UNIVERSIDAD DE CUENCA

FACULTAD DE INGENIERÍA

PROGRAMA ESPECIAL DE TITULACION DE LA MAESTRIA EN TELEMATICA

DISEÑO DE TESIS

EVALUAR LAS VULNERABILIDADES DE SEGURIDAD EXISTENTES EN LA RED DEL SISTEMA SCADA DE LA EERSSA.

PREVIO A LA OBTENCION DEL GRADO DE MAGISTER EN TELEMATICA

AUTOR: Ing. Nancy González Tandazo.
C.I. 11038691223

DIRECTOR: Ing. Sofia Priscila Arèvalo Maldonado.
C.I. 0103721031

Febrero 2016

CUENCA-ECUADOR

RESUMEN.

Los Sistemas SCADA a diferencia de los sistemas de tecnologías de la información comunes, son sistemas que permiten monitorear y controlar procesos de carácter crítico, como el suministro de energía eléctrica. Los sistemas SCADA se distinguen por mantener la continuidad de sus procesos, de manera indefinida, a través de la operación coordinada y confiable de distintos componentes, como los subsistemas de telecomunicaciones, las redes de datos, redundancia de servidores y equipos principales, los respaldos de energía, etc.; característica distinguida que los diferencia de otros sistemas de TI (Tecnologías de Información).

Inicialmente los sistemas SCADA se crearon en ambientes aislados a los corporativos, y debido a necesidades operativas y de administración ha sido necesario permitir accesos desde otras instancias como internet para la publicación de datos, así como incorporar personal multidisciplinario para la operación del sistema, lo que involucra que estas permisiones pueden ser vulnerabilidades.

Debido a que el suministro de energía eléctrica es un proceso continuo, que demanda precisión en las operaciones de control y monitoreo; en el presente trabajo se consideró evaluar las vulnerabilidades que presenta el Sistema SCADA Local de la Empresa Eléctrica Regional de Sur S.A. (EERSSA); la cual está encargada de la Generación, Distribución y Comercialización de Energía Eléctrica para las provincias de Loja y Zamora Chinchipe.

En este proyecto se ejecutó una evaluación de la seguridad informática de la red de datos del sistema SCADA de la EERSSA, así como una investigación sobre las estrategias de seguridad basadas en la Norma ISO 27002; para con ello plantear propuestas dirigidas a mejorar e implantar procedimientos de seguridad informática al sistema SCADA Local de la EERSSA.

Palabras Clave: SCADA; Seguridad; Sistema Eléctrico de Potencia.

ABSTRACT.

SCADA systems unlike common information technology systems are systems that monitor and control critical processes, like power distribution of energy. SCADA systems are distinguished by continuity of their processes in an indefinitely manner, through coordinated and reliable operation of various components, such as telecommunications subsystems, data networks, server redundancy and key equipment, energy backup systems, etc . This is a distinguishing feature that differentiates it from other IT systems (Information Technology).

Initially SCADA systems were created isolated from corporate environments, and because of operational and management needs it has been necessary to allow access from other types of connections, such as Internet for data publishing and also incorporate multidisciplinary staff to operate the system. These additional permissions can become vulnerabilities.

Because the power distribution is an ongoing process that demands precision in control operations and monitoring; in this study it was considered performing an evaluation of the vulnerabilities that are present in the Local SCADA System of Empresa Electrica Regional del Sur S.A. (EERSSA); which is responsible for generation, distribution and commercializing for the provinces of Loja and Zamora Chinchipe.

In this project was performed an evaluation of information security for the data network of EERSSA SCADA system, as well as an investigation of security strategies based on ISO 27002 standard; with the objective to make proposals to improve and implement security procedures to EERSSA Local SCADA system.

Keywords: SCADA; Security; Power System.

INDICE DE CONTENIDOS

INDICE DE FIGURAS

INDICE DE TABLAS

INDICE DE ANEXOS

Nancy Etelbida González Tandazo, autora de la tesis "EVALUAR LAS VULNERABILIDADES DE SEGURIDAD EXISTENTES EN LA RED DEL SISTEMA SCADA DE LA EERSSA", reconozco y acepto el derecho de la Universidad de Cuenca, en base al Art. 5 literal c) de su Reglamento de Propiedad Intelectual, de publicar este trabajo por cualquier medio conocido o por conocer, al ser este requisito para la obtención de mi título de MAGISTER EN TELEMATICA. El uso que la Universidad de Cuenca hiciere de este trabajo, no implicará afección alguna de mis derechos morales o patrimoniales como autora.

Cuenca, 28 de Febrero 2016.

Nancy Etelbida González Tandazo.
C.I: 1103861223

Nancy Etelbida González Tandazo, autora de la tesis "EVALUAR LAS VULNERABILIDADES DE SEGURIDAD EXISTENTES EN LA RED DEL SISTEMA SCADA DE LA EERSSA", certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autora.

Cuenca,28 de febrero 2016.

Nancy Etelbida González Tandazo

C.I: 1103861223

CAPITULO I

1. INTRODUCCION

1.1 Antecedentes.

La Empresa Eléctrica Regional del Sur (EERSSA) es una empresa de generación distribución y comercialización de energía eléctrica su área de concesión la conforman las provincias de Loja, Zamora Chinchipe y el cantón Gualaquiza de la provincia de Morona Santiago sirviendo por muchas décadas de manera eficiente a la región sur oriental del Ecuador.

La EERSSA tiene un área de concesión de 22.721Km^2 y un total de 183.353 clientes, a finales de Julio del 2014, distribuidos en alimentadores rurales y urbanos, el total de la demanda de la EERSSA es de 58 MW los cuales son suministrados por el Sistema Nacional Interconectado (SNI) a través de la subestación Loja de TRANSELECTRIC, compañía encargada del Sistema Nacional de Transmisión, que recibe la energía generada en la Central Hidroeléctrica Paute, además la EERSSA tiene dos centrales hidroeléctricas la Ing. Carlos Mora con 2.4MW, la Central Isimanchi 2.28 MW y una Central Térmica Catamayo con 10 MW.

Dispone de 19 subestaciones de reducción y 5 subestaciones de seccionamiento, y a lo largo de la red de distribución tiene instalados reconectadores, reguladores de voltaje y bancos de capacitores para una operación confiable del sistema.

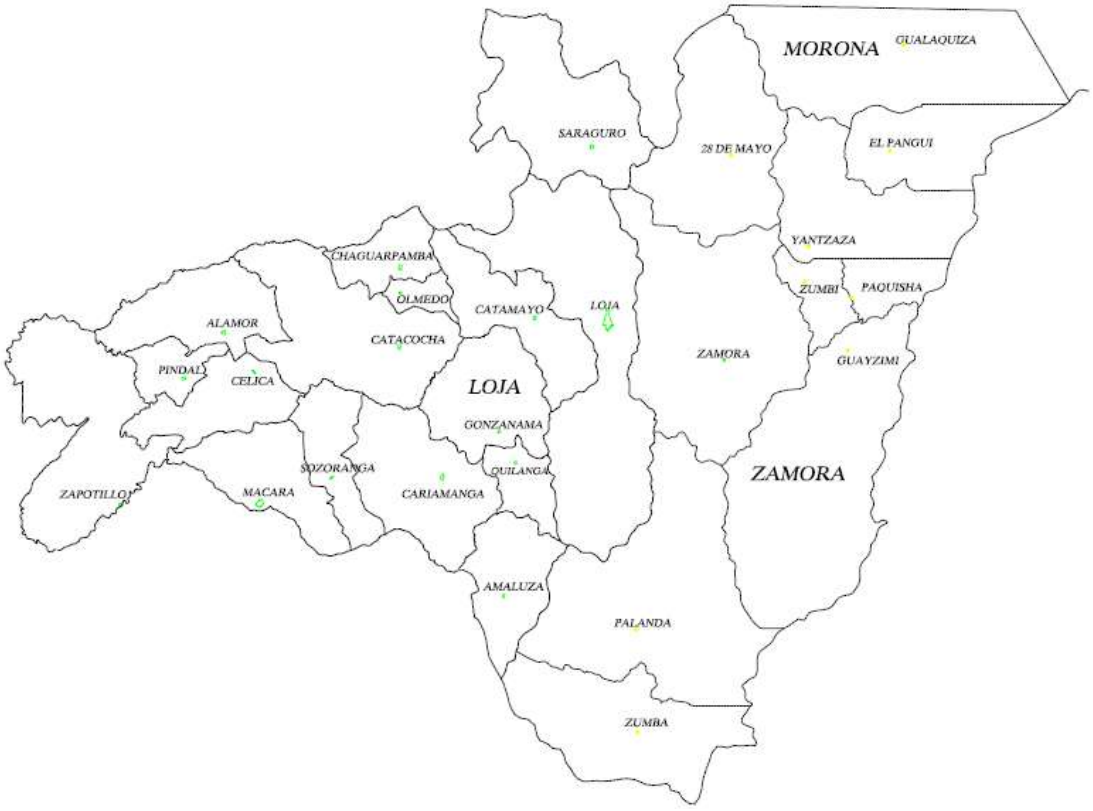

Figura 1.- *Área de concesión de la EERSSA. FUENTE: EERSSA.*

El edificio matriz se encuentra ubicado en el centro de la ciudad de Loja concentra la parte administrativa desde donde se coordinan los trabajos con las diferentes agencias asentadas en el área de concesión, además se encuentran las gerencias encargadas de la parte técnica que coordinan los trabajos de operación y mantenimiento con los diferentes grupos de trabajo.

Al tener un área de concesión muy grande y considerando que para coordinar la reposición del servicio luego de una suspensión, por operación de protecciones, se debía coordinar con el personal del sector que en ocasiones estaba laborando en sitios alejados a las subestaciones, lo que elevaba los tiempos de desconexión, se fue pensando la manera de centralizar el monitoreo y el control de los elementos de las subestaciones

Con el afán de brindar un mejor servicio y minimizar tiempos de interrupciones por maniobras en las subestaciones, la Superintendencia de Subestaciones y Comunicaciones impulsó en el 2007 el proyecto de la implementación de un sistema SCADA para la EERSSA, que permita además de monitorear y controlar de forma remota los elementos de las subestaciones, llevar un registro histórico de operaciones y de parámetros eléctricos del sistema que permitan emitir juicios de valor de una manera más acertada en caso de operación de protecciones o trabajos de mantenimiento programados y emergentes.

En el año 2009 entró a funcionar el Centro de Control instalado en el edificio matriz de la EERSSA, el software del SCADA ***Power Link Advantage*** (PLA), fue suministrado por General Electric (GE) a través de su representante, para Sudamérica, AUTOTROL empresa domiciliada en Argentina, que luego de los procesos de adjudicación implementó el Sistema SCADA Local, que en su primera etapa estaba conformado por el Centro de Control al cual reportaron 7 Subestaciones y las centrales Carlos Mora y Catamayo.

Adicionalmente al sistema SCADA, para operación del sistema de Potencia, se integraron los sistemas de vigilancia y de gestión de red de comunicaciones. El sistema de vigilancia comprende la instalación de cámaras de video Fija y PTZ con su respectivo grabador de video, sensores de movimiento para detección de ingreso de personal no autorizado, sensores de humo en caso de contingencias y controles de acceso a través de cerraduras magnéticas y lectoras con tarjetas de acceso todo esto controlado por una tarjeta de comunicación de red de Marca ***Lenel On Guard*** El sistema de gestión de la red de comunicaciones se realiza a través del software ***What´s Up*** que permite observar el comportamiento de todos los elementos que integran los enlaces en la red de transmisión de datos por radio con su respectivo

respaldo de fibra presentando alarmas cuando un dispositivo deja de operar, los equipos que se gestionan son repetidoras, switch y UPS.

A lo largo de estos años se han ido integrando más subestaciones al sistema lo que implica crecimiento en cada uno de los sistemas.

Al tratarse de un sistema de red, clave para el suministro de energía eléctrica en la región sur del país, es importante revisar cuan segura se encuentra la red, sí es lo suficientemente robusta para limitar el acceso de terceros, evitando intrusiones que podrían ser mal intencionadas.

Por ejemplo se debería realizar una revisión de los protocolos de seguridad que existen para el acceso al cuarto de servidores, ya que es el lugar más sensible, además se debe considerar si las restricciones de acceso a la red son suficientes o se debe considerar filtros adicionales, ya que desde que se implementó el sistema en el 2009, no se han realizado ajustes para evitar restricciones de acceso a la red.

Además es necesario evaluar si la red está limitando el ingreso de archivos dañinos como virus o troyanos comunes, que no son insertados directamente para vulnerar el SCADA Local de la EERSSA, pero que pueden provocar el mal funcionamiento de los servicios en los dispositivos nodos lo que resultaría en operación deficiente de los clientes, por ejemplo podría desembocar en retardo en ejecución de comandos.

El evaluar la seguridad de la red del Sistema SCADA y determinar las vulnerabilidades del mismo, permitirá evaluar si la infraestructura telemática y las seguridades son suficientes para garantizar un funcionamiento adecuado sin riesgo de intrusiones maliciosas, en caso contrario se alertará a los profesionales encargados para tomar las consideraciones del caso logrando mejorar la seguridad lo que garantizará un funcionamiento adecuado en el suministro de energía.

Para que cada una de las subestaciones reporte al Centro de Control se implementó un sistema de radio, y en ciertos puntos se cuenta con respaldo de fibra óptica, se está trabajando actualmente en la instalación de un sistema más confiable a través de bandas licenciadas de microondas.

EL SCADA Local de EERSSA cuenta con dos servidores para el sistema PLA (principal y respaldo), con dos clientes (estación de operación y proyección), un servidor de Históricos, un servidor de vigilancia con su cliente y un servidor para gestión de red, un servidor principal y de respaldo para comunicación por Protocolo entre centros de Control (ICCP Intercontrol Center Communications Protocol) con el Centro de Control del Energía CENACE, estos se sincronizan a través de un GPS, tiene instalado además un firewall para delimitar la red corporativa a través del cual se permite un acceso de la máquina para gestión de los relés de protecciones y envío de formatos de generación.

En la Figura 2 se muestra un despliegue de la pantalla del PLA que contiene los elementos que conforman la red de comunicaciones del SCADA.

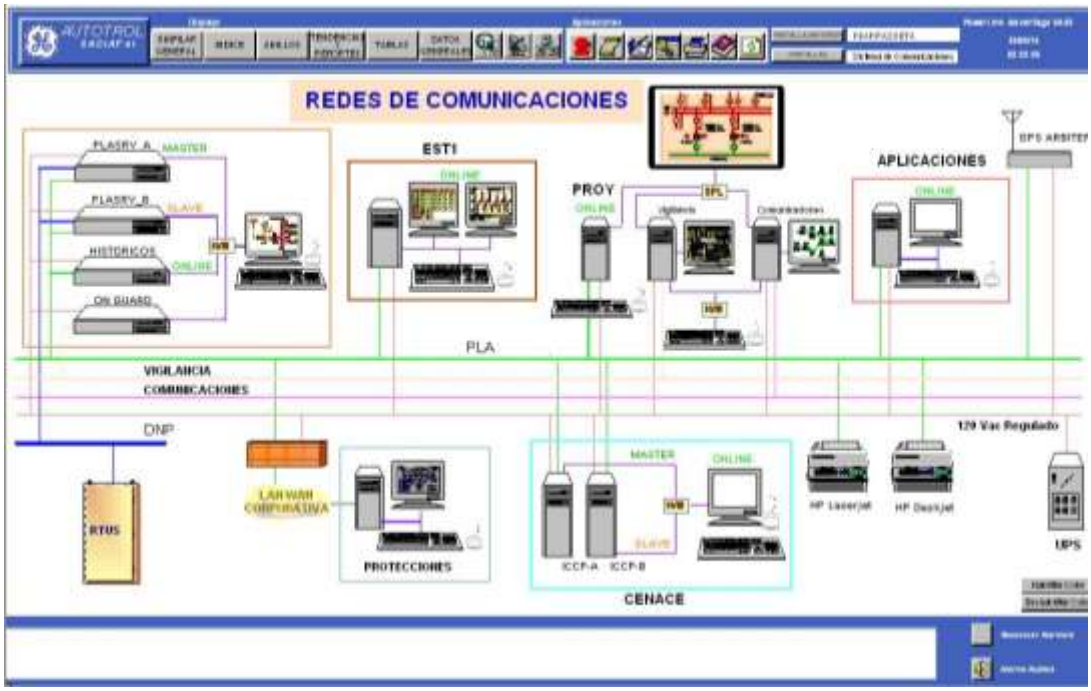

Figura 2.- *Esquema del Sistema de Comunicaciones. Fuente EERSSA*

1.2 Estado del arte.

En la mayoría de los procesos industriales: distribución de gas, transporte de petróleo, etc; y cotidianos como control de ascensores y escaleras, sistemas de semaforización; es cada vez más común encontrar sistemas de monitoreo y control que faciliten la operación y permitan tener un registro en tiempo real de eventos con el soporte de un software dedicado.

Las empresas distribuidoras de energía eléctrica a nivel mundial han implementados sistemas SCADA, para qué, como su nombre lo indica permitan Supervisar, Controlar y Adquirir Datos de los equipos que intervienen en los sistemas eléctricos, optimizando su operación, minimizando tiempos de desconexión permitiendo continuidad en el suministro del servicio, logrando mejorar sus índices de calidad y sobretodo lograr servir de mejor manera a sus clientes.

Muchas empresas se han dedicado a la elaboración de estos software a nivel mundial, ABB, General Electric, Schneider Electric, Siemens, etc se

han posicionado cubriendo los requerimientos de las distribuidoras actualmente el alcance de estos sistemas SCADA es mayor, se complementan con sistemas de gestión de interrupciones y de redes de distribución, inicialmente estos sistemas tenían código propio cada empresa desarrollaba una solución en sus propios sistemas operativos.

En el país las empresas distribuidoras también se han motivado por prestar un mejor servicio y han integrado sistemas para el monitoreo y control de los elementos de las subestaciones para poder prevenir incidentes, detectar posibles fallas y corregirlas antes de que provoquen percances mayores en el servicio, entre ellas podemos citar: Empresa Eléctrica Ambato, Empresa Eléctrica Quito, Empresa Eléctrica Centrosur, CNEL Santo Domingo, Central Eólica Villonaco, Empresa Eléctrica Regional del Sur; además el Centro Nacional de Control de Energía

CENACE tiene implementado un sistema SCADA para monitoreo del despacho de energía y del sistema nacional de transmisión.

