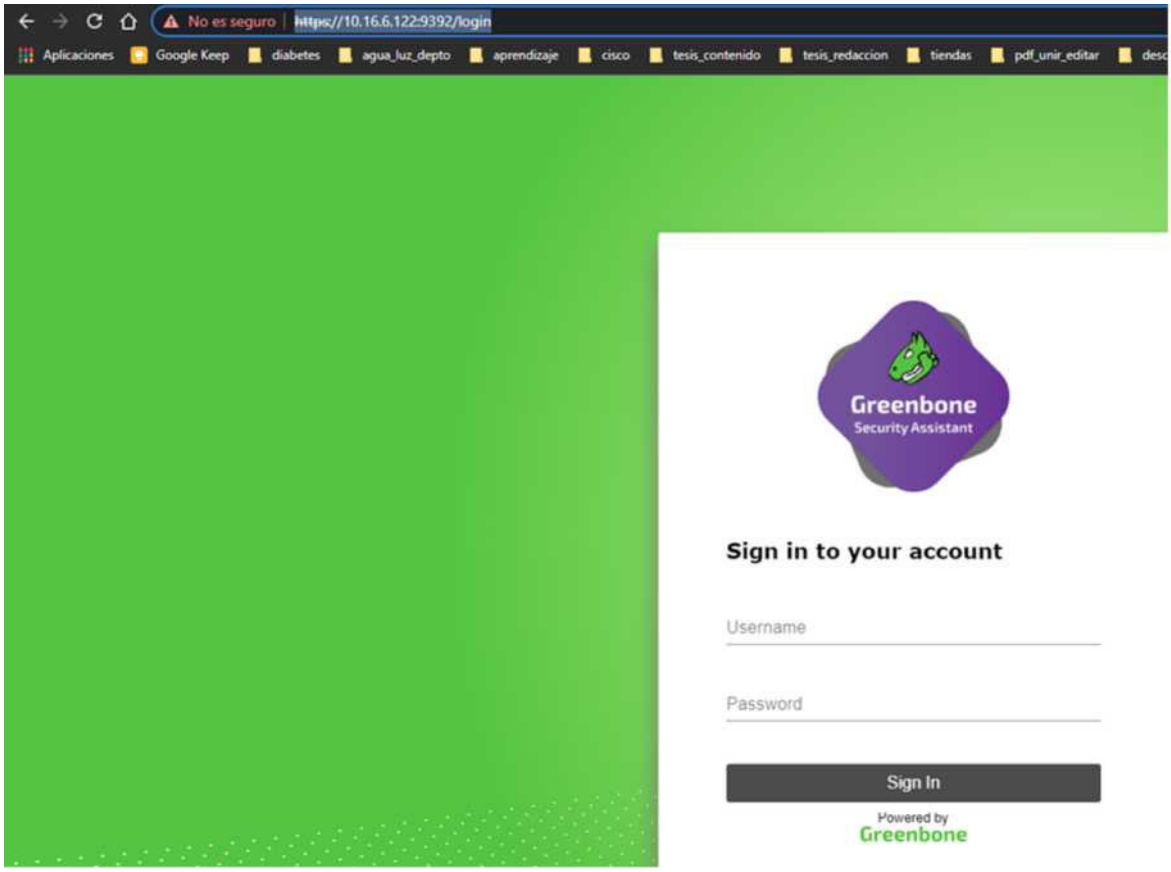



**Figura 2.57:** Pantalla de ingreso de OpenVas GVM - proceso de instalación finalizado.

17. Una vez instalada la herramienta, el siguiente paso es la configuración de la misma para realizar procesos de escaneo sobre la red. Para esto se debe crear una nueva tarea, en el menú scans seleccionar tasks, tal como se muestra en la Figura 2.58.

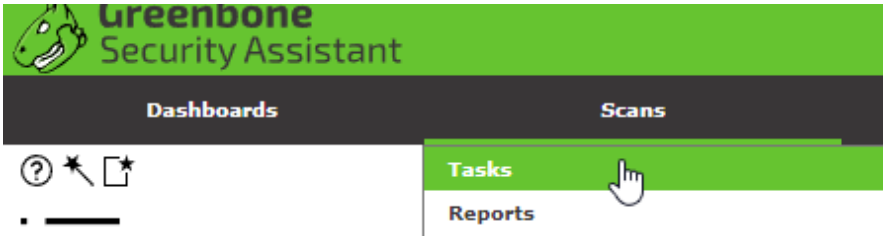



**Figura 2.58:** Creación de una nueva tarea de escaneo

18. En el menú desplegable seleccionar mostrado en la Figura 2.59 seleccionar `New Task`.

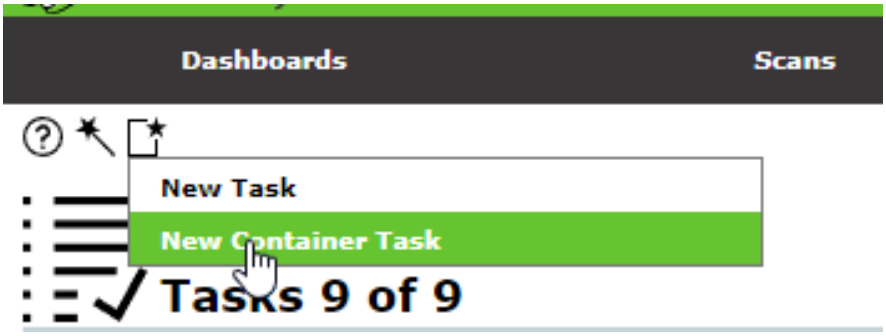



**Figura 2.59:** Menú de creación de una nueva tarea

19. En el espacio de `name` colocar un nombre a la nueva tarea, posteriormente seleccionar las direcciones IPs qué se desea escanear, esto se muestra en la Figura 2.60.


**Figura 2.60:** Pantalla

20. En la nueva ventana que se despliega seleccionar las IPs con fuente en un archivo externo (formato .txt), para este ejemplo se tomo como fuente de este archivo el inventario del Zabbix, esto se muestra en las Figuras 2.61 y 2.62.

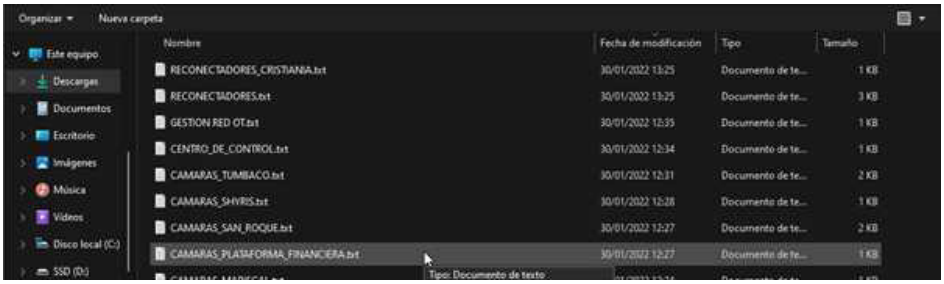



**Figura 2.61:** Selección de la fuente de información para escanear

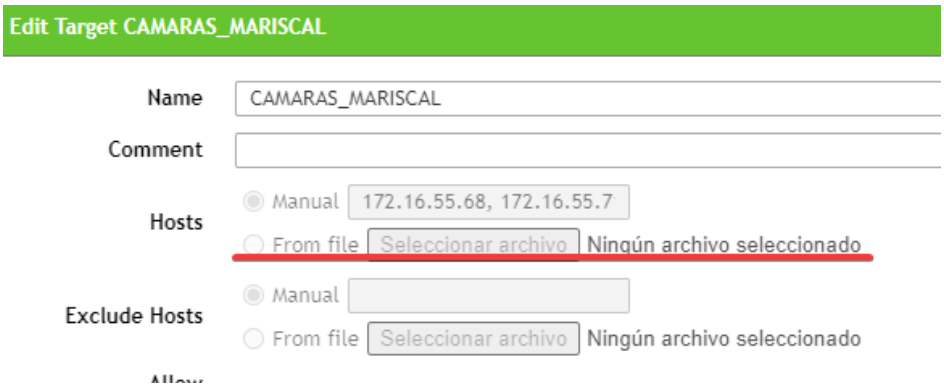



**Figura 2.62:** Selección de la fuente de información para escanear

21. Seleccionar el reporte de la nueva tarea creada tal como se muestra en la Figura 2.63.

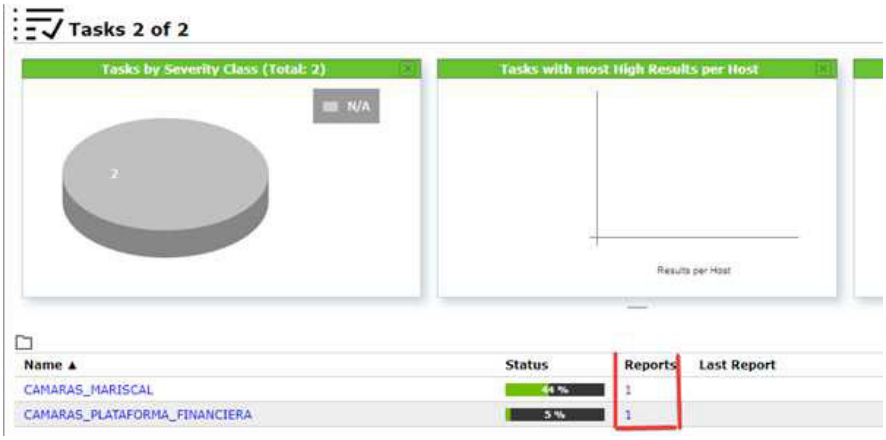



**Figura 2.63:** Selección del reporte de la tarea de escaneo realizada

22. Finalmente, en el dashboard se despliegan los datos de las vulnerabilidades encontradas en el análisis de vulnerabilidades de la subestación seleccionada, esto se muestra en la Figura 2.64. El reporte final en formato PDF se muestra en la Figura 2.65.


**Figura 2.64:** Pantalla final de presentación de resultados

Scan Report

January 31, 2022

**Summary**

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "America/Guayaquil", which is abbreviated "-05". The task was "CAMARAS_SAN_ROQUE". The scan started at Mon Jan 31 08:35:41 2022 -05 and ended at . The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

## Contents

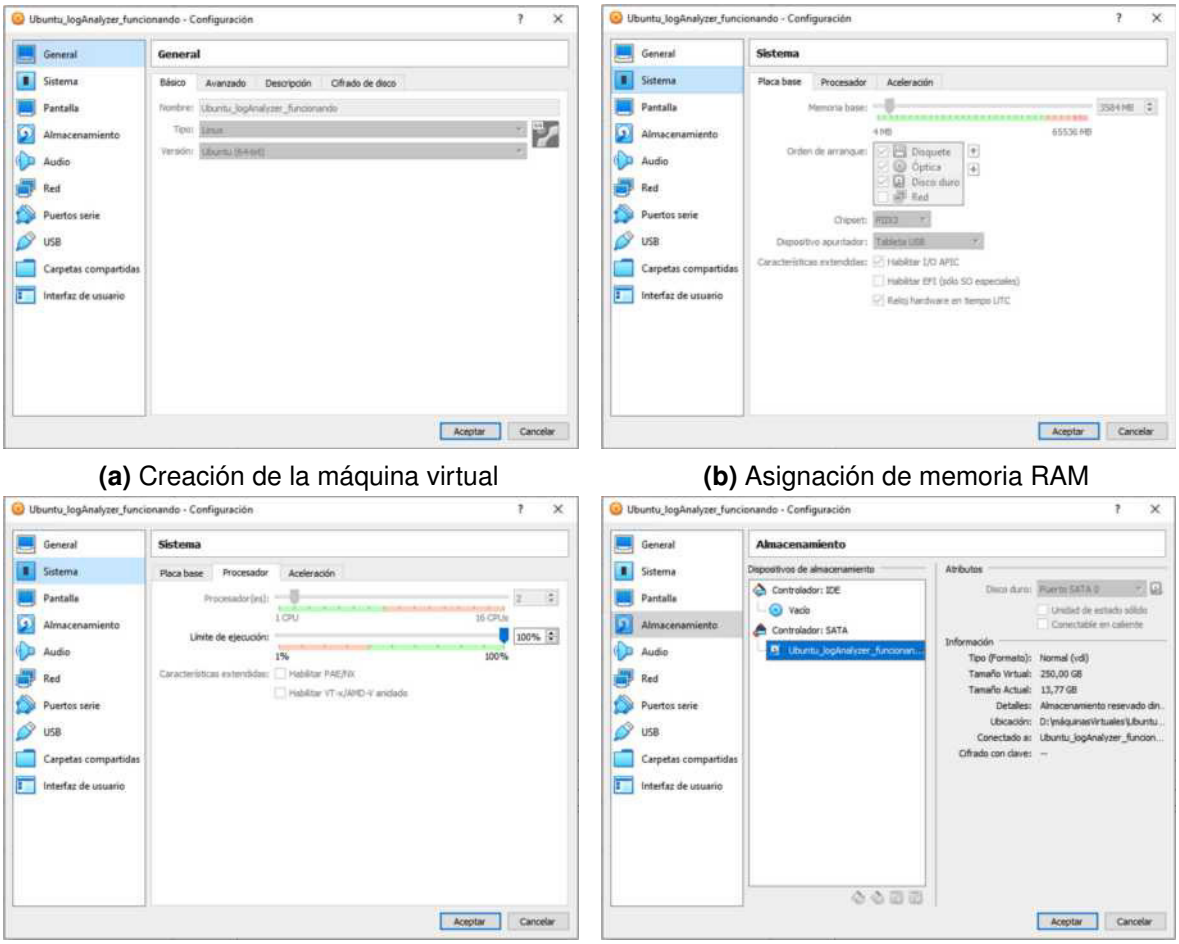


1

**Figura 2.65:** Pantalla final de presentación de resultados

### 2.2.1.3. Instalación de la herramienta Log-Analyzer

1. Creación de la máquina virtual




**(a)** Creación de la máquina virtual **(b)** Asignación de memoria RAM

**(c)** Asignación de procesadores **(d)** Asignación de almacenamiento

**Figura 2.66:** Máquina virtual creada para la instalación de la herramienta Log-Analyzer

2. Descargar e instalar apache 2, mysql y rsyslog, para esto, ejecutar los siguientes comandos:

**Código Fuente 2.14:** Instalación apache2, mysql y rsyslog

```
sudo apt update -y
sudo apt install apache2 -y
sudo apt install mysql-server -y
apt install php
apt install php php-cli php-fpm php-json php-pdo php-mysql php-
    zip php-gd php-mbstring php-curl php-xml php-pear php-bcmath
    php-mysqli -y php-mysqli
```

Resultados:

```
root@admin56000-VirtualBox:/home/admin56000/Escritorio# sudo apt update -y
Obj:1 http://security.ubuntu.com/ubuntu focal-security InRelease
Obj:2 http://ec.archive.ubuntu.com/ubuntu focal InRelease
Obj:3 http://ec.archive.ubuntu.com/ubuntu focal-updates InRelease
```

**Figura 2.67:** Ejecución `sudo apt update -y`

```
root@admin56000-VirtualBox:/home/admin56000/Escritorio# sudo apt install apache2
 -y
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
```

**Figura 2.68:** Ejecución `sudo apt install apache2 -y`

```
root@admin56000-VirtualBox:/home/admin56000/Escritorio# sudo apt install mysql-s
erver -y
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
```

**Figura 2.69:** Ejecución `sudo apt install mysql-server -y`

```
root@admin56000-VirtualBox:/home/admin56000/Escritorio# apt install php
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
```

**Figura 2.70:** Ejecución `sudo apt install php`

```
root@admin56000-VirtualBox:/home/admin56000/Escritorio# apt install php php-cli
php-fpm php-json php-pdo php-mysql php-zip php-gd php-mbstring php-curl php-xml
php-pear php-bcmath php-mysqli -y php-mysqli
Leyendo lista de paquetes... Hecho
```

**Figura 2.71:** Ejecución `apt install php php-cli php-fpm php-json php-pdo php-mysql php-zip php-gd php-mbstring php-curl php-xml php-pear php-bcmath php-mysqli -y php-mysqli`

3. Reiniciar el servicio de apache 2 con el comando `systemctl restart apache2`

```
root@admin56000-VirtualBox:/home/admin56000/Escritorio# systemctl restart apache
2
root@admin56000-VirtualBox:/home/admin56000/Escritorio#
```

**Figura 2.72:** Ejecución `systemctl restart apache2`

4. Chequear el estado del servicio de apache 2 con el comando `systemctl status apache2`

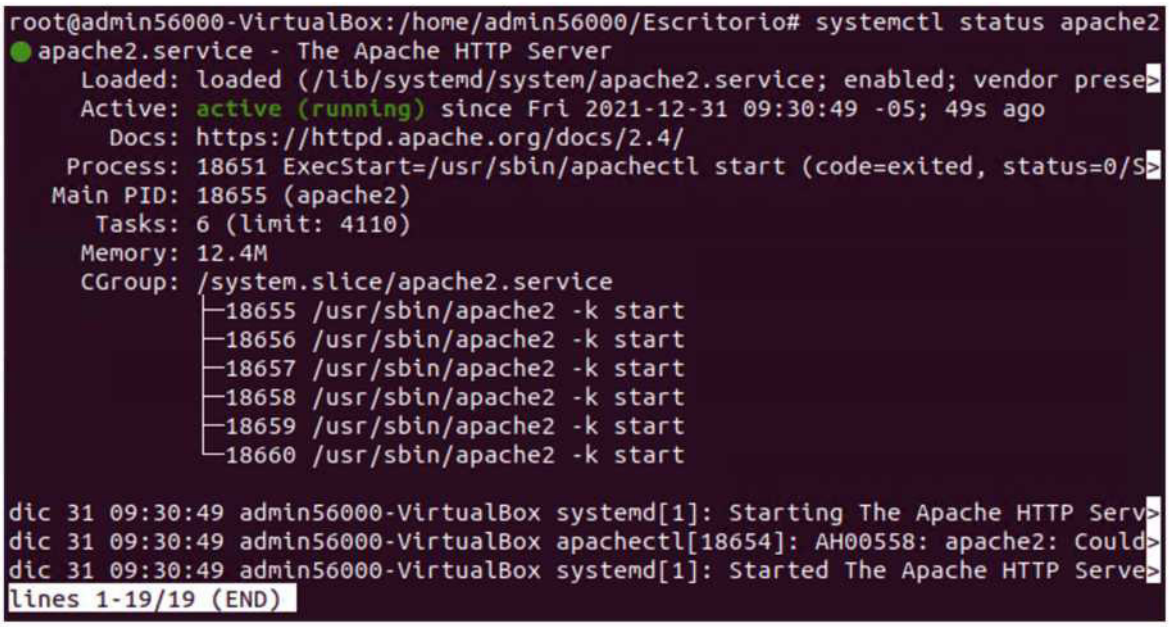



**Figura 2.73:** Ejecución `systemctl status apache2`

5. Instalar rsyslog, no configurar aún la base de datos, más adelante se hará de forma manual, para la instalación ejecutar el siguiente código `sudo apt-get install rsyslog rsyslog-mysql -y`

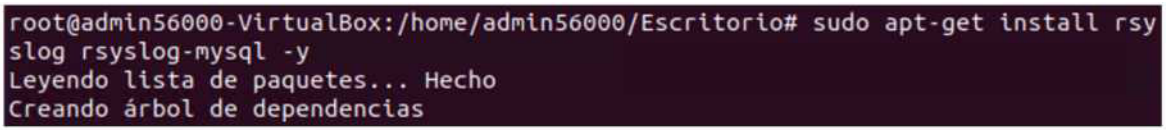



**Figura 2.74:** Ejecución `sudo apt-get install rsyslog rsyslog-mysql -y`

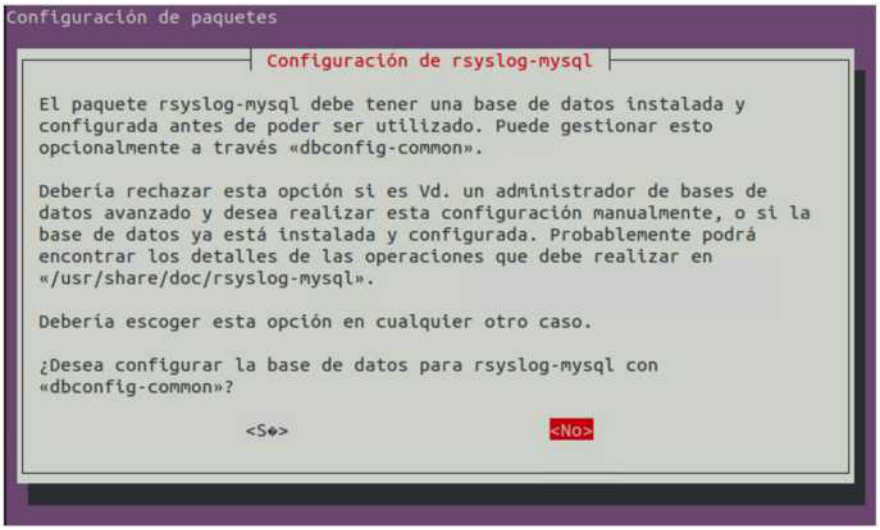



**Figura 2.75:** Configuración de `rsyslog-mysql`

6. Creación de la base de datos para el usuario de LogAnalyzer con los siguientes datos.

- ❒ Base de datos Ryslog : DBRsyslog
- ❒ Usuario Rsyslog : ******** (definida en el proceso de instalación)
- ❒ Contraseña Rsyslog : ******** (definida en el proceso de instalación)
- ❒ Ejecutar el comando `mysql -u root -p`

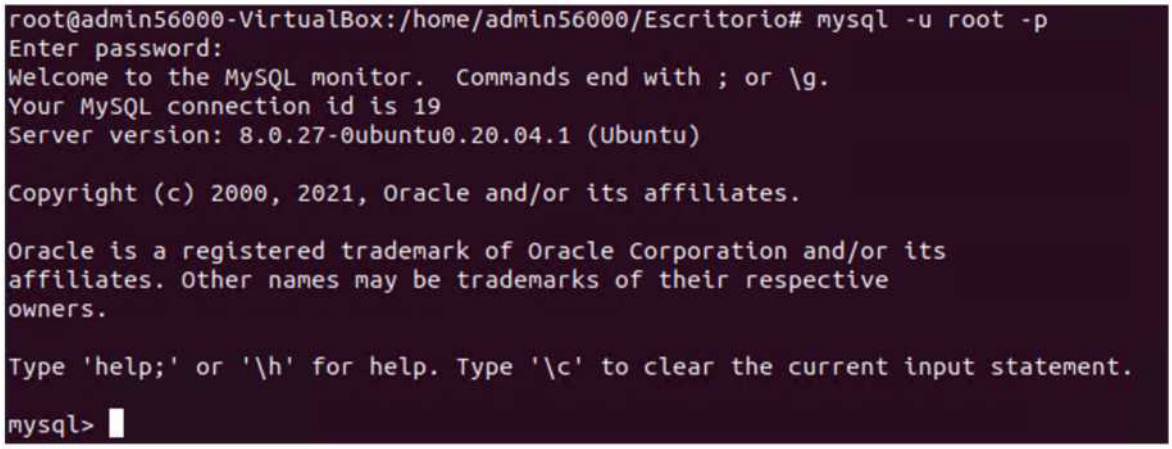



**Figura 2.76:** Configuración de `mysql -u root -p`

7. Crear la base de datos con el siguiente código `CREATE DATABASE DBRsyslog;`


**Figura 2.77:** Creación de la base de datos `CREATE DATABASE DBRsyslog;`

8. Creación del usuario definido en el proceso de instalación y otorgarle permisos.

**Código Fuente 2.15:** Creación de la base de datos del servidor Rsyslog

```
1 CREATE USER '********'@'localhost' IDENTIFIED BY '********';
- GRANT ALL PRIVILEGES ON DBRsyslog.* TO '********'@'localhost';
- FLUSH PRIVILEGES;
- exit;
```

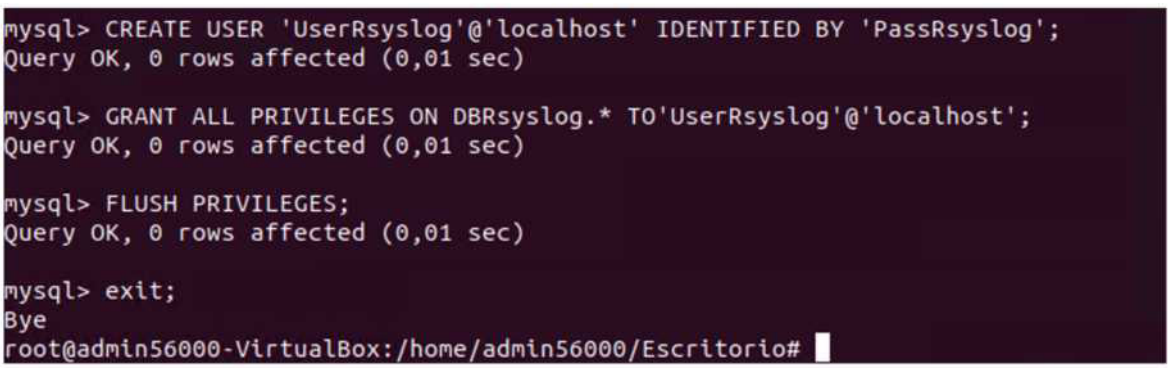



**Figura 2.78:** Creación de usuarios en la base de datos y asignación de permiso

9. Ingresar a la base de datos generada para Rsyslog ejecutando lo siguiente `mysql -u ******** -D DBRsyslog -p`

```
root@admin56000-VirtualBox:/home/admin56000/Escritorio# mysql -u  UserRsyslog -D
 DBRsyslog -p  < /usr/share/dbconfig-common/data/rsyslog-mysql/install/mysql
Enter password:
root@admin56000-VirtualBox:/home/admin56000/Escritorio#
```

**Figura 2.79:** Acceso a la base de datos `mysql -u ******** -D DBRsyslog -p`

10. Chequear que la base datos se haya generado correctamente ejecutando lo siguiente `use DBRsyslog; show tables;`

```
mysql> use DBRsyslog;
Database changed
mysql> show tables;
+-----------------------+
| Tables_in_DBRsyslog   |
+-----------------------+
| SystemEvents          |
| SystemEventsProperties |
+-----------------------+
2 rows in set (0,00 sec)

mysql>
```

**Figura 2.80:** Comprobación de la generación de la base de datos.

11. Configuración del servidor Rsyslog, primeramente realizar una copia de seguridad del archivo de configuración de Rsyslog con el siguiente código `cp /etc/rsyslog.conf /etc/rsyslog.conf.bak`

```
root@admin56000-VirtualBox:/home/admin56000/Escritorio# cp /etc/rsyslog.conf /et
c/rsyslog.conf.bak
root@admin56000-VirtualBox:/home/admin56000/Escritorio#
```

**Figura 2.81:** Copia de seguridad del archivo de configuración de Rsyslog

12. Abrir el archivo de configuración y habilitar la recepción de archivos de registro mediante los protocolos TCP y UDP en el puerto 514, editar el archivo ejecutando el siguiente código `nano /etc/rsyslog.conf`

```
module(load="imuxsock") # provides support for local system logging
#module(load="immark")  # provides --MARK-- message capability

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")
```

**Figura 2.82:** Habilitación de los puertos tcp/upd en el servidor Rsyslog

13. Agregar la siguiente plantilla para que los archivos de registro se guarden en una carpeta con el nombre de cada host.

