# UNIVERSIDAD CATÓLICA
# DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TEMA:

**Análisis y diseño de un sistema de monitoreo para una red de equipos eléctricos en una empresa de telecomunicaciones en la ciudad de Guayaquil**

AUTOR

Ing. Villalva Melgar, Francis David

Trabajo de Titulación previo a la obtención del Grado Académico de

**MAGÍSTER EN TELECOMUNICACIONES**

TUTOR:

M. Sc. Palacios Meléndez, Edwin Fernando

Guayaquil, 29 de octubre de 2020

# UNIVERSIDAD CATÓLICA
# DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el Magíster **Villalva Melgar, Francis David** como requerimiento parcial para la obtención del Grado Académico de **MAGISTER EN TELECOMUNICACIONES**.

TUTOR

M. Sc. Palacios Meléndez, Edwin Fernando

DIRECTOR DEL PROGRAMA

M. Sc. Romero Paz, Manuel de Jesús

Guayaquil, 29 de octubre de 2020

# UNIVERSIDAD CATÓLICA
# DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

## DECLARACIÓN DE RESPONSABILIDAD

Yo, **Villalva Melgar, Francis David**

**DECLARÓ QUE:**

El trabajo de titulación "**Análisis y diseño de un sistema de monitoreo para una red de equipos eléctricos en una empresa de telecomunicaciones en la ciudad de Guayaquil**", previa a la obtención del grado Académico de **Magíster en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del Trabajo de Titulación referido.

Guayaquil, 29 de octubre de 2020

EL AUTOR

Villalva Melgar, Francis David

# UNIVERSIDAD CATÓLICA
# DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

**AUTORIZACIÓN**

Yo, **Villalva Melgar, Francis David**

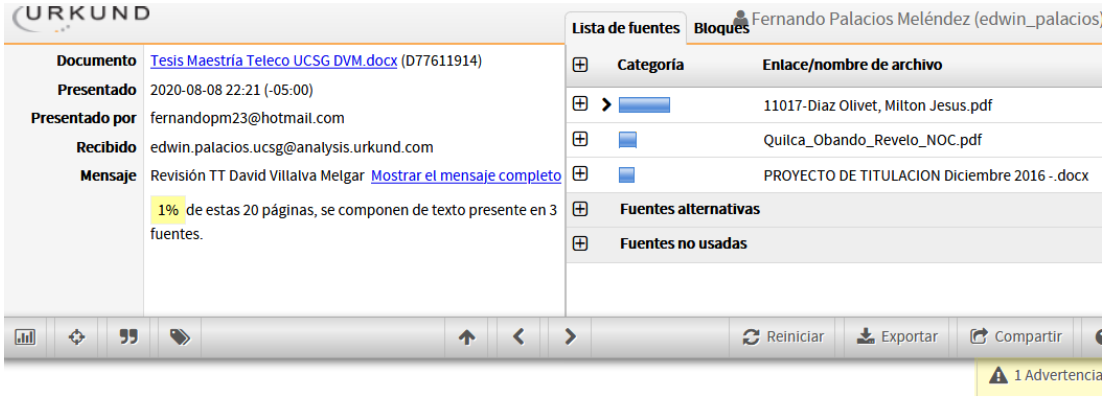
Autorizó a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del Trabajo de Titulación: **"Análisis y diseño de un sistema de monitoreo para una red de equipos eléctricos en una empresa de telecomunicaciones en la ciudad de Guayaquil"**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, 29 de octubre de 2020

EL AUTOR

Villalva Melgar, Francis David

# REPORTE DE URKUND




UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL
SISTEMA DE POSGRADO MAESTRÍA EN
TELECOMUNICACIONES

TEMA: Análisis y diseño de un sistema de monitoreo para una red de equipos eléctricos en una empresa de telecomunicaciones en la ciudad de Guayaquil.

AUTOR Ing. Villalva Melgar, Francis David

Trabajo de Titulación previo a la obtención del Grado Académico de Magíster en Telecomunicaciones

TUTOR: M. Sc. Palacios Meléndez, Edwin Fernando

Guayaquil, Ecuador

2 de Junio del 2020

UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL
SISTEMA DE POSGRADO MAESTRÍA EN
TELECOMUNICACIONES

**Dedicatoria**

A mi familia y amigos incondicionales por el apoyo que me siguen dando.

Villalva Melgar, Francis David

**Agradecimientos**

A Jehová mi Dios por darme las oportunidades necesarias en adelantar conocimiento como desarrollo personal e intelectual. A mi tutor Ing. Fernando Palacios por su paciencia y su valiosa aportación científica en el desarrollo de este proyecto; a mi familia personal por su apoyo incondicional. A la Universidad Católica Santiago de Guayaquil por la oportunidad dada de ser educado en sus aulas en su máxima de conocimiento.

Villalva Melgar, Francis David

**UNIVERSIDAD CATÓLICA**

**DE SANTIAGO DE GUAYAQUIL**

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

## TRIBUNAL DE SUSTENTACIÓN

f. _____

**M. Sc. PALACIOS MELÉNDEZ, EDWIN FERNANDO**

TUTOR

f. _____

**M. Sc. QUEZADA CALLE, EDGAR RAUL**

TUTOR

f. _____

**M. Sc. CÓRDOVA RIVADENIERA, LUIS SILVIO**

REVISOR

f. _____

**M. Sc. ROMERO PAZ, MANUEL DE JESÚS**

DIRECTOR DEL PROGRAMA

## ÍNDICE GENERAL

## ÍNDICE DE FIGURAS

**Capítulo 2:**



**Capítulo 3:**

## ÍNDICE DE TABLAS

**Capítulo 2:**



**Capítulo 3:**

**Resumen**

Se tiene como finalidad diseñar un esquema integral para la gestión de sistemas eléctricos usando la red IP fija de telecomunicaciones en la ciudad de Guayaquil. Estos sistemas eléctricos están comprendidos en rectificadores, bancos de baterías, grupo electrógeno y tableros de distribución tanto en corriente alterna como continua, cuya finalidad es de la operación y mantenimiento oportuno sobre el equipamiento eléctrico. Esto incluye integrar eficazmente los sensores de alarmas en la red IP usando como transporte de la señal, los elementos de la red fija, como son los equipos de voz, de DSLAM y MPLS pasando, en muy pocos casos debido a la versatilidad de la red, por fibra óptica mediante la red DWM. La gestión de este segmento aislado de la red proporcionará dentro de las tareas de mantenimiento correctivo, los datos adecuados para optimizar los tiempos de atención ya que esto último incide directamente en el desempeño de toda la red, traduciéndose en interrupción de servicio hacia la ciudadanía y por ello posibles sanciones del ente regulador.

**Palabras claves:** GESTION, REDES, PRTG, SNMP, ARQUICTETURAS, RECTIFICADORES.

**Abstract**

Its purpose is to design an integral scheme for the management of electrical systems using the fixed ip network of telecommunications in the Guayaquil city. These electrical systems are comprised of rectifiers, battery banks, generator set and distribution boards in both alternating and direct current, whose purpose is the timely operation and maintenance of the electrical equipment. This includes effectively integrating the alarm sensors in the IP network using as signal transport, the elements of the fixed network, such as voice, DSLAM and MPLS equipment, in very few cases due to the versatility of the network , by optical fiber through the DWM network. The management of this isolated segment of the network will provide, within the corrective maintenance tasks, adequate data to optimize the attention times since this last directly affects the performance of the entire network, resulting in service interruption towards citizenship and therefore possible sanctions of the regulator.

**Keywords:** MANAGEMENT, NETWORKS, PRTG, SNMP, ARCHICTETURES, RECTIFIERS.

# Capítulo 1: Descripción del proyecto de intervención.

Este proyecto tiene como finalidad el diseño integral de la red de los sistemas eléctricos para ser gestionados remotamente mediante la red fija de telecomunicaciones en la ciudad de Guayaquil, lo que implica la integración correcta de los elementos eléctricos con el equipamiento de la red ip, a pesar de la versatilidad de esta última por los diferentes modelos de los equipos que se tiene en esta red.

## 1.1. Introducción.

Los sistemas de eléctricos cumplen una función muy especial dentro de las redes de telecomunicaciones. Cada elemento de la red necesita de energía asegurada para cumplir su disponibilidad al 100%. Un banco de baterías, un tablero de transferencia automática o un generador eléctrico son solo alguno de los componentes de dichos sistemas, lo cual se necesitan gestionarlos para el control de su comportamiento, así como la planificación del correcto mantenimiento. Sin embargo, en muchos casos se le resta importancia en que la gestión de estos equipos pueda usar Sistemas de Gestión dentro de la misma red de telecomunicaciones, y mucho tiene que ver con el conocimiento tanto eléctrico como en redes ya que ambas áreas se combinan de manera especial para lograr efectividad al interconectar equipos que dan respaldos eléctricos a otros equipos dentro de la red.

En este proyecto se analiza detenidamente el esquema global para que todos los elementos de los sistemas eléctricos sean gestionables remotamente a través de la red de telecomunicaciones. En este sentido, la señal (de donde ese conecta el sensor), viaja a través de equipos de voz (a nivel de ip, llamados MSAN), entrando por la red MPLS y Red Troncal de Fibra Óptica, hacia la red corporativa (cuya red IP es diferente) llegando al servidor. No se considera en el presente proyecto de titulación, la configuración de firewall ni enrutadores (Routers) en la nube MPLS ni de equipos de la Red Troncal de Fibra Óptica.

## 1.2. Antecedentes.

Todos los elementos de la red de sistemas eléctricos, que son: Rectificadores, Tableros de Transferencias Automáticas, TVSS (Supresores de Transientes), Bancos de transformadores, Tablero Principal en AC, Tablero Principal en DC y Bancos de Baterías, constituyen en conjunto la sostenibilidad ante la red de telecomunicaciones, independientemente de la utilidad de los equipos de comunicación correspondiente a cada área (como pueden ser Switches [MPLS], equipos de Voz [Conmutación TDM e IP], de Datos [DSLAM], Core [softswitch], etc.). Si bien es cierto que dentro de una red de telecomunicación es esencial equipos de transmisiones de voz, datos y video, estos no podrían funcionar sin los sistemas de energía.

Sin embargo, estos equipos no operan de modo automática ni son funcionales sin mantenimientos por mucho tiempo debido a desgastes de sus elementos, variantes en su entorno (clima, falta de energía pública, falla humana, etc.) y por obsolescencia. Esta es una falencia que posee no solo una sino muchas empresas locales que trabajan directamente con estos tipos de sistemas y a la vez si son dependientes para prestar servicios a otros equipos. Si bien es cierto que paradójicamente existe en el mercado local muchas empresas que se dedican a brindar servicios de mantenimientos para equipos en sistemas eléctricos (outsourcing) pero a un costo muy elevado por lo que gerentes o administradores evitan dichos servicios a pesar de que, en función del tiempo, las perdidas monetarias son inestimables si no se da la atención necesaria en mantenimiento. Una gestión óptima sobre ellos impacta positivamente en el mantenimiento oportuno y programado generando un mínimo de interrupciones de servicio y bajo impacto en daños en todos los sistemas de telecomunicaciones.

## 1.3. Definición del problema

La falta de monitoreo sobre sistemas eléctricos que incluyen elementos de generación de energía en DC conlleva a una atención tardía en fallos recurrentes sobre nodos y centrales telefónicas cuando existe interrupción el servicio eléctrico público o fallos en elementos eléctricos, afectando gravemente la disponibilidad de la red de telecomunicaciones, así como la

interrupción de servicio (especialmente a nivel de voz y datos) y generación de sanciones por parte del ente regulador.

## 1.4. Justificación del Problema.

Este proyecto está orientado a solventar esquemáticamente el monitoreo sobre elementos de provisión de servicio eléctrico que a su vez proporcionan energía eléctrica eficaz a equipos de la red de telecomunicaciones. Se busca disminuir el tiempo de atención al generarse algún problema en toda la red de voz y datos, ya que al momento el área pertinente no posee un gestor sobre dichos elementos eléctricos.

## 1.5. Objetivos

Los objetivos que se han definido para este proyecto son los siguientes:

### 1.5.1. Objetivo General:

Diseñar un esquema funcional de gestión para el monitoreo sobre sistemas eléctricos que incluyen elementos tales como Rectificadores, Tableros de Transferencias Automáticas, Generadores Eléctricos y Bancos de Baterías, usando una red de telecomunicaciones convergente.

### 1.5.2. Objetivos específicos:

- ✓ Analizar si todos los elementos eléctricos son gestionables o no en la red de telecomunicaciones.
- ✓ Analizar y diseñar un esquema integrado de monitoreo mediante la gestión sobre rectificadores, bancos de baterías y generadores eléctricos, mediante el PRTG.
- ✓ Evaluar si el nuevo esquema integrado de gestión ayuda en la atención en mantenimientos correctivos en cada nodo y/o central.

## 1.6. Hipótesis.

El diseño de este proyecto está orientado hacia la sostenibilidad de los servicios que entrega los sistemas de energía, como es energía eléctrica asegurada (sean en AC o en DC), hacia los diferentes elementos de red, y gestionarlo remotamente mediante la infraestructura IP, lo cual permitirá la

óptima y efectiva atención de los eventos que provoquen la interrupción del servicio, sea de voz (fija o móvil), datos e internet.

### 1.7. Metodología de investigación.

La metodología aplicada en el presente proyecto es de carácter analítico y descriptivo, cuyo enfoque es en la integración por partes de cada elemento eléctrico a la red de voz. Se analiza dichos elementos si es gestionable o no y así se revisa la configuración de los equipos de voz (MSAN) para la recepción de señales y tener nuevos sensores de los equipos eléctricos.

## Capítulo 2: Fundamentación Teórica.

En este capítulo se revisa conceptos de redes, así como la descripción general de los elementos de los sistemas eléctricos y de herramientas de comunicación remota mediante interfaces físicas y lógicas.

### 2.1. Fuentes naturales de electricidad.

La mayoría de las fuentes de energía eléctrica en la naturaleza son demasiado difusas o caras de capturar para ser prácticas. La bioelectricidad ocurre en formas de vida, pero generalmente es bastante pequeña. Una excepción dramática es la anguila eléctrica, que puede desarrollar más de 300 V y puede provocar una descarga letal. Un ejemplo menos violento es la suave luz amarilla de la luciérnaga, que usa bioelectricidad en forma de electroluminiscencia. El rayo es ciertamente espectacular y poderoso; sin embargo, el contenido energético es modesto.

En la figura 2.1 se muestra un ejemplo donde se estima aproximadamente 100 MV, 20 kA y 10 μs para un rayo de tamaño mediano, el contenido de energía sería, (Gross & Roppel, 2012)

$$W = VIt = 100 \times 10^6 \cdot 20 \times 10^3 \cdot 10 \times 10^{-6} = 20\ MJ$$

Figura 2. 1: Descripción general del grupo electrógeno.
Fuente: (Gross & Roppel, 2012)

## 2.2. Sistemas de energía.

Un sistema de energía está predominantemente en funcionamiento en estado estacionario o en un estado que podría considerarse con suficiente precisión como estado estacionario. En un sistema de potencia siempre ocurren pequeños cambios de carga, acciones de conmutación y otros transitorios, de modo que, en un sentido matemático estricto, la mayoría de las variables varían con el tiempo. Sin embargo, estas variaciones son la mayoría de las veces tan pequeñas que se justifica un modelo algebraico, es decir, no variable en el tiempo del sistema de potencia.

