REPÚBLICA DEL ECUADOR

Escuela Politécnica Nacional

"E SCIENTIA HOMINIS SALUS"

ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DESARROLLO E IMPLEMENTACIÓN DE LA METODOLOGÍA DE DISEÑO PARA LA MEJORA DE LA EFICIENCIA Y SEGURIDAD CIBERNÉTICA DE LA RED DE COMUNICACIONES DEL SISTEMA SCADA/ADMS DE LAS SUBESTACIONES DE EMELNORTE S.A., SUBESTACIÓN PILOTO EL RETORNO.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN "ELECTRÓNICA Y CONTROL"

ERICK SEBASTIAN POZO BENAVIDES

DIRECTOR: SILVANA DEL PILAR GAMBOA BENÍTEZ, Dra.

CODIRECTOR: PATRICIO IVÁN CHICO HIDALGO, MSc.

Quito, diciembre 2019

AVAL

Certificamos que el presente trabajo fue desarrollado por Erick Sebastian Pozo Benavides, bajo nuestra supervisión.

ING. SILVANA GAMBOA BENÍTEZ, DRA.
DIRECTOR DEL TRABAJO DE TITULACIÓN

ING. PATRICIO CHICO HIDALGO, MSC.
CODIRECTOR DEL TRABAJO DE TITULACIÓN

DECLARACIÓN DE AUTORÍA

Yo, Erick Sebastian Pozo Benavides, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada 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 cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Erick Sebastian Pozo Benavides

DEDICATORIA

A mis padres Julio y Rosy, que siempre han sido un pilar fundamental para cumplir mis metas.

A mi hermano Alexis, que siempre estuvo a mi lado con palabras de aliento y fortaleza.

AGRADECIMIENTO

A mis padres, por su apoyo incondicional.

A mi hermano, por su gran colaboración, y día a día brindándome cariño y fuerza.

A mi tia Fany, que con su ayuda incondicional siempre estuvo presta a colaborar.

A la Dra. Silvana Gamboa, por su apropiada guía en el desarrollo de este proyecto.

Al personal del Centro de Control SCADA de EMELNORTE, especialmente al Ing. Edison Eche por su colaboración.

ÍNDICE DE CONTENIDO

RESUMEN

Las subestaciones eléctricas son consideradas puntos estratégicos ya que son los sistemas que realizan la distribución de la energía eléctrica en las ciudades, estos sistemas han ido evolucionando hasta llegar al punto de implementar sistemas SCADA que permitan realizar una supervisión y control de todo el proceso que contempla una subestación eléctrica. Es aquí donde nace la necesidad de implementar un sistema de comunicaciones dinámico, el cual permita una facilidad en la administración, gestión y además cuente con las seguridades cibernéticas necesarias para su normal operación. Es en este punto donde EMELNORTE desea que sus redes LAN de sus subestaciones eléctricas contemplen todas estas características antes mencionadas y para ello se ha desarrollado una metodología acorde a la realidad de las subestaciones eléctricas.

Este trabajo se encuentra orientado a mejorar las redes de comunicaciones de las subestaciones eléctricas de EMELNORTE, manteniendo coherencia con normativas vigentes y aplicándolas a la realidad de las subestaciones eléctricas que mantiene la concesión de EMELNORTE.

PALABRAS CLAVE: SCADA, EMELNORTE, LAN, seguridades, administración.

ABSTRACT

The electrical substations are considered strategic points since they are the systems that carry out the distribution of electric energy in the cities, these systems have evolved to the point of implementing SCADA systems that allow monitoring and control of the entire process contemplated an electrical substation. It is here that the need to implement a dynamic communications system is born, which allows an ease in administration, management and also has the necessary cybersecurity for its normal operation. It is at this point that EMELNORTE wants its LAN networks of its electrical substations to contemplate all these characteristics mentioned above and for this purpose a methodology has been developed according to the reality of the electrical substations.

This work is aimed at improving the communications networks of EMELNORTE electrical substations, maintaining consistency with current regulations and applying them to the reality of electrical substations maintained by the EMELNORTE concession.

KEY WORDS: SCADA, EMELNORTE, LAN, securities, administration.

1. INTRODUCCIÓN

En la actualidad los sistemas eléctricos son considerados sistemas estratégicos, es por ello que es importante implementar sistemas de automatización y control industrial (IACS) tales como los sistemas SCADA, que permiten el monitoreo centralizado, con el objeto de mantener un adecuado conocimiento del estado, los eventos generados, además de habilitar la operación centralizada de las estaciones remotas del mismo, optimizando así la operación de un sistema tan importante como lo es el sistema eléctrico. Pero si bien la implementación de los SCADA trae importantes beneficios en la operación de los sistemas que se encuentran distribuidos en extensas áreas geográficas como es el caso de los sistemas eléctricos, la adecuada operación del SCADA requiere de la interacción entre sus componentes de control que están distribuidos a lo largo del sistema eléctrico a controlar, haciendo que la red de comunicación sea un punto neurálgico, por lo que para su implementación se requiere considerar lineamientos para una adecuada gestión y administración, así como la implementación de mecanismos de seguridad de esta red de comunicación acorde con la información que maneja, para garantizar su correcto funcionamiento así como del sistema eléctrico que controla [1].

Frente a este antecedente EMELNORTE consciente de las debilidades del sistema de comunicación que integra las subestaciones y el centro de control deciden iniciar un proceso de desarrollo de políticas y lineamientos a los que deben sujetarse la red de comunicación de su sistema SCADA, pues en la actualidad esta presenta problemas tales como la transferencia de información entre las subestaciones y el centro de control es poco fiable, presenta intermitencia en la operación de los equipos de fuerza debido a problemas de comunicación como retardos en él envió y/o recepción de la información, perdida de información cuando se ejecutan las alarmas que dan aviso a los accionamientos de los relés, retardo en la visualización de las variables en el SCADA del centro de control, a lo que se suma la facilidad con que el sistema de comunicaciones de las subestaciones puede ser vulnerado debido a que no tiene implementado una red de comunicación dedicada sino que comparte la infraestructura con la red de información de la empresa, dando como resultado una evidente falta de seguridad en la red de comunicación de las subestaciones.

Es por ello que es indispensable realizar una evaluación del estado actual del sistema de comunicaciones que integra las subestaciones y el centro de control de EMELNORTE, considerando parámetros tales como el tráfico de información, así como su gestión, administración y seguridad, para con esto conocer el comportamiento de cada uno de los

servicios y de forma primordial el comportamiento de los protocolos de control que se manejan en la red de las subestaciones, con el propósito de plantear mecanismos para evitar la intermitencia y caída de las comunicaciones de los equipos de control pertenecientes al sistema SCADA de las subestaciones, a fin de mejorar la funcionalidad del sistema. Posterior y en base a la evaluación del sistema de comunicaciones es necesario establecer una metodología y lineamientos para la implementación de la red de comunicación del sistema SCADA en la que se contemplará la arquitectura física, arquitectura lógica, administración, gestión y seguridad cibernética de la red, así como lineamientos para una adecuada selección de equipos y la metodología para la configuración de los mismos, además la implementación de la red de comunicación acorde a la metodología desarrollada en la subestación EL RETORNO, la misma que será referente para el desarrollo de esta propuesta. Es donde el presente proyecto de titulación pretende aportar a través del desarrollo de las actividades mencionadas previamente.

1.1 OBJETIVOS

El objetivo general de este Proyecto Técnico es:

Desarrollar e implementar la metodología de diseño de la red de comunicaciones del sistema SCADA/ADMS considerando la mejora de la eficiencia y seguridad cibernética de las subestaciones de EMELNORTE S.A. tomando como subestación piloto la subestación EL RETORNO.

Los objetivos específicos del Proyecto Técnico son:

- Revisar la base teórica, normativas, estándares y disponibilidad de equipos relacionados con la temática.
- Adquirir la información del comportamiento de la red LAN de la subestación EL RETORNO que forma parte del SCADA de EMELNORTE y que servirá como modelo de estudio.
- Determinar las condiciones actuales del flujo de información de la red LAN de la subestación EL RETORNO.
- Realizar una metodología que contenga lineamientos orientados a la administración, gestión y seguridad cibernética de las redes LAN de las subestaciones eléctricas de la red SCADA/ADMS de EMELNORTE.
- Validar la propuesta metodológica por medio de la implementación de una red de comunicación piloto acorde a los lineamientos establecidos en la subestación EL RETORNO de EMELNORTE.

1.2 ALCANCE

Evaluación de la arquitectura física y arquitectura lógica implementadas actualmente en la red industrial de las subestaciones de EMELNORTE.

Evaluación de los mecanismos de gestión y administración que se encuentran implementadas actualmente en la red de comunicación de las subestaciones de EMELNORTE.

Evaluación de los mecanismos de seguridad informática implementados actualmente en la red comunicación de las subestaciones de EMELNORTE.

Diseño de metodología para la implementación de los mecanismos de gestión, administración y seguridad cibernética de la red LAN de las subestaciones de EMELNORTE que forma parte del sistema SCADA/ADMS.

Diseño de arquitectura física y arquitectura lógica para la red LAN de las subestaciones de EMELNORTE que forma parte del sistema SCADA/ADMS.

Implementación de la red de comunicación acorde a la metodología propuesta en la subestación EL RETORNO de EMELNORTE.

1.3 MARCO TEÓRICO

1.3.1 SISTEMA SCADA

Sistema SCADA (supervisory Control and Data Adquisition) es una estructura organizada que engloba múltiples tareas, desde adquirir información en línea por medio de elementos industriales hasta mantener una supervisión constante del proceso, realizando un control de forma automática y/o manual en un espacio local o remoto. Los Sistemas SCADA tienen las siguientes funciones [8]:

- Adquisición de información en línea.
- Procesamiento de información.
- Almacenamiento de información (históricos).
- Presentación de la información en una interfaz gráfica.
- Supervisión local y remota del proceso.
- Control local y remoto del proceso.

Además, cuenta con las funciones de [8]:

- **Accesibilidad.**

El sistema SCADA permite mantener un acceso continuo a la manipulación de la maquinaria de forma remota a partir de una interfaz hombre maquina (HMI), se presentará información referente al proceso, la cual el operador podrá visualizar y tener una idea de cómo se está presentando el proceso y mantenerse en la capacidad de manipular las características del proceso.

- **Mantenimiento.**

El sistema a más de presentar datos del proceso nos permite mantener un monitoreo del estado de la maquinaria es así que se pueden programar varias alarmas que permita avisar al personal de etapas de mantenimiento o realizar un mantenimiento preventivo, esto dependerá de la planificación que se tenga dentro de la entidad.

- **Gestión.**

  La red de un sistema SCADA permite gestionar el acceso a varios servicios por ejemplo la integración de nuevos equipos, implementación de herramientas visuales, etc. Esto con la finalidad de realizar un proceso dinámico donde el sistema sea capaz de responder a las necesidades de la producción.

- **Calidad y eficiencia.**

  La implementación de un sistema SCADA se lo hace con el objetivo de mejorar la producción y que sea un sistema más eficiente, donde se obtenga un producto de buena calidad con el menor costo posible, si se lleva a cabo un sistema automatizado este debe verse reflejado en optimización de proceso y de recursos y por ende en un campo económico.

Así en un sistema SCADA se verá reflejado en mejoras de la eficiencia del proceso, esto conlleva a tener los siguientes beneficios:

- Disposición de la información del proceso en tiempo real.
- Control de equipos industriales de forma remota.
- Prevención de daños en la maquinaria y registro de fallos.
- Generación automática de información referente a daños o mal funcionamiento del proceso y realimentación en función de la información que se genera en tiempo real.
- Reducción de la contaminación ambiental.
- Maniobras de operación en un entorno controlado y seguro.
- Reducción de costos económicos durante el proceso.
- Reducción de accidentes industriales.

1.3.2 ESTRUCTURA Y COMPONENTES EN LOS SISTEMAS SCADA [8].

Existen algunas variaciones de cómo se puede estructurar un sistema SCADA sin embargo un buen ejemplo de un sistema SCADA se da en las subestaciones eléctricas donde se diferencian cuatro niveles, en donde el nivel 0 tiene equipos como seccionadores, en el nivel 1 equipos como IEDs (relés, medidores) de protección y control, en el nivel 2 se tiene equipos que procesan la información de toda la subestación, en este nivel ingresaría la red de comunicaciones industrial como eje fundamental, y por último tenemos al nivel 3 el cual está designado para el centro de control[27].

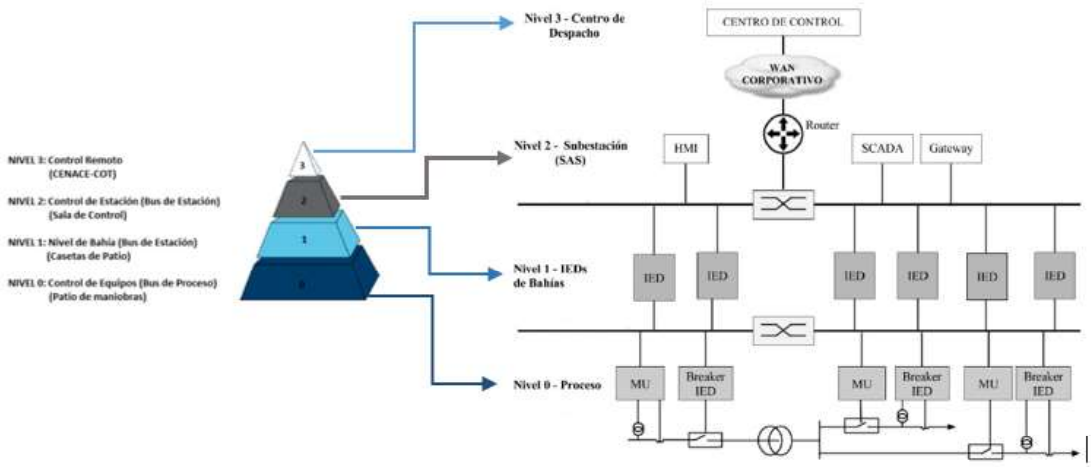

Figura 1.1. Niveles de control de una subestación eléctrica según CELEC EP-TRANSELECTRIC [27]

En la figura 1.1. se aprecia los niveles de control de un sistema SCADA propuesto por CELEC EP-TRANSELECTRIC en el año 2017 la cual es muy similar al propuesto por la norma IEC 61850, esta arquitectura define los elementos tanto de software como hardware en cada uno de los niveles, los mismos que son detallados en los siguientes numerales:

1.3.2.1 Elementos de hardware [12].

Se denomina elementos de hardware a todo equipo que forma parte de la red de comunicaciones que se encuentra interactuando por medio de protocolos de comunicación.

Interfaz hombre maquina (HMI).

Un HMI es un elemento electrónico que permite la interacción entre las personas y las máquinas, por medio de un software permite la interacción de forma gráfica, esto con la finalidad de observar el proceso e interactuar con él. Dependiendo de las características del HMI es posible que este elemento pueda interactuar con otros elementos de networking o de campo, con la finalidad de obtener información de históricos o datos en tiempo real, permitiendo una intercomunicación directa con cualquier dispositivo que forme parte de la red. Los HMI desde el punto de vista constructivo y operativo podemos encontrar como paneles touch, equipos industriales para ambientes agresivos o una PC convencional.

Unidad terminal maestra (MTU).

MTU es el elemento central del sistema SCADA, sus características, tamaño, y capacidad dependerá de los servicios que preste.

La unidad terminal maestra tiene como objetivos principales:

- **Control del almacenamiento de información:** permite filtrar la información que se recepta por parte de los RTU.
- **Administración de la información:** organiza la información dependiendo de factores como tiempo, tipo, relevancia, y otros factores que se permiten configurar.
- **Control de eventualidades en el sistema:** gracias a la capacidad de procesamiento que tiene la MTU es posible prestar el servicio de respaldo para equipos indispensables en el proceso de producción, en una situación que se suscite por daño parcial o fuera de servicio de algún elemento del proceso, se tenga la capacidad de remplazo de forma inmediata.
- **Presentación de informes automáticos:** permite mantener y reportar información referente al estado de cada uno de los equipos.
- **Seguridad cibernética:** permite mantener un control de acceso restringido hacia los dispositivos, además de la filtración de archivos no deseados y maliciosos.

Dispositivos de campo.

- **Unidad terminal remota (RTU) [12].**

Las RTUs son equipos que se encuentran ubicados en campo, básicamente realizan el control y supervisión del sistema local, además realizan el proceso de gestión de información, la cual es enviada al MTU, se pueden considerar dos tipos de RTU: unidades terminales remotas solas y unidades terminales remotas modulares.

Funciones de una RTU:

- Adquisición de datos de equipos de campo.
- Restricción de acceso local y remota.
- Generación de notificaciones por eventos fuera de rangos normales.
- Alarmas de funcionamiento del proceso de los equipos locales.
- Comunicación constante con la MTU.

- **Dispositivo electrónico inteligente (IED) [8].**

Equipos electrónicos que permiten realizar control y toma de decisiones en función de la información de equipos como sensores u equipos de campo su comunicación siempre es constante con la MTU.

- Recepción de datos de sensores y dispositivos electrónicos.
- Capacidad de enviar comandos de control.

- **Controlador lógico programable (PLC) [8].**

Un PLC es un dispositivo electrónico de campo que permite realizar control ante maquinaria, por medio de la lógica de programación realiza control. Se mantiene de forma constante la comunicación con la MTU.

1.3.2.2 Elementos de software en los sistemas SCADA.

El software en un sistema SCADA permite la interacción amigable entre los dispositivos y además con los usuarios, para ello se han denominado módulos o bloques de software que dan paso a las actividades de adquisición, supervisión y control, estos son los siguientes:

Configuración y distribución del entorno de trabajo.
Permite la definición de un entorno de trabajo de la aplicación, esto dependerá de la disposición de pantallas que se requieran y además se puede considerar los niveles de acceso para diferentes usuarios. En esta sección el usuario definirá las características de la pantalla, esto se refiere a como se representará el proceso, generalmente la pantalla es interactiva y permite la colocación de textos, graficas simples, graficas en movimiento graficas que formen parte del aplicativo o la importación de graficas desarrolladas en otro programa. Durante la configuración se debe tomar en cuenta la selección de los drivers de comunicación que permitirán el enlace con los elementos de campo y la conexión en red. En algunos sistemas también se permite la configuración de las variables que se van a visualizar, procesar o controlar [7].

Interfaz gráfico del operador.
Permite al operador controlar y supervisar el proceso. El proceso puede estar representado por medio de graficas que detallen como se encuentra estructurado el proceso, las gráficas pueden ser propias del SCADA o creadas en otros softwares de diseño (como AutoCad, solidworks, etc.) los sinópticos se forman por un fondo fijo y varias etapas dinámicas que cambian dependiendo los valores registrados en el proceso o respondiendo a las acciones del operador (como el cambio de set-point en un cuadro de texto variable.) [7] a la hora de diseñar las pantallas se debe considerar:

- Las pantallas deben presentar una imagen consistente, diferenciando las etapas del proceso, botoneras y mandos de control y mensajes de sistemas como estados y alarmas [7].
- Se recomienda la utilización de gráficos para la representación del proceso este debe ser organizado de izquierda a derecha [7].
- La información que se presenta debe aparecer sobre el elemento grafico que la genera, y se debe agrupar las señales de control por funciones [7].
- Es conveniente mantener una clasificación por colores con la finalidad de que sea más comprensible.
- Se debe seguir un orden adecuado y un uso coherente con los colores (por ejemplo, usar el color rojo en una alarma como indicativo de peligro).

Módulo de proceso.

Se denomina módulo de proceso al equipo que permite realizar acciones de forma automática, puede ser una pantalla con características administrativas donde a más de visualizar el proceso tiene la capacidad de comandar equipos de campo [7].

En cada una de las pantallas es posible programar relaciones entre las variables del ordenador o del autómata que se encuentran en ejecución mientras este activo. Es frecuente que el sistema SCADA confié a los dispositivos de campo el control directo del proceso, esto lo hace con la finalidad de concentrarse en operaciones de supervisión, como control del proceso y analizar las tendencias, generación de bitácoras. El SCADA puede ejecutar las siguientes acciones dependiendo del tipo de variable que maneje:

- Acciones de mando automáticas pre-programadas que dependen de valores de señales de entrada, salida o combinaciones de estas [7].
- Maniobras o secuencias de acciones de mando [7].
- Animación de figuras y dibujos, asociando su forma color, tamaño, etc. Al valor actual de las variables [7].
- Gestión de recetas que modifican los parámetros de producción (consignas de tiempo o de conteo, estados de variables, etc.) de forma pre-programada en el tiempo o dinámicamente según la evolución de la planta [7].

Gestión de archivo de Datos.

Es el encargado de almacenar y procesar de forma ordenada los datos según formatos inteligibles para elementos periféricos de hardware (como impresoras, registradores) o algún software (como hojas de cálculo o sistemas de base de datos), esto tiene que poseer la capacidad de compartir los datos en formatos entendibles para otros dispositivos [7]. A

pesar de que exista un registro continuo de los datos cada uno de los eventos que necesiten la información realizaran el uso de la forma y modelo que deseen (por ejemplo no todos los valores son usados en ciertos procesos, simplemente se toman valores cada intervalos de tiempo) estos datos pueden ser usados para algún software para desarrollar históricos o bitácoras posteriormente esta información puede ser usada para análisis de calidad o para realizar mantenimientos programados, esto dependerá de las necesidades de la planta y el proceso que se realiza. Es aquí donde radica la capacidad de los sistemas SCADA para mantener una información compartida entre los demás elementos que intervienen en el proceso.

Comunicación.

Los métodos para realizar un intercambio de información entre aplicaciones más comunes son:

OLE (Object Linking and Embedding) for Process Control (OPC).

Ole Process Control, es una tecnología que permite la comunicación entre aplicaciones. No depende de la fuente de los datos, más bien el formato de los datos es leíble por todos los equipos. De esta manera se puede realizar intercambio de información entre los equipos que cumplen los parámetros del estándar OPC. OPC trabaja en el modelo de cliente-servidor OPC [8].

Dentro de la norma tenemos:

- OPC DA (Data Access).
- OPC HDA (Historical Data Access).
- OPC A&E (Alarm and Events)
- OPC DX (Data Exchange).
- OPC XML (Extensive Markup Language).

Dynamic Data Exchange (DDE)

Las siglas DDE representan (Dynamic Data Exchange), es un método de intercambio de información basado en Windows [8].

En este caso el intercambio de información se realiza por medio de una memoria, usando un protocolo que gestione la comunicación, DDE permite que las aplicaciones ejecuten comandos de otras aplicaciones [8].

Las siglas OLE representan (Object Linking and Embedding) fue diseñado con el objetivo de gestionar documentos formados por elementos heterogéneos (un documento heterogéneo puede contener texto y otros elementos como imágenes, audio y video) [8].

Lenguaje de consulta estructurado (SQL).

El lenguaje de consulta estructurado es un estándar que permite la comunicación de base de datos. Este estándar permite incluir también: [8]

- Bibliotecas de comandos en las bases de datos.
- Eventos, los cuales se activan automáticamente, y son dependientes de condiciones.
- Permite duplicar y sincronizar un grupo de bases de datos.
- Permite el intercambio o envió de información dependiendo de los eventos.

Código estándar americano de cambio de información (ASCII).

Mediante el uso del formato ASCII, es posible el intercambio de información como valores numéricos, caracteres [8].

Interfaces de programación de aplicaciones (API).

Las herramientas de API permiten al usuario una Buena adaptación del Sistema por medio de códigos de programación, estas pueden ser desarrolladas en C++, Java o Visual Basic [8].

1.3.3 RED DE COMUNICACIONES EN SISTEMAS SCADA.

Uno de los elementos importantes en un sistema SCADA es la red de comunicaciones, la cual es la encargada de ser el medio por el cual la información se traslada desde los puntos de adquisición hacia equipos de visualización y control, y dada su importancia en el proceso industria, la red de comunicaciones debe proporcionar los siguientes servicios:

- Adquisición de información.
- Supervisión.
- Control.
- Comunicación remota.
- Seguridad de los datos.
- Seguridad de acceso a la red del sistema SCADA.

La adquisición de la información**,** es la capacidad de presentar datos en línea en todo momento con amplia fiabilidad, manteniendo mediciones reales y con un retardo lo

suficientemente pequeño para que el valor que se observa en una interfaz de visualización sea la que se encuentre marcando el medidor en dicho instante.

Es importante considerar una supervisión en todo momento, la existencia de varias aplicaciones específicas con el monitoreo constante, permite observar el funcionamiento del proceso en todo momento.

Mantener un control adecuado permite realizar maniobras por parte del personal desde una interfaz, para ello la red debe presentar la facilidad del uso de protocolos de aplicaciones adecuados a las exigencias del sistema.

Las redes industriales deben permitir el uso de protocolos que permitan la manipulación del sistema de forma remota ya que generalmente la operación del proceso no necesariamente se encuentra en el mismo entorno.

Es importante que la información que se encuentra en la red del sistema sea fidedigna y no sea producto de alteraciones, para ello se debe controlar el tráfico de información y mantener un registro o bitácoras que permitan detectar anomalías en la información que circula dentro de la red.

Las redes de los sistemas SCADA deben presentar restricciones para el personal, ya que solo personal autorizado y capacitado podrá tener acceso, para ello se debe garantizar que sus credenciales se ejecuten con protocolos de seguridad, además de mantener una bitácora de acceso donde se presente la identificación del personal que accedió a la red además de parámetros como fecha y hora a la cual ingreso [8].

Este trabajo está orientado a sistemas SCADA en sistemas eléctricos razón por la cual se considera los niveles que recomienda el CENACE.

Arquitectura de una red de comunicaciones industriales.

En base a la norma IEC 61850 que fue creada para la comunicación entre equipos de control, protección y medición de las subestaciones eléctricas, su objetivo principal es la interoperabilidad de dispositivos. Los beneficios que plantea el estándar se los puede resumir como [12]:

- Interoperabilidad entre los diferentes fabricantes de los equipos.
- Reducir los costos de mantenimiento.
- Simplificar configuraciones.
- Racionalización de la información.
- Mantener una buena escalabilidad.

- Reducir el cableado.

En la sección del estándar IEC 61850-7 se referencia una arquitectura que se muestra en la figura 1.2.

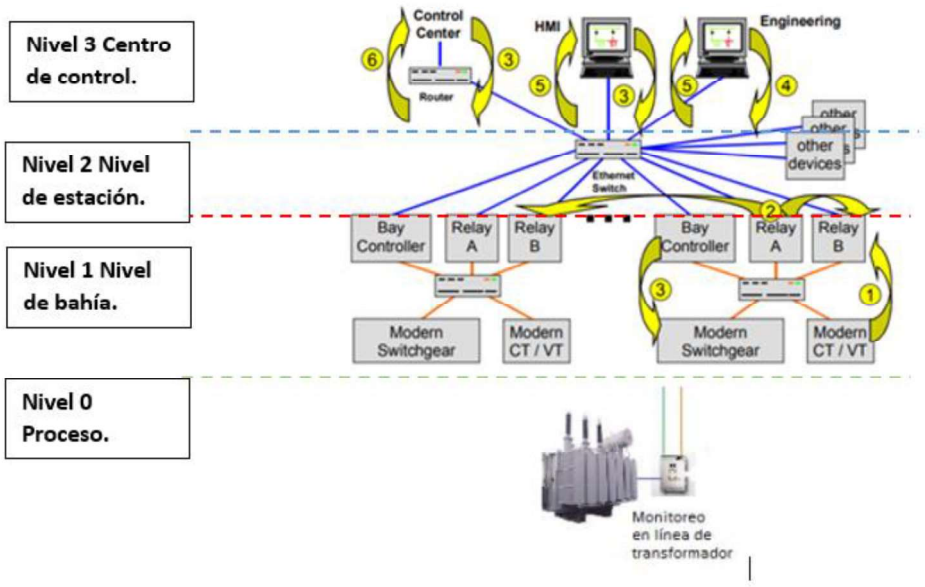

Figura 1.2. Topología de automatización de subestaciones de muestra [12]

En la figura 1.2. se muestra varias funciones en dispositivos electrónicos inteligentes (IED), varias funciones pueden implementarse en un solo IED o una función puede implementarse en un IED y otras funciones pueden hospedarse en otro IED.

Arquitectura en cascada [12]: en esta arquitectura los switches se conecta por medio de uno de sus puertos con el siguiente switch, considerar que estos puertos deben manejar mayor capacidad de tráfico de información.

Ventajas.

- Es fácil implementar nuevos equipos.
- Requiere menor cable que una topología estrella.

Desventajas.

- Si existe daños en el cable de comunicación principal, los equipos quedarían incomunicados, tantos equipos se encuentren conectados desde el punto del daño.
- Es difícil detectar un problema cuando la red cae.
- No es recomendable usar esta arquitectura para grandes instalaciones o equipos denominados como críticos.

En la figura 1.3. se observa la arquitectura en cascada.

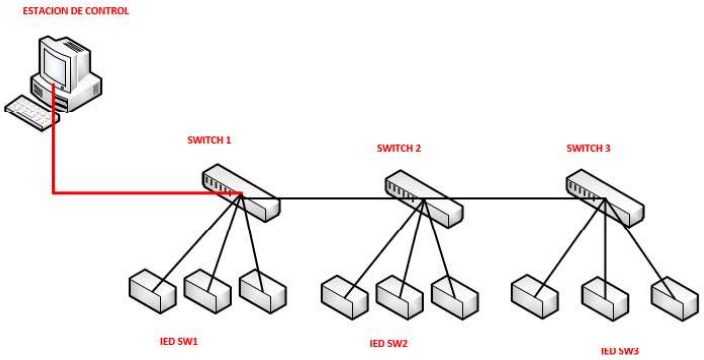

Figura 1.3. Arquitectura en cascada [12]

Arquitectura en anillo [12]: esta arquitectura mantiene una semejanza con la arquitectura en cascada sin embargo esta arquitectura cierra la conexión entre el primer switch y el ultimo switch, se podría creer que esto generaría lazos cerrados donde la información se encuentre divagando en la red hasta que esta se "dropee (término usado para decir que el dato se ha desechado por diferentes factores)" para ello se pueden usar protocolos como el STP (Spanning tree Protocol) el cual se encuentra detallado en el estándar IEEE 802.1D, el estándar permite la identificación de los lazos cerrados y da paso a un bloqueo del dato dentro del lazo, sin embargo el protocolo STP es relativamente lento y que se demora algunas décimas de segundo en realizar la reconfiguración de las vías por donde enviara la información, para corregir esta falencia se desarrolló RSTP (Rapid Spanning Tree Protocol) detallado en el estándar IEEE 802.1w. Esta arquitectura permite tener dos caminos por donde la información puede circular en la figura 1.4. se puede observar esta arquitectura.

Ventajas.

- No es necesario un nodo central para administrar la conectividad entre los equipos.
- Gracias a las conexiones punto a punto de los dispositivos, teniendo un dispositivo a cada lado, es fácil de instalar y reconfigurar ya que para instalar un nuevo dispositivo solo es necesario mover dos conexiones.
- La conexión punto a punto facilita la identificación de fallas y una facilidad para aislar el dispositivo.

Desventajas.

- Una estación de trabajo con problemas puede crear conflictos para toda la red sin embargo esto se puede solucionar con un anillo doble.

- Requiere mayor complejidad para configurar que una red en estrella.
- Se puede ver restringido en la longitud del anillo.

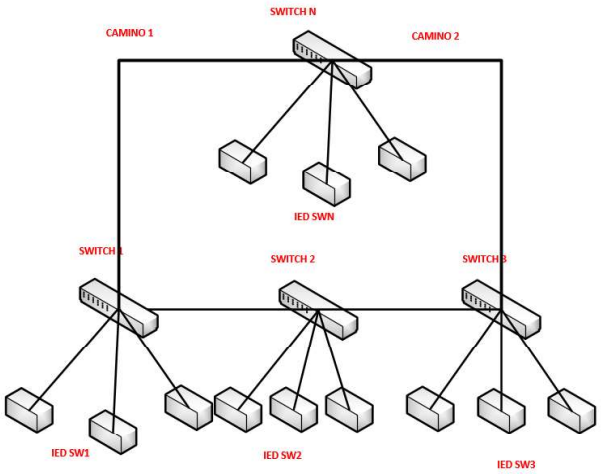

Figura 1.4. Arquitectura en anillo [12]

Una de las variaciones de la arquitectura en anillo son: topología en anillo centralizado, topología en anillo descentralizado y sistemas con varios anillos.

La arquitectura con anillo centralizado, donde todos los IEDs se encuentran conectados a un switch, en la siguiente figura 1.5. se puede observar esta topología.

Ventajas.

- Es relativamente fácil encontrar fallas o errores.
- Dado que las distancias son cortas entre la conexión de los equipos, resulta una solución económica ya que la distancia del cableado es corta.

Desventajas.

- Se recomienda su aplicación en subestaciones donde se tenga los IEDs en una misma habitación.
- dado que se recomienda para subestaciones pequeñas generalmente estos contemplan un armario donde puede presentarse dificultades en la modificación de la red.
- Limitaciones de expansión o agregar nuevos equipos.

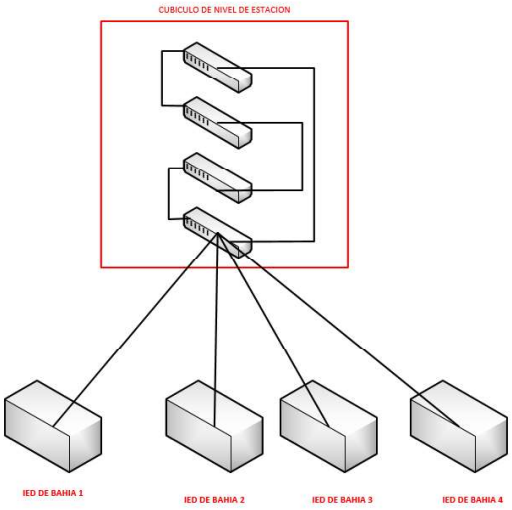

Figura 1.5. Arquitectura en anillo centralizado [12]

La arquitectura de anillo descentralizado es usada para sistemas de automatización de mayor exigencia, donde existen distancias considerables entre la estación y la bahía, es una estructura donde se usen varios IEDs en cada bahía.

Arquitectura en estrella: en la arquitectura en estrella se tiene un switch centralizado y enlaza a los otros switches con un enlace troncal, esta arquitectura es relativamente más rápida en comparación con las otras arquitecturas mencionadas ya que el número de "saltos" entre equipos es de dos.

Ventajas.

- A diferencia de las topologías en cascada y anillo, si un dispositivo sufre un daño o la conexión se rompe, solo el dispositivo deja de funcionar sin afectar a los demás equipos.
- Es fácil la implementación de un equipo a la red.

Desventajas.

- No es tan económico en comparación con topologías como cascada y anillo ya que es necesario más cable para las conexiones.
- El número de equipos conectados a la red depende de las limitaciones del equipo concentrador.

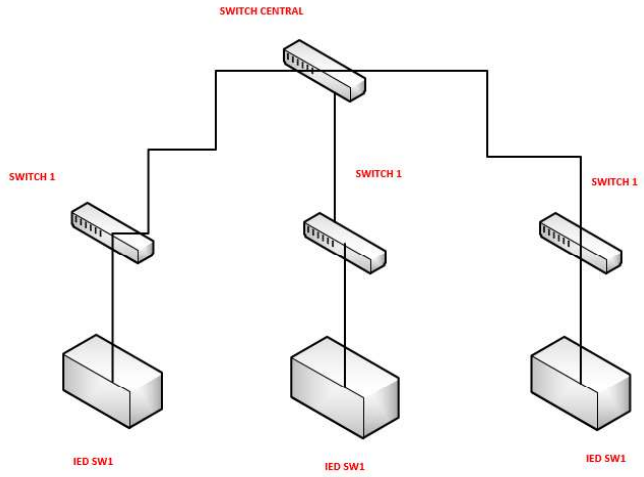

Figura 1.6. Arquitectura en Estrella [12]

Es importante considerar que, en cada una de las topologías presentadas es posible realizar enlaces redundantes, modificaciones en su estructura o agregar más equipos con la finalidad se suplir con cada una de sus debilidades y así mejorar su rendimiento, sin embargo esto dependerá de las necesidades que se presenten y además de la disponibilidad económica para la implementación de la red.

La red de comunicación que se maneja es denominada como red de comunicación industrial por las prestaciones que debe presentar ante las necesidades de los diferentes equipos que conecta, ya que estos equipos se manejan con sus propios protocolos y peculiaridades.

Una red industrial debe de estar diferenciada en un entorno donde coexiste junto con una red de información, la diferenciación debe de marcarse por medio de equipos de networking, además, su robustez debe ser acorde al entorno en el que se desarrolla permitiendo así un funcionamiento adecuado ya que estos equipos deben soportar el ruido electromagnético producido por la maquinaria y las adversidades que se presenten en el medio donde se encuentren instalados.

Las características y prestaciones de la red industrial son:

- **Organización jerárquica:** es importante mantener un orden adecuado de los equipos de networking, esto permite mejorar el rendimiento del proceso de transferencia de información.
- **Robustez adecuada al entorno donde se desarrolla:** los equipos de networking deben tener la capacidad de soportar interferencia electromagnética, un grado de robustez constructiva acorde al medio que será sometido.

- **Manejo de protocolos industriales:** los sistemas de control y los elementos electrónicos que se maneja en un SCADA fueron diseñados con características conforme a los procesos que se realizan, por ello presentan una diferenciación notable ante protocolos orientados a la información de forma general.
- **Redundancia en los equipos de networking:** una red industrial debe estar diseñada de tal manera que se garantice su operatividad de forma constante, para ello es indispensable mantener equipos o configuraciones redundantes.
- **Seguridad ante el ingreso de usuarios ajenos al proceso:** el acceso a los dispositivos debe de ser restringido solo para personal que tenga las credenciales que garanticen un adecuado manejo de la información.
- **Alta eficiencia:** la eficiencia de la red se debe ver reflejada en la capacidad de la red por transportar la información de forma rápida, fidedigna y segura entre los dispositivos de la red.
- **Uso de elementos de protección tanto físicos como virtuales:** es importante que la red presente en su arquitectura elementos que permitan proteger la información y la manipulación, esto debe observarse de forma física y además por medio de configuración, ya que una de las exigencias de los equipos de networking industriales es su alto grado de protección ya que en muchos casos los procesos industriales son puntos estratégicos.
- **Capacidad para mantener comunicación de forma remota:** algunas de las redes de los sistemas SCADA presentan el control de varias redes LAN (Redes de Área Local), por ello se debe permitir la comunicación de forma remota.

Dispositivos de comunicación industriales.

Si bien dentro de los dispositivos industriales se encuentran comprendidos equipos de accionamientos, medidores y equipos de networking, en esta sección se centrará en equipos de networking como routers y switches orientados a una subestación eléctrica. Los router como dispositivos centrales en una red LAN de una subestación eléctrica será el encargado de diferenciar la red interna de la subestación y la red externa que puede estar comprendida del centro de control donde se monitorea y controla todas las subestaciones y de las demás subestaciones eléctricas, otra actividad que realiza el router es introducir reglas de ingreso a la red, estas reglas pueden estar dadas por restricciones por IP, por MAC, etc. Esto dependerá de las características que tenga el equipo. Los switches son equipos que conmutan la información entre los equipos, estos equipos deben contener tantos puertos sea necesario para conectar los dispositivos industriales.