Debido al auge de la implementación de estos sistemas se ha desarrollado el protocolo **ICCP (Inter-Control Centre Communications Protocol)** que permite la comunicación entre centros de control logrando el intercambio de datos sobre red de área amplia, soporta cualquier interfaz física, servicio de transporte y de red, se desarrolla bajo norma **IEC 60870 part 6.**

Al momento de implementar estos sistemas principalmente se considera su funcionalidad y rendimiento, se inicia separando los entornos industriales de los corporativos de las instituciones, luego de un tiempo con el fin de facilitar el acceso remoto al personal de administración, estos entornos se comparten, si bien esta relación ayuda a reducir costos y permitir conexiones desde diversos sitios, exponen mayormente el sistema a infecciones de virus, troyanos, y son posibles entradas de infiltraciones no autorizadas. Si bien en nuestro entorno nacional no se

ha escuchado de ataques o invasiones maliciosas a sistemas SCADA de servicios, no debemos restar importancia a la seguridad que se debe tener en la red de estos sistemas suponiendo escenarios extremos.

Al emplear estos sistemas en procesos delicados que demandan continuidad en el servicio se han realizado varias investigaciones con el fin de solventar ataques que son muy comunes en sistemas de red habituales, entre los estudios realizados se encuentran los siguientes:

Guía para empresas: Seguridad de los Sistemas de Monitorización y control de los procesos e infraestructuras (SCADA), publicado por el INSTITUTO NACIONAL DE TECNOLOGIAS DE LA COMUNICACIÓN (INTECO), del Gobierno de España, aborda de manera general las prácticas de seguridad que deben cumplir las empresas de servicios que tienen instalados estos sistemas, recalcando que la seguridad de redes se ha vuelto un asunto de importancia para el gobierno Español, en este documento se citan varias referencias de organismos que han publicado normas para la seguridad de estos sistemas por ejemplo las normas NERC.[2][3]

A Plausible Solution to SCADA Security Honeypot Systems, es una publicación de IEEE, que propone el empleo de sistema honeypot o sistemas con seguridades bajas que atraigan la atención de los atacantes, el empleo de estos sistemas puede alertar a los administradores de red de posibles infiltraciones sin que se vea afectado el sistema real, simula un entorno de red honeypot y demuestra su eficiencia. [4]

Application of NTRU Cryptographic Algorithm for SCADA Security, también es una publicación IEEE, en esta investigación se propone el empleo de algoritmos NTRU , sistema de encriptación de clave pública.[5]

En todas estas investigaciones se aclara sobre la necesidad de proteger los sistemas SCADA que difieren de los comunes sistemas de red corporativas ya que tienen asociados servicios ya sea a comunidades o de procesos complejos que puede desembocar en grandes pérdidas económicas o afectaciones graves a usuarios finales si su seguridad es vulnerada.

Debido a la importancia de la aplicación de estos sistemas procesos que involucran servicios básicos y entornos de red varias organizaciones a nivel mundial han trabajado en establecer normas para evitar filtración de información entre estos organismos se encuentran: [3]

- *Centre for the Protection of National Infrastructure (CPNI).*
- *North American Electric Reliability Corporation (NERC).*
- *National Institute of Standards and Technology (NIST).*

1.3 Descripción del problema o necesidad.

1.3.1 Necesidades a ser satisfechas

- Los sistemas SCADA implican un alto grado de responsabilidad debido a que controlan procesos delicados y en el caso del presente estudio el suministro de energía eléctrica, por ello es importante considerar las precauciones necesarias para garantizar un funcionamiento adecuado del sistema; por ello la EERSSA ha visto la importancia de prevenir posibles ataques de virus o de terceras personas que intenten introducirse en la red para causar daños intencional o accidentalmente, por ello se debe detectar a tiempo las posibles vulnerabilidades que se encuentren en la estructura de la red para corregirlas o eliminarlas.

- En las instalaciones de la EERSSA los accesos a los cuartos de servidores y a las salas de operación son libres, no existen protocolos de acceso ni procedimientos de seguridad rutinarios como actualizaciones constantes de claves de ingreso a las consolas de operación.

1.4 Justificación del proyecto de tesis.

Hasta ahora no se ha realizado una evaluación completa de las seguridades y de las vulnerabilidades a las que está expuesto el sistema de SCADA Local de la EERSSA. Debido a la importancia de la operación del sistema por la sensibilidad del monitoreo y control que realiza y a la información que maneja, al ser vulnerada su seguridad podría causar grandes perjuicios a sus clientes afectando los índices de gestión de la EERSSA los cuales se enmarcan en las políticas del buen vivir.

El reforzar la seguridad de la red del SCADA Local de la EERSSA permitirá tener un sistema confiable logrando operaciones adecuadas en tiempos permitidos, logrando así el objetivo de una continuidad en el servicio.

El sistema eléctrico de potencia es dinámico y cada vez se integran al SCADA Local elementos nuevos que podrían convertirse en posibles puntos de vulnerabilidad por ello es necesario tomar medidas preventivas.

1.5 Objetivos de la tesis de grado

1.5.1 Objetivos generales.

Evaluar las vulnerabilidades de seguridad en la red del sistema SCADA de la EERSSA.

a. Objetivos específicos.

i. Identificar las vulnerabilidades de la arquitectura actual de la red de comunicaciones del Sistema SCADA de la EERSSA.

ii. Identificar las vulnerabilidades de la red telemática mediante operaciones de hacking ético.

iii. Realizar una propuesta de los recursos de seguridad necesarios para cubrir las vulnerabilidades de seguridad encontradas en la red.

1.6 Alcance del proyecto.

Este proyecto detectará las posibles vulnerabilidades para prevenir posibles ataques de red o de terceros que pongan en riesgo la operación fiable del SCADA

Recomendar soluciones basadas en herramientas y políticas de seguridad para fortalecer el sistema SCADA.

La evaluación de las vulnerabilidades se va a realizar para el sistema de vigilancia, de gestión de comunicaciones y SCADA PowerLink Advantage.

1.7 Método de trabajo.

1. Levantar la información de la red, detallar los equipos instalados con sus herramientas y políticas de seguridad.

2. Realizar pruebas de hacking ético desde diferentes puntos para observar si la red es de fácil acceso, para determinar las vulnerabilidades ocultas.

3. Revisar las políticas de acceso a las consolas de operación y servidores y las políticas de integración de nuevos equipos.

4. En base a los resultados obtenidos en las pruebas de hacking ético, en la revisión de las políticas de seguridad, se presentará las recomendaciones que la EERSSA debe aplicar para fortalecer la seguridad de su sistema SCADA local.

CAPITULO II

2. MARCO TEORICO.

Los sistemas SCADA se han desarrollado ya hace varios años principalmente con el afán de mejorar el rendimiento de sistemas críticos, su concepto principal es mantener la disponibilidad del sistema.

Los sistemas SCADA o sistemas de control Industrial SCI, han presentado cada vez mejores prestaciones a los usuarios facilitando la operación en procesos complejos que implican precisión en tiempo, actualmente son empleados en Empresas de Distribución de Energía Eléctrica. Para comprender de mejor manera el comportamiento en el área de la distribución de energía eléctrica vamos a indicar un modelo general.

Un sistema SCADA se emplea para controlar y monitorear los dispositivos instalados a lo largo del sistema eléctrico de potencia (apertura y cierre de interruptores, seccionadores, reconectadores, bancos de capacitores, etc), permite realizar un análisis de fallas, emite alarmas cuando se presenten eventualidades, permite el control a distancia de equipos, registra operaciones por actuación de protecciones o maniobras, control de carga y energía, gráfico de tendencias en tiempo real, con esto se consigue mejorar la gestión de protecciones. Gracias al aporte de estos sistemas se logra realizar una correcta configuración de relés de interruptores y reconectadores para asegurar la entrega de energía en forma ininterrumpida; en algunas empresas se emplea para realizar lecturas automáticas de medidores a grandes consumidores, para llevar a cabo todas estas actividades las operaciones se ejecutan desde un Centro de Control el cual es atendido permanentemente por personal capacitado en su operación.

Los sistemas SCADA monitorean señales de entrada y salida para procesos relacionados y específicos por lo que regularmente son elaborados con protocolos propietarios. Considerando que la prioridad es la disponibilidad del servicio que controlan, es común que en los ordenadores no se instalen antivirus ya que pueden confundir rutinas del sistema con archivos dañinos, esto los vuelve más sensibles que las redes corporativas.

En las redes SCADA la integridad de los mensajes que recibe y envía como ejecución de mandos y registros de señales es crucial para la toma de decisiones al enfrentar situaciones de emergencias, por ello los registros que se almacenan deben ser precisos sin sufrir alteraciones en estampas de tiempo.

El modelo de sistema SCADA está compuesto por un sistema controlado por un servidor con un software específico además lo conforman las Unidades Terminales Remotas RTU instaladas en las subestaciones y centrales de generación, las mismas que son las encargadas de recopilar toda la información de campo (señales digitales, analógicas, mensajes de relés) para ser remitida al servidor principal a través de una interfaz de comunicación. Debido a que el sistema de potencia es distribuido se emplean varios enlaces para comunicar las RTU con el Centro de Control estos enlaces pueden ser: radio frecuencia, fibra óptica, microondas, teléfono, entre otros; se emplean varios protocolos de comunicación tales como: DNP3 (Distributed Network Protocol versión 3), Modbus (Protocolo de comunicación serial basado en el modelo Maestro / Esclavo), IEC 60870-5-101 / 104 (norma internacional preparada para monitorizar sistemas de energía, sistemas de control y sus comunicaciones asociadas. El protocolo IEC -104 es la extensión del protocolo IEC-101), etc.

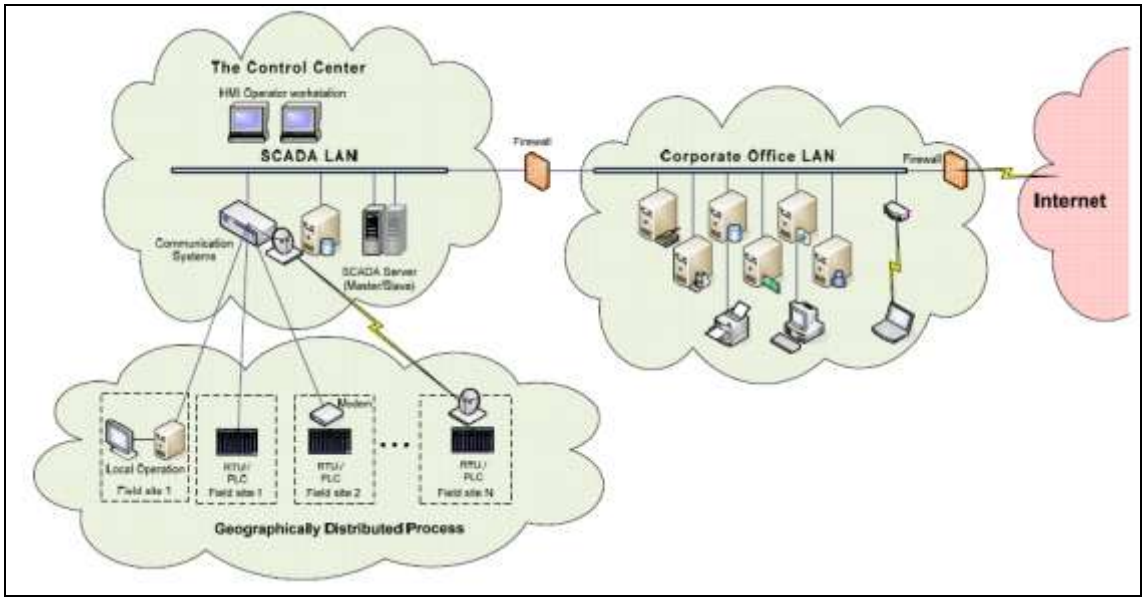

Figura 3.- *Esquema típico de una red SCADA.*
FUENTE Security Issues for SCADA Systems within Power Distribution.

En la figura 3. Se presenta un esquema típico de la disposición de una red SCADA. Como se puede apreciar son altamente distribuidos y sus elementos de control se encuentran geográficamente distantes del centro de operaciones.

Toda esta configuración involucra un trabajo arduo al momento de la implementación, en la que es posible no haber considerado apropiadamente la protección contra amenazas.

Al tratarse de sistemas dinámicos con el tiempo se expanden, por lo que se integran nuevos elementos haciendo cada vez más grande el sistema a monitorear y mantener, por lo tanto, se requiere que el personal encargado de su administración esté atento a su funcionamiento para evitar contratiempos en la operación al detectar alguna anomalía. Si un evento pone en riesgo la disponibilidad del sistema se necesita de acciones puntuales para regresar el sistema a la normalidad, para facilitar estas acciones se empieza a compartir los ambientes de la red corporativa con la de los sistemas SCADA con el fin de realizar asistencias remotas del

administrador en cualquier momento, dejando a un lado los principios de sistemas seguros esto debido a que se comparte el acceso a la red lo que

puede provocar el ingreso del malware o acceso a personal no autorizado si no se consideran procesos de autentificación, o si se comparten las claves al tratar de solventar una emergencia y luego no se la actualiza.

Se tiende a creer que en estos sistemas nadie puede interesarse; mucho menos imaginamos que podrían atacarlos al descubrir vulnerabilidades se estima que por manejar procesos poco conocidos no serán blanco de intromisiones, [6][10][21] este exceso de confianza puede ser perjudicial en sistemas que controlan y monitorean servicios ya que involucran perjuicio a la empresa y a los usuarios de dichos servicios inclusive pueden desembocar en un caos general al no comprender la causa de los fallos; a continuación describimos algunos aspectos que podrían convertirse en amenaza.[1]

Ignorancia.- Es posible que algunos de los Operadores del sistema o colaboradores de los departamentos de redes se inicien en el manejo de computadores y sin querer causar daño borren información valiosa o dejen abiertas puertas de acceso a terceros.

Venganza.- Puede ocurrir que algún empleado resentido ingrese a los sistemas a los cuales tiene acceso sin problema y provoque interrupción de servicios con la intención de perjudicar la producción.

Vanidad.- Un empleado experto puede tratar de vulnerar la seguridad de los sistemas con el afán de probar al resto su capacidad por vanagloria**.**

2.1 Seguridad en redes corporativas.

Si bien nuestro objetivo es el estudio de la seguridad de una red SCADA partiremos de la premisa que es una red de ordenadores interconectada

para compartir recursos con elementos similares a una red corporativa tales como servidores, switch, router, etc, por ello nos basaremos primero en ellas para analizar los potenciales ataques básicos a los que está expuesta y luego nos centraremos en los elementos más críticos de un sistema de Control y Adquisición de datos orientada a servicios.,

Según lo investigado en el libro de Redes de Computadoras, la seguridad de redes se puede dividir en estas áreas. [7]:

Confidencialidad.- Se encarga de mantener la información fuera del alcance de terceros o de personal no autorizado.

Autenticación.- Área que se enfoca en la confirmación de quién es el sujeto que solicita información antes de proporcionarla arbitrariamente; garantizando que es un elemento de confianza.

No repudio.- Se asegura que la información que se entregó es la solicitada, evitando que el solicitante niegue su petición o viceversa; garantiza a ambas partes el respaldo en caso de errores de interpretación

Control de integridad.- Ayuda a garantizar que el mensaje enviado no fue adulterado en su recorrido.

Por lo tanto, iniciaremos comentando que el bien más preciado en las organizaciones es la información, la misma que se almacena en servidores y es el resultado de varios procesos que se desarrollan gracias a los servicios que se ejecutan en los servidores, tornándose estos en los elementos sensibles para el correcto funcionamiento de las organizaciones.

2.2 Amenazas a una red corporativa

Las redes corporativas están expuestas a ataques los cuales pueden darse de varias maneras a continuación se presentan los más comunes resumidos en tres grupos. [1]

a.- ACCESO NO AUTORIZADO.

El acceso no autorizado se presenta cuando un equipo sin permisos consigue ingresar al entorno de red ya sea para interactuar con los dispositivos, para estar atento a la captura de claves de acceso o para eliminar información relevante.

Estos accesos pueden habilitarse por falta de precaución, un dispositivo puede estar conectado a la red y carecer de usuario y contraseña de ingreso, o tener habilitadas las claves por defecto, lo cual puede ser aprovechado por un intruso para ingresar al sistema.

Las redes de acceso Wi-Fi por lo regular son redes de acceso público con bajas restricciones de acceso por lo que se convierten en puertas de ingreso para personal propio o para particulares que buscan a través de sus dispositivos conectarse a una red, sea para ingresar a internet o para acceder a observar la red sin permisos asignados.

Como lo indica la bibliografía [1], los accesos no autorizados también pueden ser el fruto de operaciones más elaboradas como el empleo de software especializado para la escucha de tráfico en canales no seguros que permiten decodificar la información, una vez dentro de la red, el intruso con acceso a los servidores provocaría pérdida o robo de información importante o detendría procesos si el caso fuera perjudicar a la empresa.

b.- SUPLANTACION DE IDENTIDAD.

La suplantación de identidad se presenta cuando el intruso accede al sistema como un usuario más, esto debido a que hurtó una clave o usó alguna herramienta de escucha para presentar credenciales siguiendo el patrón de asignación de usuario y contraseña.

En ocasiones este tipo de ataques se presentan en entidades financieras, los intrusos acceden a las páginas de las financieras luego de emplear páginas de enlaces falsos donde los clientes proporcionan la información que ellos requieren para a efectuar sus fraudes dentro de los sistemas ingresando a los servicios a través de las páginas oficiales, actualmente se emplean mecanismos de cifrado para evitar estas intromisiones.

Es muy importante para evitar este tipo de ataque concientizar al personal que las claves de acceso deben ser memorizadas evitando en lo posible escribirlas en notas o en cuadernos cerca de los equipos, y de no ingresar información en páginas de internet a menos que exista la seguridad de que son confiables, así se evita poner en riesgo a la organización.

c.- DENEGACION DE SERVICIO.

Este tipo de ataque produce la interrupción de servicios, generalmente el atacante envía varias peticiones con el fin de saturar la red lo que provoca que el sistema responda en forma lenta, produciendo que varias peticiones se acumulen y llenando la memoria de paquetes innecesarios. En escenarios más críticos el ataque puede direccionarse a los elementos físicos produciendo daños más agresivos, podría darse el caso que se destruya el disco duro dejando los servidores inutilizados o se eliminen programas deteniendo procesos de producción.