**Código Fuente 2.16:** Plantilla para almacenamiento de logs por host

```
1 $template Incoming-logs,"var/log/%HOSTNAME%/%PROGRAMNAME%.log
- ruleset(name="remote"){
- action(type="omfile" dynafile="Incoming-logs")
- }
```

```
#############################################################################

$template Incoming-logs,"var/log/%HOSTNAME%/%PROGRAMNAME%.log
ruleset(name="remote"){
action(type="omfile" dynafile="Incoming-logs")
}
```

**Figura 2.83:** Plantilla para que los archivos de registro se guarden en una carpeta con el nombre de cada host

14. Agregar el registro de salida en el archivo de configuración de la base de datos: `/etc/rsyslog.d/mysql.conf` y escriba Nombre de usuario, Contraseña y Nombre de la base de datos.

```
### Output###
module (load="ommysql")
*.* action(type="ommysql" server="localhost" db="DBRsyslog" uid="UserRsyslog" p>
```

**Figura 2.84:** Registro de salida en el archivo de configuración de la base de datos

15. Reiniciar el servicio Rsyslog con el siguiente código `systemctl restart rsyslog`

```
root@admin56000-VirtualBox:/home/admin56000/Escritorio# systemctl restart rsyslo
g
root@admin56000-VirtualBox:/home/admin56000/Escritorio#
```

**Figura 2.85:** Reinicio del servicio Rsyslog

16. Verificar el estado del servicio Rsyslog con el siguiente código `systemctl status rsyslog`

```
root@admin56000-VirtualBox:/home/admin56000/Escritorio# systemctl status rsyslog
● rsyslog.service - System Logging Service
     Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor prese>
     Active: active (running) since Fri 2021-12-31 11:19:04 -05; 2min 9s ago
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             https://www.rsyslog.com/doc/
   Main PID: 19908 (rsyslogd)
      Tasks: 10 (limit: 4110)
     Memory: 21.8M
     CGroup: /system.slice/rsyslog.service
             └─19908 /usr/sbin/rsyslogd -n -iNONE

dic 31 11:19:04 admin56000-VirtualBox systemd[1]: Starting System Logging Servi>
dic 31 11:19:04 admin56000-VirtualBox systemd[1]: Started System Logging Servic>
dic 31 11:19:04 admin56000-VirtualBox rsyslogd[19908]: imuxsock: Acquired UNIX >
dic 31 11:19:04 admin56000-VirtualBox rsyslogd[19908]: rsyslogd's groupid chang>
dic 31 11:19:04 admin56000-VirtualBox rsyslogd[19908]: rsyslogd's userid change>
dic 31 11:19:04 admin56000-VirtualBox rsyslogd[19908]: [origin software="rsyslo>
lines 1-18/18 (END)
```

**Figura 2.86:** Verificación del servicio Rsyslog

17. Descarga la herramienta de análisis de archivos de registro LogAnalyzer con el siguiente código:

**Código Fuente 2.17:** Descarga de LogAnalyzer

```
1 cd /home
- wget https://download.adiscon.com/loganalyzer/loganalyzer-4.1.12.
    tar.gz
- tar xzf loganalyzer-4.1.12.tar.gz
```

```
root@admin56000-VirtualBox:/home# tar xzf loganalyzer-4.1.12.tar.gz
root@admin56000-VirtualBox:/home# ls
admin56000  loganalyzer-4.1.12  loganalyzer-4.1.12.tar.gz
root@admin56000-VirtualBox:/home#
```

**Figura 2.87:** Descarga la herramienta de análisis de archivos de registro LogAnalyzer

18. Mover la carpeta loganalyzer a la carpeta del servidor web con el siguiente código `mv loganalyzer-4.1.12/src /var/www/html/loganalyzer`

```
root@admin56000-VirtualBox:/home# mv loganalyzer-4.1.12/src /var/www/html/logana
lyzer
root@admin56000-VirtualBox:/home#
```

**Figura 2.88:** Copia de la carpeta loganalyzer a la carpeta del servidor web.

19. Crear el archivo `config.php` en la carpeta de la herramienta LogAnalyzer con el siguiente código:

**Código Fuente 2.18:** Creación del archivo de configuración `config.php`

```
1 cd /var/www/html/loganalyzer
- touch config.php
- chown www-data:www-data config.php
- chmod 644 config.php
```

```
root@admin56000-VirtualBox:/home# cd /var/www/html/loganalyzer
root@admin56000-VirtualBox:/var/www/html/loganalyzer# touch config.php
root@admin56000-VirtualBox:/var/www/html/loganalyzer# chown www-data:www-data co
nfig.php
root@admin56000-VirtualBox:/var/www/html/loganalyzer# chmod 644 config.php
root@admin56000-VirtualBox:/var/www/html/loganalyzer#
```

**Figura 2.89:** Creación del archivo `config.php` en la carpeta de la herramienta LogAnalyzer

20. Efectuar la configuración inicial de LogAnalyzer en su portal web a través del siguiente enlace `http://10.16.6.33/loganalyzer/`

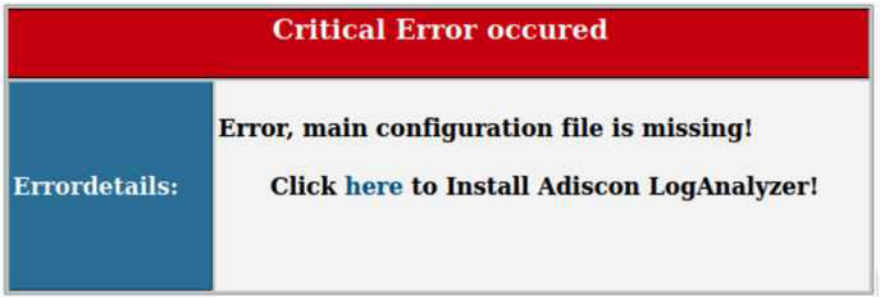



**Figura 2.90:** Configuración inicial de LogAnalyzer en su portal web.

21. Revisar los prerrequisitos y dar clic en siguiente:


**Figura 2.91:** Prerrequisitos de la herramienta LogAnalyzer en su portal web

22. Verificación de los permisos necesarios y dar clic en siguiente.

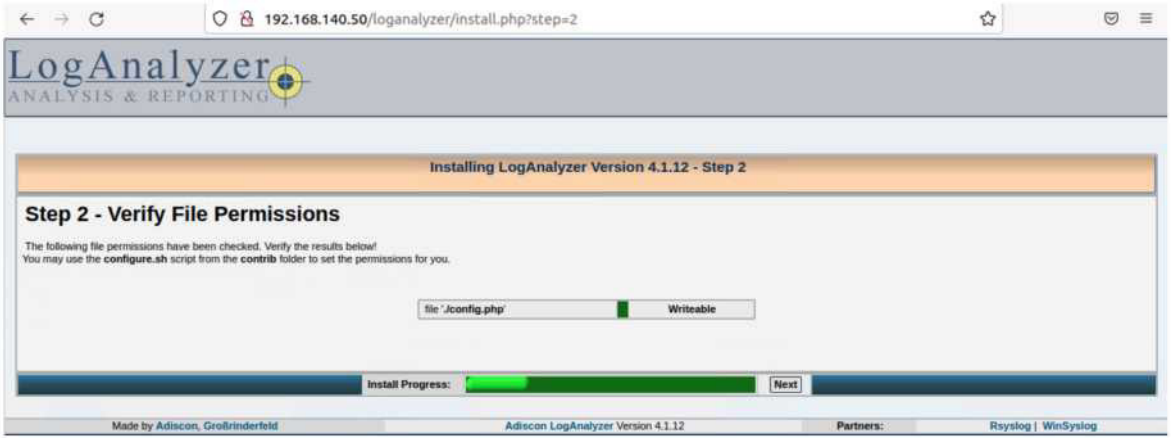



**Figura 2.92:** Verificación de los permisos necesarios de herramienta LogAnalyzer en su portal web

23. Seleccionar si en activar la base de datos de usuario y colocar el nombre, usuario y contraseña de la base de datos anteriormente generada y dar clic en siguiente:


**Figura 2.93:** Activación de la base de datos de la herramienta LogAnalyzer en su portal web

24. En este paso se comprueba la conexión a la base da datos y se generan las tablas necesarias que utilizara el sistema LogAnalyzer.


**Figura 2.94:** Comprobación de la conexión con la base de datos de la herramienta LogAnalyzer en su portal web

25. Confirmar la creación de las tablas necesarias para el sistema LogAnalyzer.


**Figura 2.95:** Comprobación de la creación de las tablas necesarias para la herramienta LogAnalyzer en su portal web

26. Creación de la cuenta de administrador en el sistema LogAnalyzer.

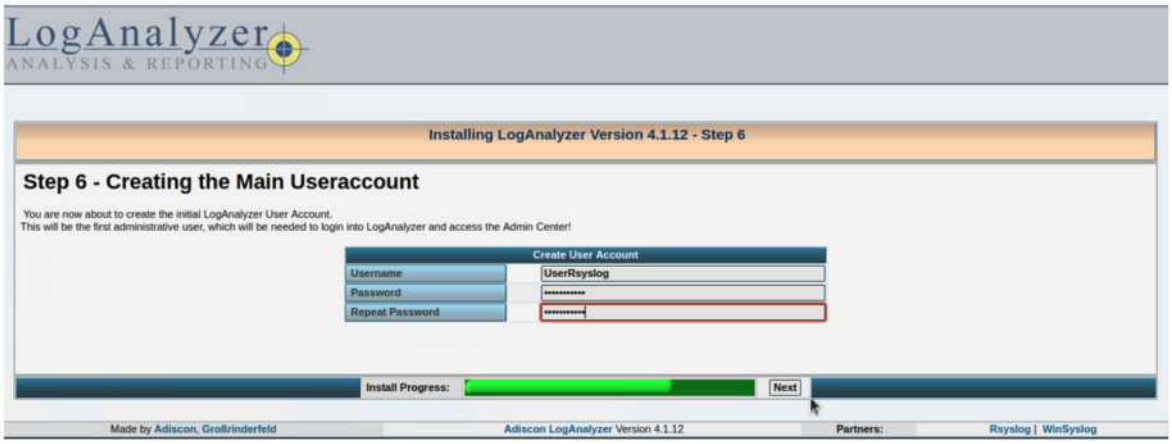



**Figura 2.96:** Creación de la cuenta de administrador para la herramienta LogAnalyzer en su portal web

27. Seleccionar el tipo de fuente de datos MYSQL Native, y colocar el nombre, usuario y contraseña de la base da datos.


**Figura 2.97:** Selección del tipo de fuente de datos MYSQL Native para la herramienta LogAnalyzer en su portal web

28. Finalización de la instalación

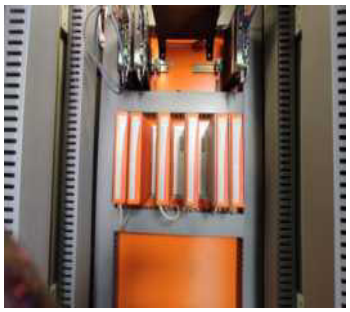

**Figura 2.98:** Finalización de instalación de la herramienta LogAnalyzer en su portal web.

### 2.2.2. PROCESO DE INTEGRACIÓN DE EQUIPOS A LA HERRAMIENTA ZABBIX

Una vez desplegada la herramienta de monitoreo Zabbix la siguiente actividad desarrollada fue la integración de los equipos terminales mediante plantillas de monitoreo. El principal objetivo de este trabajo de titulación es utilizar los protocolos desarrollados para la gestión de infraestructura, luego del inventariado de los equipos se definió como uno de los protocolos a utilizar el protocolo SNMP, adicionalmente para aquellos equipos que no cuentan con este protocolo se definió como método de monitoreo el integrarlos mediante la plan-

tilla disponible del protocolo ICMP. En la Figura 2.99 se muestran varios ejemplos de los equipos terminales integrados al monitoreo mediante la herramienta Zabbix.

**(a)** RTU Cooper



**(b)** RTU Saitel

**(c)** RTU Elliop

**(d)** Switches Ruggedcom

**(e)** Switchs/Routers Garretcom

**(f)** Routers Ruggedcom

**(g)** IEDs Siemens

**(h)** IEDs ABB

**(i)** IEDs Ingeteam

**(j)** Sensores de Transformador - SE Los Bancos

**(k)** Sensores de Transformador - SE Vicentina

**(l)** Sensores de Transformador - SE Conocoto

**Figura 2.99:** Equipos terminales de las redes de datos, industrial a ser integrados en el monitoreo con la herramienta Zabbix

En la presente sección se describe el procedimiento para la integración de los equipos terminales en donde el protocolo SNMP está disponible, estas integraciones fueron desarrolladas con las versiones v1 y v2c, la versión v3 no fue utilizada debido a la incompatibilidad

de los sistemas operativos de los equipos con unas versiones actuales de las herramientas de gestión como es el caso de Zabbix, incluso un par de situaciones tuvo que hacer cambio de versión de la v2c a la v1 por problemas en el rendimiento de los equipos en los cuales se produjeron reinicios imprevistos de los mismos.

#### 2.2.2.1. Equipos Ruggedcom RSG2100 / RSG2200 / RS8000H / RS900

Los equipos Ruggedcom cuenta con el sistema operativo Rugged Operating System (ROS). El proceso de integración de estos equipos a la herramienta Zabbix se describe a continuación:

1. Ingresar al equipo vía CLI(TELNET/SSH)
2. Seleccionar *"Administración"* y dar enter


**Figura 2.100:** Pantalla de inicio Equipos Ruggedcom

3. Seleccionar *Configure* SNMP y dar enter

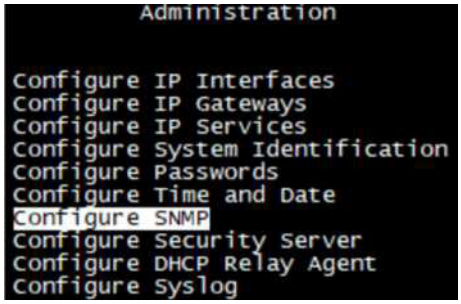



**Figura 2.101:** Menu de configuración del protocolo SNMP en Equipos Ruggedcom

4. Seleccionar *"Configure SNMP Users"* y dar enter
5. En este menú podemos configurar nuevas comunidades SNMP o editar/eliminar las comunidades actualmente existentes


**Figura 2.102:** Configuración de usuarios SNMP en Equipos Ruggedcom

*a*) Crear una nueva comunidad SNMP (Control + i)

*b*) Eliminar una comunidad SNMP (Control + l)

*c*) Editar una comunidad SNMP (dar enter sobre la comunidad seleccionada.

6. A continuación se ha creado la comunidad *"co20.21M"* (Control + i) y seguidamente se configura sus asociados parámetros:

   *a*) *"IP Address"* Dirección IP del servidor SNMP-MANAGER

   *b*) *"Auth Protocol"* Tipo de autenticación

   *c*) *"Priv Protocol"* Tipo de cifrado

   *d*) *"Auth Key"* Clave/llave de autenticación

   *e*) *"Priv Key"* Clave/llave de cifrado

   Ejemplo:
   Name = Nombre-comunidad
   IP Address = Dirección-IP-Zabbix
   No autenticación, no cifrado.

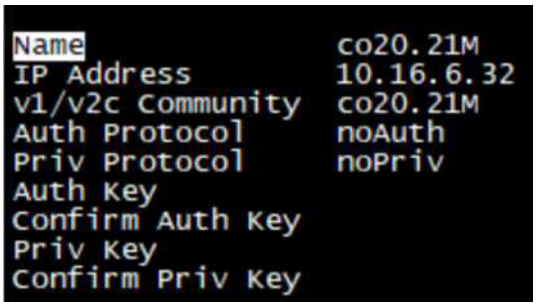



**Figura 2.103:** Configuración para el modelo RUGGEDCOM RS900GNC

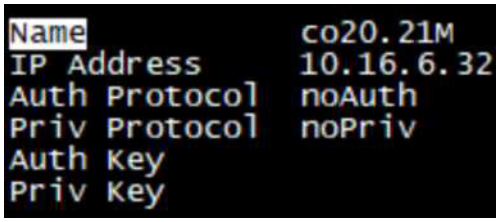



**Figura 2.104:** Para el resto de modelos de Equipos Ruggedcom

7. La configuración realizada se la ejecuta y graba con los comandos (Control + a) y posteriormente regresamos al menú SNMP con la tecla Esc

8. Seleccionamos la opción *"Configure* SNMP *Security to Group Maps"* y damos enter

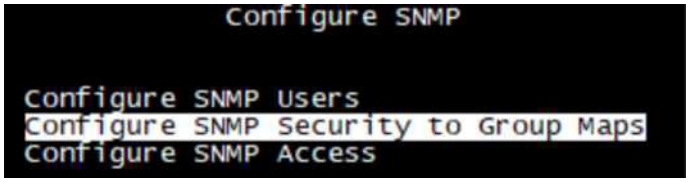



**Figura 2.105:** Configuración de los grupos SNMP

9. Aquí se crea, elimina o edita los grupos SNMP

10. Se selecciona la versión SNMP que se desea utilizar (v1, v2c o v3)

11. Emparejamos una comunidad SNMP con un grupo SNMP

    *a*) Ejemplo:

        1) Versión 2 de SNMP
        2) Nombre del grupo "G3"
        3) Nombre de la comunidad "Nombre-Comunidad" (que previamente la configuramos)

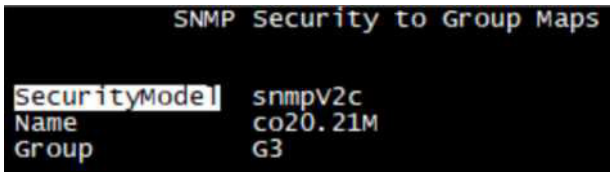



**Figura 2.106:** Configuración de los grupos SNMP - asignación de grupos

12. La configuración realizada se la ejecuta y graba con los comandos (Control + A) y posteriormente regresamos al menú SNMP con la tecla Esc

13. Seleccionar "Configure SNMP Access" y dar enter

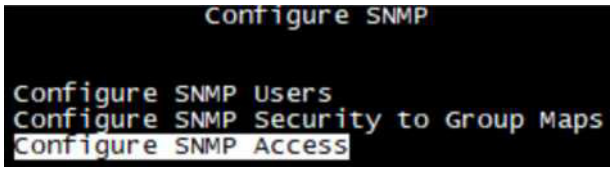



**Figura 2.107:** Asignación de grupos, comunidad y versión de SNMP previamente configurados

14. Aquí se llena los campos haciendo match con el grupo, comunidad y versión SNMP previamente configurados.

*a*) Ejemplo:

1) Nombre de grupo “G3”
2) Versión SNMP “v2c”
3) Sin autenticación
4) Se permite la visualización de todos los MIBs

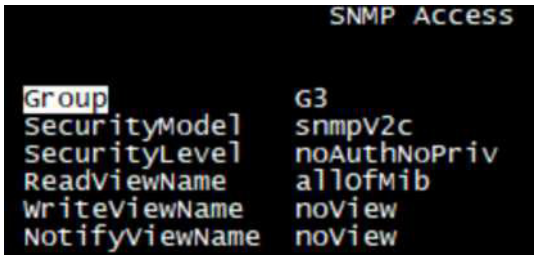



**Figura 2.108:** Ejemplo de asignación de grupos, comunidad y versión de SNMP previamente configurados

*b*) La configuración realizada se la ejecuta y graba con los comandos (Control + a) y posteriormente regresamos al menú SNMP con la tecla Esc

#### 2.2.2.2. Equipos Ruggedcom RX1501 / RX1500

Para la integración de los equipos Ruggedcom RX1501 / RX1500 la configuración fue realizada utilizando la terminal de comandos, la cual puede ser ingresada mediante acceso SSH o telnet. En el código fuente 2.19 se presenta la configuración realizada para la habilitación del protocolo SNMP en estos equipos.

**Código Fuente 2.19:** Configuración SNMP RUGGEDCOM RX1501 / RX1500

```
config
admin
snmp
snmp-community nombre_comunidad
user-name nombre_usuario
exit
  snmp-target-address ip_servidor_zabbix
   target-address ip_servidor_zabbix
   user-name      nombre_usuario
  !
  snmp-target-address "ip_servidor_zabbix version_snmp"
   target-address    ip_servidor_zabbix
   user-name         nombre_usuario
   control-community nombre_comunidad
  !
exit
  snmp-security-to-group v2c nombre_usuario
  !
  snmp-security-to-group v2c guest
  !
commit
exit
exit
exit
exit
#Verificacion de la configuración
show running-config nombre_usuario snmp
```

### 2.2.2.3. Equipos Garrettcom DX-940

Para la configuración de los equipos Garretcom DX-940 se usó el acceso vía terminal web y su menú gráfico. El procedimiento realizado se detalla a continuación:

1. Ingresar al equipo vía web (HTTPS)
2. En el panel principal ir al siguiente path y aplicar la configuración SNMP deseada: Administración ≫ SNMP ≫ Global Settings

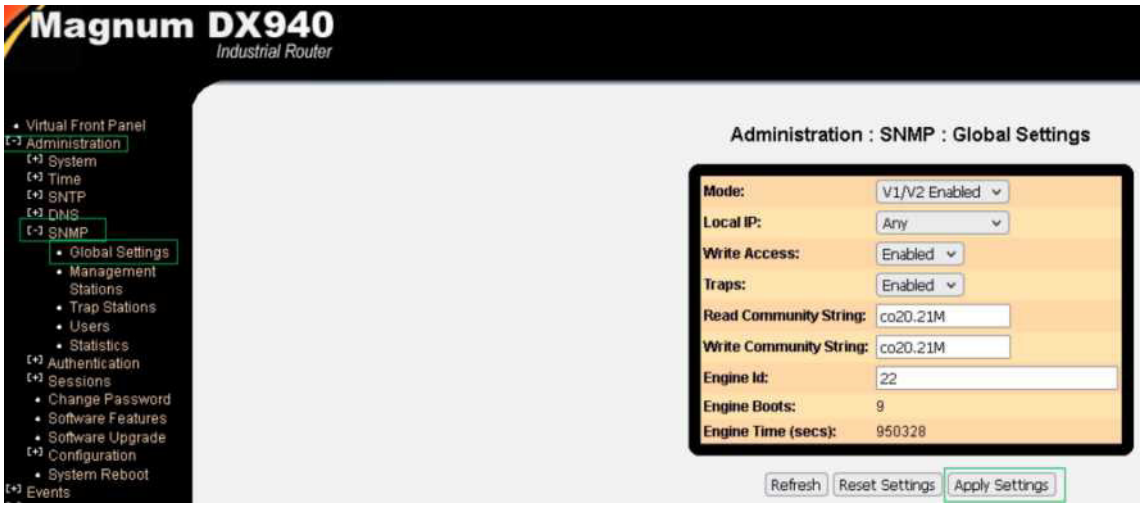



**Figura 2.109:** Configuración protocolo SNMP en los equipos Garretcom DX-940

3. Aplicar la configuración “Apply Settings”
4. Añadir un servidor con el rol de SNMP Management en el campo *“Station Name or IP”*, Administración ≫ SNMP ≫ Management Stations

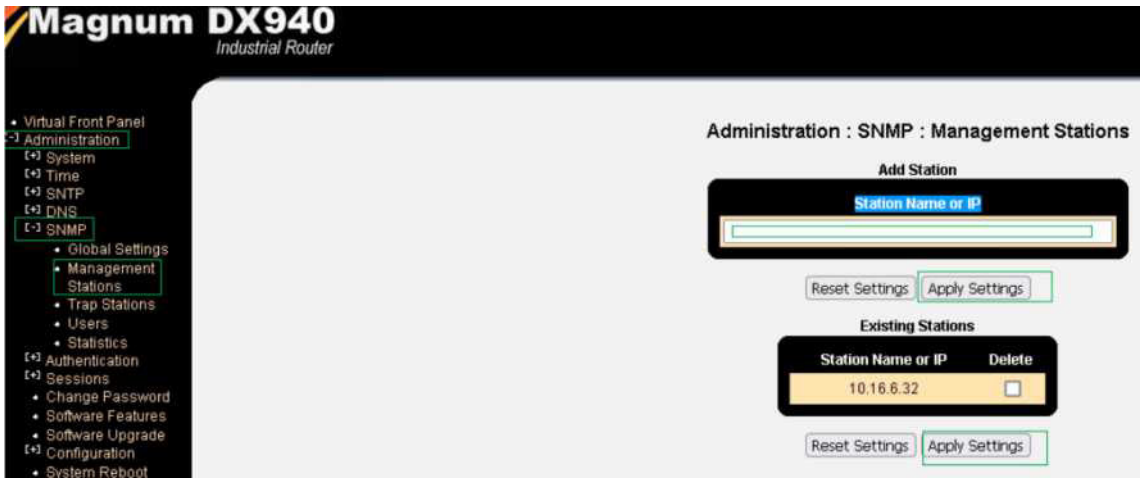



**Figura 2.110:** Asignación de terminales de recolección de datos del protocolo SNMP

5. Aplicar la configuración *“Apply Settings”*

6. Una vez aplicada la configuración, la IP del Management SNMP será desplegada en la sección *"Existing Stations"*.

#### 2.2.2.4. Equipos Garrettcom 6KL

Para los switches Garretcom 6KL la configuración del protocolo SNMP fue realizada mediante el script del Código fuente 2.20.