Todos los dispositivos de networking deben tener básicamente filtros de protección, protocolos de sincronización, protocolos de redundancia y manejar protocolos industriales entre otras características o prestaciones que hagan que la red sea más eficiente.

Protocolos industriales en los sistemas SCADA.

Existen varios protocolos que se manejan a nivel industrial como Modbus, Profibus, devicenet, DNP (Distributed Nerworking Protocol), DNP es uno de los protocolos más usados en cuanto se refiere a subestaciones eléctricas en todo el mundo, actualmente se encuentra en la versión 3.0.

Distributed Nerworking Protocol v.3 (DNP3) [24].

El protocolo fue desarrollado para una operación entre equipos como RTU, PC e IED. Los cuales a su vez mantienen una comunicación con la MTU.

Ventajas del protocolo para red distribuida.

- Se encuentra en la capa tres del modelo OSI (sistemas abiertos de interconexión).
- Se puede mantener una integración de más de 500 usuarios.
- El protocolo es robusto ya que fue diseñado para ambientes industriales.
- DNP3 es considerado como un protocolo de estándar abierto razón por la cual muchos fabricantes han incluido este protocolo en sus equipos.
- Permite varias topologías: punto a punto, maestro-esclavo, múltiples maestros.
- Generación de mensajes de difusión (broadcast) hacia todos los dispositivos esclavos.
- Permite mantener una interacción con el maestro y esclavo donde se generen respuestas no solicitadas por parte del maestro.
- Generación de escalas de relevancia en él transporte de datos.
- Él transporte de los datos es de forma fragmentada esto con la finalidad de mantener un control de errores y secuencias rápidas de comunicación.

Topologías recomendadas para el uso del protocolo DNP 3 [24].

- Maestro-Esclavo.
- Múltiples esclavos.
- Múltiples maestros.
- Arreglo jerárquico de concentradores de datos de nivel medio.

El protocolo DNP3 se ajusta al modelo de capas EPA (arquitectura de rendimiento mejorado).

Relación de capas del modelo OSI y el modelo EPA:

7	Aplicación
6	Presentación
5	Sesión
4	Transporte
3	Red
2	Enlace
1	Física
MODELO OSI	

Aplicación
Pseudo-Transporte
Enlace
Físico
MODELO EPA

Figura 1.7. Comparación entre el modelo OSI y modelo EPA [24]

Modbus.

Modbus es un protocolo que se maneja en un entorno maestro-esclavo, donde el maestro realiza un mensaje de solicitud y el esclavo realiza un mensaje de respuesta. De forma general el maestro sería una interfaz hombre maquina (HMI) o un software SCADA y el esclavo podría ser un dispositivo electrónico inteligente (IED) [9].

Cuando se determina al equipo si este es maestro o esclavo se generan ciertas limitaciones o privilegios: por ejemplo, un maestro puede realizar una comunicación punto a punto con un esclavo, o también puede realizar él envió de mensajes de difusión más conocidos como mensajes de broadcast [8].

Con el tiempo modbus ha ido desarrollando y se han creado algunas variables como:

- Modbus RTU.
- Modbus ASCII.
- Modbus plus.
- Modbus TCP

Norma IEC 60870-5-104.

La norma IEC 60870-5-104 fue dado a conocer en el año 2000 por IEC (International Electrotechnical Commission) su predecesora fue la norma IEC 60870-5-101.

IEC 60870-5-104 permite la comunicación entre una estación de control y una subestación eléctrica por medio de una red TCP/IP, donde TCP es un protocolo que trabaja en la capa de transporte.

La principal ventaja de IEC 60870-5-104 es que permite una comunicación por medio de una red estándar, esto da paso a una transmisión simultánea entre diferentes tipos de dispositivos [10].

IEC-104 es designado de acuerdo con una selección de funciones de transporte dada en el paquete del protocolo TCP/IP (RFC 2000). TCP/IP es aplicable a varios tipos de redes con: X.25. Frame Relay, ATM, ISDN, Ethernet y punto a punto en la serie (X.21) [11].

Tabla 1.1. Lista de protocolos con 104 [11]

SELECCIÓN DE FUNCIONES DE APLICACIÓN	**PROCESO DE USUSARIO**
Selección de unidades de datos de servicio de aplicación (ASDU) de IEC 60870-5-101 y 104	Capa de aplicación
Información de control de protocolo de aplicación (APCI)	
Información de control de protocolo de aplicación (APCI)	Capa de transporte
	Capa de enlace de datos
	Capa física

Formato de Información de Control de Protocolo de aplicación (APCI).

APCI (Información de Control de Protocolo de aplicación) empieza con un byte de inicio con valor 0x68 seguido de la longitud de 8 bits de APDU (Unidad de datos de Protocolo de Comunicación) y cuatro campos de protocolo de 8 bits (CF). APDU contiene un APCI o también puede contener un APCI con un ASDU, en la gráfica 1.7 podemos apreciar la estructura de APCI [11].

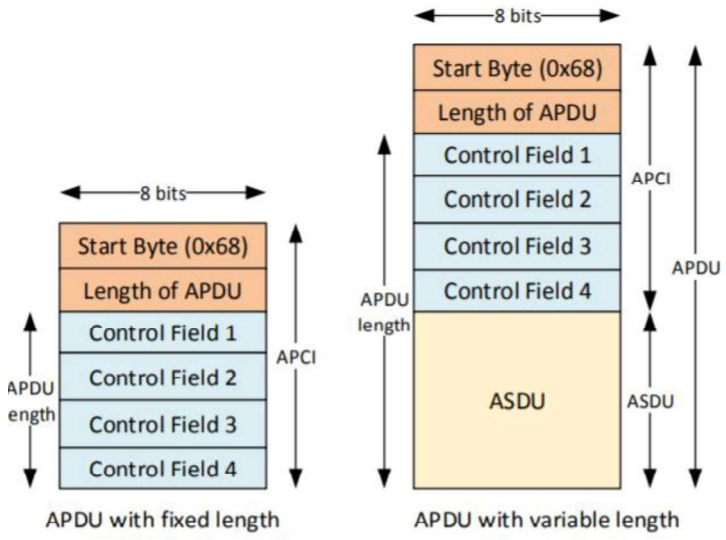

Figura 1.8. Formato de la trama APCI [11]

1.3.4 SEGURIDAD EN LOS SISTEMAS SCADA.

A través del tiempo los sistemas SCADA han ido evolucionando, con la incorporación de nuevos equipos, nuevos protocolos de comunicación, aplicativos, etc. Si bien esto ha hecho que los sistemas SCADA sean más eficientes también se han incorporado nuevas amenazas y puntos vulnerables, estas deficiencias o puntos inseguros generalmente se aprecian en la red de comunicación, donde personas ajenas al proceso han intentado ingresar con la finalidad de causar daños. En función de lo antepuesto nace el concepto de seguridad cibernética aplicada a las redes industriales, con la finalidad de prevenir y precautelar la seguridad de las instalaciones y aún más los procesos que controlan los sistemas SCADA [8].

Un análisis que realiza anualmente la empresa de seguridad Kaspersky nos proporciona datos estadísticos del crecimiento de amenazas hacia los dispositivos electrónicos, esto se puede apreciar en los siguientes datos [1]:

- Karspersky neutralizó 962.947.023 ataques lanzados por medio de recursos de internet en un entorno de 187 países.
- Registró 351.913.075 direcciones URL que provocaron la reacción del antivirus web.

- Se neutralizó 215.762 intentos de ejecución de programas maliciosos orientados a cuentas bancarias.
- Se neutralizó 158.921 ataques de cifrado.
- El antivirus detectó 192.053.604 objetos indeseables.
- Se protegieron 1.744.244 paquetes de instalación maliciosa en equipos móviles.

En la figura 1.9. se presenta estadísticas de ataques por medio de protocolos usados comúnmente.

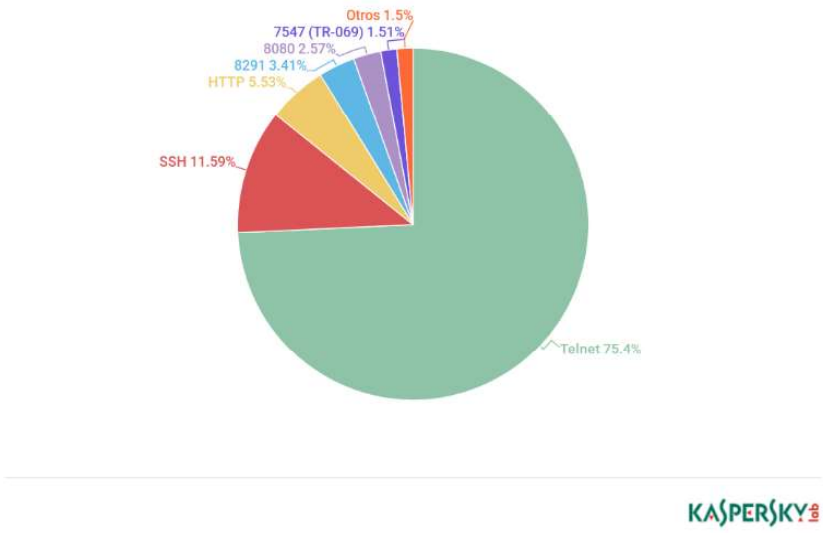

Figura. 1.9. Estadística de los protocolos de internet de las cosas más atacados según Kaspersky LAb. [1]

Como podemos observar en la gráfica de la figura 1.9 uno de los protocolos más vulnerables es el protocolo telnet, este protocolo es muy usado para realizar comunicación de forma remota. Generalmente los equipos de networking se encuentran habilitados con este protocolo el cual ocupa el puerto 23.

Existen muchas amenazas que pueden dañar nuestra red de comunicación, en esta sección presentaremos las amenazas más comunes. Entre estas tenemos [26]:

i. Suplantación de identidad.

Se refiere al ingreso de un intruso al sistema usando las credenciales de una persona autorizada.

La suplantación de identidad puede ser de forma física o de forma virtual, de forma física por medio del robo o clonación de las credenciales físicas para el ingreso hacia las

instalaciones. Y de forma virtual donde por medio del nombre de usuario y contraseña da paso al sistema, estas dos formas de suplantación de identidad son extremadamente peligrosas ya que el sistema admite al usuario y otorga todos los atributos de la persona suplantada esto da paso al robo de información.

El robo de información ocurre cuando los sistemas de seguridad son vulnerados. Los puntos principales como servidores o puntos de configuración son clave, es aquí donde el atacante puede obtener información privilegiada, y posteriormente usarla con beneficios particulares como extorción, esto trae como consecuencia manipulación y la perdida de información.

Cuando se da paso al sistema de forma fraudulenta este puede sufrir daños o configuraciones ajenas, que pueden ocasionar pérdidas que son traducidas a pérdidas económicas. En la actualidad el tema de manejo de información es extremadamente importante ya que un sistema puede quedar en evidencia sus falencias las cuales pueden ser aprovechadas por algún atacante.

ii. Suspensión de servicios.

Una de las prácticas comunes de los atacantes es privar a los clientes de los servicios que se presten en el sistema, estos pueden ser denegación de información, denegar el acceso a ciertos equipos, etc. Estos ataques tienen en su mayoría causar daños a los equipos y sistemas del proceso, ya que, por el uso excesivo de memoria, CPU, buffer se pretende realizar un ataque de Denegación de Servicio DoS. También existen ataques denominados degeneración de servicios distribuido DDoS, este ataque tiene el mismo objetivo que DoS la diferencia es que es un ataque más agresivo ya que se utilizan varias computadoras para el cometido o también el uso de “boots”, este ataque es uno de los más usados por la facilidad de su elaboración.

La mitigación de este tipo de ataque dependerá de:

- Un monitoreo constante y adecuado de tráfico de información y la detección de anomalías, para esto se necesitan políticas claras y parámetros que el personal debe seguir.
- La configuración de los equipos tenemos que limitar el número de conexiones por usuario.
- La limitación de recursos en los equipos, este parámetro también es importante para detectar estos ataques ya que cuando estos ataques están en curso es evidente que los equipos empiezan a usar más recursos como memoria y CPU.
- Políticas claras y capacitación constante al personal.

iii. Software malicioso.

Este tipo de software tiene como objetivo ingresar a los sistemas y desarrollar alguna actividad ilícita, existen varios tipos, pero se los puede clasificar de la siguiente forma:

- **Virus:** son un tipo de códigos maliciosos que se puede auto replicar, su instalación es realizada de forma automática sin los permisos o consentimiento del usuario. [2].
- **Gusanos:** estos códigos maliciosos se auto instalan de forma automática sin la necesidad de una autorización de los usuarios, la diferencia con los virus es su forma de operar ya que posterior a su auto instalación este permanece "dormido" hasta que encuentre el momento adecuado para vulnerar alguna debilidad. [2].
- **Troyanos:** este tipo de software no se oculta en archivos adjuntos como lo hacen los virus y gusanos, el modo de introducirse en los sistemas es realizando operaciones paralelas, inicialmente el troyano es un programa que se muestra como tal, sin embargo, tiene actividades maliciosas que operan de forma paralela, estos generalmente no son auto replicables. [2].
- **Ransomware:** está diseñado con el objetivo de extorsionar a la víctima es posible que aparezca en forma de pop up (ventanas emergentes que aparecen de forma inesperada), generalmente cuando emerge una ventana y se procede a dar click, se produce la vulneración del sistema, estos pueden ser mensajes de pago de dinero.
- **Backdoor:** es un software malicioso que es difícil de detectar ya que se oculta en los sistemas operativos permitiéndose pasar desapercibido, además su objetivo es implementar una comunicación remota desde donde el atacante puede robar información del sistema o instalar diferentes herramientas que le puede permitir obtener contraseñas. [2].

Según el informe presentado por la ENISA (agencia en seguridad de las redes) en junio del 2018 estos fueron los softwares maliciosos más peligrosos:

- **Primera variante de WannaCry conocida como run-of-the-mil:** uno de los softwares maliciosos (ransomware) más peligrosos el cual fue lanzado el 12 de mayo del 2017, infectando a miles de computadoras que usaban Windows, el día que fue lanzado se estima que 141000 computadoras fueron atacadas, posteriormente Windows lanzó un parche para proteger de este software malicioso.
- **EternalBlue:** es un exploit que fue lanzado por un grupo de hackers llamados "Shadow Brokers" el 14 de abril del 2017, y trabaja conjuntamente con EternalBlue.

- **STUXNET:** fue considerado el primer malware desarrollado para atacar sistemas de control industriales, específicamente deshabilitar plantas nucleares iraníes, este malware fue detectado por Kaspersky en el 2010 [28].
- **DUQU:** su principal objetivo era infectar sistemas SCADA de las empresas de oriente medio [28].
- **CrashOverride:** fue un malware exclusivo para sistemas TO, sus objetivos de ataque eran IEC 61850, IEC 101 e IEC 104 [28].

1.3.3.1 APLACAMIENTO DE LAS DEFICIENCIAS DE LA RED [26].

La mitigación o reducción de la amenaza depende de varios factores en esta sección se presentarán configuraciones recomendadas:

- **Organización de la red [26].**

Una buena práctica para mitigar las amenazas es mantener una estructura de red por medio de redes virtuales o también conocidas como VLAN, la creación de VLAN permite generar grupos de terminales ya sea por su operación en la red o por su servicio, con esta configuración podemos obtener:

- Mejoramos el desempeño de la red ya que se optimiza el ancho de banda por lo cual se generan dominios de difusión limitados.
- Se puede evitar ataques de tipo DDoS.
- Ya que los equipos se encuentran compartiendo un segmento de red es más fácil determinar las rutas de envió de información.

- **Aplicación de ACL (lista de control de acceso) [26].**

Las ACL es un método que nos permite filtrar la información, donde un router puede determinar que paquete reenvía o descarta, este método es de utilidad para controlar el tráfico que ingresa y sale de la red que deseamos proteger. Una ACL realiza las siguientes tareas:

- Las ACL pueden limitar el tráfico, esto permite que la red incremente su desempeño ya que los equipos de networking no tienen que estar constantemente verificando paquetes que no le corresponde, además de limitar o bloquear información que esta fuera de las funcionalidades por las que fue creada la red.

- Se realiza un control minucioso del flujo de tráfico, esto puede traducirse como denegar el servicio de actualización automático que tiene algunos equipos, permitiendo que las actualizaciones sean instaladas de un origen conocido.
- Las ACL es un método básico de seguridad ya que limita el acceso a ciertos equipos y además proporciona un ligero control hacia los equipos que se conectan.
- Las ACL pueden limitar el tráfico de forma selectiva permitiendo el servicio a un protocolo determinado y negando el servicio a otros protocolos.
- Existen ACL que filtran paquetes en las capas 3 o 4 del modelo OSI.

Las ACL se pueden dividir en dos tipos:

- **ACL estándar:** este tipo de ACL permite restringir el tráfico de información a nivel de capa 3.
- **ACL extendidas:** son ACL más elaboradas que permite la restricción del tráfico a nivel de capa 3 y 4.

➢ **Cortafuegos.**

Un cortafuego es un mecanismo usado para controlar y monitorear el tráfico hacia y desde una red con la finalidad de proteger los dispositivos en la red. Compara el tráfico que lo atraviesa con una política o criterios de seguridad predefinidos, descartando los mensajes que no cumplen con la política. La figura 1.10 muestra un cortafuego simple que protege una computadora personal (PC) y un controlador lógico programable (PLC) de tráfico no deseado de internet, al tiempo que permite que las solicitudes ingresen al servidor web corporativo [3].

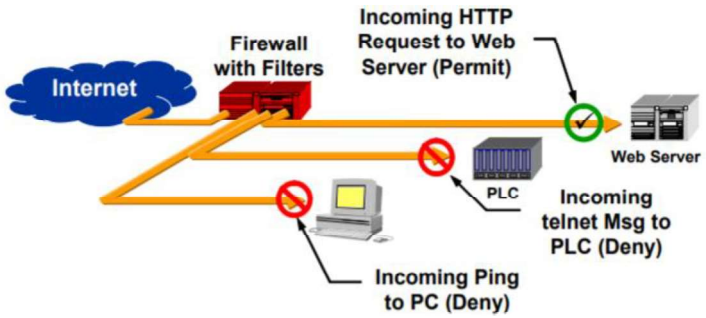

Figura 1.10. Ejemplo simple de un cortafuego orientado a internet que protege dispositivos de una red [3]

Existen varios tipos de cortafuego, pero en general los cortafuegos actúan en base a la configuración de los paquetes o la información que estos contengan, alguna de esta información puede ser:

- Dirección de fuente.
- Dirección de destino.
- De qué servicio pertenece el paquete.
- Tipo de puerto.
- Banderas de estado.

Esta es alguna información que puede analizar el cortafuego y determinar una acción con el paquete. En este punto el cortafuego deja pasar la información o la "dropea" (termino que se utiliza para indicar que el paquete se desechó). Es así que los tipos de cortafuegos pueden separarse como:

- **Cortafuego de filtro de paquetes:** la clase la simple de cortafuegos se conoce como cortafuegos de filtro de paquetes. Tiene una serie de reglas estáticas y las utiliza para tomar medidas sobre paquetes recibidos de forma individual [3].
- **Cortafuego de estado:** un cortafuego más sofisticado, conocido como cortafuego con estado, rastrea de manera inteligente las interrelaciones entre los paquetes que pueden fluir a través de él. Al mantener un historial de paquetes aceptados y el estado de las conexiones actuales, solo puede aceptar tráfico "anticipado" los conjuntos de reglas de firewall con estado pueden ser condicionales debido a la inteligencia del cortafuego [3].
- **Cortafuegos de aplicación en proxy:** los cortafuegos Proxy de aplicación abren paquetes en la capa de aplicación, los procesan según las reglas de aplicación específicas, luego los vuelven a unir y los envían al dispositivo de destino deseado. Por lo general están diseñados para concentrarse en una variedad de protocolos de aplicación (como Telnet, FTP, HTTP, etc.) a través de una sola máquina, pero luego se envía el tráfico a otros terminales. En lugar de concentrarse directamente a un servidor externo, el cliente se conecta a un servidor de seguridad proxy, que a su vez inicia una conexión con el servidor externo solicitado [3].

- **Protocolos de seguridad de cifrado [26].**

Un protocolo de cifrado tiene como objetivo codificar la información de forma que esta sea ilegible cuando se está transportando, esto se lo realiza con la finalidad de limitar el acceso y proteger la información, y solo el equipo receptor que contenga la forma de decodificación podrá acceder a los datos para ello encontramos dos protocolos de cifrado SSL y TLS.

- **SSL (capa de zócalos seguros):** este protocolo utiliza certificados digitales (la emisión de los certificados digitales la realiza la autoridad de certificación la cual

realiza verificaciones que garantizan que el certificado entregado sea legítimo.). los desarrolladores de SSL fueron Netscape sin embargo la IETF (grupo de trabajo de ingeniería de internet) ha mantenido el desarrollo de SSL hasta su versión 3 posterior a esta versión se desarrolló TLS.

- **TLS (capa de transporte seguro):** TLS y SSL no interactúan, el protocolo TLS permite que se identifiquen las dos partes tanto el cliente como el servidor.
  Tanto el cliente como el servidor permiten establecer las claves secretas con la que se comunican.

- **Antivirus.**

Los antivirus son software que iniciaron su desarrollo con el objetivo de detección y eliminación de amenazas comunes como troyanos virus y gusanos que en la actualidad son considerados software maliciosos antiguos, esto se debe a que ya existen otros métodos mucho más avanzados y eficientes para realizar ataques.

Podemos clasificar a los antivirus según su objetivo como:

- **Antivirus preventores:** su característica principal es una acción anticipatoria para evitar el ingreso de un programa malicioso al sistema, este tipo de antivirus se almacenan en la memoria y cuando la maquina inicia su actividad el antivirus realiza actividades como un escaneo total o parcial, es por ello que este tipo de software generalmente vuelven un poco lento a los sistemas.
- **Antivirus identificadores:** su función se retrata en su nombre, identificar a programas maliciosos para esto generalmente realizan un análisis de secuencias de bytes de los códigos que se encuentran relacionados con softwares maliciosos.
- **Antivirus descontaminadores:** el objetivo principal es la eliminación de los softwares maliciosos y además intentar reconstruir un estado en el cual el sistema se encontraba realizando sus actividades de forma normal antes de la infección, (procesos de autoconfiguración).

Existen otras formas de clasificar a los antivirus como: según su función, su objetivo específico o según su categoría.

La capacidad de los antivirus ha ido evolucionando volviéndose softwares mucho más elaborados con varias de las funciones mencionadas ya incluidas en un solo paquete.

- **Antimalwares.**

Un antimalware también realiza varias actividades similares a las de un antivirus sin embargo a pesar de que el termino malware contenga a todos los programas maliciosos un antimalware se ha desarrollado con la finalidad de proteger a los equipos de softwares maliciosos más específicos y más recientes en la red, una característica importante de este tipo de software es la capacidad de actualización específica, esto quiere decir que integra protecciones recientes y permite una protección actual ante nuevos programas atacantes, es aquí donde radica la diferencia entre un antivirus ya que un antivirus contiene una base de datos extensa sin embargo para programas maliciosos tradicionales como gusanos troyanos y virus.

1.3.3.2 HACKING ÉTICO

El hacking ético se refiere a la acción de una persona para utilizar sus habilidades en la informática con la finalidad de encontrar vulnerabilidades en su sistema de comunicaciones, posterior a determinar las vulnerabilidades se encarga de mitigarlas por medio de herramientas informáticas.

Sin embargo, no siempre las personas utilizan sus habilidades para contribuir al mejoramiento de la infraestructura informática, es aquí donde nace el concepto de Hacker y Cracker [26].

- **Hacker**: como un individuo que tiene amplios conocimientos referentes a la penetración de redes y sistemas de comunicación, sin embargo, su finalidad no es destructiva, ya que su actividad es regida por un proceso en el cual se necesita realizar estudio de cierta red o sistema de comunicación estas actividades pueden ser con permisos de administración y en un entorno controlado [26].
- **Cracker:** son individuos con grandes conocimientos informáticos y tiene la capacidad de vulnerar y aprovechar las debilidades de los sistemas con finalidades maliciosas o uso personal [26].

1.3.3.3 GESTIÓN DE SEGURIDAD DE LA RED.

Es importante mantener parámetros de gestión de seguridad por medio de especificaciones: técnicas operativas y procedimientos que permitan mantener un sistema cibernético seguro, para ello se deben tomar algunos parámetros a considerar como:

- **Puertos y Servicios.**

En la tabla 1.2. podemos encontrar tanto los requerimientos como algunas recomendaciones para la administración.

Tabla 1.2. Requisitos y medidas referentes a puertos y servicios [6]

Número	Requerimientos	Medidas
1	Realizar la habilitación de puertos y servicios específicos requeridos para el sistema, incluyendo rangos o servicios se requiera manejar puertos dinámicos	Se debe incluir, pero no limitarse a: • Documentación que demuestre la necesidad de la habilitación de los puertos y servicios. • Listado de los puertos, de forma selectiva y por grupos y los servicios que requieren ser habilitados. • Documentación de archivos de configuración de los dispositivos de red en los cuales se de validación a los puertos y servicios que se encuentren habilitados.
2	Proteger el uso físico de los puertos de entrada y salida innecesarios utilizados para la conectividad de la red comandos de la consola o medios extraíbles.	Para evidenciar se puede incluir la documentación que valide los tipos de protecciones del puerto, tanto físico como lógica.

- **Gestión de parches de seguridad.**

En la tabla 1.3. se presentan los requerimientos y medidas propuestas por el estándar NERC CIP-007-6 referentes a la gestión de parches de seguridad.

Tabla 1.3. Requerimientos y medidas referentes a parches y servicios [6]

Número	Requerimientos	Medidas
1	Mantener un procedimiento que permita la administración de los parches de seguridad, que debe incluir evaluación e instalación de parches, e identificar la fuente de la entidad que libera el parche.	Se debe incluir la siguiente información pero no debe limitarse, se debe presentar la validación de los parches de seguridad, que debe incluir almenas la versión del parche y evidenciar las mejoras respecto a su antecesor.
2	como periodo mínimo de 35 días se debe validar el funcionamiento del parche, esto implica verificar si la fuente ha liberado nuevas actualizaciones o se han	Para evidenciar se debe incluir los resultados de la evaluación del parche.

	presentado problemas de funcionalidad posterior a la aplicación del parche.	
3	Para realizar las aplicaciones del parche, una vez que se haya cumplido el numeral 2 se debe tomar una de las siguientes acciones: • Aplicar los parches. • Crear un plan de mitigación en caso de falla de funcionalidad tras la aplicación del parche. • Revisar un plan de mitigación existente. Los planes de mitigación deben incluir acciones planificadas de la entidad responsable para la mitigación de las vulnerabilidades corregidas por cada parche de seguridad y un marco de tiempo para completar estas mitigaciones.	Para evidenciar e debe incluir, pero no debe limitarse a: • Los registros de instalación del parche (como ejemplo: las exportaciones de las herramientas de gestión automática de parches que proporcionan fechas de instalación, la verificación de la versión del software, componentes del sistema o la exportación del registro que muestran el software instalado). • Un plan de fecha que debe presentar cuando y como se abordara la vulnerabilidad para incluir la documentación de las acciones a realizar por la entidad responsable para mitigar las vulnerabilidades corregidas por el parche.

- **Prevención de códigos maliciosos.**

En la tabla 1.4. se da a conocer los requerimientos y medidas propuestas por el estándar NERC CIP-007-6 referente a la prevención de códigos maliciosos.

Tabla 1.4. Requerimientos y medidas referente a la prevención de códigos maliciosos [6]

Número	Requerimientos	Medidas
1	Implementar el método o métodos para disuadir detectar y prevenir código malicioso.	Para evidenciar se debe incluir, pero no debe limitarse a: • la documentación que valide la utilización de antivirus, configuraciones de hardening en los dispositivos de red, políticas de seguridad, etc.

2	Mitigar la amenaza de código malicioso detectado.	Para evidenciar se debe incluir, pero no debe limitarse a: • los registros de los procesos de respuesta para la detección de códigos maliciosos. • Los registros de los resultados de estos procesos cuando existe la detección de los códigos maliciosos.
3	Para los métodos que se definieron en el numeral 1 se debe mantener un proceso para la actualización de firmas o patrones.	Para evidenciar se debe incluir, pero no debe limitarse a: • La documentación que valide el proceso utilizado para la actualización de firmas o patrones.

- **Monitoreo de eventos de seguridad.**

En la tabla 1.5. se da a conocer los requerimientos y medidas propuestas por el estándar NERC CIP-007-6 referente al monitoreo de eventos de seguridad.

Tabla 1.5. Requerimientos y medidas referente al monitoreo de eventos de seguridad [6]

Número	Requerimientos	Medidas
1	Mantener un registro de los eventos a nivel del sistema cibernético con la finalidad de realizar una investigación de los incidentes de seguridad, se de considerar al menos: • Detección de intentos de conexión con éxito. • Detección de intentos de acceso fallidos y de intentos de conexión fallidos • Detección de códigos maliciosos.	Para evidenciar se debe incluir, pero no debe limitarse a: • Un listado automático o manual de los incidentes de seguridad que se destacaron.
2	Generación de alertas para eventos de seguridad, se considerará al menos alertas generados por los incidentes:	Para evidenciar se debe incluir, pero no debe limitarse a: • Generación de un listado de forma automática o manual de las

	• Detección de códigos maliciosos. • Detección de intentos de conexión y accesos.	alertas generadas, que contenga los archivos de configuración que permitan identificar los parámetros de disparo para las alertas.
3	El almacenamiento de información histórica es importante durante al menos 90 días.	Para evidenciar se debe incluir, pero no debe limitarse a: • Registro de bitácoras y actas de revisión.
4	Se debe mantener un registro de todos los incidentes, con la finalidad de mantener bitácoras, las cuales se debe revisar durante intervalos no mayores a 15 días con la finalidad de identificar patrones que permitan identificar futuros ataques de seguridad.	Para evidenciar se debe incluir, pero no debe limitarse a: • Registro de bitácoras y actas y actas de revisión.

- **Sistema de control de acceso.**

En la tabla 1.6. se da a conocer los requerimientos y medidas propuestas por el estándar NERC CIP-007-6 referente al sistema de control de acceso.

Tabla 1.6. Requerimientos y medidas referente al sistema de control de acceso [6]

Número	Requerimientos	Medidas
1	Disponer de métodos de autenticación de acceso de usuarios, siempre que se considere técnicamente factible.	Para evidenciar se debe incluir, pero no debe limitarse a: • Documentación que describe como se autentica el acceso.
2	Identificar e investigar todas las cuentas genéricas, considerando si pertenecen a una localidad, sistema o grupo.	Para evidenciar se debe incluir, pero no debe limitarse a: • Generación de una lista de todas las cuentas genéricas.
3	Identificar a las personas que han autorizado el acceso a cuentas compartidas.	Para evidenciar se debe incluir, pero no debe limitarse a: • Generación de listas de cuentas compartidas y los individuos que realizaron la autorización del acceso a cada cuenta compartida.

4	Cambio de contraseña por defecto.	Para evidenciar se debe incluir, pero no debe limitarse a: • Procedimiento de cambio de contraseñas para dispositivos nuevos y los que se encuentren ya en operación. • Documentación de los dispositivos entregados por el proveedor, donde conste una validación de las contraseñas por defecto y se garantice que sean únicas y se dé a conocer a los usuarios, para cada dispositivo.
5	Para realizar la autenticación de las contraseñas de los usuarios se debe considerar los siguientes parámetros: • Se debe tener una contraseña de al menos 8 caracteres, o la cantidad máxima que soporte el dispositivo. • La contraseña debe tener un cierto grado de complejidad mínima donde se tenga: letras mayúsculas, minúsculas, números y un carácter.	Para evidenciar se debe incluir, pero no debe limitarse a: • Se debe tener como documentación capturas de pantalla del sistema que den paso a una validación de la complejidad de la contraseña. • Documentos de certificación que contengan referencias a los procedimientos que se han realizado para la configuración de la contraseña.
6	Se debe considerar el cambio de contraseñas al menos una vez en un periodo de 15 meses.	Para evidenciar se debe incluir, pero no debe limitarse a: • Informes generados por el sistema o capturas de la pantalla que den paso a la validación de la complejidad de la contraseña. • Se debe incluir el detalle de la referencia de los procedimientos que se realizaron para la configuración de la contraseña.
7	Si es técnicamente posible se debe considerar:	Para evidenciar se debe incluir, pero no debe limitarse a, documentación de configuración que permitan:

	• Se debe mantener un límite de intentos de declaración como fallidos para la autenticación. • Se debe realizar la configuración de alertas después de un máximo de intentos fallidos de autenticación.	• Validación de parámetros de bloqueo frente a un determinado número de intentos de autenticación fallidos.

1.3.5 CRITERIOS PARA LA EVALUACIÓN DE UNA RED LAN.

Para el desarrollo de los criterios de evaluación se toma como referencia a la norma IEC-61850-7, y en función de los requerimientos planteados en la metodología se procede a considerar parámetros de evaluación de la red LAN de una subestación eléctrica, el método que se elige para realizar la evaluación es el método denominado como evaluación forzada, sin embargo no es el único método e inclusive es posible utilizar programas que ayuden a determinar parámetros de red, tomando en cuenta que estos programas tienen costos elevados.

Posterior a considerar el método de evaluación se determinan factores críticos de la red para su posterior evaluación, estos factores se encontrarán dentro de tres bloques, estos tres bloques estarán estrechamente relacionados para su buen funcionamiento. Dichos bloques son denominados como:

- Análisis de la arquitectura física de la red LAN.
- Análisis de la administración y gestión de la red LAN.
- Análisis de las vulnerabilidades de la red LAN.

1.3.5.1 ANÁLISIS DE LA ARQUITECTURA FÍSICA DE LA RED LAN

En una red LAN de una subestación eléctrica es indispensable considerar enlaces redundantes y redundancia en los equipos, además de una arquitectura sólida que permita un buen funcionamiento de la red para ello se ha determinado los siguientes criterios:

- Redundancia de enlaces.
- Redundancia de switches.
- Redundancia de routers.
- Flexibilidad.
- Escalabilidad.
- Disponibilidad.

- Confiabilidad.

Después de haber determinado los criterios de evaluación de la arquitectura física se prosigue a determinar cuándo un criterio será excelente, bueno, deficiente e inexistente. Para ello tenemos:

Estructura de cómo se desarrollará el análisis.

I. Redundancia de enlaces.

- **Excelente:** cuando cumpla con la metodología y se presente una red con varios enlaces y además sea una arquitectura cerrada.
- **Buena:** cuando la arquitectura presente más de dos caminos por los cuales la información de puede trasladar de un equipo a otro.
- **Deficiente:** cuando la conexión de los equipos sea solo por un enlace y no se tenga una arquitectura cerrada.
- **Inexistente:** cuando no exista infraestructura de comunicación.

II. Redundancia de switches.

- **Excelente:** cuando cumpla con la arquitectura mencionada en la metodología.
- **Buena:** cuando cumpla con la arquitectura de la metodología, pero no se contemple colocar dos switches para los relés.
- **Deficiente:** cuando no se tenga una arquitectura establecida ni switches redundantes en la red.
- **Inexistente:** cuando la arquitectura sea concentrada y lodos los equipos se conecten a un solo switch.

III. Redundancia en el router.

- **Excelente:** cuando se tenga en la red dos equipos y se apliquen protocolos como VRRP.
- **Buena:** cuando se tengan dos equipos redundantes de frontera en la red.
- **Deficiente:** no aplica.
- **Inexistente:** cuando solo se tenga un equipo de frontera en la red.

IV. Flexibilidad.

- **Excelente:** cuando se pueda agregar más equipos que no necesariamente pertenezcan al mismo fabricante con facilidad.
- **Buena:** cuando se pueda agregar equipos de diferentes fabricantes, pero se limiten sus operaciones.
- **Deficiente:** cuando no exista compatibilidad entre los equipos y no sea posible agregar equipos de diferentes marcas.

- **Inexistente:** no aplica.

V. **Escalabilidad.**

- **Excelente:** cuando la red tenga la capacidad de añadir más equipos sin modificar la estructura de la red.
- **Buena:** cuando la red tenga la capacidad de añadir más equipos, pero se debe modificar la estructura de la red.
- **Deficiente:** cuando se deban realizar cambios que modifiquen en su totalidad la estructura de la red.
- **Inexistente:** cuando en la red no se tenga la capacidad de añadir un equipo más.

VI. **Disponibilidad.**

- **Excelente:** cuando todos los equipos de la red se encuentren en línea, y la red no salga de comunicaciones en un periodo de tiempo de 0 a 6 minutos por año.
- **Buena:** cuando todos los equipos de la red se encuentren en línea y la red no salga de comunicaciones en un periodo de tiempo de 7min a 1 hora por año.
- **Deficiente:** cuando todos los equipos de la red se encuentren en línea y la red no salga de comunicaciones en un periodo de tiempo de 1 hora a 9 hora por año.
- **Inexistente:** no aplica.

VII. **Confiabilidad.**

- **Excelente:** cuando la comunicación en la red no presente intermitencia.
- **Buena:** no aplica
- **Deficiente:** cuando la red sea intermitente y la aplicación de comandos de comunicación no se ejecuten instantáneamente y se tenga que aplicar varias veces.
- **Inexistente:** cuando no hay respuesta de comunicaciones entre los equipos.

1.3.5.2 ANÁLISIS DE ADMINISTRACIÓN Y GESTIÓN DE LA RED LAN

Para el análisis de la administración y gestión se analizará los siguientes criterios:

Estructura de cómo se desarrollará el análisis.

I. **Topología.**

- **Excelente:** cuando se ha definido una arquitectura específica a una red de comunicaciones en una subestación eléctrica.
- **Bueno:** cuando se tenga una arquitectura y esta no necesariamente este orientada a las redes de comunicaciones en subestaciones eléctricas.
- **Deficiente:** cuando se tenga presente equipos de comunicación interconectados comunicando a la subestación, pero sin criterios de diseño de topología de redes de comunicación para una subestación eléctrica.

- **Inexistente:** cuando no presente una infraestructura de comunicación.

II. **Redundancia física.**

- **Excelente:** cuando la red de comunicaciones cuente con enlaces redundantes y equipos redundantes en puntos críticos, que permitan más de dos caminos por donde la comunicación se transfiera.
- **Bueno:** cuando la red presente enlaces redundantes entre los dispositivos.
- **Deficiente:** cuando la información solo tenga un camino para comunicarse entre otros dispositivos.
- **Inexistente:** no presente una infraestructura de comunicaciones.

III. **Redundancia lógica.**

- **Excelente:** cuando presente configuraciones de redundancia entre los enlaces y además configuraciones de PAgP en CISCO o LACP.
- **Bueno:** cuando presente configuraciones de redundancia.
- **Deficiente:** cuando no presente configuraciones de redundancia.
- **Inexistente:** cuando no presente una infraestructura de comunicación.

IV. **Direccionamiento.**

- **Excelente:** cuando todo equipo que se encuentre en la red haya sido direccionado.
- **Bueno:** cuando los equipos críticos como relés y medidores mantengan un direccionamiento.
- **Deficiente:** cuando el direccionamiento sea parcial en los equipos de la red de comunicaciones de la subestación.
- **Inexistente:** cuando ningún equipo de la red de la subestación se encuentre asignado una dirección.