Cuando el ataque se realiza desde varios equipos, esta amenaza se conoce como Denegación de Servicio Distribuido. Este método es aún más complejo

de solventar debido a que es difícil determinar de dónde proviene el ataque, por lo regular de varios usuarios que desconocen que son utilizados para este fin.

El ataque de Denegación de servicio DoS, causa la interrupción de uno o varios servicios mediante el uso excesivo de recursos en los servidores o elementos de red intermedios, pueden consumir ancho de banda, alterar los ciclos de cpu, limitar la memoria, alterar bases de datos.

Detectar ataques de DoS y Denegación de servicio Distribuido DDoS, no es tarea fácil, pero se pueden emplear acciones para minimizarlas.

- Monitorizar el tráfico en la red, revisión de tráfico por puerto esto se realiza con ayuda de software como TCPDUMP, Wireshark, es necesario revisar e tráfico encriptado para descartar ataques.
- Revisar el comportamiento habitual de la red permite obtener patrones de comportamiento de los clientes o direcciones IP. Permiten identificar comportamientos dudosos de peticiones no reales.
- Medición de rates, número de peticiones por cliente, tráfico generado por IP.
- Configurar equipos desactivar la fragmentación IP en el router con el fin de evitar vulnerar la seguridad del firewall.
- Limitar el número de conexiones por usuario.
- Aplicar políticas de calidad de servicio para flujos de tráfico.
- Minimizar los temporizadores de conexiones establecidas y de espera.
- Limitar el uso de recursos en sistemas compartidos.

El minimizar esto tipos de ataques a puesto a los fabricantes de dispositivos de red a trabajar para encontrar soluciones automáticas para asegurar el funcionamiento de los sistemas garantizando su funcionamiento procesando tráfico legítimo, se deben proteger los puntos extremos de la red para evitar

que se conviertan en elementos que envían mensajes empleando recursos de red como recomienda CISCO en su publicación "*Previniendo Ataques DDoS con Redes Cisco que Se Autodefienden*" [43]

Los sistemas automáticos de detección de estos ataques ayudan a minimizar los tiempos de respuesta de los sistemas ya que permiten identificar el ataque así mismo luego de detectado los uptimes de los

dispositivos mejoran pues se buscan alternativas de contingencias para superar el ataque entre ellas podemos citar:

- Realizar conexiones Bypass, si se determina que el ataque afecta a equipos intermedios de la red.
- Deshabilitar el servicio que está siendo atacado, esto en sistemas donde sea posible o corran otros servicios, donde se espera sacrificar ciertos clientes y no todos los de la empresa.

2.2.1 Mitigación.

Para contrarrestar en cierta forma estas amenazas existen configuraciones de red que además permiten ordenar los dispositivos de la red.

a. **VLAN (Red de área local virtual**).

Es una red que agrupa un conjunto de dispositivos de red de forma lógica, o por función consiguiendo que la información se conserve solo dentro del grupo de trabajo.

Las VLAN agrupan usuarios relacionados independientemente de las conexiones físicas a la red. [7]

Además la implementación de VLAN, permite:

- Mejorar la optimización del ancho de banda, al crear dominios de broadcast más pequeños.

- Realizar un balance de carga al determinar mejores rutas.
- Que la información no salga del entorno del grupo de trabajo.

El standard IEEE 802.1Q determina el formato para las tramas de Ethernet. [7], la cual indica que las conexiones entre vlan se configuran en los elementos de interconexión (switch), para ello se modificó la trama agregando los campos prioridad, CFI (Indicador de formato), e identificar de VLAN.

b. VPN (Red privada virtual).

Es una red privada construida dentro de una infraestructura de red pública, estas redes se emplean para conectar de forma remota y segura a usuarios con equipos instalados en las oficinas a través de enlaces como internet. La información que se transmite por la red privada virtual se encuentra protegidos de accesos no autorizados gracias a los niveles de seguridad que cumplen (IPsec, SSL).

Una VPN es una red superpuesta que se utiliza para proporcionar una medida de seguridad.[7],

c. ACL (Listas de Control de accesos).

Las ACL son listas de instrucciones que se aplican a una interfaz del router, para indicarle que tráfico está permitido y cual debe denegar, estas condiciones se basan en especificaciones como dirección origen, dirección destino, número de puerto, protocolo, etc.

El uso de ACL en materia de seguridad evita que ciertos equipos o hosts accedan a cierto dispositivo aun encontrándose instalados en la misma red.
Las ACL pueden clasificarse en:

ACL Estándar.- puede bloquear el tráfico de una red o de un host específico, puede permitir todo el tráfico de una red específica o denegar paquetes por protocolos.

ACL Extendidas.- son más versátiles. Verifican direcciones origen y destino de los paquetes, protocolos, números de puerto y otros parámetros específicos.

d.- Seguridad Perimetral.-

- Cortafuegos.- También conocidos por su nombre en Inglés, Firewall; son dispositivos o sistemas que tienen como objetivo evitar el ingreso de paquetes no autorizados a un ambiente de red estableciendo enlaces controlados elevando una pared de seguridad al perímetro. [36]

El cortafuegos establece un punto de resistencia que mantiene los usuarios no autorizados fuera de la red que protege, presenta protección ante ataques de suplantación de IP y enrutamiento. Permite supervisar sucesos relacionados con seguridad permitiendo implementar controles y alarmas.

Pueden emplear varias técnicas para controlar los accesos: [36]

- Control de Servicio .- el cortafuegos puede filtrar el tráfico en base a direcciones IP y número de puertos TCP. Con la integración de funciones de proxy recibe e interpreta las solicitudes de acceso antes de proporcionar el ingreso.
- Control de Dirección.- determina en qué dirección el cortafuegos puede iniciar las solicitudes de servicios particulares y en qué dirección se permite el ingreso a través del cortafuegos.
- Control de usuario.- Controla el acceso al servicio en función del usuario que solicita el ingreso, puede emplearse para usuarios internos y externos.
- Control de comportamiento.- Controla como se utilizan los servicios, por ejemplo el cortafuegos puede filtrar correo basura.

- Sistema de detección de Intrusiones (IDS).- Un sistema de detección de intrusiones es un sistema cuya misión en detectar y alertas sobre intento de intrusiones a un sistema o red. Se considera instrucción a toda actividad no autorizada o que no se espera que suceda en el normal funcionamiento de la red.

A diferencia de los cortafuegos que contienen aplicaciones para cumplir con reglas basadas en protocolos que limitan el acceso y pueden ser vulneradas al estar determinadas por direcciones, los IDS son capaces de detectar cuando un atacante intenta enmascarar tráfico.

Tipos de IDS.-

- HIDS (Host IDS).- Sistema de detección de intrusiones en el Host, se encuentra en un determinado host (servidor, Pc,), Monitoriza eventos analizando actividades con precisión determinando qué procesos y usuarios se encuentran relacionados con una actividad. Analizan información del sistema (ficheros, log, recursos, mensajes, etc), paquetes que entran y salen del host en busca de incidencias.
- NIDS (Net IDS).- Sistema de detección de intrusiones en la Red, capturan y analizan paquetes que viajan a lo largo de la configuración de la red en busca de actividades anormales, emplea un adaptador de red en modo promiscuo con el fin de pasar desapercibido.

- Protocolos de Transmisión Segura de Datos.- La transmisión segura de datos tiene como objetivo, encriptar la información, es decir, codificarla de manera que si es interceptada por un tercero sea ininteligible, y que además llegue a su destino conservando su integridad.

Entre los principales protocolos de transmisión segura de datos podemos mencionar SSL, TSL, WTSL.

SSL.- Secure Socket Layer, es un protocolo desarrollado a principio de los años 90, con el fin de proteger las conexiones entre clientes y servidores WEB, con el fin de que los datos confidenciales llegaran a los destinos correctos.

TLS.- Transport Layer Security, es una evolución del protocolo SSL 3.0, proporciona Ofrece conexión segura entre cliente y servidor por medio de un canal cifrado, es utilizado por aplicaciones con protocolos como HTTP, SMTP, IMAP y POP 3.

WTLS.- Wireless Transport Layer Security, pertenece a la familia de protocolos WAP (Wireless Application Protocol) para el acceso a las redes móviles, está basado en TLS, su principal diferencia se encuentra en el uso del ancho de banda que puede ser limitada.

El empleo de estos protocolos permite:

- evitar escuchas.
- evitar falsificación de identidad del remitente.
- mantener la integridad del mensaje
- mantener una comunicación segura
- intercambiar parámetros criptográficos entre diferentes aplicaciones
- emplear algoritmos de criptografía

Estos protocolos son ampliamente utilizados en comercio electrónico, especialmente en transacciones que involucran el pago con tarjetas de crédito.

e.- Antivirus.-

Son programas que tienen como propósito detectar y evitar la activación de los virus.

Los virus son programas que intervienen en el normal funcionamiento de los computadores causando problemas de hardware o del sistema operativo, suelen reproducirse fácilmente y son difíciles de detectar sin herramientas adecuadas.

Los antivirus comparan el código de los archivos con una base de datos que contiene códigos de virus descubiertos, por ello se recomienda su actualización permanente.

En los sistemas SCADA también se ha reportado casos de ataques por gusanos o virus como Slammer y Stuxnet, para combatir estos códigos maliciosos varias compañías desarrolladoras de antivirus han trabajado en conjunto con proveedores de sistemas SCADA para proporcionar protección sin comprometer su funcionamiento.

A continuación se describen varios antivirus que se encuentran disponibles:

McAfee.- Es un producto de la compañía de software especializada en seguridad informática Intel Security [37].

Para protección con sistemas de control industrial cuenta con el producto McAfee Security Connected, adicionalmente esta empresa se ha aliado [38] con la compañía Schneider Electric empresa especializada en soluciones de integración de sistemas industriales en las áreas de petróleo, agua, gas, redes eléctricas.

Esto permitirá a los clientes de Schneider Electric proteger sus sistemas de infraestructura crítica de código malicioso o malware sin comprometer su código propietario manteniendo el sistema operativo.

Kaspersky.- Es una empresa proveedora de protección de sistemas informáticos. Esta compañía también ha apostado por el desarrollo de soluciones para evitar infecciones de virus en sistemas de control industrial

es así que mantiene un convenio de cooperación con Microsoft para evitar la propagación del gusano Stuxnet. [39][40].

F-Secure.- Es otra reconocida compañía de seguridad informática, también ha dirigido sus investigaciones a proteger sistemas de código malicioso, esta

compañía ha registrado la propagación de malware HAVEX dirigido a sistema de control industrial [41], igualmente ofrece soluciones para combatir el gusano Stuxnet.

2.3 Seguridad en sistemas SCADA.

Los sistemas SCADA cada vez han ido ganando espacio es sistemas industriales y de complejidad, ya sea para control de semaforización, transporte de petróleo y, lo que es motivo de este estudio, en las empresas distribuidoras de Energía Eléctrica; es por ello que se van innovando para prestar mejores servicios.

Debido a esto la comunidad mundial se ha ido interesando en protegerlos es así que el Gobierno Español ha creado el INSTITUTO NACIONAL DE TECNOLOGIAS DE LA COMUNICACIÓN (INTECO) que ha publicado varios documentos referentes a la seguridad de la información y ha dedicado publicaciones para los entornos SCADA.[2]

En una de sus publicaciones INTECO hace referencia a los complejos procesos que manejan los SCADA, ya que de ellos depende la pronta solución de problemas en líneas de producción. Los SCADA reportan todas las anomalías a los centros de control minimizando tiempos de respuesta y presentando la información suficiente para el diagnóstico de los fallos. INTECO manifiesta que en ocasiones se descuidan los parámetros de seguridad al pensar que son sistemas en los que nadie se interesa y creer que es dominio de pocos conocer su funcionamiento. [3]

En el día a día el funcionamiento de las empresas se considera cotidiano y es normal creer que la organización marcha sin mayores contratiempos, pero a medida que estos sistemas van escalando es necesario considerar que existen amenazas que no percibimos tales como malos trabajadores que desean boicotear el trabajo de otros, empleados resentidos que desean perjudicar a la organización o subversivos que desean provocar daños a

gran escala., para el sistema que estamos analizando sería crítico que existiera una intromisión pues puede provocar una suspensión del suministro de energía no autorizada que involucre toda el área de concesión provocando paralizaciones en los procesos de producción ocasionando pérdidas económicas a la distribuidora, estás pérdidas también se presentan en comercios donde los refrigeradores o equipos de aire acondicionado dejan de funcionar, podría ocasionar caos en el tráfico al mantener apagados los semáforos por largos periodos de tiempo y si esto ocurriera en horario nocturno podría provocar un caos mayor tal como lo ocurrido con el apagón de varios estados de USA y Canadá en el año 2003 [14], en principio se especuló que se trataba de un atentado terrorista pero se concluyó oficialmente que se el fallo de debió a un problema en el sistema de control de la Central eléctrica del Niágara.

Centrándonos un poco más en la seguridad de los sistemas SCADA en Empresas de Distribución Eléctrica, es necesario prestar atención a los puntos vulnerables para evitar incidentes que afecten el adecuado funcionamiento de los elementos del sistema de potencia.

2.3.1 Principales Vulnerabilidades de los Sistemas SCADA.

Para determinar las diferencias entre red corporativa y Sistemas SCADA y poder determinar las vulnerabilidades, se hace una diferencia de prioridades entre Confidencialidad, Integridad y Disponibilidad CID, que existe entre las

redes corporativas y las redes SCADA como se indica en la siguiente Tabla.[9]

	Sistemas Corporativos	Sistemas SCADA
Confidencialidad	ALTA	BAJO
Integridad	ALTA	MEDIA
Disponibilidad	BAJO	ALTA

Tabla 1.- *Importancia de CID en Sistemas Corporativos y Sistemas SCADA*

En la tabla 1. Se puede apreciar que lo más relevante para los sistemas SCADA es la disponibilidad del servicio, contrariamente a lo indicado para una red corporativa en la que prima la confidencialidad e integridad de la información.

Las vulnerabilidades en un sistema SCADA pueden ser tanto físicas como lógicas, a continuación se detallan algunas:

- **Concientización del personal.-** Estos sistemas operan continuamente su disponibilidad es de 24 horas al día, por lo cual, el personal que labora en los centros de control es rotativo y generalmente esta mentalizado en que el sistema debe estar operativo y funcional permanentemente, no tienen una conciencia sobre la seguridad que se debe mantener para evitar intrusiones, sin proponerse pueden brindar información confidencial acerca del sistema. Sin malas intenciones pueden contaminar la red con software malicioso como virus al tener acceso a las consolas de operación o administración.

- **Conexión a Redes Corporativas.-** En principio, por la importancia de los procesos, los sistemas SCADA se implementaban como sistemas de red aislados, limitados en accesos sólo el personal que lo operaba tenía permiso de ingresar a obtener datos de las consolas de operación o de gestión de servidores. Con el tiempo estos sistemas

se han ido renovando presentando mejores atributos de operación, de respaldo de históricos, etc., esto intrínsecamente conlleva a que más

personas intervengan en sus procesos o requieran información en tiempo real del sistema, por ejemplo, para elaboración de reportes; por lo que se van abriendo los accesos a la red corporativa. El principal riesgo al que se exponen es a la intromisión de virus o troyanos ya que la red corporativa tiene acceso a internet.

- **Conexión Remota.-** Debido a las prestaciones y a la disponibilidad del sistema se considera que al presentarse un evento inesperado el Administrador de la red debe auxiliar al Operador del sistema para mantener la continuidad del servicio, como se ha dicho antes estos sistemas operan permanentemente por ello las novedades pueden presentarse en horarios no laborables (para el personal de jornada normal), y para comodidad del personal que los gestiona se habilitan accesos remotos para solventar dichas emergencias.

El nexo a Internet puede permitir el acceso remoto del Administrador de la red para solventar problemas en cualquier momento, con las consecuentes vulnerabilidades.

- **Vulnerabilidades en el código de aplicaciones OWASP**.- El Proyecto Abierto de Seguridad en Aplicaciones Web (OWASP por sus siglas en inglés). [30], es una herramienta libre que permite optimizar la seguridad de los sistemas, está dirigida a todos los interesados en aplicar pruebas para determinar vulnerabilidades.

  La publicación [30], OWASP TOP 10- 2013, Presenta los Diez Riesgos de Seguridad en Aplicaciones, los cuales se presentan a continuación identificando los posibles agentes de ataque.

- **A1 Inyección**.- Considera a cualquiera que pueda enviar información no confiable al sistema, incluye usuarios internos y externos de la organización y personal de administración.

- **A2 Pérdida de autenticación y Gestión de Sesiones.-** Considera atacantes anónimos externos, a usuarios que intenten robar cuentas de otros, trabajadores que ocultan sus acciones.
- **A3 Secuencia de Comandos en sitios cruzados.**- Considera que el atacante puede enviar cadenas de texto que son secuencia de comandos de ataque.
- **A4 Referencia Directa Insegura a Objetos.-** Se debe considerar los tipos de usuarios o privilegios, se debe analizar si los usuarios tienen acceso parcial al sistema.
- **A5 Configuración de Seguridad Incorrecta.-** Considera atacantes anónimos externos así como usuarios con sus propias cuentas que pueden atacar accediendo a cuentas por defecto, archivos sin protección, para obtener acceso no autorizado.
- **A6 Exposición de Datos Sensibles.-** Los ataques pueden producirse por robo de claves, accediendo a datos sensibles o a sus respaldos.
- **A7 Ausencia de Control de Acceso a Funciones.-** Cualquiera con acceso a la red puede enviar peticiones a la aplicación, un usuario normal puede acceder a una función con privilegios.
- **A8 Falsificación de Peticiones en Sitios Cruzados.-** Se debe considerar si cualquier persona puede cargar contenido en los navegadores de los usuarios.
- **A9 Utilización de Componentes con Vulnerabilidades Conocidas.-** Componentes vulnerables pueden ser identificados y explotados con herramientas automatizadas, el atacante puede identificar componentes débiles a través de escaneos automáticos o análisis manuales.
- **A10 Redirecciones y Envíos no válidos.-** El atacante puede crear enlaces a redirecciones no validadas y engañar para que se utilicen esos enlaces. el atacante tienen como objetivos

2.3.2 Políticas de Seguridad en Sistemas SCADA.

Entre las principales políticas de seguridad para estos sistemas, en varias publicaciones: ***Diseño de seguridad de redes*** [1], ***Gestión Segura de Redes SCADA*** [6], recomiendan las siguientes:

Actualizar frecuentemente las credenciales o claves de acceso a los sistemas, bloquear las cuentas que sobrepasen un número determinado de intentos fallidos, emplear mecanismos de encriptado para proteger los accesos al sistema.