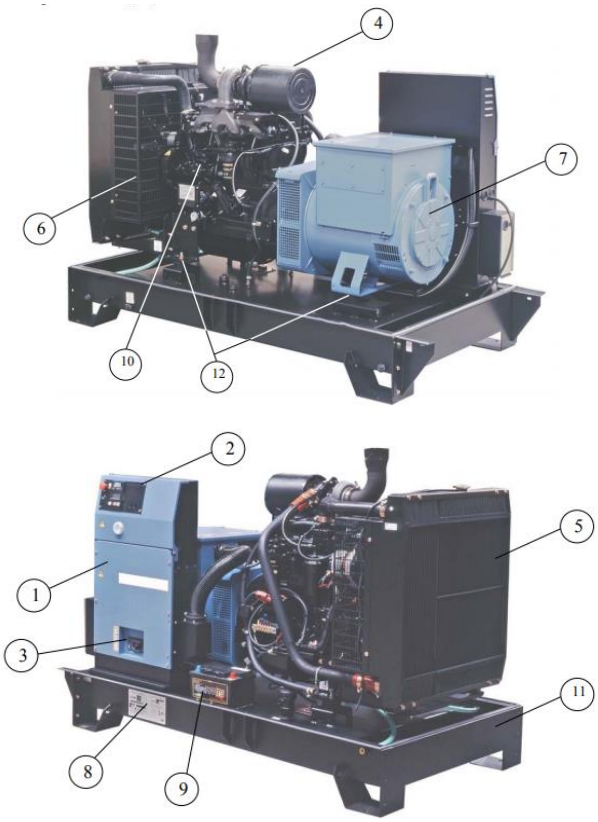
Un cortocircuito en un sistema de energía claramente no es una condición de estado estable. Tal evento puede iniciar una variedad de fenómenos dinámicos diferentes en el sistema, y para estudiar estos modelos dinámicos son necesarios. Sin embargo, cuando se trata de calcular las corrientes de falla en el sistema, se pueden usar modelos de estado estable (estático) con valores de parámetros apropiados. Una corriente de falla consta de dos componentes, una parte transitoria y una parte de estado estacionario, pero dado que la parte transitoria se puede estimar a partir de la de estado estable, el análisis de corriente de falla se limita comúnmente al cálculo de las corrientes de falla de estado estacionario. (Raviprasad et al., 2012)

Por ejemplo, los sistemas de eléctricos que dan servicios a redes de telecomunicaciones tienen características particulares dependiendo de la técnica de acceso que utilicen, la frecuencia de operación y el uso o no de diversidad, entre otros aspectos (Candotti & Mavares, 2012, p. 212).

En la publicación de (Cruz Felipe et al., 2013, p. 86) indican que los equipos dentro de los sistemas eléctricos, en sus diferentes variantes, son de actividades críticas y de mayor control por cuanto “abastecen” servicios a otros equipos de las diferentes redes como son: Redes de Acceso fijo – Móvil, Red MPLS, Red Troncal de Fibra Óptica, etc., por lo que los planes de Operación y Mantenimiento deben cumplir 100% de disponibilidad de esta red.

### 2.2.1. Grupo Electrógeno.

Se definen como grupo electrógeno básicamente al generador eléctrico. En caso de que exista fallo de energía de la red pública, el grupo electrógeno proporciona la energía alterna necesaria para que los elementos de la red de telecomunicaciones funciones a pesar de la falta de energía publica que se pueda presentar. En la siguiente figura 1, se muestra las partes esenciales de un grupo electrógeno:




| | | | | | |
|---|---|---|---|---|---|
| 1 | Consola | 5 | Radiador | 9 | Batería de arranque |
| 2 | Caja de control | 6 | Rejilla de protección de las piezas giratorias | 10 | Motor |
| 3 | Disyuntor | 7 | Alternador | 11 | Chasis |
| 4 | Filtro de aire | 8 | Placa de identificación | 12 | Contactos de suspensión |

Figura 2. 2: Descripción general del grupo electrógeno.
Fuente: (SDMO, 2015)

Estos equipos deben ser sometidos a mantenimientos programados para un correcto funcionamiento y disponibilidad hacia la red. Los planes de mantenimiento (tablas de mantenimiento periódico) se definen en la documentación correspondiente (manual de mantenimiento) a los motores, los alternadores y determinados accesorios. Por norma general, en estos planes se distingue entre el funcionamiento en modo continuo y el funcionamiento en condiciones de emergencia. Para ello se tiene en cuenta los elementos que

intervienen, como por ejemplo la proporción de azufre del gasóleo o la calidad del aceite de lubricación. De este modo, una vez que se reciba el grupo y teniendo en cuenta los elementos anteriormente mencionados, se deben estudiar estos planes de mantenimiento para determinar su periodicidad que es necesario llevar a cabo. Como complemento a dichos planes de mantenimiento, es recomendable realizar las siguientes comprobaciones:

Mecánicos:

- controles mecánicos (ajustes mecánicos, tensión de las correas, etc.)
- control de los equipos de refrigeración.
- control del ajuste de las fijaciones de los equipos, reajuste de los tornillos y pernos.

Eléctricos:

- controles eléctricos, de automatismo y seguridad.
- comprobación de los dispositivos de regulación eléctrica.
- control del aislamiento del alternador.
- reajuste del juego de barras del alternador.
- comprobación del aislamiento de los auxiliares y del consumo de corriente de estos.
- control de los sistemas de carga de las baterías de arranque
- control de las baterías.

Estas comprobaciones se deben llevar a cabo en los plazos recomendados a continuación (o de acuerdo con las especificaciones del fabricante):

- funcionamiento del grupo en condiciones de emergencia ($\leq$100 horas al año): una vez al año.
- funcionamiento del grupo en condiciones de emergencia ($\leq$500 horas al año): 3 veces al año.
- funcionamiento continuo del grupo:
    - comprobaciones mecánicas: durante el proceso de vaciado del aceite.
    - comprobaciones eléctricas: cada 6 años.

Los GE son fuente importante de suministro de energía eléctrica y, dependiendo de la función que cumplen, pueden utilizarse de tres formas: como fuente primaria, en cuyo caso son la única fuente disponible de energía y operan de manera continua; como fuente de cogeneración, en cuyo caso el GE interviene para reducir los picos de máxima demanda; y como fuente de emergencia, en cuyo caso el grupo es utilizado únicamente cuando hay interrupción de la red de suministro principal (Francisco et al., 2007).

Es posible encontrar GE con potencias entre 500 VA y 500 KVA e incluso superiores, los cuales incorporan automatismos de complejidad creciente, dependiendo de la potencia de operación (Giangrandi, 2011). En equipos con potencias de entre 10 y 50 KVA se integran automatismos básicos, compuestos por relés, temporizadores y contactores, los cuales permiten el arranque y apagado del motor, junto con la conexión y desconexión del grupo electrógeno y de la red a la carga.

Las variables por monitorear se pueden dividir en dos grupos: las del motor y las del generador. En las primeras se encuentran la temperatura, la presión de aceite y la velocidad de rotación del motor. Entre las segundas se tienen: tensión de generación, la corriente suministrada por el generador, la frecuencia y la secuencia de fases del generador. Adicionalmente se deben conocer las variables eléctricas asociadas a la red convencional, especialmente la tensión, la frecuencia y la secuencia de fases.

Las variables por monitorear en el motor de combustión interna son: velocidad de rotación, presión de aceite y temperatura. La tarjeta electrónica propuesta se basa en un microcontrolador PIC16F873, encargado de procesar estas variables. Como elementos de captación se utilizaron: un sensor de efecto Hall OH090U y un anillo de ocho imanes acoplados al eje del motor; un sensor LM35, debidamente encapsulado para detectar las variaciones de la temperatura y un sensor de presión de estado sólido MPX5700DP. Para más información consultar a Fernández y Duarte (Fernández Morales y Duarte, 2013).

### 2.2.2. Rectificadores.

Los equipos rectificación cumplen un rol esencial dentro de los sistemas de energía y climatización en la red de telecomunicaciones. El sistema de rectificación ayuda al suministro de corriente continua de manera compacta, es decir, sin corrientes parásitas y de potencia ajustable, desarrollada específicamente para la industria de las telecomunicaciones.

Básicamente, un rectificador es un dispositivo eléctrico que convierte la corriente alterna, que invierte periódicamente la dirección, en corriente continua, que fluye en una sola dirección. La figura 2.3 muestra un circuito esquemático de una planta DC unifilar. El rectificador tiene dos requisitos principales, el principal es proporcionar energía de corriente continua (CC) a las cargas soportadas, así como cargar y mantener las baterías de la planta de CC para mantener la planta en funcionamiento en caso de un corte de energía. Al buscar opciones, es importante revisar la eficiencia, la redundancia y el modularidad del sistema de la planta de CC.

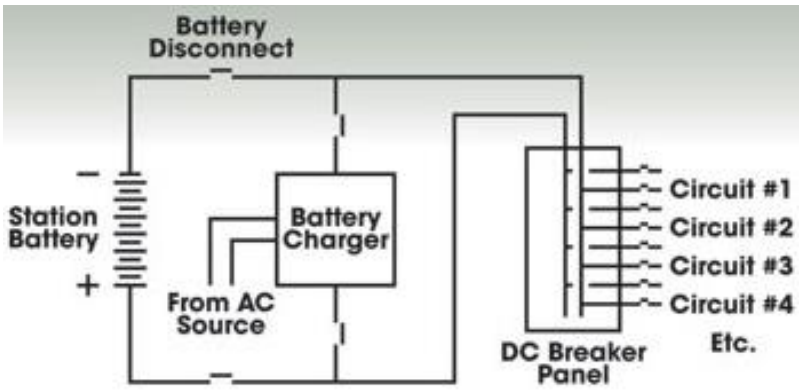



Figura 2. 3: Esquemático de una planta DC unifilar.
Fuente: (Schairer, 2018)

Cosas para tener en cuenta al elegir un rectificador:

¿El sistema del que se realiza la copia de seguridad necesita redundancia?

¿Es la eficiencia importante para este sistema?

¿El sistema eventualmente necesita crecer o escalar? Algunos sistemas de plantas de CC son modulares y fácilmente escalables, lo que permite una expansión futura sin cambios de infraestructura significativos.

**Controlador:** para algunos sistemas, puede haber un controlador separado. El controlador es esencialmente el "cerebro" de su planta de corriente continua (CC). Proporciona la lógica al resto del sistema, observando el rectificador, las baterías y la distribución, dándoles comandos de funcionamiento y proporcionando información sobre el estado y la funcionalidad de la unidad. Para el controlador, es importante comprender qué tipo de requisitos de comunicación de red existen. Por ejemplo, ¿la unidad debe conectarse al sistema de automatización del edificio? ¿Necesita conectividad de red a través de SNMP u otro protocolo de comunicación?

En la figura 2.4 se muestra un sistema de rectificadores fabricada por QP Solutions. En la figura 2.5 se muestra el equipo de rectificación instalado en la empresa de telecomunicaciones CNT. Este tipo de equipamiento contiene soportes para breakers que van a distribuir la corriente a los demás elementos.

Figura 2. 4: Sistema de rectificación Vertiv NetSure
Fuente: (Schairer, 2018)

Los módulos rectificadores (véase la figura 2.6) incorpora el monitoreo de energía como solución remota, puesto que usan un microprocesador interno que proporciona actualizaciones al segundo del sistema controlador y rectificadores adyacentes. Esta garantiza el intercambio de carga

estrechamente controlado entre los rectificadores y proporciona el estado e información de identificación al controlador. Con solo cuatro unidades de rack altas, estos compactos rectificadores proporcionan hasta 1600 vatios y permiten hasta a 10 módulos rectificadores en un sub-bastidor de 23 pulgadas u ocho módulos en un subrack de 19 pulgadas. Generalmente son diseñados teniendo en cuenta la diversidad y capacidad de operación en una gama completa de interiores y aplicaciones al aire libre.

Figura 2. 5: Sistema de Rectificación en CNT.
Elaborado por: Autor

Figura 2. 6: Arreglo de módulos rectificadores
Elaborado por: Autor

Dentro de los sistemas de rectificación, están las controladoras para conexiones en red (llamadas SMU o ACC), generalmente con gestor propio. Dicha tarjeta monitorea todos los parámetros del sistema, incluidos: voltaje DC, corriente rectificadora, temperatura del rectificador, capacidad del

sistema, parámetros de la batería y estado del interruptor automático, tal como se muestra en la figura 2.7.

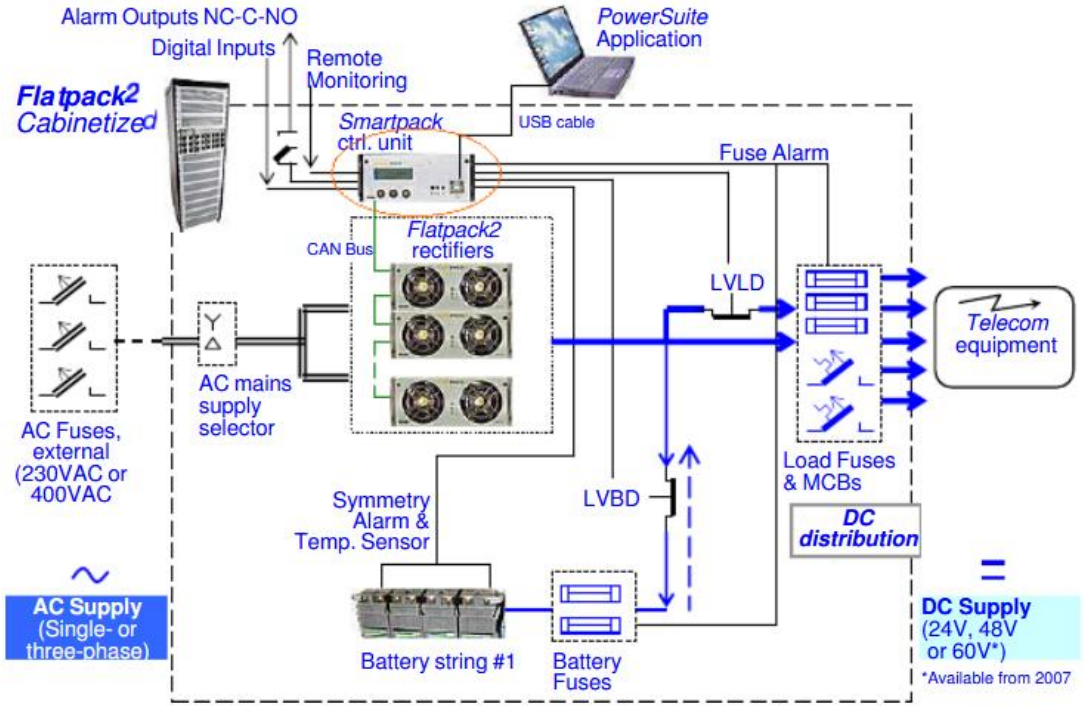



Figura 2. 7: Esquema general de conexión del Rectificador al gestor.
Fuente: (Eltek, 2006)

Las notificaciones de alarma y advertencia se indican mediante LED del panel frontal y mediante posibles contactos de alarma libres que permiten la señalización remota. La monitorización externa de las alarmas se realiza a través de un puerto USB o RS232 utilizando el software apropiado (integrado la MIB y comunidades SNMP) basado en PC. Estas tarjetas controladoras tienen un puerto Ethernet que permite el control sobre una red TCP/IP y soporte basado en la web. Las alarmas se pueden mapear mediante trampas SNMP a las plataformas OSS del cliente.

Para cumplir con los requisitos individuales del sitio, la tarjeta controladora contiene una Unidad lógica programable que se puede utilizar para controlar y modificar los requisitos especificados. Esto permite que el enrutamiento de alarma individual y las operaciones lógicas se establezcan como acciones, las alarmas se activen y las salidas se activen en función de la supervisión, comparación y procesamiento de señales internas y externas.

### 2.2.3. Bancos de Baterías

Las baterías son una fuente de voltaje y se utilizan para soportar los sistemas de telecomunicaciones durante un corte de energía alterna. Estos elementos ayudan a dar sostenimiento a la disponibilidad de la red junto con los rectificadores. La figura 2.8 muestra la forma que tiene una batería estándar de un banco de baterías.

Figura 2. 8: Batería estándar
Fuente: (Eltek, 2006)

Las baterías deben cumplir con características propias que puedan dar sostenimiento eléctrico en DC por un determinado tiempo. En la figura 2.9 se muestra de cómo las baterías trabajan al momento de ejercer carga en DC a los elementos de red; sin embargo, también se denota las fases de carga y descarga con el régimen de saturación que, generalmente, es dañino para la batería.

Si la entrada de AC al sistema de alimentación es normal y cumple con los requisitos de carga, los rectificadores suministran corriente continua a las cargas y carga las baterías. Si la entrada de AC es anormal o los rectificadores están sobrecargados o son defectuosos, las baterías suministran energía a las cargas. Después de rectificar la falla, los rectificadores continúan suministrando corriente continua y cargando las baterías.

Generalmente, en equipamiento de los sistemas de rectificadores, están las SMU o ACC, los cuales permite que las baterías se cambien entre la carga de flotación y la carga ecualizada ajustando la tensión de salida.

- Carga flotante: la SMU o ACC compensa la electricidad consumida por la autodescarga después de la carga completa.

- Carga ecualizada: la SMU o ACC carga completamente las baterías rápidamente al aumentar la tensión de salida. Durante la carga ecualizada, la SMU o ACC limita la corriente de salida del rectificador para evitar daños a la batería causados por una corriente de carga mayor.