V. **Configuraciones de enrutamiento.**

- **Excelente:** cuando se tiene configuraciones de enrutamiento estático.
- **Bueno:** cuando presenta configuraciones sean estáticos o dinámicos.
- **Deficiente:** cuando no se haya establecido configuraciones de enrutamiento.
- **Inexistente:** cuando no presente equipos de enrutamiento.

VI. **Configuraciones administrativas básicas.**

- **Excelente:** cuando se tengan configuraciones no por defecto del equipo, referentes a configuraciones como tiempo de acceso de usuario, numero de intentos para ingresar al equipo y todas las configuraciones que se permitan en el equipo.
- **Bueno:** cuando existe una configuración parcial del equipo.
- **Deficiente:** cuando las configuraciones se encuentren por defecto.
- **Inexistente:** cuando no presente configuraciones básicas.

VII. Credenciales.

- **Excelente:** cuando las credenciales cumplan con las recomendaciones dela metodología.
- **Bueno:** cuando las credenciales cumplan parcialmente los requerimientos de la metodología.
- **Deficiente:** cuando las credenciales se encuentren por defecto.
- **Inexistente:** cuando no existan credenciales.

VIII. Protocolos de sincronización de red.

- **Excelente:** cuando en todos los equipos se encuentre configurado un protcolo de sincronización, y cumpla con la metodología.
- **Bueno:** cuando en la red no se tenga un servidor de sincronismo, pero las actualizaciones se las realice manualmente de forma periódica.
- **Deficiente:** cuando no existan configuraciones de sincronización de forma parcial en los equipos de la red.
- **Inexistente:** cuando no se configure protocolos de sincronización en ninguno de los equipos de la red.

IX. Configuraciones de seguridad de red.

- **Excelente:** cuando se presente un firewall y restricciones de acceso hacia la red interna de la subestación y cumpla con la metodología.
- **Bueno:** no aplica.
- **Deficiente:** cuando se presenta configuraciones por defecto de seguridad.
- **Inexistente:** cuando no se presente ninguna restricción para acceder hacia los equipos de la red de la subestación.

X. Estado de uso de memoria y CPU de equipos.

- **Excelente:** cuando el porcentaje de los recursos del equipo son menores al 50%.
- **Bueno:** cuando el porcentaje de los recursos del equipo se encuentran entre 50% y 70%.
- **Deficiente:** cuando el porcentaje de los recursos del equipo se encuentran entre 70% y 85%.
- **Inexistente:** no aplica.

XI. Configuraciones de calidad de servicio.

- **Excelente:** cuando se encuentran configuraciones de calidad de servicio según la metodología.
- **Bueno:** cuando se presenta configuraciones parciales de configuración de calidad de servicio.

- **Deficiente:** cuando
- **Inexistente:** cuando no presenta configuraciones de calidad de servicio en la red.

XII. Políticas de seguridad.

- **Excelente:** cuando se tiene una metodología y se la cumple, referente a políticas de seguridad.
- **Bueno:** no aplica.
- **Deficiente:** cuando se tiene una documentación referente a políticas de seguridad, pero no se aplica, o su aplicación es de forma parcial.
- **Inexistente:** cuando no se tiene una guía o documentación de políticas de seguridad y no se aplica ningún lineamiento.

XIII. Procedimientos de administración y gestión.

- **Excelente:** cuando se tiene una metodología que permita mantener un procedimiento de administración y gestión en la red de forma adecuada.
- **Bueno:** no aplica.
- **Deficiente:** cuando se tiene una documentación referente a administración y gestión, pero no se aplica, o su aplicación es de forma parcial.
- **Inexistente:** cuando no se tiene una guía o documentación de administración y gestión y no se aplica ningún lineamiento.

1.3.5.3 ANÁLISIS DE VULNERABILIDADES DE LA RED LAN

Existen varios métodos para evaluar las vulnerabilidades de un sistema de comunicaciones, sin embargo, el análisis de vulnerabilidades por medio de la habilitación de puertos es un buen referente a la hora de identificar falencias de seguridad en la red. Para el análisis de vulnerabilidades por medio de puertos existen varios programas uno de ellos es NESSUS, este software analiza a cada uno de los dispositivos de la red que se encuentren direccionados y el método que usa es un análisis por medio de puertos, esto ayudara a identificar los puertos que se encuentren habilitados y los servicios que conllevaría la habilitación de cada puerto, además de una detallada información de las vulnerabilidades que pueden ser explotadas y posibles soluciones.

1.3.6 SOFTWARES PARA EL ANÁLISIS DE REDES DE COMUNICACIÓN.

1.3.4.1 Software orientado al análisis de las seguridades cibernéticas en redes de comunicación.

En la actualidad existen gran variedad de programas que permiten obtener un análisis de vulnerabilidades en las redes, estos programas ayudan a los administradores a corregir

falencias dentro de un sistema de comunicación, la importancia del uso de estos elementos radica en la mitigación de problemas de [25]:

- Programación.
- Actualización de protocolos.
- Actualización de certificaciones.
- Evaluación del estado del sistema.
- Métodos para explotar vulnerabilidades.
- Puertos y servicios críticos, entre otras características que dependerán del analizador.

En el mercado tenemos algunos programas que permitan analizar las redes de comunicación.

Estos programas también son conocidos como sniffer ya que capturan las tramas que circulan en la red, la interpretación de cada programa dependerá de su orientación, para que fue creado. Existen algunos programas en el mercado sin embargo un software destacado es NESSUS.

Software para analizar vulnerabilidades usando la metodología de puertos y servicios activos NESSUS.

Nessus es un software de la casa Tenable, este programa está orientado a la detección de vulnerabilidades en las redes y en los equipos que se encuentran conectados en la red, Nessus realiza un escaneo de los puertos que se encuentren abiertos. Posteriormente ejecuta una explotación de estas vulnerabilidades. Nessus ejecuta una lista de plugins que son escritos en NASL (Nessus Attack Scriting Language). Posteriormente el programa nos presenta sus resultados en formato de texto.

Es importante tener cuidado a la hora de la ejecución de este software ya que puede causar que los equipos se saturen y salgan de servicio.

En la figura1.11. se presenta una imagen típica de resultados del análisis de vulnerabilidades usando Nessus.

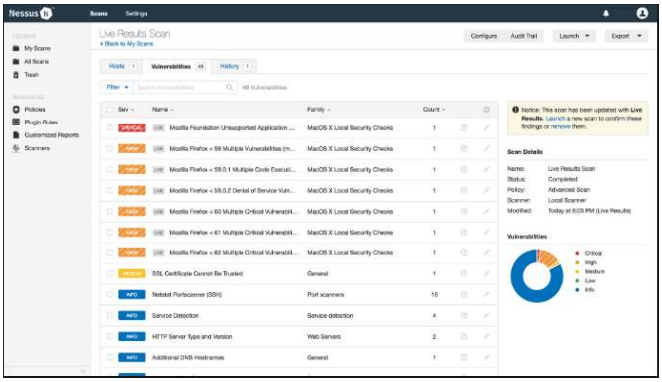

Figura 1.11. Presentación de resultados del análisis de vulnerabilidades por Nessus [13]

Software orientado a evaluación de las redes de comunicación.

Los analizadores de redes son programas creados para capturar tramas que circulan dentro de una red son conocidos también como sniffer, estos programas se pueden usar para varias actividades, esto dependerá de las intenciones de las personas, sin embargo, sus usos principales son:

- Captura de información sin cifrar para obtener nombres de usuario y contraseñas.
- Captura de tramas, con el objetivo de encontrar fallas de comunicación, fallos de conectividad, fallas de interpretación de protocolos, entre otros usos.
- Realizar evaluaciones del estado de la red.

Los sniffer son programas de mucha utilidad para realizar una buena administración de la red, en el mercado se encuentra una gran variedad de programas que permiten realizar estas actividades.

2. METODOLOGÍA

En la actualidad EMELNORTE cuenta con la concesión de dieciséis subestaciones eléctricas las cuales hace dos años han pasado a tener una administración centralizada, ya que se implementó un sistema SCADA el cual ha permitido que las operaciones y maniobras se las ejecute desde un centro de control, el cual se encuentra en la ciudad de Ibarra. Sin embargo, en cada una de las subestaciones eléctricas no se ha establecido lineamientos de arquitectura, administración y parámetros de seguridad en la red LAN de las subestaciones eléctricas.

Debido a que EMELNORTE no ha realizado o aplicado una norma o metodología que permita establecer una estandarización de la infraestructura informática por ello es importante realizar un análisis del estado actual de las redes LAN de las subestaciones de la concesión de EMELNORTE.

Sin embargo, al proceder a realizar el levantamiento de información se evidencia que todas las redes LAN de las subestaciones mantienen la misma estructura de administración gestión y seguridad, además de las mismas arquitecturas, es por ello que se considera realizar el análisis minucioso en una de estas redes sin importar alguna particularidad en la elección.

Se elige la subestación eléctrica EL RETORNO en donde se procede a realizar un levantamiento de información completo y un análisis minucioso de las condiciones en las que se encuentra la red de comunicaciones. Para ello se evaluará la arquitectura de la red, administración y gestión y así como la seguridad de la red.

2.1 LEVANTAMIENTO DE INFORMACIÓN Y ANÁLISIS DEL ESTADO ACTUAL DE LA SUBESTACION EL RETORNO.

El presente levantamiento de información y análisis se realizó para la subestación eléctrica EL RETORNO que se encuentra en operación a cargo de la empresa eléctrica EMELNORTE S.A., con la finalidad de constatar cómo se encuentra la arquitectura física, arquitectura lógica, administración, gestión y seguridad de la red de comunicaciones de la subestación eléctrica. La subestación se encuentra ubicada en la avenida Atahualpa en la ciudad de Ibarra-Ecuador, a continuación, se detalla y se describe la organización, estructura y estado actual en la que se encuentra la subestación.

2.1.1 RED LAN DE LA SUBESTACIÓN EL RETORNO.

En esta sección se presenta direccionamientos IP censurados por seguridad de la red de comunicaciones de la subestación eléctrica EL RETORNO.

2.1.1.1 Arquitectura física de la red LAN de la subestación EL RETORNO.

La subestación eléctrica EL RETORNO cuenta con la arquitectura fisica de comunicaciones detallada en la figura 2.1. donde se puede apreciar en la parte inferiror de la figura que existe un equipo que concentra todos los reles y medidores, y en la parte superior se encuentra el concentrador de datos, ademas se aprecia que los equipos switch #1-2-3 no realizan ninguna actividad.

Si bien el alcance de este proyecto no abarca la red WAN, es importante mecionar ciertas caracteristicas que ayudaran con el desarrollo de este proyecto. Asi tenemos:

- Por la red WAN circula el tráfico tanto del sistema SCADA como datos corporativos como audio, video y mensajeria.
- La red WAN que se encuentra en Ibarra esta comunicada por medio de fibra óptica y pertenece a EMELNORTE.
- Las subestaciones fuera de la ciudad de Ibarra se comunican por medio de una VPN contratada por la Corporación Nacional de Telecomunicaciones (CNT).
- No existe una distinción física ni lógica entre la información corporativa con la información generada por el sistema SCADA.
- Las mediciones de ancho de banda fueron otorgadas por el personal de TICs de EMELNORTE y se encuentran alrededor de 30Kbit/s.

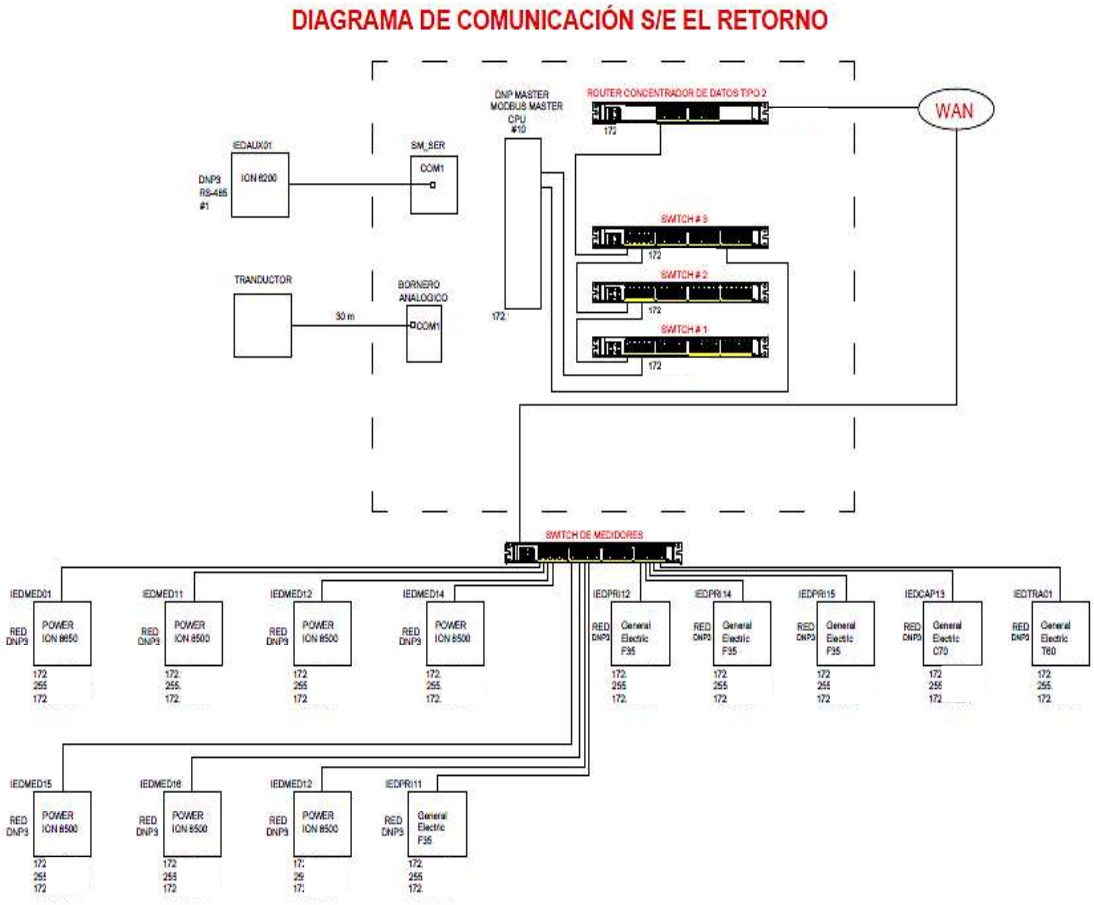

Figura 2.1. Diagrama de conexión actual de la red LAN de la subestación EL RETORNO

2.1.1.2 Arquitectura lógica de la red LAN de la subestación EL RETORNO.

La red LAN de la subestación EL RETORNO se encuentra estructurada acorde al direccionamiento mostrado en la tabla 2.1. donde se presenta la dirección de red, el prefijo, la máscara, direcciones IP disponibles y la puerta de enlace.

Tabla 2.1. Direccionamiento de la subestación EL RETORNO

RED	PREFIJO	MASCARA	IP INICIAL	IP FINAL	PUERTA DE ENLACE
172.17.58.XX	/24	255.255.XX.XX	172.17.58.XX	172.17.58.XX	172.17.58.XX

El direccionamiento que se encuentra en la subestación EL RETORNO es tipo “C” con mascara /24, este direccionamiento se encuentra establecido en cada uno de los equipos

que conforman la red de comunicaciones de la subestación eléctrica EL RETORNO, el direccionamiento se presenta en la tabla 2.2.

Tabla 2.2. Direccionamiento de la subestación EL RETORNO

NRO	MARCA	ION	EQUIPO	IP	MASK	MASK	GATEWAY
1	SCHNEIDER	8500	CIRCUITO R1	172.	/24	255	172
2	SCHNEIDER	8500	CIRCUITO R2	172.	/24	255	172
3				172.	/24	255	172
4	SCHNEIDER	8500	CIRCUITO R4	172.	/24	255	172
5	SCHNEIDER	8500	CIRCUITO R5	172.	/24	255	172
6	SCHNEIDER	8600	CIRCUITO CAPACIT	172.	/24	255	172
7	SCHNEIDER	8600	CIRCUITO GENERA	172.	/24	255	172
8				172.	/24	255	172
9				172.	/24	255	172
10				172.	/24	255	172
11	GE RELAY	F35	CIRCUITO R1	172.	/24	255	172
12	GE RELAY	F35	CIRCUITO R2	172.	/24	255	172
13				172.	/24	255	172
14	GE RELAY	F35	CIRCUITO R4	172.	/24	255	172
15	GE RELAY	F35	CIRCUITO R3	172.	/24	255	172
16	GE RELAY	C70	-	172.	/24	255	172
17	GE RELAY	T60	CIRCUITO TRA01	172.	/24	255	172
18				172.	/24	255	172
19				172.	/24	255	172
20			CONCENTRADOR	172.	/24	255	172
21			SW1	172.	/24	255	172
22			SW2	172.	/24	255	172
23			SW3	172.	/24	255	172
24			GATEWAY E3	172.	/24	255	172
25			GATEWAY E6	172.	/24	255	172
26	TSI		INVERSOR	172.	/24	255	172

2.1.2 ELEMENTOS ACTIVOS DE LA RED LAN DE LA SUBESTACIÓN EL RETORNO.

En la tabla 2.3. se detalla los equipos que se encuentran en funcionamiento en la subestación EL RETORNO.

Tabla. 2.3. Elementos que conforman la red LAN de la subestación EL RETORNO

Cantidad	Equipo	Marca	Modelo	Característica	Observación
1	Switch	General Electric	ML2400	Puertos de fibra y cobre.	Conexión de relés no se encuentra asignada una dirección IP.
3	Switch	GarrettCom	Magnum 6KL	4 puertos cobre RJ45, 4 puertos fibra óptica LC	Redundantes
1	Router	GarrettCom	DX940	4 puertos cobre RJ45, 2 puertos abiertos SFP	Concentrador de datos tipo 2
4	IED	General Electric	8500		Medición datos eléctricos
2	IED	General Electric	8600		Medición datos eléctricos
4	IED	General Electric	F35		Relé protección
1	IED	General Electric	T60		Relé transformador
1	IED	General Electric	C70		Relé de los capacitores

1	CPU maestro DNP	Schneider Electric	CPU866		
1	CPU maestro	ASAT			No se encuentra en operación pero forma parte de la red
1	Pantalla táctil	Intel	ipcc6172A		

En la figura 2.2. podemos observar el rack donde se encuentran los equipos de comunicación industrial de la subestación EL RETORNO.

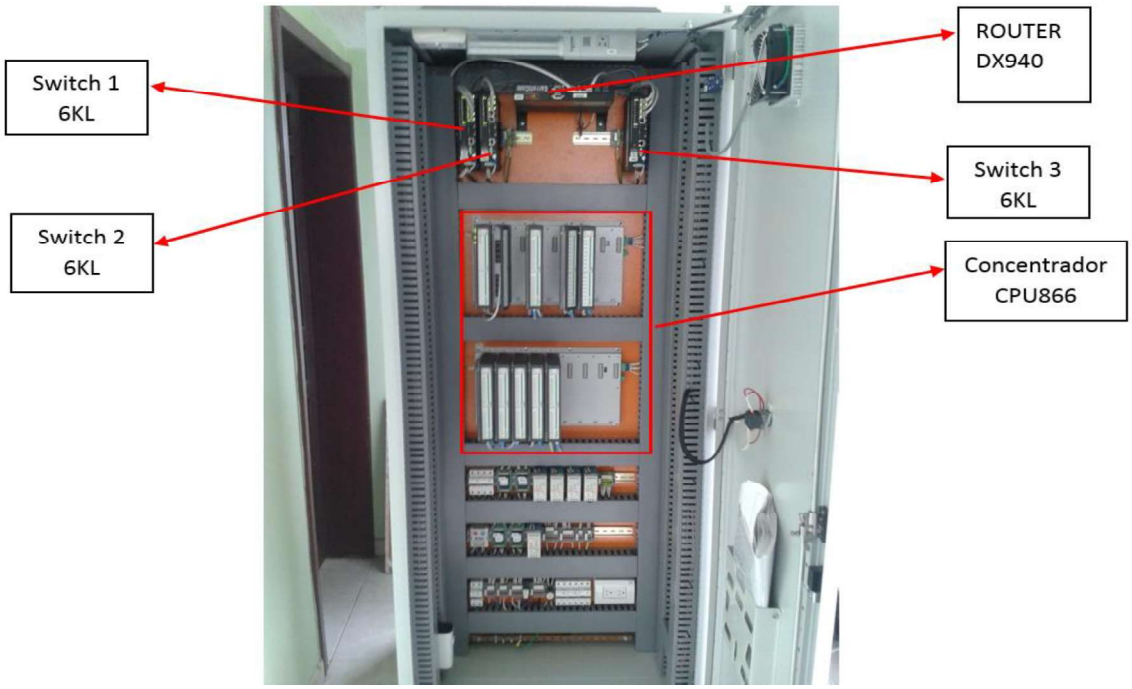

Figura 2.2. Concentrador de datos de la subestación EL RETORNO

En la figura 2.3. se muestra el rack de comunicaciones que se encuentra en la caseta se la subestación EL RETORNO.

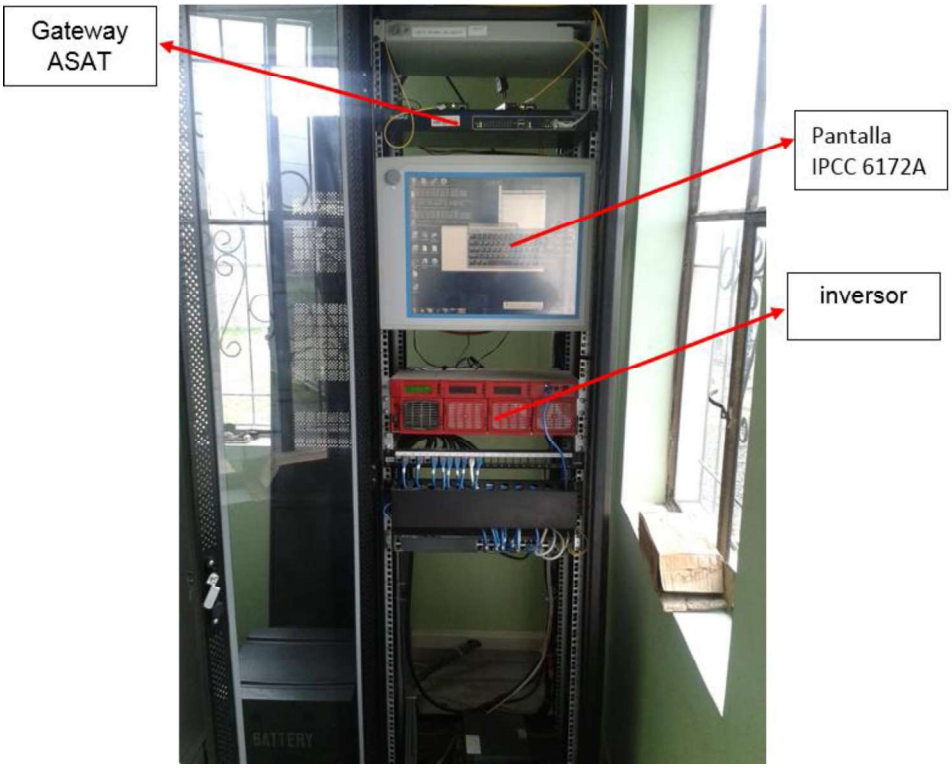

Figura 2.3. Rack de comunicaciones de la subestación EL RETORNO

2.1.1.1 Switch General Electric ML2400

En la figura 2.4. se puede observar el switch que se encuentra operativo en la subestación EL RETORNO, en este equipo se conectan todos los relés de la subestación por medio de fibra óptica.

Figura 2.4. Switch de la subestación EL RETORNO [29]

Sus características generales son:

- El equipo puede admitir hasta 32 puertos RJ45 de cobre de 10/100Mb.
- 12 puertos con conectores tipo LC, MTRJ de fibra óptica.
- 8 puertos de fibra o cobre de 1 Gb.
- Es posible el montaje de los puertos en la parte frontal o posterior.

- Tiene doble fuente de alimentación, esta puede ser DC o AC universal.
- Tiene la capacidad de configurar VLANs.
- Configuraciones de QoS.

2.1.1.2 Switch GarretCom Magnum 6KL [14].

En la figura 2.5. se puede observar el switch que se encuentra operativo en la subestación EL RETORNO, el equipo se encuentra comunicando el concentrador de datos.

Figura 2.5. Switch de la subestación EL RETORNO [14]

Sus características generales son:

- Switch para trabajo en ambientes industriales.
- Cuenta con 4 puertos de cobre 10/100 (regulados por PoE).
- Cuenta con 4 puertos de fibra óptica de 100Mb.
- 2 puertos Gb que pueden configurarse como puertos SFP.
- Administración SNMP v2, v3.
- Priorización de QoS 802.1p.
- Capacidad de realizar VLANs.
- Configuración de puertos por medio de RSTP-2004.

2.1.1.3 Router GarretCom DX940 [15].

En la figura 2.6. se puede observar el router que se encuentra operativo en la subestación EL RETORNO, el equipo se encuentra comunicando la CPU del concentrador de datos.

Figura 2.6. Router de la subestación EL RETORNO [15]

Sus características generales son:

- Presenta una alta velocidad por medio de comunicaciones celulares, (interfaz WAN celular 3G).
- Tiene puertos Ethernet Gb, 100Mb y cuatro puertos serie.
- Permite la transferencia de datos por medio de VPN en base a la norma NERC-CIP.
- Presenta funciones de seguridad IPsec/VPN (incluidos los tuneles GRE para VPN), firewall de estado, RADIUS, syslog, Secure Seal SSL, reenvio de puertos SSH y otras seguridades por medio de una licencia MNS-DX-SECURE.
- Contiene funciones de firewall IP que incluye: inspección, filtración de direcciones y puertos.
- Cifrado AES y certificados de clave compartida (PSK) Y X.509.
- Enrutamiento OSPF BGP se puede habilitar mediante la licencia del software MNS-DX-ADVAR.
- Cumple con especificaciones IEEE 1613 E IEC 61850-3 orientado a la protección EMI/ESD.
- Cumple con IP52 y protección contra humedad y corrosión.

2.1.1.4 Relé General Electric F35 [17].

En la figura 2.7. se puede observar el relé que se encuentra operativo en la subestación EL RETORNO, el equipo es el encargado de comandar las funciones de cierre y apertura para los diferentes circuitos de la subestación eléctrica.

Figura 2.7. Relé de la subestación EL RETORNO [17]

Sus características generales son:

- Usa el estándar IEC61850-9-2, permitiendo la interoperabilidad, optimización de la administración del dispositivo.
- Permite mantener comunicaciones de mensajería como GOOSE.
- Permite realizar una comunicación por medio de RS485 y RS485(Modbus RTU, DNP)

2.1.1.5 Relé General Electric T60 [18].

En la figura 2.8. se puede observar el relé que se encuentra operativo en la subestación EL RETORNO, y es el encargado de comandar la apertura o cierre del transformador de la subestación eléctrica.

Figura 2.8. Relé operativo en la subestación EL RETORNO [18]

Sus características generales son:

- Seguridad en la protección con transformadores, compatibilidad con IEEE C37.91.
- Cumplimiento del estándar IEC 61850 ed. 1 y ed. 2 implementaciones certificadas.

- Configuraciones a través de archivos SCL, e interoperabilidad con el uso de IEC 61850-9-2.
- Comunicación por medio de mensajería tipo GOOSE.
- Contiene tres puertos de fibra optica o cobre, independientes.
- Contiene seguridad cibernética de acuerdo al estándar NERC-CIP, AAA, Radius, RBAC, Syslog.

2.1.1.6 IED Schneider 8500 (medidor) [16].

En la figura 2.9. se observa el medidor que se encuentra en la subestación EL RETORNO, El equipo está orientado a realizar mediciones de voltaje, corriente, potencia y frecuencia de cada uno de los circuitos de la subestación eléctrica.

Figura 2.9. Medidor de la subestación EL RETORNO [16]

Sus características generales son:

- Su comunicación se la realiza por medio de los protocolos RS232 o RS485.
- Comunicación ethernet 10Mbps.
- Comunicaciones como telnet, Modbus/TCP.
- Funciona como servidor SMTP.

2.1.1.7 IED Schneider 8600 (medidor) [19].

En la figura 2.10. se observa el medidor que se encuentra en la subestación EL RETORNO, este equipo es un medidor de calidad de energía orientado a las redes de servicios públicos.

Figura 2.10. Medidor operativo de la subestación EL RETORNO [19]

Sus características generales son:

- El equipo puede manejar protocolos como DNP3, ION, Telnet, el estándar IEC61850, TCP/IP y Modbus.
- Los puertos de comunicación que maneja son: RS485, thernet RJ45, infrared, RS485/RS232 sub-D 9.

2.1.1.8 IED General Electric C70 (relé) [20].

En la figura 2.11. se observa el equipo que está orientado a la protección y control de los bancos de capacitores.

Figura 2.11. Relé operativo en la subestación EL RETORNO [20]

Sus características generales son:

- Cumple con el estándar IEC 60870-5-104, referentes a la interoperabilidad.
- Presenta un perfil de comunicación por medio del protocolo DNP v3, protocolo Modbus RTU.
- Tiene puertos de conexión como RS232/RS485 y puerto ethernet.

2.1.1.9 CPU maestro DNP Schneider Electric CPU 866 [26].

En la figura 2.12. se observa el concentrador de datos modular, el cual se encuentra operativo en la subestacion EL RETORNO, este equipo concentra la informacion de los medidores y reles de la subestacion, posteriormente seran enviados a los servidores que se encuentran en las instalaciones del centro de control.

Figura 2.12. Concentrador DNP CPU866

Sus características generales son:

- Unidad de procesamiento 32-bit micro-power MPC 90 MHz.
- Memoria flash 16*32MB.
- Memoria RAM estática 512KB-4MB.
- RAM estática backup bacteria/supercapacitor.
- RAM dinámica 32-128MB.
- Canal consola RS-232.
- Conexión canal RJ45.

2.1.1.9 PANTALLA ADVANTECH IPCC6172A.

En la figura 2.13. se observa la pantalla tactil que se encuentra en la subestación EL RETORNO.

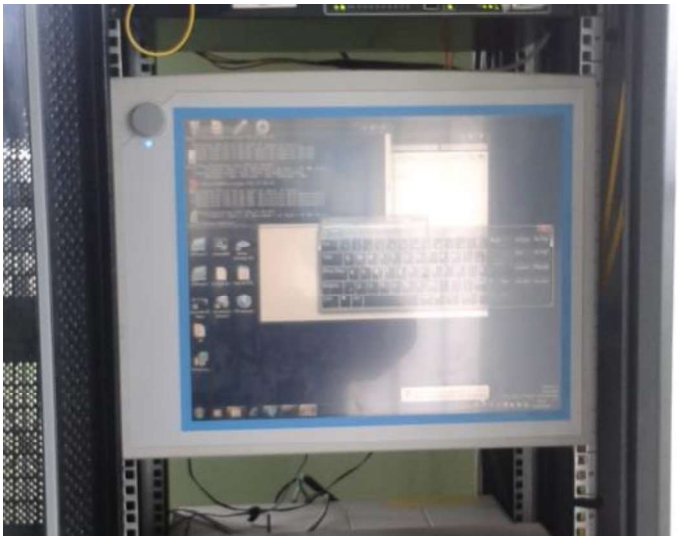

Figura 2.13. Pantalla táctil operativa de la subestación EL RETORNO

Sus características generales son:

- La pantalla advantech ipcc6172A es una computadora con características industriales.
- Presenta un procesador Intel core 2 Duo CPU 2.8GHz.
- Sistema operativo Windows 7 Professional, service Pack 1.
- Memoria Ram 4GB.
- Este equipo se encuentra como elemento de soporte para realizar diferentes actividades administrativas dentro de la red de la subestación EL RETORNO.

2.2 ANÁLISIS DE SEGURIDAD Y EVALUACION DE LA RED

Es necesario determinar cómo se encuentra inicialmente estructurada la red, para poder establecer el estado de su arquitectura física, administración, gestión y seguridad cibernética, a continuación se ha planteado los siguientes pasos:

I. Se analizará la arquitectura que se encuentra establecida en la red de comunicaciones de la subestación EL RETORNO.

II. Se efectuará pruebas de conectividad desde el centro de control y se determinara los medios de comunicación remota que se encuentran activados.

III. Se ejecutará un análisis referente a la administración y gestión que se encuentra implementado en la red de comunicaciones de la subestación EL RETORNO.

IV. Finalmente, se ejecutará un análisis de vulnerabilidades utilizando el software NESSUS.

2.2.1 ANÁLISIS DE LA ARQUITECTURA DE LA RED LAN DE LA SUBESTACIÓN EL RETORNO.

En base a la figura 2.1. podemos determinar el tipo de arquitectura que presenta la red de la subestación EL RETORNO, la cual presenta las siguientes características:

- La arquitectura es simple centralizada.
- No presenta enlaces físicos redundantes en los switches.
- No presenta enlaces físicos redundantes en el router.
- Los IEDs se encuentran centralizados en un solo switch.
- La arquitectura no es escalable.
- La arquitectura es poco flexible para realizar cambios.
- Existen equipos que se encuentran operativos pero que no realizan ningún aporte a la red como un concentrador de marca ASAT el cual no realiza ninguna actividad.
- La red se encuentra con una disponibilidad del 99.99% ya que ha salido de operación alrededor de 52.6 minutos/año.

RESULTADOS GLOBALES DEL ANÁLISIS DE LA ARQUITECTURA FÍSICA DE LA RED LAN DE LA SUBESTACIÓN EL RETORNO.

En la tabla 2.4. se observan los resultados obtenidos posterior al análisis de la arquitectura física de la red LAN de la subestación EL RETORNO. Es importante mencionar que los criterios para realizar el análisis se encuentran en el numeral 1.3.5.

Tabla 2.4. Resultados de la evaluación de la arquitectura física de la red LAN EL RETORNO

#	DESCRIPCIÓN	ESTADO			
		Excelente	Buena	Deficiente	Inexistente
1	Redundancia de enlaces.			✓	
2	Redundancia de switch.				✓
3	Redundancia de router.				✓
4	Flexibilidad.			✓	
5	Escalabilidad			✓	
6	Disponibilidad			✓	
7	Confiabilidad			✓	

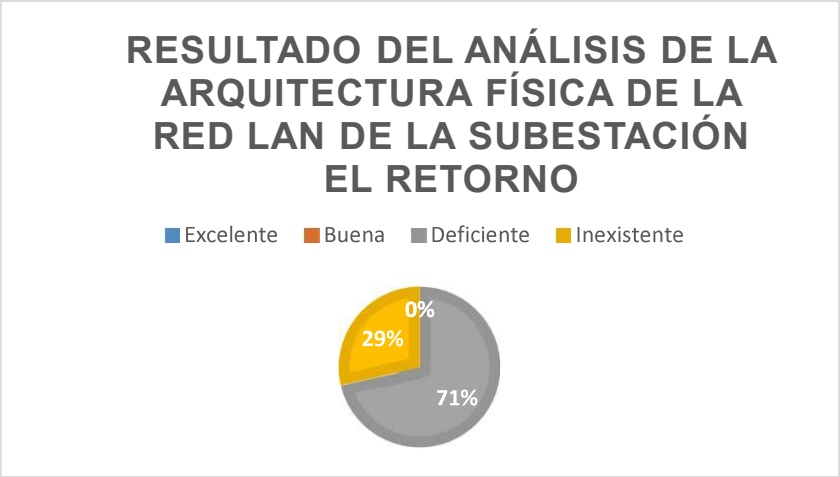

Figura 2.14. Resultados globales del análisis de arquitectura de la red LAN de la subestación EL RETORNO

2.2.2 PRUEBAS DE CONECTIVIDAD.

Las pruebas de conectividad se desarrollaron con la finalidad de comprobar el estado de los equipos al realizar o establecer un enlace de comunicación entre un equipo dentro de la red de EMELNORTE. La comunicación se desarrolló desde una computadora que no necesariamente pertenece a fines administrativos técnicos. Las pruebas de conexión desarrolladas se las realizo por medio de tres métodos:

- Comunicación por medio de escritorio remoto.
- Comunicación por medio de un cliente.
- Comunicación por medio del browser.

2.2.2.1 Comunicación por medio de escritorio remoto.

Se realiza la prueba de comunicación remota por medio de escritorio remoto, usando una computadora que se encuentra en la subestación el retorno que forma parte de los equipos que se encuentran en la red LAN de la subestación.

En la figura 2.15. se observa la dirección del equipo dentro de la subestación al cual deseamos establecer comunicación y en la figura 2.16. se ingresa la contraseña.

Figura 2.15. Conexión por escritorio remoto

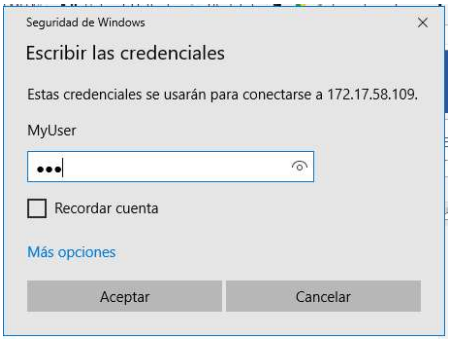

Figura 2.16. Ingresamos la clave de acceso

Se pudo realizar el ingreso hacia el computador sin restricción ya que la clave de acceso cuenta con un número de caracteres bajo.

En la figura 2.17. se observa la pantalla advantech ipcc6172A que se encuentra en las instalaciones de la subestación EL RETORNO.

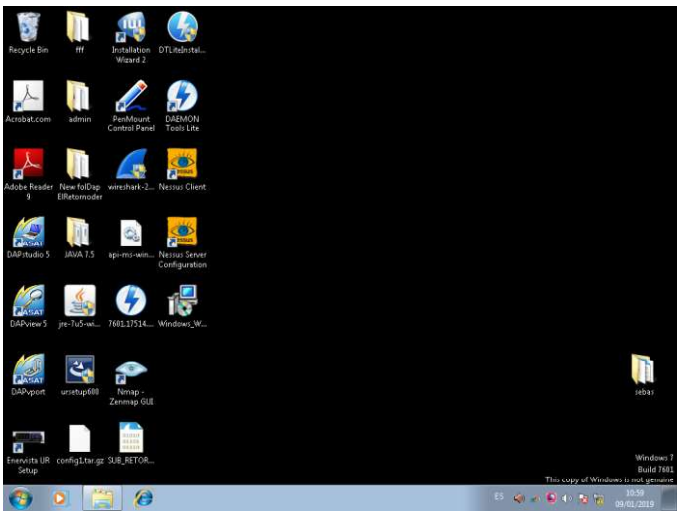

Figura 2.17. Pantalla advantech ipcc6172A

2.2.2.2 Comunicación por medio de un cliente.

El cliente que se escogió para realizar esta prueba de comunicación es Putty, el cual nos permite establecer una comunicación remota por medio de diferentes protocolos tales como: Raw, Telnet, Rlogin SSH y serial.

En la figura 2.18. se aprecia la ventana que nos presenta el cliente Putty.