Se debe considerar además:

- Para la protección de datos se debe determinar quienes tendrán acceso a monitorear en tiempo real o en los históricos los datos, y cómo se realizará el repositorio para que estén disponibles si se los requiere analizar luego de algún tiempo [6].

- La configuración del hardware y el software para evitar el ingreso de virus, además se debe incrementar el control de accesos con métodos de autenticación, se tiene que evitar el uso de contraseñas cortas o por defecto [6].

- La seguridad en las comunicaciones en un aspecto que no suele considerarse en los modelos de sistemas distribuidos, en el caso de las empresas distribuidoras al tener sus subestaciones dispersas las comunicaciones se realizan a través de varios medios entre ellos radio enlaces, satélites, fibra óptica entre otros; que permiten la interacción remota [6].

- La capacitación al personal sobre el manejo del sistema para monitoreo y control; preparación para operación manual emergente en caso de que el sistema colapse.

- La seguridad física hacia los cuartos de equipos o servidores, se debe controlar los accesos para evitar intrusiones de personal con malas intenciones, así también el ingreso hacia la sala de control u operación permitiendo que sólo el personal encargado del sistema tenga privilegios de ingreso con tareas específicas.

Estos parámetros los resume el estudio de la Universidad de Málaga: Gestión Segura de Redes SCADA [6].

Dentro del marco de las políticas de seguridad se debe considerar el comportamiento en planes de contingencia, por ejemplo, cómo levantar el sistema SCADA en situaciones fortuitas en el menor tiempo posible, para ello, se debe respaldar el proyecto en copias de seguridad y asignar el personal responsable de ejecutar la acción así como el registro de los eventos que dieron lugar al colapso para su posterior análisis y tomar las acciones correctivas para evitar que ocurra nuevamente.

2.4 Hacking ético.

En la investigación “Gestión Segura de Redes SCADA” [6] manifiesta:

> *“La monitorización de recursos proporciona un mecanismo que puede ayudar a detectar un comportamiento anómalo o prever un posible fallo del sistema ocasionado por una intrusión. Una sobrecarga injustificada del procesador, un incremento anómalo del tráfico de red y la disminución drástica de la memoria libre o del espacio de disco disponible pueden ser síntomas, entre otros, de que el sistema está siendo atacado o bien se está empleando para atacar otros sistemas. Además, es conveniente emplear soluciones de auditoría de sistemas en los equipos pertenecientes a la red SCADA. De esta forma es posible rastrear las acciones realizadas en un equipo para descubrir tantas evidencias de ataques cómo el alcance de estos ataques en su entorno*.” Departamento de Lenguajes y Ciencias de la Computación, Universidad de Málaga

Esta breve introducción nos permite tener una idea de la actividad de hacking ético que se debe realizar en los sistemas SCADA.

El término hacker se asocia con un experto en informática que emplea técnicas para ingresar a una red a la que habitualmente no tiene permiso ya sea por curiosidad, por vanidad o con intenciones maliciosas.

Estas técnicas han llevado a clasificar a los hacker en varios grupos entre ellos los siguientes.

- Hacker de sombrero Blanco.
- Hacker de sombrero Negro.
- Hacker de sombrero Gris.

Hacker de Sombrero Blanco:- Son expertos informáticos que buscan vulnerabilidades en su propia red por medio de análisis y pruebas con el fin de encontrar puntos sensibles y corregirlos para mejorar su estructura de información y comunicación.

Hacker de Sombrero Negro:- Son expertos informáticos que buscan vulnerabilidades en redes de comunicación e información para sabotear estos sistemas ya sea por robo de información o intrusión de archivos dañinos como virus o troyanos que causen daño a la red.

Hacker de Sombrero Gris:- Se encuentran en el centro de la definición de los dos anteriores, son expertos informáticos que buscan vulnerabilidades en la red con el fin de encontrar puntos sensibles y comunicar al Administrador de la red ofreciéndose a corregirlos o recibir una recompensa por su información.

El Hacker de sombrero blanco se enmarca en el concepto del hacking ético, pues es el encargado de realizar el análisis, prueba y corrección de vulnerabilidades en el entorno de red que se quiere proteger, la finalidad es

adelantarse a un hacker de sombrero negro que tenga malas intenciones por ello este tipo de hacking ético se realiza con personal especializado en seguridad informática.

2.5 Analizador de protocolos.

Los analizadores de protocolos o Sniffer, son aplicaciones que permiten capturar los paquetes en un proceso de comunicación para entender mejor su comportamiento.

Un sniffer ejecuta tres fases:

- Captura: Realiza la recolección de paquetes.
- Conversión: Se toman los datos binarios y se les da formato para facilitar su lectura.
- Análisis: Se analiza la información obtenida. [9]

Las aplicaciones Sniffer se pueden emplear para:

- Captura automática de contraseñas enviadas en claro y nombres de usuario de la red.
- Conversión del tráfico de red en un formato inteligible por los humanos.
- Análisis de fallos.
- Medición del tráfico, mediante el cual es posible descubrir cuellos de botella en algún lugar de la red.
- Detección de intrusos. [10]

Existen varios analizadores de protocolos unos de código libre y otros licenciados, algunos poseen un número limitado de protocolos, la mayoría presentan interfaces amigables con el usuario.

En la tabla 2 se presenta información acerca de algunos analizadores de protocolos de uso libre.

Analizador de Protocolo	Desarrollador	Última versión	URL
WIRESHARK.	The Wireshark Team	1.12.2	http://www.wireshark.org/
TCPDUMP	Open Source	4.6.2 / 1.6.2	http://www.tcpdump.org/
DARKSTAT	Emil Mikulic	3.0.719	http://unix4lyfe.org/git/darkstat
TRAFFIC – VIS	Damien Miller	0.35	http://www.ilogic.com.au/~dmiller/traffic-vis.html
SNORT	Martin Roesch, Sourcefire, Inc.	2.9.7.0	https://www.snort.org
ETTERCAP		0.8.2	http://ettercap.github.io/ettercap

Tabla 2.- *Información de analizadores de protocolos.*

2.6National Institute of Standards and Technology NIST Información General.

El National Institute of Standards and Technology (NIST) es una agencia federal no regulada perteneciente al Departamento de Comercio Exterior de Estados Unidos cuya misión es promover la innovación y la competitividad industrial en base a normas y tecnología para mejorar la estabilidad económica y la calidad de vida.[21].

2.6.1 National Institute of Standards and Technology NIST 800-82.

La Publicación Especial 800-82, titulada Guide to Industrial Control System (ICS) Security, identifica amenazas y vulnerabilidades típicas de los sistemas de control industrial y provee recomendaciones para mitigar riesgos.

2.6.1.1.- Amenazas de Sistemas de Control Industrial.

Las amenazas pueden clasificarse en:

- Adversarios.
- Accidentales
- Estructurales.
- Ambientales.

a. Adversarios.-

La información que se almacena en el sistema puede ser requerida por cualquier individuo y dejar intencionalmente el equipo expuesto ya sea a un miembro externo a la organización, a un empleado de otro departamento, a un proveedor de equipos, a un competidor. La exposición se produce al ocupar las herramientas tecnológicas como Pendrives, compartir recursos, enviar información por correo.

b. Accidentales.-

Se presentan por acciones erróneas que realizan los usuarios en la ejecución de sus actividades diarias ya sea con su acceso limitado o con privilegios de Administrador.

c. Estructurales.-

Los equipos pueden fallar o deteriorase, se puede presentar una falla en el equipo que regula la ventilación en el cuarto de servidores, Software sin mantenimiento debido al tiempo de funcionamiento, situaciones que no se tienen previstas pero que pueden presentarse por agotamiento de los dispositivos como saturación de memoria.

d. Ambientales.-

Desastres naturales o provocados por el hombre, fuego, inundaciones, terremotos, bombardeos, falla en el respaldo de energía, falla en el sistema de comunicaciones.

2.6.1.2 .- Vulnerabilidades en Sistemas de Control Industrial.

El NIST recomienda considerar la siguiente clasificación de vulnerabilidades.

- De Políticas y Procedimientos.
- De Arquitectura y Diseño.
- De Configuración y Mantenimiento.
- Físicas.
- De desarrollo de Software.
- De comunicaciones y redes.

Para un mejor análisis de esta clasificación, las tablas de esta publicación se indican en el ANEXO A.

2.6.2 National Institute of Standards and Technology NIST 800-53.

La publicación NIST 800-53 titulada Security and Privacy Controls for Federal Information Systems and Organizations,[41] ofrece un catálogo de políticas de control y privacidad de información para los sistemas federales y organizaciones además un proceso para proteger las operaciones de la organizaciones contra cyber ataques, desastres naturales, fallas estructurales y errores humanos.

Está publicación enfatiza que la seguridad es un aspecto que toda organización debe considerar para garantizar un funcionamiento adecuado de los bienes y servicios.

Recomienda una evaluación permanente de posibles amenazas y vulnerabilidades a fin de tomar medidas correctivas para evitar consecuencias graves.

2.7 Normas de seguridad

2.7.1 ISO 17799.

Es una norma Internacional que ofrece recomendaciones para la gestión de seguridad de la información, dirigida a los responsables de mantener e implementar sistemas, para ello considera los siguientes factores de éxito:

Factores de éxito críticos. [42]

a) política, objetivos y actividades de seguridad de información que reflejan los objetivos comerciales.

b) un enfoque y marco referencial para implementar, mantener, monitorear y mejorar la seguridad de la información que sea consistente con la cultura organizacional.

c) soporte visible y compromiso de todos los niveles de gestión.

d) un buen entendimiento de los requerimientos de seguridad de la información, evaluación del riesgo y gestión del riesgo.

e) marketing efectivo de la seguridad de la información con todo los gerentes, empleados y otras partes para lograr conciencia sobre el tema.

f) distribución de lineamientos sobre la política y los estándares de seguridad de la información para todos los gerentes, empleados y otras partes involucradas.

g) provisión para el financiamiento de las actividades de gestión de la seguridad de la información.

h) proveer el conocimiento, capacitación y educación apropiados.

i) establecer un proceso de gestión de incidentes de seguridad de la información.

j) implementación de un sistema de medición que se utiliza para evaluar el desempeño en la gestión de la seguridad de la información y retroalimentación de sugerencias para el mejoramiento.

Basados en estos factores la Norma recomienda considerar 11 dominios para la gestión de seguridad.

1.-Política de seguridad.- Dirigir y dar soporte a la gestión de la seguridad de la información.

2.-Aspectos organizativos para la seguridad.- Gestión dentro de la organización, manejo de recursos, activos.

3.- Clasificación y control de activos.- tener un inventario de los recursos de la información y asegurar que se brinde un nivel adecuado de protección.

4.-Seguridad de recursos humanos.-capacitar e informar a los empleados actuales y potenciales en materia de seguridad y de asuntos de confidencialidad, para evitar errores humanos o mal uso de recursos.

5.-Seguridad física y del entorno.-protección de áreas, evitando accesos no autorizados que puedan provocar daños a las instalaciones o datos.

6.-Gestion de comunicaciones y operaciones.-instalación de un software o sistema seguro y protegido contra amenazas.

7.-Control de accesos.- Evitar accesos no autorizados a la red.

8.-Adquisicion desarrollo y mantenimiento de los sistemas.- mantener la seguridad mediante el uso de controles de seguridad, evitando pérdidas o modificaciones.

9.-Gestion de incidentes de la seguridad de la información.- Comunicar eventos y debilidades que afecten al sistema de manera rápida a fin de tomar medidas correctivas en el menor tiempo.

10.-Gestion de continuidad del negocio.- Reaccionar a la interrupción de actividades de la empresa y proteger los procesos críticos frente a fallas, ataques o desastres.

11.-Cumplimiento.- Gestionar la seguridad de la información de conforme con la legislación vigente, evitando incumplimiento de leyes, regulaciones, obligaciones y otros requisitos de seguridad..

2.7.2 ISO 27000.

La norma ISO 27000, es la norma para la Gestión Segura de la Información se fundamenta en Planificar, Hacer, Verificar, Actuar, también conocido como el proceso de mejora continua, sus siglas en inglés PDCA, como se ilustra en la siguiente gráfica.

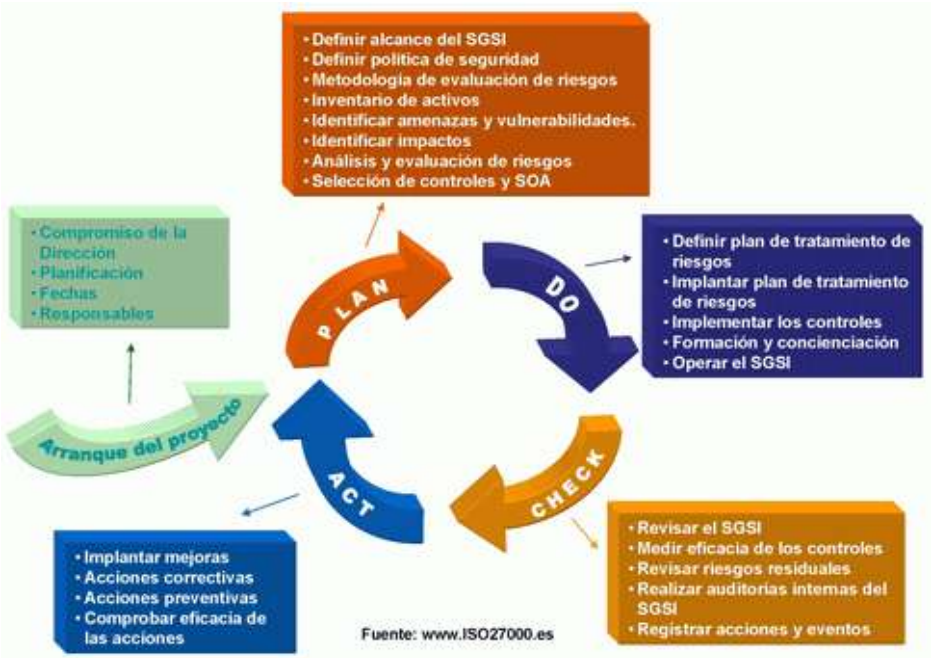

Figura 4.- *Modelo de aplicación de la Norma ISO 27000. FUENTE ISO 27000.*

Esta guía presenta un resumen de lo que implica cada una de sus etapas, a continuación se detallan.

Arranque del proyecto.-

En la etapa de arranque se debe tener claro los objetivos y se debe contar con el compromiso de los dirigentes de la organización a fin de dar continuidad al proceso para lograr el objetivo planteado, es de considerar que esta propuesta no va a ser una solución definitiva pero va a permitir minimizar los riesgos.

Se debe organizar un plan determinando responsables para llevar el seguimiento y fijándose fechas para su desarrollo.

Planificación.-

En esta etapa se determina el alcance del proyecto. Se deben definir las políticas de seguridad basadas en la actividad de la empresa y en la legislación que la rige partiendo de la identificación de vulnerabilidades y amenazas que afecten el entorno de red considerando los impactos que provocaría la pérdida de confidencialidad o disponibilidad de la información.

Implementación.-

En esta etapa se tiene que definir el plan de tratamiento del riesgo que identifique las acciones a tomar para luego implementarlas en base a los objetivos de la planificación; capacitación al personal en lo referente a seguridad de la información.

Se debe establecer normas y procedimientos además instrucciones para detección y acciones a seguir en caso de incidentes de seguridad.

Seguimiento.-

En esta etapa se realizan las pruebas ejecutando los procedimientos para revisión de su efectividad analizando los resultados para comprobar si el objetivo se está cumpliendo, es una etapa muy necesaria pues ayuda a

identificar si existen falencias en los procedimientos para tomar las acciones correctivas.

También es la etapa que alerta sobre los cambios que se dan a lo interno de la organización y si se está cumpliendo con la norma ISO 27001, para determinar mejoras a los procedimientos de SGSI.

Mejora Continua.-

En esta fase se ponen en marcha todas las mejoras que se recomiendan en la fase anterior, sean estas acciones correctivas o preventivas, para alcanzar el objetivo planteado además se encarga de socializar las variantes a todos los niveles de la organización.

La seguridad es un proceso que implica el compromiso de todos en la organización, incluida la dirigencia es importante la concientización de los colaboradores en busca de disminuir las vulnerabilidades; mejorar la configuración de seguridad es un proceso continuo pues no existe un nivel de seguridad absoluto.

Beneficios del empleo de esta norma:

• Establecimiento de una metodología de gestión de la seguridad clara y estructurada.

• Reducción del riesgo de pérdida, robo o corrupción de información.

• Los riesgos y sus controles son continuamente revisados.

• Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.

• Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.

• Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001L).

• Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.

• Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.

• Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.

• Confianza y reglas claras para las personas de la organización.

• Reducción de costes y mejora de los procesos y servicio.

• Aumento de la motivación y satisfacción del personal.

• Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

Toda la información acerca de esta norma se ha tomado de una publicación genérica oficiala la que se puede acceder a través del link: *www.iso2700.es*

2.7.3 COBIT.

Los Objetivos de Control para la Información y la Tecnología relacionada COBIT. es una guía de mejores prácticas dirigida al control y supervisión de tecnología de la información, mantenido por ISACA (Asociación de Auditoría y Control de Sistemas de Información), organización internacional que apoya y patrocina el desarrollo de metodologías y certificaciones de auditorías y control en sistemas de información. Ayuda a crear o mantener valores óptimos de tecnológicas de información, manteniendo un balance entre los beneficios, riesgos y recursos.

Existen varias versiones de COBIT la que citaremos es la COBIT 5 publicada en el 2012. [44]

Los cinco principios de COBIT 5 son:

- **Satisfacer las necesidades de los interesados.-** Dado que toda empresa tiene objetivos diferentes, se puede personalizar COBIT 5 para adaptarlo a su propio contexto mediante metas, traduciendo metas corporativas de alto nivel en otras metas más manejables, especificas, relacionadas con TI.

- **Cubrir la empresa de extremo a extremo.-** Integra el gobierno y la gestión de TI en el gobierno corporativo.

  + Cubre las funciones y procesos dentro de la empresa COBIT 5, no se enfoca sólo en la "función TI", sino que trata la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la empresa.
  + Considera que los catalizadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin, incluyendo a todos internos y externos que sean relevantes para el gobierno y la gestión de la información de la empresa.

- **Aplicar un solo marco integrado.-** existen estándares y buenas prácticas relativas a TI, ofreciendo cada uno ayuda para un subgrupo de actividades de TI. COBIT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las TI de la empresa.