**Código Fuente 2.20:** Configuración SNMP GARRETTCOM 6KL

```
#SNMP#
set snmp type=v1
snmp
community write=nombre_comunidad read=nombre_comunidad trap=
   nombre_comunidad
authentraps disable
mgrip add ip=ip_zabbix
traps add type=snmp ip=ip_zabbix
exit
set snmp type=v1
rmon
exit
save
#Verificacion de configuracion
show snmp
```

#### 2.2.2.5. Equipos Foundry FESX424-PREM

La configuración de los equipos Foundry FESX424-PREM fue realizada con el script del Código fuente 2.21.

**Código Fuente 2.21:** Configuración SNMP FOUNDRY FESX424-PREM

```
configure terminal
snmp-server community 1 $ds|Q&|Zk ro nombre_comunidad
snmp-server community 1 $ds|Q&|Zk rw nombre_comunidad
snmp-server host ip_zabbix version v1 1 $Si2^=d
snmp-server host ip_zabbix version v2c 1 $Si2^=d
snmp-server group G3 v2c
snmp-client ip_zabbix
exit
write memory
#Verificacion
show snmp
show running-config | begin snmp
```

#### 2.2.2.6. Equipos Alstom T1000 / S2020

La configuración de los equipos ALSTOM T1000 / S2020 fue realizada con el script del Código fuente 2.22.

**Código Fuente 2.22:** Configuración SNMP ALSTOM T1000 / S2020

```
configure terminal
snmp-server host ip_zabbix
 no shutdown
 host ip_zabbix 162 traps
snmp-server community v2c nombre_comunidad RO
!
exit
copy running-config startup-config
#Verificacion
show snmp
show running-config feature snmp
```

#### 2.2.2.7. Equipos Cisco Series 1841

La configuración de los equipos Cisco Series 1841 fue realizada con el script del Código fuente 2.23.

**Código Fuente 2.23:** Configuración SNMP CISCO Series 1841

```
configure terminal
snmp-server community nombre_comunidad
do wr
exit
#Verificacion
show snmp community
show snmp
show running-config | section snmp
```

#### 2.2.2.8. Equipos Fortinet FG300E

La configuración de los firewalls Fortinet 300E fue realizada con el script del Código fuente 2.24.

**Código Fuente 2.24:** Configuración SNMP FORTINET FG300E

```
config system snmp community
    edit 10
        set name nombre_comunidad
        config hosts
            edit 1
                set ip ip_zabbix mascara_zabbix
            next
        end
        set query-v1-status disable
        set trap-v1-status disable
    next
end
#Verificacion
show system snmp community
```

#### 2.2.2.9. Equipos Fortianalyzer FAZ200F

La configuración de los equipos Fortianalyzer FAZ200F fue realizada con el script del Código fuente 2.25.

**Código Fuente 2.25:** Configuración SNMP FORTINET Fortianalyzer FAZ200

```
config system snmp community
    edit 1
        set events disk_low intf_ip_chg sys_reboot cpu_high mem_low
           log-alert log-rate log-data-rate lic-gbday cpu-high-
           exclude-nice
            config hosts
                edit 1
                    set ip ip_zabbix mascara_zabbix
                next
            end
        set name "nombre_comunidad"
    next
end
#Verificacion
show system snmp community
```

### 2.2.2.10. Equipos Hirschmann MACH1020

La configuración de los equipos Hirschmann MACH1020 fue realizada con el script del Código fuente 2.26.

**Código Fuente 2.26:** Configuración SNMP HIRSCHMANN MACH102

```
configure
snmp-access global enable
snmp-access version v2 enable
snmp-server community "nombre_comunidad"
exit
copy system:running-config nvram:startup-config
```

### 2.2.2.11. Equipos Ruggedcom RX1000

Para la configuración del protocolo SNMP en los equipos Ruggedcom RX1000 se realizó el siguiente procedimiento:

1. Ingresar al dispositivo vía web (https port 10000)
2. En el menú, seleccionamos la opción *"SNMP Configuration"*

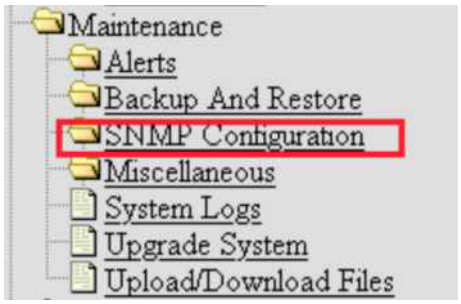
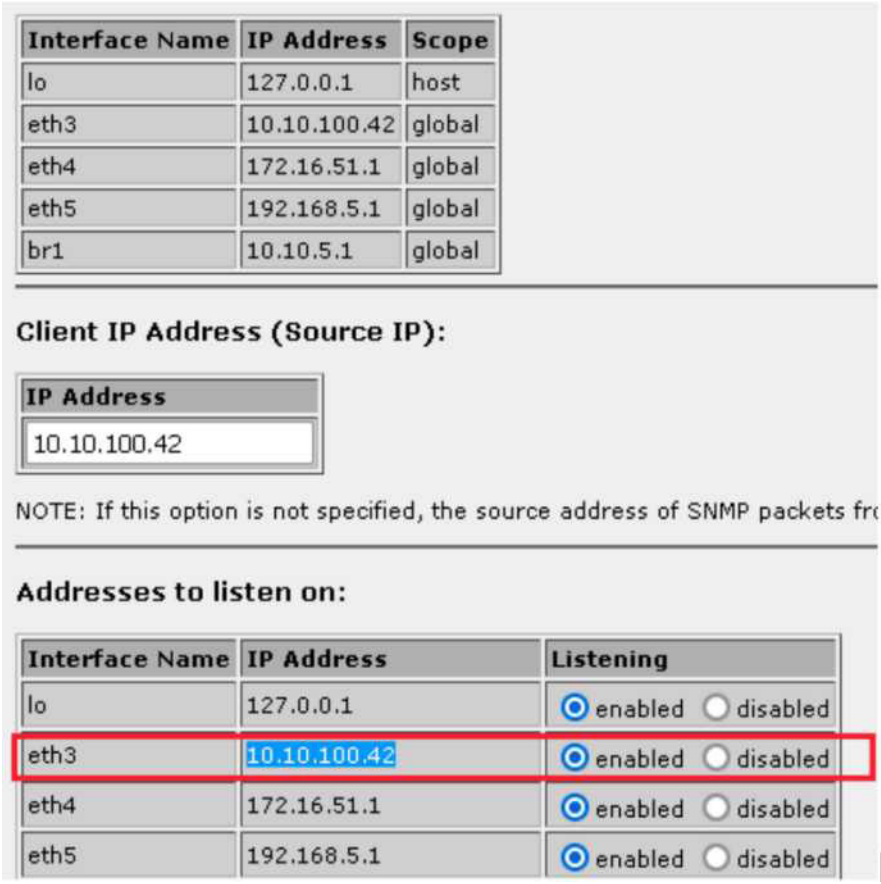



**Figura 2.111:** Menú de configuración SNMP equipos Ruggedcom RX1000

3. Seleccionar el icono *"Network Addressing Configuration"*


**Figura 2.112:** Menú de configuración de direcciones IP para SNMP en equipos Ruggedcom RX1000

4. Se debe verificar que la dirección IP con la que se trabajara esta habilitada para SNMP (en nuestro caso 10.10.100.42)



| Interface Name | IP Address | Scope |
|---|---|---|
| lo | 127.0.0.1 | host |
| eth3 | 10.10.100.42 | global |
| eth4 | 172.16.51.1 | global |
| eth5 | 192.168.5.1 | global |
| br1 | 10.10.5.1 | global |

**Client IP Address (Source IP):**

| IP Address |
|---|
| 10.10.100.42 |

NOTE: If this option is not specified, the source address of SNMP packets fr

**Addresses to listen on:**

| Interface Name | IP Address | Listening |
|---|---|---|
| lo | 127.0.0.1 | enabled disabled |
| eth3 | 10.10.100.42 | enabled disabled |
| eth4 | 172.16.51.1 | enabled disabled |
| eth5 | 192.168.5.1 | enabled disabled |

**Figura 2.113:** Menú de configuración de direcciones IP para SNMP - direcciones asignadas

5. Aplicar los cambios realizados y regresar a la configuración. SNMP

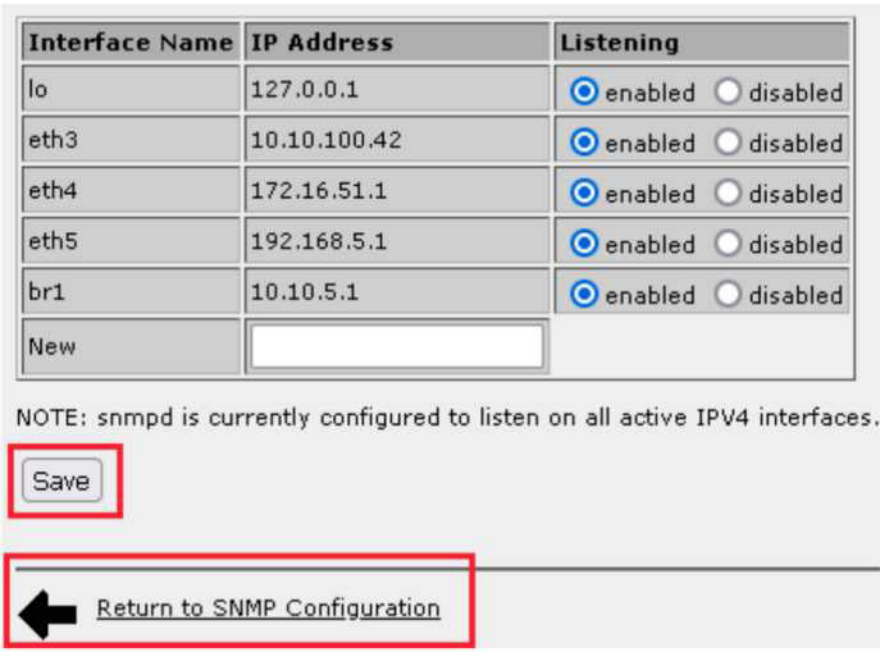



**Figura 2.114:** Menú de configuración de direcciones IP para SNMP - guardar cambios

6. Seleccionar el icono *"Access Control"*


**Figura 2.115:** Configuración de la lista de control de acceso para la IP de la herramienta Zabbix

7. Llenar los campos *"Community Name"* y *"Source IP"* y pinchar en *"Add"*

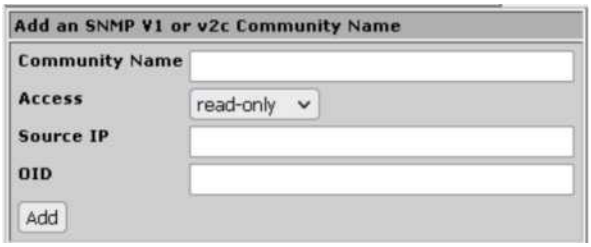



**Figura 2.116:** Configuración de la comunidad y dirección IP

8. La configuración aplicada se mostrará en la parte superior


**Figura 2.117:** Chequeo de la configuración aplicada

9. Por *default* el demonio SNMPD viene deshabilitado. Para habilitarlo, se selecciona la opción *"Bootup and Shutdown"* del menú principal


**Figura 2.118:** Habilitación del demonio SNMPD - acceso desde el menú principal

10. Dar clic en el checkbox del demonio *"snmp"*


**Figura 2.119:** Habilitación del demonio SNMPD

11. Posteriormente pinchar en el botón *"Start SelectednNow And Boot"*

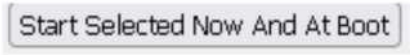



**Figura 2.120:** Encendido del demonio SNMPD

12. Instantes después se podrá visualizar que el demonio snmpd está corriendo

| | | | | |
|---|---|---|---|---|
| ☐ | snmpd | Yes | Yes | SNMP (Simple Network Management Protocol) |

**Figura 2.121:** Chequeo del encendido del demonio SNMPD

### 2.2.2.12. Equipos Redline RDL3100

Para la configuración de los equipos Redline RDL3100 se realizó el siguiente proceso:

1. Ingresar al dispositivo vía WEB (https)
2. En el menú principal se selecciona *"SNMP"*


**Figura 2.122:** Menú de configuración SNMP en equipos Redline RDL3100

3. En la sección *"SNMP Communities"* seleccionar *"Add"* y posteriormente llenar los campos de la comunidad SNMP y pinchar en el botón *"Add Community"*


**Figura 2.123:** Configuración de las comunidades SNMP

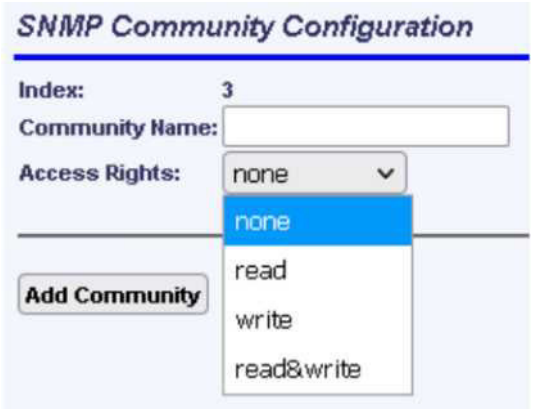



**Figura 2.124:** Configuración de las comunidades SNMP - permisos.

4. Una vez que se ha añadido la comunidad *SNMP*, aplicar y guardar la configuración


**Figura 2.125:** Guardar la configuración realizada

#### 2.2.2.13. Configuración De Alerta Temprana Y Notificación Vía Correo Electrónico

Luego de haber reintegrado los equipos terminales de redes hacia la herramienta Zabbix, de contar con pantallas de visualización de la Red LAN interna en cada uno de los nodos de la Red WAN el siguiente paso es la habilitación de la emisión de alertas tempranas vía correo electrónico. Contar con la habilitación de esta característica permitirá disminuir los tiempos de respuesta y elevar la disponibilidad de la red de datos Optimizando la gestión de recursos técnicos involucrados en realizar un monitoreo manual de la infraestructura integrada a la herramienta Zabbix.

La habilitación de la emisión de alertas tempranas mediante correo electrónico toma como punto de inicio contar con una cuenta de correo desde la cual la herramienta Zabbix generen los correos electrónicos que serán enviados hacia los administradores de la red de datos. Los contenidos de estos correos son generados con base en ciertas plantillas en donde se indican los equipos terminales alarmados y mensajes básicos que detallan los problemas reportados sobre estos equipos. Para la habilitación de estas características decía siguiente proceso:

1. Seleccionar el menú Administración y dentro de este seleccionar tipos de medios.
2. Luego de ingresar el menú medios se despliegan los tipos de medios a través de los cuales se generarán las alertas tempranas, de entre estas posibilidades se seleccionó


**Figura 2.126:** Acceso a la configuración de emisión de alertas tempranas

usar `Email`[3]. Los mensajes generados usando esta característica se envían en texto plano.

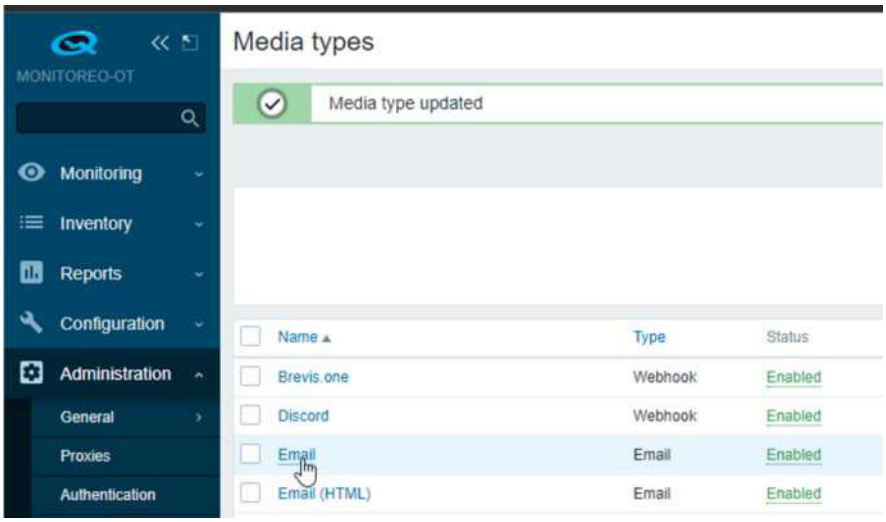



**Figura 2.127:** Opciones para la emisión de alertas tempranas

3. En el submenú tipo de medio, colocar el nombre del servidor *SMNT*, el puerto, el email desde el cual se enviaran la alertas, en seguridad de la conexión seleccionar de acuerdo al número de puerto usado, en este caso la selección correspondiente al puerto 465 es *SSL/TLS*, en autenticación seleccionar usuario y contraseña y colocar las credenciales.

[3] **Email(HTML):** es una variante de *Email* con texto formateado en lenguaje html

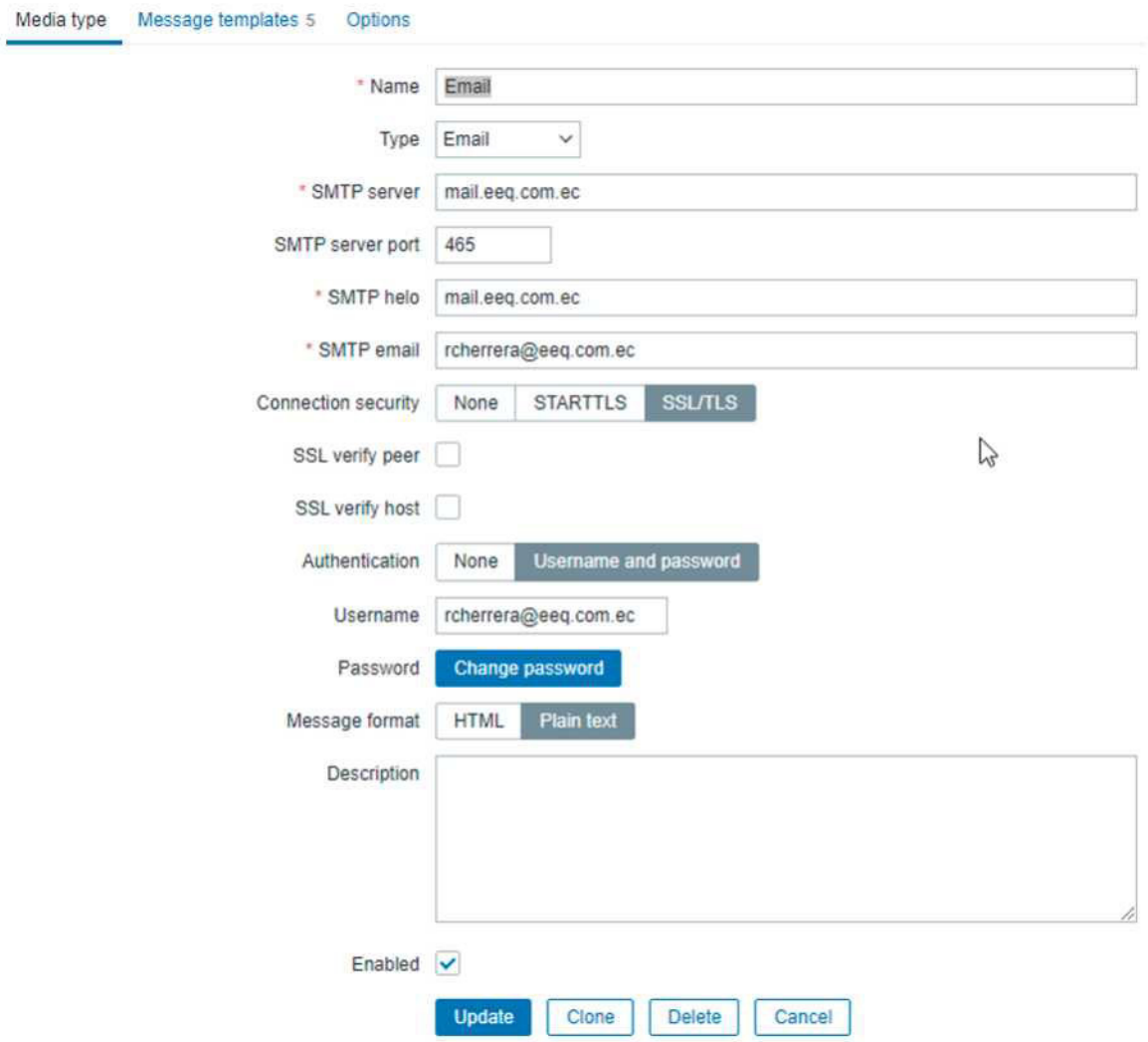



**Figura 2.128:** Configuración de la emisión de alertas tempranas a través del correo origen

4. En el menú de configuración *Media types* se configura el número de intentos en un valor de 1, en intervalos de 10 segundos.

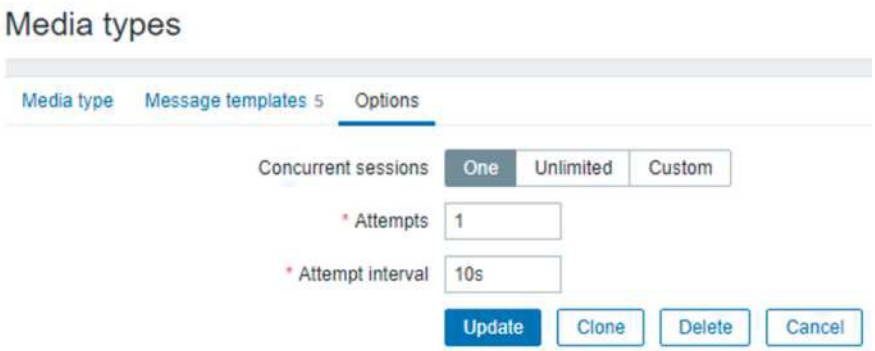



**Figura 2.129:** Configuración de número de intentos a intervalos de cinco reintentos

5. Luego desde el menú de administración seleccionar usuarios.


**Figura 2.130:** Configuración de usuarios para la emisión de alertas tempranas

6. En el menú de usuario se debe seleccionar el usuario a través del cual se generarán los correos con la emisión de alertas tempranas, para este escenario de configuración se seleccionó el usuario administrador.


**Figura 2.131:** Asignación de usuarios para la emisión de alertas tempranas

7. Una vez seleccionado el usuario luego en el menú superior seleccionar el medio.


**Figura 2.132:** Selección de medio por el cual el usuario asignado emitirá las alertas tempranas

8. Seleccionar en tipo de medio Email, en enviar a colocar el correo electrónico al cual se van a enviar las alertas, en horario de actividad establecer que el envío de alertas se mantenga los siete días de la semana y las veinticuatro horas del día y en severidad seleccionamos en que tipo de nivel de incidencias (no clasificado, información, advertencia, medio, alto, desastre) queremos que se envíe la advertencia mediante correo electrónico.