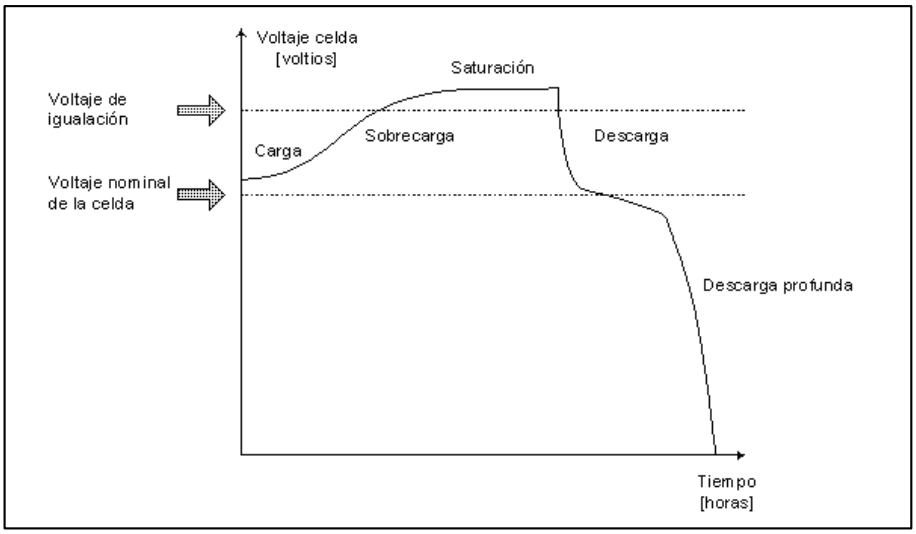



Figura 2. 9: Fases de carga y descarga de las baterías
Fuente: (Eltek, 2006)

### 2.2.4. Tipos de Baterías

Actualmente se tiene los siguientes tipos de baterías:

- Plomo Acido, que a su vez pueden ser:
  - Sumergidas (abiertas ventiladas)
    - Plomo-Acido regulada por válvula, VRLA (selladas), conteniendo lámina de fibra de vidrio absorbente AGM y Gel.
- Níquel Cadmio

## 2.3. Gestión de la red IP fija de telecomunicaciones

"La gestión de red se refiere a las actividades, métodos, procedimientos y herramientas que pertenezcan a la operación, administración, mantenimiento y aprovisionamiento de los sistemas de red".

Donde:

• Operación, tiene que ver con tener la red funcionando sin interrupciones. Esto incluye el monitoreo de la red para establecer los

problemas que están presentes lo más rápido posible, idealmente antes de que el usuario se entere de la existencia de dicho problema.

• Administración, que involucra el seguimiento de los recursos de la red y como están asignados.

• Mantenimiento, que se refiere a las actualizaciones y reparaciones para el correcto desempeño de la red. El mantenimiento también incluye las medidas correctivas y preventivas dentro de la red.

• Aprovisionamiento, se refiere a la configuración de los recursos para soportar los servicios que requieran.

Existen definiciones dadas por instituciones de estandarización como la ISO (International Standarization Organization), la cual define que: “La gestión de red es un conjunto de facilidades para controlar, coordinar y monitorizar los recursos que soportan las comunicaciones”

Sin embargo, así como los agentes de gestión actúan como un Proxy que representan el mundo real con el fin de gestionar los recursos, así mismo, un sistema de gestión actúa como Proxy para la organización de soporte de operaciones. Un sistema de gestión proporciona las herramientas para gestionar la red, estas herramientas que incluyen aplicaciones para monitorear la red, sistemas de aprovisionamiento de servicios, analizadores de tráfico, etc.

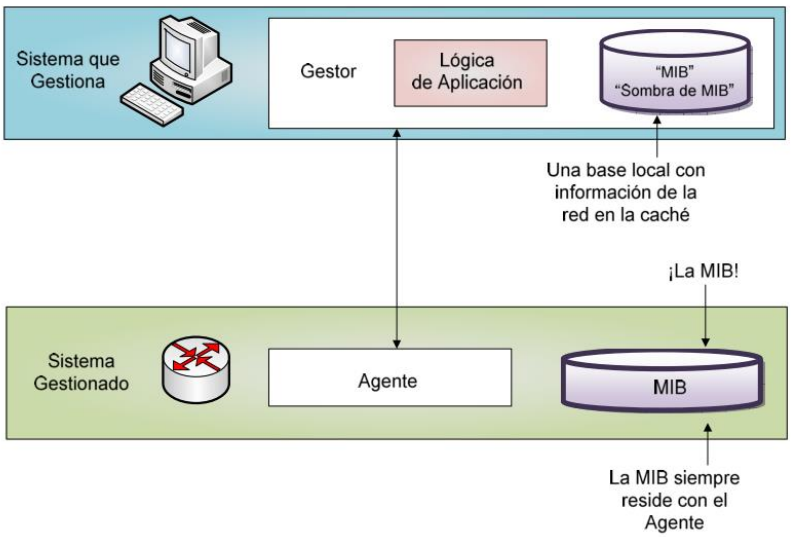



Figura 2. 10: Ubicación de la MIB en un sistema de gestión.
Fuente: (Olga, 2009)

Para tener una mejor eficiencia, muchos sistemas de gestión construyen su propia base de datos, en la cual mantienen información temporalmente para evitar tener que regresar al elemento de red repetidamente por la misma información. Esta base de datos interna se la conoce como MIB de la caché o "shadow MIB". En la figura 2.10 se muestra un esquema general el uso y ubicación de la MIB cuando esta trabaja en una red centralizada bajo un solo gestor.

### 2.3.1. Elementos de la Red

Comúnmente son llamados dispositivos en la red las cuales son gestionados. El elemento de red forma parte del proceso de gestión. Para poder ser gestionado este proporciona una interfaz para poder comunicarse con el sistema de gestión. A través de esta interfaz el elemento de red puede recibir peticiones del sistema de gestión y así mismo responder estas solicitudes. El dispositivo de red dentro del proceso de gestión toma el rol de "agente" y es el que soporta a las peticiones del "gestor" de manera proactiva, notificándole si ocurre algún evento inesperado.

### 2.3.2. Gestor

El gestor es un elemento de sistema cuya tarea es enviar requerimientos de gestión hacia los agentes para el control, coordinación y monitoreo de la red. En la práctica, el gestor es la aplicación (software) que emite las directivas de operaciones de gestión y recibe notificaciones y respuestas. Este se implementa en una estación de gestión (Workstation o una PC) en la cual se tiene una Base de Información de Gestión (MIB: Management Information Base) del dispositivo gestionado y una interfaz de usuario (Olga, 2009).

### 2.3.3. Agente

El agente es un elemento de sistema hacia el cual se dirigen los comandos de gestión para el control, coordinación, y monitoreo de la red. Los agentes ejecutan operaciones sobre los objetos gestionados de acuerdo con los requerimientos del gestor, y retransmiten mensajes emitidos por los objetos gestionados hacia el gestor (Ver figura 2.11). El agente responde a las directivas enviadas por el gestor que se accede a la Base de Información de

Gestión (MIB) para manipular los objetos involucrados en la operación. El agente se encuentra ubicado en el dispositivo de red gestionado.

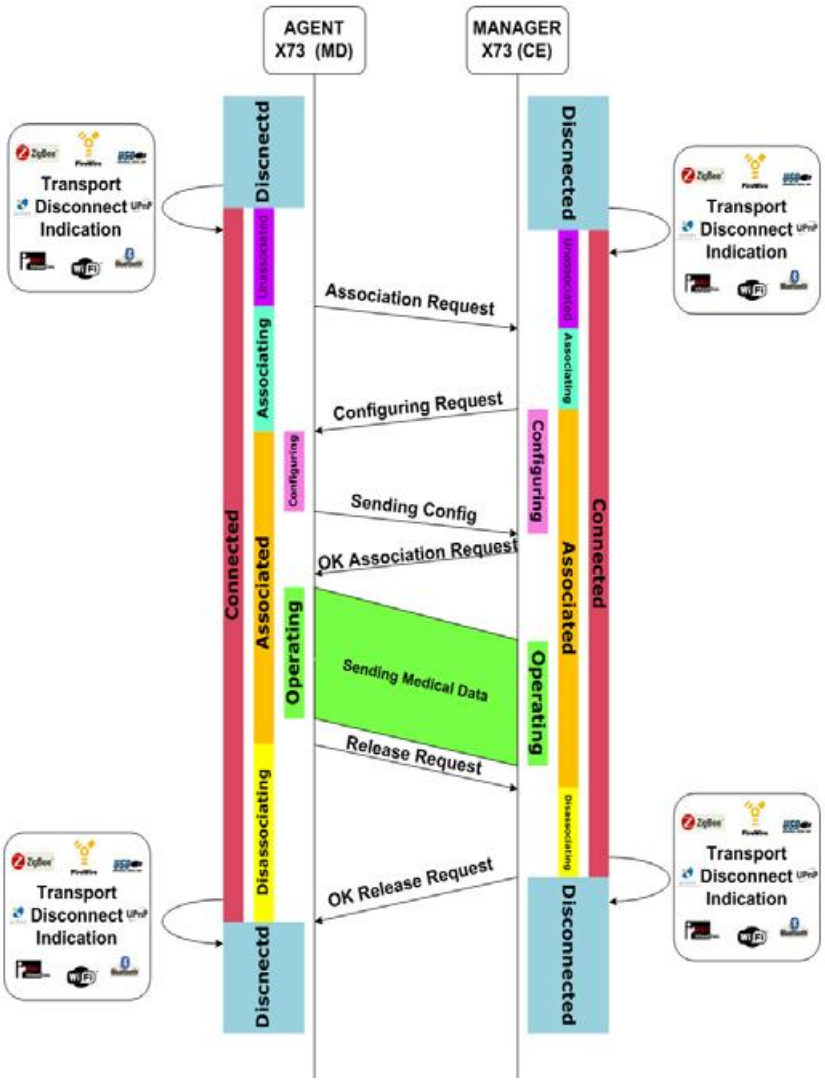



Figura 2. 11: Comunicación Gestor – Agente
Fuente: (Martínez et al., 2010)

La relación entre el gestor y el agente se puede comparar a la que existe dentro de un sistema cliente/servidor. La comunicación entre un gestor y agente se da de forma asimétrica como se puede ver en la figura 2.12. El agente de gestión es el componente de software que le permite al elemento de red realizar su rol de agente.

El elemento de red puede tener varios agentes de gestión (ver figura 2.12) a pesar de que desempeñe un solo rol como agente, ya que de esta manera permite a los agentes de gestión poder servir a funciones diferentes. Los agentes se componen de la siguiente manera (véase la figura 2.13).

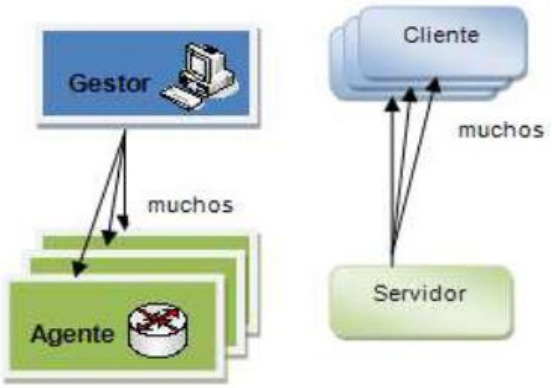



Figura 2. 12: Comparación de Agente vs Cliente
Fuente: (Olga, 2009)

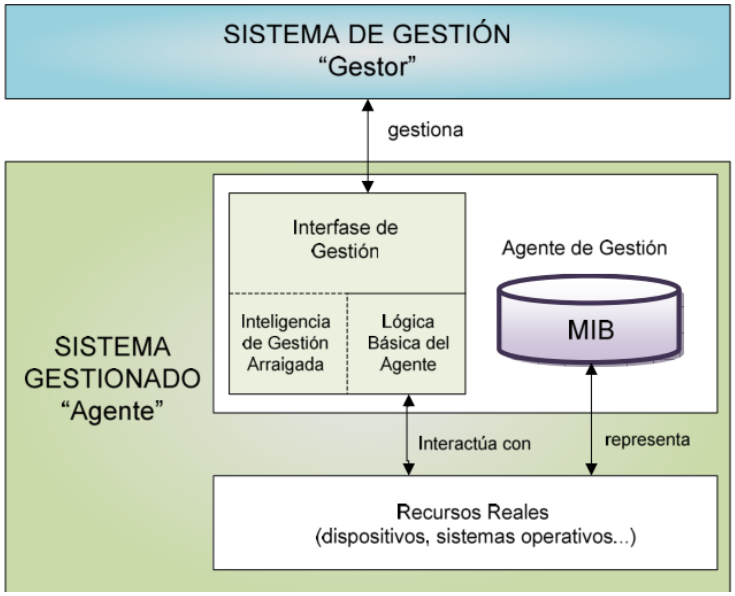



Figura 2. 13: Componente de un agente de gestión.
Fuente: (Olga, 2009)

La Interface de Gestión, que es la encargada de manejar las comunicaciones de gestión, la cual soporta los protocolos de gestión para permitir la comunicación entre el agente y la aplicación de gestión. *La Base de Gestión de Información (MIB)*, que es donde se almacenan datos de manera conceptual, que representan la información desde el punto de vista de gestión. No se debe confundir una MIB con una base de datos real. La MIB es la información del dispositivo a la que se accede a través del protocolo de gestión. *La lógica básica del Agente*, que es la que realiza la traducción entre la operación de la interface de gestión, la MIB y el dispositivo actual gestionado. Además de estas funciones básicas, el agente lógico puede incluir

funciones adicionales y realizar un procesamiento requerido por aplicaciones de gestión, a lo que se le denomina “Embedded Management Intelligence”.

### 2.3.4. Gestor de red PRTG (Paessler Router Traffic Grapher)

El PRTG Network Monitoring es una plataforma que ayuda en la administración y gestión de redes WAN, LAN, HTTP, cuyas funcionalidades sean convergentes, para todo tipo de elementos que desee monitorear. En la figura 2.14 muestra que el PRTG sostiene una arquitectura cliente –servidor en la que el Web Server es imperceptible al usuario, lo que hace que la configuración para cada nuevo elemento solo debe registrar la IP bajo el dominio de la empresa que usa y a la vez, de manera intra-office, segmentar a nivel de MPLS mediante las VLAN previamente asignadas.

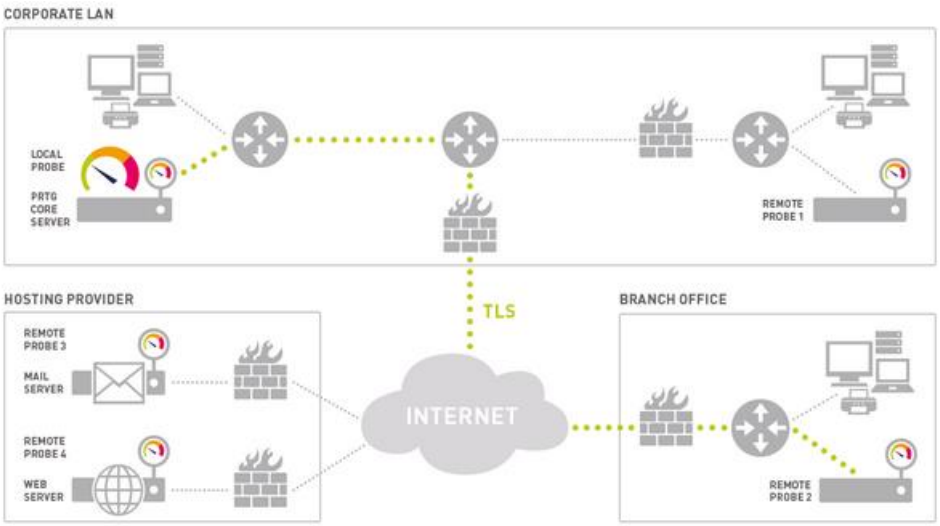



Figura 2. 14: Esquema general del PRTG
Fuente: (Paessler, 2019)

El software es fácil de configurar y usar y monitorea una red usando Simple Network Protocolo de administración (SNMP), Instrumental de administración de Windows (WMI), sniffer de paquetes, Cisco NetFlow (así como sFlow y jFlow) y muchos otros protocolos estándar de la industria. Se ejecuta en una máquina basada en Windows en su red las 24 horas todos los días. PRTG Network Monitor registra constantemente los parámetros de uso de la red y la disponibilidad de los sistemas de red. Los datos grabados se almacenan en una base de datos interna para su posterior análisis (Paessler PRTG Network Monitor 9 Guide Manual, 2016).