- **Hacer posible un enfoque holístico.-** Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. COBIT 5 define un conjunto de catalizadores para apoyar la implementación de un sistema de gobierno y gestión global para las IT de la empresa. Define siete categorías.

- Principios, Políticos y Marcos de Trabajo.
- Procesos.
- Estructuras Organizativas.
- Cultura, Ética, y Comportamiento
- Información.
- Servicios, Infraestructuras y Aplicaciones.
- Personas, Habilidades y Competencias.

- **Separar el gobierno de la gestión.-** El marco de trabajo COBIT 5 establece una clara distinción entre gobierno y gestión, ya que tienen diferentes actividades, requieren diferentes estructuras organizativas.

  + Gobierno.- Asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas; estableciendo la dirección y la toma de decisiones; midiendo el rendimiento y el cumplimiento.

  + Gestión.- Planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzarla metas empresariales.

2.8 NAS (Network Attached Storage).

Un NAS es un servidor separado que tiene su propio sistema operativo y un software de configuración, posee su propio sistema de archivos que aloja al sistema operativo, también una serie de discos independientes que se utilizan para alojar los datos que se van a guardar.

Estos sistemas constan de tres elementos procesador, unidades físicas de almacenamiento y módulo de conexión de red. [24]

Los beneficios del empleo de NAS según proveedor D-LINK son:

+ Permite compartir los dispositivos y recursos de almacenamiento entre múltiples clientes y tipos de sistemas informáticos a través de la red LAN.
+ Proporciona una solución de bajo costo, sencilla de gestionar.
+ Buen nivel de escalabilidad.

2.9 RFC 1244 (Request for comments).

RFC Request for Comments, Petición de comentarios son publicaciones del grupo de ingeniería de Internet IETF, que describen varios aspectos del funcionamiento de internet y otras redes de computadoras. Cada RFC constituye un monográfico o memorando que ingenieros o expertos en la materia han hecho llegar al grupo de ingeniería de Internet (IETF), para que éste sea valorado por el resto de la comunidad. Cada RFC tiene un título y un número asignado. [25]

El RFC 1244 es una guía para el establecimiento de políticas y procedimientos de seguridad informática. Esta guía enumera los problemas y factores que un sitio debe tener en cuenta al establecer sus propias políticas. [26]

2.10 Test de Penetración y análisis de vulnerabilidades.

Los Test de penetración permiten evaluar las vulnerabilidades de los sistemas de control industrial. El objetivo de los test de penetración es comprobar cuan difícil resulta el ingreso a los sistemas, simulando ataques desde el exterior y desde la propia institución, para lograr encontrar vulnerabilidades que pongan en riesgo los sistemas; estas pruebas se realizan de común acuerdo con los administradores de los sistemas SCADA o de control Industrial

Entre las vulnerabilidades comunes se puede mencionar [31]:

- Fallas en el software.
- Configuraciones inapropiadas
- Operación ineficiente.
- Factor Humano

Antes de realizar estas pruebas se debe iniciar con la recopilación de información sobre el objetivo de ataque, se debe identificar los posibles puntos de ingreso y llevar un registro detallado de los resultados.

Las pruebas de penetración pueden ser [32]:

- Pruebas de penetración con objetivo.- Buscan vulnerabilidades en partes específicas de los sistemas.

- Pruebas de penetración sin objetivo.- Examinan la totalidad de los componentes de los sistemas.

- Pruebas de penetración a ciegas.- Se realizan con información pública de la empresa.

- Pruebas de penetración informadas.- Se emplea información privada de la empresa, simulan ataques desde adentro de la institución.

- Pruebas de penetración externas.- Se ejecutan desde lugares externos a las instalaciones de la empresa, evalúan las seguridades perimetrales.

- Pruebas de penetración internas.- permiten evaluar desde dentro de la institución políticas y mecanismos internos.

Al término de cada prueba se debe elaborar un reporte y al concluir con las pruebas se presentarán los resultados, los cuales determinaran las medidas correctivas a tomar, ya que no existe seguridad total.

2.11 Control de Acceso Físico a las Instalaciones.

Los controles de acceso físico a las instalaciones de las empresas y a los puntos críticos como centros de control y cuarto de equipos son importantes para evitar manipulaciones mal intencionadas de los equipos o robo de información. Las puertas que restringen el acceso deben ser resistentes al fuego, ser robustas para evitar sabotajes o intentos de ingreso forzados, suelen contar con cerraduras magnéticas, llaves especiales con código, o controles biométricos.

Los controles de acceso tienen como objetivo evitar el acceso no autorizado garantizando con ello el funcionamiento del cuarto de equipos y centro de control, por ello deben restringirse y documentarse.

Los accesos físicos pueden administrarse por medio de políticas basadas en la norma ISO 27002, apartado Seguridad Física y del Entorno. [45].

Estas políticas de controles de accesos se aplican a todo el personal que solicita el ingreso sea a los cuartos que almacenan los servidores y a los centros de control desde donde se monitorean los sistemas, pertenezcan directamente al área de telecomunicaciones, al personal administrativo, personal de otras empresas que mantengan convenios con la institución o presten servicios.

CAPITULO III

3. RED SCADA LOCAL DE LA EERSSA

3.1.- Descripción de la arquitectura de la red SCADA Local de la EERSSA.

La red del sistema SCADA de la EERSSA está conformada por tres sistemas:

- Sistema de Vigilancia (Lenel OnGuard).
- Sistema de Gestión de Comunicaciones (What´s Up Gold).
- Sistema SCADA (PowerLink Advantage GE).

3.1.1 Sistema de Vigilancia.

El sistema de vigilancia trabaja sobre la plataforma Lenel OnGuard, la cual presenta soluciones de seguridad al integrar controles de acceso y gestión de video.

Tanto en el Centro de Control como en las Subestaciones se tiene integrado los siguientes equipos en el sistema de Vigilancia:

- Cámaras PTZ IP, para exteriores.
- Cámaras Fijas IP, para interiores.
- LNVR Grabador de video
- Panel de control de Accesos.
  - Sensores de movimiento
  - Sensores de humo
  - Cerraduras magnéticas
  - Lectoras de tarjetas
  - Tarjetas de accesos

Figura 5.- *Equipos del sistema de Vigilancia.*
FUENTE Centro de Control EERSSA

A través del puerto de red estos dispositivos se conectan al switch de la subestación reportando los eventos al servidor instalado en el cuarto de servidores desde donde se realiza la gestión de vigilancia como el ingreso de nuevos dispositivos, en el Centro de Control se dispone de un cliente para el monitoreo de las cámaras y el control de accesos.

Figura 6.- *Monitoreo del sistema de Vigilancia.*
FUENTE Centro de Control EERSSA

3.1.2 Sistema de Comunicaciones.

Debido a que las subestaciones se encuentran distantes del Centro de Control, distribuidas en el área de concesión se estableció un sistema de monitoreo por radios de modulación digital de banda ancha con comunicación punto a punto.

Los elementos de este sistema son:

- Radios.
- Switchs Capa 3.
- Antenas
- Unidades de respaldo de energía (UPS´s).

Existen enlaces con respaldo de fibra óptica gracias a un convenio interinstitucional entre la EERSSA y TRANSELECTRIC, el canal de fibra se establece como principal y el de radio como respaldo backup.

Para administrar este sistema desde el Centro de Control se emplea el Software de Gestión What´s Up Gold.

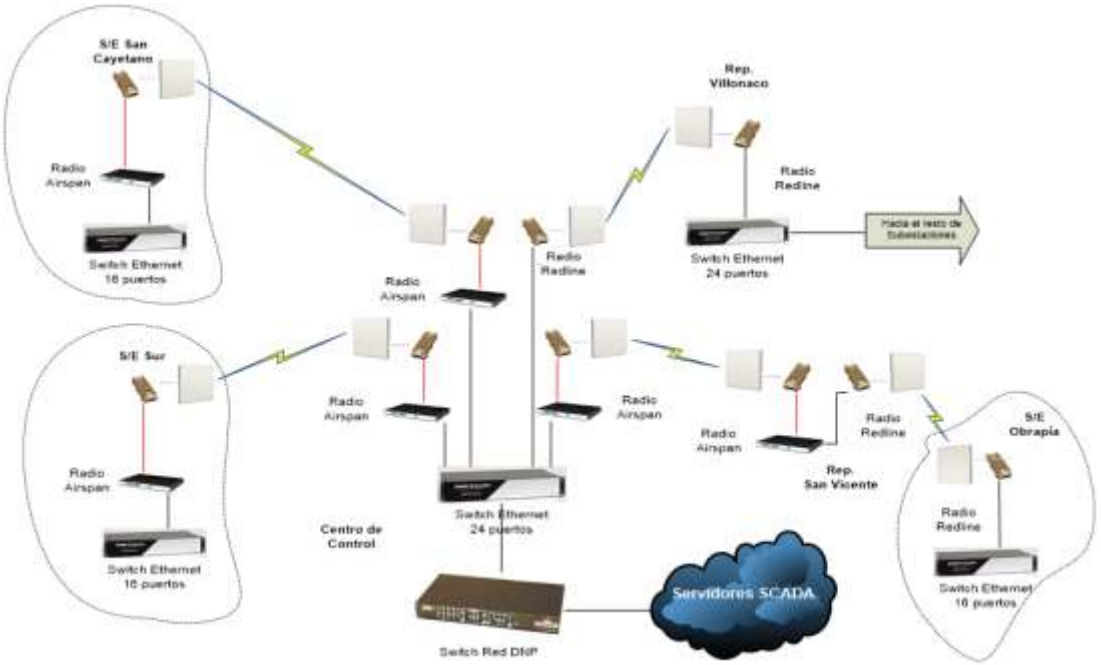

Figura 7.- *Esquema de Equipos que se emplean en la red de Comunicaciones del Sistema SCADA de la EERSSA. FUENTE EERSSA*

3.1.3 Sistema SCADA Local (PLA).

El sistema de monitoreo y control del SCADA Local de la EERSSA está compuesto por:

- Servidor Principal
- Servidor de Respaldo
- Servidor de Históricos
- GPS
- Grabador de cintas
- Switch de comunicaciones

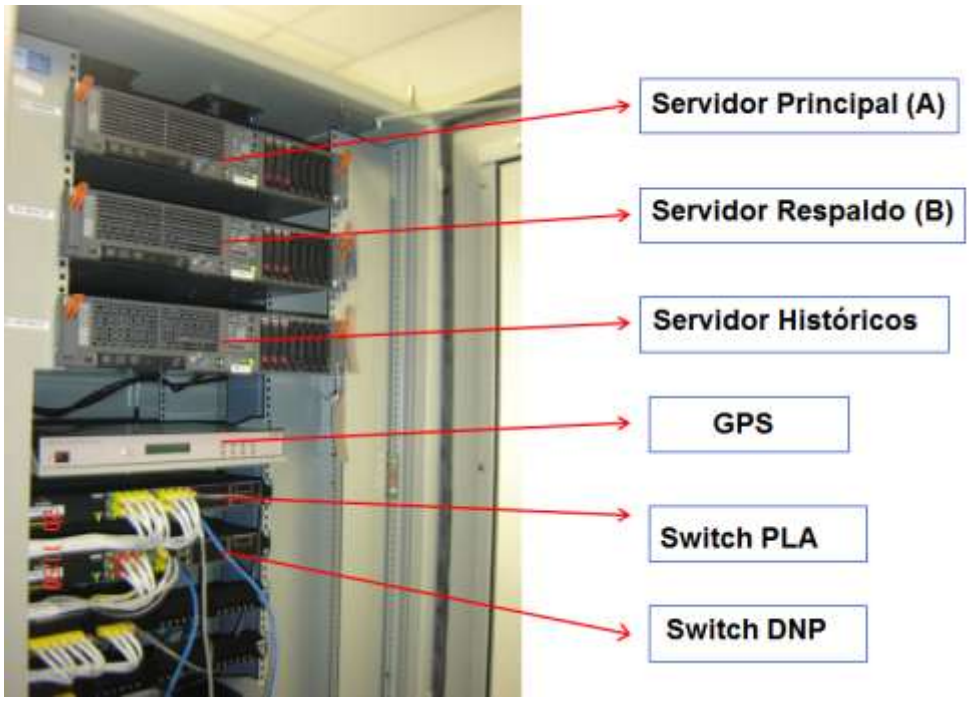

Figura 8.- *Rack del Sistema SCADA de la EERSSA.*
FUENTE Centro de Control EERSSA

Los servidores: principal y respaldo trabajan en modo Hot-Standby, en el Centro de Control se tienen instalados los clientes denominados Estación de Operación (EST 1) y Estación de Proyección (Proy).

Al servidor de históricos se lo gestiona desde el Centro de Control.

El cuarto de servidores se encuentra cerca del Centro de Control, las instalaciones están compartidas con el departamento de Sistemas, existen instalados 2 Racks para el sistema SCADA, el primero contiene los servidores del PLA y el segundo almacena los equipos de comunicaciones y vigilancia.

Para sincronizar los dispositivos a la misma estampa de tiempo se dispone de un GPS el cual envía comandos de sincronismo a los servidores. estos replican el comando hacia las remotas y estás a los equipos aguas abajo; los grabadores de video se sincronizan a través de líneas de comandos a uno de los servidores.

En las subestaciones se encuentran instaladas las RTU que concentran la información y reportan hacia el software SCADA instalado en los servidores, a través de protocolo DNP 3.0

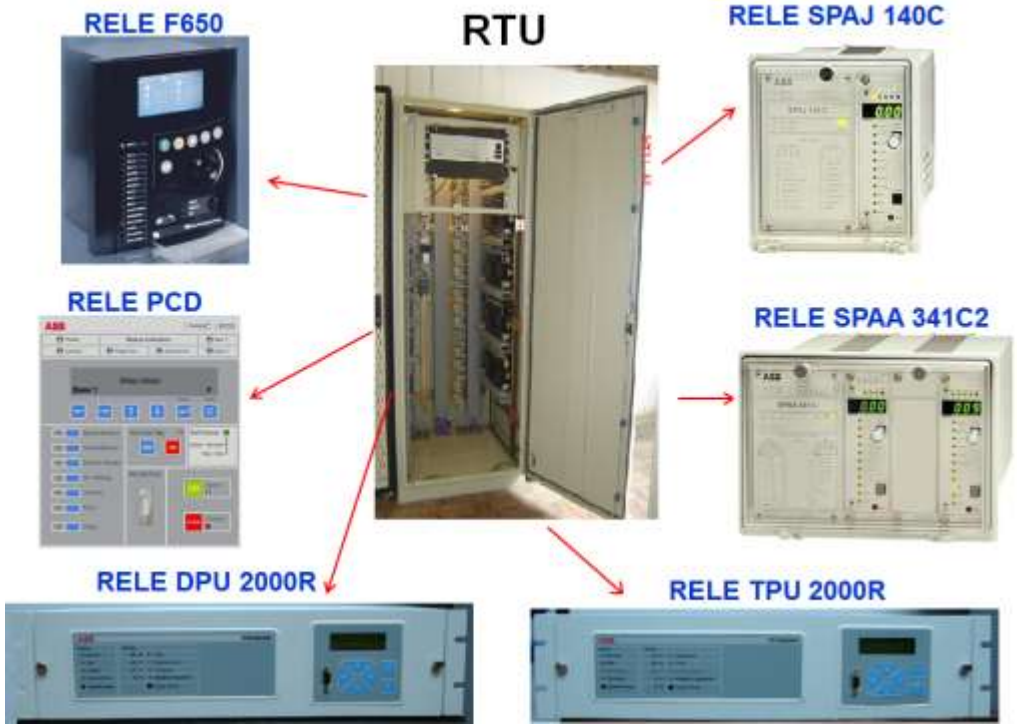

Figura 9.- *RTU instalada en las Subestaciones, parte de los relés que se encuentran integrados al SCADA.*

En esta red también se integran la consola ICCP, a través de la cual se intercambia información con el Centro de Control de Energía (CENACE), se dispone de Servidor Principal y Respaldo.

Adicionalmente la consola del Sistema de Gestión de Energía (EMS), con software dedicado ProsoL permite correr flujos, realizar análisis de cortocircuitos y estimaciones de estado. Esta consola posee dos interfaces de red, una en el entorno de red PLA y la otra tiene asignada una dirección para gestión remota.

Figura 10.- *Consola de comunicación ICCP y de EMS.*

Para Gestionar los Servidores de todos los sistemas se encuentra en el Centro de Control una consola denominada de Ingeniería que se conecta a los servidores a través de un switch KVM (Keyboard, Video, Mouse).

Cuando se integra una nueva subestación o se agrega un nuevo dispositivo, el proyecto PLA cambia, todas las actualizaciones se realizan en un computador portátil denominado PC de desarrollo que no está conectada a la red, luego de ello se traslada el proyecto al Servidor PLA Principal para correr el proyecto actualizado.

Adicionalmente se tiene una consola para gestión de protecciones que está conectada a la red corporativa con acceso a internet para envió del registro de operación de las centrales de generación y la lectura de los medidores de los grupos de generación al Centro Nacional de Control de Energía CENACE estos reportes se envían diariamente.

Se tiene instalado un firewall, el cual está programado para limitar el ingreso a la red.