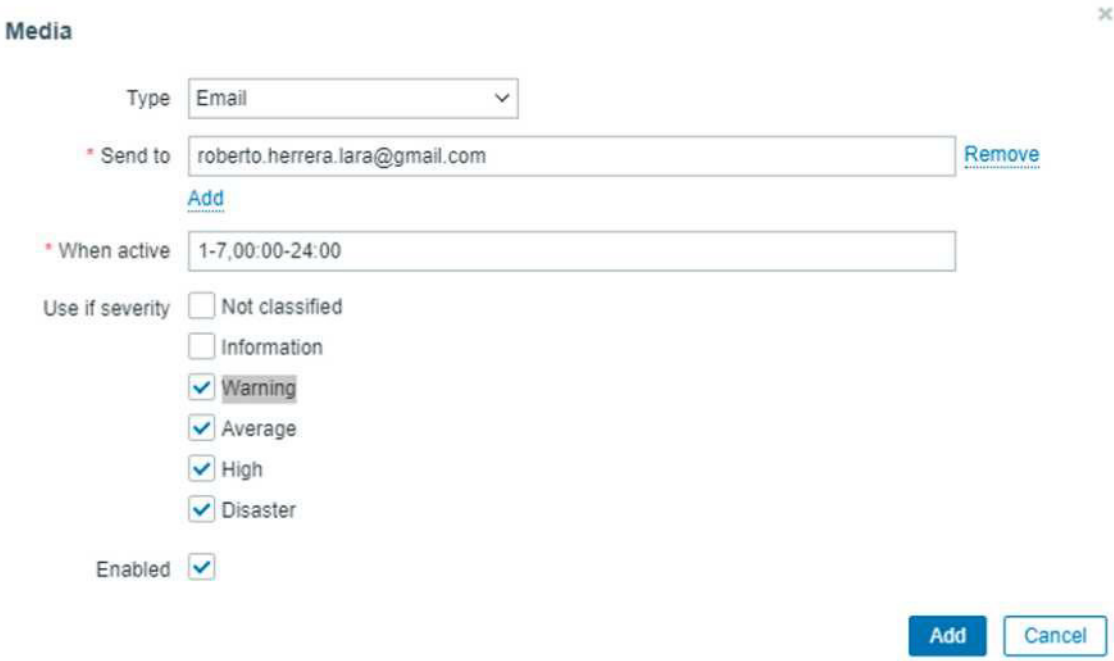



**Figura 2.133:** Configuración de los parámetros de emisión de las alertas tempranas

9. Luego desde el menú de configuración seleccionar acciones.

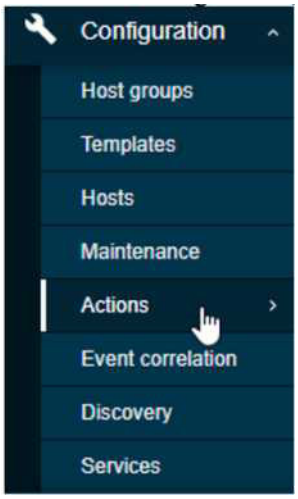



**Figura 2.134:** Selección del submenú acciones

10. Desde el menú acciones habilitar la opción de reportar problema al administrador de Zabbix.

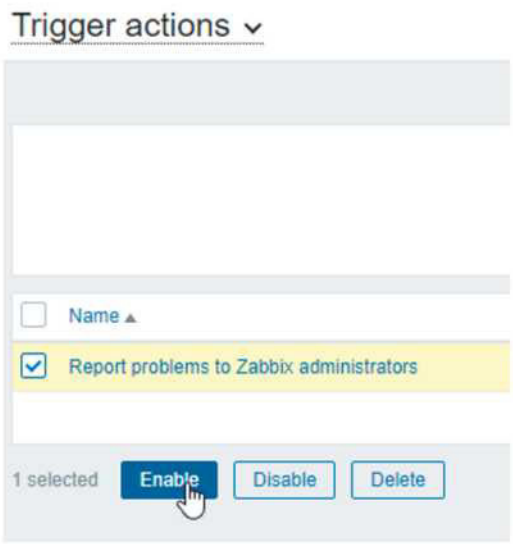



**Figura 2.135:** Habilitación de reportes de problemas vía alertas tempranas

11. En el menú de configuración seleccionar acciones.

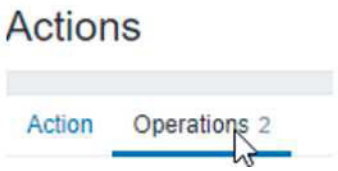



**Figura 2.136:** Menú de configuración, selección submenú acciones

12. Habilitación de disparadores (trigger) para el reporte de problemas.

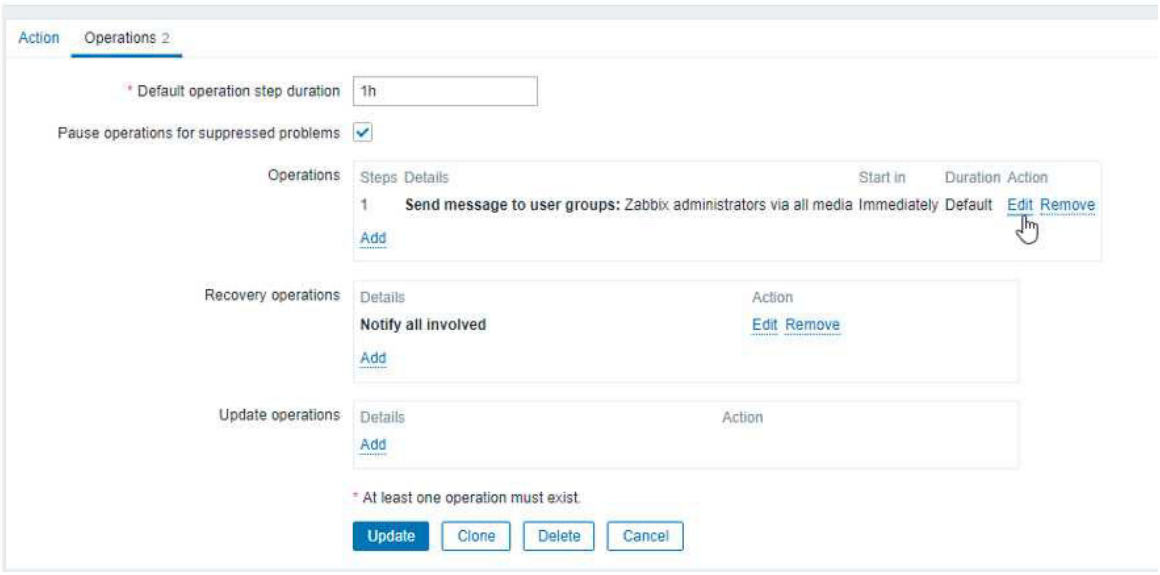



**Figura 2.137:** Habilitación de disparadores (trigger)

13. En el menú superior seleccionar el submenú operaciones.

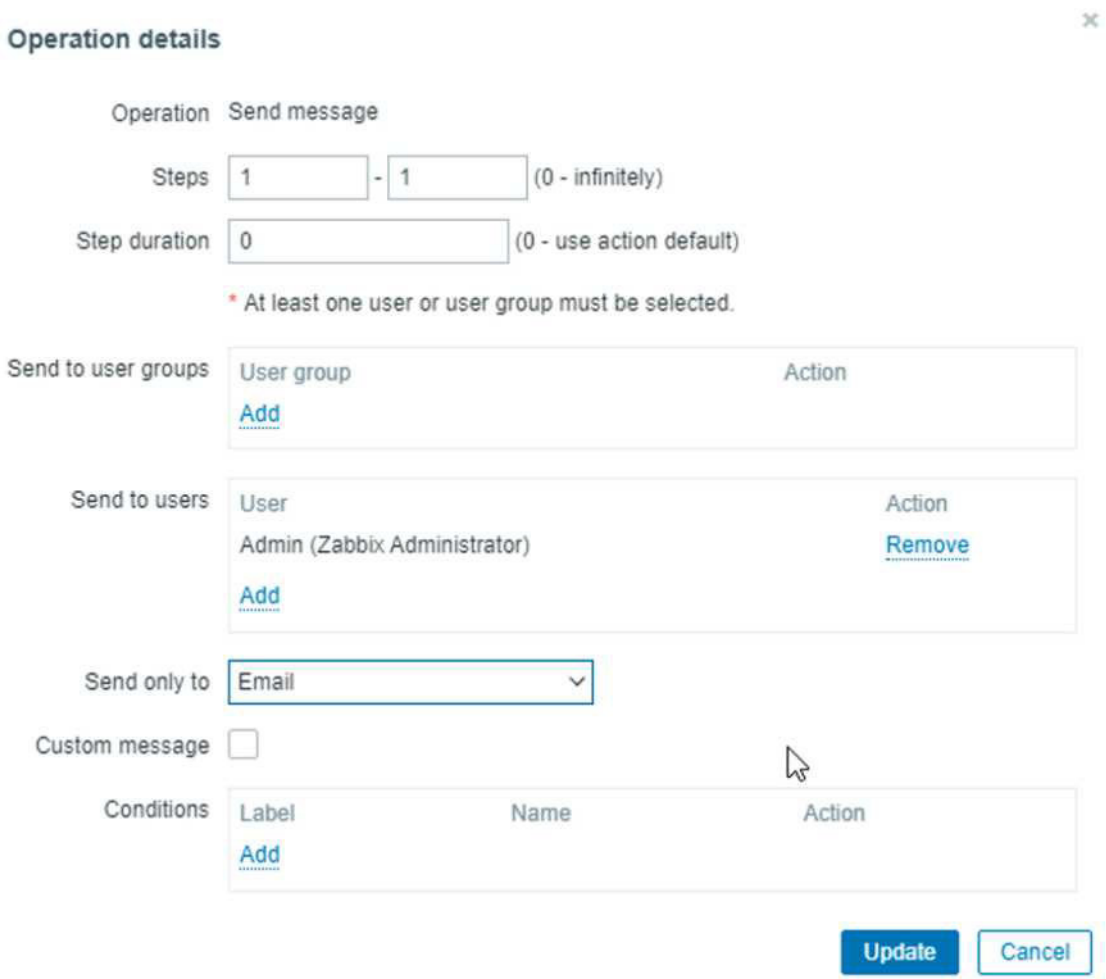



**Figura 2.138:** Selección del menú operaciones

14. Verificar el envío de alertas al correo electrónico. En el menú reportes dar clic en registros de acción, se visualiza las alertas enviadas al email establecido.

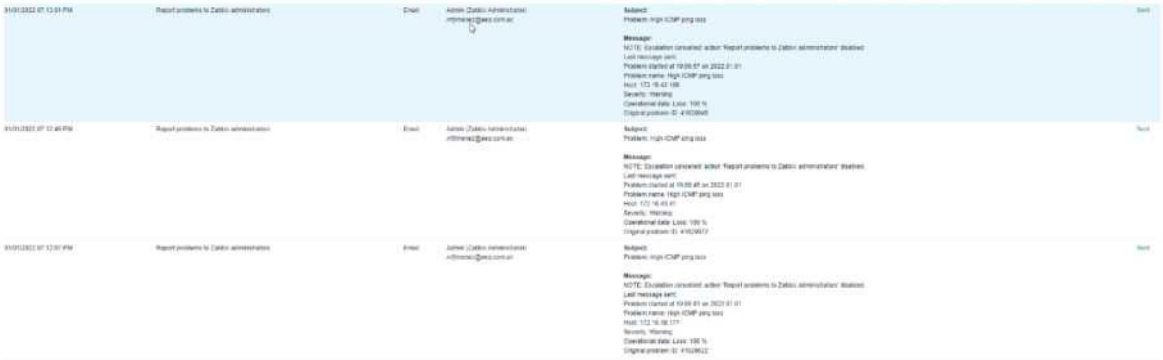


**Figura 2.139:** Verificación de envío de alertas

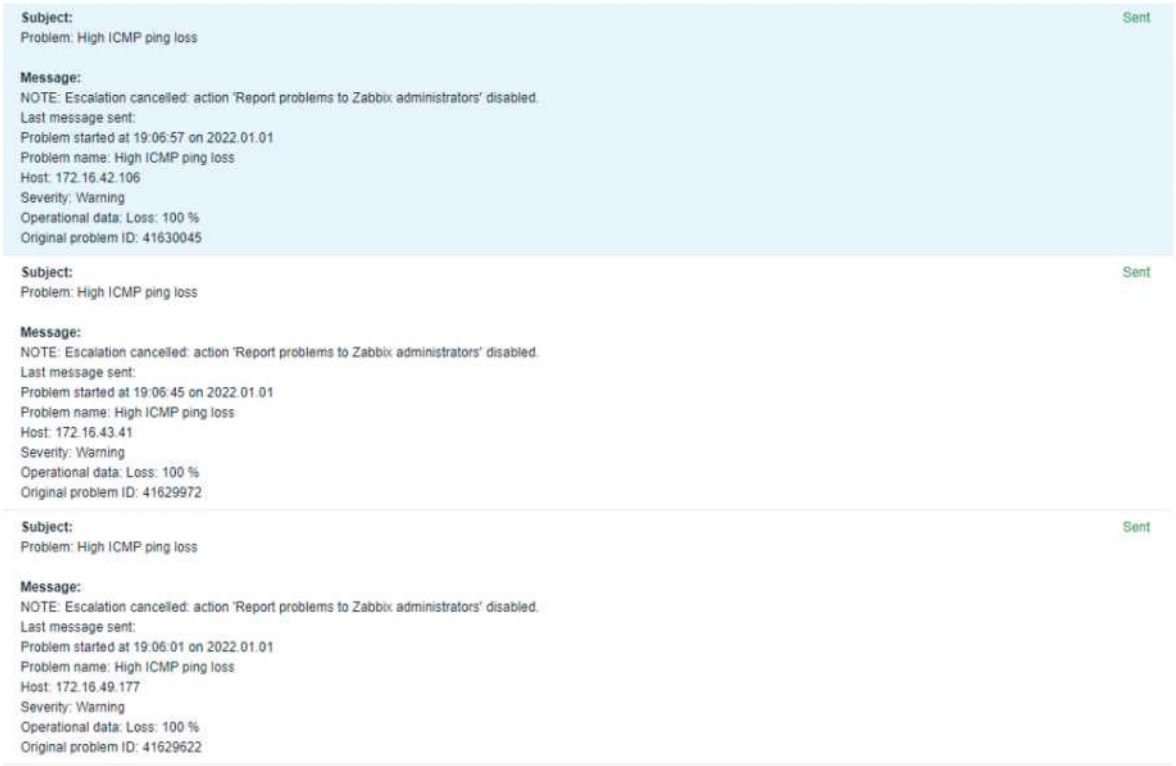



**Figura 2.140:** Verificación de envío de alertas - detalle de envíos

15. Verificación de recepción de los correos de alerta temprana y en las bandejas de las cuentas asignadas


**Figura 2.141:** Correo de alerta temprana emitida con reporte de problema equipo fuera de Red

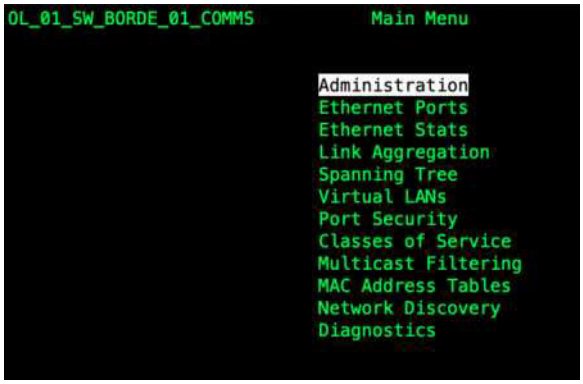

**Figura 2.142:** Correo de alerta temprana emitida con reporte de problema equipo (Reconectador R0411) fuera de Red

### 2.2.3. PROCEDIMIENTO DE INTEGRACIÓN DE LOS EQUIPOS A LA HERRAMIENTA LOG-ANALYZER

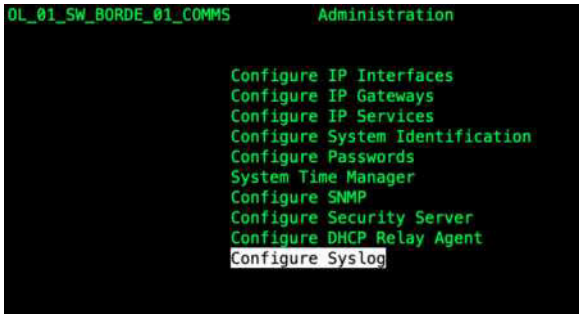
Para la integración de los equipos terminales hacia el gestor de registros de eventos (logs) es suficiente con asignar la dirección IP del servidor de recepción de los mensajes del protocolo SYSLOG en la configuración de los equipos de red y demás equipamiento que cuente con esta funcionalidad. Como detalle adicional en la configuración se debe tener en cuenta que el puerto destino para la emisión de mensajes debe ser el 514 ya sea UDP o TCP.

En la configuración de los equipos terminales consideraciones adicionales pueden ser realizadas para la habilitación del protocolo Syslog, sin embargo, para los propósitos de este trabajo de titulación la configuración tiene como alcance la emisión de mensajes hacia el

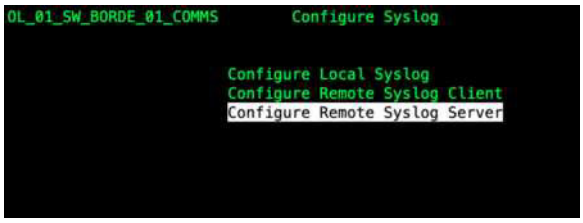
servidor desplegado. En la Figura 2.143 se muestra un ejemplo básico de la configuración del protocolo Syslog hacia el servidor desplegado.



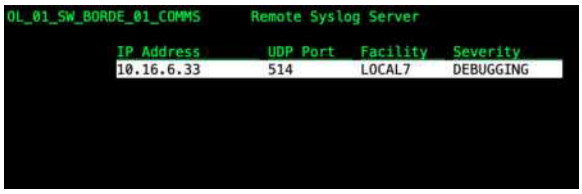

**(a)** Menú de configuración inicial



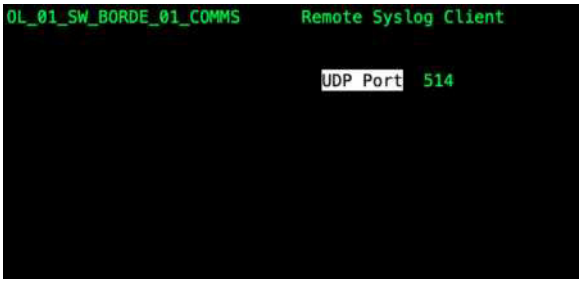

**(b)** Selección de configuración protocolo Syslog




**(c)** Configuración de servidor Syslog




**(d)** Configuración del puerto de emisión de mensajes Syslog




**(e)** Configuración de los datos del servidor Syslog

**Figura 2.143:** Ejemplo de configuración del protocolo Syslog para los equipos Ruggedcom

### 2.2.4. PROCESO DE INTEGRACIÓN DE EQUIPOS DE RED A LA HERRAMIENTA ZABBIX USANDO EL PROTOCOLO SNMP

La integración de los equipos de red a la herramienta Zabbix usando SNMP se la realizó siguiendo los siguientes pasos:

1. Ingresar el equipo a la herramienta de monitoreo a traves del menu Configuración → Hosts → Create new host, en donde se mostrará, tal como se muestra en la en la Figura 2.144.

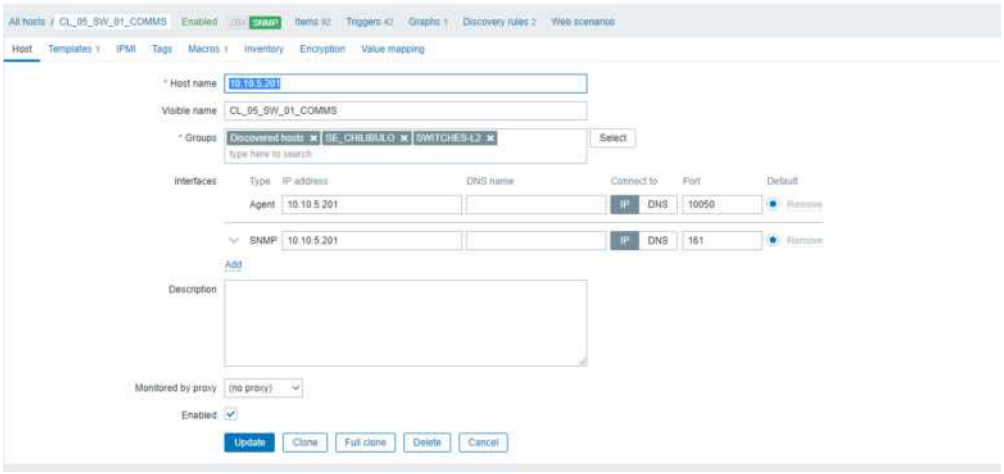



**Figura 2.144:** Pantalla inicial de ingreso de un equipo nuevo a la herramienta Zabbix

2. En el menu de plantillas disponibles se debe escoger *Network Generic Device Template* , tal como se muestra en la en la Figura 2.145.

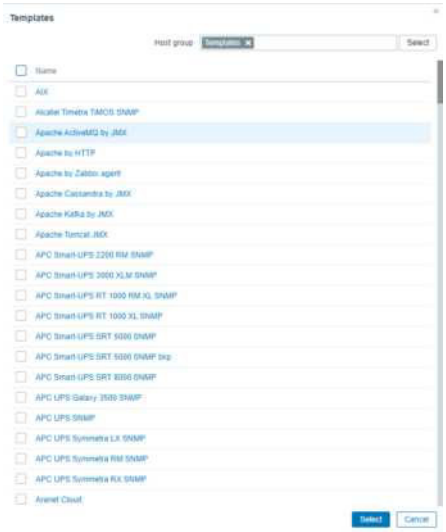



**Figura 2.145:** Asignación de plantilla de monitoreo al equipo nuevo ingresado a la herramienta Zabbix

3. Una vez se haya asignado la plantilla *Network Generic Device Template*, se debera guardar la configuración dando click en *Update*, tal como se muestra en la en la Figura 2.146.

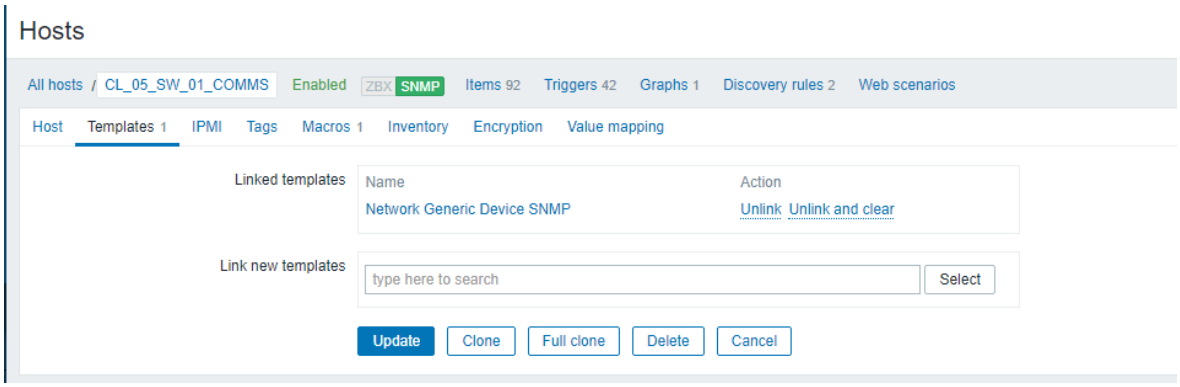



**Figura 2.146:** Confirmación de captura de datos usando ICMP sobre el equipo ingresado

4. El siguiente paso es asignar el nombre de la comunidad que consta en la configuración del equipo de red que esta siendo agregado, este proceso se lo realizó tal como se muestra en la en la Figura 2.147.

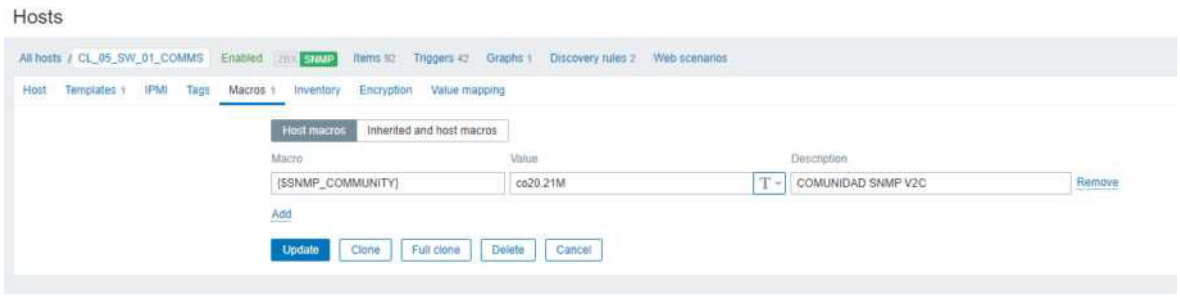



**Figura 2.147:** Confirmación de la plantilla de monitoreo asignada al equipo nuevo ingresado a la herramienta Zabbix

5. Para confirmar la configuración adecuada del ingreso de los nuevos equipos a la herramienta de monitoreo se debe buscar el equipo en el menu de monitoreo y acceder al submenu de *Latest data*, tal como se muestra en la en la Figura 2.148.

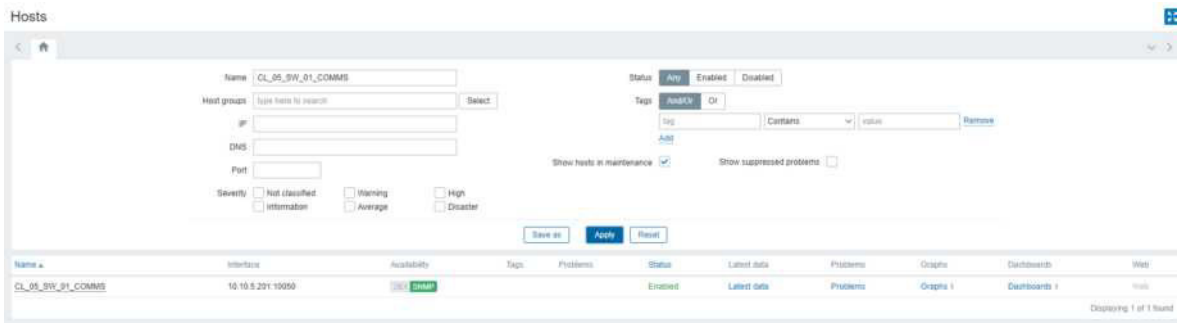



**Figura 2.148:** Confirmación de la plantilla de monitoreo asignada al equipo nuevo ingresado a la herramienta Zabbix

6. Finalmente los datos que se estan adquiriendo a traves de la herramienta de monitoreo desde el equipo terminal se proyectaran en pantalla de manera similar a lo mostrado en la Figura 2.149.

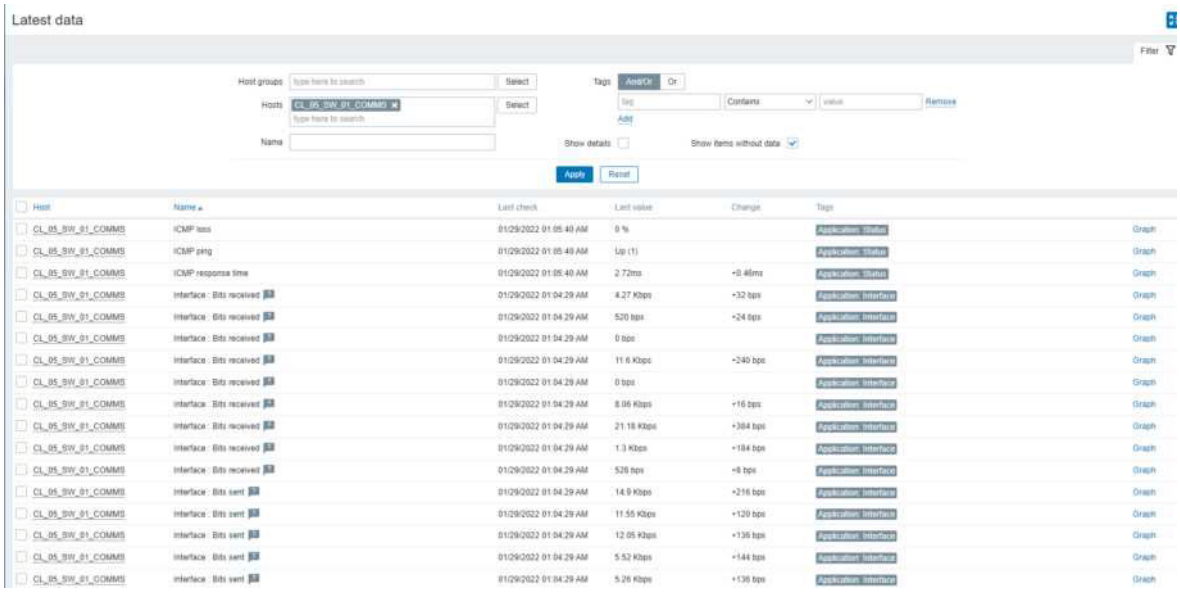



**Figura 2.149:** Visualización los datos capturados usando ICMP sobre el equipo ingresado

7. Uno de las situaciones más útiles de tener integrado los equipos de redes por medio del protocolo SNMP es contar con información en tiempo real del tráfico de datos a través de los puertos de red de los equipos áctivos, un ejemplo de esto se presenta en la Figura 2.150.