El PRTG utiliza una interfaz gráfica a nivel web, en cuya configuración inicial y a la vez, los subsecuentes, se agregan etiquetas por cada objeto a gestionar. No sólo puede nombrar objetos, sino también definir etiquetas en la configuración de un objeto para marcar un objeto como miembro de ciertas categorías.

Aunque hay etiquetas predefinidas al agregar objetos, existe también de manera libre de la forma en que agrega etiquetas. Por ejemplo, puede marcar todos los sensores de ancho de banda que son especialmente importantes para usted con una etiqueta bandwidth_important. Más tarde, puede ver listas de objetos con ciertas etiquetas o elegir sensores por etiqueta al crear informes. Una disposición inteligente de las etiquetas ahorra mucho tiempo (Paessler PRTG Network Monitor 9 Guide Manual, 2016)

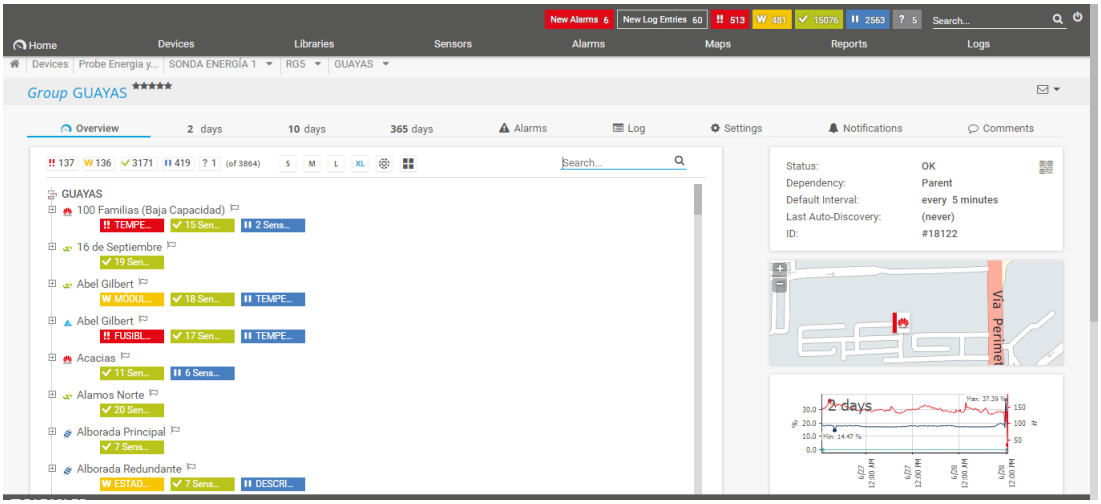



Figura 2. 15: Interfaz general del PRTG
Elaborado por: Autor

Las etiquetas en la configuración de un objeto se heredan automáticamente a todos los demás objetos abajo en la jerarquía. Entonces, por ejemplo, un dispositivo con la etiqueta Bucay hereda de forma automática e invisible esta etiqueta a todos los sensores creados en ella. Esto no será visible en la configuración de etiquetas del sensor, pero los sensores aparecerán en la lista cada vez que busque Bucay (véase la figura 2.15). Esto es útil, por ejemplo, cuando se agregan sensores por etiqueta en la configuración de informes.

De esta forma, para configurar su configuración para buscar todos los sensores en un dispositivo por etiqueta, no tiene que etiquetar todos los sensores, pero es suficiente para etiquetar el dispositivo. La herencia de las etiquetas no se puede deshabilitar.

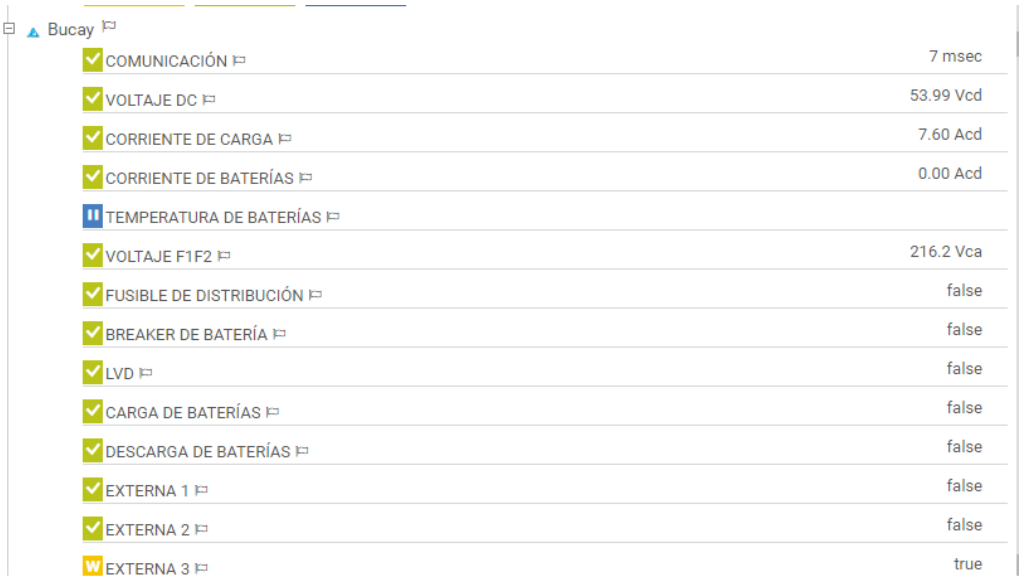



Figura 2. 16: Etiquetas de sensores
Elaborado por: Autor

### 2.3.5. SNMP

SNMP (Protocolo Simple de Administración de Red) es parte de la variedad de protocolos que presenta la Arquitectura TCP/IP. SNMP basa su funcionamiento sobre UDP, es decir, un protocolo no orientado a conexión. Por esta razón, cada intercambio de información entre la estación de gestión y el agente, es una operación diferente (Olga, 2009).

La arquitectura SNMP está conformada por un modelo de comunicación administrador-agente. Un sistema de gestión típico basado en SNMP consta de un administrador, un elemento gestionado y un conjunto de mensajes de protocolo SNMP. El elemento gestionado contiene el agente SNMP con los objetos gestionados. En su comunicación, el administrador y el agente SNMP se refieren a la MIB para intercambiar datos definidos. Como se mencionó anteriormente, el administrador y el agente se comunican a través de mensajes específicos proporcionados por el protocolo SNMP. A través de este tipo de comunicación, el agente proporciona una interfaz para que el

administrador llegue a los objetos administrados. Por otro lado, proporciona una interfaz para que el administrador de la red humana llegue al sistema de gestión, tal como se muestra en la figura 2.17.

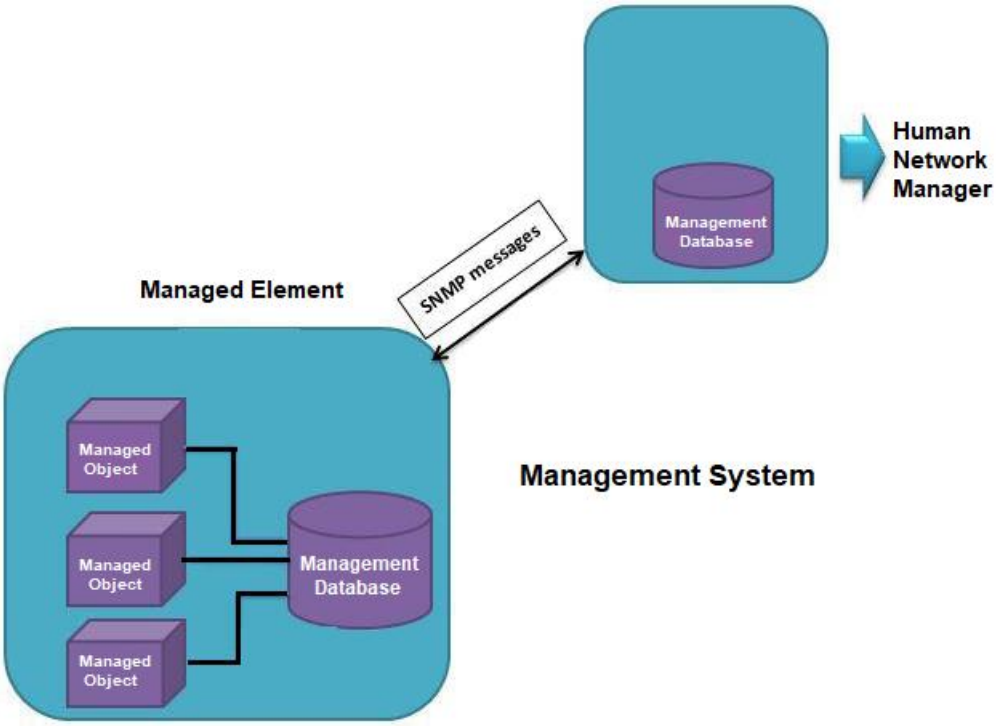



Figura 2. 17: Sistema de gestión SNMP
Fuente: (Dalibalta, 2015)

El protocolo SNMP es "simple" (pero no necesariamente su implementación) ya que contiene solo algunas operaciones importantes que se muestran en la tabla 2.1.

Tabla 2. 1: Tipos de mensajes SNMP

| Mensaje SNMP | Descripción |
|---|---|
| GET | Recuperar datos de un nodo de red |
| GETNEXT | Recuperar el siguiente elemento de un nodo de red |
| SET | Enviar comandos de configuración o control a un nodo de red |
| TRAP | Un nodo de red puede enviar una notificación a la estación de administración. |
| INFORM | Una trampa reconocida (los nodos de red pueden intentar enviarla nuevamente si no se recibe reconocimiento) |

Fuente: (Dalibalta, 2015)

Este protocolo usa un tipo de mensajes relevantes que se puede identificar en la figura 2.18.

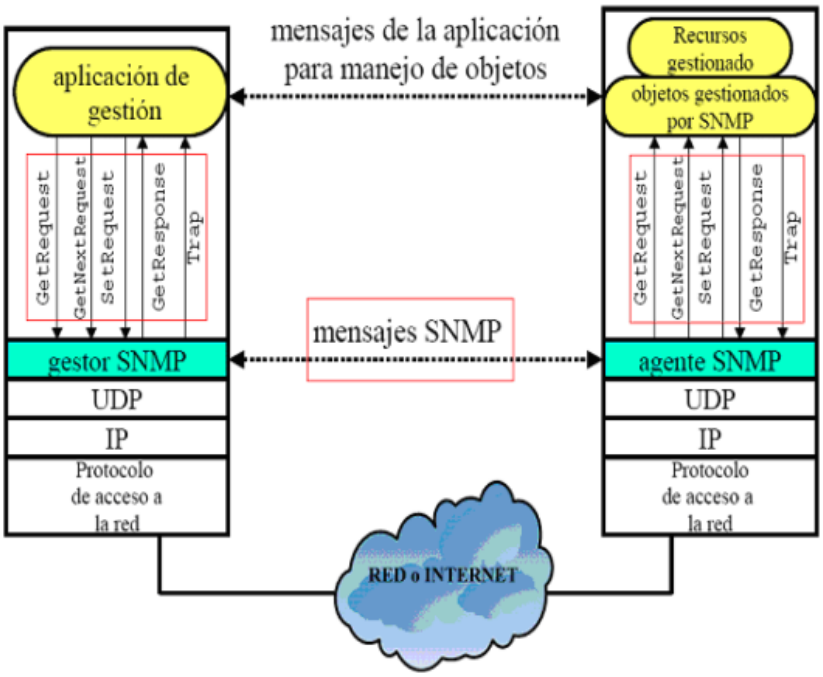



Figura 2. 18: Mensajería usando SNMP
Fuente: (Olga, 2009)

Una red SNMP generalmente consta de entidades SNMP, cada una de las cuales consta de uno o más agentes SNMP y uno o más administradores SNMP (aunque una entidad puede comprender tanto un agente como un administrador) que se comunican mediante mensajes SNMP. Un administrador SNMP (o NMS (estación de administración de red)) es responsable de administrar uno o más agentes SNMP dentro del dominio del administrador SNMP. Se incluye un agente SNMP en cada nodo (o host) de la red (por ejemplo, computadora, servidor, etc.) que es administrado por un administrador SNMP. Cada agente recopila datos sobre el nodo administrado respectivo y proporciona la información adecuada al administrador SNMP designado. (Maceda Dal-re, 2016)

El agente envía la información adecuada (configuración, parámetros ... etc.) Como respuesta a las solicitudes de su gerente. Cada agente SNMP mantiene una MIB local donde almacena todos los datos recopilados sobre el nodo administrado y su entorno. En el caso de mantener una colección de

objetos gestionados dentro de un elemento gestionado, el agente SNMP puede almacenar todos los datos recopilados en forma de módulos MIB.

### 2.3.6. Tipos de mensajes en SNMP.

Existen dos tipos de mensajes en SNMP: (1) manager-to-agent (administrador a agente), y (2) agent-to-manager (agente a administrador). Los mensajes de administrador a agente son solicitudes enviadas desde una estación de administración de red a un elemento de red, por ejemplo, “GetRequest”, para recuperar el valor de una variable o una lista. de valores y “SetRequest” para cambiar el valor de una variable o una lista de valores. Los mensajes de agente a administrador suelen ser respuestas a la estación de administración de la red desde un elemento de la red, como respuestas a los mensajes GetRequest y SetRequest, pero también pueden ser mensajes asincrónicos en segundo plano.

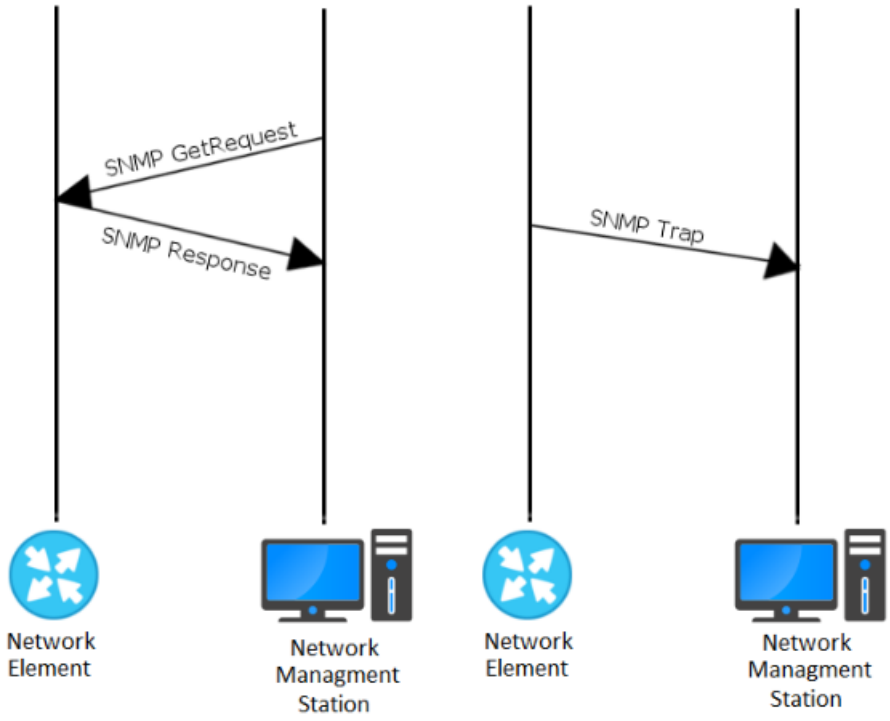



Figura 2. 19: Ejemplo de solicitud/respuesta SNMP a la izquierda y un ejemplo de trampa a la derecha.
Fuente: (Hajdarevic, 2018)

En la figura 2.19 se muestran los mensajes de trampa, es decir, aquellos mensajes no solicitados enviados por un agente de administración en un elemento de red a una estación de administración de red para indicar a la

estación de administración de red la ocurrencia de eventos significativos, por ejemplo, “linkDown” para notificar a la estación de administración de red que un enlace de red caído (no funciona). Para reducir el ancho de banda utilizado por las trampas, solo se envía un identificador de objeto *(Object IDentifier, OID)* a la estación de administración de red. La estación de administración de red luego empareja este OID con un OID en una Base de información de administración (MIB) que tiene una descripción detallada de este OID de trampa. (Boyko et al., 2019)