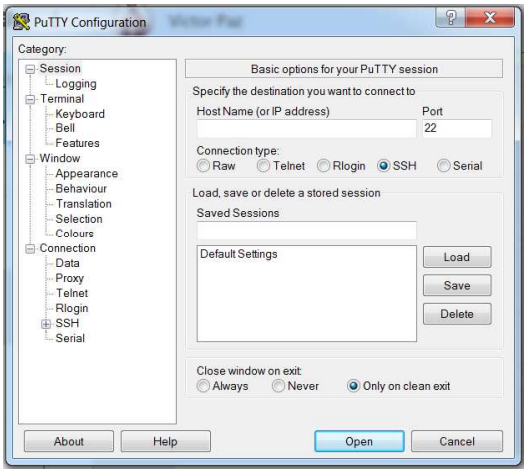

Figura 2.18. Interfaz de Putty

- Intentamos realizar una comunicación por medio de SSH que es un protocolo de comunicación remota cifrada que utiliza el puerto 22 sin embargo no fue posible mantener comunicación por medio de dicho protocolo ya que no presenta la posibilidad de habilitar dicho protocolo, así que se realizó la comunicación por medio de Telnet.
- Se plantea realizar comunicaciones básicas a puntos clave de la red de la subestación el Retorno, estos puntos clave son: el concentrador de datos y el switch que concentra a los IEDs. En la figura 2.19. se puede observar que se logra mantener una comunicación por medio del protocolo Telnet a la dirección 172.17.58.xx correspondiente a la dirección asignada al concentrador de datos de la subestación, a pesar de que el router mantiene una seguridad básica donde pide al usuario, una clave y un tiempo de repulsión al intentar el ingreso de la clave por 3 ocasiones.

Figura 2.19. Ingreso por Telnet

- En la figura 2.20. se observa que existe comunicación por medio del protocolo Telnet hacia el switch de dirección 172.17.xx.xx, que concentra los IEDs, a

diferencia del router éste nos otorga mayor cantidad de información como la marca del dispositivo, la versión que se encuentra instalada entre otro tipo de información, se puede observar que también mantiene una configuración de seguridad básica donde pide usuario, clave y realiza la denegación de acceso temporal al ingresar la clave por 3 ocasiones.

Figura 2.20. Pantalla de telnet al switch

- Se realiza una última prueba de conectividad por medio del cliente Putty hacia uno de los medidores del circuito, los resultados se pueden observar en la figura 2.21, en la cual se observa que nos presenta una pequeña descripción del equipo que se está comunicando con el cliente, posteriormente observamos que también presenta configuración de seguridad básica.

Figura 2.21. Pantalla de Telnet al medidor

2.2.2.3 Comunicación por medio de Browser.

Para realizar esta prueba se utilizó el buscador google Chrome, por medio de las direcciones IP se logró en ciertos casos ingresar a la configuración de los equipos ya que

las credenciales eran las asignadas por defecto, en otros casos se mantiene la comunicación con la petición de credenciales sin embargo no son las usadas por defecto. A continuación, se presenta los resultados obtenidos:

En la figura 2.22. se puede observar que al ingresar la dirección en el buscador este accede sin la petición de credenciales alguna.

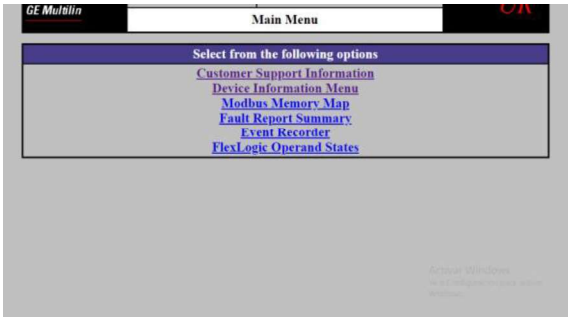

Figura 2.22. Interfaz del relé general electric F35

En la figura 2.23. si bien existe la petición de credenciales, estas credenciales son las asignadas por defecto, en la figura 2.24 se observa el ingreso hacia el equipo después de digitar las credenciales por defecto.

Figura 2.23. Concentrador de la subestación EL RETORNO

Figura 2.24. Concentrador de la subestación EL RETORNO

RESULTADOS GLOBALES DE LAS PRUEBAS DE CONECTIVIDAD DE LA RED LAN DE LA SUBESTACIÓN EL RETORNO.

La conectividad fue satisfactoria 100% en todos los equipos sin embargo cabe destacar que existe una extrema facilidad para ingresar a los equipos de la subestación, ya que estos equipos solo presentan configuraciones básicas.

Cabe destacar también que las pruebas de conectividad se desarrollaron desde un equipo que no pertenecía a EMELNORTE y además se utilizó la red inalámbrica, esto deja en evidencia las falencias que se tiene en el sistema de comunicaciones de la subestación EL RETORNO.

2.2.3 ANALISIS DE LA ADMINISTRACIÓN Y GESTIÓN ACTUAL DE LA RED LAN DE LA SUBESTACIÓN EL RETORNO.

El análisis de administración y gestión se lo realiza con la finalidad de determinar si la red cuenta con criterios y configuraciones que permitan un buen funcionamiento, para ello se realiza el análisis por cada uno de los equipos que se encuentran direccionados en la red y se revisa las configuraciones que se encuentran en cada uno de los equipos.

- **SCHNEIDER ION 8500 (medidor).**

En la tabla 2.5. se observa el direccionamiento del equipo, en el cual se analizará las configuraciones que posea.

Tabla 2.5. Direccionamiento de medidor

#	MARCA	MODELO	EQUIPO	IP	PREFIJO	MASCARA	GATEWAY	DESCRIPCIÓN	OBS
1	Schneider	8500	Circuito R1	172.17.58.XX	24	255.255.255.XX	172.17.58.XX	Salida 1 san Antonio	Pri_11 equipo de medición

CONSIDERACIÓN.

El equipo permite realizar configuraciones y visualización de los parámetros por medio de un software “Schneider Electric ION setup” (cliente) que forma parte del set del equipo.

CARACTERISTICAS DE CONFIGURACIÓN.

- El equipo se encuentra operativo.

- Las credenciales se encuentran por defecto para el ingreso hacia el equipo por medio de un cliente.
- Para realizar una comunicación por medio del browser no se requiere credenciales, pero solo permite realizar ciertas configuraciones y una visualización total de las mediciones que realiza el equipo como voltajes corrientes, frecuencia, etc.
- El equipo no permite una configuración por SSH.
- El equipo no se encuentra sincronizado la fecha y hora no son los correctos y se puede apreciar en la figura 2.25.

Figura 2.25. Visualización de la falta de sincronismo del equipo

- Presenta configuraciones de repulsión de clientes por tiempo máximo de 5 minutos.

➢ **SWITCH GARRETCOM 6KL.**

En la tabla 2.6. se observa el direccionamiento del equipo, en el cual se analizará las configuraciones que posea.

Tabla 2.6. Direccionamiento de del switch 1

#	MARCA	MODELO	EQUIPO	IP	PREFIJO	MASCARA	GATEWAY	DESCRIPCIÓN	OBS
21	Garretcom	6KL	Sw1	172.17.58.101	/24	255.255.255.0	172.17.58.1		

CARACTERISTICAS DE CONFIGURACIÓN.

- El dispositivo presenta credenciales por defecto.
- No presenta niveles de acceso por el interfaz de línea de comando(CLI).
- Es posible el acceso por medio del buscador con credenciales por defecto.
- Es posible el acceso por medio de un cliente usando telnet.
- No es posible acceder al equipo por medio de SSH.

- No presenta configuraciones de FTP que se aprecian en la figura 2.26.

Figura 2.26. Configuración de FTP en el switch 1 de la subestación EL RETORNO

- No presenta configuraciones de TFTP que se aprecia en la figura 2.27.

Figura 2.27. Configuración de TFTP en el switch 1 de la subestación EL RETORNO

- El switch no presenta sincronismo, la fecha y hora no son correctas y se aprecia en la figura 2.28.

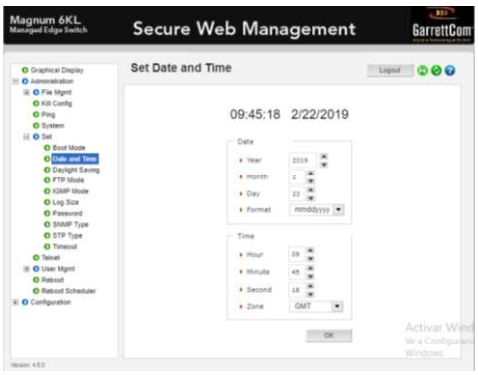

Figura 2.28. Configuración de fecha y hora en el switch 1 de la subestación EL RETORNO

- Se encuentra habilitado el protocolo HTTPs.

Figura 2.29. Configuración de HTTPs en el switch 1 de la subestación EL RETORNO

- Se presenta habilitado el protocolo SSL.

En la figura 2.30. se observa el estado del protocolo de cifrado SSL en el switch 1 de la subestación EL RETORNO

Figura 2.30. Estado de SSL

- No presenta configuraciones de VLANs.

En la figura 2.31. se observa el estado de las VLANs en el switch 1 de la subestación EL RETORNO.

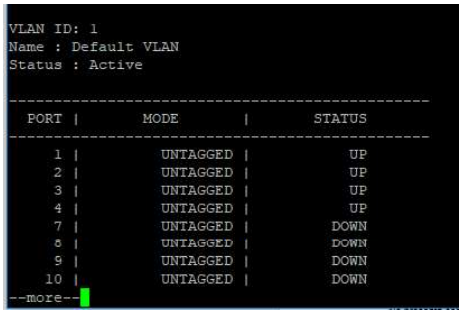

Figura 2.31. Estado de VLANs

- No existe restricciones de puertos seguros.

En la figura 2.32. se observa el estado de los puertos del switch 1 de la subestación EL RETORNO.

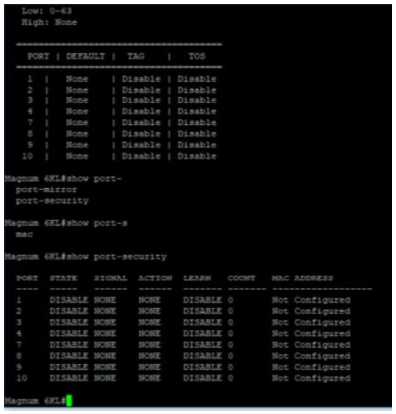

Figura 2.32. puertos del switch 1

- No existe restricciones por IP para acceder al equipo.
- No existe configuración del protocolo SNMP (sugerida versión 3 autenticación MD5).
- No existe protección por tormentas de broadcast.

- **ROUTER GARRETCOM DX940.**

En la tabla 2.7. se observa el direccionamiento del equipo, en el cual se analizará las configuraciones que posea, este equipo se encuentra comunicando el concentrador de datos.

Tabla 2.7. Direccionamiento del router DX940

#	MARCA	MODELO	EQUIPO	IP	PREFIJO	MASCARA	GATEWAY	DESCRIPCIÓN	OBS
22	garretcom	DX940	Gateway E3	172.17.58.XX	/24	255.255.255.XX	172.17.58.XX	-	-

CARACTERISTICAS DE CONFIGURACIÓN.

- **ADMINISTRACIÓN.**
  - En la figura 2.33. se observa la Información básica, y se determina que el dispositivo se encuentra con una administración por defecto.

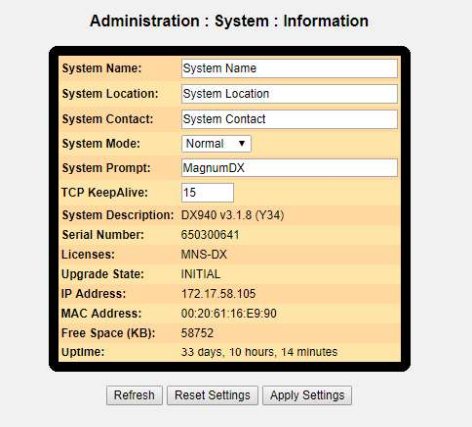

Figura 2.33. Configuración básica del sistema del router de la subestación EL RETORNO

  - En la figura 2.34. se observa el estado de uso de las características físicas del equipo.

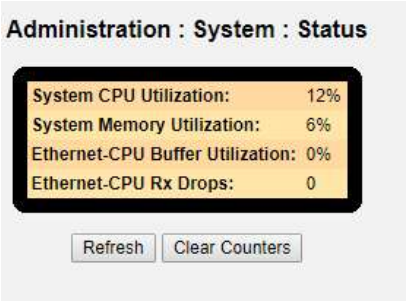

Figura 2.34. Estado de recursos del router de la subestación EL RETORNO

  - En la figura 2.35. se observa el estado de la red.

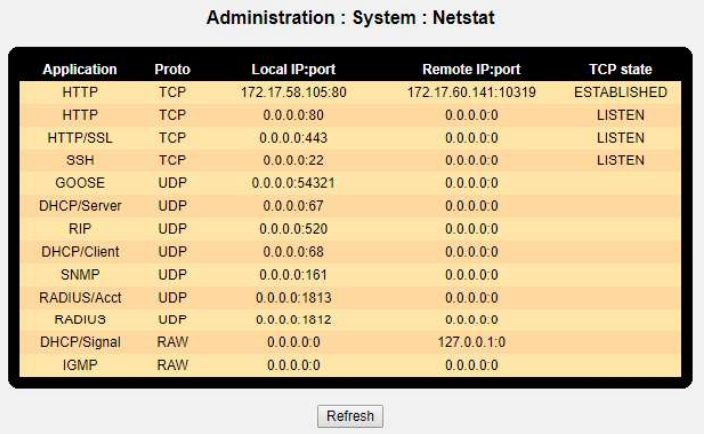

Figura 2.35. Registro de comunicación hacia el router de la subestación EL RETORNO

- No se encuentra sincronizado el equipo.
- No se encuentra habilitado el protocolo SNTP.
- No existe configuraciones de DNS.
- No existe configuración de SNMP.
- No presenta políticas de autenticación.
- No presenta políticas de sesión.
- En la figura 2.36 se observa los archivos de revisiones y configuraciones del equipo.

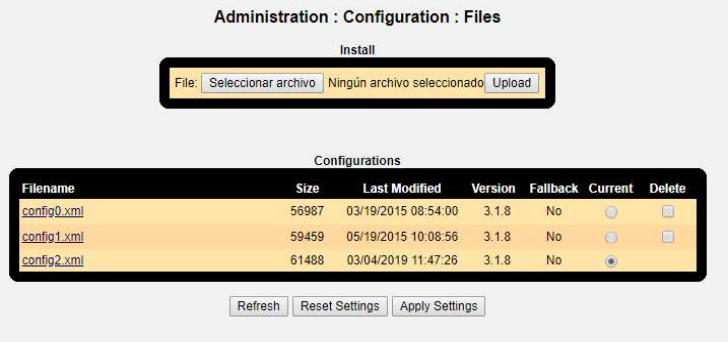

Figura 2.36. Memorias de configuración del router de la subestación EL RETORNO

- Se encuentra habilitado el protocolo rapid spanning tree protocol (RSTP).
- No existe configuración de RSTP.
- Configuración de VLANs. Deshabilitado.
- Configuración de mensajería GOOSE no se encuentra activo.

CONFIGURACIÓN DE RUTEO.

- En la figura 2.37 se observa la configuración de interfaces en el equipo.

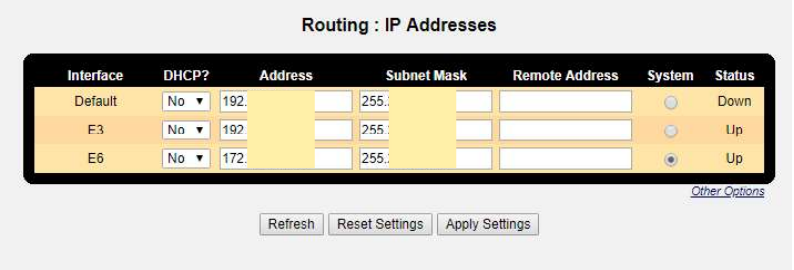

Figura 2.37. Direcciones IP en el router de la subestación EL RETORNO

- No existe configuración de ruteo estático.
- No existe configuraciones de redundancia en el router.
- En la figura 2.38. se observa que existen configuraciones Network Address Translation (NAT) mínima.

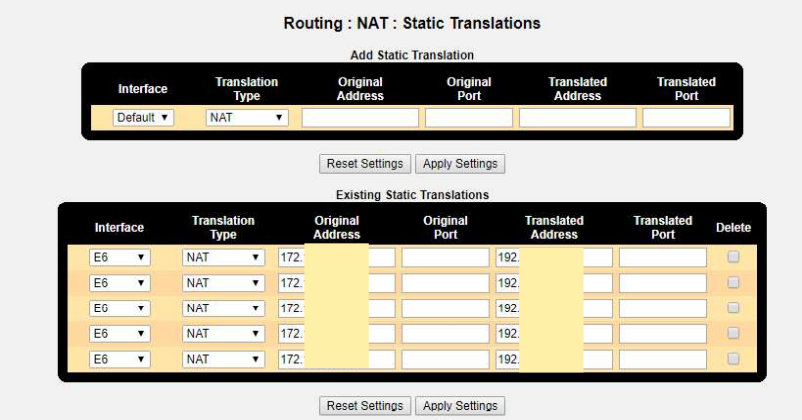

Figura 2.38. Configuración de NAT en el router de la subestación EL RETORNO

- No existe configuración de DHCP.
- No existe configuraciones de prioridades en QoS.
- No existe la habilitación de certificados de seguridad.

Nota: El análisis de administración y gestión completo se adjunta en el ANEXO A, denominado “A-1_ANALISIS DE LA ADMINISTRACIÓN Y GESTIÓN ACTUAL”.

RESULTADOS GLOBALES DEL ANÁLISIS DE ADMINISTRACIÓN Y GESTIÓN DE LOS EQUIPOS DE LA RE DE LA SUBESTACIÓN EL RETORNO.

En la tabla 2.8. se aprecian los resultados obtenidos posterior al análisis de administración y gestión de los equipos de la red de comunicaciones de la subestación RETORNO. Es importante mencionar que los criterios para realizar el análisis se encuentran en el numeral 1.3.5.

Tabla 2.8. Resultados globales de la administración y gestión de la red LAN EL RETORNO

#	DESCRIPCIÓN	ESTADO			
		Excelente	Buena	Deficiente	Inexistente
1	topología			✓	
2	Redundancia física.			✓	
3	Redundancia lógica.				✓
4	Direccionamiento.			✓	
5	Configuraciones de enrutamiento.		✓		
6	Configuraciones administrativas básicas.			✓	
7	Credenciales.			✓	
8	Protocolos de sincronización de red.				✓
9	Configuraciones de seguridad de red.			✓	
10	Estado de uso de memoria y CPU de equipos.	✓			
11	Configuraciones de calidad de servicio.				✓
12	Políticas de seguridad.				✓
13	Procedimientos de administración y gestión.				✓

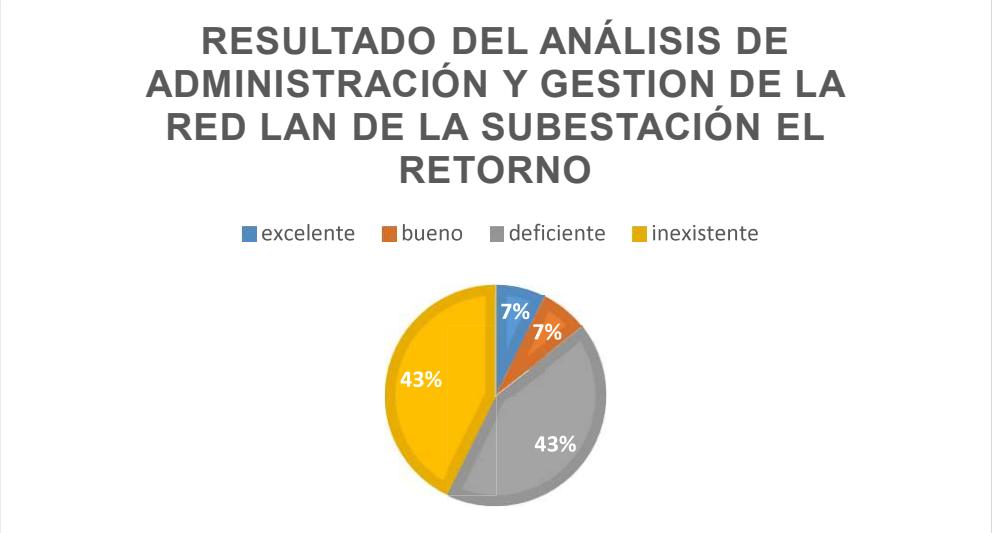

Figura 2.39. Resultados del análisis de administración y gestión de la red LAN de la subestación EL RETORNO

2.2.4 ANÁLISIS DE VULNERABILIDADES DE LA RED LAN DE LA SUBESTACIÓN EL RETORNO.

Para realizar el análisis de vulnerabilidades de la red LAN de la subestación EL RETORNO se utilizó el software conocido como NESSUS el cual nos permite establecer los siguientes

factores que se deben considerar al realizar el análisis de puertos abiertos, estado del puerto, descripción general y la vulnerabilidad, con la cual se puede someter el puerto o configuración, además se ha considerado establecer de forma visual la gravedad del estado de los equipos referentes a las seguridades, para ello se ha establecido en la tabla 2.9:

Tabla 2.9. Resultados del análisis de vulnerabilidades

Color asignado	Estado	Descripción
	Informativo	Información que se debe considerar
	baja	El sistema es seguro
	Medio	Se debe realizar ciertas mejoras
	alto	Se deben realizar correcciones considerables
	critico	Se necesita realizar correcciones de alto riesgo ya que el sistema se encuentra considerablemente en peligro.

El análisis se lo ha desarrollado tomando en cuenta cada uno de los elementos que forman parte de la red LAN de la subestación EL RETORNO, a continuación, se presenta los equipos y los resultados obtenidos por medio del software NESSUS.

- **SCHNEIDER ION 8500 (medidor).**

Figura 2.40. Medidor que se encuentra en las instalaciones de la subestación EL RETORNO [16]

Descripción del equipo de la figura 2.40.

Schneider ION 8500 es un equipo encaminado a realizar mediciones de voltaje, corriente, potencia, factor de potencia y energía.

En la red LAN es el encargado de realizar mediciones de la salida 1 asignado a San Antonio, en el siguiente cuadro se detalla la configuración de direccionamiento del equipo.

En la tabla 2.10. se observa el direccionamiento y descripción del equipo a analizar.

Tabla 2.10. Direccionamiento del equipo ION 8500

#	MARCA	MODELO	EQUIPO	IP	MASK	MASCARA	GATEWAY	DESCRIPCIÓN
1	Schneider	8500	Circuito R1	172.17.xx.xx	/24	255.xx.xx.xx	172.17.xx.xx	Salida 1 san Antonio

En la tabla 2.11. se observan los resultados del análisis.

ESTADO	PUERTOS ABIERTOS	OBSERVACION	VULNERABILIDAD
medio	23	El puerto 23 es usado para comunicaciones remotas TCP/IP por medio de un cliente, el puerto está asociado a TELNET.	El protocolo TELNET establece una comunicación la cual no está cifrada, por ello es de fácil interpretación, para ello es posible obtener información por medio de un sniffer.

Tabla 2.11. Resultados obtenidos después de ejecutar el software NESSUS para el host de la tabla 2.10.

- **PANTALLA ADVANTECH IPCC6172A.**

Figura 2.41. Pantalla que se encuentra en las instalaciones de la subestación EL RETORNO

Descripción del equipo de la figura 2.41.

La pantalla se encuentra en el rack dentro de las instalaciones de la subestación EL RETORNO, es un equipo con el cual se puede realizar escritorio remoto:

Su software es Microsoft Windows vista y su procesador es un Core 2 Duo. Este equipo se encuentra como soporte administrativo de la subestación, en el siguiente cuadro se detalla la configuración de direccionamiento del equipo.

En la tabla 2.12. se observa el direccionamiento y descripción del equipo a analizar.

Tabla 2.12. Direccionamiento del equipo pantalla advantech ipcc6152

#	MARCA	MODELO	EQUIPO	IP	PREFIJO	MASCARA	GATEWAY
29	TSI	Ipcc6172A	Pantalla advantech ipcc6172A	172.17.xx.xx	/24	255.xx.xx.xx	172.17.xx.xx

En la tabla 2.13. se observan los resultados del análisis.

Tabla 2.13. Resultados obtenidos después de ejecutar el software NESSUS en la pantalla advantech ipcc6172A.

ESTADO	PUERTO ABIERTO	CARACTERISTICA	DESCRIPCIÓN	SOLUCIÓN
critico	3389	MS14-066: Una vulnerabilidad en Schannel podría permitir la ejecución remota de código (2992611)(verificación sin credencial)	El host de Windows remoto está afectado por una vulnerabilidad de ejecución de código remoto debido al procesamiento inadecuado de paquetes por parte del paquete de seguridad de canal seguro (Schannel). Un atacante podría explotar este problema enviando paquetes especialmente diseñados a un servidor de Windows. Se debe tener en cuenta que este complemento envía un mensaje de saludo TLS certificado del cliente seguido de un mensaje Certificate Verify. Algunos hosts de Windows cerrarán la conexión al recibir un certificado de cliente que no solicito con un mensaje CertificateRequest. En este caso el complemento no puede proceder a una detección de vulnerabilidad ya que no es posible enviar el mensaje CertificateVerify.	Actualmente Microsoft ha lanzado un conjunto de parches tanto para Windows 2003, Windows 7, Windows 2008 R2,8, 2012, 8.1 y 2012 R2.
critico	445	MS17-010: Actualización de seguridad para el servidor SMB de Microsoft Windows (4013389) (eternalblue) (eternalchampion) (eternalromance) (eternalsynergy) (WannaCry)(EternalRocks) (Petya) (cheque sin credencial)	El host remoto que usa Windows está afectado por las siguientes vulnerabilidades: • Se presentan varias vulnerabilidades de ejecución de forma remota con el protocolo SMBv1 esto se presentó debido a un manejo inadecuado de ciertas solicitudes, un atacante puede explotar una vulnerabilidad por medio de paquetes especialmente diseñados para ejecutar código arbitrario. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0146, CVE-2017-0148)	Microsoft proporciono algunos parches para: Windows vista, 2008 ,7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10 y 2016. Para sistemas operativos como Windows XP se recomienda suspender el uso de SMBv1,

			ETHERNALBLUE, ETHERNALCHAMPION, ETERNALROMANCE, TERNALSYNERGY son 4 vulnerabilidades divulgadas en el 2017-04-14 por un grupo llamado Shadow Brokers. WannaCry / WannaCrypt es un programa ransomware que usa el exploit ETERNALBLUE, ETERNALROCKS es un gusano que usa siete vulnerabilidades, Petya es un programa ransomware que permite la utilización de CVE-2017-0199, es una vulnerabilidad de Microsoft office y luego fue propagada por ETERNALBLUE.	ya que carece de características de seguridad.
critico	8834	Vulnerabilidades múltiples (TNS-2016-16) (sweet32)	• Existe una vulnerabilidad por medio de denegación de servicio en el componente Open SSL debido a una falla al asegurar adecuadamente el uso de las operaciones de tiempo constante. Un atacante remoto podría explotar esta vulnerabilidad por medio de un ataque de canal lateral de temporización. Para la información de clave DSA. (CVE-2016-2178) • También se encontró una vulnerabilidad por denegación de servicio en el componente OpenSSL en la implementación de DTLS debido a una falla al restringir de forma adecuada el tiempo de vida de las entradas de cola asociadas con los mensajes fuera de servicio que no se utilizan. Una persona podría atacar esta vulnerabilidad de forma remota, por medio de la apertura de múltiples sesiones DTLS con la finalidad de agotar la memoria. (CVE-2016-2179). • Se presentó un error de lectura fuera de límites en el componente OpenSSL cuando se implementaba el protocolo X.509 de infraestructura de clave pública (TSP). Esta vulnerabilidad podría ser explotada de forma remota por un atacante, se realizaría el ataque por medio de un archivo de sello de tiempo elaborado que es mal manejado por el comando ´openssls´, con el objetivo de causar denegación de servicio u obtener información delicada. (CVE-2016-2180) • Una vulnerabilidad llamada SWEET32, en el componente OpenSSL en los algoritmos 3DES y Blowfish esto debido al uso de	Una solución sería la actualización de SSL

			cifras débiles de 64 bits de forma predeterminada. Un atacante de forma hombre en el medio podría explotar esta vulnerabilidad por medio de un ataque de ´cumpleaños´ (CVE-2016-2183) • Se detectó una falla en el componente SSL en la función TLS decrypt ticket (en t1_lib.c) esto producido por un manejo incorrecto de los resúmenes HMAC de tickets. Por medio de esta falla un atacante podría explotar esta vulnerabilidad por medio de la denegación de servicio. (CVE-2016-6302) • Se presentó una condición de desbordamiento de entero en el componente OpenSSL en la función MDC2-Update () en mdc2dgst.c debido a una validación incorretade la entrada que fue proporcionada por el usuario. Un atacante remoto no autenticado podría explotar esto para causar un desbordamiento de bufer, esto daría como resultado una condición de denegación de servicio o también la ejecución de código arbitrario. (CVE-2016-6303) • Se presentó una falla en el componente OpenSSL en la función ssl parse client hello tlsext en t1_lib.c producido por el manejo incorrecto de extensiones de solicitud de estado de OCSP, los mensajes son muy grandes de los clientes. Un atacante de forma remota podría explotar esta vulnerabilidad por medio de grandes extensiones de solicitud de estado de OCSP, con la finalidad de agotar los recursos de la memoria, esto daría como resultado una condición de denegación de servicio. (CVE-2016-6304) • Se presentó una falla en el componente OpenSSL en la función SSL_peek () en rec_layer_s3.c producido por un manejo incorrecto de registros vacíos. Un atacante de forma remota podría explotar esta vulnerabilidad por medio de la desencadenarían de un registro de longitud cero en una llamada SSL_peek, esto causaría un bucle infinito, dando como resultado una condición de denegación de servicio. (CVE-2016-6305) • Se presentó un error de lectura fuera de límites en el componente OpenSSL en el analizador de	

			certificados que podría permitir a un atacante de forma remota, cause una denegación de servicio por medio de operaciones de certificados elaborados. (CVE-2016-6306)	
alto	443	Detección de protocolo SSL versión 2 y 3	El servicio remoto permite conexiones cifradas usando SSL 2.0 y/o SSL 3.0. dichas versiones de SSL son afectadas por varios defectos criptográficos, que pueden incluirse como: • Presenta un esquema inseguro con cifrado CBC. • El esquema de regeneración y reanudación de sesión es inseguro. Presentada esta información se puede determinar que es relativamente fácil acceder, un atacante podría explotar estos defectos para realizar un ataque de intermediarios o descifrar las comunicaciones entre el servicio afectado y los clientes. SSL/TLS tienen un medio seguro para poder elegir una versión más compatible del protocolo de modo que estas versiones de usaran solo si el cliente o servidor no admite nada mejor, la mayoría de navegadores web implementan este sistema de manera insegura es así que permite a un atacante bajar una conexión como un 'poodle' es por ello que lo más recomendado es deshabilitar estos protocolos por completo. NIST por sus siglas en inglés (National institute standarts and Technology) ha determinado que SSL 3.0 ya no se acepta para comunicaciones seguras. Esto se determinó a partir de la fecha de aplicación de PCI DSS v3.1 (a partir del 30 de junio del 2018 todas las entidades deberán dejar de seguir usando SSL/TLS)	Se debe deshabilitar SSL 2.0 y 3.0. Se debe empezar a usar TLS 1.1 (con un conjunto de cifrado aprobado).
alto	3389	MS12-020: las vulnerabilidades en el escritorio remoto podrían permitir la ejecución remota de código (2671387)(verificación sin credencial)	Existe una vulnerabilidad arbitraria de código remoto en la implementación del protocolo de escritorio remoto conocido como (DRP) presente en el host remoto de Windows. Esta vulnerabilidad es debida a la forma en que RDP accede un objeto en l memoria que se ha inicializado incorrectamente o se ha eliminado. RDP se encuentra habilitado razón por la cual un atacante de forma remota podría aprovechar esta vulnerabilidad para hacer que el sistema ejecute un código arbitrario al enviarle una secuencia de paquetes RDP especialmente diseñados con fines maliciosos. También se puede presentar una denegación de servicio en Microsoft Terminal Server.	Una posible solución es ejecutar un parche para Windows XP, 2003, vista, 2008, 7 y 2008 R2. Es importante tomar en cuenta que se requiere un contrato de soporte extendido con Microsoft para poder obtener el parche para esta vulnerabilidad de Windows 2000.

medio	502	Acceso a la bobina Modbus/TCP	Modbus es un protocolo que permite leer las bobinas en un esclavo Modbus, y generalmente es utilizado por los dispositivos de campo SCADA. Las bobinas hacen referencia a la configuración de salida binaria, y generalmente son asignados a los actuadores. La capacidad de leer las bobinas puede ayudar a un atacante a perfilar un sistema e identificar varios rangos de registros para modificar a través de mensajes de las bobinas de escritura.	Una solución factible seria restringir el acceso al puerto Modbus TCP/502. Con esto solo los clientes autorizados podrán acceder.
medio	443	Certificado SSL no puede ser confiable	No es posible confiar en el certificado X.509 del servidor. Esto puede suceder por tres motivos en las que se puede romper la cadena de confianza, como se indica: • Primero tenemos que la parte superior de la cadena de certificación enviada por el servidor podría no descifrarse de una autoridad de certificación publica conocida. Esto podría ocurrir cuando la parte superior de la cadena es un certificado autofirmado no reconocido o cuando faltan certificados intermedios que conectarían la parte superior de la cadena de certificados con una autoridad de certificación publica conocida. • En segundo lugar, tenemos que la cadena de certificados puede contener un certificado que no es válido en el momento del escaneo. Esto podría ocurrir cuando el escaneo ocurre antes de una de las fechas y no antes del certificado, o después de uno de los certificados no después. • En tercer lugar, tenemos que la cadena de certificados puede contener una firma que no coincide con la información que presenta el certificado o no es verificable. Estas malas firmas se pueden arreglar consiguiendo que el certificado con las firmas incorrectas sea reescrito por su emisor. Las firmas que no se pueden verificar son el resultado de que el emisor del certificado utiliza un algoritmo de firma que nessus no reconoce o no admite.	Lo recomendable seria comprar o generar un certificado apropiado para dicho servidor.
medio	443	Certificado SSL firmado con algoritmo de hash débil	El servicio de comunicación de forma remota utiliza una decena de certificados SSL que se ha firmado utilizando un algoritmo hash criptográfico débil (por ejemplo, tenemos: MD2, MD4, MD5 o SHA1). Se conoce que estos algoritmos de firma son vulnerables a los conocidos como ataques de colisión. Un atacante podría explotar esto para generar otro certificado con la misma firma digital, esto permitiría	Lo que se debería hacer es contactar a una autoridad de certificación para que se vuelva a emitir el certificado.

			que un atacante se enmascare o suplante como el servicio afectado. Es importante tomar en cuenta que este complemento informa a todas las cadenas de certificados SSL firmadas con SHA1 que caducan después del 1 de enero del 2017 como vulnerables.	
medio	443	Certificado autofirmado SSL	La cadena de certificados X.509 para este servicio no se encuentra firmada por una autoridad de certificación reconocida. Si el host remoto es un host público en producción, esto anularía el uso de SSL, ya que cualquiera podría establecer un ataque conocido como ´´man-in-the-middle´´ en contra del host remoto. También se debe tomar en cuenta que este complemento no verifica las cadenas de certificados que terminan en un certificado que no está autofirmado, sino que se encuentra formado por una autoridad certificadora desconocida.	Lo recomendable es comprar o generar un certificado apropiado para este servicio.
medio	80	Información de encabezado de ETag del servidor Apache	El servidor web remoto se ve afectado por una vulnerabilidad de divulgación de información producido por el encabezado ETag el cual proporciona información delicada que podría ayudar a un atacante.	La solución a esta vulnerabilidad seria modificar el encabezado ETag HTTP del servidor web para no incluir nodos de archivo cuando se realiza el cálculo del encabezado ETag, para ello es mejor activar el protocolo HTTPs.
media	80	Método HTTP TRACE/TRACK permitidos	El servidor web remoto puede admitir los métodos TRACER y/o TRACK. TRACE Y TRACK son métodos de HTTP que son usados para la depuración de conexiones de servidores web.	Sería recomendable deshabilitar estos métodos.
medio	22	Algoritmos débiles SSH compatibles	Se detectó que el servidor SSH remoto se encuentra configurado para usar el cifrado de flujo Arcfour o no cifrar nada. RFC 4253 nos aconsejó que no se deba usar Arcfour debido a un problema con las teclas débiles.	Póngase en contacto con el proveedor o consulte la documentación del producto para eliminar las cifras débiles.
medio	3389	Servidor del protocolo de escritorio remoto de Microsoft Windows Debilidad del hombre en el medio	La versión del protocolo de escritorio remoto (Servicio Terminal) es vulnerable a un ataque conocido como ´hombre en el medio´ (MiTM). El cliente RDP no se esfuerza por validar la identidad del servidor al realizar la configuración de cifrado, esto podría generar que un atacante que tenga la capacidad de interceptar el tráfico del servidor RDP puede establecer el cifrado con el cliente y el servidor sin que este sea	una posible solución sería forzar el uso de SSL como capa de transporte para este servicio si es compatible y/o seleccionando

			detectado. Un ataque de hombre en el medio de este tipo permitiría al atacante obtener toda la información que se encuentre transmitiendo, como por ejemplo claves de acceso nombres de usuario etc. Este error se genera porque el servidor RDP almacena una clave privada RSA codificada en la biblioteca mstlsapi.dll.	la configuración ´permitir una conexión solo desde las computadoras que ejecutan escritorio remoto con una autenticación. de nivel de red. Si se encuentra disponible.
medio	49155	MS16-047: Actualización de seguridad para los protocolos SAM y LSAD (3148527)(Badlock)(verificación sin credencial)	El host remoto de Windows se encuentra afectado por una vulnerabilidad de elevación de privilegios en los protocolos Administrador de cuenta de seguridad (SAM) y también autoridad de seguridad local conocida como (Política de Dominio)(LSAD) esto se produjo por una negociación incorrecta del nivel de autenticación por medio de canales de llamada a procedimiento remoto (RPC).	Una solución nos da Microsoft al poner a disposición varios parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT8.1, 2012 R2 y 10.
medio	445	SMB signing no requerido	No sería necesario firmar en el servidor SMB remoto. Esto podría dar pasó a un ataque conocido como: ¨ataque de hombre en el medio¨ contra el servidor SMB.	Su solución sería aplicar la firma de mensaje en la configuración de host. En Windows.
medio	3389	Suites de cifrado de intensidad media SSL compatibles	El host remoto puede admitir el uso de cifrado SSL el cual es considerado un cifrado de intensidad media. Para Nessus la intensidad media como cualquier encriptación que utiliza longitudes de clave de al menos 64bits y menos a 112 bits. Es importante tomar en cuenta que es más fácil evitar el cifrado de intensidad media si el atacante se encuentra en la misma red física.	Se debe volver a configurar la aplicación afectada, para evitar el uso de cifras de intensidad media.
media	3389	El nivel de Encriptación de Servicios de Terminal es Medio o Bajo	Se encontró que el servicio de Terminal Services remoto no se encuentra configurado para usar una criptografía sólida. Cuando se mantiene el uso de una criptografía débil con este servicio es posible permitir que un atacante escuche las comunicaciones con mayor facilidad y pueda obtener capturas de pantalla y/o pulsaciones de teclas.	Se debe cambiar el nivel de cifrado RDP a un nivel alto.
bajo	3389 443	Compatible con SSL C4 Cipher Suites (Bar Mitzvah)	El host admite el uso de RC4 en uno o más conjuntos de cifrado. Si el texto sin formato se encripta de forma repetitiva por ejemplo (cookies HTTP), un atacante podría fácilmente cifrar esta información.	Se debe evitar el cifrado RC4, lo recomendable seria usar TLS 1.2 con suite AES-GCM sujetas a soporte de navegador y servidor web.

bajo	22	Cifrados del modo CBC del servidor SSH habilitados	El servidor SSH se encuentra configurado para admitir el cifrado Cip (cipher Block Chaining). Esto podría permitir que un atacante pueda obtener los mensajes de texto cifrado y fácilmente descifrarlos. Es importante tener en cuenta que este complemento solo busca las opciones del servidor SSH y no se verifica si hay versiones de software vulnerable.	Sería recomendable la habilitación descifrado CTR o GCM y deshabilitar el modo CBC.
bajo	22	SSH algoritmos MAC débiles habilitados	Elservidor remoto SSH se encuentra configurado para permitir algoritmos MAC MD5 0 96 bits, ambos son considerados débiles.	Se recomienda la debilitación de MAC MD5 y 96 bits.