**Figura 2.150:** Visualización los datos de tráfico recibidos a través del protocolo SNMP sobre el equipo ingresado

### 2.2.5. PROCESO DE INTEGRACIÓN DE RTUS, IEDS, RECONECTADORES A LA HERRAMIENTA ZABBIX

Las Unidades Remotas de Control (RTU) son computadoras de propósito específico que tienen por objetivo procesar la información generada por los equipos electrónicos inteligentes IED y en base a las lógicas de control presentes en su configuración toman decisiones sobre el infraestructura de control industrial de una subestación, central de generación o grupo de reconectadores. En la Figura 2.151 se presenta un ejemplo de una RTU de marca SIEMENS.

**Figura 2.151:** Unidad Remota de Control - RTU

Las Equipos Electrónicos Inteligentes (IED) son equipos electrónicos destinados a tomar mediciones analógicas y digitales sobre la red eléctrica, recibir y ejecutar las órdenes o comandos emitidos por las unidad remota de control (RTU). En la Figura 2.152 se presenta ejemplos de IEDs en varias marcas y modelos.

Las reconectadores son equipos eléctricos de pontencia que sirven para ejecturar operaciones sobre la red eléctrica los cuales en acompañamiento a un sistema de control electrónico pueden ser tele comandados y automatizados a través del uso de equipos electrónicos inteligentes y unidades remotas de control. En la Figura 2.153 se presenta un ejemplo comparativo de un reconectar sin caja de control y uno con caja de control y automatización.

Para propósitos prácticos de este trabajo de titulación las RTUs, IEDs y reconectadores serán tratados como equipos terminales que disponen de una tarjeta de red. Para este grupo de equipos en específico la integración en la herramienta de monitoreo si la realizó a través del protocolo ICMP, es decir se realiza un monitoreo pasivo de su disponibilidad, tiempos de respuesta y confiabilidad del enlace de la red de datos (niveles de pérdidas / ICMP loss).

**(a)** IEDs de la marca ABB

**(b)** IEDs de la marca Siemens

**(c)** IEDs de la marca Schneider Electric

**(d)** IEDs de la marca Ingeteam

**Figura 2.152:** Equipos electrónicos inteligentes (IEDs) de diferentes marcas y modelos

**(a)** Reconectador eléctrico sin equipos de control remoto

**(b)** Reconectador eléctrico con equipamiento para control remoto

**Figura 2.153:** Reconectador eléctrico sin equipos de control remoto versus Reconectador eléctrico con equipamiento para control remoto

La integración de las RTUs, IEDs y reconectadores se la realizó siguiendo los siguientes pasos:

1. Ingresar el equipo a la herramienta de monitoreo a traves del menu Configuración → Hosts → Create new host, en donde se mostrará, tal como se muestra en la en la Figura 2.154.

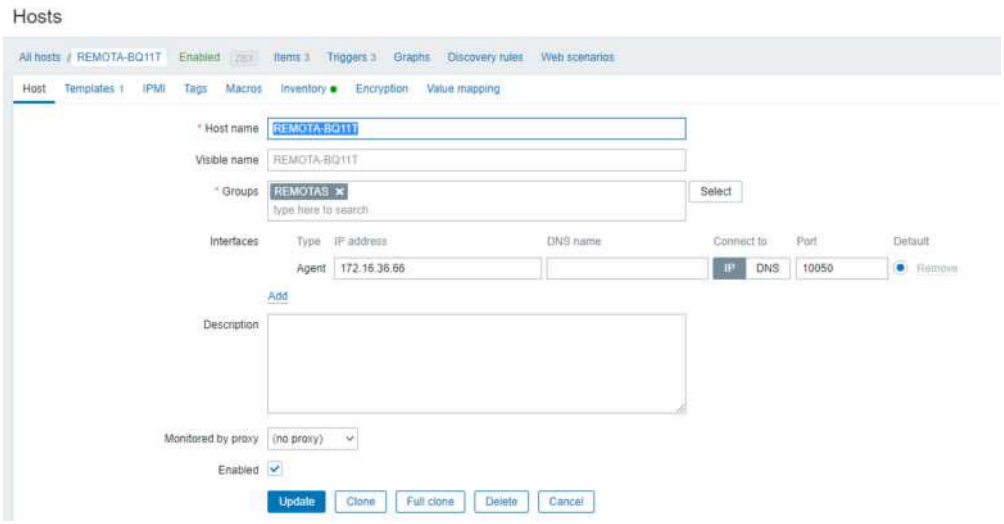



**Figura 2.154:** Pantalla inicial de ingreso de un equipo nuevo a la herramienta Zabbix

2. En el menu de plantillas disponibles se debe escoger *ICMP Template* , tal como se muestra en la en la Figura 2.155.

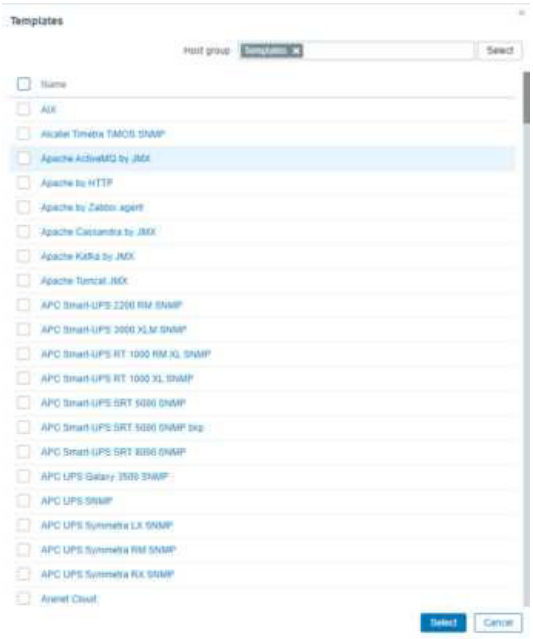



**Figura 2.155:** Asignación de plantilla de monitoreo al equipo nuevo ingresado a la herramienta Zabbix

3. Una vez se haya asignado la plantilla ICMP Template, se debera guardar la configuración dando click en *Update*, tal como se muestra en la en la Figura 2.157.

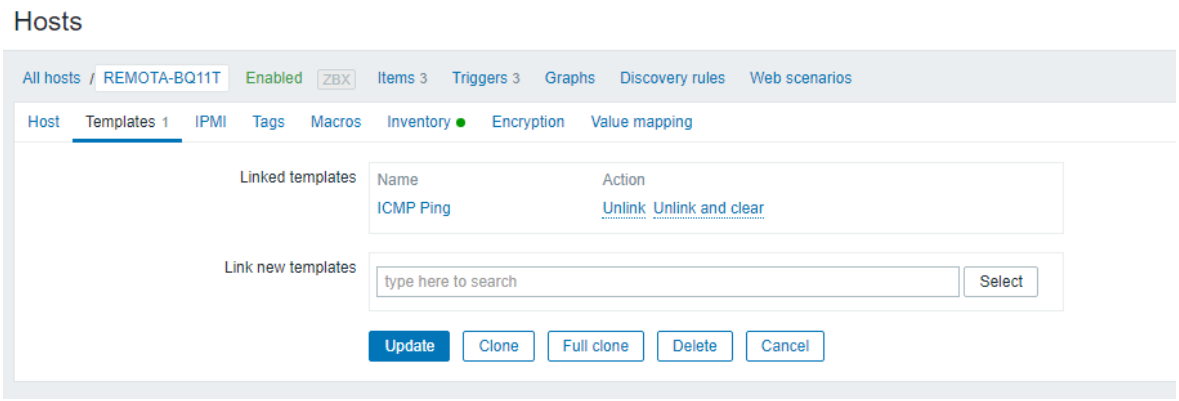



**Figura 2.156:** Confirmación de captura de datos usando ICMP sobre el equipo ingresado

4. Para confirmar la configuración adecuada del ingreso de los nuevos equipos a la herramienta de monitoreo se debe buscar el equipo en el menu de monitoreo y acceder al submenu de *Latest data*, tal como se muestra en la en la Figura 2.156.

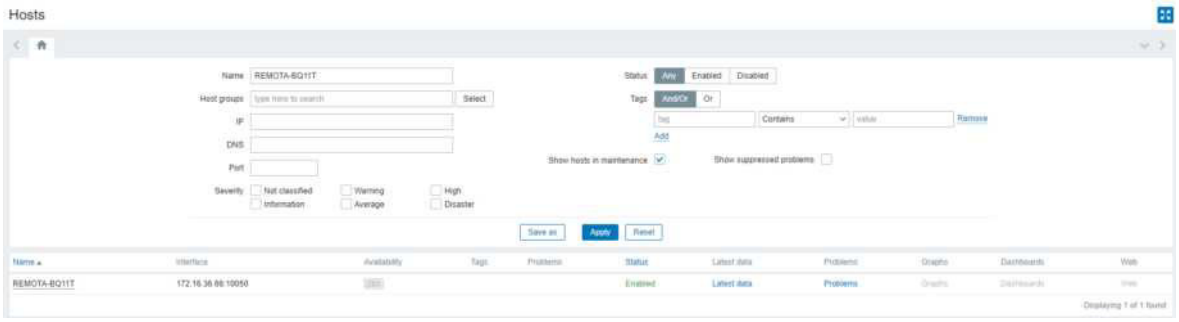



**Figura 2.157:** Confirmación de la plantilla de monitoreo asignada al equipo nuevo ingresado a la herramienta Zabbix

5. Finalmente los datos que se estan adquiriendo a traves de la herramienta de monitoreo desde el equipo terminal se proyectaran en pantalla de manera similar a lo mostrado en la Figura 2.158.

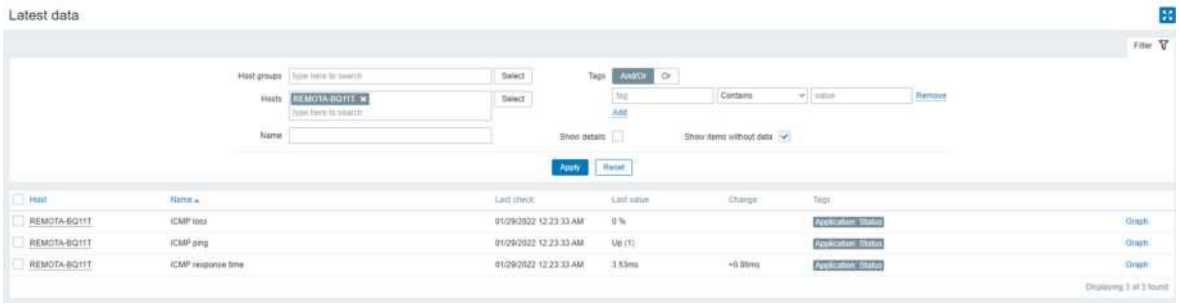



**Figura 2.158:** Visualización los datos capturados usando ICMP sobre el equipo ingresado

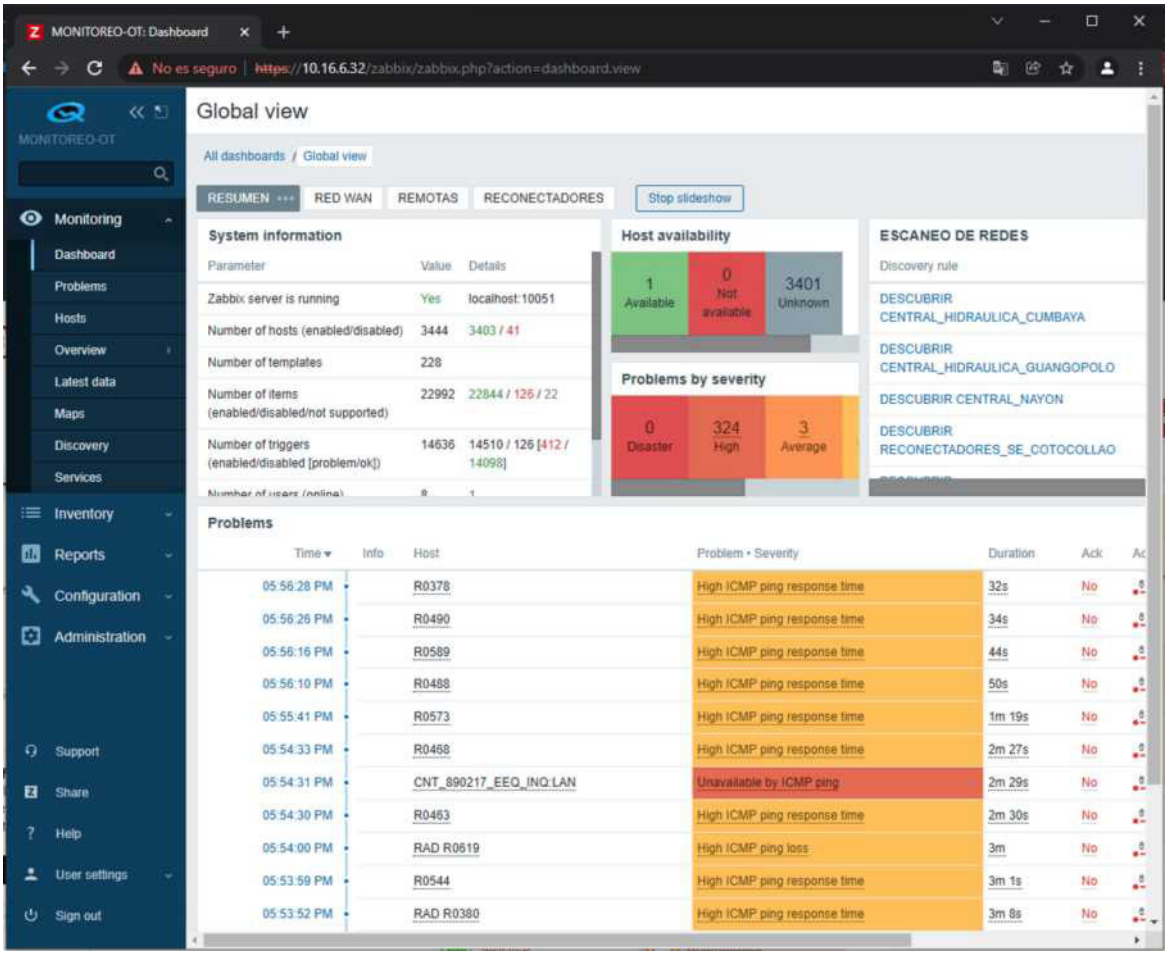
### 2.2.6. CONFIGURACIÓN DE LAS PANTALLAS DE INICIO EN LAS HERRAMIENTAS INSTALADAS

Luego de finalizada la instalación de la herramienta Zabbix siguiente paso a realizar es la configuración de las pantallas de inicio. En esta configuración se define la información que se mostrará como primer contacto con la pantalla, diagramas de monitoreo, pantallas deslizantes, ubicación de alarmas, y demás detalles fijados en la etapa de diseño.

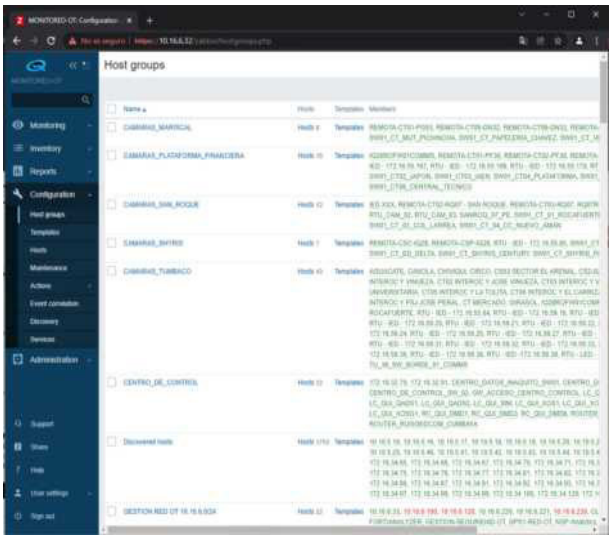
En la Figura 2.159a se muestran las implementaciones realizadas en la configuración de las pantallas, donde en la pantalla inicial se presenta el resumen de los equipos integrados a la solución, supervisión de redes mediante escaneo continuo, gestión de alarmas y monitoreo en tiempo real, pantallas deslizantes en donde se despliega la Red WAN, el conjunto de unidades remotas de control y el conjunto de reconectadores como equipo crítico a ser monitoreado.

En la Figura 2.159b y Figura 2.159c se configuran los grupos de equipos terminales y se realizan los esquemas de red a ser monitoreados. Los diagramas de Red desarrollados en la Figura 2.159c pueden ser utilizados en cualquiera de las pantallas deslizantes mostradas en la Figura 2.159a, ya sea como pantallas individuales o como en mapas subordinados. Para el caso la pantalla demostrada como Red WAN Dispone de diagramas ordenados en los que se muestran interconectadas las subestaciones, centrales de generación, puntos de acceso hacia la Red inalámbrica de reconectadores, cámaras de soterramiento, Centros de Datos y Centro de control.

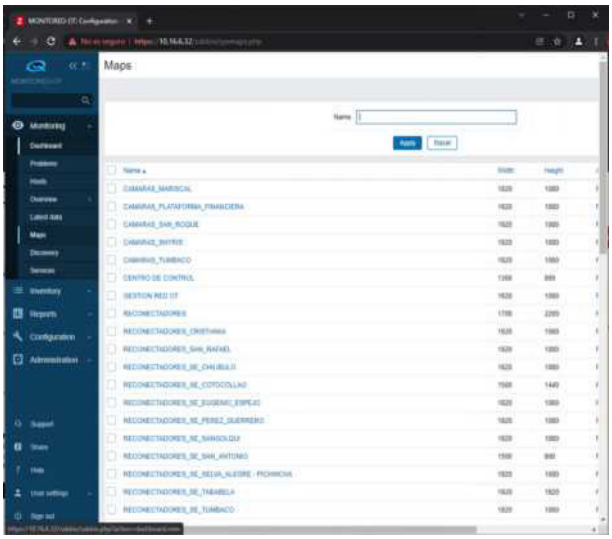
En la Figura 2.160 se muestren en detalle las pantallas configuradas para el monitoreo de estos de los sistemas industriales de la E.E.Q. En la Red WAN se pueden visualizar de manera clara los estados normal y alarmados de las redes de datos locales integradas en el diagrama. Estas redes a su vez pueden ser visualizadas a través del acceso a los mapas subordinados teniendo la capacidad de disponer del detalle del comportamiento de los equipos terminales monitoreados. En caso de necesitarse métricas adicionales de equipos específicos se puede acceder dando un clic directamente sobre el equipo y accediendo al menú $\gg$ `Latest data`, dónde se disponen de todas las métricas que está haciendo recuperadas y almacenados para su análisis como monitoreada la infraestructura instalada.




**(a)** Pantalla inicial configurada - pantallas deslizantes

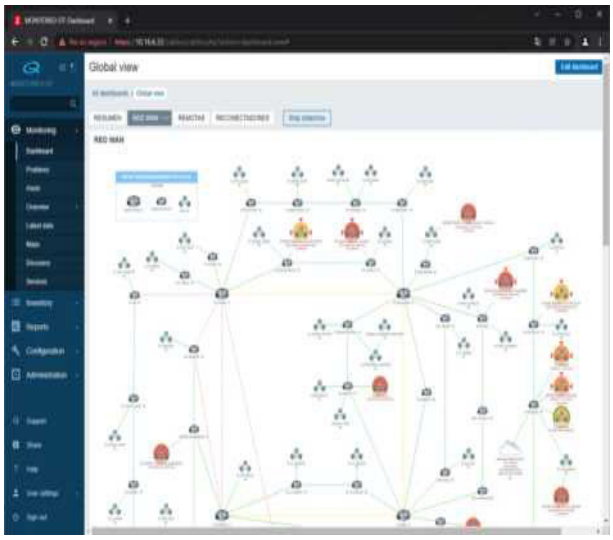



**(b)** Grupos de equipos terminales

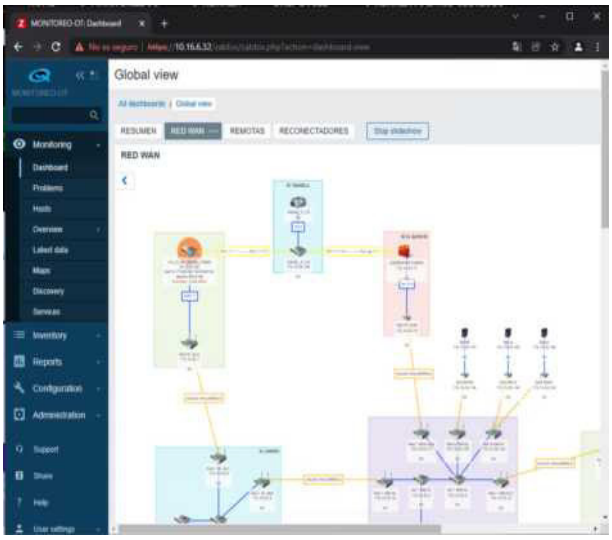



**(c)** Pantalla de configuración de diagramas

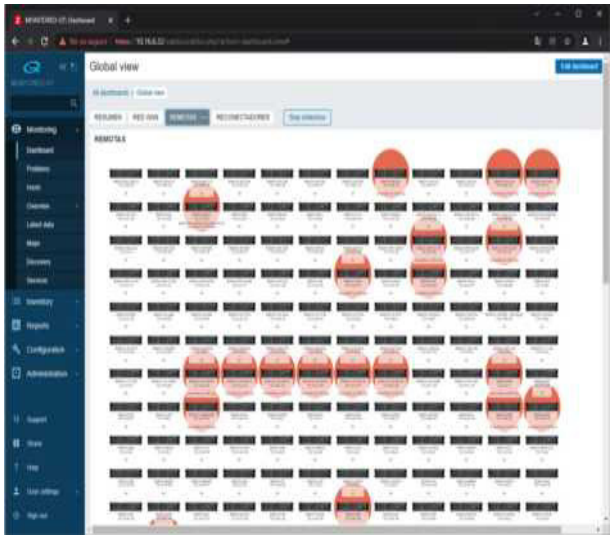
**Figura 2.159:** Configuración inicial de pantallas en Zabbix



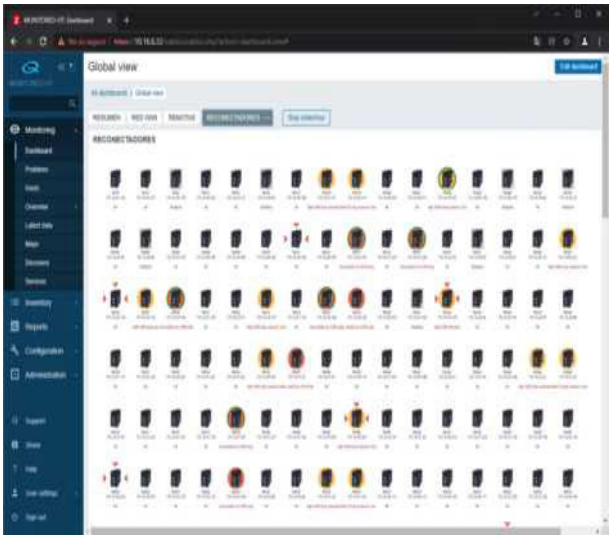

**(a)** Red WAN monitoreada con Zabbix




**(b)** Ejemplo de diagrama subordinado




**(c)** Pantalla creada para el monitoreo de RTUs




**(d)** Pantalla de monitoreo de Reconectadores

**Figura 2.160:** Pantallas configuradas en la solución de monitoreo Zabbix

# 3. RESULTADOS Y DISCUSIÓN

En el presente capítulo se detallan las pruebas de la solución implementada haciendo referencia a los protocolos de gestión utilizados. Para la realización de las pruebas de funcionamiento del despliegue de las herramientas instaladas se fijarán como métricas de evaluación el rendimiento de los recursos asignados para la creación de las máquinas virtuales y la comprobación del funcionamiento según las integraciones y protocolos de gestión habilitados.

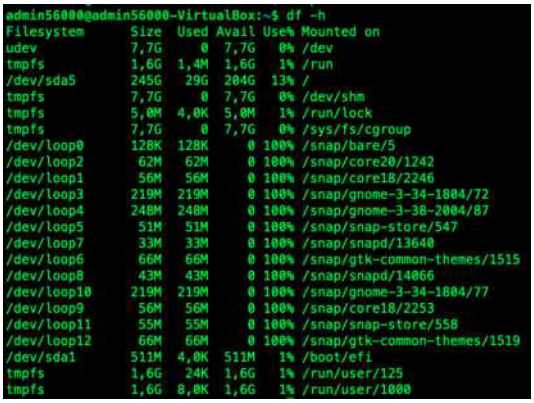
Cómo protocolo de evaluación de la solución desplegada se consideraron las siguientes métricas:

- ❒ Evaluación del rendimiento y uso de los recursos asignados.
- ❒ Funcionalidad de las aplicaciones instaladas.
- ❒ Pruebas de respuesta frente a distintos disparadores (trigers) de alarmas.
- ❒ Generación de reportes e información sumarizada.
- ❒ Generación de alarmas y su emisión como métodos de alerta temprana.