SNMP versión 1 (SNMPv1) carece de algunas características importantes, principalmente algunas funciones faltantes y una falta casi total de seguridad. Los contadores para el seguimiento de la actividad tienen solo 32 bits de longitud, lo que limita algunas de las funciones. Por ejemplo, una interfaz Ethernet de 1 Gbps puede envolver un contador “ifInOctets*” de 32 bits en 34 s, por lo que, si el contador se consulta a intervalos de un minuto, mostrará datos engañosos. (Nariman et al., 2018)

SNMPv1 no es confiable cuando se opera sobre el protocolo de datagramas de usuario *(User Datagram Protocol, UDP)*, ya que la entrega no está asegurada y los paquetes descartados no se informan, por lo que no hay garantía de que las trampas lleguen a su destino ni de que se devuelva la información solicitada. Además, todas las unidades de datos del protocolo SNMP (PDU) entre nodos se envían en texto sin cifrar, lo que en la práctica no proporciona ninguna seguridad. (Fanggidae et al., 2019)

SNMP versión 2 (SNMPv2) aborda el problema de los contadores de 32 bits mediante la implementación de contadores de 64 bits. También aborda el problema de la poca confiabilidad implementando un nuevo tipo de mensaje: solicitudes de información (inform requests). Las solicitudes de información son idénticas a las trampas, pero la estación de administración de red reconoce la recepción del elemento de red de la solicitud de información, lo que asegura a la fuente que esta PDU ha llegado; de lo contrario, el dispositivo intentará transmitir la solicitud de información nuevamente. (Zhang et al., 2020)

SNMPv2 se dividió más tarde en varios subprotocolos: comunidad SNMP versión 2 (SNMPv2c), SNMP versión 2 basada en el partido (SNMPv2p) y SNMP versión 2 basada en el usuario (SNMPv2u), donde cada uno se centra en un enfoque diferente. (Chun, 2019)

Por último, se lanzó una versión 3 de SNMP "reunida" (SNMPv3) (véase la figura 2.20) que fusiona las funciones de los subprotocolos anteriores en un solo protocolo y mejora la seguridad al agregar cifrado y autenticación. (Arribas A., 2012)

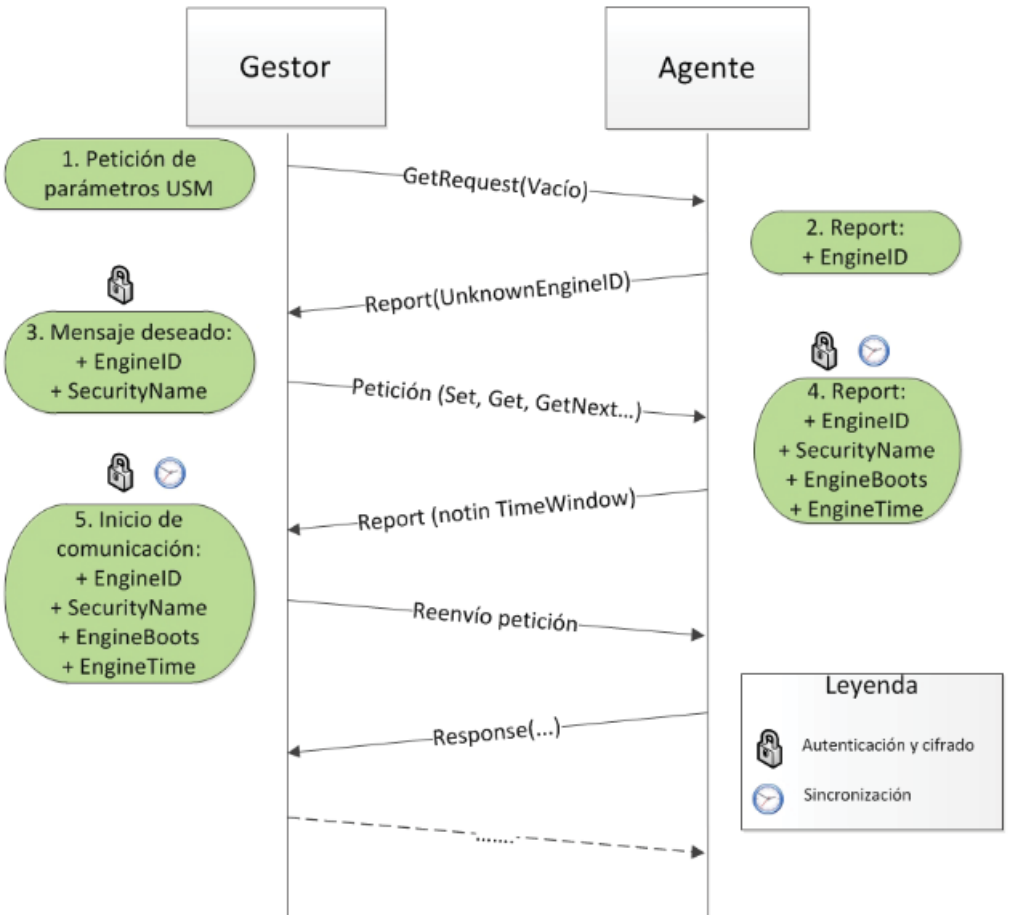



Figura 2. 20: Ejemplo de solicitud/respuesta SNMPv3.
Fuente: (Arribas A., 2012)

## Capítulo 3. Diseño de Red para la Gestión de Sistemas Eléctricos.

En este capítulo se presenta el diseño para gestionar los elementos de los sistemas de energía en una red de telecomunicaciones, considerando que la red es hibrida por efecto de análisis de la comunicación hacia el gestor PRTG.

### 3.1. Fase de planificación.

La fase de planificación del proyecto se crearon las especificaciones de requisitos de seguridad. Con base en estos requisitos, se realizó la planificación de un nuevo segmento de red, así como el nuevo hardware del servidor y el software de monitoreo.

#### 3.1.1. Especificaciones de requisitos

Este proyecto de titulación inició con las especificaciones de requisitos de seguridad. Los requisitos se dividieron en tres grupos diferentes, tal como se muestra en las tablas 3.1, 3.2 y 3.3.

Tabla 3. 1: Funciones de software requeridas.

| Referencia | Descripción | Prioridad |
|---|---|---|
| F1 | Detección de fallos de hardware | 1 |
| F2 | Leer estado del sistema de máquina virtual | 2 |
| F3 | Recopilar el estado del sistema de hardware (ON/OFF) | 2 |
| F4 | Informes básicos | 2 |
| F5 | Alerta al operador de PRTG sobre fallas de HW/SW/red | 3 |
| F6 | Monitoreo/Syslog/SNMP | 2 |
| F7 | Monitoreo de Hardware (CPU, RAM, temp, RAID) | 2 |
| F8 | Monitoreo UPS (Eaton) | 2 |
| F9 | Monitoreo de Puerto iDRAC | 3 |

Elaborado por: Autor

Tabla 3. 2: Referencias de interconexión del sistema con otros sistemas y entornos.

| Referencia | Descripción | Prioridad |
|---|---|---|
| I1 | Interfaz Web / Software GUI | 1 |
| I2 | Acceso remoto al software de monitoreo del sistema. | 1 |
| I3 | Interfaz con el sistema de monitoreo del cliente | 3 |

Elaborado por: Autor

Tabla 3. 3: Otras características requeridas del software de monitoreo seleccionado.

| Características | Descripción | Prioridad |
|---|---|---|
| Usabilidad | La interfaz gráfica de usuario (GUI) debe ser fácil de operar | 2 |
| Seguridad | Solo personal autorizado puede operar el sistema | 1 |
| Precio | Opciones de precios razonables / prueba gratuita | 2 |
| Detección de errores | El operador de PRTG puede detectar errores de hardware fácilmente | 1 |
| Segmento | Nuevo segmento de red para la PRTG | 1 |
| Hardware | Nuevo hardware para el sistema de monitoreo (servidor) | 1 |
| Red | Monitoreo de tráfico de red (SNMP/NetFlow ...) | 2 |
| Escalabilidad | Opción para extender el monitoreo a un nivel superior | 3 |
| Parches del Software | Opción para actualizar remotamente | 2 |

Elaborado por: Autor

### 3.1.2. Software

PRTG como monitoreo de red fue seleccionado para realizar pruebas en función de estos requisitos y la compatibilidad que PRTG tiene con los

dispositivos de red ya existentes en las estaciones. También se consideraron otras opciones de software, pero se descartaron en el proceso de prueba de PRTG debido a las excelentes propiedades de la PRTG. Como el entorno predeterminado de la PRTG utilizada en este trabajo de titulación ya está en producción, no se requirió ninguna otra planificación con respecto al hardware o software utilizado en las fases de tanto de prueba como de la implementación.

### 3.1.3. Red.

La planificación de un nuevo segmento de red para el software de monitoreo se realizó en colaboración con la empresa de telecomunicaciones CNT. Esto también requirió la planificación de nuevas reglas de seguridad firewall, asignaciones de puertos y rutas para aplicar en la configuración de Fortigate (es un dispositivo de seguridad como firewalls, prevención de intrusiones, filtrado web, entre otras), tal como se muestran en las figuras 3.1 y 3.2.

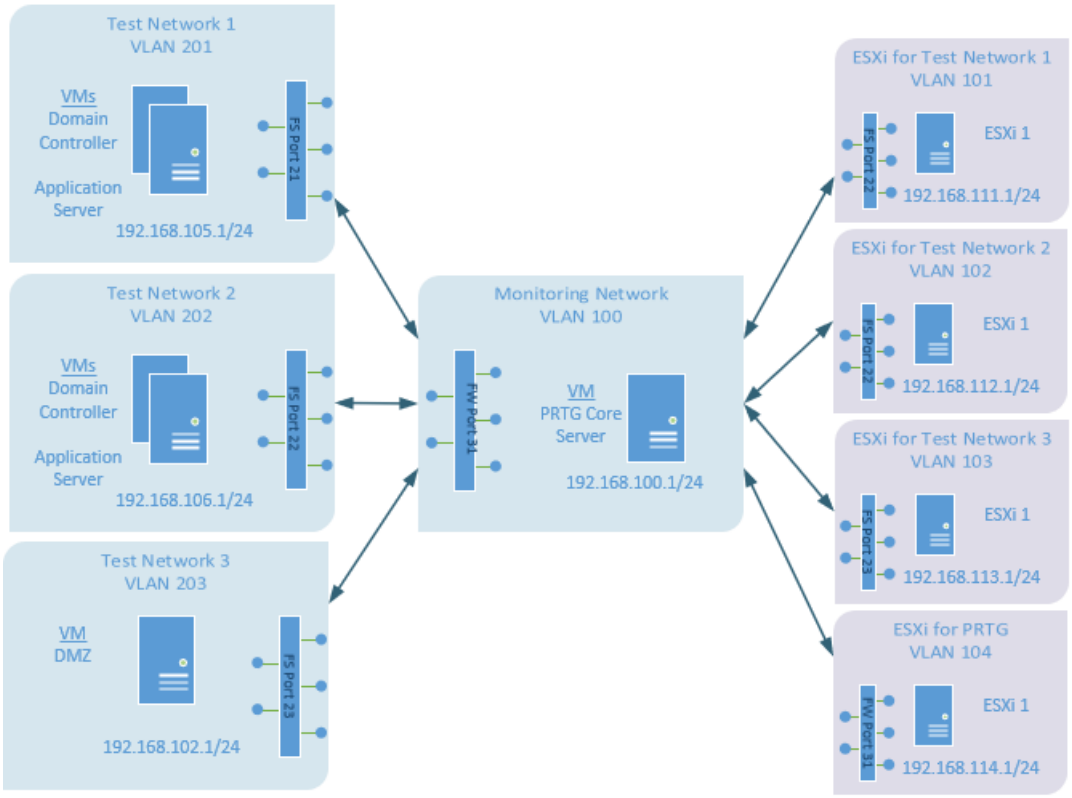



Figura 3. 1: Segmentos de red y rutas creadas en la configuración de Fortigate.
Elaborado por: Autor.

Es importante indicar que las direcciones IP y las ID de VLAN utilizadas en este documento no se correlacionan con las utilizadas en la empresa por cuestiones de seguridad.

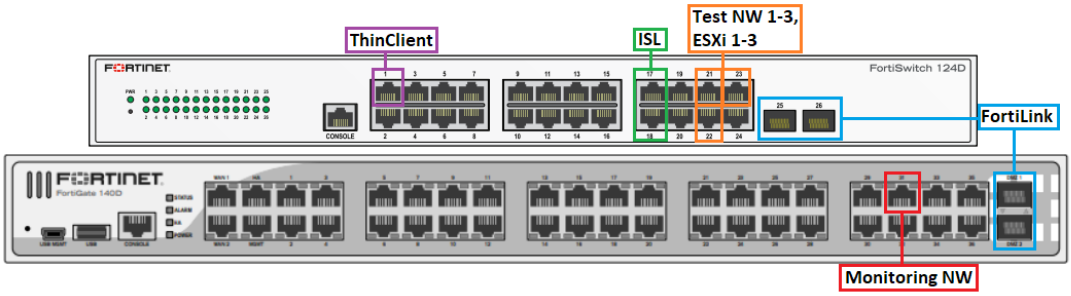



Figura 3. 2: Asignaciones de puertos Fortigate y Fortiswitch.
Elaborado por: Autor

### 3.1.4. Hardware

CNT decidirá el hardware utilizado en el futuro para el servidor central PRTG en el entorno de monitoreo de red, ya que aún no forma parte del software predeterminado. En este trabajo de titulación, el servidor central se instaló en un servidor de escritorio Dell T640 (véase la figura 3.3) que ejecuta el sistema operativo Windows Server2019 R2 de 64 bits.

Figura 3. 3: Servidor Dell PowerEdge T640.
Elaborado por: Autor

## 3.2. Fase de implementación.

Para probar la solución de monitoreo de red con éxito, se tuvo que configurar una versión de prueba de la configuración de sWOIS utilizando los

componentes y dispositivos explicados en esta sección. En las siguientes subsecciones se detallan los procesos de la fase de implementación.

### 3.2.1. Requerimientos del Hardware.

En la tabla 3.4 se enumera todo el hardware utilizado en el entorno de prueba, excepto los cables de red.

Tabla 3. 4: Componentes del Hardware.

| Dispositivos | Sistema Operativo | Información adicional |
|---|---|---|
| Fortigate 140D Firewall | FortiOS 5.4, build1138 | 2x firewalls en HA clúster |
| Fortiswitch 124D | S124DN-v3.6.2-build382 | 2x Switches en ISL |
| Dell PowerEdge T630 | Windows Server2019 R2 | ESXi, PRTG Core Server |
| Dell PowerEdge R430 | Windows Server2019 R2 | ESXi, Test Network 1 |
| Dell PowerEdge R430 | Windows Server2019 R2 | ESXi, Test Network 2 |
| Dell PowerEdge R420xr | Windows Server2019 R2 | ESXi, Test Network 3 |
| HP Z440 | Windows 10 | Management PC |

Elaborado por: Autor

### 3.2.2. Dispositivo firewall Fortigate 140D.

El componente principal de la red en sWOIS es el firewall Fortigate 140D (véase la figura 3.4), que se utiliza para crear políticas de firewall entre segmentos de red para enrutar el tráfico de red y también bloquea y registra cualquier conexión no autorizada. El firewall se puede configurar mediante una interfaz gráfica de usuario *(Graphical User Interface, GUI)*, una interfaz de línea de comandos *(Command Line Interface, CLI)* o un software FortiExplorer conectándose al puerto USB del dispositivo. Aunque, en el presente trabajo de titulación se utiliza solo una GUI.

Figura 3. 4: Dispositivo firewall Fortigate.
Elaborado por: Autor

### 3.2.3. Clúster de alta disponibilidad de Fortigate.

Utilizando dos de estos firewalls, forman un clúster de alta disponibilidad (High-Availability, HA) para mejorar la confiabilidad de la red. El propósito principal de utilizar un clúster HA es la redundancia; si un firewall funciona mal o se reinicia, el otro firewall tomará su lugar sin causar ningún tiempo de inactividad en la red. Los dos cortafuegos funcionan en modo activo-pasivo, lo que significa que solo uno de los cortafuegos está enrutando activamente el tráfico de red mientras que el otro permanece inactivo.