En la tabla 2.14 se aprecian resultados informativos, también otorgados por software NESSUS.

Tabla 2.14. Resultados de estados informativos que forman parte del análisis de vulnerabilidades de la pantalla advantech ipcc6172A

ESTADO	PUERTOS ABIERTOS	OBSERVACIÓN	VULNERABILIDAD
informativo	135	El puerto 135 conocido como de llamada a procedimiento remoto (RPC) es usado en aplicaciones de cliente/servidor.	Es vulnerable a ataques de denegación de servicio. MS Security Bulletin nos da otra vulnerabilidad de RPC que se debe tomar en cuenta, saturación de buffer, lo que se debe hacer es filtrar el puerto 135 por medio de un firewall.
informativo	139	Este puerto es usado por NEtBIOS, Windows admite el tráfico para poder compartir archivos e impresoras usando el protocolo SMB (bloque de mensajes de servicio) que se encapsula en TCP	Existen varios malwares que pueden atacar este puertos algunos como: el mensaje de Dios, Netlog entre otros.
informativo	554	El puerto 554 usa el protocolo TCP para transportar información de tipo audio y video, el protocolo usado es RTSP (Real Time Streaming Protocol)	Aunque no sería una vulnerabilidad netamente dicha si es una desventaja tener en el mismo segmento de red información tipo bull y la información de mediciones.

El análisis de las vulnerabilidades que nos presenta NESSUS de toda la red LAN de la subestación EL RETORNO se observa en la figura 2.42.

Figura 2.42. Disco estadístico obtenido del análisis de vulnerabilidades usando el software NESSUS

En la tabla 2.15. se observan los resultados obtenidos del análisis de vulnerabilidades con el software NESSUS.

Tabla 2.15. Resultados porcentuales del análisis de vulnerabilidades aplicado a la subestación EL RETORNO usando NESSUS

ESTADO	PORCENTAJE
Informativo	56%
Bajo	5%
Medio	27%
Alto	5%
Critico	7%

Nota: El análisis de vulnerabilidades completo se adjunta en el ANEXO A, denominado "A-2_ANÁLISIS DE VULNERABILIDADES USANDO EL SOFTWARE NESSUS_SUB_RETORNO".

En la siguiente sección se desarrollará la metodología para mejorar la administración, gestión y seguridad de las redes LAN de las subestaciones eléctricas de EMELNORTE, la cual ha sido estructurada bajo el formato de una normativa, en vista que esta será tomada como especificación referente por EMELNORTE.

2.3 METODOLOGÍA PARA LA IMPLEMENTACIÓN DE UNA RED LAN EN UN SISTEMA SCADA/ADMS DE LAS SUBESTACIONES DE EMELNORTE.

2.3.1 PROPÓSITO DE LA METODOLOGÍA.

La siguiente metodología tiene como propósito presentar lineamientos que permitan estructurar una red LAN dentro de una subestación eléctrica de EMELNORTE, dicha metodología pretende mejorar aspectos como: organización, administración, seguridad y eficiencia, de la red de comunicaciones que forma parte del sistema SCADA/ADMS de la empresa eléctrica EMELNORTE S.A.

2.3.2 INTERPRETACIÓN DE LA METODOLOGÍA.

La metodología se encuentra estructurada de forma jerárquica por capítulos, categorías y subcategorías. Los capítulos engloban a las diferentes categorías donde se detalla la información de cada una de las temáticas, en la tabla 2.16. se expone los diferentes tópicos que abarca la metodología:

Tabla 2.16. Estructura de la metodología planteada

CAPITULOS	CATEGORIAS	SUBCATEGORIAS
CAPITULO 1: ARQUITECTURA FÍSICA PARA UNA RED LAN EN UNA SUBESTACIÓN.	ARQUITECTURAS FÍSICAS SUGERIDAS.	DIAGRAMA 1.
		DIAGRAMA 2.
		LINEAMIENTOS CONSTRUCTIVOS DE LOS EQUIPOS A INSTALAR.
CAPITULO 2: ADMINISTRACIÓN Y GESTIÓN DE LA INFORMACIÓN EN UNA SUBESTACIÓN.	EQUIPOS DE PROCESO.	DISPOSITIVOS ELECTRONICOS INTELIGENTES (IEDs).
	EQUIPOS DE PROTECCION LOCAL Y ADMINISTRACION LOCAL.	CONTROLADOR LOGICO PROGRAMABLE (PLC).
		COMPUTADOR PERSONAL (PC).
		INTERFAZ HOMBRE MAQUINA (HMI).
		EQUIPOS DE SEGURIDAD FÍSICA DE LA SUBESTACIÓN.
	EQUIPOS DE NETWORKING DE UNA SUBESTACIÓN.	LINEAMIENTOS DE CONFIGURACIÓN GENERAL BÁSICA.
		LINEAMIENTOS DE ADMINISTRACIÓN DE ROUTER.

		LINEAMIENTOS DE ADMINISTRACIÓN DE SWITCH.
		LINAMIENTOS PARA LA ADMINISTRACION DE PROTOCOLOS INDUSTRIALES.
		LINEAMIENTOS PARA LIMITAR LA CONEXIÓN DE DISPOSITIVOS EXTERNOS POR MEDIO DE LA ADMINISTRACIÓN DE PUERTOS FÍSICOS.
		LINEAMIENTOS PARA ASIGNACIÓN DE DIRECCIONES A LOS DISPOSITIVOS.
		LINEAMIENTOS PARA SEGMENTACIÓN DE LA RED Y CREACIÓN DE REDES VIRTUALES (VLANs).
		LINEAMIENTOS PARA SINCRONIZACIÓN DE EQUIPOS DE NETWORKING.
		LINEAMIENTOS PARA LA CONFIGURACIÓN DE CALIDAD DE SERVICIO.
		LINEAMIENTOS PARA EL RESPALDO DE CONFIGURACIONES DE LOS EQUIPOS DE NETWORKING.
CAPITULO 3: SEGURIDAD EN LAS INSTALACIONES Y RED LAN DE UNA SUBESTACIÓN.	SEGURIDAD CIBERNÉTICA.	LINEAMIENTOS DE CONTROL DE ACCESO.
		LINEAMIENTOS PARA EL USO DE PROTOCOLOS DE CIFRADO.
		LINEAMIENTOS PARA ACTUALIZACIÓN DE PARCHES.
		LINEAMIENTOS PARA ADMINISTRACIÓN DE PUERTOS Y SERVICIOS.
		LINEAMIENTOS PARA TRATAMIENTO DE CODIGOS MALICIOSOS.
		LINEAMIENTOS PARA ACCESO AL SISTEMA DE FORMA LOCAL Y REMOTA.
		LINEAMIENTOS PARA LA CONFIGURACIÓN DE CREDENCIALES EN LOS EQUIPOS DE NETWORKING.
	POLÍTICAS DE SEGURIDAD.	LINEAMIENTOS PARA LA ESTRUCTURA

		ORGANIZACIONAL DEL PERSONAL.
		LINEAMIENTOS PARA ASIGNACIÓN Y RETIRO DE CREDENCIALES A LOS TRABAJADORES.
		LINEAMIENTOS PARA CAPACITACION AL PERSONAL.
	SEGURIDAD EN LAS INSTALACIONES DE UNA SUBESTACIÓN.	LINEAMIENTOS PARA CONTROL DE ACCESO A PERSONAL.
		LINEAMIENTOS PARA EQUIPOS DE VIDEOSUPERVISIÓN Y ALMACENAMINETO DE VIDEO.

Nota:

I. Esta metodología tomará como referencia a la propuesta del diagrama 2 sin dejar a un lado la posibilidad de implementar la propuesta del diagrama 1.

II. Los modelos de verificación de la metodología se encuentran en el ANEXO B, "B-20_MODELOS DE DOCUMENTACIÓN DE VERIFICACIÓN" Estos documentos son guías de cómo se debe documentar la aplicación de la metodología, considere que los modelos no son mandatorios y tampoco se limitan a lo mencionado.

2.3.3 CAPITULO 1: ARQUITECTURA FÍSICA PARA UNA RED LAN EN UNA SUBESTACIÓN.

Propósito:

- Proponer una topología física redundante.
- Plantear una arquitectura que cumpla con requisitos mínimos para una buena operación.
- Proponer una estructura que sea flexible, administrable y segura.
- Mejorar su rendimiento.
- Proponer lineamientos claros que permitan guiar al personal con la instalación de los equipos.

2.3.3.1 Categoría: ARQUITECTURAS FÍSICAS SUGERIDAS.

La arquitectura presentada en este proyecto se fundamenta en la norma IEC 61850-7 (Basic communication structure for substation and feeder equipment [12].

DIAGRAMA 1.

En la figura 2.43. se observa la arquitectura física propuesta para una red LAN en una subestación eléctrica.

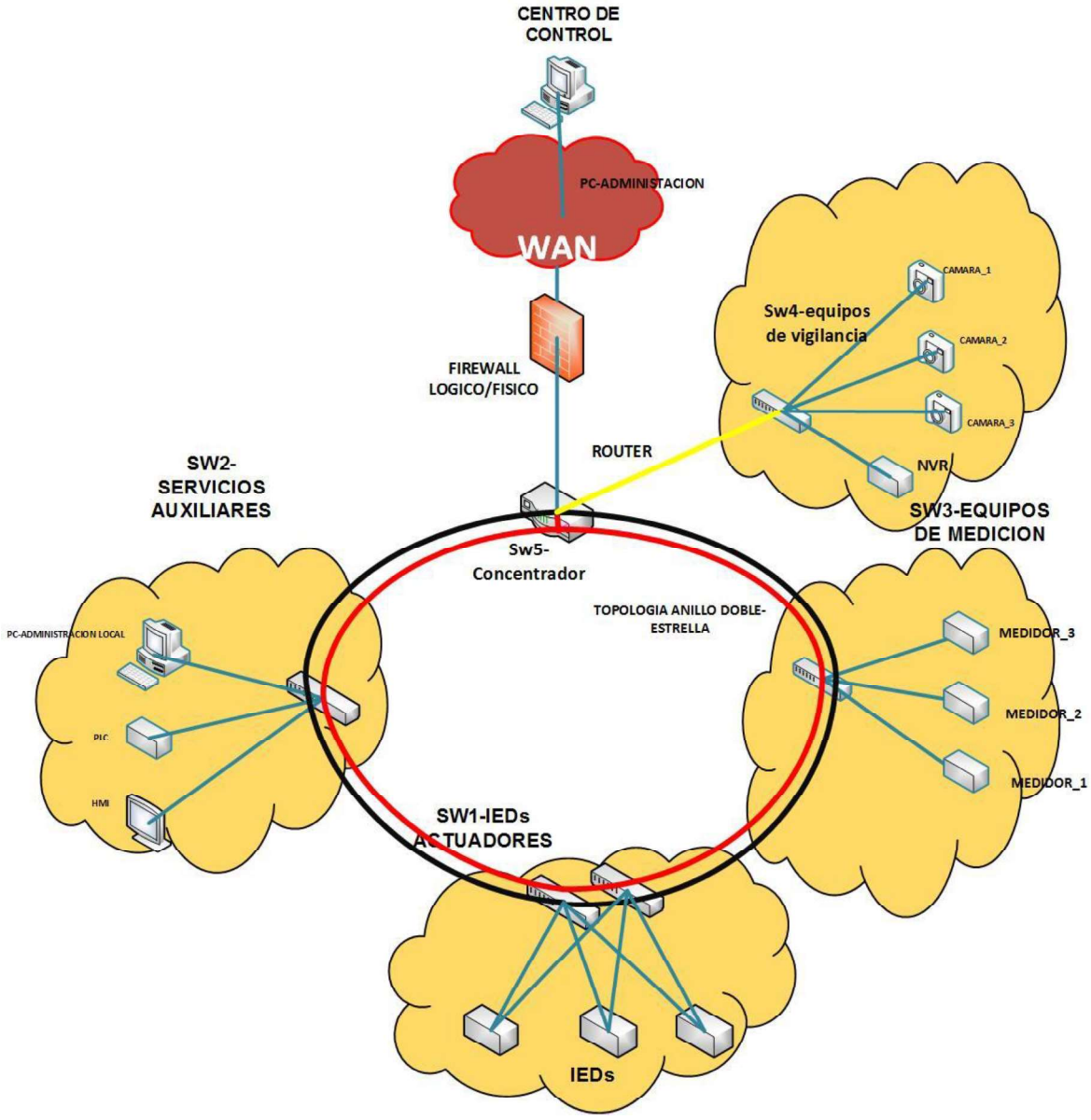

Figura 2.43. Arquitectura física con router concentrado

- **DIAGRAMA 1 CON VARIACIÓN AL INTRODUCIR UN SWITCH CONCENTRADO.**

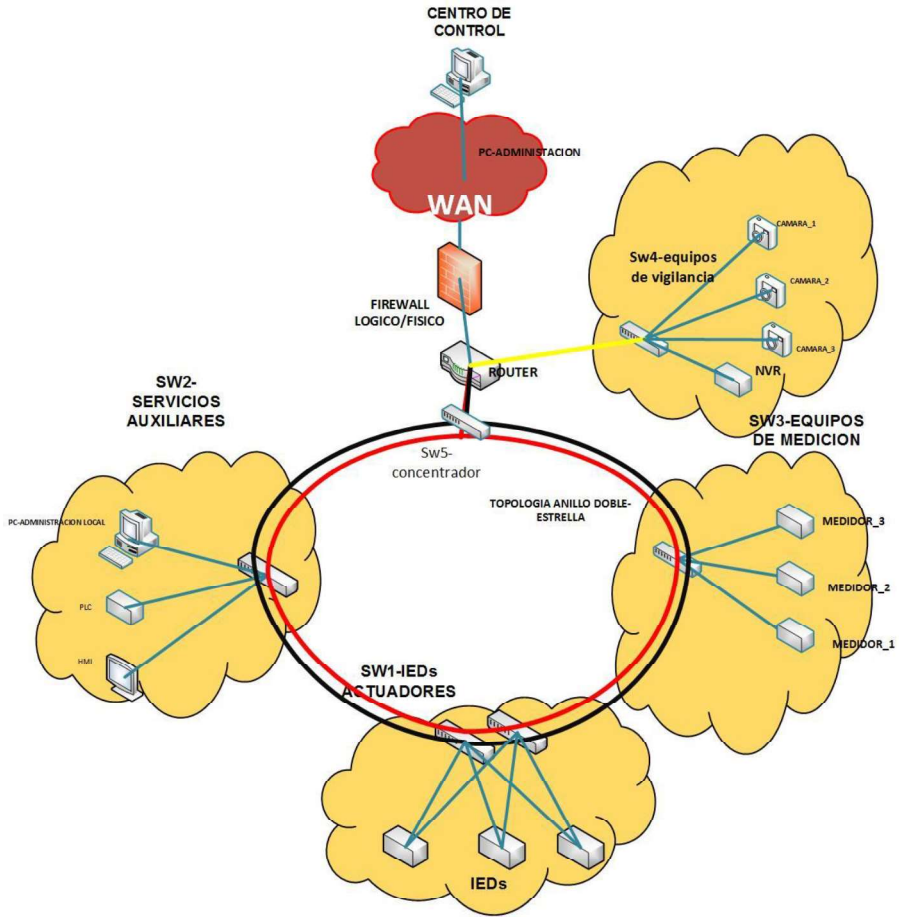

Figura 2.44. Arquitectura física para una red LAN de una subestación con switch concentrado

CARACTERISTICAS DE LA ARQUITECTURA DEL DIAGRAMA 1.

Las siguientes características detallan la arquitectura que se presenta en el diagrama 1 como referente para la implementación de una red LAN en una subestación eléctrica.

- La arquitectura del diagrama 1 tiene una topología en anillo doble, con ramales en cada uno de los equipos de conmutación (switches).
- La topología en anillo doble nos permite tener un sistema fiable donde uno de los anillos es usado para la transmisión de información y el otro anillo es un anillo de reserva.
- En la parte superior se propone un firewall físico o lógico antes del router como equipo de protección principal.
- Cada uno de los equipos que se encuentran presentes en el anillo doble deben ser switches que presenten un mínimo de puertos de conexión, considerando todos los

equipos que se conectaran en el presente, y un 50% de disponibilidad de puertos sin usar, como reserva.

- Se debe agrupar los equipos de similares características en cada uno de los switches, por ejemplo, en el diagrama 1 se ha optado por separar los equipos por funcionalidad, y se distingue 4 grupos denominados de la siguiente manera: SW1-IEDs (equipos de maniobra. Considere redundar con un switch si los IEDs permiten doble canal de comunicación), SW2-SERVICIOS AUXILIARES (equipos encargados de la operación interna de la subestación, en este grupo se propone colocar: PLC, HMI, PC administrativa.), SW3-EQUIPOS DE MEDICIÓN (equipos orientados a la medición de las variables de energía de las instalaciones de la subestación. Considere redundar con otro switch si los medidores permiten doble canal de comunicación) SW4-EQUIPOS DE VIGILANCIA (cámaras de vigilancia), los cuatro grupos presentados en esta sección no son mandatorios y puede ser sujeto a modificación, aquello dependerá de las necesidades o casos especiales que se presenten, los cuatro bloques presentados en esta sección son sugeridos.
- En la parte superior se presenta un router, el cual es encargado de realizar el proceso de enrutamiento y conexión de las redes, en este caso la red LAN de la subestación y la WAN. El dimensionamiento de este equipo dependerá de un análisis posterior orientado a la capacidad y tráfico que circula o concentra el router.
- Las conexiones de la topología LAN deben ser por medio de fibra óptica multimodo (tener presente la distancia del cableado para utilizar fibra multimodo o monomodo) para evitar interferencias electromagnéticas.
- Se debe tener una disponibilidad de 30% de puertos en el router libres de los que se plantea.
- En el caso de no cumplir con el inciso anterior se propone la concentración de los datos de la LAN por medio de un switch 5, para posteriormente enlazarlo con un router, como se aprecia en el diagrama de la figura 2.44.

REQUERIMIENTOS DEL DIAGRAMA 1.

Para dar paso al buen funcionamiento de esta arquitectura se recomienda tener en cuenta los siguientes ítems:

- Presentar el dimensionamiento de la red LAN esto conlleva a determinar el número de equipos que se instalaran para los diferentes servicios tanto para el proceso principal como los servicios internos necesarios para el funcionamiento.
- Organizar los equipos por su función, o por características similares.

- El diagrama como mínimo debe tener: un switch designado para los IEDs, un switch designado para las cámaras de vigilancia y un switch para equipos que no realicen actividades directamente del proceso, pero sirvan para mantener un buen funcionamiento de la subestación.
- Un router con la cantidad de puertos necesarios y con la capacidad de procesamiento necesaria para toda la red.
- El firewall debe ser físico.

VENTAJAS

- Al plantear una topología en anillo doble el sistema es redundante ya que presenta un mínimo de 2 caminos para transportar la información.
- Facilidad para encontrar errores en la red.
- Facilidad para realizar trabajos de mantenimiento de la red, sin la necesidad de detener el proceso de la subestación.
- Mantiene un orden de la red al presentar una organización de los equipos agrupados por su función.
- La arquitectura presenta una flexibilidad a la hora de implementar nuevos equipos tanto en el anillo principal como en cada uno de los ramales, sin interrumpir el proceso.
- Permite configuraciones de balance de carga.

POSIBLES DESVENTAJAS A CONSIDERAR.

- Se debe tomar en cuenta las distancias de conexión de los equipos y si la información se envía por cable de cobre o fibra óptica.
- La información que circula en esta arquitectura debe dar un mayor número de saltos para llegar a su destino, sin embargo, es más confiable por la redundancia de enlaces que presenta.

DIAGRAMA 2.

En la figura 2.45. se observa una variación, donde se establecen dos enlaces desde el router hacia los switches que comunican los reles.

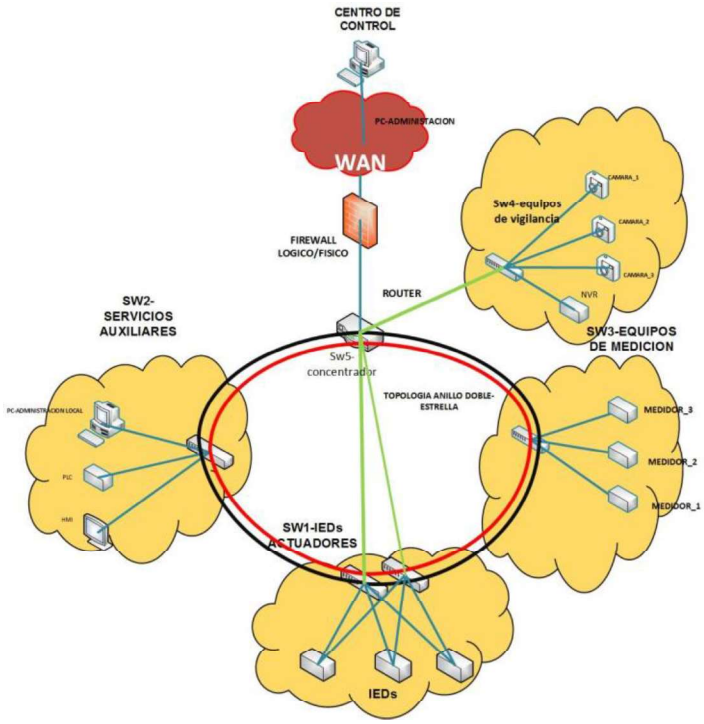

Figura 2.45. Arquitectura física propuesta para una red LAN de una subestación

- **DIAGRAMA 2 CON SWITCH CONCENTRADO Y DOBLE ENLACE.**

En la figura 2.46. cuenta con una variación al introducir un switch concentrado y dos enlaces directos desde sw5 hacia sw1 donde se conectan los relés de la subestación.

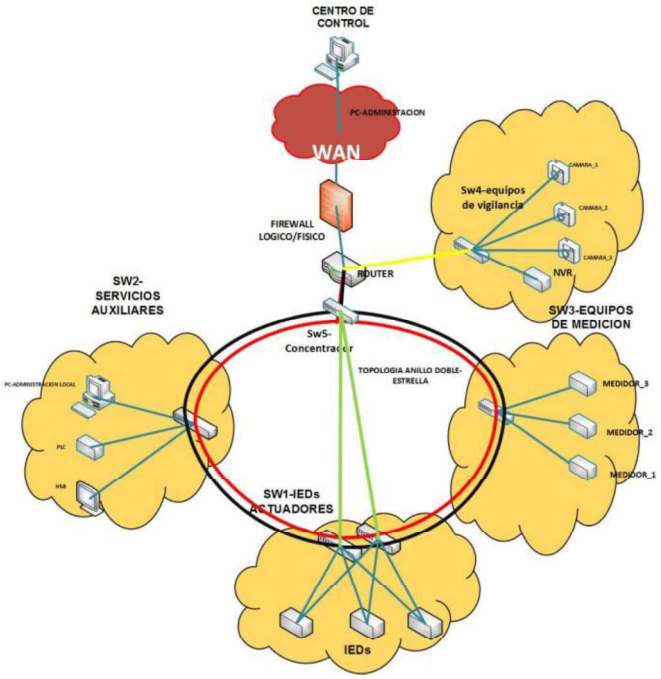

Figura 2.46. Arquitectura física propuesta para una red LAN de una subestación con los enlaces directos

CARACTERISTICAS DE LA ARQUITECTURA DEL DIAGRAMA 2.

Las siguientes características detallan la arquitectura que se presenta en el diagrama 2 como referente para la implementación de una red LAN en una subestación eléctrica.

- En la parte superior se colocó un firewall el cual puede ser físico o lógico, en esta propuesta se plantea colocar un firewall lógico ya que muchos routers prestan los servicios de filtrado.
- La arquitectura principal sigue siendo un anillo doble, pero se propone una conexión directa entre el router y el switch que conecta los IEDs.
- Existen varios tipos de IEDs, se recomienda que estos equipos tengan doble tarjeta de red, con la finalidad de redundar su comunicación con otro switch.
- Se debe agrupar los equipos de similares características en cada uno de los switches, por ejemplo, en el diagrama 2 se ha optado por separar los equipos por funcionalidad, y se distingue 3 grupos denominados de la siguiente manera: SW1-IEDs (equipos orientados a apertura/cierre y medición de circuitos de potencia), SW2-SERVICIOS AUXILIARES (equipos encargados de la operación interna de la subestación, en este grupo se propone colocar: PLC, HMI, PC administrativa.), SW3-EQUIPOS DE MEDICIÓN (equipos orientados a la medición de las variables de energía de las instalaciones de la subestación.) SW4-EQUIPOS DE VIGILANCIA (cámaras de vigilancia), los tres grupos presentados en esta sección no son mandatorios y puede ser sujeto a modificación, aquello dependerá de las necesidades o casos especiales que se presenten, los tres bloques presentados en esta sección son sugeridos.
- La configuración en anillo tiende a ser un poco lenta en comparación con otras configuraciones, con la conexión directa se mejora este factor.
- La arquitectura permite configuraciones de balance de carga.
- La conexión existente entre el router al switch1-IEDs disminuye las posibilidades de salida de servicio de la subestación, y disminuye los tiempos en que la red transporta la información, esta conexión debe ser considerada como principal.

REQUERIMIENTOS DEL DIAGRAMA 2

- Presentar el dimensionamiento de la red LAN esto conlleva a determinar el número de equipos que se instalaran para los diferentes servicios tanto para el proceso principal como los servicios internos necesarios para el funcionamiento.
- Organizar los equipos por su función, o por características similares.

- El diagrama como mínimo debe tener dos switches designados para los IEDs (considere que estos equipos son críticos para el manejo operación y maniobra de la subestación además generalmente presentan doble canal de comunicación), un switch designado para las cámaras de vigilancia y un switch para equipos que no realicen actividades directamente del proceso, pero sirvan para mantener un buen funcionamiento de la subestación.
- Un router con la cantidad de puertos necesarios y con la capacidad de procesamiento necesaria para toda la red.
- Esta configuración requiere un mayor número de interfaces.

VENTAJAS

- Al plantear una topología en anillo doble el sistema es redundante ya que presenta un mínimo de 2 caminos para transportar la información.
- Facilidad para encontrar errores en la red.
- Facilidad para realizar trabajos de mantenimiento de la red, sin la necesidad de detener el proceso de la subestación.
- Mantiene un orden de la red al presentar una organización de los equipos agrupados por su función.
- La arquitectura presenta una flexibilidad a la hora de implementar nuevos equipos tanto en el anillo principal como en cada uno de los ramales, sin interrumpir el proceso.
- Permite configuraciones de balance de carga.

POSIBLES DESVENTAJAS A CONSIDERAR.

- Como las exigencias del diseño son redundantes, la cantidad de equipos de networking es alto.
- Su administración es relativamente más compleja.
- La capacidad de procesamiento del equipo es mayor.
- Se necesita mayor cantidad de puertos en los equipos de red.
- El cableado es más complejo.

NOTA: Se debe tener una documentación clara y detallada que contenga las siguientes generalidades:

  - Una topología clara y detallada (las imágenes deben ser a color y de alta calidad.).
  - La nomenclatura debe ser clara y con letras arial, tamaño 12.

- Se debe asignar con detalle y coherencia la nomenclatura que se encuentra en la topología y en un registro que posteriormente se debe complementar con el direccionamiento de cada uno de los equipos, documentación de verificación en el ANEXO B, denominado “B-20_MODELOS DE DOCUMENTACIÓN DE VERIFICACIÓN” documento 1.

LINEAMIENTOS CONSTRUCTIVOS DE LOS EQUIPOS DE LA RED LAN DE LA SUBESTACIÓN.

REQUERIMIENTOS.

- **Los equipos deben ser robustos en su aspecto constructivo:**

  - Los equipos que conforman la red serán manejados en un área industrial por ello su carcasa debe ser metálica con buena ventilación.
  - Tener una certificación IPXX acorde al área donde los equipos desarrollarán sus actividades. Determine si el equipo se encontrara en exteriores o interiores esto dependerá en gran parte de las características constructivas de cada fabricante, sin embargo, se debe considerar: temperatura de exposición, humedad, si el equipo tendrá tendencia a sufrir golpes, exposición a líquidos, exposición a polvo o partículas de fibras orgánicas e inorgánicas.

- **Resistencia a EMI (interferencia electromagnética):**

Un parámetro importante a considerar es el ruido que producen elementos industriales, esto puede provocar un mal funcionamiento del equipo en las subestaciones eléctricas se maneja un alto diferencial de potencial, razón por la cual los equipos deben presentar certificaciones de protección contra interferencias electromagnéticas.

Nota: Estas recomendaciones no son mandatarias ni únicas, pero se recomienda tomar en cuenta el ambiente al que se encontraran sometidos los equipos de comunicación para procurar un mejor desempeño y durabilidad.

2.3.4 CAPITULO 2: ADMINISTRACIÓN Y GESTIÓN DE LA INFORMACIÓN DE UNA SUBESTACIÓN.

Propósito:

- Presentar un direccionamiento ordenado.
- Disminuir los tiempos de resolución de problemas.
- Mantener una organización jerárquica en los equipos.

CONSIDERACIÓN.

En base a la topología física planteada podemos realizar el diseño de la gestión y administración de la red de la subestación tomando en cuenta que en esta sección solo se presentara parámetros de funcionamiento de la red, posteriormente se realizara un análisis de la seguridad del sistema allí se planteará lineamientos referentes a la configuración de los equipos que permitan tener una estructura de red acorde con las necesidades del proceso.

- Equipos de proceso.
- Equipos de protección local y administración local.
- Administración de equipos de networking de una subestación.

2.3.4.1 Categoría: EQUIPOS DE PROCESO.

Son los equipos considerados de operación directa en el proceso de distribución energética.

DISPOSITIVOS ELECTRONICOS INTELIGENTES (IEDs).

- **IEDs de protección (Relés).**

Los relés en la subestación realizan el monitoreo del circuito al que fue asignado y envían señales de control y alarma en el caso de existir una falla además tiene la capacidad de reaccionar contra sobrecarga.

- **IEDs de medición (Medidores).**

Generalmente los medidores realizan actividades de medición como voltaje, corriente, potencia y frecuencia. Estos equipos deben tener la capacidad de una administración local y remota.

Requerimientos básicos de configuración de los IEDs.

- Si la administración es local se debe realizar configuraciones de ingreso por credenciales asignadas por medio de las configuraciones básicas de seguridad, todos los equipos tienen en sus características configuraciones básicas de seguridad las cuales deben ser activadas.

- Si la comunicación es de forma remota se prefiere que se use un cliente que pueda mantener una comunicación segura para ello es recomendable usar el protocolo SSH, en el caso de no ser posible usar este protocolo se procede a la configuración de la activación de comunicación remota por medio del protocolo telnet.
- La configuración y activación de estos protocolos debe formar parte de la configuración del equipo a la hora de su implementación.
- Esta configuración procede para todos los IEDs que formen parte del proceso.

2.3.4.2 Categoría: EQUIPOS DE PROTECCIÓN LOCAL Y ADMINISTRACIÓN LOCAL.

En esta sección se presentarán equipos que no son parte directa de las prestaciones de la subestación sin embargo son necesarias para la operación interna de la subestación, equipos tales como:

CONTROLADOR LOGICO PROGRAMABLE (PLC).

Este equipo es usado para administrar las alarmas internas de la subestación como fallas de los equipos de ventilación de los transformadores sensores de temperatura, etc.

Desde el punto de vista de la red LAN el PLC debe tener las siguientes características administrativas:

- Presentar un medio local y remoto de configuración de preferencia cifrado en el caso de que la comunicación sea remota para ello si el equipo permite el uso de protocolo SSH caso contrario se debe habilitar la comunicación por medio de Telnet.
- En muchos de los casos actuales los transformadores integran un control administrativo similar a un PLC, el cual debe ser administrado de igual forma.

COMPUTADOR PERSONAL (PC).

En cada una de las subestaciones es necesario tener un equipo que permita una administración local y cargado con la información y programas necesarios para respaldar el funcionamiento de la subestación.

El equipo debe presentar las siguientes características mínimas:

- debe presentar un procesador que satisfaga las necesidades de procesamiento de las aplicaciones que se instalaran en dicho equipo. Como referencia para el programa OASyS de Scheneider un procesador Intel I7 de séptima generación es suficiente.
- Una memoria RAM de 4 GB.
- La pantalla debe ser táctil y de construcción industrial.

INTERFAZ HOMBRE MAQUINA(HMI).

Es recomendable tener una pantalla táctil con una interface que permita la visualización de forma gráfica del proceso local, esto con la finalidad de tener una rápida información de lo que está sucediendo en la subestación.

EQUIPOS DE SEGURIDAD FÍSICA DE LA SUBESTACIÓN.

Los equipos que se tiene en esta etapa son equipos de vigilancia que no realizan una actividad directa con el proceso sin embargo es indispensable para la seguridad de las instalaciones de la subestación, la cantidad de equipos de vigilancia dependerán de las dimensiones de la casa de control, en una etapa siguiente se realizara observaciones detalladas de los equipos.

2.3.4.3 Categoría: EQUIPOS DE NETWORKING DE UNA SUBESTACIÓN.

Como se observó en la topología física del diagrama 1 y 2 se mantiene una configuración en anillo doble. Esto con la finalidad de tener un sistema de comunicación redundante.

LINEAMIENTOS DE CONFIGURACIÓN GENERAL BÁSICA.

REQUERIMIENTOS.

- No permita que el nombramiento de los equipos sea por defecto.
- Identifique a cada uno de los equipos de networking por un nombre establecido.
- Genere la documentación necesaria para la asignación de nombres a los equipos de networking, documentación de verificación ANEXO B, “B-20_MODELOS DE DOCUMENTACIÓN DE VERIFICACIÓN” documento 2.

LINEAMIENTOS DE ADMINISTRACIÓN DEL ROUTER.

REQUERIMIENTOS.

- En el caso de no colocar un firewall físico se recomienda que el router tenga la capacidad de configurar un firewall lógico, sin antes destacar que la mejor opción es colocar un firewall físico.
- Permitir comunicación por medio de VPN. Si la red se encuentra extendida hacia las subestaciones, se debe tener una clara diferenciación entre la red administrativa y la red de comunicación industrial, por esta razón se considera que la red LAN de las subestaciones son seguras a partir del punto en el cual se encuentra dentro de la red de la empresa, esto considerando que existe una clara diferenciación de la red administrativa como de la red de comunicaciones de las subestaciones.

SEGURIDAD EN EL BORDE DE LA RED LAN (ROUTER).

REQUERIMIENTOS.

Generación de ACL (Listas de Control de Acceso).

- Con las listas de acceso es posible limitar el tráfico de la red elevando el rendimiento por ejemplo restringir él envió de video o audio hacia el interior de la red LAN.
- Permite tener un adecuado control de flujo de tráfico restringiendo las entregas de actualizaciones de routing, esto con la finalidad de conocer el origen de las actualizaciones.
- Restricción selectiva de acceso a diferentes hosts.
- Filtración de tráfico, con esto se pretende tener un tráfico selectivo.
- Discriminar al acceso de los datos por usuario, con esto se pretende limitar la información que se genere dentro de la red por medio de los usuarios.

Proceso de traducción de direcciones de red (NAT).

- Determinar si la interfaz es pública o privada, si es publica es mandatorio que se cumpla el proceso de NAT en el caso de ser privada es posible que se asigne una dirección específica para la red interna.
- Determinar la interfaz por la cual se configura NAT, recuerde que esta interfaz será el medio de conexión entre el “exterior (global) e interior (local)” de la red de la subestación.
- En una red de comunicación de una subestación el direccionamiento es estático por ello se debe asignar una dirección de entrada y salida para la red interna y externa.

- Determinar las direcciones global y local.
- Se debe configurar el proceso de NAT en el router.
- La configuración debe contemplar una dirección de entrada y otra dirección de salida.
- Si es necesario se debe asignar además el puerto original y el puerto al cual se desea trasladar.
- Realizar una documentación adecuada de la traducción de la red global ante la red local.
- El proceso de NAT se lo debe realiza en TCP, **NO** en UDP y de preferencia a todas las direcciones de la red LAN.

IMPLEMENTACIÓN DE UN RUTEO ESTÁTICO COMPLETAMENTE ESPECIFICADO.

- La finalidad de tener un ruteo completamente especificado es protección y rendimiento, ya que a menos que se realicen modificaciones de la red en ella no debe conectarse ningún equipo ajeno al funcionamiento de la subestación.
- La finalidad de tener un ruteo estático es incrementar el rendimiento de la red.
- Además, es un detalle de seguridad ya que el router no necesita aprender su ruta ya que esta se encuentra fija en la subestación, esta también será una alarma para detectar comportamientos anormales dentro de la red por si una persona con objetivos maliciosos vulnera la red.
- Si se considera una ruta estática se debe desactivar el uso del protocolo DHCP en el router.
- Documentación pertinente a las configuraciones de ruteo estático ANEXO B, "B-20_MODELOS DE DOCUMENTACIÓN DE VERIFICACIÓN" documento 2.

ADMINISTRACIÓN REMOTA.

Para realizar la administración remota se debe considerar que la comunicación que se enlaza será desde el centro de control, por lo tanto, se plantea la existencia de una PC de administración o un grupo de computadoras que se encuentren en el centro de control, desde donde se permita realizar una comunicación remota. En la figura 2.47 se muestra la arquitectura para el desarrollo.