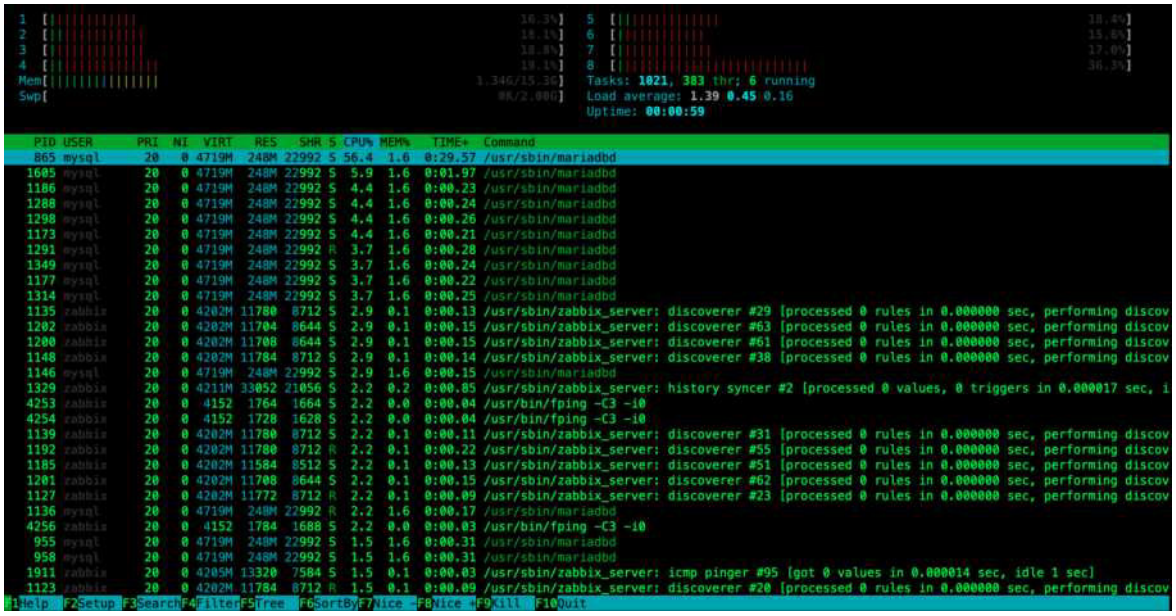
## 3.1. RESULTADOS

### 3.1.1. PRUEBAS DE FUNCIONAMIENTO DE LA HERRAMIENTA ZABBIX

En esta primera sección se realiza una evaluación del desempeño de la máquina virtual creada para la instalación de la herramienta Zabbix. En la Figura 3.1a presenta en los resultados del uso del almacenamiento asignado a la fecha de esta evaluación. En la Figura 3.1b se presenta en los resultados de la evaluación realizada al uso de los procesadores y la memoria RAM asignada.




**(a)** Uso del almacenamiento asignado

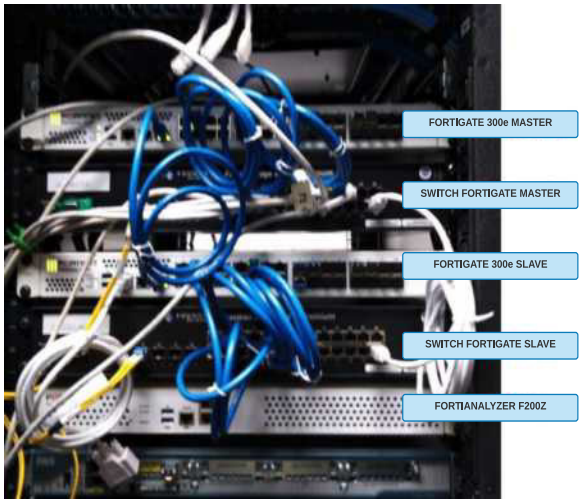



**(b)** Evaluación del uso del procesamiento y la memoria RAM asignada

**Figura 3.1:** Evaluación del rendimiento de la máquina virtual donde se instaló la herramienta Zabbix

#### 3.1.1.1. Pruebas De Funcionamiento Usando El Protocolo SNMP

Para la evaluación de la herramienta usando el protocolo SNMP se realizaron pruebas de funcionamiento a través del análisis del tráfico de la Red de datos usando como herramienta de pruebas el firewall perimetral de la red operativa. En la Figura 3.2a se muestra la conexión del firewall perimetral hacia el hardware físico que aloja la máquina actual en donde se instaló la herramienta Zabbix. En la Figura 3.2b se muestran los resultados del análisis de datos en la Red de ingreso hacia la máquina de la herramienta Zabbix, con lo que se puede comprobar el correcto funcionamiento de la infraestructura instalada.

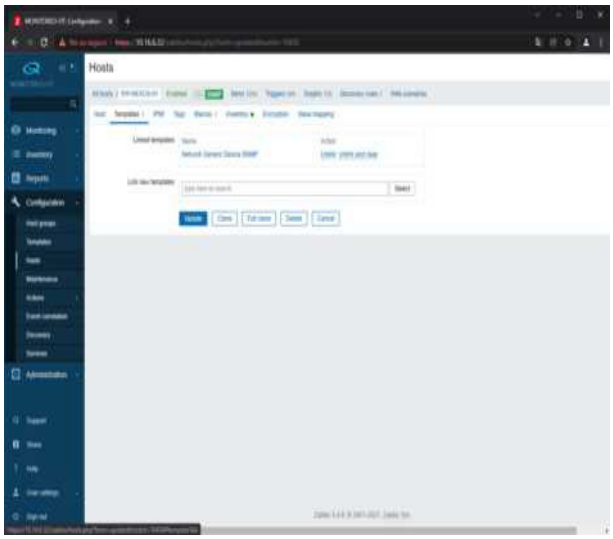



**(a)** Conexiones del firewall perimetral hacia los servidores físicos

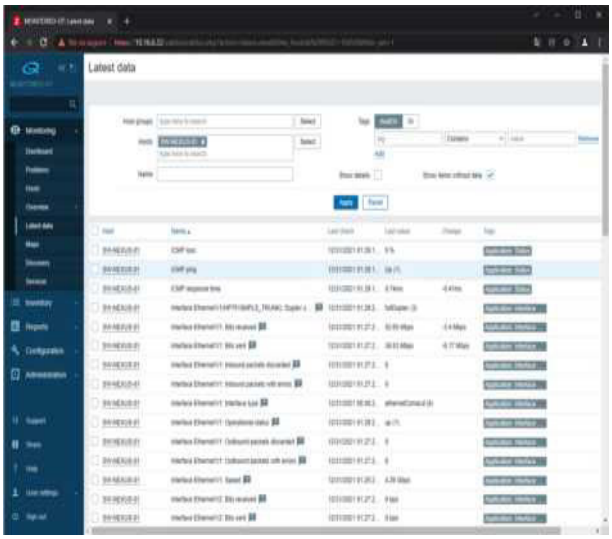
```
FW300E_CORE_SCADA $ diagnose sniffer packet any 'port 161 and net 10.16.6.32/32' 4
interfaces=[any]
filters=[port 161 and net 10.16.6.32/32]
0.920349 FW_NSP_VLAN555 in 10.16.6.32.35636 -> 10.10.26.204.161: udp 45
0.920393 FW_INOPE_VLN40 out 10.16.6.32.35636 -> 10.10.26.204.161: udp 45
0.920394 port7 out 10.16.6.32.35636 -> 10.10.26.204.161: udp 45
0.923896 FW_INOPE_VLN40 in 10.10.26.204.161 -> 10.16.6.32.35636: udp 50
0.923984 FW_NSP_VLAN555 out 10.10.26.204.161 -> 10.16.6.32.35636: udp 50
0.923984 WAN_AGREGADO out 10.10.26.204.161 -> 10.16.6.32.35636: udp 50
0.923985 port8 out 10.10.26.204.161 -> 10.16.6.32.35636: udp 50
0.924322 FW_NSP_VLAN555 in 10.16.6.32.38661 -> 172.16.40.183.161: udp 45
0.924353 FW_INOPE_VLN40 out 10.16.6.32.38661 -> 172.16.40.183.161: udp 45
0.924354 port7 out 10.16.6.32.38661 -> 172.16.40.183.161: udp 45
0.930669 FW_INOPE_VLN40 in 172.16.40.183.161 -> 10.16.6.32.38661: udp 57
0.930676 FW_NSP_VLAN555 out 172.16.40.183.161 -> 10.16.6.32.38661: udp 57
0.930677 WAN_AGREGADO out 172.16.40.183.161 -> 10.16.6.32.38661: udp 57
0.930677 port8 out 172.16.40.183.161 -> 10.16.6.32.38661: udp 57
0.931636 FW_NSP_VLAN555 in 10.16.6.32.35660 -> 172.16.38.119.161: udp 192
0.931664 FW_INOPE_VLN40 out 10.16.6.32.35660 -> 172.16.38.119.161: udp 192
0.931666 port7 out 10.16.6.32.35660 -> 172.16.38.119.161: udp 192
0.961472 FW_INOPE_VLN40 in 172.16.38.119.161 -> 10.16.6.32.35660: udp 228
0.961478 FW_NSP_VLAN555 out 172.16.38.119.161 -> 10.16.6.32.35660: udp 228
0.961479 WAN_AGREGADO out 172.16.38.119.161 -> 10.16.6.32.35660: udp 228
0.961479 port8 out 172.16.38.119.161 -> 10.16.6.32.35660: udp 228
0.961832 FW_NSP_VLAN555 in 10.16.6.32.55974 -> 172.16.34.119.161: udp 45
0.961859 FW_INOPE_VLN40 out 10.16.6.32.55974 -> 172.16.34.119.161: udp 45
0.961860 port7 out 10.16.6.32.55974 -> 172.16.34.119.161: udp 45
0.964751 FW_INOPE_VLN40 in 172.16.34.119.161 -> 10.16.6.32.55974: udp 49
0.964757 FW_NSP_VLAN555 out 172.16.34.119.161 -> 10.16.6.32.55974: udp 49
0.964758 WAN_AGREGADO out 172.16.34.119.161 -> 10.16.6.32.55974: udp 49
0.964758 port8 out 172.16.34.119.161 -> 10.16.6.32.55974: udp 49
1.967634 FW_NSP_VLAN555 in 10.16.6.32.55436 -> 10.10.26.205.161: udp 45
1.967653 FW_INOPE_VLN40 out 10.16.6.32.55436 -> 10.10.26.205.161: udp 45
1.967654 port7 out 10.16.6.32.55436 -> 10.10.26.205.161: udp 45
1.970874 FW_INOPE_VLN40 in 10.10.26.205.161 -> 10.16.6.32.55436: udp 50
1.970878 FW_NSP_VLAN555 out 10.10.26.205.161 -> 10.16.6.32.55436: udp 50
1.970878 WAN_AGREGADO out 10.10.26.205.161 -> 10.16.6.32.55436: udp 50
1.970879 port8 out 10.10.26.205.161 -> 10.16.6.32.55436: udp 50
1.971187 FW_NSP_VLAN555 in 10.16.6.32.60646 -> 10.10.37.201.161: udp 45
1.971208 FW_INOPE_VLN40 out 10.16.6.32.60646 -> 10.10.37.201.161: udp 45
```

**(b)** Análisis de del tráfico de la red de datos a través del firewall perimetral - Protocolo SNMP

**Figura 3.2:** Prueba de acceso de tráfico SNMP a la herramienta Zabbix

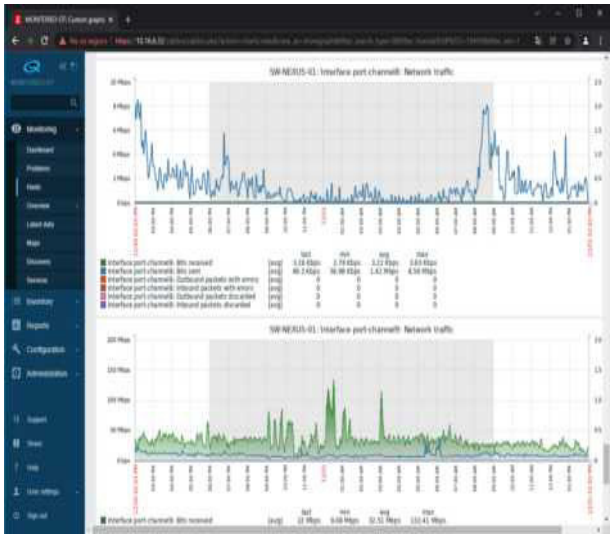



**(a)** Configuración de un elemento integrado mediante el protocolo SNMP

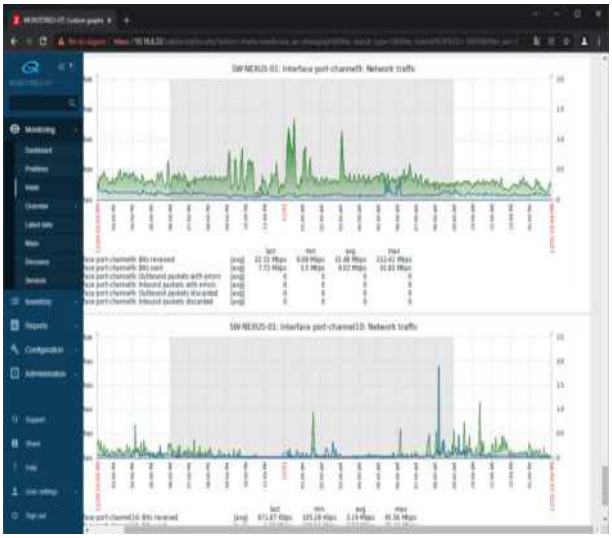



**(b)** Información recuperada mediante el protocolo SNMP

**Figura 3.3:** Prueba de funcionalidad realizada desde la herramienta Zabbix hacia un equipo integrado mediante protocolos SNMP - Ejemplo Equipo Ruggedcom

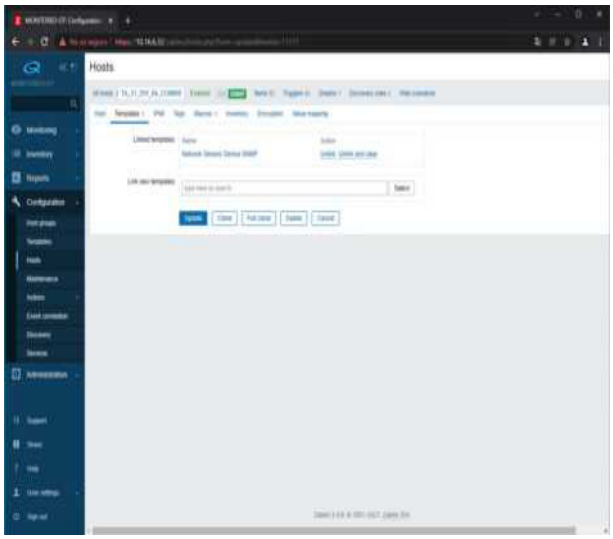


**(a)** Curvas de tendencias realizadas con base en los datos recibidos por medio del protocolo SNMP - Interfaces de red

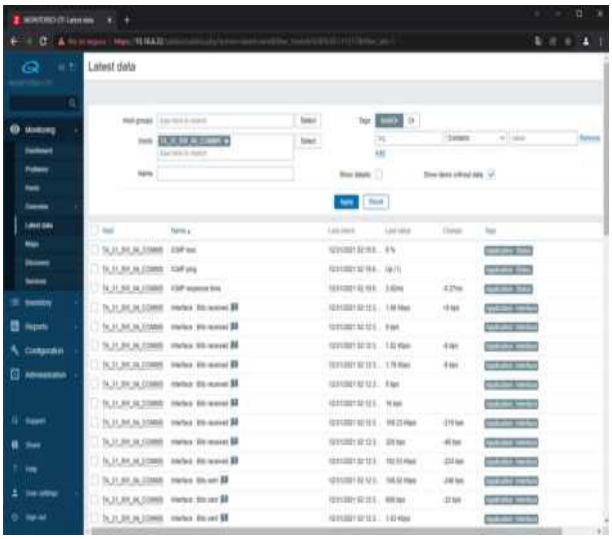


**(b)** Curvas de tendencias realizadas sobre la base de los datos recibidos por medio del protocolo SNMP - Interfaces de red

**Figura 3.4:** Prueba de funcionalidad realizada desde la herramienta Zabbix hacia un equipo integrado mediante protocolos SNMP - Ejemplo Equipo Ruggedcom (cont. . . . )

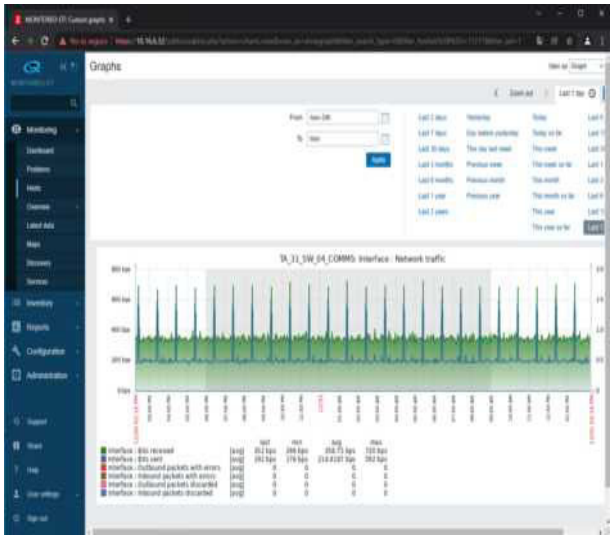


**(a)** Configuración de un elemento integrado mediante el protocolo SNMP

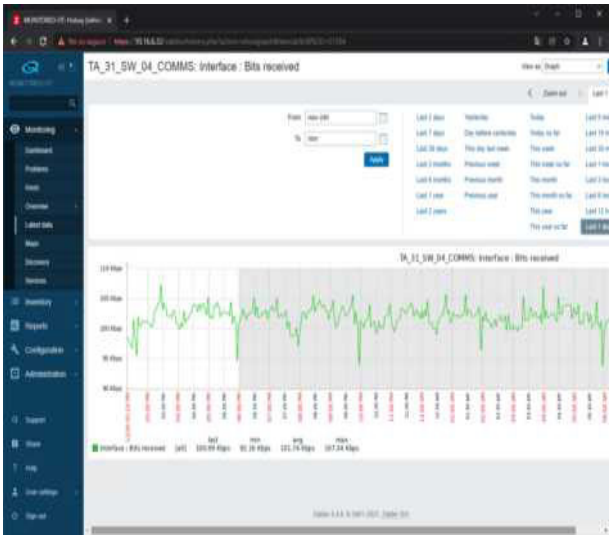


**(b)** Información recuperada mediante el protocolo SNMP

**Figura 3.5:** Prueba de funcionalidad realizada desde la herramienta Zabbix hacia un equipo integrado mediante protocolos SNMP - Ejemplo Equipo Garretcom




**(a)** Curvas de tendencias realizadas con base en los datos recibidos por medio del protocolo SNMP - Interfaces de red

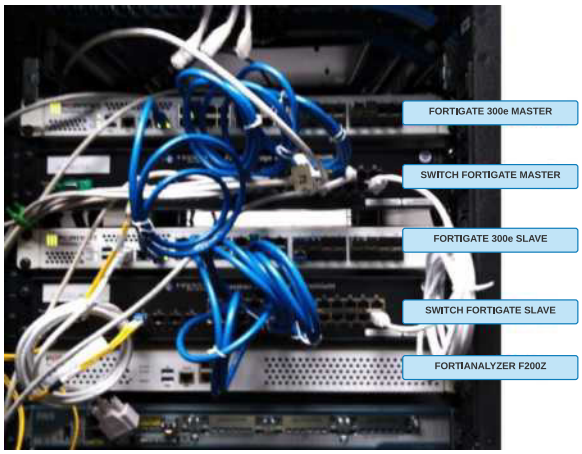



**(b)** Curvas de tendencias realizadas sobre la base de los datos recibidos por medio del protocolo SNMP - Interfaces de red

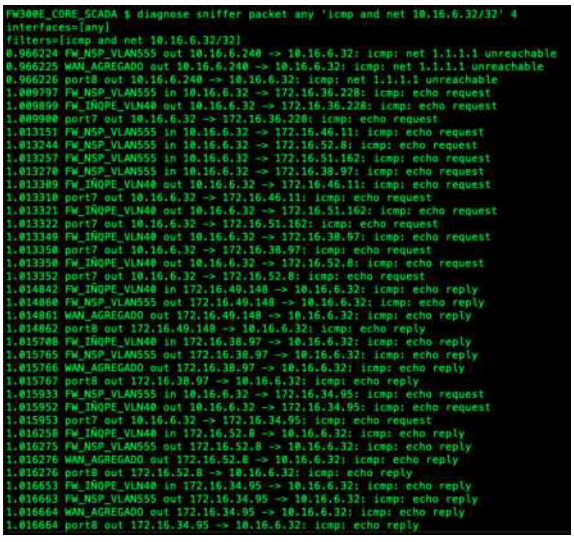
**Figura 3.6:** Prueba de funcionalidad realizada desde la herramienta Zabbix hacia un equipo integrado mediante protocolos SNMP - Ejemplo Equipo Garretcom (cont. . . . )

### 3.1.1.2. Pruebas De Funcionamiento Usando El Protocolo ICMP

Para la evaluación del rendimiento de la solución de la herramienta Zabbix usando el protocolo ICMP se realizaron evaluaciones similares a las efectuadas con el protocolo SNMP.




**(a)** Conexiones del firewall perimetral hacia los servidores físicos

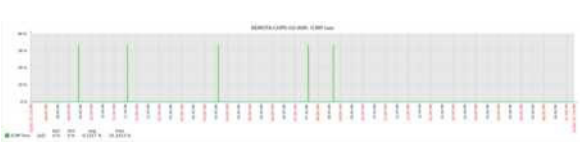



**(b)** Prueba de acceso de tráfico ICMP a la herramienta Zabbix

**Figura 3.7:** Pruebas de funcionamiento de Zabbix con el protocolo ICMP

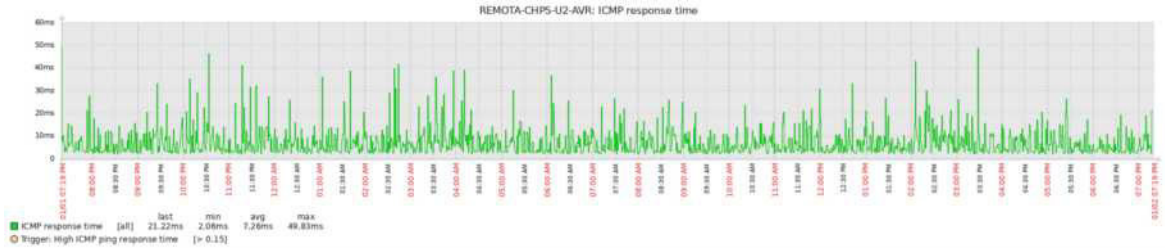
La primera comprobación fue analizar el tráfico de la Red de datos a través del firewall perimetral, luego se realizaron curvas de tendencias con los datos recuperados a través

de la integración de los equipos terminales sobre este protocolo. Los resultados de estas evaluaciones se muestran en la Figura 3.8.



**(a)** Curva de pérdidas con el protocolo ICMP

**(b)** Curva de disponibilidad con el protocolo ICMP

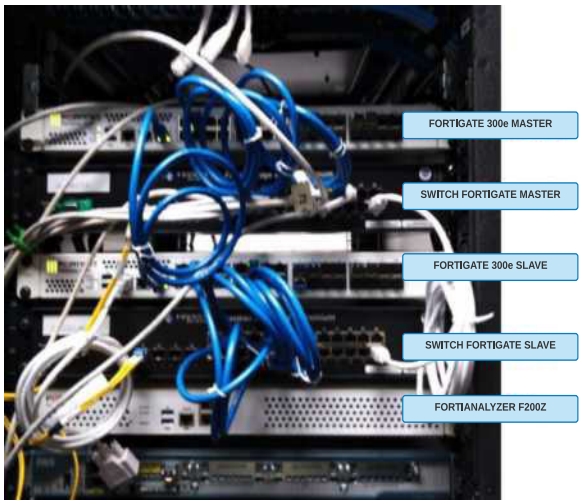



**(c)** Curva de tiempos de respuesta con el protocolo ICMP

**Figura 3.8:** Curvas de tendencia de las pruebas de funcionamiento con el protocolo ICMP

### 3.1.2. PRUEBAS DE FUNCIONAMIENTO DE LA HERRAMIENTA LOG-ANALYZER

De manera similar a las pruebas realizadas sobre el protocolo SNMP, las pruebas realizadas sobre el protocolo SYSLOG inicien también con el análisis de datos a través del firewall perimetral, comprobando que los puertos utilizados establezcan sesiones hacia el puerto 512 UDP/TCP, los resultados de esta primera prueba se muestran en la Figura 3.9.