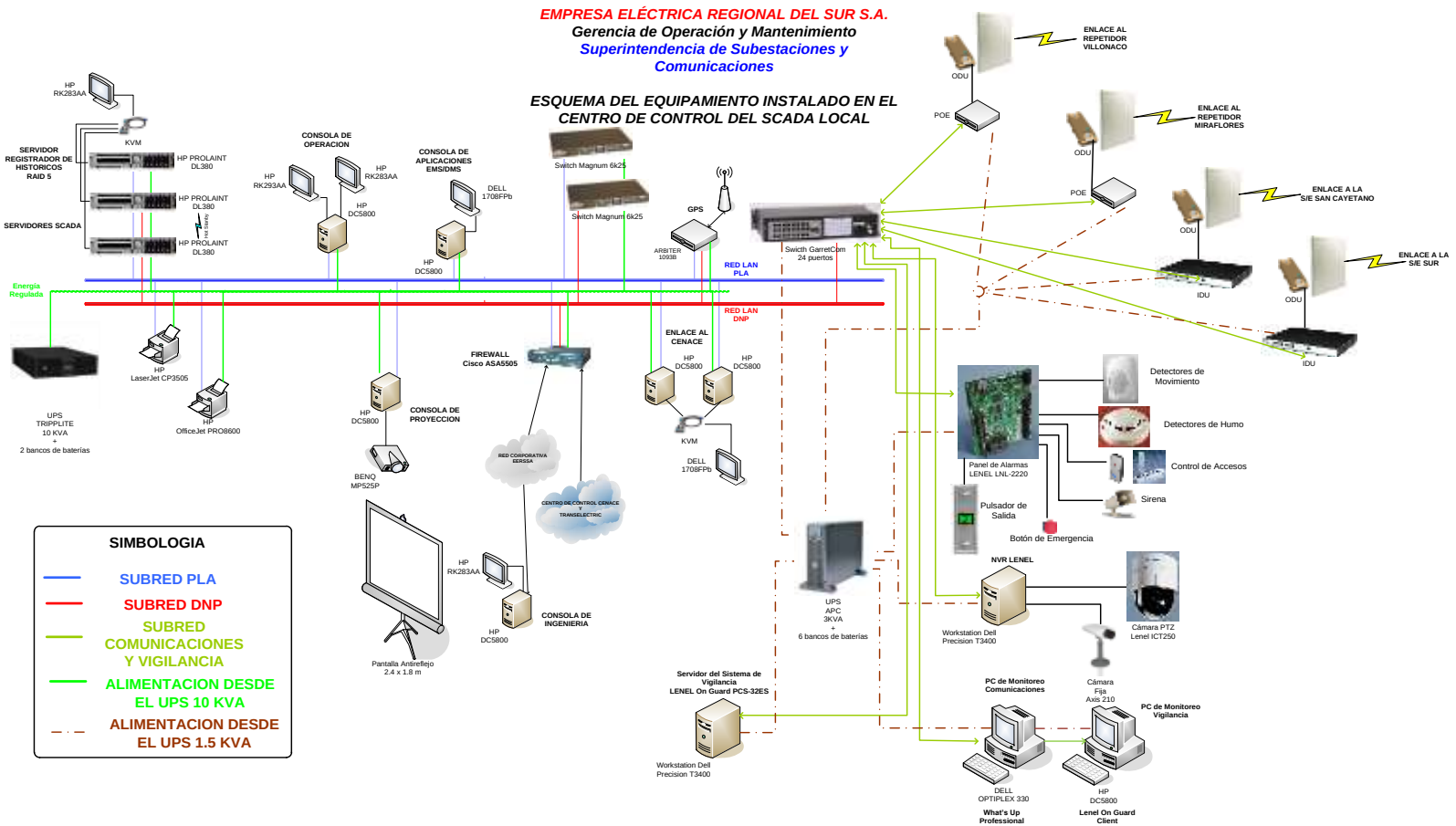

Figura 11.- *Esquema de los equipos instalados en el Centro de Control FUENTE EERSSA*

En la figura 11 se observa los equipos de la red SCADA Local de la EERSSA que se encuentran instalados en el Centro de Control. La subred PLA incluye todos los dispositivos que interactúan en el Centro de Control: Servidores PLA, consolas de operación, Servidores ICCP, impresoras, etc., la subred DNP abarca los dispositivos que interactúan con los equipos de campo: RTU, relés, etc. a través de protocolo DNP 3, la subred de comunicaciones y vigilancia incluye las cámaras, grabadores de video dispositivos de control de accesos.

CAPITULO IV.

4. IDENTIFICACION DE VULNERABILIDADES

4.1 Análisis Realizados en el SCADA Local de la EERSSA.

Para la realización de estos análisis se consideró las recomendaciones dadas en el documento de INTECO, y las publicadas por el NIST, CPNI y NERC

4.1.1. Análisis de tráfico con ayuda de Sniffer WIRESHARK.

a. Situación Inicial.

La red del sistema SCADA de EERSSA entró en operación en Julio del 2009. En la red de comunicaciones de la red SCADA de la EERSSA se identifican diversos sistemas en funcionamiento, tales como: el Sistema SCADA propiamente dicho que permite el monitoreo y control de los elementos que conforman el sistema eléctrico de potencia está conformado por Unidades Terminales Remotas RTU, Dispositivos Electrónicos Inteligentes IED, etc.; el Sistema de Video vigilancia que lo componen las cámaras de video, los grabadores de video, sensores de movimiento, etc; el Sistema de monitoreo de los dispositivos de networking que conforman la red de comunicaciones What´s Up Gold; Sistema de telefonía IP. Para permitir el trabajo de los distintos sistemas la red se encuentra organizada según se indica en la Tabla 3, esta organización consiste en una segmentación simple a través de la conformación de varias subredes.

Segmentación de la red SCADA de la EERSSA.		
División	Máscara	Nombre de la Subred
192.X.03.X	255.255.255.0	Telefonía IP
192.X.20.X	255.255.255.0	Vigilancia
192.X.30.X	255.255.255.0	Comunicaciones
192.X.40.X	255.255.255.0	Comunicaciones
192.X.100.X	255.255.255.0	PLA
192.X.101.X	255.255.255.0	DNP

Tabla 3.- *Identificación de subredes existentes en la red SCADA de la EERSSA. FUENTE EERSSA.*

Los diversos sistemas que trabajan en esta red están compuestos por diferentes equipos que han sido asignados a las diferentes subredes, los cuales se detallan en la Tabla 4.

Equipos instalados en la red SCADA de la EERSSA.		
Elementos	Subred	Cantidad
SERVIDORES	PLA/DNP	2
SERVIDORES	PLA	3
SERVIDORES	VIGILANCIA	1
CONSOLAS CLIENTE	PLA	2
EMS	PLA	1
RTU	DNP	19
IED	DNP	135
LNVR	VIGILANCIA	19
CAMARAS	VIGILANCIA	52
PANEL DE ACCESOS	VIGILANCIA	19
REPETIDORAS	COMUNICACIONES	13
UPS	COMUNICACIONES	16
FIREWALL	COMUNICACIONES	1
SWITCH	COMUNICACIONES	20

Tabla 4.- *Resumen de equipos que forman parte del sistema SCADA de la EERSSA.*

El backbone principal está conformado por un sistema de radio de 2.4 a 5.4 Ghz, en enlaces no licenciados, el servicio de última milla también se realiza a través de enlace radial existiendo en algunos lugares conexiones a la red por medio de fibra óptica.

En la figura 12 se muestra un esquema simplificado de los nodos que permiten la comunicación con las subestaciones, en esta figura se detallan los enlaces radiales y los enlaces de respaldos de fibra.

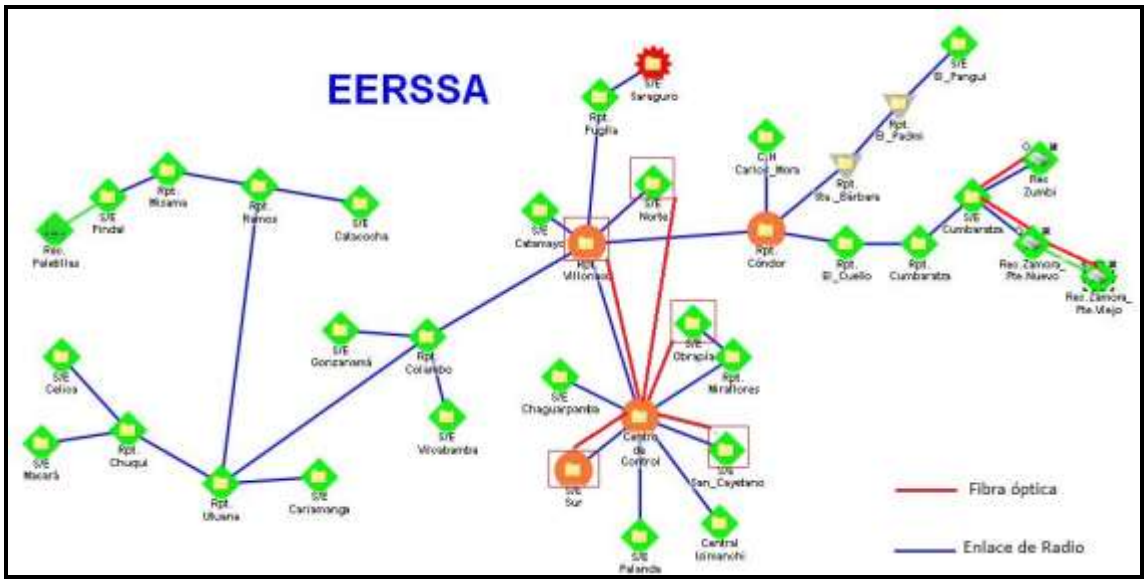

Figura 12.- *Diagrama simplificado de los nodos que permiten establecer la red de telecomunicación del sistema SCADA de la EERSSA.*
FUENTE Centro de Control EERSSA

Desarrollo.

Con el fin de analizar las vulnerabilidades de la red de comunicaciones se realizaron pruebas de análisis de tráfico en la red, con ayuda del software libre Wireshark. Sniffer que permitió observar el tipo de información que cruza por los nodos seleccionados.

Estas pruebas se llevaron a cabo colocando la herramienta en puntos aleatorios de la red como se representa en la figura 13.

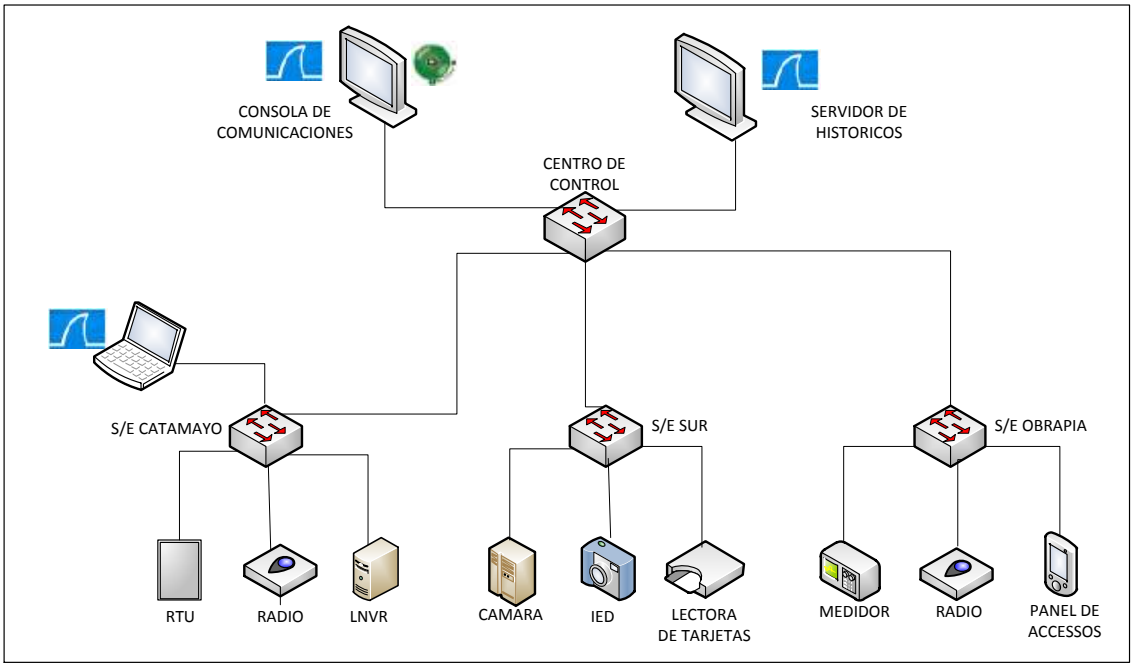

Figura 13.- *Esquema de toma de muestras con sniffer Wireshark.*

La autorización del Ing. Administrador de la red SCADA Local, fijó la frecuencia de la toma de muestras en 4 horas cada mes, durante 3 meses seguidos, de las cuales se indican las siguientes estadísticas.

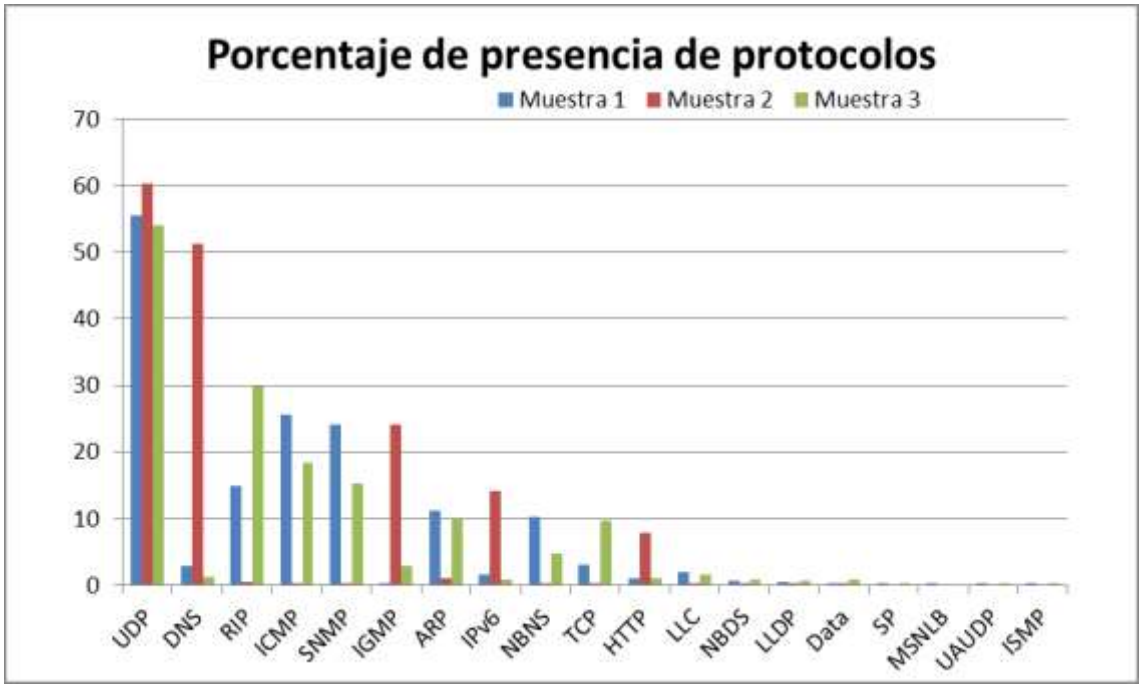

Figura 14.- Presencia de protocolos, resultado en servidor de históricos.