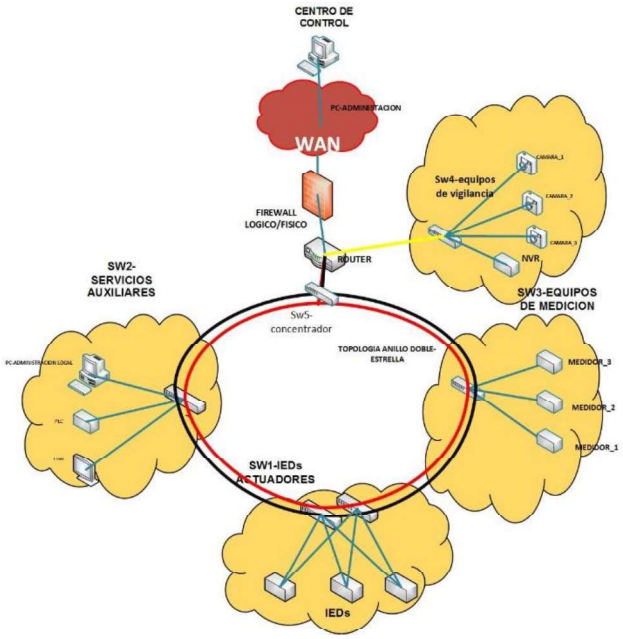

Figura 2.47. Arquitectura física para una red LAN de una subestación con switch concentrado

- En la parte superior de la figura 2.47 se observa una computadora representativa o grupo de computadoras con permisos necesarios para realizar una administración remota. Este equipo debe ser designado como punto de enlace entre la subestación.
- El equipo debe ser administrado exclusivamente por personal capacitado y con la asignación de credenciales.
- Se debe tener un acceso remoto hacia los equipos dentro de la subestación para ello se debe restringir el protocolo telnet en caso de ser posible, y usar SSH, posteriormente se detallará el uso de estos protocolos.
- El router, switches, IEDs, PC de administración local, HMI (de ser necesario), PLC deben permitir la configuración del protocolo SSH.
- Se recomienda activar el protocolo RDP (Remote Desktop Protocol) para tener la administración por medio de escritorio remoto, esto en el caso que los equipos usen un sistema operativo de Microsoft.
- La comunicación de escritorio remoto es realizada desde el equipo administrativo del centro de control con el equipo “PC-ADMINISTRACION LOCAL”.

REQUERIMIENTOS.

- Los equipos deben permitir la configuración del protocolo SSH.

REDUNDANCIA EN LOS ENLACES DEL ROUTER.

Es primordial tener redundancia en el equipo de borde para eso se debe utilizar configuraciones físicas y lógicas. Para ello se propone el uso de protocolos como Hot Standby Router Protocol (HSRP) (propietario cisco) o Virtual Router Redundancy Protocol (VRRP) (no propietario definido en el RFC 3768).

REQUERIMIENTOS.

- Disponibilidad de un router o varios routers.
- La capacidad de configuración de HSRP o VRRP.
- Generar la documentación necesaria donde se especifiquen características de configuración, documentación de verificación ANEXO B, "B-20_MODELOS DE DOCUMENTACIÓN DE VERIFICACIÓN" documento 2.

LINEAMIENTOS DE ADMINISTRACIÓN DE LOS SWITCH.

CAPACIDAD DE REALIZAR REDES LAN VIRTUALES.

REQUERIMIENTOS.

- Las redes LAN virtuales o mejor conocidas como VLAN permiten una adecuada segmentación, y evita mensajes de difusión (broadcast), además una flexibilidad de organización (si se necesita mayor información se recomienda referirse a las especificaciones: IEEE 802.Q).
- En la subestación se deben de generar básicamente tres VLANs las cuales son: VLAN de equipos orientados al proceso en el caso de subestaciones todos los relés, VLAN de equipos auxiliares y VLAN de equipos complementarios.
  - Generar la documentación necesaria donde se especifique las VLANs creadas, documentación de verificación ANEXO B, "B-20_MODELOS DE DOCUMENTACIÓN DE VERIFICACIÓN" documento 2.

- **VLAN de equipos auxiliares.**

  - En esta VLAN se tendrán todos los dispositivos que realicen actividades auxiliares para el funcionamiento de la subestación por ejemplo un PLC que se encargue de la ventilación de los transformadores, sensores de temperatura,

entre otros dispositivos formen parte de la operación de la subestación, pero no sean parte del proceso principal que es la distribución de energía eléctrica.

- El monitoreo de las UPS forman parte de los servicios auxiliares.
- Todos los equipos que realicen actividades de seguridad física de la subestación. Y se requiera de un monitoreo deben de pertenecer a esta VLAN.
- En esta red virtual también se puede colocar la PC de monitoreo local, esta PC está orientada a tener toda la documentación y software que se requiera para realizar configuraciones dentro de la subestación además este quipo puede prestar diferentes servicios como una comunicación por medio de escritorio remoto.

- **VLAN de equipos complementarios.**

En esta VLAN se recomienda que se coloquen equipos referentes a cámaras de vigilancia y equipos de almacenamiento audio y video como NVR.

Se debe asignar una dirección única a cada una de las cámaras para ello las cámaras deben ser IP, además de poseer una visión nocturna.

Cada subestación debe tener un mínimo de cuatro cámaras colocadas recomendablemente de la siguiente forma:

- **Cámara 1:** esta se mantendrá colocada con línea de vista hacia el RACK principal el cual debe encontrarse dentro de la casa de control.
- **Cámara 2:** esta se mantendrá colocada con línea de vista hacia la puerta de ingreso de la casa de control de la subestación.
- **Cámara 3:** esta cámara se colocará en los exteriores de la subestación con línea de vista directamente hacia la puerta de entrada a las instalaciones de la subestación.
- **Cámara 4:** esta cámara debe colocarse con línea de vista hacia los equipos de campo como las bahías.
- **NVR:** NVR (Network Video Recorder) es el equipo donde se grabarán los videos de seguridad, la capacidad de este debe ser mínimo 1TB.

Se debe mantener un adecuado mantenimiento de los equipos.

Revisión del funcionamiento de las cámaras en periodos de tiempo prudentes recomendado cada 3 meses, borrado de los videos del NVR cada semana si se sigue el modelo de cuatro cámaras y un NVR (1TB) dado que en las subestaciones solo existe

una línea de comunicación se propone que el NVR se encuentre en la localidad de cada subestación.

- **VLAN de proceso principal.**

En esta red virtual se colocarán los equipos que estén orientados directamente al proceso de la subestación como: relés y medidores (estas especificaciones no se limitan a los equipos mencionados, pero si deben pertenecer al grupo mencionado).

CONFIGURACIÓN DE INTERFACES TRONCALES ENTRE LOS SWITCHES.

REQUERIMIENTOS.

- Los switches deben permitir la configuración de VLANs nativas en base a las especificaciones de la IEEE 802Q.
- Se deben configurar enlaces troncales a lo largo de toda la red de anillo doble.
- El HMI y la PC-ADMINISTRACION LOCAL se podrían configurar para que tengan acceso hacia las demás VLANs o formen parte de la VLAN que se genera en el switch de los IED de accionamiento y medidores.

PROTOCOLOS DE REDUNDANCIA.

Los protocolos de redundancia nos permiten mejorar la confiabilidad y la disponibilidad ya que se genera una estructura redundante en capa 1 y capa 2, evitando lazos en capa dos y generar un sistema más eficiente. Para ello se tiene:

REQUERIMIENTOS.

- El dispositivo debe tener la capacidad de manejar protocolos como STP o RSTP.
- STP (spanning tree protocol) o RSTP (rapid spanning tree protocol) que se encuentra especificado en la IEEE 802.1w.
- Es importante al activar el protocolo RSTP y determinar las rutas de redundancia que se ejecutaron a partir del algoritmo de redundancia.
- En una gran mayoría de switches el protocolo RSTP se encuentra activado por defecto, en el caso de no ser así realizar verificaciones de funcionamiento del protocolo.

- Generar la documentación necesaria donde se especifiquen características de configuración, documentación de verificación ANEXO B, “B-20_MODELOS DE DOCUMENTACIÓN DE VERIFICACIÓN” documento 2.

PROTOCOLOS DE BALANCE DE CARGA Y AGREGACIÓN DE ENLACES.

Es importante considerar que las interfaces físicas que se establecen en la arquitectura del diagrama 1 y 2 son con el objetivo de redundar en la red, aprovechando estas interfaces no es recomendable que permanezcan inactivas, para ello se configura y se usa el concepto de EtherChannel por medio del protocolo PAgP (protocolo de agregación de puertos) si se usa equipos de la marca CISCO, si se usa otros equipos se presenta el protocolo LACP (protocolo de control de agregación de enlaces), estos protocolos nos permiten realizar:

- Balance de carga.
- Incrementar la velocidad de transmisión de la información, por ende, mejora los tiempos de envío y recepción de información en la red.
- Permite la agrupación de interfaces físicas, haciendo que se comporten como un enlace lógico único.
- Disminuye la latencia en los equipos.
- Eleva la eficiencia del sistema.
- Se usa para mejorar el rendimiento de las VLAN.

Nota: PAgP y LACP realizan el mismo trabajo y tiene el mismo objetivo, la diferencia es que PAgP es exclusivo de equipos CISCO y LACP es un protocolo que se encuentra en IEEE 802.1AX (redes de área local y metropolitana).

En esta metodología se usará como referencia al protocolo LACP.

REQUERIMIENTOS.

- Determinar si el equipo permite el manejo del protocolo PAgP o LACP (recordando que si usa PAgP es exclusivo de dispositivos CISCO.).
- En la actualidad se pueden formar hasta 8 interfaces físicas en un enlace lógico usando el protocolo LACP, sin embargo, se recomienda la revisión de los equipos ya que esto dependerá de los fabricantes y las mejoras que realicen continuamente.
- Determinar los enlaces físicos en la topología que se desea agrupar para formar un solo enlace lógico.

- Los enlaces que se desea agrupar deben tener la misma velocidad de trasmisión por ejemplo si son fastEthernet o gigabiEthernet, no es posible realizar configuraciones de diferentes velocidades de transmisión.
- Primero se debe activar el protocolo ¨modo activo¨.
- Generar el canal de grupo este generalmente es asignado por medio de un número.
- Recuerde que estos enlaces deben ser troncales, así que deben configurarse como troncales.
- Posteriormente se da el permiso para el tránsito de las VLAN que van a circular.
- Después de realizar las configuraciones de la habilitación de los canales es recomendable verificar la configuración.

LINEAMIENTOS PARA LA ADMINISTRACION DE PROTOCOLOS INDUSTRIALES EN LA RED LAN DE LA SUBESTACIÓN.

NOTA: esta sección no pretende especificar los protocolos industriales como tal, ya que excede el alcance de este trabajo, lo que se pretende es recomendar una homogenización de los protocolos que se utilicen en la red de comunicaciones de las subestaciones eléctricas.

DNP3

El protocolo que se recomienda usar en los equipos industriales de campo como medidores y relés es el DNP3. Por lo tanto, los equipos que formen parte de esta sección de campo deben presentar esta característica.

REQUERIMIENTOS.

- el dispositivo debe tener la capacidad de implementar este protocolo en TCP.

IEC-61850 GOOSE.

Si se desea implementar protocolos como GOOSE se debe utilizar el protocolo IEC-61850, se recomienda que para este protocolo se trabaje con equipos de una sola marca para evitar problemas de interoperabilidad.

Si se desea mantener una comunicación entre varias subestaciones es importante la habilitación de la mensajería GOOSE ya que esta nos permitirá una comunicación horizontal entre los dispositivos de accionamiento como los relés.

REQUERIMIENTOS.

- Habilitación del servicio de mensajería GOOSE en los equipos como IEDs de accionamiento.
- Se puede realizar coordinación entre subestaciones para ello se debe configurar el protocolo en el router de cada una de las subestaciones.
- Se debe especificar el tipo de alarma o accionamiento que se desea coordinar de forma local o entre subestaciones.

LINEAMIENTOS PARA LIMITAR LA CONEXIÓN DE DISPOSITIVOS EXTERNOS POR MEDIO DE LA ADMINISTRACIÓN DE PUERTOS FÍSICOS.

Se debe restringir la conexión de dispositivos ajenos a los equipos de networking, ya que estos son los que presentan características de configuración para limitar conexiones de equipos intrusos a la red LAN de las subestaciones.

- Esta configuración permite que no se conecten más equipos a los equipos de networking establecidos en la red LAN de la subestación.
- Bloqueo del puerto al desconectar un elemento de networking que no esté registrado su dirección MAC.

REQUERIMIENTOS.

- Registro de admisión en el puerto por medio de la dirección MAC.
- Se debe bloquear todo equipo que no forme parte de los registros y direcciones asignadas para la administración.
- Si se realiza una configuración local, el equipo debe encontrarse con todos los registros y debe ser de uso exclusivo para la configuración, control y manejo de los equipos de las subestaciones.
- Si se desea una administración local se debe configurar el puerto con un número máximo de direcciones MAC.
- Se debe especificar el caso de violación y la acción a tomar, esto dependerá del equipo que se configura, pero en general los equipos de networking actuales presentan configuraciones al violentar un puerto, estas pueden ser:

    - Shutdown: bloqueo del puerto conectado.
    - Protect: impide él envió de tramas sin la necesidad de bloquear el puerto.

- Restric: restringe él envió de tramas sin bloquear el puerto, pero además envía un mensaje por medio del protocolo SNMP como alarma.

Es recomendable usar equipos que permita el envío de mensajes de alarma ya que esto incrementara la seguridad del sistema.

LINEAMIENTOS PARA ASIGNACIÓN DE DIRECCIONES A LOS DISPOSITIVOS.

DIRECCIONAMIENTO DE LA RED LAN.

- La dirección se asigna de forma única y exclusiva para cada uno de los equipos dentro de la subestación.
- Se puede utilizar un direccionamiento tipo IPV4 o IPV6 esto dependerá de la disponibilidad de direcciones en la red. Además considere que en la actualidad se habla del internet de las cosas (IOT) esto podría incrementar el número de direcciones razón por la cual se podría migrar a IPV6.
- Se debe presentar el direccionamiento de cada uno de los equipos de las subestaciones en función de la tabla 2.17.

Tabla 2.17. Modelo de organización del direccionamiento de los equipos dentro de las subestaciones

UBICACIÓN	RED	PREFIJO DE LA MASCARA	MASCARA	IP INICIO	IP FINAL	PUERTA DE ENLACE	OBSERVACIONES
Nombre de la subestación	xxx.xxx.xxx.xxx	/xx	xx.xx.xx.xx	xx.xx.xx.xx	xx.xx.xx.xx	xx.xx.xx.xx	Especificar su uso o condición.

- **UBICACIÓN:** se debe colocar la referencia de la subestación como el nombre de la localidad o el nombre de la subestación que debió ser asignada.
- **RED:** se refiere al segmento de red que fue asignado a la subestación, esta debe contar con un modelo similar a 172.154.02.0.
- **PREFIJO DE LA MASCARA:** el prefijo de la máscara es el encargado de indicarnos cuál es el segmento de red y el diferencial del host, y se debe expresar de la con una barra diagonal seguida de dos dígitos que indican el segmento de red (/xx).
- **MASCARA:** en esta sección se debe detallar la máscara de la siguiente forma xxxx.xxxx.xxxx.xxxx.
- **IP INICIO:** es importante mantener un registro de la primera dirección útil en la red.

- **IP FINAL:** registrar la dirección final útil dentro de la red.
- **PUERTA DE ENLACE:** registro de la dirección de salida de la subestación.
- **OBSERVACIÓN:** nombrar alguna característica del equipo.

LINEAMIENTOS PARA SEGMENTACIÓN DE LA RED Y CREACIÓN DE REDES VIRTUALES (VLANs).

GENERACIÓN DE REDES VIRTUALES.

Como se estableció en el capítulo 2, categoría: equipos de networking de una subestación, lineamientos de administración de switch, ´´Capacidad de realizar redes LAN virtuales´´, este es un requerimiento de los switches que se debe tener en cuenta en la implementación de la red LAN de las subestaciones, en esta sección se detallara como deben estar estructuradas estas redes virtuales.

Partiendo del planteamiento del capítulo antes mencionado donde se tienen:

- VLAN de equipos auxiliares (equipos para la buena operación de los equipos eléctricos y demás equipos que no sean directamente del proceso).
- VLAN de equipos complementarios (cámaras de vigilancia).
- VLAN de proceso principal (medidores y equipos de accionamiento como los relés y medidores).

Al asignarse la red a la subestación, esta debe ser segmentada en tres grupos, así usando el segmento de red de la subestación EL RETORNO 172.17. XX. XX.

REQUERIMIENTOS.

- Determinar el número de VLANs que se van a crear.
- Constatar el número de VLANs permitidas en el equipo.
- Asignación de las tres redes virtuales a un número o a un nombre.
- Asignación del puerto, (recuerde que la creación de una red virtual se encuentra asociada a un puerto.)
- Asigne la dirección IP de la red virtual.

A continuación, se presenta un ejemplo de cómo se debe ejecutar la implementación de la red virtual.

1. **VLAN 10**: asignación de la red virtual. (Cuando se realiza la creación de una red virtual se asigna generalmente un número lógico a la red virtual).

2. **VLAN de equipos auxiliares**: nombramiento de la red virtual (posterior al número de red virtual se debe nombrar a la red, el nombre se asignará con referencia a la actividad que realizan los equipos que se encuentran dentro de esta red virtual).
3. **Asignación de interface:** se debe asignar una única interface para cada uno de los equipos que pertenezcan a la VLAN que se desea comunicar.
4. Cuando se asigna el direccionamiento a los equipos es una buena práctica incluir la numeración usada para la VLAN que pertenece. Por ejemplo, tenemos: IP Address 172.17.**10**.10, el número 10 es referencia al direccionamiento IP referente al número de la VLAN creada en el punto 1.
5. Recuerde que generalmente la red virtual 1 no se debe usar ya que en los switches esta red virtual acoge a todos los puertos del switch por eso se recomienda usar una VLAN de administración que es la encargada de dar paso a las VLAN etiquetadas.

NOTA: Este procedimiento se debe realizar a cada una de las redes virtuales que se desea crear. Hasta este momento se ha creado las redes virtuales de forma local en cada uno de los switches. Posteriormente se debe habilitar las redes troncales las cuales son las que se encuentran conectando o comunicando entre switches, en la figura 2.48. se puede observar las redes virtuales y las redes troncales.

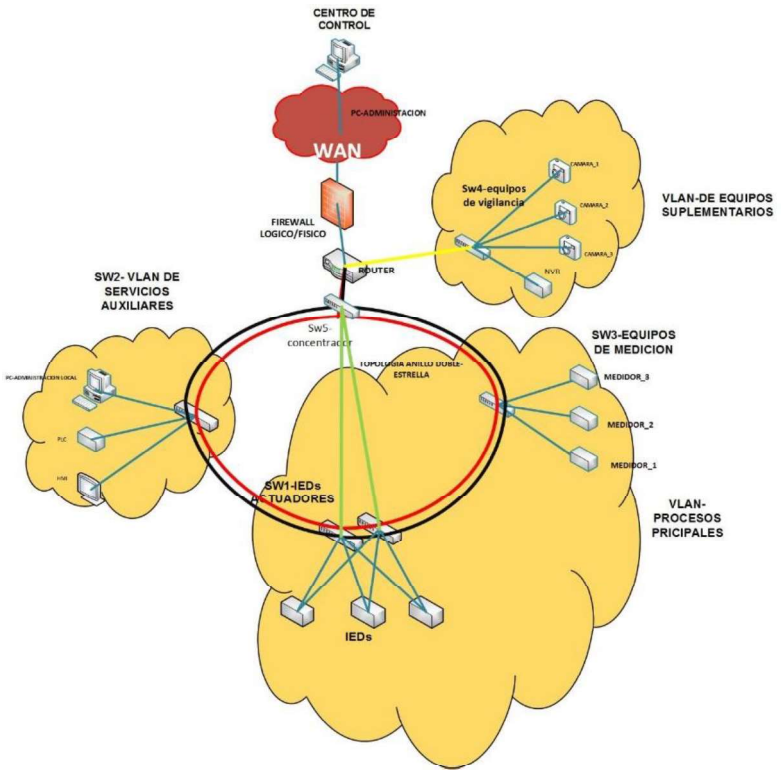

Figura 2.48. En la presente figura se observa diferenciadas las 3 redes virtuales

GENERACIÓN DE REDES VIRTUALES TRONCALES.

Las redes troncales nos permitirán encaminar la información por cada uno de los switches que se encuentran comunicados.

REQUERIMIENTOS.

- Identificar los enlaces que existen entre los switches, partiendo de la figura 2.46 se pueden identificar 4 enlace troncales (considere las interfaces redundantes).
- El encapsulamiento para los enlaces troncales debe ser 802.1q, este encapsulamiento debe verificarse que se encuentre activado en caso de no estar activo.
- En cada uno de los enlaces entre los switches debe establecerse las VLAN que permitirá que formen parte del tráfico, así que se debe permitir la circulación de las VLAN que se desean en el caso de la figura # serán 3 VLANs.
- Considere que algunas marcas de equipos de comunicación no usan el termino troncal sino etiqueta (tag) sin embargo realizan el mismo trabajo.

LINEAMIENTOS PARA SINCRONIZACIÓN DE EQUIPOS DE NETWORKING.

Es importante que los equipos se encuentren sincronizados, para ello se recomienda utilizar un equipo que administre la sincronización de todos los equipos que estén en la red de la subestación.

REQUERIMIENTOS.

- Todos los equipos deben permitir la sincronización por medio de un servidor que constantemente este sincronizando a los equipos.
- Instalar un equipo de sincronización en la subestación.
- Realizar las configuraciones de sincronización reales para la localidad en la cual se encuentran, esto se refiere a determinar el tiempo universal coordinado (UTC) de la localidad.
- El protocolo que se recomienda utilizar es el protocolo simple de hora de red (SNTP), sin embargo, existen otros protocolos como el protocolo de tiempo de precisión (PTP), pero se debe determinar primero si todos los dispositivos presentan configuraciones de esta característica.

LINEAMIENTOS PARA LA CONFIGURACIÓN DE CALIDAD DE SERVICIO.

Realizar configuraciones de calidad de servicio permitirá dar privilegios a ciertos paquetes de información. Se recomienda realizar configuraciones de calidad de servicio cuando se tenga en la red dos tipos de información, por ejemplo, información de los equipos de la subestación e información como mensajería, audio o video.

REQUERIMIENTOS.

- si se comparte información en la red se recomienda realizar la configuración de calidad de servicio en los switches y router.
- Los equipos de networking deben permitir realizar este tipo de configuración.
- Determinar la interfaz del router por la cual se ejecutará la calidad de servicio.
- Determinar la interfaz del switch por la cual se ejecutará la calidad de servicio.
- Siempre se dará privilegio a la información del proceso de la subestación ante cualquier información ajena a ella.

LINEAMIENTOS PARA EL RESPALDO DE CONFIGURACIONES DE LOS EQUIPOS DE NETWORKING.

Es importante mantener registro de las configuraciones realizadas en los equipos de networking, por si estos necesitan ser reemplazados.

REQUERIMIENTOS.

- El equipo debe permitir obtener respaldo de las configuraciones.
- Se debe almacenar las configuraciones de forma digital.
- Verificar cual es el método por el cual se debe obtener el respaldo de información del equipo y como se puede ingresar la configuración hacia el equipo.

2.3.5 CAPITULO 3: SEGURIDAD EN LAS INSTALACIONES Y RED LAN DE UNA SUBESTACIÓN.

Propósito:

- Proponer parámetros que mejoren la seguridad de las instalaciones de la subestación.
- Proponer parámetros que mejoren la seguridad de la red LAN de la subestación.
- Dar una guía para llevar un buen funcionamiento de la red LAN de la subestación.
- Presentar lineamientos y recomendaciones del buen manejo de datos al personal.

- Dar lineamientos del manejo de asignación y manejo de credenciales.

2.3.5.1 Categoría: SEGURIDAD CIBERNÉTICA.

Consideración para la aplicación de la metodología.

- Establecer si se usará un firewall físico o un firewall por software integrado dentro del router en ambos casos se debe presentar los siguientes lineamientos.

LINEAMIENTOS DE CONTROL DE ACCESO.

CARACTERISTICAS DEL ROUTER O FIREWALL PARA ESTABLECER EL CONTROL DE ACCESO.

El acceso debe ser restringido tanto de entrada como salida para esto se deben crear ACLs (listas de control de acceso), las cuales permiten configurar la información que ingresa al sistema como la información saliente. A continuación, se dan algunas recomendaciones para la implementación de esta herramienta de regulación de acceso:

- El equipo debe permitir la configuración de listas de control de acceso (ACLs) extendidas.
- La configuración de las ACL debe encontrarse en el router/firewall que conecta la red interna con la red externa.
- Se debe configurar las ACLs para cada protocolo de red que se encuentre configurado en cada una de las interfaces del router.
- Las ACL se pueden configurar por protocolo, por interfaz y por sentido (información entrante o saliente del equipo).
- Las listas de acceso se fundamentan en permitir o denegar.
- Las listas de acceso deben ser lo más específicas posible, en ella se debe diferenciar y configurar de la siguiente forma: dirección de fuente, dirección de destino, protocolo e interfaz.

REQUERIMIENTOS.

Nota: Estos requerimientos no son mandatorios y pueden ser modificados dependiendo la justificación y las necesidades que se presenten.

- Se debe negar (visto desde la consola ubicada en el centro de control hacia el interior de la red LAN de la subestación), (listas de acceso de entrada) los siguientes:

    - Telnet (protocolo de comunicación remota no cifrado), este protocolo se debe restringir, en el caso que todos los equipos dentro de la subestación eléctrica tengan la posibilidad de habilitar la comunicación remota por medio de SSH, en el caso que no se tenga disponible este protocolo se debe habilitar telnet, en el elemento gestor, sea este un router o firewall o ambos, pero se debe mantener habilitado en los demás equipos el protocolo SSH y negar el protocolo Telnet.
    - Denegación de actualizaciones automáticas como: actualizaciones de parches, actualizaciones de software de dispositivos y sistemas operativos de cada uno de los elementos dentro de la red.
    - Protocolos de audio y video (como: RTSP, RTP, y similares).
    - Denegar todo host que no se encuentre registrado como equipo habilitado para la administración remota.
    - Se debe usar como protocolo de transporte a TCP por lo tanto UDP es un protocolo que se debe negar.
    - Si los equipos permiten una administración por medio del browser
- Se debe implementar una ACL por protocolo, con la finalidad de limitar los protocolos que se manejen dentro de la red LAN.
- Se debe implementar una ACL por interfaz, se debe usar la interfaz de cada uno de los equipos para direccionar la información.
- Se debe permitir (visto desde la consola ubicada en el centro de control hacia el interior de la red LAN de la subestación), (listas de acceso de entrada) los siguientes:

    - La dirección e interfaz del equipo del centro de control asignado o asignados y denegar toda dirección e interfaz que no se encuentre en la lista de acceso.
    - Se debe permitir el acceso remoto por medio del protocolo SSH y en el caso que amerite el protocolo telnet, tomando en cuenta que se prefiere SSH como medio de comunicación remota.
    - Se debe especificar los protocolos que se manejaran por ejemplo TCP, IPsec, HTTPS, ICMP (este protocolo debe estar limitado en cada uno de los dispositivos para evitar ataques por denegación de servicio) TLS (Transport

Layer Security), SNMP (Simple Network Management Protocol), RSTP (Rapid Spanning Tree Protocol), PTP (Precision Time Protocol), GOOSE.

ADMINISTRACIÓN DE CONTRASEÑAS EN LOS EQUIPOS DE NETWORKING.

Todo equipo de networking tiene la capacidad de configurar credenciales de acceso las cuales deben ser:

- Credenciales de acceso remoto al equipo.
- Credenciales de acceso por consola (router switch).
- Credenciales para el acceso a modo de configuración.
- Realice configuraciones básicas de autenticación como:
  - Numero de intentos fallidos.
  - Tiempo de bloqueo (temporal).
  - Clave con un estándar seguro, esto dependerá del equipo a configurar.
  - Considere los niveles de privilegio que se da para acceder al equipo.
  - Se recomienda generar dos usuarios uno completamente administrable y otro de visualización.
- Generar la documentación necesaria para las credenciales creadas y asignadas a los dispositivos de networking, documentación de verificación en el ANEXO B.

NOTA: la creación de contraseñas y la limitación de acceso a los equipos dependerá de las prestaciones que el equipo permita, sin embargo, se presentan las configuraciones que se debería aplicar.

LINEAMIENTOS PARA EL USO DE PROTOCOLOS DE CIFRADO.

Siempre es conveniente mantener una comunicación remota de forma cifrada principalmente en los equipos que realicen maniobras en el sistema, para ello se puede establecer ciertos protocolos que se manejan en un ambiente con mayor seguridad.

REQUERIMIENTOS.

- Se recomienda la adquisición de un certificado de cifrado que debe ejecutarse en el router principal.
- Se recomienda el protocolo de cifrado TLS en su versión más actual.
- Permanecer en constante actualización el protocolo de cifrado.
- Revisión periódica de nuevas actualizaciones.

- Realizar una documentación que contenga un registro de actualizaciones referente al protocolo de cifrado que se usa.

LINEAMIENTOS PARA ACTUALIZACIÓN DE PARCHES.

Se debe realizar una verificación de todos los software que se empleen en la red de la subestación ya que estos deben presentar las actualizaciones de los parches de seguridad actualizados a las últimas versiones disponibles. Para ello tenemos los siguientes requerimientos.

REQUERIMIENTOS.

- El estándar NERC CIP-007-6 RECUADRO 2 nos recomienda que se revise las actualizaciones cada 35 días.
- Para realizar la aplicación de un parche se debe considerar primero la verificación del mismo, para eso se debe considerar:
  - su procedencia.
  - Generar un respaldo del sistema antes de la aplicación del parche.
  - Verificar que no se haya afectado o modificado configuraciones operativas de importancia para el proceso.
  - Además, se debe realizar un plan para mitigar el parche en el caso que su aplicación cause conflictos o afecte al buen funcionamiento del sistema.
  - Si es posible realizar la verificación del parche en un equipo con similares características, pero aislado del sistema (equipos de prueba).
  - Se debe generar un registro o una documentación donde se especifique la fecha de última actualización, fecha de todas las actualizaciones, modificaciones del sistema, observaciones del funcionamiento del sistema antes y después de la instalación del parche, firma de responsabilidad de la persona que realizo la instalación del parche.
- Generación de documento donde se especifica las actualizaciones de parches realizados, la documentación de verificación de encuentra en el ANEXO B.

LINEAMIENTOS PARA ADMINISTRACIÓN DE PUERTOS Y SERVICIOS.

REQUERIMIENTOS:

Los requerimientos de habilitación de puertos y servicios no se limitan a lo mencionado sin embargo se debe considerar las justificaciones para restringir o permitir ciertos puertos y servicios.

- Se debe establecer los puertos y servicios que se desea habilitar, especificando las necesidades del sistema para la habilitación de ellos.
- Bloquear puertos y servicios que no se requieran para el funcionamiento de la red.
- La administración de los puertos y servicios debe ser configurada en el router o firewall.
- Se deben establecer listas de puertos y servicios que se manejaran dentro de la red LAN de la subestación, para ello se debe tener constancia documentada de los puertos activos y puertos bloqueados realizando su respectiva justificación.
- Es importante realizar configuraciones en los puertos físicos de los equipos, estos pueden ser la inactividad del puerto luego del cambio de estado o restricciones por MAC, esto dependerá de las prestaciones del equipo.

En esta sección se planteará los puertos y servicios que deben ser activados sea el caso para la aplicación del modelo administrativo que se plantea, tomando en cuenta que de ser el caso es posible habilitar otros puertos y servicios siempre y cuando se realice una justificación documentada.

- Puertos y servicios para establecer una comunicación remota por medio de un cliente:

Tabla 2.18. Puertos usados para comunicación remota

#	Puerto	Servicio asociado	Estado preferencial	Observación
1	23	telnet	desactivado	Existen equipos como medidores que no manejan otro protocolo que permita administrarlo de forma segura para ello habilitar este protocolo de administración remota.
2	22	SSH	Activo	Protocolo con características criptográficas se recomienda usar este protocolo como método de administración remota.

- Puertos y servicios para establecer comunicación remota por medio de buscadores.

Tabla 2.19. Puertos usados para una comunicación por medio del buscador

#	Puerto	Servicio asociado	Estado preferencial	Observación
1	80	HTTP	desactivado	Este protocolo nos permite una comunicación remota por medio de un buscador sin embargo no es fiable ya que la información es cifrada
2	443	HTTPS	Activo	Este protocolo nos permite una comunicación por medio del buscador de forma segura ya que la comunicación es cifrada, se recomienda su uso.

- Puertos y servicios para la administración de los protocolos industriales.

Tabla 2.20. Puertos para protocolos industriales comunes en las redes de las subestaciones eléctricas

#	Puerto	Servicio asociado	Estado preferencial	Observación
1	502	Modbus/TCP	Activado	Este puerto es el asociado al uso de Modbus por medio de TCP.
2	20000	DNP	Activado	Protocolo que manejan los IEDs

- Puerto y servicios para mensajería de impresoras.

Tabla 2.21. Puerto usado para protocolos de mensajería de impresoras

#	Puerto	Servicio asociado	Estado preferencial	Observación
1	445	SMBv1	desactivado	El protocolo permite la emisión de mensajería para equipos de impresión, existe un malware muy complejo de evitar para este puerto.

- Puertos y servicios para el uso de protocolos de cifrado de información.

Tabla 2.22. Puertos usados por protocolos de cifrado

#	Puerto	Servicio asociado	Estado preferencial	Observación
1	443	SSL/TLS	activado	Realizar revisión periódica de posibles actualizaciones o pago de licencias para el uso de este protocolo, en el router.

- Puertos y servicios para el uso de escritorio remoto.

Tabla 2.23. Puertos usados para el uso del servicio de escritorio remoto

#	Puerto	Servicio asociado	Estado preferencial	Observación
1	3389	RDP	desactivado	Este puerto nos permite la habilitación del escritorio remoto de Microsoft, lo cual se podría usar para ingresar al computador de cada subestación, sin embargo se necesita tener mucha precaución con la activación de este puerto, no es necesario establecer una comunicación de forma remota si se tiene presente métodos más seguros de comunicación remota como SSH, HTTPs.

LINEAMIENTOS PARA TRATAMIENTO DE CODIGOS MALICIOSOS.

SUGERENCIA A CONSIDERAR.

Se debe tener presente la actualización de softwares que permitan la protección del sistema de códigos maliciosos, los antimalwares deben encontrarse en el servidor de la red que administra la instalación y administración de un equipo que contenga un antimalware se encuentra fuera del alcance de esta metodología sin embargo se presentan requerimientos que ayuden a mitigar la problemática.

REQUERIMIENTOS:

- Realizar un plan para la detección y mitigación de un código malicioso.
- Registrar comportamientos fuera de lo normal dentro de la red para ello se debe tener un software que permita el monitoreo constante de la red, para este requerimiento se puede utilizar cualquier software de administración de redes como

wireshark que es un software libre, sin embargo, existen servicios de monitoreo pagados que tiene mejores prestaciones.

- Generar el procedimiento de control de los códigos maliciosos que se presenten en el medio de forma actualizada.
- Se debe generar la documentación de incidente en caso de registrar alguna anormalidad en el equipo, documentación de verificación ANEXO B, "B-20_MODELOS DE DOCUMENTACIÓN DE VERIFICACIÓN" documento 3.

LINEAMIENTOS PARA ACCESO AL SISTEMA DE FORMA LOCAL Y REMOTA.

- **ACCESO DE FORMA LOCAL.**

Se considera el ingreso de forma local cuando el acceso sea de forma directa hacia uno de los equipos dentro de las instalaciones de la subestación.

REQUERIMIENTOS.

- El acceso de forma local debe ser establecido por un computador portátil registrado como equipo de administración local.
- Se debe generar la documentación necesaria para justificar la comunicación de forma local hacia los equipos de networking de la red LAN de las subestaciones, documentación de verificación ANEXO B, "B-20_MODELOS DE DOCUMENTACIÓN DE VERIFICACIÓN" documento 3.

- **ACCESO DE FORMA REMOTA.**

Se considera acceso de forma remota cuando se lo haga a través del segmento de red al que pertenece la subestación, sin la necesidad que la persona se encuentre dentro de las instalaciones de la subestación.

REQUERIMIENTOS.

- El acceso de forma remota solo será de forma exclusiva para equipos de las instalaciones del centro de control.
- Instalar un programa que permita establecer una comunicación de forma remota por medio de cliente-servidor, este puede ser: Putty o Tera Term.

- El acceso a cada uno de los equipos de networking debe ser por medio del protocolo SSH. En los equipos como IEDs se debe realizar el ingreso por SSH de no ser posible se lo realizaría por Telnet.
- Para realizar una comunicación de forma remota se debe generar una documentación que, de reporte al ingreso remoto, documentación de verificación ANEXO B, "B-20_MODELOS DE DOCUMENTACIÓN DE VERIFICACIÓN" documento 3.

2.3.5.2 Categoría: POLÍTICAS DE SEGURIDAD.

Propósito:

- presentar una estructura de cuidado y buenas prácticas del manejo de información dentro y fuera de las instalaciones.
- Dar a conocer a los trabajadores las nuevas amenazas y formas de vulnerar al sistema.
- Generar una concientización al personal.

SUGERENCIA A CONSIDERAR.

Es importante que el personal encargado de controlar y monitorizar el sistema SCADA tenga claro los parámetros para un buen manejo de la información y mantenga cuidados acordes a la importancia que se maneja para ello se sugiere lo siguiente:

LINEAMIENTOS PARA LA ESTRUCTURA ORGANIZACIONAL DEL PERSONAL.

REQUERIMIENTOS.

- Mantener una organización jerárquica o distribuida referente a las responsabilidades que tiene el personal, se debe asignar las responsabilidades de forma clara y precisa.
- Mantener un orden y comunicaciones claras interpersonales por ejemplo la generación de reporte de eventos que se genera dentro de las subestaciones, esta debe ser registrada con fecha, hora, nombre del responsable y su firma.
- Informar al personal de las sanciones establecidas por el mal uso de los recursos o instalaciones.

- Documentación para la estructura organizacional del personal, ANEXO B, “B-20_MODELOS DE DOCUMENTACIÓN DE VERIFICACIÓN” documento 3.

LINEAMIENTOS PARA ASIGNACIÓN Y RETIRO DE CREDENCIALES A LOS TRABAJADORES.

REQUERIMIENTOS.

- Las asignaciones de las credenciales deben ser únicas e intransferibles.
- El monitoreo del uso de las credenciales personales deben ser registradas.
- Las credenciales deben ser asignadas dependiendo del grado de responsabilidad o acceso a los equipos.
- Reportar de forma inmediata la pérdida o robo de credenciales físicas.
- En el caso de retiro de credenciales por salida del personal de la institución, esta debe ser registrada de forma inmediata no posterior a 48 horas y el cambio de contraseñas y accesos deben ser bloqueados en un lapso máximo de tres semanas.
- Documentación de la asignación y retiro de credenciales al personal, ANEXO B, “B-20_MODELOS DE DOCUMENTACIÓN DE VERIFICACIÓN” documento 3.

LINEAMIENTOS PARA CAPACITACIÓN AL PERSONAL.

REQUERIMIENTOS.

- Se recomienda capacitar al personal encargado de administrar las redes del SCADA de los cuidados de nuevas amenazas en un periodo no mayor a tres meses.
- Es importante dar las facilidades y espacio pertinente para desarrollar actividad de concientización referente a los cuidados y buenas prácticas del manejo de la información.
- Documentación para la capacitación al personal, ANEXO B, “B-20_MODELOS DE DOCUMENTACIÓN DE VERIFICACIÓN” documento 3.