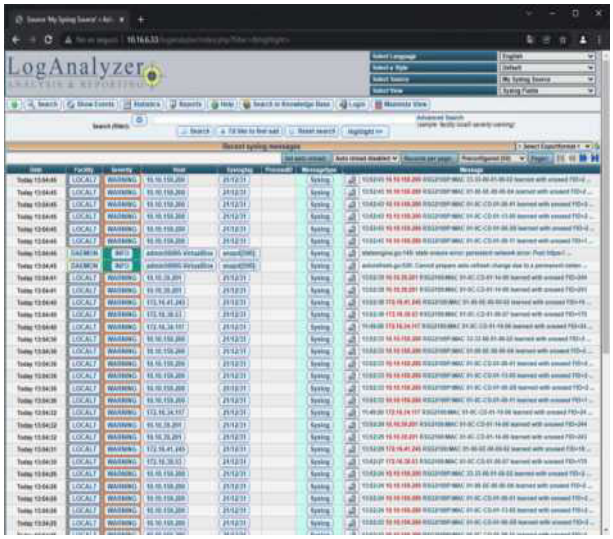



**(a)** Conexiones del firewall perimetral hacia los servidores físicos

```
FW300E_CORE_SCADA $ diagnose sniffer packet any 'net 10.16.6.33/32' 4
interfaces=[any]
filters=[net 10.16.6.33/32]
12.759928 FW_INQPE_VLN40 in 172.16.40.120.514 -> 10.16.6.33.514: udp 72
12.759952 FW_NSP_VLAN555 out 172.16.40.120.514 -> 10.16.6.33.514: udp 72
12.759953 WAN_AGREGADO out 172.16.40.120.514 -> 10.16.6.33.514: udp 72
12.759953 port8 out 172.16.40.120.514 -> 10.16.6.33.514: udp 72
17.761543 FW_NSP_VLAN555 out arp who-has 10.16.6.33 tell 10.16.6.240
17.761544 WAN_AGREGADO out arp who-has 10.16.6.33 tell 10.16.6.240
17.761545 port8 out arp who-has 10.16.6.33 tell 10.16.6.240
17.761708 FW_NSP_VLAN555 in arp reply 10.16.6.33 is-at 8:0:27:1e:cf:ae
18.138730 FW_INQPE_VLN40 in 172.16.40.123.514 -> 10.16.6.33.514: udp 72
18.138753 FW_NSP_VLAN555 out 172.16.40.123.514 -> 10.16.6.33.514: udp 72
18.138754 WAN_AGREGADO out 172.16.40.123.514 -> 10.16.6.33.514: udp 72
18.138755 port8 out 172.16.40.123.514 -> 10.16.6.33.514: udp 72
18.403776 FW_INQPE_VLN40 in 172.16.40.119.514 -> 10.16.6.33.514: udp 72
18.403799 FW_NSP_VLAN555 out 172.16.40.119.514 -> 10.16.6.33.514: udp 72
18.403799 WAN_AGREGADO out 172.16.40.119.514 -> 10.16.6.33.514: udp 72
18.403800 port8 out 172.16.40.119.514 -> 10.16.6.33.514: udp 72
18.448960 FW_INQPE_VLN40 in 172.16.40.121.514 -> 10.16.6.33.514: udp 72
18.448984 FW_NSP_VLAN555 out 172.16.40.121.514 -> 10.16.6.33.514: udp 72
18.448984 WAN_AGREGADO out 172.16.40.121.514 -> 10.16.6.33.514: udp 72
18.448985 port8 out 172.16.40.121.514 -> 10.16.6.33.514: udp 72
18.615896 FW_INQPE_VLN40 in 172.16.40.122.514 -> 10.16.6.33.514: udp 72
18.615924 FW_NSP_VLAN555 out 172.16.40.122.514 -> 10.16.6.33.514: udp 72
18.615924 WAN_AGREGADO out 172.16.40.122.514 -> 10.16.6.33.514: udp 72
```

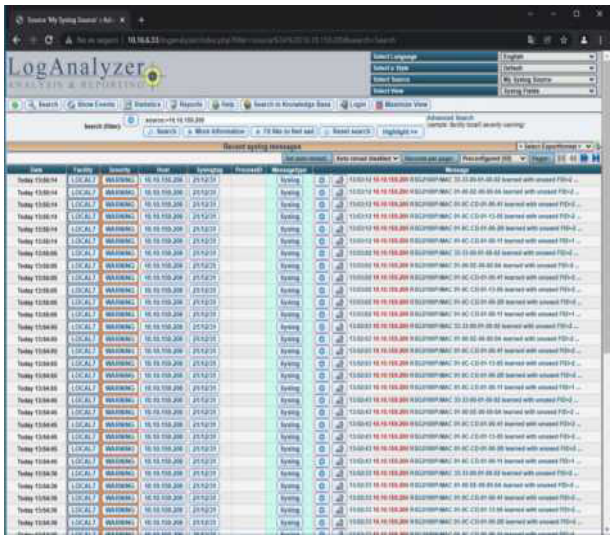
**(b)** Análisis de del tráfico de la red de datos a través del firewall perimetral - Protocolo Syslog

**Figura 3.9:** Prueba de Análisis de datos para el protocolo Syslog

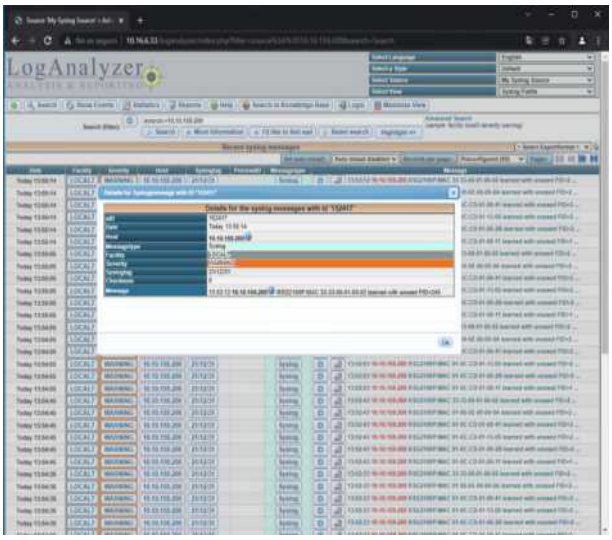


**(a)** Menú inicial de la herramienta LogAnalyzer - lectura de mensajes Syslog

**(b)** Estadísticas de los mensajes Syslog recibidos



**(c)** Filtrado de mensajes leídos para la IP 10.10.159.200

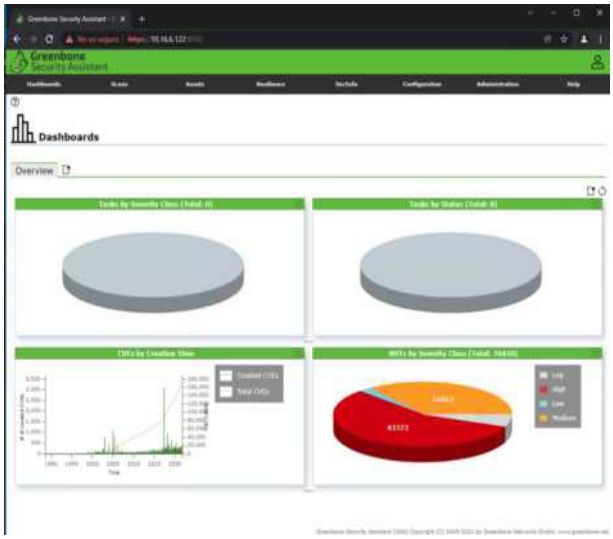


**(d)** Visualización de los mensajes Syslog recibidos

**Figura 3.10:** Pruebas de funcionamiento de la herramienta LogAnalyzer usando el protocolo Syslog

### 3.1.3. PRUEBAS DE FUNCIONAMIENTO DE LA HERRAMIENTA OPENVAS

El funcionamiento de la herramienta OpenVAS fue comprobado asumiendo como escenario de pruebas en el análisis de vulnerabilidades sobre el segmento de Red 10.16.6.0/24. Los resultados de este análisis se muestran en la Figura 3.12.




**(a)** Pantalla de inicio al ingresar a la herramienta

Scan Report

September 30, 2021

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Immediate scan of IP 10.16.6.0/24". The scan started at Thu Sep 30 04:01:03 2021 UTC and ended at Thu Sep 30 04:55:09 2021 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents



**(b)** Detalle reporte generado con la herramienta OpenVAS (I)

**Figura 3.11:** Pruebas de funcionamiento con la herramienta OpenVAS.

1 Result Overview

| Host | High | Medium | Low | Log | False Positive |
|---|---|---|---|---|---|
| 10.16.6.221 | 2 | 0 | 0 | 0 | 0 |
| 10.16.6.129 | 2 | 0 | 0 | 0 | 0 |
| 10.16.6.220 | 3 | 4 | 1 | 0 | 0 |
| 10.16.6.123 | 2 | 6 | 1 | 0 | 0 |
| 10.16.6.15 | 1 | 1 | 1 | 0 | 0 |
| 10.16.6.121 | 0 | 2 | 0 | 0 | 0 |
| 10.16.6.240 | 0 | 2 | 1 | 0 | 0 |
| 10.16.6.32 | 0 | 1 | 1 | 0 | 0 |
| 10.16.6.222 | 0 | 1 | 0 | 0 | 0 |
| 10.16.6.12 | 0 | 1 | 0 | 0 | 0 |
| 10.16.6.10 | 0 | 1 | 0 | 0 | 0 |
| 10.16.6.13 | 0 | 1 | 0 | 0 | 0 |
| 10.16.6.11 | 0 | 1 | 0 | 0 | 0 |
| 10.16.6.14 | 0 | 1 | 0 | 0 | 0 |
| 10.16.6.30 | 0 | 0 | 1 | 0 | 0 |
| 10.16.6.31 | 0 | 0 | 1 | 0 | 0 |
| Total: 16 | 10 | 22 | 7 | 0 | 0 |

**(a)** Detalle reporte generado con la herramienta OpenVAS (II)

2.2 10.16.6.129

Host scan start Thu Sep 30 04:01:23 2021 UTC
Host scan end Thu Sep 30 04:19:37 2021 UTC

| Service (Port) | Threat Level |
|---|---|
| general/tcp | High |
| 445/tcp | High |

2.2.1 High general/tcp

High (CVSS: 10.0)
NVT: OS End Of Life Detection

**Product detection result**
cpe:/o:microsoft:windows_xp
Detected by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)

**Summary**
OS End Of Life Detection.
The Operating System on the remote host has reached the end of life and should not be used anymore.

**Vulnerability Detection Result**
The "Windows XP" Operating System on the remote host has reached the end of life.
CPE: cpe:/o:microsoft:windows_xp
EOL date: 2014-04-08
EOL info: https://support.microsoft.com/en-us/lifecycle/search?sort=PN&alpha=Microsoft%20Windows%20XP&Filter=FilterNO

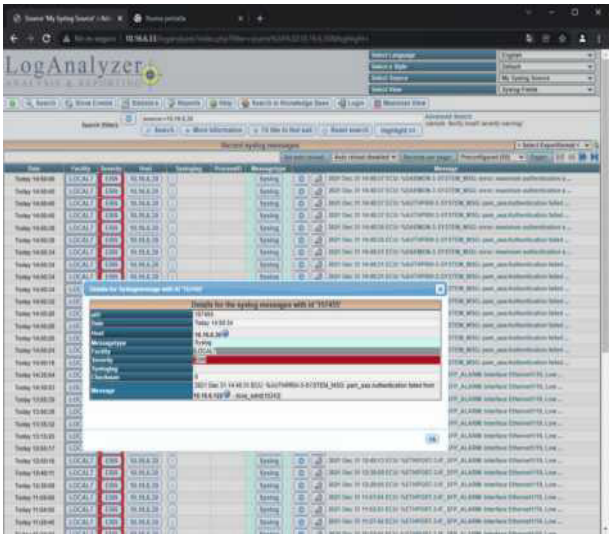
**(b)** Detalle reporte generado con la herramienta OpenVAS (III)

**Figura 3.12:** Pruebas de funcionamiento con la herramienta OpenVAS (cont. . . . )

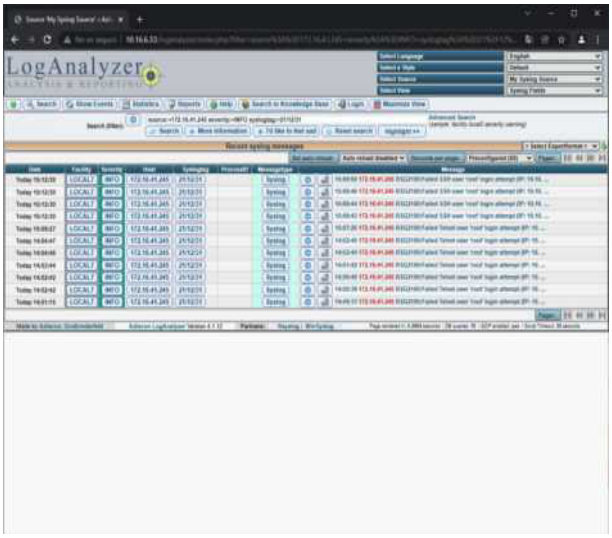
### 3.1.4. PRUEBAS DE GENERACIÓN DE ALARMAS EN UN ATAQUE SOBRE LA RED DE DATOS

Uno de los escenarios más básicos en donde las herramientas implementadas resultan de su utilidad es el monitoreo del comportamiento de los equipos de redes versus accesos no autorizados. Para esto se ha generado un escenario de pruebas entonces se espera que los equipos de redes generen mensajes de alerta frente a los intentos de acceso simulando ataques sobre la infraestructura instalada.

En la Figura 3.13 se muestra la generación de los mensajes de alerta frente a los intentos fallidos de acceso hacia los equipos de redes a través del protocolo SSH. El contenido detallado de los mensajes generados se muestra en la Figura 3.14. En los dos escenarios de las pruebas realizadas destaca el hecho de qué los mismos mensajes son catalogados de manera distinta en cada uno de los fabricantes, he aquí la importancia del análisis de los datos por parte de los técnicos responsables de la administración de la infraestructura instalada. En el primer caso, se cataloga como un error en el acceso no autorizado mostrándose en color rojo mientras que en el segundo fabricante se cataloga como un mensaje informativo mostrándose en color verde.

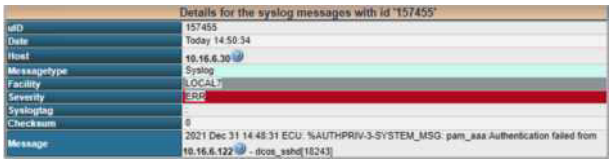



**(a)** Generación de mensajes de alerta frente a intentos de accesos no autorizados a la IP 10.16.6.30

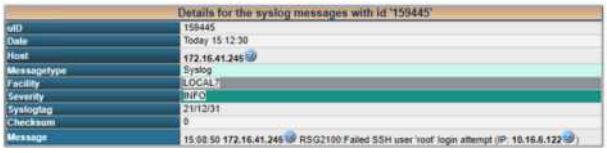



**(b)** generación de mensajes de alerta frente a intentos de accesos no autorizados a la IP 172.16.41.245

**Figura 3.13:** Prueba del uso de las herramientas de análisis de registro de eventos frente a ataques de red - Escenario de acceso no autorizado.




**(a)** Generación de mensajes de alerta frente a intentos de accesos no autorizados a la IP 10.16.6.30 - Detalle del mensaje

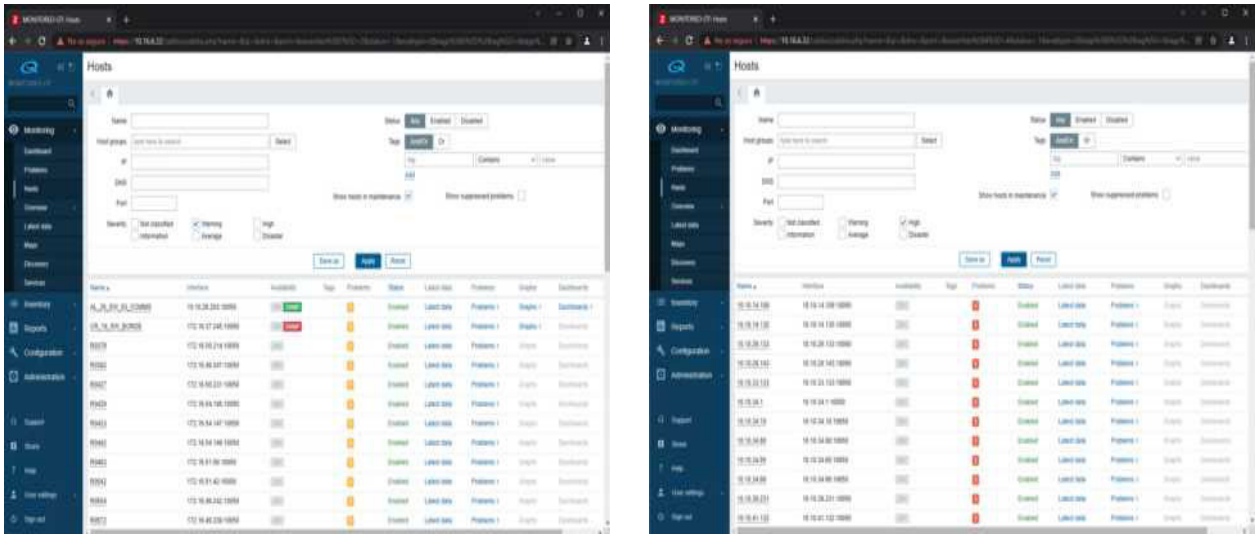



**(b)** generación de mensajes de alerta frente a intentos de accesos no autorizados a la IP 172.16.41.245 - Detalle del mensaje

**Figura 3.14:** Prueba del uso de las herramientas de análisis de registro de eventos frente a ataques de red - Escenario de acceso no autorizado - Detalle del mensaje.

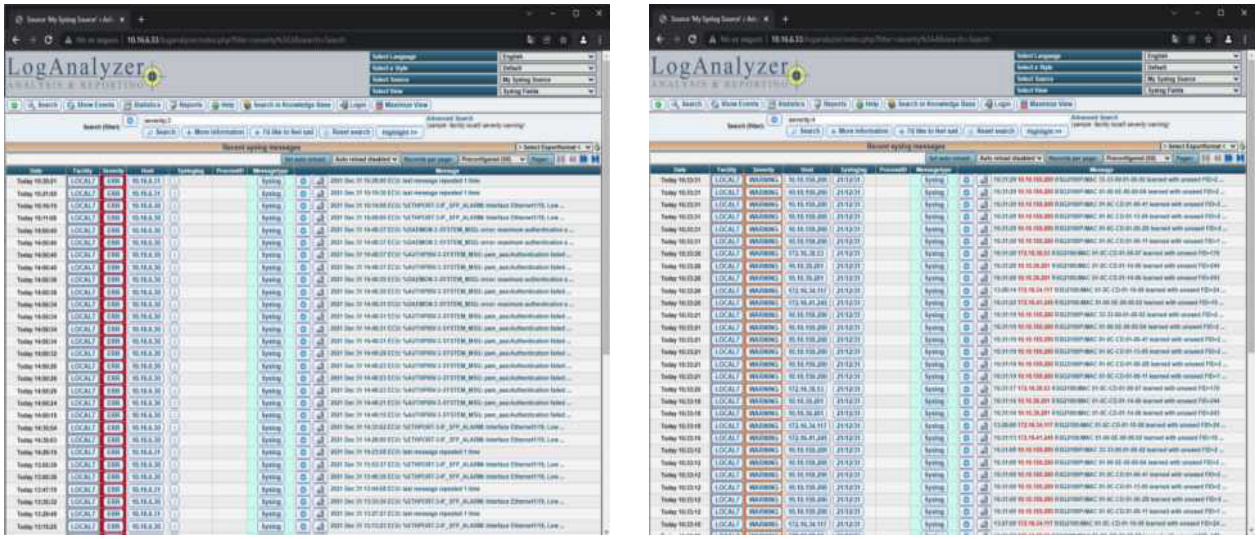
### 3.1.5. PRUEBAS DE GENERACIÓN DE ALARMAS EN LOS EQUIPOS INTEGRADOS

Una característica importante del uso de las herramientas instaladas dentro de la solución tecnológica desarrollada en este trabajo de titulación es el manejo de alarmas sobre el comportamiento físico de los equipos instalados, es decir conocer en tiempo real si estos equipos presentan alertas o algún tipo de alarmas necesarias de ser atendida por parte de los administradores de la red de datos. Los resultados de la prueba realizada sobre esta funcionalidad se muestran en las Figuras 3.15 y 3.17.



**(a)** Alertas - alarmas generadas **(b)** Alertas - errores críticos

**Figura 3.15:** Prueba de la funcionalidad de la generación de alarmas usando Zabbix

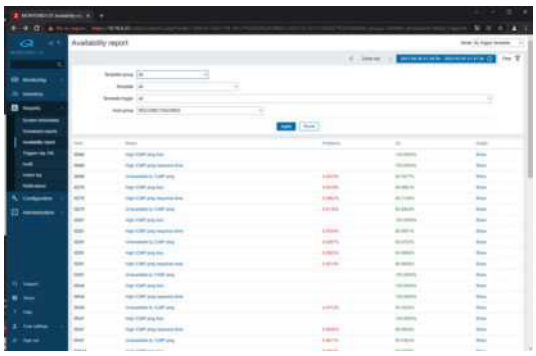


**(a)** Alertas - errores críticos **(b)** Alertas - alarmas generadas

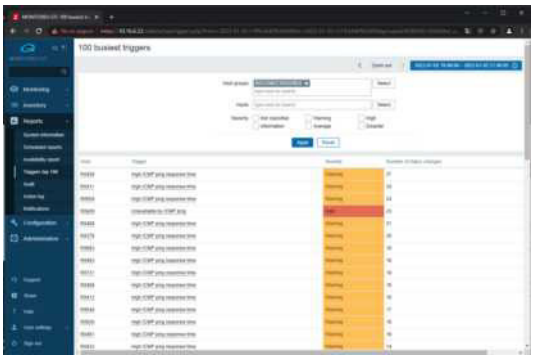
**Figura 3.16:** Prueba de la funcionalidad de la generación de alarmas usando LogAnalyzer

### 3.1.6. GENERACIÓN DE REPORTES SOBRE LA INFORMACIÓN ADQUIRIDA

Las herramientas explicadas en este trabajo de titulación generan información de manera masiva, dicha información es aprovechada a través de la generación de reportes de análisis de estos datos. Las herramientas instaladas disponen de plantillas cargadas para generar estos reportes. La Figura 3.17 se presentan ejemplos de la generación de estos reportes a través de la herramienta Zabbix, los reportes generados corresponden a la medición de la disponibilidad de los equipos terminales monitoreados y al número de eventos y alarmas generadas por equipo terminal. En lo que corresponde a la información del protocolo Syslog, en la Figura 3.18 se presenta en los reportes disponibles en LogAnalyzer.

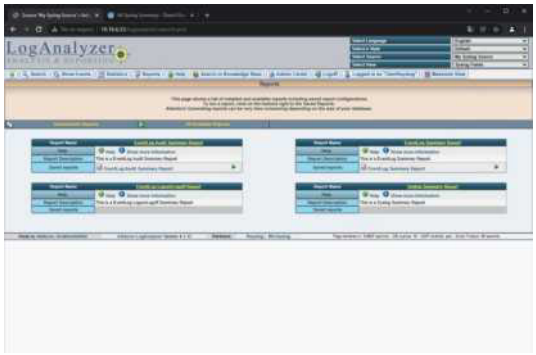


**(a)** Generación de reportes - número de cambios de estado

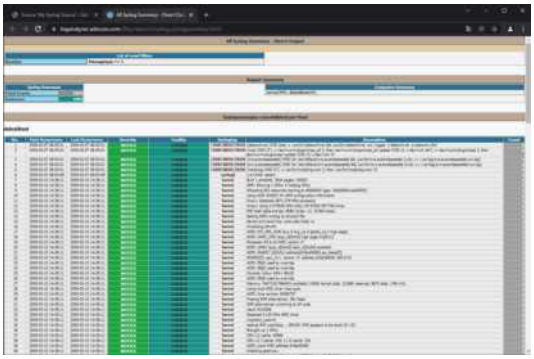


**(b)** generación de reportes - disponibilidad de equipos

**Figura 3.17:** Prueba de la funcionalidad de la generación de reportes usando Zabbix



**(a)** Generación de reportes - plantillas disponibles



**(b)** generación de reportes - eventos generados por equipo terminal

**Figura 3.18:** Prueba de la funcionalidad de la generación de reportes usando LogAnalyzer

## 3.2. DISCUSIÓN

### 3.2.1. MEJORAS EN LA GESTIÓN TÉCNICA DE LOS EQUIPOS DE REDES DE DATOS

- Uno de los resultados más relevantes obtenidos con la implementación de la solución tecnológica desarrollada en este trabajo de titulación es disponer de la capacidad de visualización completa de la infraestructura instalada. Inicialmente, no se disponía de herramientas que permitan monitorear el estado de los equipos en las redes de datos, al momento las herramientas instaladas permiten dar seguimiento al estado de alrededor de 3000 equipos instalados en la Red de datos de los sistemas de automatización industrial de la E.E.Q.

- Otro resultado importante derivado de la puesta en marcha de las herramientas de gestión implementadas es poder visualizar el estado de la configuración de los equipos de las redes de datos instalados en los sistemas de automatización industrial de la E.E.Q., los cuales luego de haber sido integrados a las herramientas de gestión mostraron en errores en su configuración, mismos que no se corregidos afectan negativamente el rendimiento de los equipos y de la red de datos, ejemplos de estos son problemas de sincronización, problemas en la configuración de los protocolos de Red, posibles fallos de hardware y errores en las interfaces de conexión de los equipos.

- Los problemas encontrados en la configuración de los protocolos de redes de los equipos activos se centran en la implementación base de las redes de datos de los sistemas automatización industrial aún presentes en la E.E.Q., esta implementación se fundamenta en enlaces en capa dos. Por este motivo los mensajes de error se centralizan en detalles de corrección sobre el protocolo RSTP, correcciones a los cambios de topología, problemas con tablas ARP, entre otros. Toda esta información previo a la implementación de esta solución administración y gestión de redes de datos no era visualizable.

- En la actualidad la seguridad tecnológica de las infraestructuras empresariales se ha convertido en un tema central de análisis, gestión y mejora continua. Previo la implementación de la herramienta de evaluación de vulnerabilidades no se conocía el nivel de cuán vulnerable está la infraestructura tecnológica instalada. Al momento con las evaluaciones realizadas es posible contar con una línea base sobre la cual trabajar para mitigar los riesgos identificados. Sobre las vulnerabilidades identificadas haciendo uso de la herramienta desplegada es importante remarcar que la infraestructura instalada corresponde a equipamiento de tipo industrial, por lo que todos estos equipos al contrario de lo que podría esperarse ya no cuentan con soporte de fábrica

ni actualizaciones disponibles, de ahí la necesidad de implementar estrategias que permitan mitigar los riesgos generados por las vulnerabilidades identificadas.

- En la actualidad las soluciones tecnológicas tienden a ser implementados haciendo uso de la automatización de procesos a fin de optimizar los recursos técnicos necesarios para garantizar la continuidad de los servicios tecnológicos. En la solución desarrollada en este trabajo de titulación se implementó un mecanismo de notificación de alertas tempranas frente a fallos en la infraestructura monitoreada. Estas alertas tempranas serán notificadas vía correo electrónico, mecanismo que evitan disponer de recursos técnicos adicionales para hacer uso de las herramientas de gestión instaladas. La emisión de estas alertas tempranas tomará como base el monitoreo que se realiza de manera continua sobre los equipos integrados en las redes de datos de los sistemas de automatización industrial de la E.E.Q.