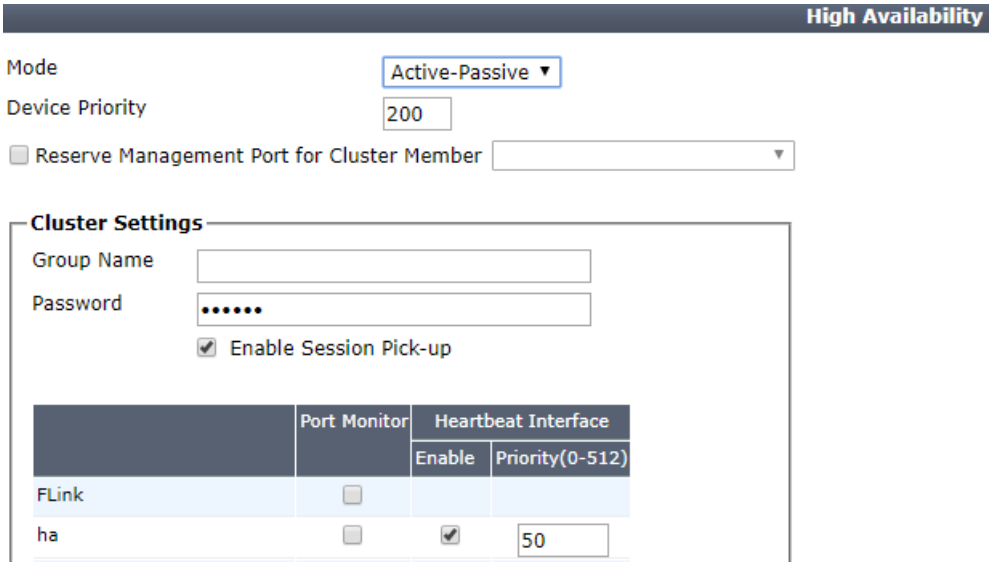



Figura 3. 5: Configuración de cluster de alta disponibilidad para Fortigate.
Elaborado por: Autor

Para formar el clúster HA, los firewalls se vinculan mediante un cable Ethernet RJ-45 en sus puertos HA y la configuración del clúster se establece en ambos firewalls (Nombre de grupo, Contraseña y Prioridad del dispositivo).

En esta configuración, los puertos HA también se configuran como interfaces heartbeat en la configuración de Fortigate, tal como se muestra en la figura 3.5.

La interfaz de heartbeat se utiliza entre los dos firewalls para sondearse entre sí: si el firewall activo deja de responder a la unidad en espera, sus funciones se cambian sin causar ningún tiempo de inactividad significativo. También es posible agregar más de una interfaz heartbeat si es necesario, pero esta configuración no utiliza ningún puerto adicional para la supervisión de HA. Una vez que se ha editado la configuración y se ha conectado el cable HA, Fortigate formará automáticamente el clúster HA a través del Protocolo de agrupación de Fortigate (FGCP)/7/. En la figura 3.6 se muestra la información del sistema Fortigate con un clúster HA sincronizado.

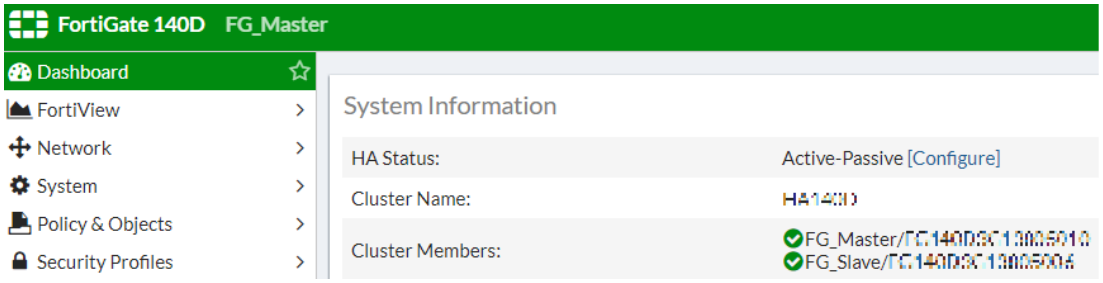



Figura 3. 6: Cluster de alta disponibilidad de Fortigate creado con éxito.
Elaborado por: Autor

### 3.2.4. Interfaces de red Fortigate.

Cada dispositivo o subred requiere su propia interfaz de red en el firewall Fortigate o Fortiswitch. Un puerto físico en el firewall o conmutador puede contener múltiples interfaces lógicas o subredes. En la Figura 15 se muestra una descripción general de las interfaces de red en la interfaz gráfica de usuario de Fortigate.

Como la empresa de telecomunicaciones utiliza estas interfaces y direcciones IP en producción, no se agregarán a este documento en su totalidad. En la tabla 3.5 define las direcciones IP y los segmentos de red utilizados en este trabajo de titulación (con las IP y las ID de VLAN modificadas).

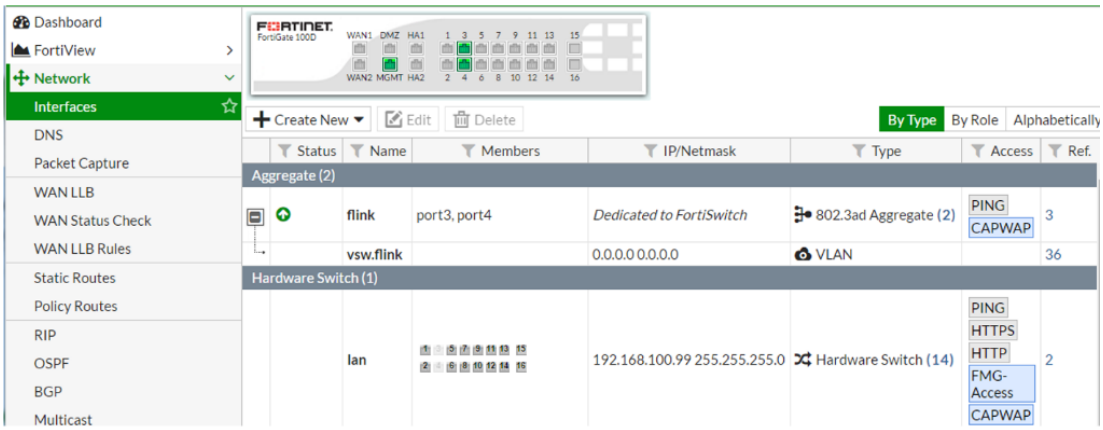



Figura 3. 7: Configuración de las interfaces de red para Fortigate.
Elaborado por: Autor

Tabla 3. 5: Direcciones IP y segmentos de red utilizados en la implementación.

| | | | |
|---|---|---|---|
| Monitoreo NW | 181.112.90.1/24 | 100 | Servidor central PRTG |
| Test NW 1 | 181.112.95.1/24 | 201 | 2 VMs, IIS |
| Test NW 2 | 181.112.96.1/24 | 202 | 2 VMs, IIS |
| Test NW 3 | 181.112.92.1/24 | 203 | DMZ VM |
| Administración NW | 181.112.144.1/24 | 110 | Administración - PC |
| ESXi 1 | 181.112.101.1/24 | 101 | ESXi para Test NW1 |
| ESXi 2 | 181.112.102.1/24 | 102 | ESXi para Test NW2 |
| ESXi 3 | 181.112.103.1/24 | 103 | ESXi para Test NW3 |
| ESXi 4 | 181.112.104.1/24 | 104 | ESXi para PRTG |
| InTouch NW | 181.112.190.1/24 | 200 | ThinClient |

Elaborado por: Autor

Todas las interfaces se crean con la interfaz gráfica de usuario de Fortigate. Los administradores del sistema pueden crear o modificar las interfaces, tal como se muestra en la figura 3.8.

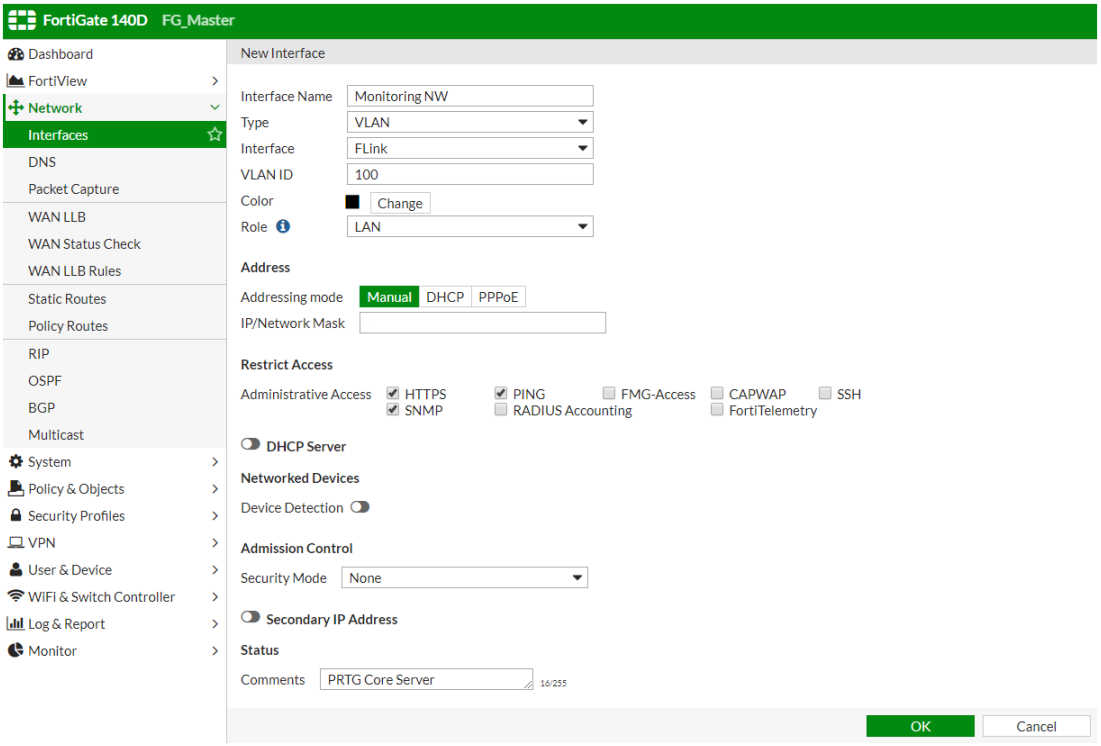



Figura 3. 8: Configuración de creación de una nueva interfaz GUI para Fortigate.
Elaborado por: Autor

### 3.2.5. Políticas de Fortigate Firewall.

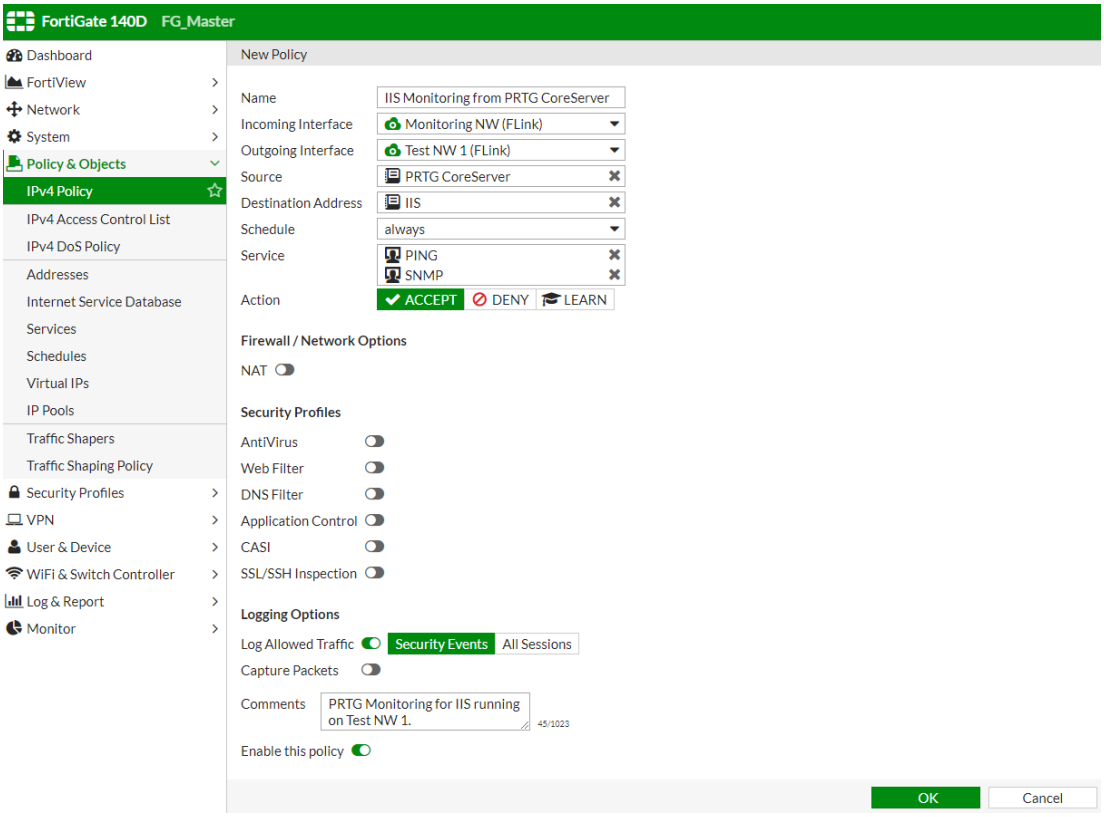



Figura 3. 9: Configuración de política de firewalls para supervisión de IIS.
Elaborado por: Autor

Las políticas de firewall se utilizan para enrutar el tráfico entre segmentos de red y es la función principal del firewall de Fortigate. Esto también permite a los administradores de red especificar los protocolos, la VLAN o los servicios que pueden pasar a través de la red. En la figura 3.9 se muestra la configuración de la creación de políticas de firewalls.

En la figura 3.10 se muestran los procesos de las políticas de firewall en las redes.


Figura 3. 10: El principio de una política de firewall.
Elaborado por: Autor

### 3.2.6. Configuración de Fortigate SNMP, NetFlow y Syslog

Además de las políticas de firewall, para habilitar SNMP, la comunidad SNMP v2c debe configurarse en Fortigate. La configuración utilizada se muestra en la figura 3.11.

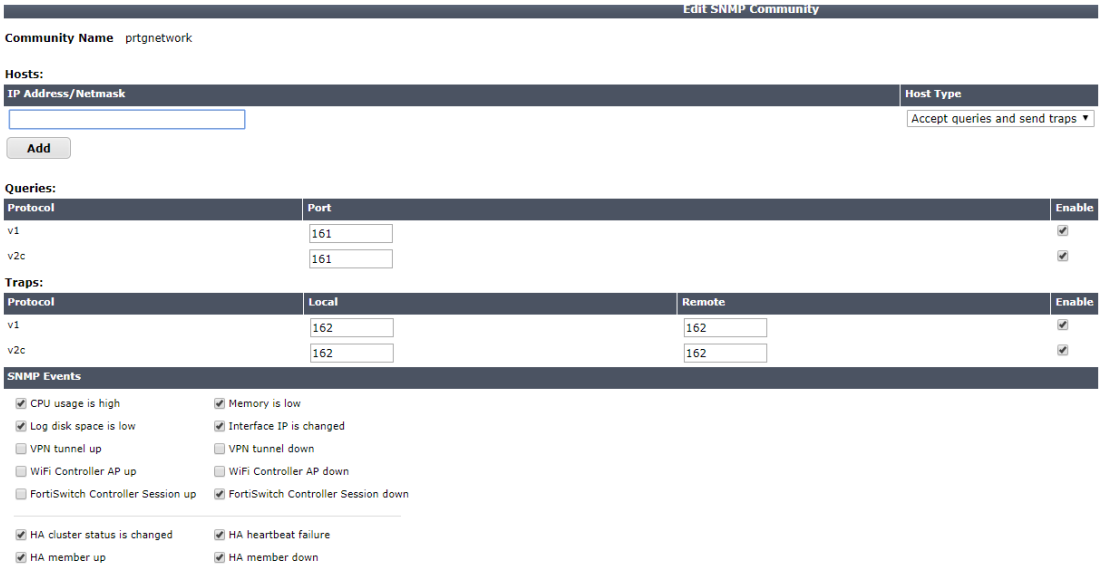



Figura 3. 11: Configuración de la comunidad Fortigate SNMP.
Elaborado por: Autor

Para permitir la comunicación en la red entre dispositivos, se aplican las siguientes configuraciones:

- Dirección IP / máscara de red
  - Esta es la IP del servidor central PRTG

- Puerto de protocolo
  - El puerto 161 se utiliza en todos los dispositivos de red para comunicarse mediante SNMP

- Eventos SNMP
  - Eventos varios de Fortigate se envían a PRTG

NetFlow es una función que proporciona la capacidad de recopilar tráfico de red IP cuando entra o sale de una interfaz/23/. En PRTG, este tráfico se puede visualizar para determinar la fuente y el destino del tráfico, el tipo de servicio y las causas de la congestión. Para habilitar esta función en Fortigate, la configuración debe realizarse para cada interfaz individualmente utilizando la CLI.