2.3.5.3 Categoría: SEGURIDAD EN LAS INSTALACIONES DE UNA SUBESTACIÓN.

LINEAMIENTOS PARA EL CONTROL DE ACCESO A PERSONAL EN LAS SUBESTACIONES.

- **REGISTRO DE PERSONAL POR MEDIO DE EQUIPO ELECTRÓNICO.**

REQUERIMIENTOS.

- Se debe presentar en la entrada de cada uno de los accesos a la subestación un lector biométrico.
- Se debe negar el acceso a todo personal que no se encuentre registrado en la base de datos del lector biométrico.
- Documentación para control de acceso a personal en las subestaciones, ANEXO B, "B-20_MODELOS DE DOCUMENTACIÓN DE VERIFICACIÓN" documento 3.

- **BUENAS PRACTICAS DE SEGURIDAD Y MANIPULACIÓN DE LA INFORMACION QUE SE OBTIENE DE LAS REDES DE LAS SUBESTACIONES.**

REQUERIMIENTOS.

- No se debe permitir la extracción de información por medios físicos que no sean de uso exclusivo para la administración de la red, estos pueden ser laptop, pendrive, disco duro externo, CDs, o cualquier dispositivo de almacenamiento masivo de información.
- La información que se extraiga de las configuraciones de los equipos, administración, gestión o seguridad cibernética debe ser justificado.
- Generación de un reporte referente a la manipulación de información de la subestación, documentación en el ANEXO B, "B-20_MODELOS DE DOCUMENTACIÓN DE VERIFICACIÓN" documento 3.

LINEAMIENTOS PARA EQUIPOS DE VIDEOSUPERVISIÓN Y ALMACENAMINETO DE VIDEO.

SUGERENCIAS A CONSIDERAR.

Se debe tener un sistema de seguridad que permita la visualización de las instalaciones de la subestación. Estos equipos deben colocarse en puntos estratégicos de la subestación para ello se plantea los siguientes requerimientos:

REQUERIMIENTOS.

- Determinar los puntos de seguridad para ello se debe tener presente los planos arquitectónicos de la subestación.
- Determinar los puntos de acceso a la subestación y los puntos considerados clave para la observación.
- Considere el Angulo de vista de las cámaras.
- Las cámaras deben permitir la visualización del sector en un entorno carente de luz.
- Evite la colocación de cámaras en sectores que permitan tener puntos ciegos.
- El número de cámaras depende del número de equipos que se desea vigilar.
- Determine los puntos en los cuales las cámaras se encontrarán expuestas al medio exterior ya que estas deben presentar características para su operación en la intemperie.
- Documentación para la verificación de equipos de video supervisión y almacenamiento de video, ANEXO B, “B-20_MODELOS DE DOCUMENTACIÓN DE VERIFICACIÓN” documento 3.

3. RESULTADOS Y DISCUSIÓN

Se procedió a aplicar la metodología propuesta para la implementación de una red LAN en un sistema SCADA/ADMS de la subestación EL RETORNO, considerando las limitaciones de los equipos y mencionando las observaciones pertinentes para el desarrollo de la aplicación de la metodología.

La aplicación de la metodología cuenta con algunas limitaciones, las cuales fueron acordadas, estas limitaciones sin embargo no son críticas por lo tanto se pueden obviar, las siguientes limitaciones en la implementación fueron:

- En la arquitectura física el anillo principal no es por fibra óptica en su totalidad.
- En la arquitectura lógica no se realizaron configuraciones de VLAN ya que se decidió que las cámaras pasen a ser instaladas en el dispositivo frontera que administra el departamento de comunicaciones de EMELNORTE por lo tanto en la red de la subestación el RETORNO únicamente se tienen equipos concernientes al funcionamiento de la subestación.
- No se realizó el anillo secundario completo ya que los enlaces con los cuales se pretendía hacerlo, posteriormente serán utilizados para implementar la pantalla táctil y el concentrador ASAT, esto a petición del departamento.
- Tampoco se implementó redundancia en el router ya que no existía disponibilidad de los equipos, sin embargo, en recomendaciones se sugiere tener un router de similares características en stock.
- No fue factible habilitar el protocolo SSH en todos los equipos ya que no contaban con dicho servicio, sin embargo, se realizó la recomendación respectiva en la sección de recomendaciones.

A pesar de las limitaciones mencionadas estas no son críticas, pero se debe considerarlas.

3.1 ARQUITECTURA FÍSICA APLICADA A LA SUBESTACIÓN PILOTO EL RETORNO.

Para aplicar la metodología en esta etapa se tienen las siguientes consideraciones como un cableado mixto, en el cual se tiene etapas de cobre y fibra óptica, además de un anillo completamente cerrado y un semi-anillo.

Se procedió a realizar la implementación de la arquitectura física mencionada en la metodología, en la figura 3.1 se observa la arquitectura aplicada a la red de la subestación EL RETORNO.

Es importante considerar ciertas limitaciones que se tuvieron al momento de realizar la implementación en la subestación EL RETORNO. Esto corresponde a la implementación del capítulo 1, categoría: arquitecturas físicas sugeridas y subcategoría diagrama 1 de la metodología planteada.

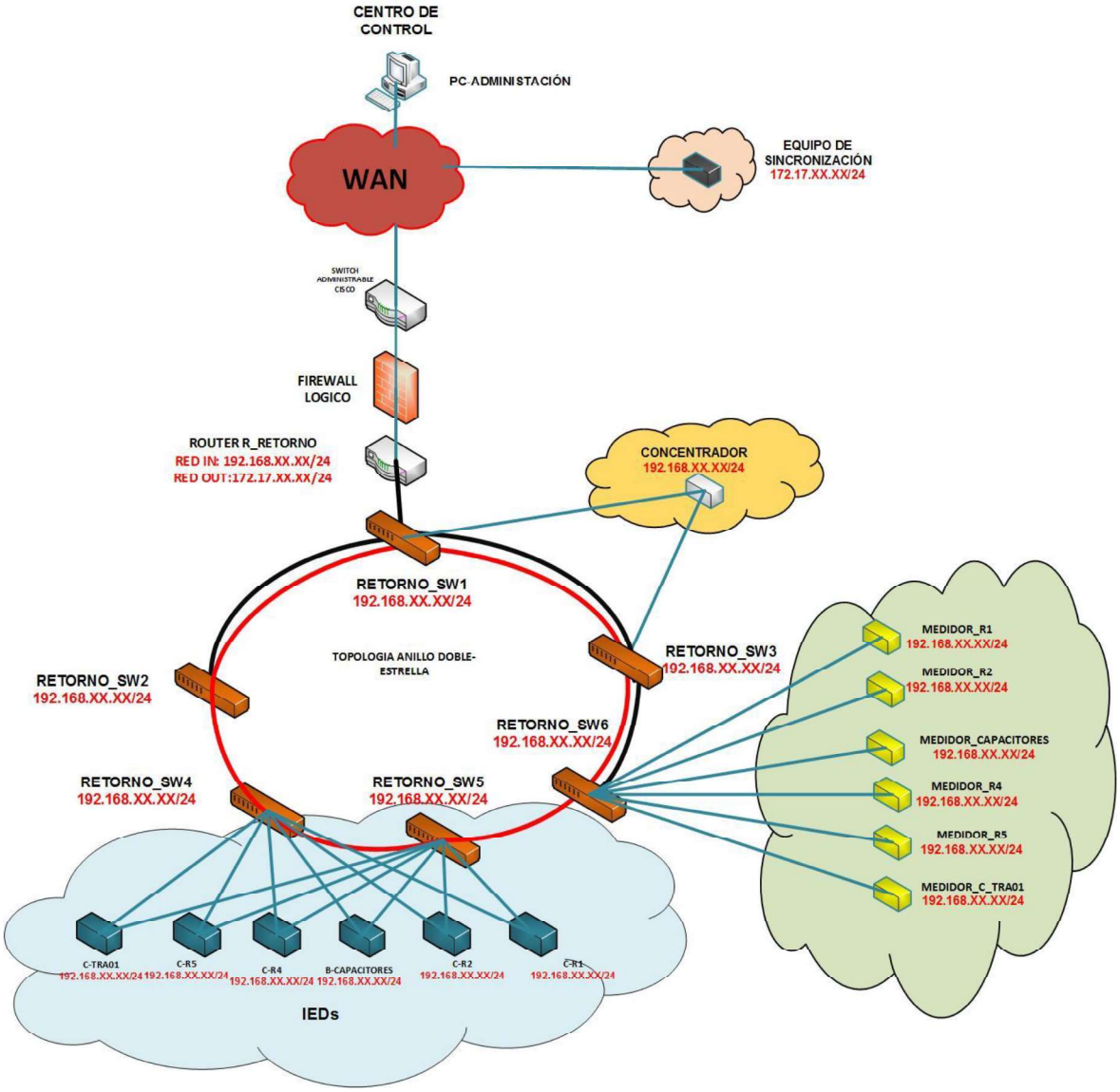

figura 3.1. Arquitectura en la subestación EL RETORNO

NOTA: la documentación de verificación de la arquitectura se encuentra en el ANEXO B, denominado “B-17_ARQUITECTURA DE LA SUBESTACIÓN EL RETORNO”.

3.2 CONFIGURACIONES DE ADMINISTRACIÓN Y GESTIÓN APLICADOS A LA RED DE LA SUBESTACIÓN PILOTO EL RETORNO.

3.2.1 CONFIGURACIÓN DE NETWORK ADDRESS TRASLATION (NAT) EN ROUTER GARRETCOM MAGNUM DX940 DE LA RED DE LA SUBESTACIÓN EL RETORNO.

Esta sección corresponde a la implementación del capítulo 2, categoría: equipos de networking en una subestación y subcategoría lineamientos de administración de router en el inciso denominado proceso de traducción de direcciones de red (NAT), referente a la metodología planteada.

En la figura 3.2. se observa el estado inicial de NAT, posteriormente en la figura 3.3. se aprecia las direcciones agregadas.

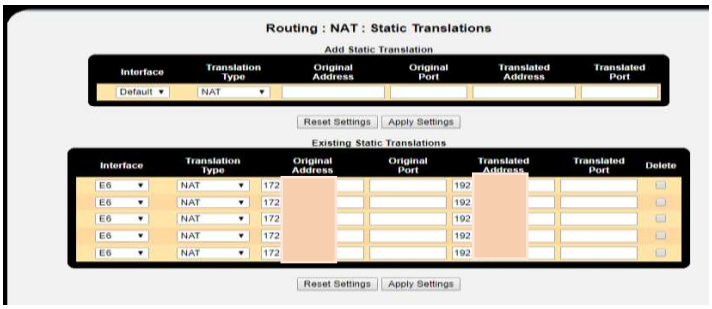

Figura 3.2. Estado inicial del router Garretcom Magnum DX940

En la figura 3.3 se muestra las nuevas direcciones a las cuales se realiza NAT del router Garretcom Magnum DX940

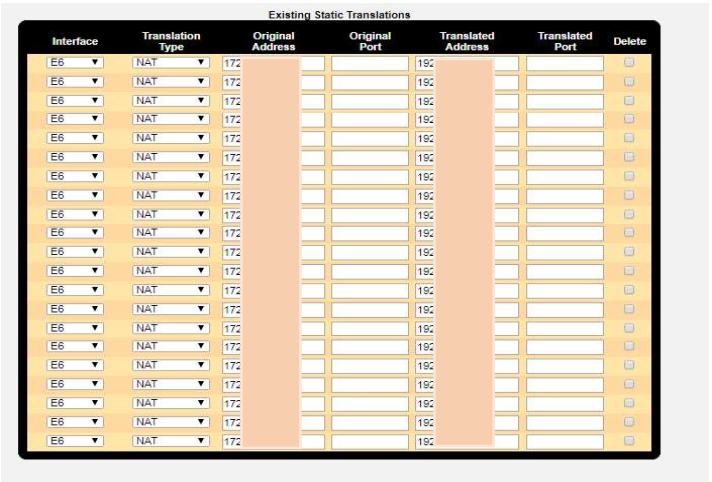

Figura 3.3. Configuración de NAT del router Garretcom Magnum DX940

3.2.2 CONFIGURACIÓN DE ENRUTAMIENTO DEL ROUTER GARRETTCOM DX940. (RETORNO_R).

Esta sección corresponde a la implementación del capítulo 2, categoría: equipos de networking en una subestación y subcategoría lineamientos de administración de router en el inciso denominado implementación de un ruteo estático completamente especificado referente a la metodología planteada.

Se procede a realizar una configuración de ruteo estático de “siguiente salto” (en función de vector distancia), la configuración se puede apreciar en la figura 3.4.

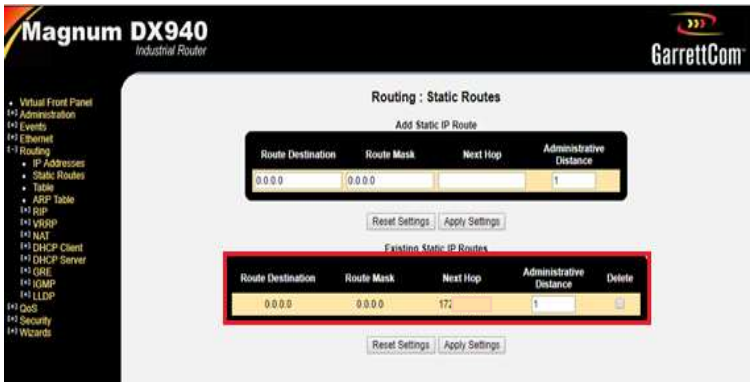

Figura 3.4. Configuración de ruteo estático

En la figura 3.5. se aprecia la tabla de ruteo del equipo.

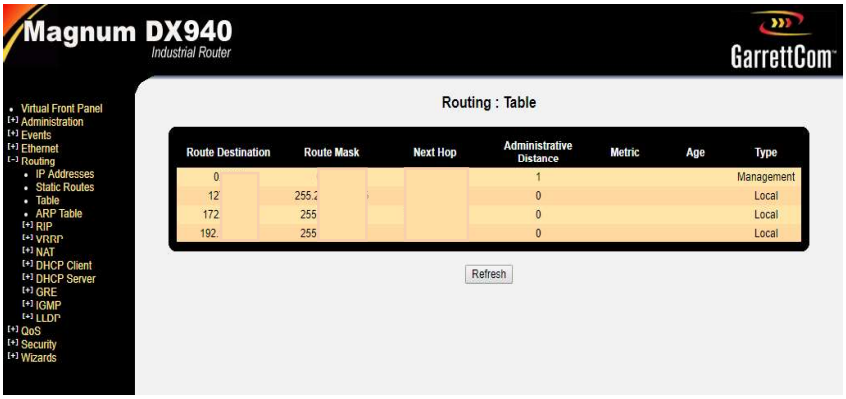

Figura 3.5. Tabla de ruteo del router garretcom Magnum DX940

3.2.3 CONFIGURACIONES DE ACCESO DE FORMA REMOTA DE LOS EQUIPOS DE NETWORKING.

Esta sección corresponde a la implementación del capítulo 3, categoría: seguridad cibernética y subcategoría lineamientos para acceso al sistema de forma local y remota, en el inciso denominado acceso de forma remota, referente a la metodología planteada.

En esta sección se considera las limitaciones de los equipos para ser configurados con el protocolo SSH ya que se habilito este protocolo en los equipos que presentaban este servicio, en los equipos que no fue posible usar SSH se habilito Telnet.

Para verificar el acceso de forma remota se utilizo el cliente Putty.

Router garrettcom DX940. (RETORNO_R)

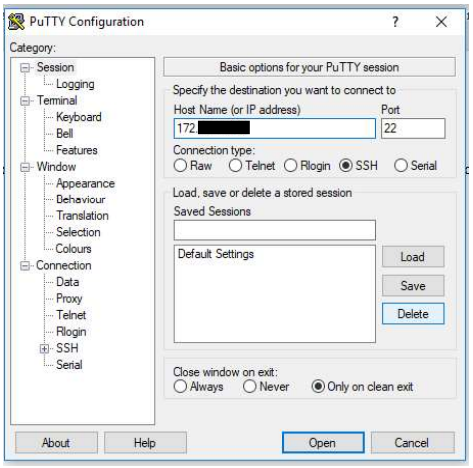

Figura 3.6. Ingreso al router por medio de Putty

En la figura 3.7. se puede observar el acceso por medio de SSH.

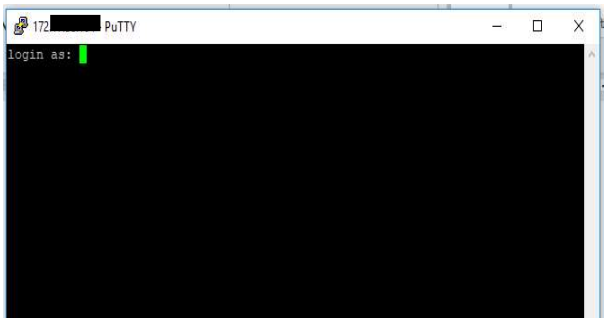

Figura 3.7. Pantalla inicial por medio del cliente Putty

Si intentamos realizar el ingreso por medio de telnet podemos constatar que no es posible ya que se encuentra bloqueado.

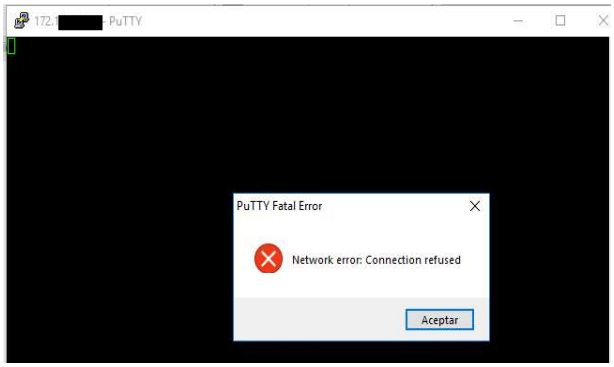

Figura 3.8. Negación de acceso por medio de Telnet

Nota: el documento completo de encuentra en el ANEXO B, denominado "B-3_CONFIGURACIONES DE ACCESO DE FORMA REMOTA DE LOS EQUIPOS DE NETWORKING".

3.2.4 CONFIGURACIÓN DE RAPID SPANNING TREE PROTOCOL (RSTP). ROUTER GARRETCOM MAGNUM DX940.

Esta sección corresponde a la implementación del capítulo 2, categoría: equipos de networking de una subestación y subcategoría lineamientos de administración de switch en el inciso denominado protocolos de redundancia, referente a la metodología planteada.

En esta sección se realiza la habilitación del protocolo RSTP en el router y el los switches.

En la figura 3.9. se observa que el protocolo RSTP se encuentra deshabilitado en el router Garretcom Magnum DX940.

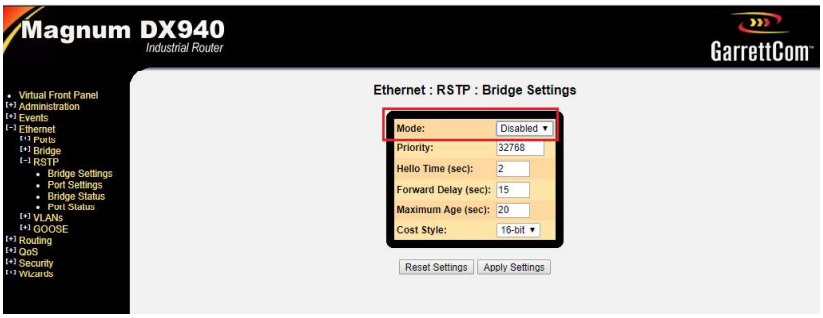

Figura 3.9. RSTP deshabilitado

En la figura 3.10. se observa que se procedió a la habilitación de RSTP en el router.

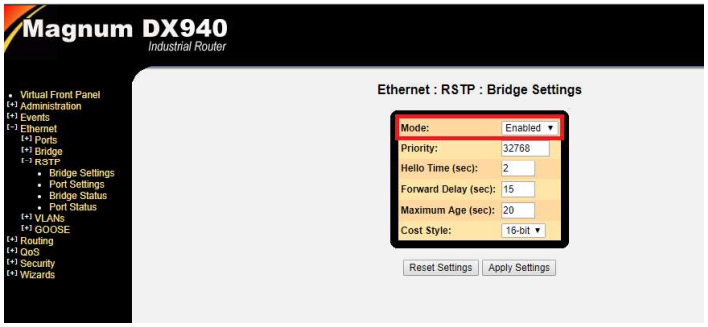

Figura 3.10. Habilitación del protocolo RSTP

En la figura 3.11. se observa la habilitación de RSTP y se configura los siguientes parámetros, con el valor de prioridad (32768) determinamos el equipo denominado como puente raíz.

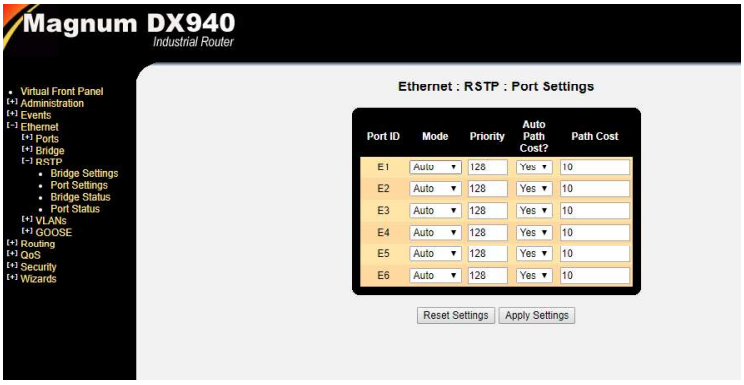

Figura 3.11. Parámetros de RSTP en el router

En la figura 2.12 se observa el estado del protocolo RSTP.

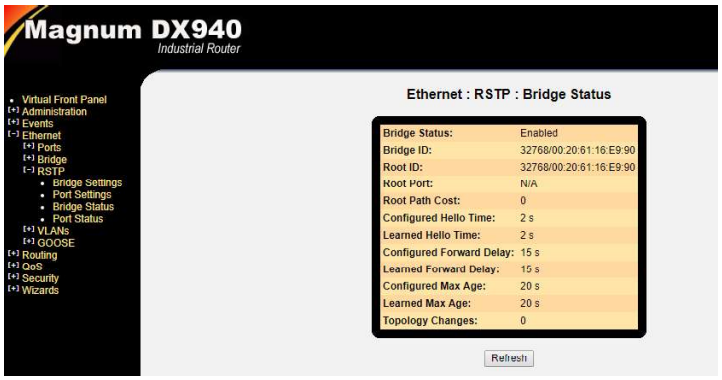

Figura 3.12. Estado del protocolo RSTP

Nota: el documento completo de encuentra en el ANEXO B, denominado "B-4_CONFIGURACIÓN DE RAPID SPANNING TREE PROTOCOL (RSTP)".

3.2.5 CONFIGURACIÓN DE LINK AGGREGATION CONTROL PROTOCOL (LACP).

Esta sección corresponde a la implementación del capítulo 2, categoría: equipos de networking de una subestación y subcategoría lineamientos de administración de switch en el inciso denominado protocolos de balance de carga y agregación de enlaces, referente a la metodología planteada.

en esta sección se utilizó el protocolo de control de agregación de enlaces (LACP) el cual fue implementado en los switches: switch 1, switch 2, switch 3 y switch 6.

Para el switch RETORNO_SW1.

En la figura 3.13. se puede observar los enlaces que se encuentran asociados en grupos, los grupos se encuentran dados por la prioridad, se aprecia 4 enlaces con LACP y dos grupos.

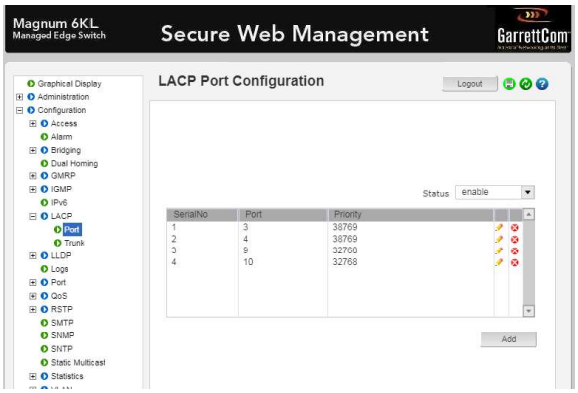

Figura 3.13. Configuración de LACP

En la figura 3.14. se aprecia los enlaces troncales formados y los puertos primarios

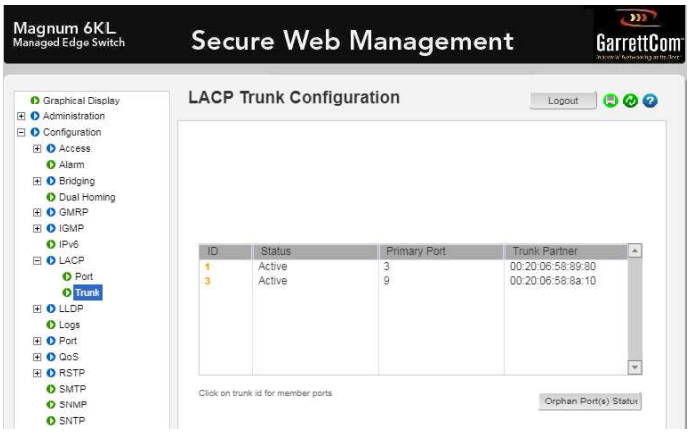

Figura 3.14. Configuración de enlaces troncales

En la figura 3.15. se aprecia el grupo ID 1, el puerto y la diferencia del cual es primario y secundario

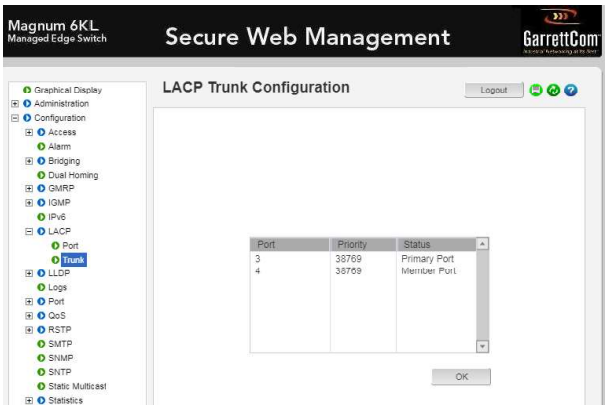

Figura 3.15. Enlaces primarios y secundarios en ID1

En la figura 3.16. se aprecia el grupo ID 3, el puerto y la diferencia del cual es primario y secundario.

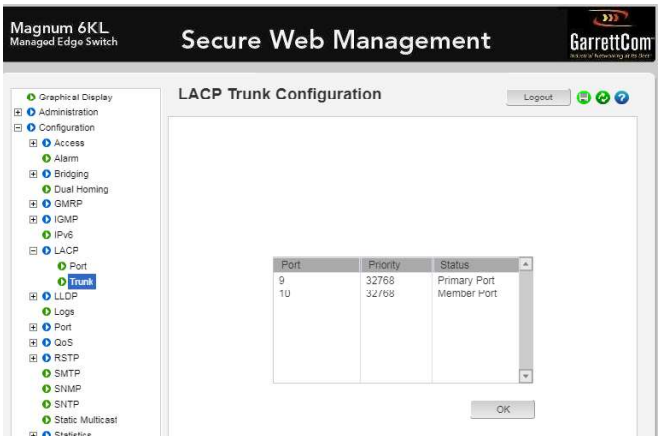

Figura 3.16. Enlaces primarios y secundarios en ID3

Nota: el documento completo de encuentra en el ANEXO B, denominado “B-5_CONFIGURACIÓN DE LINK AGGREGATION CONTROL PROTOCOL (LACP)”.

3.2.6 DIRECCIONAMIENTO DE LOS EQUIPOS QUE CONFORMAN LA RED LAN DE LA SUBESTACIÓN EL RETORNO.

Esta sección corresponde a la implementación del capítulo 2, categoría: equipos de networking de una subestación y subcategoría lineamientos para asignación de direcciones

a los dispositivos, en el inciso denominado direccionamiento de la red LAN, referente a la metodología planteada.

DIRECCIONAMIENTO DE LOS EQUIPOS DE NETWORKING

ROUTER GARRETCOM MAGNUM DX940 (RETORNO_R).

Aunque la dirección de la interfaz E3 se encuentra con NAT, se otorga como dirección del sistema a la interfaz E6.

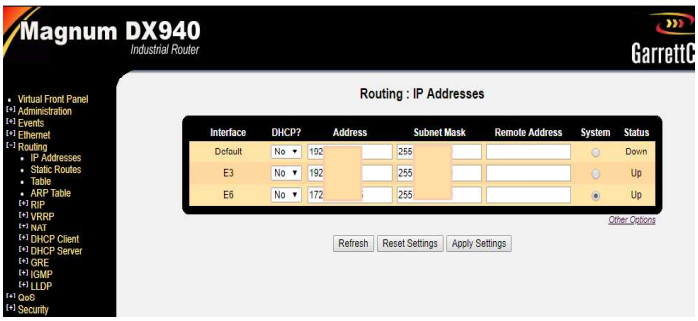

Figura 3.17. Direccionamiento a las interfaces habilitadas E3 y E6

SWITCH GARRETCOM MAGNUM 6KL (RETORNO_SW1).

En la figura 3.18. se presenta el direccionamiento del equipo.

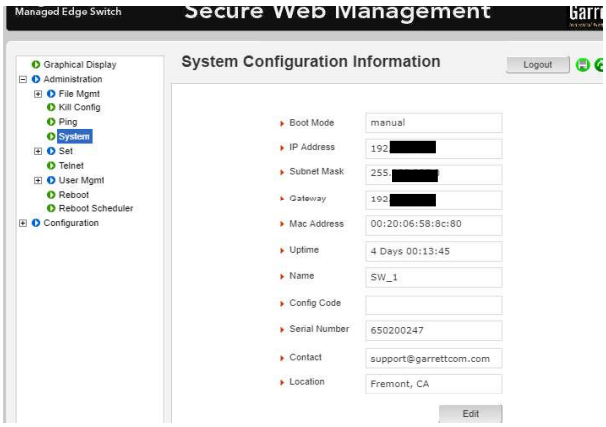

Figura 3.18. Direccionamiento de RETORNO_SW1

Nota: el documento completo de encuentra en el ANEXO B, denominado “B-6_DIRECCIONAMIENTO DE LOS EQUIPOS QUE CONFORMAN LA RED LAN DE LA SUBESTACION EL RETORNO”.

3.2.7 CONFIGURACIÓN DEL PROTOCOLO DE SINCRONIZACIÓN DE LOS EQUIPOS DE NETWORKING.

Esta sección corresponde a la implementación del capítulo 2, categoría: equipos de networking de una subestación y subcategoría lineamientos sincronización de equipos de networking, referente a la metodología planteada.

Se realiza la configuración de sincronización en los equipos por medio de un "servidor reloj", en la figura 3.19. se aprecia el interfaz del equipo de sincronización.

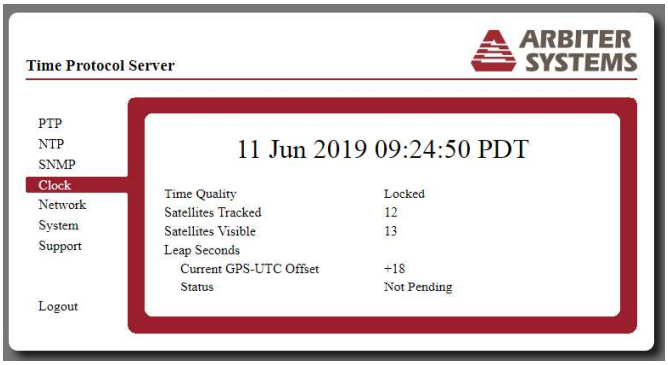

figura 3.19. Equipo de sincronización

Para realizar la sincronización se utilizó el protocolo simple de hora de red (SNTP). Además, se procede a ingresar la dirección del servidor que dará la sincronización adecuada a los equipos de networking.

ROUTER GARRETCOM DX940 (R_RETORNO).

Se procede a habilitar el protocolo SNTP.

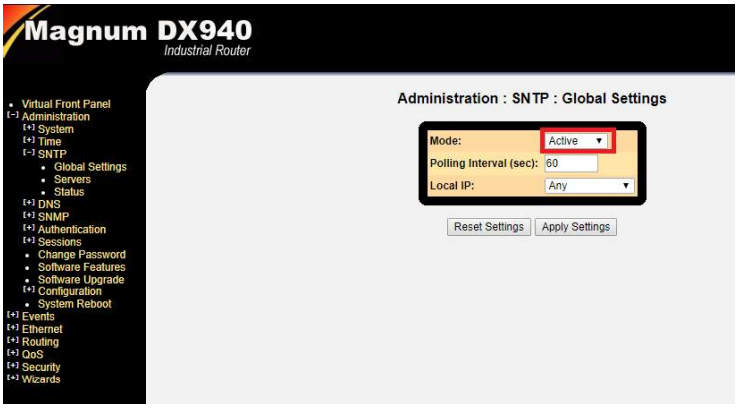

Figura 3.20. Habilitación del protocolo

En la figura 3.21. se aprecia el ingreso de la dirección del servidor de sincronismo

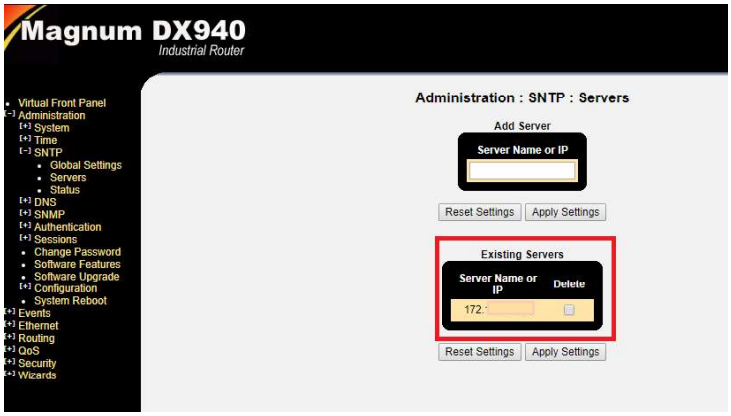

Figura 3.21. Dirección del servidor de sincronismo

En la figura 3.22. se aprecia la verificación de fecha y hora adecuada.

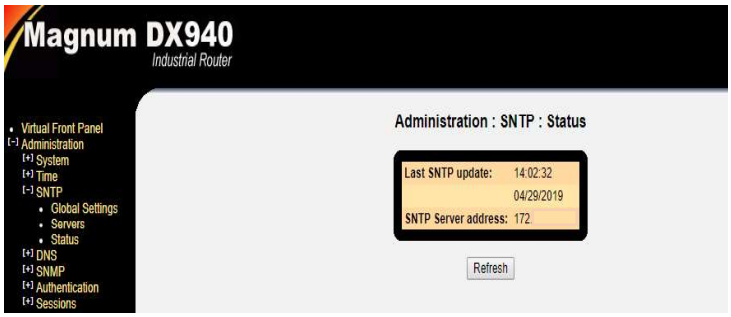

Figura 3.22. Hora y fecha adecuados

SWITCH GARRETCOM MAGNUM 6KL (RETORNO_SW1).

En la figura 3.23 se aprecia la habilitación del protocolo SNTP.

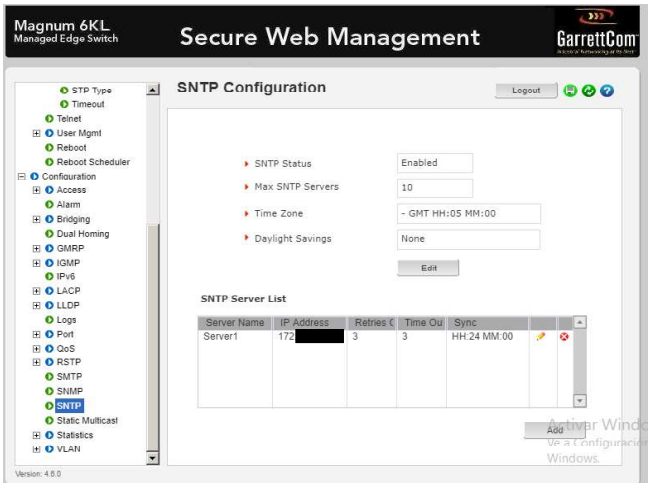

Figura 3.23. Habilitación del protocolo SNTP

Nota: el documento completo de encuentra en el ANEXO B, denominado "B-7_CONFIGURACIÓN DEL POTOCOLO DE SINCRONIZACIÓN DE LOS EQUIPOS DE NETWORKING".

3.2.8. CONFIGURACIÓN DE CALIDAD DE SERVICIO(QoS) EN LA SUBESTACION EL RETORNO.

Esta sección corresponde a la implementación del capítulo 2, categoría: equipos de networking de una subestación y subcategoría lineamientos para la configuración de calidad de servicio, referente a la metodología planteada.

Para la configuración de calidad de servicio en la red de la subestación se procede a crear un gropo denominado SCADA en el cual se configura las prioridades maximas permitidas por el equipo.

ROUTER GARRETCOM MAGNUM DX940.

En la figura 3.24 se observa la configuración de calidad de servicio en el grupo SCADA.

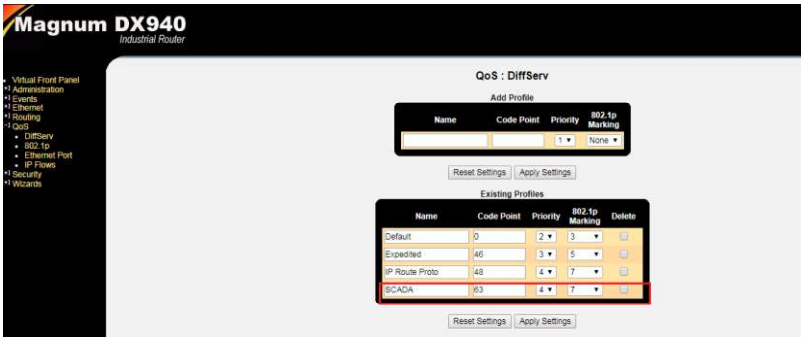

Figura 3.24. Configuración del grupo SCADA

En la figura 3.25 se observa las interfaces en las cuales se habilito QoS.

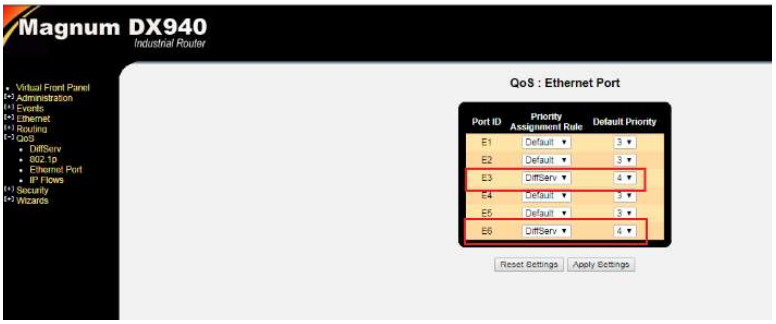

Figura 3.25. Habilitación de QoS

Nota: el documento completo de encuentra en el ANEXO B, denominado "B-14_CONFIGURACIÓN DE CALIDAD DE SERVICIO".