- Definir procesos de gestión de los equipos de las redes de datos, métricas de evaluación de la continuidad del servicio y disponibilidad de la interconexión entre equipos terminales y garantizar la seguridad hacia esta infraestructura crítica permitirá garantizar y mejorar los indicadores empresariales de calidad de servicios dictados por la ARCONEL (FMIK, TTIK, SAIDI, SAIFI), los mismos que dependen de un correcto funcionamiento de los sistemas de automatización industrial.

### 3.2.2. RENDIMIENTO DE LA SOLUCIÓN DESPLEGADA

- Con los resultados descritos en la fase de pruebas de la solución desplegada se puede poner de manifiesto la practicidad de la propuesta desarrollada en este trabajo de titulación, la cual además de no incluir costos derivados de licenciamiento la compra de software demostró un alto rendimiento con recursos de hardware limitados.

- El despliegue en ambientes virtualizados de las herramientas de software incluidas en la solución tecnológica desarrollada en su trabajo de titulación permite que de ser el caso se puede incluir más recursos de hardware que garanticen su correcto funcionamiento y una experiencia final de usuario adecuada. Las herramientas instaladas pueden ser exportados en formatos de virtualización abiertos (.ovf) lo que a su vez garantiza el no incurrir en costos derivados de la compra de software para la puesta en marcha de las herramientas instaladas.

- La solución desplegada en caso de qué el crecimiento de la automatización de la Red eléctrica incluye la instalación masiva de equipos electrónicos no se verá limitada, ya que podrá ser escalada fácilmente sin generar costos significativos en cuanto a nuevos recursos de hardware.

- La implementación de la solución tecnológica diseñada en este trabajo de titulación permitió tener un contacto directo con las dificultades implicadas en el monitoreo y gestión de redes de datos implementadas sin que se tenga en cuenta los estándares y buenas prácticas en la gestión de la infraestructura tecnológica.

- Si bien el protocolo SNMP es inter operable entre marcas, en la integración de los equipos terminales a la herramienta Zabbix se presentaron inconvenientes en el funcionamiento que generaron reinicios imprevistos de los equipos terminales integrados vía este protocolo. Por este motivo se optó por deshabilitar esta característica y monitorear estos equipos vía protocolo ICMP.

- Los mensajes generados vía el protocolo Syslog presentan grandes diferencias entre marcas, sobre los resultados obtenidos de este, resaltan los mensajes de autenticación dices fallidos y los equipos terminales. Dichos mensajes para unas marcas son catalogados como errores críticos mientras para otras como alarmas de tipo informativo, en este escenario resulta de suma importancia el análisis detallado por parte de los técnicos administradores de la red de datos.

# 4. CONCLUSIONES Y RECOMENDACIONES

## 4.1. CONCLUSIONES

1. Una vez realizado el estudio de las características y funcionalidades de un NOC, un SOC y las ventajas de un NSOC frente a estos, se concluye que ante el aumento de los ciberataques en la actualidad las organizaciones tienden a desplegar estas dependencias para mejorar la gestión y monitorización de las redes de datos. Estos sistemas al estar aislados rara vez tienen una visión clara y coherente de lo que está ocurriendo en la red. Las diferencias entre estos sistemas dejan vacíos en los análisis necesarios para cumplir cualquiera de los objetivos de estos dos sistemas. Esta situación ha llevado a la creación de un nuevo enfoque, la creación de un sistema que pueda llevar la visibilidad y el control de la seguridad al NOC, y proporcionar los requisitos operativos y la visibilidad de la red y el flujo de trabajo al SOC, al combinar estos sistemas en una solución centralizada, las organizaciones pueden centrarse en el flujo de trabajo seguro, agilizando las operaciones y gestionando de forma proactiva los eventos de seguridad críticos.

2. El diseño de la solución desarrollada en este trabajo de titulación tomó como base los requerimientos recibidos del personal técnico de la E.E.Q. a los que tuvieron que anexarse las limitaciones propias de los equipos instalados, obsolescencia tecnológica, incompatibilidad entre marcas, indisponibilidad de protocolos de gestión abiertos, limitantes propias de los equipos instalados, incompatibilidad en el software de gestión, entre otros. Para la versión final del prototipo desplegado se dio especial importancia a la practicidad y fiabilidad de los resultados en la integración de los equipos hacia las herramientas de gestión, es decir se optó por utilizar todas las herramientas y protocolos abiertos a fin de evitar fallos en la herramienta instalada o datos que no se consideren fiables.

3. En la implementación de la solución tecnológica diseñada en este trabajo de titulación se concluyo con base en las pruebas realizadas que las herramientas de código abierto tuvieron un desempeño muy potente, esto quedo evidenciado al realizar el monitoreo de 3400 equipos. Las herramientas de código abierto también evitaron incurrir en gastos derivados de la compra de software o licenciamiento de cualquier tipo.

4. La solución desarrollada en este trabajo de titulación fue probada de manera directa sobre la infraestructura de las redes de datos de los sistemas de automatización

industrial de la E.E.Q. Los resultados obtenidos garantizan el correcto funcionamiento de la solución implementada, y demuestran de manera clara la importancia de contar con estas herramientas en la gestión de las redes de datos.

5. Los resultados de la implementación del Centro de Operaciones de Seguridad y Redes proporcionan un aporte crucial para la gestión de las Redes de datos de la E.E.Q., lo que ha permitido ayudar a mejorar los tiempos de respuesta. Este trabajo de titulación está alineado al marco de referencia FCAPS, siendo el primer punto de este la gestión de fallos y siendo parte fundamental de esta gestión la rápida detección de estos. Esta solución tecnológica al detectar rápidamente los fallos, mejora el tiempo de respuesta del equipo de tecnologías de la operación de la Empresa Eléctrica Quito y al tener una respuesta más rápida, la disponibilidad de la red va a ser igualmente mejorada.

6. La E.E.Q. cuenta con equipos muy costosos en el ámbito de automatización industrial, pero en cuanto a la red de datos a pesar de que los equipos activos con costos, su rendimiento no podía verse aprovechado, ya que no se contaba con una solución adecuada para la gestión y monitorización de estos equipos. Luego de la implementación de la solución NSOC en este trabajo de titulación se pudieron identificar varias correcciones en la configuración de los equipos de redes de datos, las cuales una vez ejecutadas permitieron optimizar el funcionamiento de los equipos de redes de datos, hecho que impacta positivamente en el rendimiento de los sistemas de automatización de la red eléctrica beneficiando el proceso de venta de energía en la E.E.Q.

7. La seguridad de la infraestructura tecnológica instalada al contrario de lo que podría pensarse depende de un correcto uso de la información generada por los equipos instalados, la implementación de procesos de gestión adecuados, la aplicación de buenas prácticas en cuanto a la configuración y evaluación de los equipos terminales y sobre todo esto a la evaluación continua de la seguridad integral de la infraestructura instalada, es decir la fortaleza de la infraestructura instalada dependerá de una correcta gestión y administración de todo el equipamiento que forma parte de la red de datos, incluyendo los equipos de automatización industrial. Con lo indicado debe evitarse por sobre todas las cosas la instalación de equipamiento que obstaculicen o dificulte el normal funcionamiento de los sistemas de automatización industrial versus contar con una u otra característica tecnológicamente reciente para la gestión de la seguridad de la infraestructura tecnológica.

8. El Framework de ciberseguridad del NIST es el marco de trabajo de ciberseguridad más usado hoy en día por las organizaciones, este Framework puede adaptarse a

cualquier tamaño de organización, a cualquier alcance seleccionado dentro de la organización y puede tener diferentes fines. El principal es llevar los riesgos de ciberseguridad a un nivel adecuado para la organización y a un costo razonable con relación al impacto de los riesgos.

9. La solución desplegada en este proyecto de titulación fue desarrollada a la medida y al contrario de lo que podría presuponerse la instalación de las herramientas usadas necesita un período de afinamiento y ajuste en su rendimiento. En este caso se puede concluir que para el despliegue de herramientas de gestión de redes grandes como las de la E.E.Q. (alrededor de 3400 equipos) las herramientas de gestión deben ajustarse a fin de que puedan desarrollar un rendimiento adecuado en la gestión de los equipos terminales. Del estudio introductorio realizado se fija como norma común recomendar recursos de hardware según un número de equipos referencial, el ajuste a desarrollar toda esta base evaluando el rendimiento de la herramienta y la experiencia de usuario, es decir se debe evitar sobredimensionar los recursos de hardware sin dejar de lado que la respuesta frente al uso de las herramientas sea adecuada.

10. En este proyecto de titulación además de haber trabajado en el desarrollo de la solución tecnológica implementada fue posible constatar de manera cercana la importancia de la compatibilidad tecnológica entre los equipos instalados en la infraestructura empresarial y las soluciones de gestión de infraestructura. Además, salieron a flote las características inherentes de los sistemas tecnológicos industriales y en especial de sus redes de datos. Como ultima conclusión se puede mencionar la importancia de la caracterización de los sistemas tecnológicos y de sus procesos de gestión, así como también los graves efectos en caso de que estos no existan lo cual afecta directamente al rendimiento de los sistemas instalados. Para el caso de los sistemas de redes de datos industriales existes normas y procedimientos claramente definidos en donde se hace especial hincapié en la naturaleza de estos frente al giro del negocio, un ejemplo claro de esto son las normas que rigen el sector eléctrico a nivel mundial.

## 4.2. RECOMENDACIONES

1. Se deben implementar mecanismos de mantenimiento de las herramientas de gestión instaladas en especial mantenimiento sobre la base de datos instalada en cada una de estas herramientas. Para el caso de la herramienta de monitoreo de red es importante definir períodos de vida prácticos en los cuales la información sea útil y utilizable, es decir se deben evitar situaciones en donde se requieran recursos de almacenamiento masivos que no sean plenamente justificados. Para el caso de la herramienta de evaluación de vulnerabilidades se deberá garantizar que la base de datos de las

definiciones de estas vulnerabilidades se mantenga actualizada. Finalmente, para el registro de eventos al igual que en el caso de la herramienta de monitoreo de red se deberá garantizar un espacio adecuado y un periodo de vida útil práctica para el uso de la información.

2. Los procesos de gestión de las redes de datos deben incluir mecanismos de actualización de los sistemas operativos de los equipos de redes y en muchos de los casos también de los equipos terminales a fin de que su integración, gestión y monitoreo puede realizarse de manera adecuada. Debido a los desfases tecnológicos entre los protocolos de gestión disponibles en los equipos integrados a la solución y las herramientas instaladas se pudo constatar que los equipos integrados presentaban comportamientos erráticos que los reiniciaban, en especial con el protocolo SNMP, por lo que en esos casos se optó por monitorearlos solamente por ICMP. No realizar estos procesos de actualización generan brechas de seguridad que pueden poner en riesgo crítico la infraestructura de los sistemas de automatización industrial.

3. Sobre la implementación de la solución tecnológica desarrollada en este proyecto de titulación surgen mejoras en cuanto a la inclusión de herramientas de detección de intrusiones tales como las indicadas en el capítulo introductorio. Una de las herramientas que podría generar nuevas funcionalidades en la solución tecnológica implementada es Security Onion, la cual además de ser una distribución de Linux diseñada para la detección de intrusos (Intrusion Detection System (IDS)) permite monitorear también la seguridad de la red de datos e incluye facilidades en la gestión de los registros de eventos. En lo que respecta a la gestión de los registros de eventos esto no implica alterar la implementación actual y a qué se puede hacer un reenvío de los registros almacenados en el servidor implementado hacia cualquier nueva implementación y herramienta de análisis. Security Onion incluye también herramientas como Snort y Suricata, las cuales para ser utilizadas necesitan configuraciones adicionales en los equipos de red y contar con tarjetas de red en donde recibir las muestras de tráfico capturadas. Implementando tarjetas de red adicionales el siguiente paso y mejores posibles e implementar son herramientas de análisis forense en donde entran en escena utilidades como el Wireshark y el Networkminer.

4. Mejoras adicionales a la solución tecnológica desarrollada en este proyecto de titulación incluyen el despliegue de sistemas Security Information and Event Management (SIEM), los cuales gestionan los eventos de seguridad detectando y correlacionando patrones de comportamiento fuera de lo normal mediante la monitorización de la infraestructura en tiempo real. Estas soluciones permiten también gestionar la información de seguridad centralizando los registros de eventos de seguridad, permitiendo interpretarlos de tal manera que se puedan realizar actuaciones inmediatas frente a

eventos emergentes de ataques cibernéticos a la infraestructura tecnológica empresarial.

5. Además de las implementaciones de los sistemas SIEM otra de las posibilidades de mejora la solución tecnológica desarrollada en este proyecto de titulación es la implementación de sistemas Security Orchestration Automation and Response (SOAR). Los sistemas SOAR están conformados por un conjunto de herramientas que permiten la automatización de procesos en la gestión de la seguridad de la infraestructura tecnológica. En proyecto de titulación se desarrolló un procedimiento base de gestión de la red de datos y de la seguridad tecnológica de la infraestructura industrial, dichos constituirían la base para el despliegue de la automatización de procesos de gestión usando las soluciones SOAR. Las soluciones SOAR además de la automatización de tareas garantizan un aumento en la productividad del grupo de trabajo del NSOC y mejorando y dinamizando la capacidad de respuesta ante ataques cibernéticos. Finalmente, se debe considerar también que si bien en esta última posibilidad de mejora las ventajas son varias, el presupuesto económico para la implementación de soluciones SOAR frente a las soluciones anteriormente mencionadas es considerablemente mucho más costoso.

6. Si bien en la implementación de este proyecto de titulación se consideró como método de mitigación ante posibles problemas de hardware el utilizar herramientas de virtualización, la virtualización no considera escenarios en donde el centro de datos, donde esta solución fue instalada presente situación de fallo. Los problemas en los centros de datos así como también en el suministro eléctrico pueden llegar a inhabilitar completamente las funcionalidades de las herramientas instaladas para el sistema NSOC diseñado en este proyecto. Para mitigar estos problemas en mejoras futuras del proyecto se puede incluir soluciones de respaldo en un centro de datos alterno. Con un respaldo en hardware y software instalado en el centro de datos alterno, las soluciones principales y de respaldo podrían sincronizarse a través de protocolos de alta disponibilidad trabajando en modalidad maestro-esclavo. Los equipos terminales facilitan también el despliegue de estas arquitecturas de gestión de la red de datos, ya que en muchos de los equipos gestionados de la solución implementada, se pueden agregar uno o varios servidores de gestión en especial con los protocolos SNMP o SYSLOG, siendo posible reportar los datos de gestión a varios sitios remotos en los centros de datos.

# 5. REFERENCIAS BIBLIOGRÁFICAS


[1] P. C. Verhoef, T. Broekhuizen, Y. Bart y col., «Digital transformation: A multidisciplinary reflection and research agenda,» *Journal of Business Research*, vol. 122, págs. 889-901, 2021. DOI: 10.1016/j.jbusres.2019.09.022.

[2] L. Dogaru, «The Main Goals of the Fourth Industrial Revolution. Renewable Energy Perspectives,» *Procedia Manufacturing*, vol. 46, págs. 397-401, 2020. DOI: 10.1016/j.promfg.2020.03.058.

[3] F. P. Sioshansi, *Smart Grid Integrating Renewable, Distributed & Efficient Energy*. Amsterdam: Elsevier/Academic Press, 2012, págs. 3-28.

[4] J. Bruinenberg, L. Colton, E. Darmois y col., *CEN -CENELEC - ETSI: Smart Grid Coordination Group - Smart Grid Reference Architecture Report 2.0*, [Online], 2012. dirección: https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf (visitado 15-02-2022).

[5] R. Radvanovsky y A. McDougall, *Critical Infrastructure Homeland Security and Emergency Preparedness, Fourth Edition*, 4.ª ed. United States of America: CRC Press, 2021, pág. 2.

[6] M. Uslar, M. Specht, S. Rohjans, J. Trefke y J. M. González, *The Common Information Model CIM: IEC 61968/61970 and 62325 - A Practical Introduction to the CIM*. Berlin, Germany: Springer Publishing Company, Incorporated, 2012.

[7] H. Falk, *IEC 61850 Demystified*, ép. Artech House power engineering series. Norwood, MA, US: Artech House, 2018.

[8] NERC, *CIP Standards,* North American Electric Reliability Corporation - Nerc.com, [Online]. dirección: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx (visitado 15-02-2022).

[9] K. A. Stouffer, J. A. Falco y K. A. Scarfone, «SP 800-82. Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations Such as Programmable Logic Controllers (PLC),» Gaithersburg, MD, USA, inf. téc., 2011.

[10] G. Różański, «Security of communication in the special communications systems,» en *Radioelectronic Systems Conference 2019*, International Society for Optics y Photonics, vol. 11442, SPIE, 2020, págs. 241-252. DOI: 10.1117/12.2565307.

[11] D. Verma, *Principles of Computer Systems and Network Management*. Yorktown Heights, NY, USA: Springer-Verlag, ene. de 2009, págs. 1-260. DOI: 10.1007/978-0-387-89009-8.

[12] M. Xifeng y F. Yuanyuan, «Network management system design and implementation,» en *2011 IEEE 3rd International Conference on Communication Software and Networks*, 2011, págs. 373-375. DOI: 10.1109/ICCSN.2011.6013851.

[13] R. Boutaba y J. Xiao, «Network Management: State of the Art,» *IEEE PIMRC'95*, vol. 1, ene. de 2004. DOI: 10.1007/978-0-387-35600-6_5.

[14] A. Clemm, *Network Management Fundamentals*, 1st. Indianapolis, IN, US: Cisco Press, 2006.

[15] E. Cruz, J. Perea y J. Ruiz, *Aplicación de las TIC en los Sectores Económicos (Productivo, Comercial y Servicios)*, ép. Artech House power engineering series. Bogotá, Colombia: Scientometric E. Researching Consulting Group, 2018, págs. 117-125.

[16] E. Simpson, *The Best NOC and Service Desk Operations*. Intelligent Enterprise, oct. de 2009, pág. 484.

[17] S. Yadav, *Data Center NOC Room | NOC Roles & Responsibilities | Architecture*, NetForChoice Blog -, [Online], 2020. dirección: https://www.netforchoice.com/blog/data-center-noc-room (visitado 15-02-2022).

[18] M. Long, *A Small Business Guide to Network Operations Center (NOC)*, The Blueprint, [Online], 2020. dirección: https://www.fool.com/the-blueprint/noc/ (visitado 15-02-2022).

[19] S. Salinas, *Security Operations Center: Ultimate SOC Quick Start Guide*, Exabeam, [Online], 2021. dirección: https://www.exabeam.com/security-operations-center/security-operations-center-a-quick-start-guide/ (visitado 15-02-2022).

[20] J. Muniz, G. McIntyre y N. AlFardan, *Security Operations Center: Building, Operating, and Maintaining Your SOC*, 1st. Indianapolis, IN, US: Cisco Press, 2015.

[21] D. Nathans, *Designing and Building a Security Operations Center*, 1st. Waltham, MA, USA: Syngress Publishing, 2014.

[22] O. Cassetto, *Security Operations Center Roles and Responsibilities*, Exabeam, [Online], 2021. dirección: https://www.exabeam.com/security-operations-center/security-operations-center-roles-and-responsibilities/ (visitado 15-02-2022).

[23] *The SOC, SIEM, and Other Essential SOC Tools - Exabeam*, Exabeam, [Online], 2022. dirección: https://www.exabeam.com/explainers/siem/the-soc-secops-and-siem/ (visitado 15-02-2022).

[24] L. Kessem, *Threat Actors' Most Targeted Industries in 2020: Finance, Manufacturing and Energy — IBM, X-Force Threat Intelligence*, Security Intelligence, [Online], 2021. dirección: https://securityintelligence.com/posts/threat-actors-targeted-industries-2020-finance-manufacturing-energy/ (visitado 15-02-2022).

[25] T. Shyh, L. Kok, S. Nyi y T. Choon, «SMART NETWORK AND SECURITY OPERATIONS CENTRE,» 2016. dirección: https://www.dsta.gov.sg/docs/default-source/dsta-about/smart-network-and-security-operations-centre.pdf?sfvrsn=2 (visitado 15-02-2022).

[26] N. Hernandez, «NOC/SOC Integration: Opportunities for Increased Efficiency in Incident Response within Cyber-Security,» 2021. dirección: https://sansorg.egnyte.com/dl/cNkVP4S4Ux (visitado 15-02-2022).

[27] U. I. de Telecomunicaciones, *ITU-T M.3010, Principios para una red de gestión de las telecomunicaciones*, https://handle.itu.int/11.1002/1000/4869, Maintenance responsibility: ITU-T Study Group 2, feb. de 2000. (visitado 15-02-2022).

[28] J. R. Santamaria-Sandoval, «La La gestión en redes definidas por software (SDN) desde la perspectiva de FCAPS,» *Repertorio Científico*, vol. 23, n.º 2, págs. 1-12, 2020. DOI: 10.22458/rc.v23i2.2870.

[29] A. Pascal, *Industrial Cybersecurity: Efficiently secure critical infrastructure systems*. Birmingham, UK: Packt Publishing Ltd., oct. de 2017, págs. 7-31.

[30] R. Leszczyna, *Cybersecurity in the Electricity Sector: Managing Critical Infrastructure*, 1.ª ed. Cham, Switzerland: Springer International Publishing, 2019, págs. 68-73.

[31] L. Obregon, *Secure Architecture for Industrial Control Systems*, sep. de 2015. dirección: https://www.sans.org/white-papers/36327/ (visitado 15-02-2022).

[32] F. Sevillano, *Ciberseguridad industrial e infraestructuras críticas*, 1.ª ed. Paracuellos de Jarama, Madrid, España: RA-MA Editorial, 2021, págs. 233-323.

[33] A. M. Ayala, *Acuerdo Ministerial Nro. 031-2020, Norma Técnica que regula el Proceso para la evaluación de viabilidad técnica de Proyectos de Gobierno Electrónico y Autorización de Criticidad*, https://www.gobiernoelectronico.gob.ec, oct. de 2020. (visitado 15-02-2022).

[34] C. Samitier, *Utility Communication Networks and Services: Specification, Deployment and Operation*. Cham, Switzerland: Springer International Publishing, 2017, págs. 213-240.

[35] Y. Haik, T. Shahin y S. Sivaloganathan, *Engineering Design Process*. Cengage Learning, 2010.

[36] Emmett Dulaney A, *Comptia Network+ N10-006 Exam Cram*. Indianapolis, Indiana: Pearson Education, 2015, págs. 381-389.

[37] M. Liotine, *Mission-critical network planning*. Boston: Artech House, 2003, págs. 31-60.

[38] Zabbix LLC, *Hardware Requirements*, Zabbix.com, [Online], 2021. dirección: https://www.zabbix.com/documentation/current/en/manual/installation/requirements (visitado 15-02-2022).

[39] Greenbone Networks GMBH, *Greenbone Security Manager with Greenbone OS 20.08 – User Manual — Greenbone Security Manager (GSM) 20.08.13 documentation*, Docs.greenbone.net, [Online], 2021. dirección: https://docs.greenbone.net/GSM-Manual/gos-20.08/en/ (visitado 15-02-2022).

[40] Adiscon LogAnalyzer, *LogAnalyzer - Documentation*, Loganalyzer.adiscon.com, [Online], 2021. dirección: https://loganalyzer.adiscon.com/ (visitado 15-02-2022).

# ABREVIATURAS

**ADMS** Advanced Distribution Management System. 6, 7

**CCTV** Circuito Cerrado de Televisión. 6, 7

**CDP** Cisco Discovery Protocol. 30

**CIS** Center for Internet Security. 31

**CLI** Command-Line Interface. 106

**CVSS** Common Vulnerability Scoring. 31

**E.E.Q.** Empresa Eléctrica Quito. 1–7, 15, 39, 42, 45–50, 70

**FCAPS** Falla, Configuración, Contabilidad, Desempeño, Seguridad. 10, 11

**IACS** Sistema de Control y Automatización Industrial. 13

**ICMP** Internet Control Message Protocol. 2, 3, 7, 40, 105

**ICS** Sistemas de Control Industrial. 13

**IDS** Intrusion Detection System. 155

**IED** Equipos Electrónicos Inteligentes. 3, 7, 45, 48, 131

**ISA-95** Integración de los Sistemas de Control Empresarial. 12

**ITU** International Telecommunication Union. 6

**ITU-T-X.805** ITU-T X.805 : Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo. 14

**LDAP** Lightweight Directory Access Protocol. 12

**LLDP** Link Layer Discovery Protocol. 30

**MIB** Management Information Base. 8

**MINTEL** Ministerio de Telecomunicaciones y de la Sociedad de la Información. 15

**NERC** North American Electric Reliability Corporation. 14

**NERC-CIP** North American Electric Reliability Corporation - Critical Infrastructure Protection. 6

**NIST** National Institute of Standards and Technology NIST. 6, 13, 31

**NMS** Network Management System. 52

**NOC** Centro de Operaciones de Red. 1, 2, 8, 9, 17, 18, 23–27

**NSM** Sistema de Gestión de Red. 8, 18

**NSOC** Centro de Operaciones de Seguridad en Redes. 1–3, 7, 9, 21–26

**RADIUS** Remote Authentication Dial In User Service. 12

**ROS** Rugged Operating System. 106

**RTU** Unidades Remotas de Control. 3, 7, 44, 49, 131

**SCADA** Supervisory Control And Data Acquisition. 2, 4, 7

**SGAM** Smart Grid Architecture Model. 5

**SIEM** Security Information and Event Management. 20, 22, 155

**SNMP** Simple Network Management Protocol. 2, 3, 7, 8, 39, 40, 52, 104–110, 114, 115

**SOAR** Security Orchestration Automation and Response. 20, 22, 156

**SOC** Centro de Operaciones de Seguridad. 1, 2, 9, 19, 20, 23–27

**SSH** Secure SHell. 51, 52, 106

**SYSLOG** System Logging Protocol. 2, 3, 7

**TACACS** Terminal Access Controller Access Control System. 12

**TELNET** Teletype Network. 106

**TIC** Tecnologías de la Información y de las Comunicaciones. 4

**VPN** Virtual Private Network. 18, 20, 23