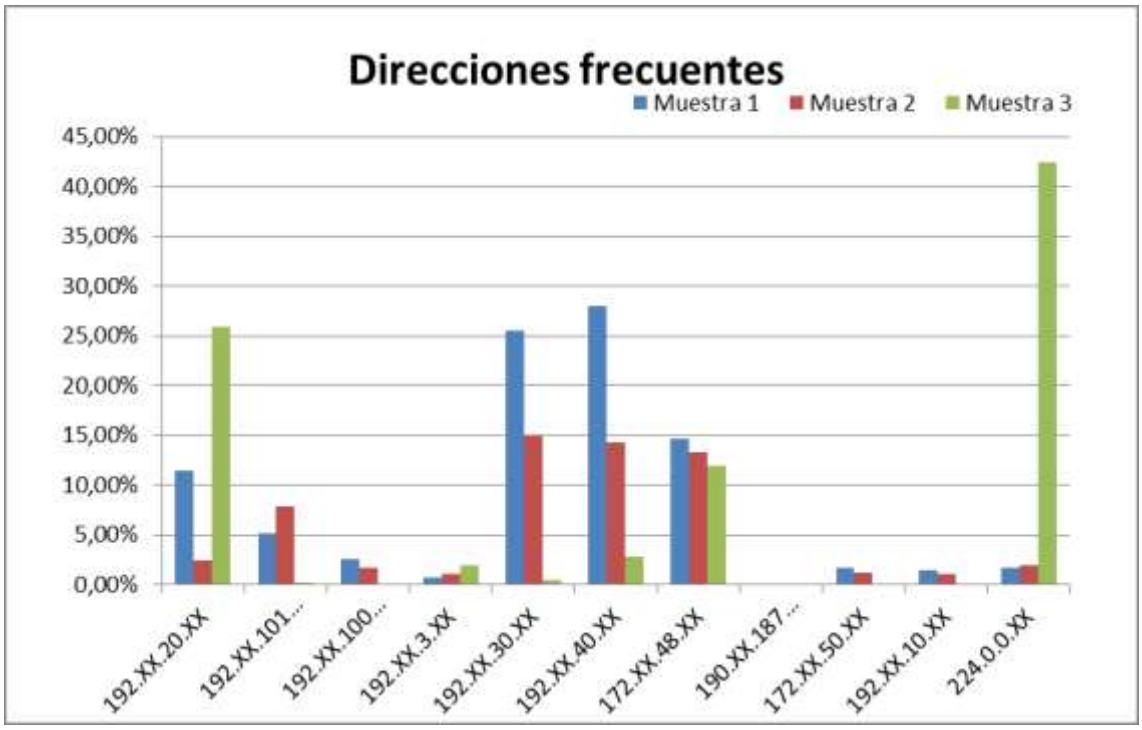

Figura 15- *Direcciones frecuentes, resultado en servidor de históricos.*

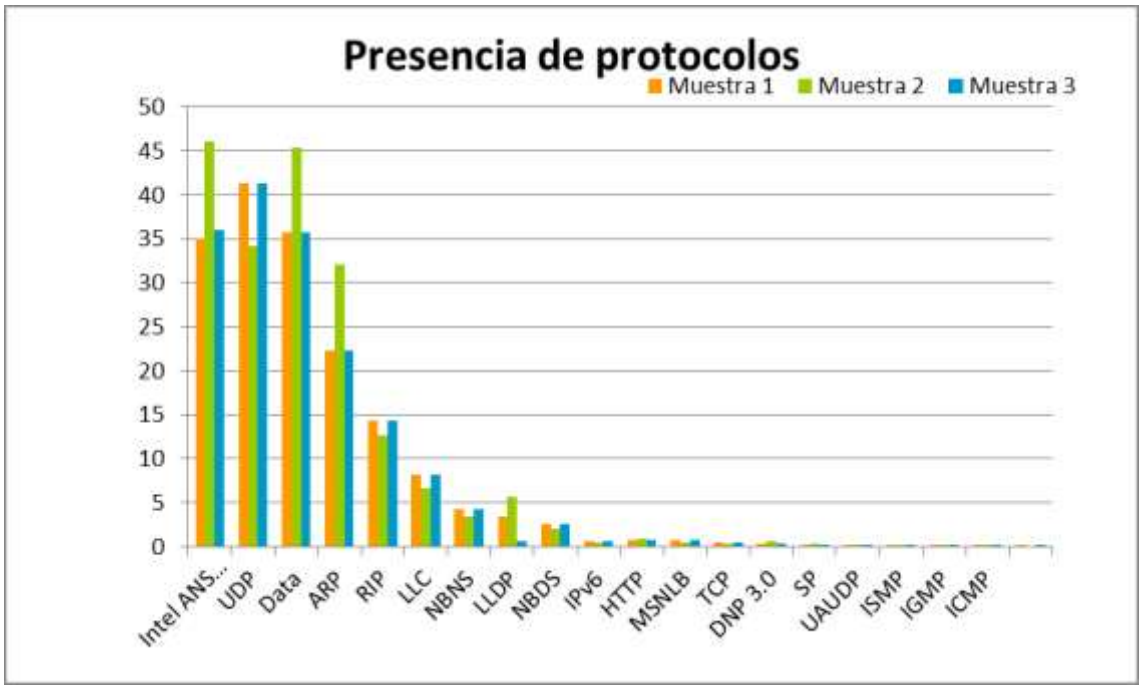

Figura 16.- *Presencia de protocolos, resultado en Switch S/E Catamayo.*

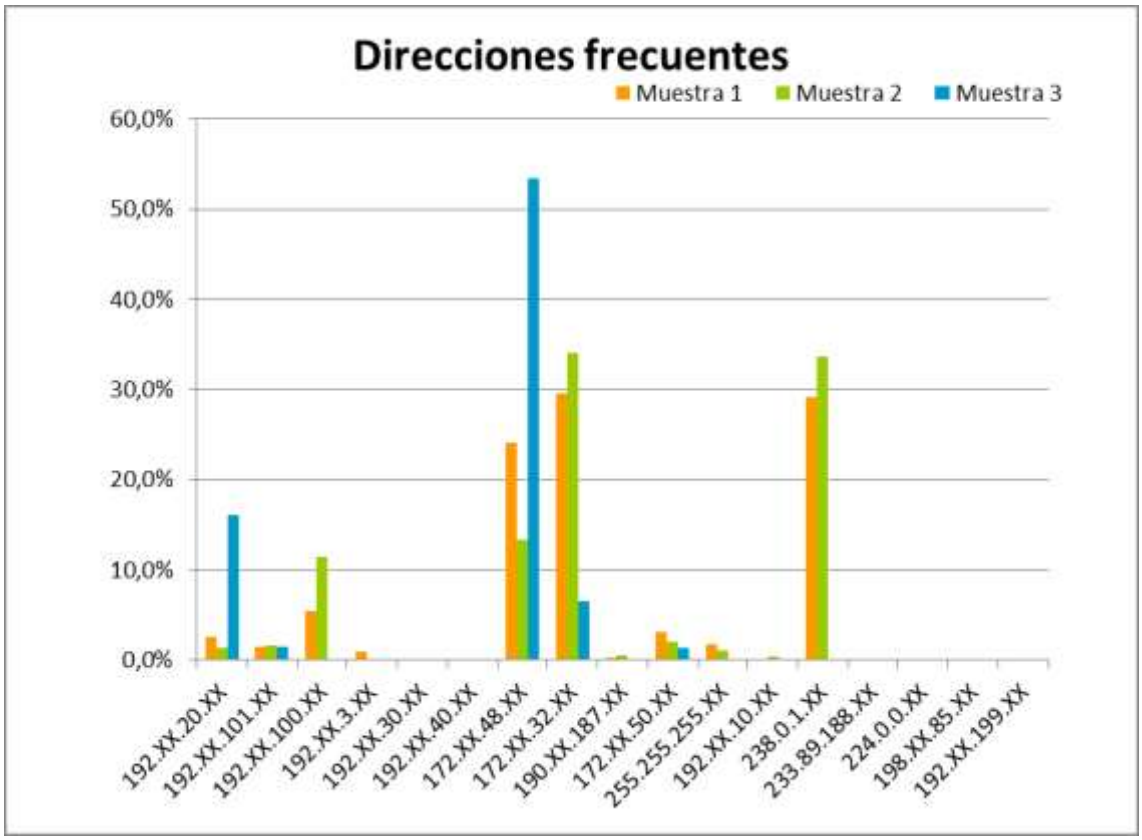

Figura 17.- *Direcciones frecuentes, resultado en Switch S/E Catamayo.*

Figura 18.- *Presencia de protocolos, resultado en Consola de Comunicaciones.*

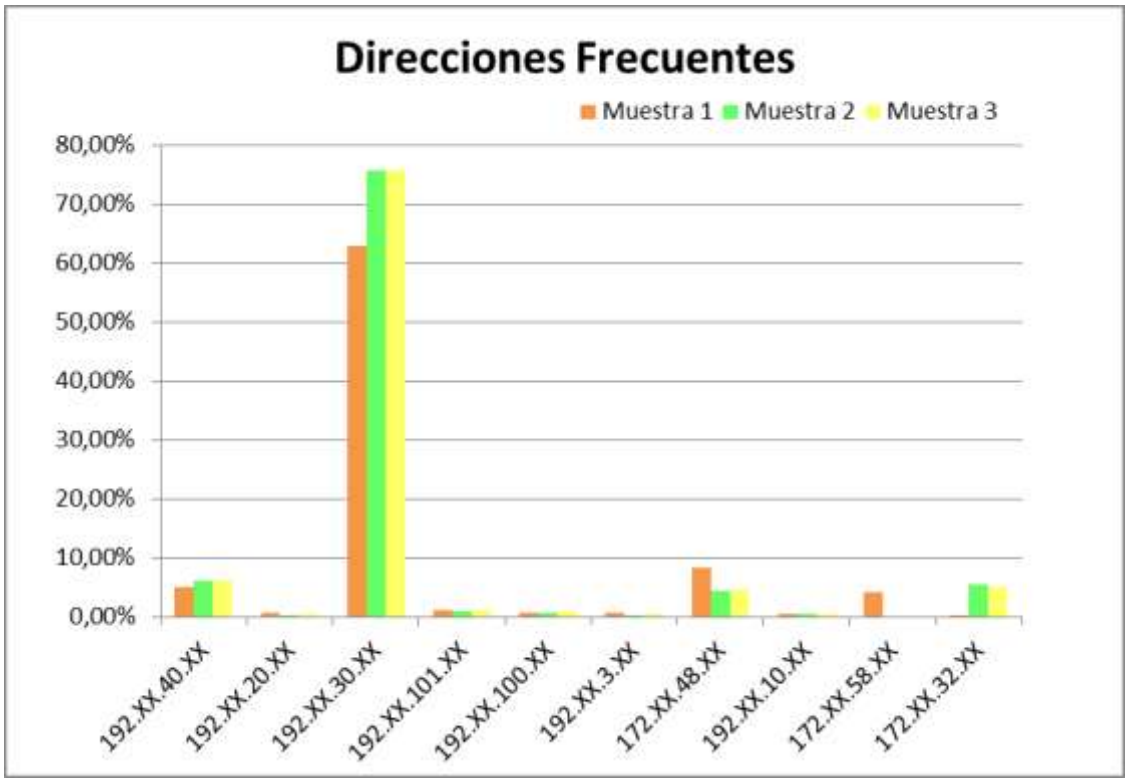

Figura 19.- *Direcciones frecuentes, resultado en Consola de Comunicaciones.*

De las muestras obtenidas con la herramienta Wireshark se puede identificar que en los nodos de monitoreo cruza tráfico de diferentes segmentos de red de la EERSSA, es decir los segmentos se interconectan directamente a un switch.

Esta configuración puede provocar que exista bajo rendimiento en la red ya que el dominio de broadcast es muy amplio, además se observa que los paquetes contienen direcciones que no constan dentro del listado de segmentos de red SCADA Local pero que forman parte de la red corporativa.

No se emplea encriptación en los mensajes, ya que el sistema SCADA Local para transmisión de paquetes emplea protocolo DNP para comunicación desde las RTU al Servidor PLA, y desde la RTU hacia los dispositivo IED de campo se emplea Protocolo SPABUS, DNP, protocolos que no soportaban servicios de seguridad.[28]

Existen varias Investigaciones que se ha realizado con el fin de buscar que los paquetes no sean blanco de ataques, entre ellas se puede citar a:

- Application of NTRU Cryptographic Algorithm for SCADA security [5]
- Cryptographic Protection of SCADA Communications. Part 1: Background, Polices and Test Plan. [20]
- Investigating the Security of Electrical Power Systems SCADA [12]

4.1.2 Análisis de la Dirección de Mantenimiento.-

Situación Inicial.

Durante la implementación del sistema SCADA Local se habilitó una dirección de red para mantenimiento remoto, que permita al personal de Autotrol, empresa proveedora del producto PLA, disponer de un acceso.

Actualmente la administración de la red SCADA Local de la EERSSA está a cargo de la Superintendencia de Subestaciones y comunicaciones, y se mantiene la dirección habilitada o disponible para la administración remota, mediante la cual el Ingeniero de Telecomunicaciones realiza labores de monitoreo, cambios, actualizaciones y ejecuta acciones emergentes de ser necesario.

Desarrollo.

La disponibilidad de este acceso remoto para ejecutar tareas de mantenimiento de la red SCADA Local de la EERSSA, supone una puerta para accesos no autorizados, y que amerita analizar las posibles vulnerabilidades que se puedan presentar.

Para el análisis de las inseguridades de este punto de acceso se ha propuesto las siguientes pruebas.

1.- **Exploración de la red.-** Con la herramienta Advanced IP Scanner; herramienta que escanea redes en tiempos cortos identificando dispositivos instalados en un rango de red, es de acceso libre. Se instaló está herramienta en una máquina de la oficina de Subestaciones y se realizó una revisión de los dispositivos de red basados en la dirección IP de la máquina donde se encontraba la herramienta se estableció el rango de búsqueda.

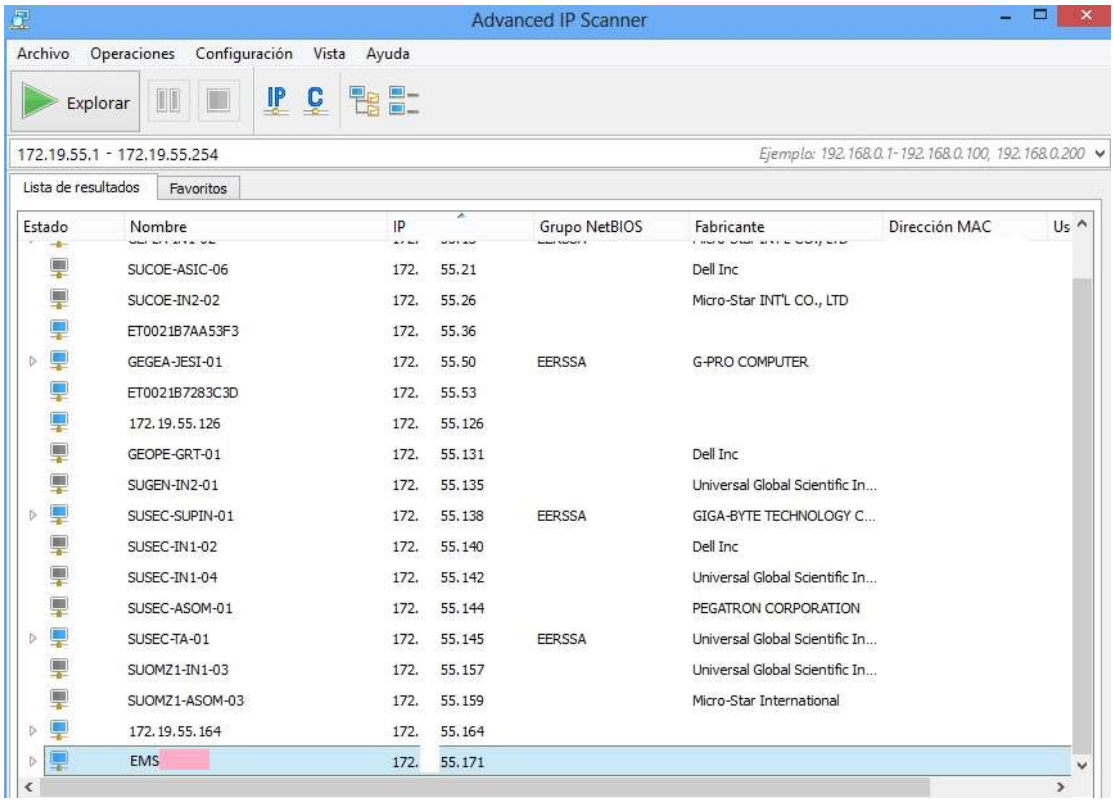

Figura 20.- *Resultado de escaneo de red con herramienta Advanced IP Scanner.*

En la figura 20 se aprecia un listado de direcciones con el nombre del host como resultado de la exploración realizada, en donde se identifica un nombre de host bajo el identificativo *"EMS"* con una dirección IP 172.X.55.171, el cual corresponde al equipo de mantenimiento de la red SCADA Local y que por la dirección expuesta pertenece a la red Corporativa de la EERSSA.

2.- **Pruebas de conectividad**.- Un análisis del resultado de la prueba anterior pone de manifiesto que una máquina de la red corporativa interna de la EERSSA puede tener acceso; por lo que a continuación se procede a

comprobar conectividad a través del protocolos ICMP ejecutando el comando ping en varias máquinas de diferentes áreas y dispuestas en diferentes puntos del Edificio Central de la EERSSA, a la dirección que corresponde al equipo de mantenimiento del sistema SCADA Local.

Prueba de conectividad				
Dirección de Origen	Departamento	Protocolo	Dirección de Destino	Resultado
172.X.53.12	Archivo	ICMP (Ping)	172.X.55.X	Responde
172.X.53.168	Call Center	ICMP (Ping)		Responde
172.X.54.5	Secretaria Ejecutiva	ICMP (Ping)		Responde
172.X.55.138	Subestaciones	ICMP (Ping)		Responde
172.X.55.139	Subestaciones	ICMP (Ping)		Responde
172.X.55.140	Subestaciones	ICMP (Ping)		Responde
172.X.55.142	Subestaciones	ICMP (Ping)		Responde
172.X.55.158	Gerencia Operación	ICMP (Ping)		Responde
172.X.55.52	Gerencia Planificación	ICMP (Ping)		Responde
172.X.55.62	Contraloría Interna	ICMP (Ping)		Responde
172.X.55.8	Gerencia Ambiental	ICMP (Ping)		Responde
192.168.2.21	Wi-fi	ICMP (Ping)		Responde

Tabla 5.- *Respuesta a ejecución de comando ping a dirección de mantenimiento.*

Un resumen de los resultados de las pruebas de conectividad se presenta en la Tabla 5; en donde se puede apreciar la ejecución de una prueba desde un host conectado a través de la red inalámbrica (WI-FI), disponible para visitantes en el edificio de la EERSSA.

3.- **Prueba de acceso.-** Tras confirmar la conectividad desde diferentes hosts al equipo de mantenimiento EMS, dentro de la red corporativa, es conveniente continuar con una siguiente prueba para intentar probar diferentes servicios que permitan acceder al host de destino.

Se elige probar con uno de las herramientas más conocidos a nivel del entorno Windows como es el acceso a través de Escritorio Remoto.

Figura 21.- *Imagen de acceso a través de escritorio remoto a la dirección de mantenimiento***.**

El acceso a escritorio remoto se ejecuta satisfactoriamente y presenta una ventana con requerimientos de usuario y password; si bien el requerimiento de un usuario y clave de ingreso son limitantes para completar el acceso a la consola EMS de mantenimiento, estas pueden ser vulneradas tras un ataque más agresivo o pueden ser divulgadas en casos de requerir asistencia de terceros.

Conclusión.

Este es un punto crítico pues una vez que se logra acceder a esta consola, se ingresa al entornó de la red SCADA Local de EERSSA, en la cual las configuraciones de acceso a los demás dispositivos de la red son generales o por defecto abriendo un campo de vulnerabilidad amplio.

4.1.3 Análisis de contraseñas de acceso.

Los datos que se muestran en la Tabla 6, fueron recopilados de los registros facilitados por el Administrador de la red.

Actualmente no se realiza cambio de contraseñas. Para el ingreso hacia las consolas de operación o clientes del Scada PLA los Operadores emplean sus usuarios y contraseñas que identifican el cambio de Operador las cuales se acreditaron cuando pasaron a operar el Centro de Control.

La consola de Ingeniería es de uso exclusivo del Administrador de la red, el ingreso se realiza con el usuario y contraseña por defecto.

De igual manera para las consolas de vigilancia existe un usuario y una contraseña estándar para todos los Operadores.

Al servidor de vigilancia ingresa el Ingeniero encargado de la administración del sistema de Vigilancia con el usuario y clave por defecto.

Como se indicó en el capítulo 3 las consolas de operación y de ingeniería comparten el mismo espacio físico, si bien hasta ahora no se ha presentado ningún reporte de usurpación de identidad para el ingreso al sistema es conveniente adoptar una política de cambio de contraseñas.

Según recomendaciones de Seguridad de redes [1], los cambios de contraseñas deben realizarse periódicamente cada dos o tres meses, no es necesario cambiar la contraseña a cada dispositivo de administración de red como Switch, firewall, u otros dispositivos, puede ser la misma contraseña pero se debe renovar mensualmente.

Registro de Contraseñas en equipos del Scada Local de EERSSA									
			Actualización de contraseñas por año						
	Acceso con contraseña	Tipo de acceso	2009	2010	2011	2012	2013	2014	2015
Servidores PLA	Si	Administrador	Puesta en marcha	Sin cambio	Sin cambio	Sin cambio	Sin cambio	Sin cambio	Sin cambio
Servidor Vigilancia	Si	Administrador	Puesta en marcha	Sin cambio	Sin cambio	Sin cambio	Sin cambio	Sin cambio	Sin cambio
Consolas de operación	Si	Operador	Puesta en marcha	Sin cambio	Sin cambio	Sin cambio	Sin cambio	Sin cambio	Sin cambio
LNVR	Si	Operador	Puesta en marcha	Sin cambio	Sin cambio	Sin cambio	Sin cambio	Sin cambio	Sin cambio
RTU	Si	Administrador	Puesta en marcha	Sin cambio	Sin cambio	Sin cambio	Sin cambio	Sin cambio	Sin cambio
Acceso Remoto	Si	Administrador	Puesta en marcha	Sin cambio	Sin cambio	Sin cambio	Sin cambio	Sin cambio	Sin cambio
Switch	Si	Administrador	Puesta en marcha	Sin cambio	Sin cambio	Sin cambio	Sin cambio	Sin cambio	Sin cambio
Firewall	Si	Administrador	Puesta en marcha	Sin cambio	Sin cambio	Sin cambio	Sin cambio	Sin cambio	Sin cambio

Tabla 6.- *Resumen de cambio de contraseñas realizadas en el sistema SCADA Local de la EERSSA.*

El tema del uso de las contraseñas se ha tratado en diversas investigaciones [2] [3] en las cuales se considera que el factor humano es muy importante y el que puede exponer a un sistema sin siquiera proponérselo, puede compartir su claves de acceso en un diálogo o en una emergencia y luego olvidar cambiar su clave. Se recomienda que las contraseñas deben contener caracteres compuestos por letras mayúsculas, minúsculas, una extensión mínima de 7 caracteres para que sean fáciles de recordar. Para lo cual se pueden seguir recomendaciones como emplear iniciales de nombres al inicio o al final que permitan su fácil memorización [3].