3.2.9 CONFIGURACION DE DIALOGOS DE ADVERTENCIA EN LOS EQUIPOS DE NETWORKING.

Esta sección corresponde a la implementación del capítulo 2, categoría: equipos de networking de una subestación y subcategoría lineamientos de configuración general básica, referente a la metodología planteada.

Se ha procedido a redactar un mensaje de advertencia para cada uno de los equipos de networking.

ROUTER GARRETCOM MAGNUM DX940.

En la figura 3.26. se aprecia el anuncio del dispositivo.

Figura 3.26. Anuncio del dispositivo

Nota: el documento completo de encuentra en el ANEXO B, denominado “B-15_CONFIGURACIÓN DE DIALOGOS DE ADVERTENCIA”.

3.2.10 RESPALDO DE CONFIGURACIONES DE LOS EQUIPOS DE NETWORKING.

Esta sección corresponde a la implementación del capítulo 2, categoría: equipos de networking de una subestación y subcategoría lineamientos para el respaldo de configuraciones de los equipos de networking, referente a la metodología planteada.

ROUTER GARRETCOM DX940 (R_RETORNO).

En la figura 3.27. se aprecia los archivos de configuración en .xml

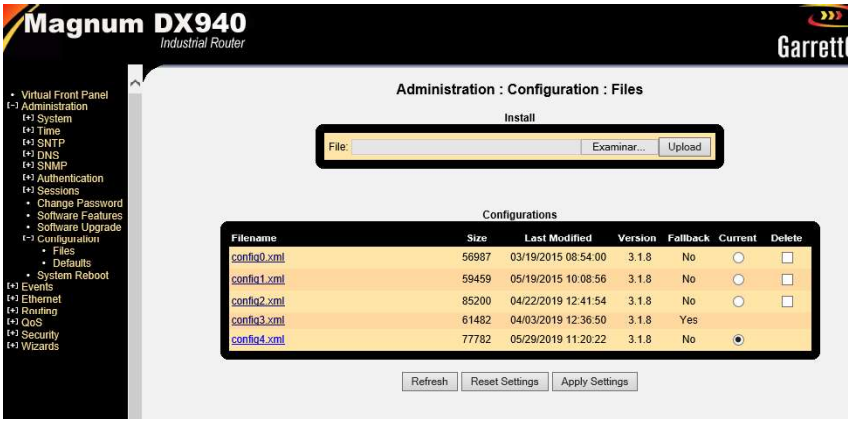

Figura 3.27. Archivos de configuración en .xml

Nota: el documento completo de encuentra en el ANEXO B, denominado "B-16_RESPALDO DE CONFIGURACIONES".

3.2.11 ASIGNACIÓN DE NOMBRES A LOS EQUIPOS DE NETWORKING.

Esta sección corresponde a la implementación del capítulo 2, categoría: equipos de networking de una subestación y subcategoría lineamientos de configuración general básica, referente a la metodología planteada.

Es importante mantener una asignacion de nombres y una distincion en los equipos de networking, esto permite mantener una mejor adminitración de los equipos, facilicitando el reconocimiento del equipo que se esta administrando.

1. **ROUTER GARRETCOM MAGNUM DX940 (R_RETORNO).**

En la figura 3.28. se aprecia el nombre del equipo

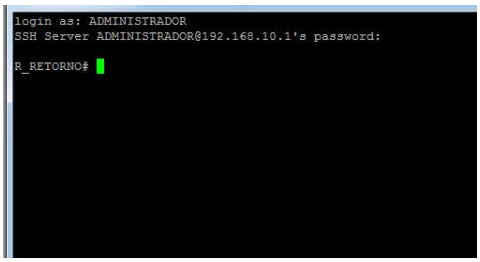

Figura 3.28. Nombre del equipo

Nota: el documento completo de encuentra en el ANEXO B, denominado "B-18_NOMBRAMIENTO DE LOS EQUIPOS".

3.3 CONFIGURACIONES DE SEGURIDAD CIBERNÉTICA APLICADA A LA RED DE LA SUBESTACIÓN PILOTO EL RETORNO.

3.3.1 CAMBIO DE CREDENCIALES Y CREACIÓN DE USUARIOS.

Esta sección corresponde a la implementación del capítulo 3, categoría: seguridad cibernética y subcategoría lineamientos de control de acceso, en el inciso denominado administración de contraseñas en los equipos de networking, referente a la metodología planteada.

Las contraseñas son determinadas por el jefe encargado del departamento SCADA para ello se crearon 2 usuarios y dos contraseñas otorgadas a cada uno de los usuarios.

A continuación, se presenta el acceso por medio del buscador sin embargo el acceso no se limita por medio del buscador, también por medio de algún cliente como Putty.

Router garrettcom DX940. (R_RETORNO).

En la figura 3.29. se observa el Ingreso por medio del usuario administrador

Figura 3.29. Verificación del uso de credencial administrador

Se verifica que el usuario es administrador y se encuentra autorizado a realizar modificaciones a la configuración del equipo.

Figura 3.30. Usuario administrador con la capacidad de realizar modificaciones

En la figura 3.31. se realiza el ingreso con el modo de operador.

Figura 3.31. Ingreso por medio de credenciales restringidas

En la figura 3.32. se verifica que este usuario tiene restricciones, y solo puede visualizar.

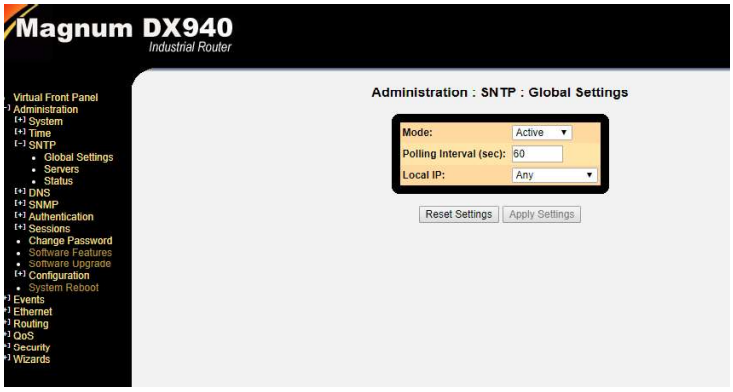

Figura 3.32. Acceso y restricciones de configuración de usuario

Nota: el documento completo de encuentra en el ANEXO B, denominado “B-8_CAMBIO DE CREDENCIALES Y CREACIÓN DE USUARIOS”.

3.3.2 HABILITACIÓN DEL PROTOCOLO SSL/TLS EN LOS EQUIPOS DE NETWORKING.

Esta sección corresponde a la implementación del capítulo 3, categoría: seguridad cibernética y subcategoría lineamientos para el uso de protocolos de cifrado, referente a la metodología planteada.

ROUTER GARRETCOM DX940 (R_RETORNO).

En la figura 3.33 se observa la habilitación del protocolo SSL.

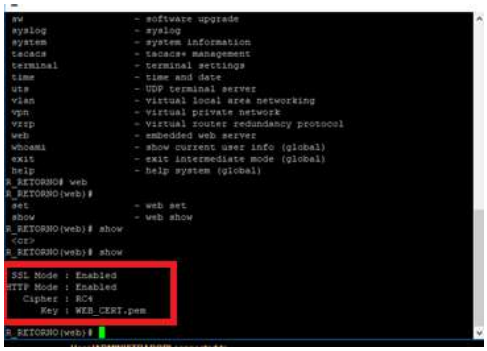

Figura 3.33. Habilitación del protocolo SSL

SWITCH GARRETCOM MAGNUM 6KL (RETORNO_SW1).

En la figura 3.34 se observa la habilitación del protocolo SSL.

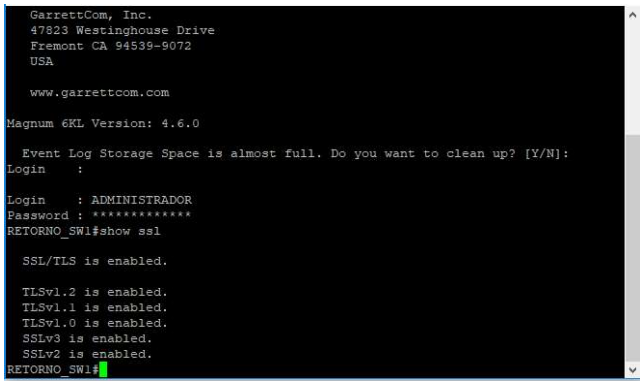

Figura 3.34. Habilitación del protocolo SSL

Nota: el documento completo de encuentra en el ANEXO B, denominado "B-9_HABILITACIÓN DEL PROTOCOLO SSL/TLS".

3.3.3 ACTUALIZACIÓN DEL SOFTWARE DE LOS EQUIPOS DE NETWORKING.

Esta sección corresponde a la implementación del capítulo 3, categoría: seguridad cibernética y subcategoría lineamientos para actualización de parches, referente a la metodología planteada.

ACTUALIZACIÓN DE LOS EQUIPOS DE NETWORKING.

Se realiza la verificación de la versión del software que se encuentra instalado en cada uno de los dispositivos de networking como router y switches, posteriormente se verifica la existencia de nuevas actualizaciones de software para los dispositivos y se procede a realizar la actualización de los mismos.

ROUTER GARRETCOM MAGNUM DX940.

El router presentaba una versión antigua (DX940 v3.1.8 (Y22).)

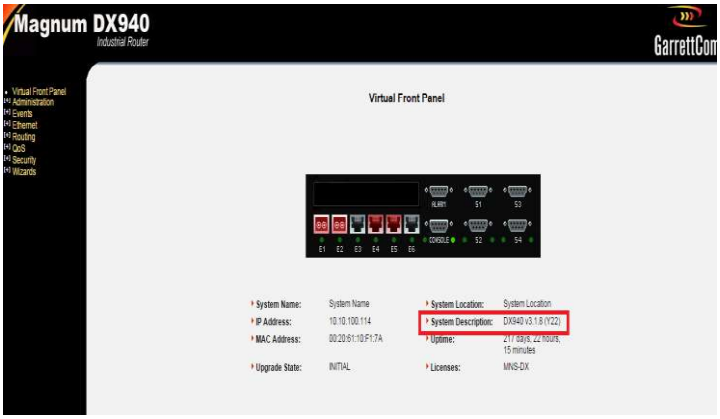

Figura 3.35. Verificación de versión de software

El router se actualizo a la versión DX940 v3.1.8 (Y48).

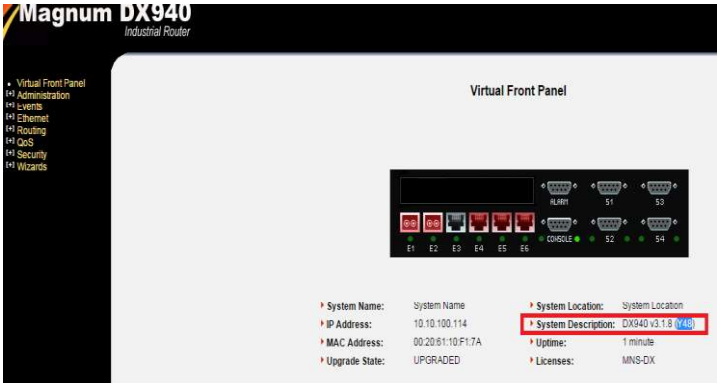

Figura 3.36. Actualización del software a la versión más actual a fecha

ACTUALIZACIÓN DE SWITCHES GARRETCOM MAGNUM 6KL.

Para el switch RETORNO_SW1.

En la figura 3.37. se observa que el equipo presentaba una versión antigua (v4.5.0).

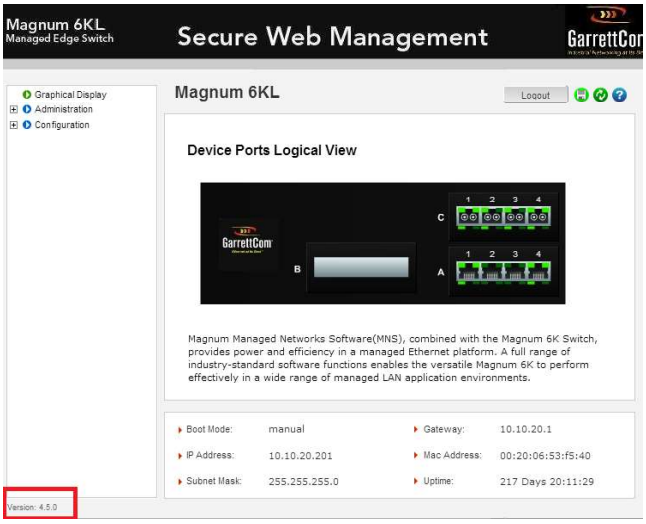

Figura 3.37. Se verifica la versión de software

Se actualizo a la versión más actual (versión 4.6.0).

Figura 3.38. Actualización del software a la versión más actual a fecha

Nota: el documento completo de encuentra en el ANEXO B, denominado "B-10_ACTUALIZACIÓN DEL SOFTWARE DE LOS EQUIPOS DE NETWORKING".

3.3.4 CONFIGURACIÓN DE LA LICENCIA DE FIREWALL.

Esta sección corresponde a la implementación del capítulo 3, categoría: seguridad cibernética y subcategoría lineamientos para actualización de parches, referente a la metodología planteada.

Para realizar la instalacion de la licencia de firewall se debe proceder al ingreso por medio de un cliente (Putty), por medio de linea de comando, se realiza la verificación de la actividad de una licencia.

En la figura 3.39. se observa que el equipo inicialmente no cuenta con una licencia de firewall.

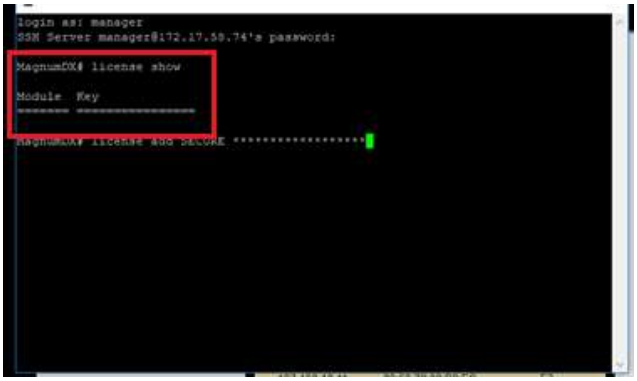

Figura 3.39. Licencia de firewall del equipo

En la figura 3.40. se procede a ingresar la clave de la licencia para su habilitación, la licencia fue adquirida por EMELNORTE.

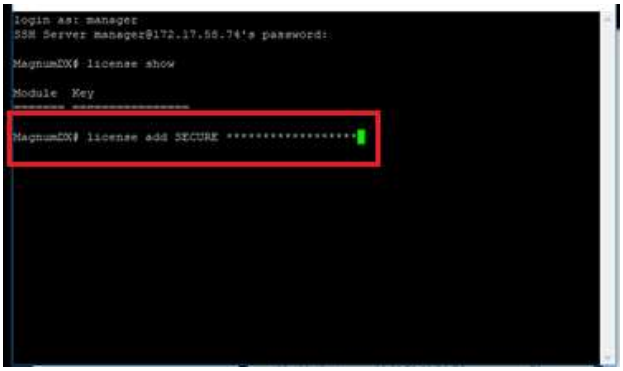

Figura 3.40. Ingreso de la licencia

3.3.5 CONFIGURACIÓN DE FIREWALL.

Esta sección corresponde a la implementación del capítulo 3, categoría: seguridad cibernética y subcategoría lineamientos de control de acceso, referente a la metodología planteada.

Se procede a realizar configuraciones básicas en la sección de firewall del router.

Router garrettcom DX940. (R_RETORNO).

En la figura 3.41 se observa las configuraciones globales de firewall.

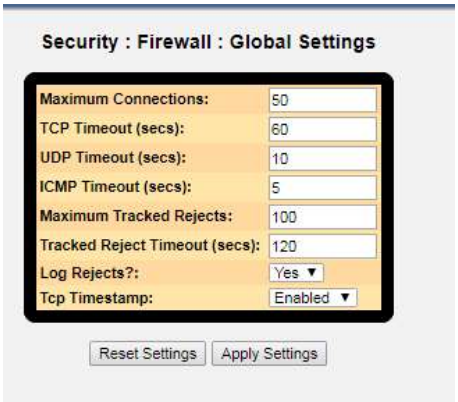

Figura 3.41. Configuraciones globales de firewall

En la figura 3.42. se observa la generación de un grupo en el cual se coloca las reglas de acceso.

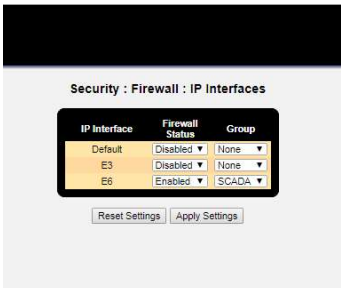

Figura 3.42. Reglas de acceso

En la figura 2.43. se observa cómo se procede a asociar el grupo con la interfaz del equipo.

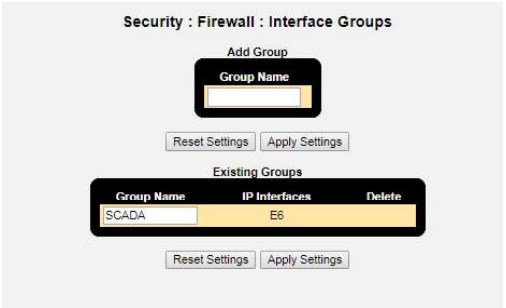

Figura 3.43. Asociación del grupo con la interfaz del equipo

En la figura 3.44. se aprecia la lista de direcciones que se permite el ingreso.

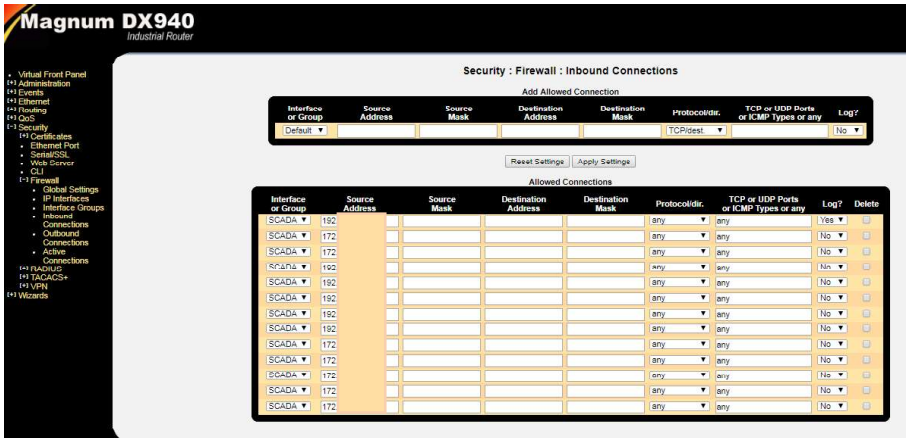

Figura 3.44. Direcciones habilitadas el ingreso

3.3.6 CONFIGURACIÓN DE PUERTOS SEGUROS.

Esta sección corresponde a la implementación del capítulo 3, categoría: seguridad cibernética y subcategoría lineamientos para administración de puertos y servicios., referente a la metodología planteada.

Router garrettcom DX940. (R_RETORNO).

Se procedió realizar la configuración de puerto seguro únicamente al puerto E6 donde la acción permite que el puerto se bloquee al pasar de estado “UP” a “DOWN”

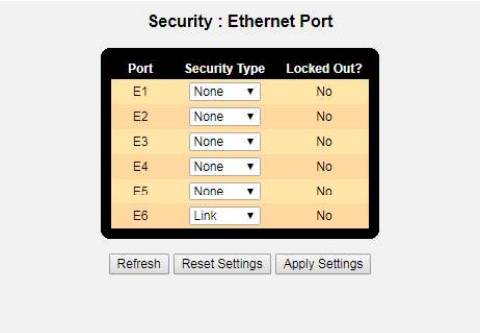

Figura 3.45. Se habilita la interface y la acción posterior

Posterior a realizar la aplicación de la metodologia en la subetacion el retorno se realiza las siguientes evaluaciones donde se obtienen los siguientes resultados.

3.4. RESULTADOS GLOBALES DEL ANÁLISIS DE LA ARQUITECTURA FÍSICA DE LA RED LAN DE LA SUBESTACIÓN EL RETORNO POSTERIOR A LA IMPLEMENTACIÓN DE LA METODOLOGÍA.

En base a la figura 3.1. podemos determinar el tipo de arquitectura que presenta la red de la subestación EL RETORNO, la cual presenta las siguientes características:

- La arquitectura es denominada anillo con enlaces redundantes.
- Presenta enlaces físicos redundantes en los switches.
- Los relés se encuentran en dos switches.
- La arquitectura es escalable ya que se pueden colocar más equipos.
- La arquitectura es flexible para realizar cambios.
- Todos los equipos que se encuentran comunicando dentro de la red se encuentran operativos.
- La red se encuentra con una disponibilidad de 100%, sin embargo, se recomienda realizar un registro anual del tiempo que la red salga de servicio.

En la tabla 3.1. se detalla los resultados obtenidos en la red de comunicaciones de la subestación eléctrica EL RETORNO, posterior a la aplicación de la metodología. Es importante mencionar que los criterios para realizar el análisis se encuentran en el numeral 1.3.5.

Tabla 3.1. Resultados de la evaluación de la arquitectura física de la red LAN EL RETORNO posterior a la aplicación de la metodología

#	DESCRIPCIÓN	ESTADO			
		Excelente	Buena	Deficiente	Inexistente
1	Redundancia de enlaces.	✓			
2	Redundancia de switches.	✓			
3	Redundancia de router.				✓
4	Flexibilidad.	✓			
5	Escalabilidad	✓			
6	Disponibilidad	✓			
7	Confiabilidad	✓			

Figura 3.46. Resultados globales del análisis de arquitectura de la red LAN de la subestación EL RETORNO posterior a la aplicación dela metodología

3.5 RESULTADOS GLOBALES DEL ANALISIS DE ADMINISTRACIÓN Y GESTIÓN DE LOS EQUIPOS DE LA RED DE LA SUBESTACIÓN EL RETORNO POSTERIOR A LA APLICACIÓN DE LA METODOLOGÍA.

Posterior a realizar la aplicación de la metodología y realizar las configuraciones necesarias en los equipos de networking se llegó a los resultados mostrados en la tabla 3.2. Es importante mencionar que los criterios para realizar el análisis se encuentran en el numeral 1.3.5.

Tabla 3.2. Resultados globales de la administración y gestión de la red LAN de la subestación EL RETORNO

#	DESCRIPCIÓN	ESTADO			
		Excelente	Buena	Deficiente	Inexistente
1	topología	✓			
2	Redundancia física.	✓			
3	Redundancia lógica.	✓			
4	Direccionamiento.	✓			
5	Configuraciones de enrutamiento.	✓			
6	Configuraciones administrativas básicas.	✓			
7	Credenciales.	✓			
8	Protocolos de sincronización de red.	✓			
9	Configuraciones de seguridad de red.	✓			

10	Estado de uso de memoria y CPU de equipos.	✓			
11	Configuraciones de calidad de servicio.		✓		
12	Políticas de seguridad.	✓			
13	Procedimientos de administración y gestión.	✓			

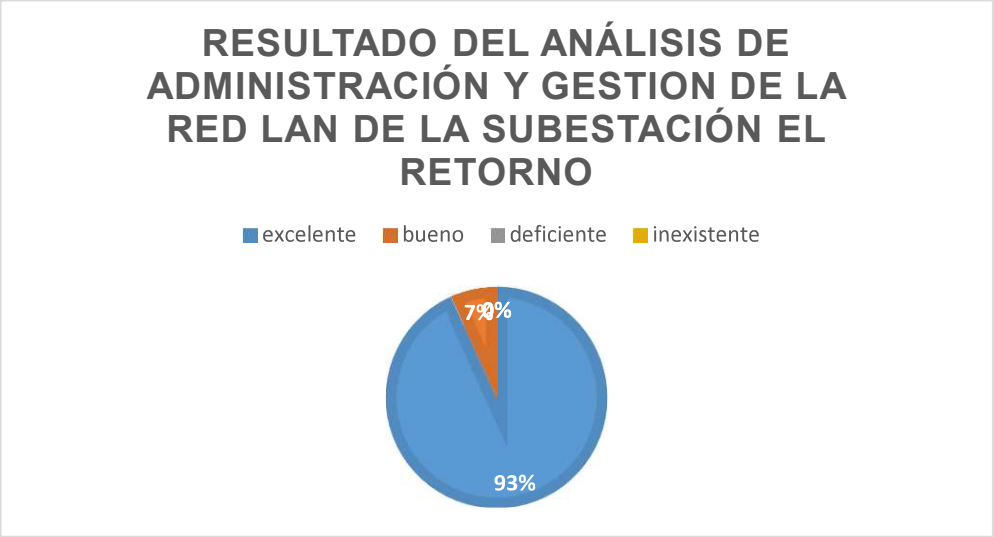

Figura 3.47. Resultados del análisis de administración y gestión de la red LAN de la subestación EL RETORNO

NOTA: el analisis de administración y gestion posterior a la aplicación de la metodología se encuentra en el ANEXO B, denominado "B-19_RESULTADOS DEL ANÁLISIS POSTERIOR A LA APLICACIÓN DE LA METODOLOGÍA".

3.6 RESULTADOS GLOBALES DEL ANÁLSIS DE VULNERABILIDADES POSTERIOR A LA APLICACIÓN DE LA METODOLOGÍA.

Se debe considerar que para realizar el análisis fue necesario habilitar la dirección del equipo con el que se realizó el análisis antes de la aplicación de la metodología, esto demuestra que la red es más segura.

El análisis de las vulnerabilidades que nos presenta NESSUS de toda la red LAN de la subestación EL RETORNO se observa en la figura 3.48.

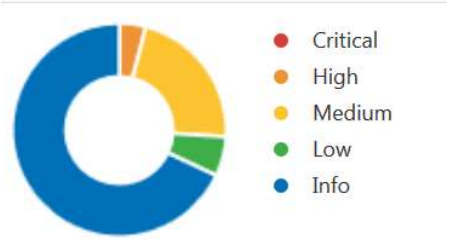

Figura 3.48. Disco estadístico obtenido del análisis de vulnerabilidades usando el software NESSUS

En la tabla 3.3. se observa los resultados porcentuales del análisis de vulnerabilidades obtenido por NESSUS.

Tabla 3.3. Resultados porcentuales del análisis de vulnerabilidades aplicado a la subestación EL RETORNO usando NESSUS

ESTADO	PORCENTAJE
informativo	64%
bajo	7%
medio	26%
alto	3%
critico	0%

Como podemos observar en los porcentajes del analisis se logro eliminar el estado critico del sistema ademas cae mensionar que el estado alto mensionado corresponde a la habilitacion del protoclo telnet el cual se dejo habilitado ya que no en todos los equipos se podia habilitar el protocolo SSH, sin embargo con el firewall implementado la red ya es mas segura.

NOTA: el analisis de administración y gestion posterior a la aplicación de la metodología se encuentra en el ANEXO B, denominado “B-19_RESULTADOS DEL ANÁLISIS POSTERIOR A LA APLICACIÓN DE LA METODOLOGÍA”.

Posterior a realizar la aplicación de la metodologia en la subestacion EL RETORNO y comparando los resultados obtenidos se puede decir que los resultados fueron optimos ya que la red actualemte se encuentra en perfecto estado y a fecha de este trabajo no se han presentado fallas que dejen fuera de servicio.

Las red de comunicaciones de la subestacion EL RETORNO es mas segura ya que su acceso fue completamente limitado evitando asi posibles afectaciones.

3.7 RESULTADOS GLOBALES COMPARATIVOS

En esta sección se presentarán los resultados comparativos antes de aplicar la metodología y posterior a la aplicación de la metodología.

En la figura 3.49. se presenta los resultados comparativos del análisis de la arquitectura física de la red LAN de la subestación EL RETORNO.

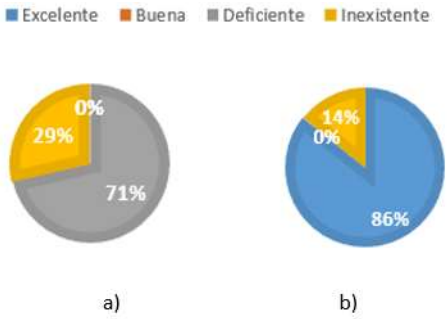

Figura 3.49. a) Resultados iniciales del análisis, b) Resultados posteriores a la aplicación de la metodología

En la figura 3.50. se presenta los resultados comparativos del análisis de administración y gestión de los equipos dela red LAN de la subestación EL RETORNO.

Figura 3.50. a) Resultados iniciales del análisis, b) Resultados posteriores a la aplicación de la metodología

En la figura 3.51. se presenta los resultados comparativos del análisis de vulnerabilidades.

ESTADO	PORCENTAJE
Informativo	56%
Bajo	5%
Medio	27%
Alto	5%
Critico	7%

a)

ESTADO	PORCENTAJE
informativo	64%
bajo	7%
medio	26%
alto	3%
critico	0%

b)

Figura 3.51. a) Resultados iniciales del análisis, b) Resultados posteriores a la aplicación de la metodología

4. CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- El presente proyecto ha cumplido con satisfacción los objetivos planteados, ya que se logró realizar una metodología que permite mantener una arquitectura física acorde a las necesidades de una red de comunicaciones en las subestaciones eléctrica, una buena administración, gestión y seguridad cibernética dentro de las redes de comunicaciones de las subestaciones eléctrica de EMELNORTE.

- La organización de la red de comunicaciones mejoró notablemente ya que se estructuró un método estandarizado y minucioso el cual permite tener una red con mayor disponibilidad gracias a su arquitectura parcialmente redundante.

- Se logró separar la red de comunicaciones industriales de la subestación y la red de comunicaciones administrativas, de forma lógica, la cual forma parte del sistema SCADA de EMELNORTE, por medio de la administración total del departamento SCADA.

- Se propuso y valido los parámetros de seguridad cibernética donde se realizaron restricciones de acceso lo cual permite mantener a la red fuera del alcance de personal no autorizado.

- Se realizó la configuración de credenciales en donde se tiene un perfil de operador el cual tiene solo atributos de lectura, además se crearon credenciales de administrador el cual permite una total manipulación y acceso hacia los equipos de networking, esto ha permitido una mejora en la administración de la red.

- Se logró configurar un servidor SNTP que permite mantener a toda la red de comunicaciones de la subestación eléctrica EL RETORNO en sincronismo, lo que más adelante se traducirá en evitar desfases temporales en los eventos que se generan en la operación del equipo de accionamiento.

4.2 RECOMENDACIONES

- En la actualidad la seguridad cibernética es tema que se debe tratar de forma primordial en la empresa eléctrica EMELNORTE ya que las subestaciones eléctricas son consideradas puntos estratégicos para el desarrollo del país.

- Para realizar la incorporación de un equipo nuevo a la red de la subestación es importante realizar una limpieza de las tablas ARP que se encuentran en el switch administrable de borde.
- Se debe habilitar los puertos seguros en todos los equipos de networking de la red de comunicaciones de la subestación EL RETORNO con la finalidad de evitar el ingreso de personal no autorizado.
- Es importante mantener una documentación clara minuciosa de las configuraciones realizadas y de las modificaciones que se pueden aplicar.
- Si se desea introducir a la red el equipo ASAT y la pantalla táctil se debe realizar las actualizaciones necesarias ya que la pantalla cuenta con un sistema operativo perteneciente a Microsoft, y este sistema generalmente es víctima de ataques, por ello es indispensable realizar las actualizaciones necesarias o en el mejor de los casos migrar a un sistema operativo como Linux..
- Se debe asignar a personal encargado para mantener las redes de comunicación actualizadas y en buen funcionamiento.
- Se recomienda instalar un programa de monitoreo en un equipo especifico del centro de control, para así poder realizar un monitoreo minucioso del estado de los equipos.
- Se recomienda realizar restricciones totales de acceso al segmento de red otorgado a las comunicaciones del sistema SCADA.
- Realizar mantenimiento y verificación de las configuraciones y funcionamiento de la red en un periodo no mayor a 8 meses.
- Se recomienda implementar las cámaras de vigilancia y el NVR en el switch administrable de frontera considerando siempre privilegios al tráfico de la red de comunicaciones de la subestación eléctrica.
- Si se desea implementar el protocolo IEC 61850 tomar en consideración que este protocolo se desenvuelve mejor en equipos de la misma marca, o en el caso de no tener equipos de la misma marca considerar la interoperabilidad de los mismos.
- Si se migra al protocolo IEC 61850 se recomienda implementar el protocolo GOOSE para una comunicación horizontal.

- Se recomienda implementar un equipo de sincronización de forma local, ya que en la actualidad el equipo se encuentra en una subestación cercana.
- Se recomienda implementar una línea de comunicación física única y exclusiva para todas las subestaciones de EMELNORTE así te tendrá una separación física de la red industrial y de la red corporativa.
- Se recomienda tener registros de tiempo de disponibilidad de la red de forma anual para posteriores evaluaciones de la red.
- Se recomienda realizar la aplicación de la metodología en todas las subestaciones eléctricas de la concesión de EMELNORTE.
- Se recomienda habilitar las configuraciones de puerto seguro para todos los dispositivos de networking de la subestación eléctrica EL RETORNO.
- Si se habilita el servidor HTTP en los equipos de networking, este debe ser momentáneo, ya que es recomendable realizar configuraciones por línea de comando.

5. REFERENCIAS BIBLIOGRÁFICAS

- [1] Victor Chebyshev, Fedor Sinitsyn, Denis Parinov, Alexander Liskin, Leg Kupreev. (2018, agosto 6) “desarrollo de las amenazas informaticas en el Segundo trimester de 2018 Estadística [online] disponible: https://securelist.lat/it-threat-evolution-q2-2018-statistics/87391/

- [2] C.S. Lewis. (2013, octubre 29) “Clasificacion de malwares” [online] disponible: https://latam.kaspersky.com/blog/clasificacion-de-malwares/1608/

- [3] Centre for the protection of National Infraestructure. (2005 febrero 15) “FIREWALLDEPLOYMENT FOR SCADA AND PROCESS CONTROL NETWORKS”

- [4] Fernando Cevilla (2015, febrero 12) ”aplicación de tecnologías antimalware en entornos OT” disponible: http://www.ciberseguridadlogitek.com/aplicacion-de-tecnologias-antimalware-en-entornos-ot/

- [5] Cesar Otero (2017, abril 4) “Los Tres Tipos de hacker que existen en el mundo” disponible: https://as.com/betech/2017/04/04/portada/1491340019_511041.html

- [6] NERC-CIP STANDARD “CIP-007-6 (Cyber Security-System Security management)” version 5, junio 2014.

- [7] Esteban Pérez López “Los Sistemas SCADA en la automatización Industrial”, tecnología en marcha, vol 28, nº 4, octubre-diciembre. Pag 3-14, 27, febrero 2015.

- [8] Aquilino Rodríguez Penin “Sistemas SCADA” Alfaomega Grupo Editor, S.A. de CV., México ISBN: 978-607-707-406-9, tercera edición, mayo 2013.

- [9] National Instrument (16, octubre 2014) “Informacion detallada sobre el Protocolo Modbus” disponible: http://www.ni.com/white-paper/52134/es/

- [10] J. Feria, J. Camargo, E. Muskus “Disño e implementación de un algoritmo para traslación de protocolo entre las normas IEC60870-5-104 y MODBUS TCP/IP”, Ingenium, vol. 16, nº32. Pp. 118-125, junio 2015.

- [11] P. Matousek faculty of information technology “description of analysis of IEC 104 Protocol” reporte técnico no. FIT-TR-2017-12, diciembre, 2017

- [12] IEC 61850-7-1 “COMMUNICATION NETWORKS AND SYSTEMS IN SUBSTATION-PART 7-1: Basic communication structure for substation and feeder equipment-Principles and models”, primera edicion, julio 2003.
- [13] Tenable-Nessus, (21, noviembre 2018) página official de Tenable, disponible: https://www.tenable.com/products/nessus/nessus-professional
- [14] Manual de características de: switch GarretCom Magnum 6KL, disponible: https://www.belden.com/hubfs/resources/technical/catalogs/6K%20Series.pdf?hsLang=en&t=1533325453757
- [15] Manual de características de: Router GarretCom Magnum DX940, disponible: http://media.beldensolutions.com/garrettcom/techsupport/hardware/datasheets/dx940ds.pdf
- [16] manual de características de ION 8500, disponible: http://www2.schneider-electric.com/resources/sites/SCHNEIDER_ELECTRIC/content/live/FAQS/239000/FA239172/en_US/ION8300_8400_8500_Installation_Guide_70000-0206-13.pdf
- [17] manual de características del relé general electric T35, disponible: http://www.gegridsolutions.com/products/manuals/t35/t35man-w1.pdf
- [18] manual de características del relé general electric T60, disponible: https://www.gegridsolutions.com/products/manuals/t60/t60mansp.pdf
- [19] manual de características del medidor Schneider 8500, disponible: https://download.schneider-electric.com/files?p_File_Name=M8600A0C0E5E0A0A_DATASHEET_WW_en-WW.pdf&p_Reference=M8600A0C0E5E0A0A_DATASHEET
- [20] manual de equipo de protección del banco de condensadores y Sistema De Control C70 de General Electric, disponible: http://www.gegridsolutions.com/products/manuals/c70/c70man-u3.pdf
- [21] G. Combs, (2008). Wireshark (versión III) disponible: https://www.wireshark.org/
- [22] Paessler, (2018, diciembre 11). Monitoreo de redes (versión 18.4.47.1962) disponible: https://www.es.paessler.com/
- [23] ipswitch, (2010). whatsUp Gold, disponible: https://es.ipswitch.com/

- [24] V. Guerrero, R. Yuste, L. Martínez, *Comunicaciones Industriales*. (primera edicion). Barcelona-España, editorial MARCOMBO, 2010.
- [25] E. Thomson, *Cybersecurity Incident Response.* (primera edición). Illinois-E.E.U.U., 2018.
- [26] TELVENT, catálogo de Saitel I2000DP, disponible: info@telvent.com.
- [27] E. Terán, "Guía de conceptos, características y funciones de los sistemas de automatización de subestaciones y sus componentes", CELEC EP-TRANSELECTRIC, G.01.PV.02.03, versión 1.0, 2017-11.
- [28] INCIBE, (2018, septiembre 18). Las claves de los últimos ataques en sistemas de control industrial, [online], disponible: https://www.incibe-cert.es/blog/las-claves-los-ultimos-ataques-sistemas-control-industrial.
- [29] Manual de características de: switch General Electric ML2400, disponible: https://www.gegridsolutions.com/products/manuals/multilink/ml24man-ad.pdf

6. ANEXOS

Los anexos se adjuntan de forma digital debido a la cantidad de imágenes y tablas que se generaron en el estudio técnico.

Los anexos son los siguientes:

ANEXO A.: Análisis de la administración, gestión y seguridad cibernética de la red de comunicaciones de la subestación EL RETORNO. Realizado en el periodo (junio-diciembre del 2018).

ANEXO B.: Aplicación de la metodología.

ANEXO C.: Manuales de los equipos de networking.

ORDEN DE EMPASTADO