La información de NetFlow se exporta desde el dispositivo fuente mediante el protocolo de datagramas de usuario *(User Datagram Protocolo, UDP)* y se recoge mediante un recopilador (en este caso, PRTG). El dispositivo emisor es el cortafuegos Fortigate, que utiliza el puerto UDP estándar NetFlow 2055. Los comandos CLI utilizados para habilitar la función NetFlow en Fortigate se enumeran a continuación:

1. Configuración de la IP del recopilador NetFlow:

```
config system netflow
set collector-ip <ipv4_addr>
set collector-port <port_int>
end
```

2. Habilitar NetFlow en la interfaz

```
config system interface
edit <interface name>
set netflow-sampler both
end
```

Syslog se agregó a este trabajo de titulación para recibir mensajes de eventos en PRTG. Syslog en sí es un protocolo utilizado por dispositivos de

red para enviar información a un servidor Syslog (en este caso, PRTG). Para permitir que Fortigate reenvíe estos mensajes, se configuró la siguiente actualización en las opciones de registro del firewall, tal como se muestra en la figura 3.12. La dirección IP del servidor Syslog es la dirección del servidor central de PRTG.

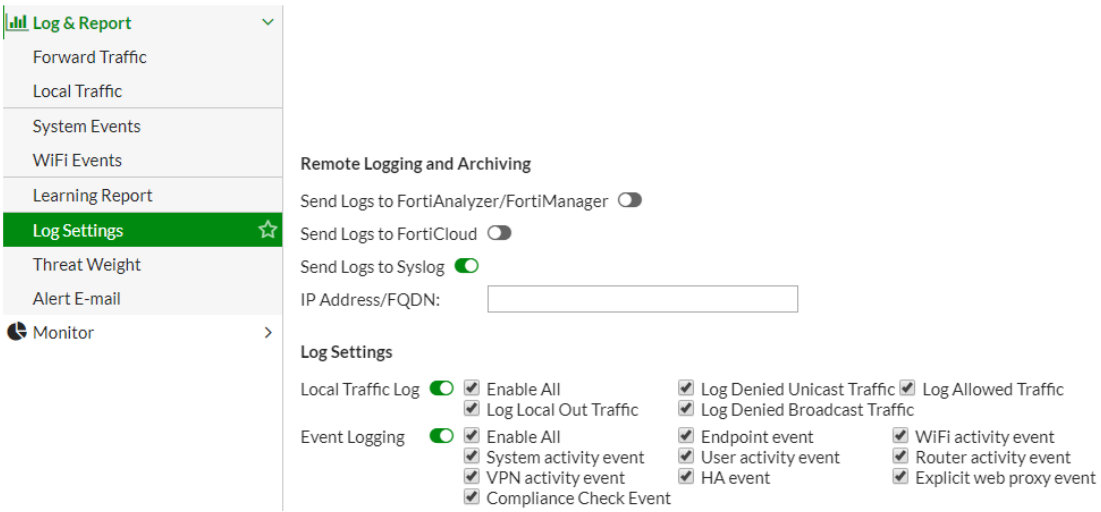



Figura 3. 12: Configuración de registros al servidor Syslog PRTG de Fortigate.
Elaborado por: Autor

### 3.2.7. Configuración de Fortiswitches.

Los dispositivos Fortiswitches (véase la figura 3.13) se utilizan en esta configuración para agregar más puertos físicos para los dispositivos conectados. En una instalación de equipos de telecomunicaciones más grande, la cantidad de puertos de red necesarios puede ser superior a 50, dependiendo de la cantidad del sistema de rectificación y sistemas auxiliares.

Aparte de la instalación física de Fortiswitch, toda la administración y configuración se realizan en la GUI de Fortigate. Los Fortiswitches tienen su propia GUI y CLI disponibles, pero no se recomienda utilizar estas funciones mientras están bajo el control remoto de Fortilink.

Figura 3. 13: Dispositivo Fortiswitch.
Elaborado por: Autor

La figura 3.14 muestra todos los puertos activos en Fortiswitches en verde, mientras que los puertos 17 y 18 son los puertos ISL interconectados.

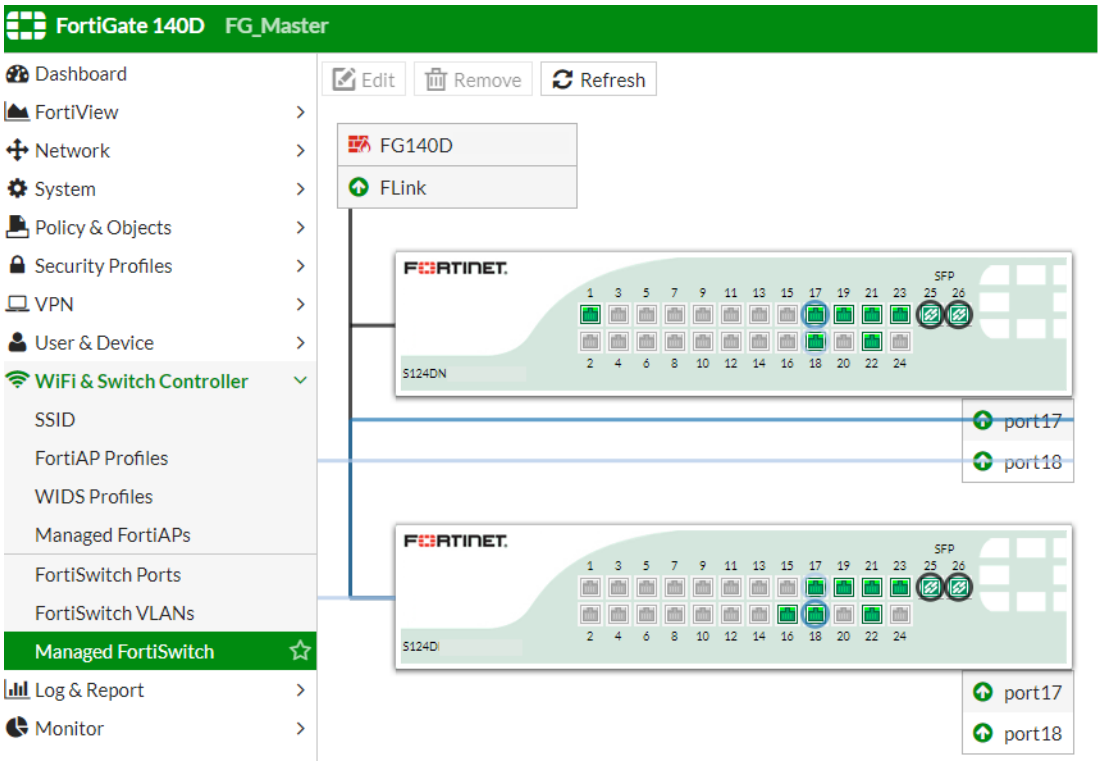



Figura 3. 14: Gestión de Fortiswitches desde la interfaz gráfica de usuario (GUI) de Fortigate.
Elaborado por: Autor

### 3.2.8. Configuración del servidor principal de PRTG

El software PRTG se instaló en un servidor Dell PowerEdge T630 que se ejecuta bajo el sistema operativo Windows Server 2019 R2 de 64 bits. El instalador de Windows está disponible en el sitio web de PRTG y no requiere ninguna configuración adicional antes o durante el procedimiento de instalación. Durante la instalación, la PRTG configura todos los componentes de software necesarios para ejecutar el software, incluido el servidor web para el acceso a la interfaz gráfica de usuario (GUI) web, la base de datos para el almacenamiento y la consola Enterprise que se utilizará como una aplicación nativa de Windows.

Una vez completada la instalación, se puede acceder a la PRTG mediante un navegador (Google Chrome 61 o posterior, Mozilla Firefox 56 o posterior o Microsoft Internet Explorer 11) desde la dirección de host local 127.0.0.1, puerto 8080, tal como se muestra en la figura 3.15.


Figura 3. 15: Acceso a la interfaz web de PRTG.
Elaborado por: Autor

Tras la instalación, el servidor central de PRTG crea una sonda local, que se utiliza para monitorear la red local. Las sondas en PRTG son los componentes que realizan el monitoreo real. En este caso, como la red no está abierta a Internet, solo se utiliza una sonda local. También es posible monitorear diferentes ubicaciones y redes utilizando un solo servidor central y múltiples sondas remotas que reportan y envían datos al servidor central. La sonda local tiene sus propios sensores integrados que se crean en la primera instalación, tal como se muestra en la figura 3.16. Estos sensores, como cualquier otro sensor de PRTG, se pueden modificar o eliminar.

Durante el primer inicio de sesión, también se solicita a los administradores del sistema que cambien las credenciales de inicio de sesión predeterminadas. Esto se vuelve más importante si el servidor central está expuesto a Internet para evitar cualquier intento de inicio de sesión no autorizado.

### 3.3. Red del Sistema Eléctrico.

Los sistemas actuales de energía tienen como elementos, algunos equipos que no poseen interfaces para poder gestionarlo remotamente.

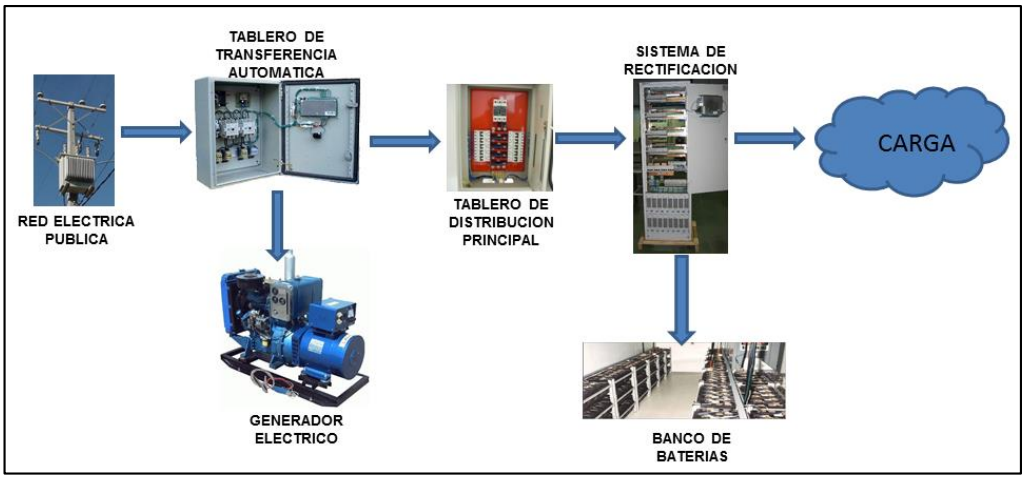



Figura 3. 16: Esquema general del sistema
Elaborado por: Autor

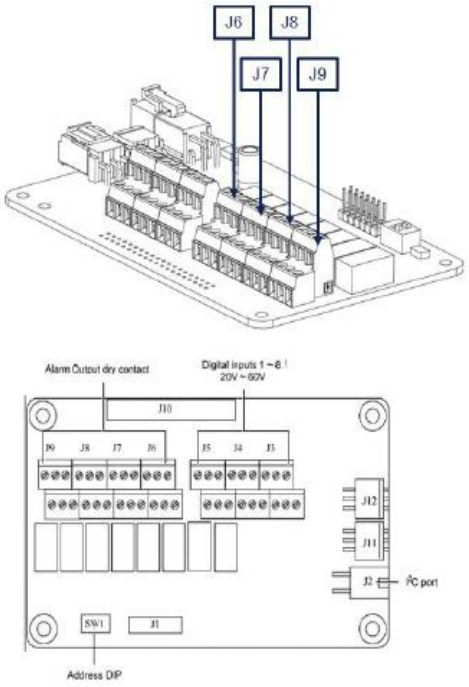
Este diseño conceptual que esta implementado desde hace varios años sin que haya sido modificado por lo que la operación y mantenimiento de los mismos deben ser atendidos en sitio. Esta atención, normalmente emergentes, implican interrupción de servicio de la carga que sostiene el sistema eléctrico.

### 3.4. Interconexión del Sistema Eléctrico hacia la gestión en el PRTG

Existen 179 sitios dentro de la ciudad de Guayaquil con equipos de telecomunicaciones que son a su vez “clientes” de los sistemas eléctricos por cada uno de eso sitios. De todos los elementos eléctricos, solo el sistema de rectificación posee las características para integrar una comunicación bidireccional de entre los demás elementos, mediante interfaz Ethernet que tienen en su módulo de control. En la figura 3.17 se muestra la estructura de dicho modulo y en la cual, están definidos cada punto terminal.

En dicho punto terminal, se encuentran los pines correspondientes para la conexión de sensores de acuerdo con el requerimiento de los elementos del sistema Eléctrico, mediante una configuración personalizada. La Figura 3.17 muestra la identificación del puerto, a su vez el número de pines sobre ese puerto y la definición (nombre) de cada pin. Los puertos J6 hasta el puerto J9 son usados para la gestión de alarmas externas.

**Tarjeta de relés**




| Port | Pin # | Pin name | Definition |
|---|---|---|---|
| J6 | 1 | DO1_NC | NC contact of relay 1 |
| | 2 | DO2_NC | NC contact of relay 2 |
| | 3 | DO1_COM | Common contact of relay 1 |
| | 4 | DO2_COM | Common contact of relay 2 |
| | 5 | DO1_NO | NO contact of relay 1 |
| | 6 | DO2_NO | NO contact of relay 2 |
| J7 | 1 | DO1_NC | NC contact of relay 3 |
| | 2 | DO2_NC | NC contact of relay 4 |
| | 3 | DO1_COM | Common contact of relay 3 |
| | 4 | DO2_COM | Common contact of relay 4 |
| | 5 | DO1_NO | NO contact of relay 3 |
| | 6 | DO2_NO | NO contact of relay 4 |
| J8 | 1 | DO1_NC | NC contact of relay 5 |
| | 2 | DO2_NC | NC contact of relay 6 |
| | 3 | DO1_COM | Common contact of relay 5 |
| | 4 | DO2_COM | Common contact of relay 6 |
| | 5 | DO1_NO | NO contact of relay 5 |
| | 6 | DO2_NO | NO contact of relay 6 |
| J9 | 1 | DO1_NC | NC contact of relay 7 |
| | 2 | DO2_NC | NC contact of relay 8 |
| | 3 | DO1_COM | Common contact of relay 7 |
| | 4 | DO2_COM | Common contact of relay 8 |
| | 5 | DO1_NO | NO contact of relay 7 |
| | 6 | DO2_NO | NO contact of relay 8 |

Figura 3. 17: Sistema de Energía Actual
Elaborado por: Autor

La conexión física es desde la interfaz del rectificador hacia la red IPMLS, es decir, se asigna un puerto ETH en el router de capa 3 bajo una ip de gestión ya definido y a la vez, definir dicha IP en el servidor del PRTG.

| Alarm Severity Levels | Red LED | Yellow LED | Alarm Buzzer | Alarm Call-back | Remark |
|---|---|---|---|---|---|
| Critical Alarm(CA) | ON | / | ON | Yes | Call-back function enabled |
| Major Alarm(MA) | ON | / | ON | Yes | Call-back function enabled |
| Observation(OA) | OFF | ON | OFF | No | / |
| No Alarm(NA) | OFF | OFF | OFF | No | / |

Figura 3. 18: Niveles de alarmas
Elaborado por: Autor

En la figura 3.18 se muestran los niveles de alarmas que normalmente están configurados en los Sistemas de Rectificación, pero solo los niveles Critical y Major, y solo pueden ser visualizados en modo local, es decir, cuando se atiende en sitio. Sin embargo, estos niveles no aplican generalmente cuando están conectados, por ejemplo, el Tablero de

Transferencia Automático, Tablero de Distribución en AC o el Generador, orientándose solo a Baterías, y Rectificadores.

| Pos | Sensor | Status | Message | Graph | Priority |
|---|---|---|---|---|---|
| 1. | COMUNICACIÓN | Up | OK | Ping Time 20 ms/sec | ★★★☆☆ |
| 2. | VOLTAJE DC | Up | OK | Value 54.5 Vcd | ★★★☆☆ |
| 3. | CORRIENTE DE CARGA | Up | OK | Value 49.0 Acd | ★★★☆☆ |
| 4. | CORRIENTE DE BATERÍAS | Up | OK | Value 0.0 Acd | ★★★☆☆ |
| 5. | TEMPEARTURA DE BATERÍAS | Up | OK | Value 20.0 °C | ★★★☆☆ |
| 6. | VOLTAJE F1F1 | Up | OK | Value 213.0 Vca | ★★★☆☆ |
| 7. | FUSIBLE DE DISTRIBUCIÓN | Up | OK | Value 0 # | ★★★☆☆ |
| 8. | BREAKER DE BATERÍAS | Up | OK | Value 0 # | ★★★☆☆ |
| 9. | LVD | Up | OK | Value 0 # | ★★★☆☆ |
| 10. | MÓDULOS RECTIFICADORES | Up | OK | Value 5 # | ★★★☆☆ |
| 11. | CARGA DE BATERÍAS | Up | OK | Value 0 # | ★★★☆☆ |
| 12. | DESCARGA DE BATERÍAS | Up | OK | Value 0 # | ★★★☆☆ |

1 to 12 of 12

Figura 3. 19: Registro de sensores en el PRTG
Elaborado por: Autor

Cada sensor es colocado en cada elemento del sistema eléctrico, lo que, a su vez, envía la señal (sea analógica o digital) hacia el rectificador que es donde se encuentra el módulo e interfaces de conexión. Cada uno de estos sensores, se registran en el PRTG por sitio, lo que se genera regularmente 12 sensores que cubren la mayor disponibilidad del fluido eléctrico mientras los demás equipos trabajan. La Figura 3.4 se muestra los nombres genéricos de cada sensor y que es común en todos los sitios. El color verde muestra que el elemento eléctrico del cual está alojado el sensor está operando normalmente (status up). A continuación, la tabla 3.6 presenta el uso de cada sensor con su respectivo nombre genérico:

Estos nombres son registrados tanto en el PRTG, así como en todas las conexiones del SNMP pasando por la IPMPLS. Por cada asignación, van precedidas por un código que actúa como flag en cada puerto ethernet en ambos extremos. Estos nombres son tal como se muestra en la tabla 3.6 en donde cada sensor es instalado acorde a la funcionalidad dentro del elemento del sistema eléctrico.

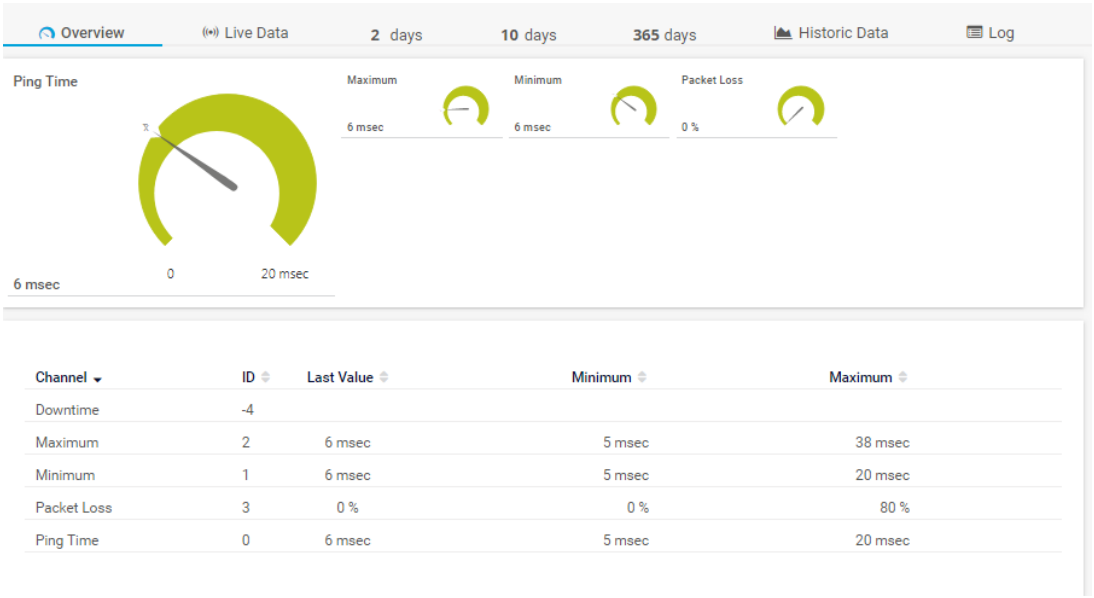
Tabla 3. 6: Nombres genéricos de los sensores en el PRTG.

| ITEM | NOMBRE GENERICO DEL SENSOR | FUNCION |
|---|---|---|
| 1 | COMUNICACIÓN | INDICADOR DEL STATUS DE CONEXIÓN SNMP DESDE EL EQUIPO DEL SISTEMA ELECTRICO HACIA EL PRTG |
| 2 | VOLTAJE DC | INDICADOR DEL STATUS DEL TABLERO DE DISTRIBUCION EN DC |
| 3 | CORRIENTE DE CARGA | INDICADOR DEL CONSUMO GENERAL DE ENERGIA DC EN AMPERIOS, SOBRE EQUIPOS. |
| 4 | CORRIENTE DE BATERIA | INDICADOR DEL STATUS DE FUNCIONALIDAD DE LOS BANCOS DE BATERIAS CON CARGAS (EN AH) |
| 5 | TEMPERATURA DE BATERIA | INDICADOR DE LA TEMPERATURA DEL BANCO DE BATERIAS CON RESPECTO AL AMBIENTE. |
| 6 | VOLTAJE F1 F2 | INDICADOR DEL STATUS DE VOTAJE EN LAS FASES DESDE EL TABLERO DE DISTRIBUCION PRINCIPAL EN AC |
| 7 | FUSIBLE DE DISTRIBUCION | INDICADOR DE PROTECION (FUSIBLES) SOBRE LAS DIFERENTES CARGAS EN DC. |
| 8 | BREAKER DE BATERIAS | SENSOR DE PROTECCION DEL BANCO DE BATERIAS. |
| 9 | LVD (Low Voltage Battery Disconnect) | INDICADOR SI EL CONTACTOR CAMBIA DE ESTADO O NO. |
| 10 | MODULOS RECTIFICADORES | INDICADOR DEL ESTADO DE CADA MODULO RECTIFICADOR. |
| 11 | CARGA DE BATERIAS | INDICADOR DEL PROCESO DE CARGA DE LAS BATERIAS PARA QUE LLEGUE A SU VALOR NORMAL DE FUNCIONAMIENTO. |
| 12 | DESCARGA DE BATERIAS | INDICADOR DE QUE LAS BATERIAS ESTN TRABAJANDO CUANDO HAY AUSENCIA DE ENERGIA ELECTRICA COMERCIAL. |

Fuente: Autor

Tal como muestra la Figura 3.20, el sensor de comunicación presenta varios ítems en la cual se puede comprobar la normalidad de los equipos reflejados en el gestor. La comunicación es vía SNMP V2, generando ping

hacia el puerto ETH en el módulo de control del rectificador mediante un Path Cord UTP hacia un puerto, asignado previamente más el direccionamiento IP, en el Switch donde están los equipos a gestionar. Además, mediante este sensor, ayuda a




| Channel | ID | Last Value | Minimum | Maximum |
|---|---|---|---|---|
| Downtime | -4 | | | |
| Maximum | 2 | 6 msec | 5 msec | 38 msec |
| Minimum | 1 | 6 msec | 5 msec | 20 msec |
| Packet Loss | 3 | 0 % | 0 % | 80 % |
| Ping Time | 0 | 6 msec | 5 msec | 20 msec |

Figura 3. 20: Sensor de comunicaciones
Fuente: Autor

# Conclusiones.

- La interfaz del PRTG es amigable, incluso para las personas que no poseen conocimiento de redes. Además, puede ser usado no solo en empresas de telecomunicaciones sino en tipo de empresas que necesiten que sus sistemas técnicos o maquinas – herramientas deban ser correctamente monitoreadas en tiempo real y 24 horas, 7 días a la semana.

- Los elementos del sistema eléctrico no necesariamente deben tener puertos de comunicación, ya que éstas se concentran en una salida desde la tarjeta I/O con puertos ethernet, generalmente desde el rectificador. No se necesita definir VLAN's en este punto sino solo desde el router MPLS con la agregación de la IP estática.

- Las conexiones SNMP desde el rectificador hacia la gestión del PRTG por medio de la red MPLS, funcionan con la asignación de IP estáticas.

- Se generan ordenes de trabajo para la optimización de los recursos de red y registro de las IP usadas, así como la asignación de VLAN's del lado de MPLS, puesto que la expansión de la red por los elementos eléctricos es ilimitada.

# Recomendaciones.

1. Los sistemas antiguos de rectificación se deben acondicionar tener relés para para que actúen a manera de direccionar estos conectarlos mediante un Patch Cord hacia puertos de la red MPLS previamente habilitados.

2. La gestión del PRTG está sujeta a actualizaciones periódicas por el fabricante por lo que se debe verificar periódicamente los atributos de licencias.

## Referencias


Arribas A., J. C. (2012). Implementación automática de un agente SNMP a partir de la definición formal de su MIB - Repositorio Institucional de Documentos [Proyecto Fin de Carrera, Universidad de Zaragoza]. https://zaguan.unizar.es/record/8769/

Boyko, A., Varkentin, V., & Polyakova, T. (2019). Advantages and Disadvantages of the Data Collection's Method Using SNMP. 2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon), 1–5. https://doi.org/10.1109/FarEastCon.2019.8934069

Candotti, K. M., & Mavares, D. T. (2012). Entorno de simulación para sistemas de comunicaciones inalámbricos de alta capacidad usando MATLAB. Universidad, Ciencia y Tecnología, 16(64), 212–217.

Chun, B.-T. (2019). A Study on Similarity Analysis of SNMP MIB File. Journal of Software Assessment and Valuation, 15(1), 37–42. https://doi.org/10.29056/jsav.2019.06.04

Cruz Felipe, M., Martínez Gómez, R., & Crespo García, Y. (2013). Análisis de la QoS en redes inalámbricas. Revista Cubana de Ciencias Informáticas, 7(1), 86–96.

Dalibalta, D. (2015). SNMP MIB for OpenFlow-Capable Switch [Thesis].

Eltek, E. (2006). User's Guide Monitoring and Control Unit: Flatpack2 DC Power Supply Systems. Smartpack.

Fanggidae, A. M., Hermawan, H., & Pratiwi, H. I. (2019). Sistem Monitoring Server Dengan Menggunakan SNMP. WIDYAKALA JOURNAL, 6(2), 163. https://doi.org/10.36262/widyakala.v6i2.218

Gross, C. A., & Roppel, T. (2012). Fundamentals of Electrical Engineering. CRC Press Taylor & Francis Group [distributor. http://proquest.safaribooksonline.com/9781439898079

Hajdarevic, K. (2018). Cyber Security Audit in Business Environments. International Burch University.

Maceda Dal-re, P. (2016). SNMP vs COAP en sistemas de distribución eléctrica [Trabajo Fin de Grado, Universidad Pontificia Comillas]. https://repositorio.comillas.edu/xmlui/handle/11531/16653

Martínez, I., del Valle, P., Muñoz, P., Trigo, J. D., Escayola, J., Martínez-Espronceda, M., Muñoz, A., Serrano, L., & García, J. (2010). Interoperable and standard e-Health solution over Bluetooth. 2010 Annual International Conference of the IEEE Engineering in Medicine and Biology, 2192–2195. https://doi.org/10.1109/IEMBS.2010.5626053

Nariman, T., Kawa, S., & Luqman, Y. (2018). SNMP Service. https://doi.org/10.13140/RG.2.2.35823.07846

Olga, R. V. P. S. D. (2009). Estudio y desarrollo de una metodología para la implementación de un modelo de gestión y administración de red para la UTEQ.

Paessler, A. G. (2019). Introduction: Monitoring with PRTG | PRTG Manual. https://www.paessler.com/manuals/prtg/introduction_monitoring_with_prtg

Raviprasad, V., Shanker, T., & Ravindra, K. (2012). Power Architectures for Telecommunications—A Review. Proc. of the Intl. Conf. on Advances in Electronics, Electrical and Computer Science Engineering, 1(1).

Schairer, K. (2018, julio 13). The Main Components of a DC Power System. Www.Qpsolutions.Net. https://www.qpsolutions.net/2018/07/dc-control-system/

SDMO. (2015). Manual de uso y mantenimiento: Grupo electrógeno—Generalidades—Instrucciones de seguridad—Instalación—Instrucciones específicas de mantenimiento. https://grupofeynsa.files.wordpress.com/2015/10/manual_grupos_sdm opt1.pdf

Zhang, W., Dong, M., Ota, K., Li, J., Yang, W., & Wu, J. (2020). A Big Data Management Architecture for Standardized IoT Based on Smart Scalable SNMP. ICC 2020 - 2020 IEEE International Conference on Communications (ICC), 1–7. https://doi.org/10.1109/ICC40277.2020.9149368

# DECLARACIÓN Y AUTORIZACIÓN

Yo, **Villalva Melgar, Francis David** con C.C: # 091551927-6 autor del trabajo de titulación: Análisis y diseño de un sistema de monitoreo para una red de equipos eléctricos en una empresa de telecomunicaciones en la ciudad de Guayaquil, previo a la obtención del título de **Magister en Telecomunicaciones** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 29 de octubre de 2020

f. _____

Nombre: **Villalva Melgar, Francis David**

C.C: 091551927-6

# REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

## FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

| | | | |
|---|---|---|---|
| **TÍTULO Y SUBTÍTULO:** | Análisis y diseño de un sistema de monitoreo para una red de equipos eléctricos en una empresa de telecomunicaciones en la ciudad de Guayaquil | | |
| **AUTOR(ES)** | Villalva Melgar, Francis David | | |
| **REVISOR(ES)/TUTOR(ES)** | M. Sc. Córdova Rivadeneira, Luis Silvio; M. Sc. Quezada Calle, Edgar Raúl / M. Sc. Palacios Meléndez, Edwin Fernando | | |
| **INSTITUCIÓN:** | Universidad Católica de Santiago de Guayaquil | | |
| **FACULTAD:** | Sistema de Posgrado | | |
| **PROGRAMA:** | Maestría en Telecomunicaciones | | |
| **TITULO OBTENIDO:** | Magister en Telecomunicaciones | | |
| **FECHA DE PUBLICACIÓN:** | Guayaquil, 29 de octubre de 2020 | **No. DE PÁGINAS:** | 66 |
| **ÁREAS TEMÁTICAS:** | Sistemas de Comunicaciones, Gestión de Redes | | |
| **PALABRAS CLAVES/ KEYWORDS:** | Gestión, Redes, PRTG, SNMP, Arquitecturas, Rectificadores | | |


RESUMEN/ABSTRACT (150-250 palabras):

Se tiene como finalidad diseñar un esquema integral para la gestión de sistemas eléctricos usando la red IP fija de telecomunicaciones en la ciudad de Guayaquil. Estos sistemas eléctricos están comprendidos en rectificadores, bancos de baterías, grupo electrógeno y tableros de distribución tanto en corriente alterna como continua, cuya finalidad es de la operación y mantenimiento oportuno sobre el equipamiento eléctrico. Esto incluye integrar eficazmente los sensores de alarmas en la red IP usando como transporte de la señal, los elementos de la red fija, como son los equipos de voz, de DSLAM y MPLS pasando, en muy pocos casos debido a la versatilidad de la red, por fibra óptica mediante la red DWM. La gestión de este segmento aislado de la red proporcionará dentro de las tareas de mantenimiento correctivo, los datos adecuados para optimizar los tiempos de atención ya que esto último incide directamente en el desempeño de toda la red, traduciéndose en interrupción de servicio hacia la ciudadanía y por ello posibles sanciones del ente regulador.


| | | |
|---|---|---|
| **ADJUNTO PDF:** | ☒ SI | ☐ NO |
| **CONTACTO CON AUTOR/ES:** | **Teléfono:** 0996728041 | E-mail: davisinho28@gmail.com |
| **CONTACTO CON LA INSTITUCIÓN (COORDINADOR DEL PROCESO UTE):** | **Nombre:** Manuel Romero Paz | |
| | **Teléfono:** 0994606932 | |
| | **E-mail:** manuel.romero@cu.ucsg.edu.ec | |

| **SECCIÓN PARA USO DE BIBLIOTECA** | |
|---|---|
| **Nº. DE REGISTRO (en base a datos):** | |
| **Nº. DE CLASIFICACIÓN:** | |
| **DIRECCIÓN URL (tesis en la web):** | |