4.1.4 Pruebas de acceso físico.

Situación Inicial.

Cuando se implementó el sistema SCADA Local de la EERSSA se acondicionó un área para alojar adecuadamente a los servidores, se consideró la instalación de un aire acondicionado de precisión que mantenga la temperatura adecuada para un correcto funcionamiento de los dispositivos; adicionalmente para el ingreso a la sala de servidores se instaló un control de accesos que consta de una tarjeta electrónica y una lectora la cual comprueba que la tarjeta tenga asignada el código de ingreso; además se cuenta con la instalación de una cámara de seguridad que es monitoreada desde el Centro de Control. Esta sala se comparte con equipos de la red corporativa interna de EERSSA, por ello el acceso a esta sala está autorizado al personal de la Superintendencia de Sistemas que se encarga de la administración de la infraestructura de la red corporativa y al personal del área de la Superintendencia de Subestaciones y Comunicaciones que tiene a cargo la administración del sistema SCADA de la EERSSA.

La sala dispuesta para la operación del sistema SCADA, o Centro de Control propiamente dicho, igualmente consta con controles de acceso en sus dos puertas de ingreso y una cámara de vigilancia tipo PTZ, el acceso a esta sala está limitado a los ingenieros que laboran en la Superintendencia de Subestaciones y Comunicaciones de la EERSSA, los cuales se encargan de

administrar el sistema SCADA y operar el sistema de potencia a nivel de Subestaciones, cada uno de ellos posee una tarjeta de ingreso, los videos se almacenan en un Lenel Video Recorder (LNVR) ubicado en la sala de servidores donde también se encuentra la tarjeta del panel de accesos.

En las subestaciones integradas al sistema SCADA, se dispone de 2 cámaras de vigilancia una fija instalada en la casa Comando donde se ubican los controles para operación en sitio o local de los interruptores, y una cámara PTZ en la parte exterior, que rota por el área de la subestación en rutinas constantes, se dispone de control de accesos a nivel de lectora y tarjeta, además se encuentran instalados sensores de movimiento en la parte posterior de los tableros de control de la casa comando y en el cuarto de baterías, para evitar algún inconveniente en estas instalaciones se cuenta también con sensores de humo y movimiento. Así mismo en cada subestación se cuenta con un equipo grabador de video y la lectora de tarjeta de control de accesos. A las instalaciones de las subestaciones el acceso es igualmente restringido, las personas que cuentan con tarjetas de acceso son los jefes de Agencia, jefes zonales, y jefes de cuadrilla o grupos de trabajo de subestaciones. Cuando el personal necesita ingresar a las Subestaciones deben informar al Centro de Control el motivo de su ingreso.

Debido a convenios que se mantienen con empresas como TRANSELECTRIC, CNT, Claro y empresas clientes de CNT y de TRANSELECTRIC, se ha logrado en ciertos sitios contar con canales de fibra óptica y disponer de enlaces desde las subestaciones al Centro de Control; para esto se ha permitido que estas empresas instalen sus equipos nodos en las subestaciones y en la sala de servidores de la EERSSA. Cuando se requiere realizar un mantenimiento de los equipos de estas empresas sea en la sala de servidores o en las subestaciones deben enviar a una consignación detallando el tiempo que durará el mantenimiento y el trabajo a realizarse para que el Ingeniero Administrador de la red SCADA

local, lo considere y apruebe o niegue la intervención en las instalaciones de la EERSSA.

Desarrollo.-

Debido a la información que se almacena en el servidor de históricos y a los procesos que se ejecutan en los servidores del SCADA Local de la EERSSA, se consideró analizar si el acceso a la sala de servidores y al Centro de Control es restringido.

Primero se consideró ingresar a la sala de servidores luego de las horas laborables, si bien la puerta de acceso al área de sistemas se encuentra cerrada la puerta del Centro de Control se encuentra abierta para que el personal que realiza la limpieza ingrese a realizar su labor por lo cual nada impide avanzar hasta la puerta de la sala de servidores. Una vez ahí la cerradura magnética limita el acceso, pero la tarjeta asignada al personal de sistemas se encontraba junto a la cerradura magnética, por lo que el acceso a la sala de equipos resultó exitoso.

Registro de accesos de terceros a las instalaciones de la EERSSA				
N° Consignación	Empresa	Sitio de Ingreso	Fecha	Horario
Petición por mensaje de correo *tecproddatosportadores@claro.com.ec*	Claro	SALA DE SERVIDORES	18/02/2015	08h00 a 17h00
Petición por mensaje de correo remigio.pilco@cnt.gob.ec	CNT	SALA DE SERVIDORES	19/03/2015 al 20/03/2015	20h00 a 05h00
TRANELECTRIC: Requerimiento # 251	CNT	S/E CAYETANO, S/E PANGUI, OF. PANGUI	13/04/2015 al 17/04/2015	08h00 a 17h00

Tabla 7.- *Tabla de los accesos de personal de otras empresas que ingresaron a las instalaciones de la EERSSA, donde se dispone de equipos de networking de la red SCADA Local de la EERSSA. FUENTE: Centro de Control EERSSA.*

En la Tabla 7, se presenta un detalle de ingreso de personal de las empresas que tienen sus nodos de fibra en la Sala de Servidores del Centro de Control luego de tener el acceso aprobado, ingresan a la sala de servidores con la asistencia del Operador del Centro de Control, la cámara observa el ingreso por la puerta, luego abren los armarios por la parte posterior, lo que queda fuera del rango de vista de la cámara que al ser fija el rango de visión no abarca lo que ocurre en la parte posterior, esto se convierte en una vulnerabilidad, ya que el personal de la EERSSA sólo permite que ingresen pero no están autorizados a mantenerse supervisando el trabajo que realizan pues deben regresar a operar el sistema SCADA.

Figura 22.- *Imagen que se observa en la cámara fija instalada en el Sala de Servidores de la EERSSA.*

En las Subestaciones se observó que de igual manera se debe autorizar el ingreso a las instalaciones a personal de la EERSSA como a terceros. El personal de la EERSSA, en las subestaciones que se encuentran distribuidas en la provincia, ingresan luego de coordinar con el Centro de Control con sus tarjetas autorizadas y en caso de no portarla el Centro de

Control les habilita remotamente el ingreso, en la casa comando la cámara fija registra el ingreso frontal pero la parte posterior a los tableros es un punto ciego.

En la figura 22 se muestra la imagen que observa la cámara en el cuarto de servidores y en la figura 23 se indica en forma general la disposición de los servidores con lo que se puede evidenciar que al ingresar a la sala de servidores los accesos a los equipos no se observan.

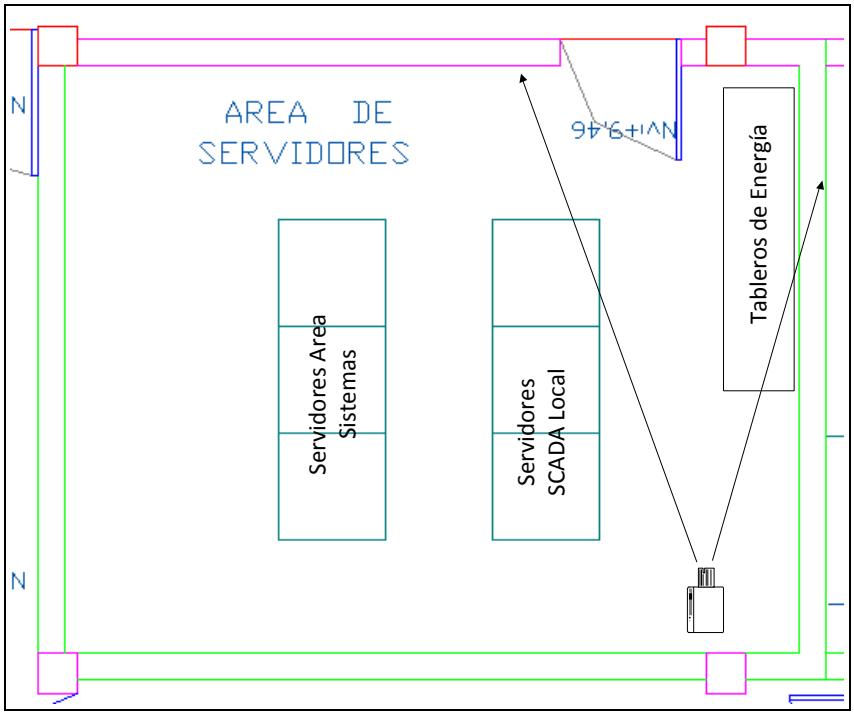

Figura 23.- *Rango de visión de cámara instalada en la Sala de servidores de la EERSSA y relación con los accesos a los equipos de red***.**

4.1.5 Respaldos de información crítica.

Situación Inicial.-

Para el normal funcionamiento del sistema SCADA Local de la EERSSA, como se menciona en el capítulo 3, se dispone de dos servidores en estado Standby con la finalidad que si un servidor deja de funcionar, este evento sea transparente para el Operador ya que las consolas clientes nunca pierden la conexión ya que los servicios seguirán ejecutándose desde el servidor de respaldo.

Para los sistema de vigilancia existe un servidor y un cliente; para el sistema de monitoreo de telecomunicaciones se dispone de un cliente y para almacenamiento de datos históricos existe un servidor en el que además se encuentran instalados los servicios de monitoreo de Telecomunicaciones, es decir las funciones de servidor para el monitoreo de comunicaciones y almacenamiento de datos históricos radican en un único equipo físico.

Una de las características que hacen diferente estos sistemas a los usualmente empleados en tecnologías de información es que la vida útil de los equipos es de más de 5 años por lo que son susceptibles a fallas de funcionamiento debido a sus elementos constructivos por ello se debe dar especial importancia a los respaldos de las configuraciones de estos equipos con la finalidad de poder recuperar su funcionalidad en tiempos cortos que no involucren indisponibilidad del sistema.

De igual manera si se presentara un ataque al sistema que lograra borrar parte importante de los servidores lo ideal sería contar con un respaldo que permita volver a colocar un servidor con las mismas configuraciones sin entorpecer la operación del Centro de Control.

Desarrollo.

Según la publicación *NIST Special Publication 800-82***,** el mantener un respaldo de la información crítica y copia de configuraciones de los equipos de Networking que conforman los sistemas de control industrial ayudan a mejorar la seguridad y la disponibilidad pues el tiempo de recuperación será más corto que iniciar a configurar los equipos desde cero.

Para identificar cuan preparada esta la EERSSA para afrontar un incidente como los mencionados anteriormente se realizó la consulta al ingeniero Administrador del sistema referente a como se almacenan y registran las configuraciones o copias de respaldo.

Registro de respaldos de información y configuración crítica					
Configuración	Existe configuración de respaldo	Imagen completa del equipo	Última fecha de respaldo	Registro	Observaciones
Proyecto PLA	SI	N/A	30/07/2015	No	Integración de IED de protección en S/E Obrapía.
Remota	SI	N/A	29/06/2015	No	Integración de IED de protección en S/E Obrapía.
Servidor Principal	No	No	-	No	
Servidor Respaldo	No	No	-	No	
Servidor Históricos	No	No	-	No	
Servidor de Vigilancia	No	No	-	No	
Servidores ICCP	No	No	-	No	
Firewall	No	N/A	-	No	
Switch	No	N/A	-	No	
Switch de Subestación	No	N/A	-	No	
Consola de Operación PLA	No	No	-	No	
Consola de Vigilancia	No	No	-	No	
Consola de Comunicaciones	No	No	-	No	
Consola EMS	No	No	-	No	

Tabla 8.- *Resumen de información de respaldo y configuraciones de los equipos del SCADA Local de la EERSSA. FUENTE SUSEC.*

Como se aprecia en la Tabla 8, no existe un registro documentado de respaldo de configuraciones críticas de los dispositivos firewall, switch, consolas de operación, esto podría demorar la disponibilidad en caso de que uno de estos equipos deje de operar adecuadamente, pues no existe un detalle de las configuraciones y los objetivos o funcionalidades de cada una.

Si bien los registros actuales, según se observa en la tabla 8, corresponden a respaldo del proyecto PLA y de las RTU, no se documenta cada archivo que se actualiza ni el motivo del cambio de configuración, cabe aclarar que un sistema de potencia es muy dinámico y constantemente existirán cambios sea por la integración de nuevos dispositivos de campo o por funcionalidades que se agregan a los dispositivos existentes actualmente.

El correcto almacenamiento de la información permitirá una recuperación rápida ante incidentes, en la actualidad existen sistemas para organizar la información de manera automática basada en sistemas AS/RS (Automated Storage / Retrieval System), esto ayudará a minimizar errores humanos en la obtención de respaldos, optimizando las tareas de almacenamiento.

4.1.6 Análisis de software malicioso (Virus).

Situación Inicial.-

Los equipos se instalaron en el Centro de Control en el 2009, por recomendación del proveedor del sistema no se instaló antivirus en los servidores ni en los clientes del sistema SCADA Local de la EERSSA, ya que se podían confundir rutinas o servicios con código malicioso lo que podría ocasionar que el sistema deje de operar correctamente.

A continuación describiremos las variaciones que se han realizado en la configuración de la red, eventos que pueden provocar el ingreso de código malicioso o virus que puede exponer al sistema.

Inicialmente la red SCADA Local de la EERSSA se mantenía aislada de la red corporativa, con el tiempo se fue abriendo conexiones con la red corporativa para la recolección de los datos históricos y las lecturas diarias de los medidores de las centrales de Generación. Así también se abrió el enlace de mantenimiento que conecta directamente la red SCADA Local con la corporativa.

El sistema SCADA Local consta de dos equipos portátiles de campo con las que se realiza las actualizaciones de las configuraciones de las RTU y del proyecto PLA, estos equipos inicialmente se empleaban exclusivamente para estas actividades, luego por las necesidades operativas de la Superintendencia de Subestaciones y Comunicaciones se fue compartiendo su uso, ya sea para las configuraciones de los IED de protección y configuración de los equipos de comunicaciones, esto implica que la información que se almacena en ellas pueda ser extraída por medio de dispositivos de almacenamiento que están en contacto con otros computadores, esto puede abrir una puerta de acceso a virus, troyanos, etc.

Desarrollo.-

El personal de EERSSA, realiza análisis de virus en los servidores con el antivirus adquirido por la Empresa, “ESET NOD 32 Antivirus” para ejecutar éste análisis se retira de línea uno de los servidores luego de analizar el resultado se conecta a la red y se desconecta el otro servidor para realizar el mismo procedimiento, con los equipos clientes se procede de igual manera consola por consola, considerando la recomendación de Autotrol de no instalarlo en los equipos para evitar inconvenientes de operación por rutinas desconocidas.

El Administrador del SCADA Local de la EERSSA ha ejecutado el antivirus en varias ocasiones según reportes del Centro de Control los cuales se resumen en la Tabla 7.

Resultado de análisis con antivirus ESET en equipos del Scada Local de EERSSA							
	2011	2011	2011	2012	2013	2014	2015
	21-mar	08-abr	06-jul	29-may	18-dic	02-may	05-mayo
Servidor PLA Principal	0	0	0	0	0	0	0
Servidor PLA Respaldo	0	0	0	0	0	0	1
Servidor Históricos	0	0	0	0	0	0	1
Servidor Vigilancia	0	0	0	0	0	0	0
Servidor ICCP A	0	0	0	0	0	0	0
Servidor ICCP B	0	0	0	0	0	0	0
Estación de operación 1	0	0	0	0	0	0	0
Estación de operación 2	0	0	0	0	3	0	0
EMS	0	0	0	0	0	0	0

Tabla 9.- *Resultado de virus encontrados en los dispositivos del Sistema SCADA Local de la EERSSA Exploración realizada con Antivirus ESET NOD 32. FUENTE Centro de Control EERSSA.*

En el último análisis realizado a los equipos se observó la presencia de un archivo malicioso que se encontró en el servidor B o de respaldo, el Gusano: Win32/Conficker.AA, es un malware que apareció en el 2008, un gusano que explota una vulnerabilidad en el servicio Windows Server en los sistemas Windows 2000, server 2003.

“Esta vulnerabilidad podría permitir a un usuario remoto malintencionado y que no está autenticado poner en peligro el sistema basado en Microsoft Windows y tomar el control del mismo”. [22]

Esta vulnerabilidad se encuentra enlistada en base de datos de NIST con el código CVE-2008-4250, para solventarla Microsoft presentó el parche MS08-067. La ficha de la base de datos de NIST califica esta vulnerabilidad como alta ya que permite la divulgación no autorizada de la información, la modificación no autorizada e interrupción del servicio. [23]

CAPITULO V.

5 PROPUESTAS DE MECANISMOS DE SEGURIDAD

5.1 PROPUESTAS PARA MEJORAR LA SEGURIDAD DE LA RED SCADA DE LA EERSSA.

Luego de las pruebas realizadas y del análisis de la operación del sistema SCADA Local de la EERSSA, se ha determinado que no existen políticas de control y procedimientos para gestionar la seguridad, tan solo algunas reglas básicas,

La implementación de políticas conlleva el compromiso de todo el personal involucrado en la operación del sistema incluido directivos, Administrador y Operadores

A continuación se presentan algunas propuestas, basadas en la Norma ISO 27000 que inicia con la etapa de planificación en la que se propone las actividades a realizarse, la etapa de implementación no corresponde al presente trabajo se plantea como recomendación así también la revisión de los resultados.

Considerando las pruebas que se realizaron en el capítulo 4; se proponen medidas que ayudaran a mitigar las vulnerabilidades encontradas.

5.1.1 Organización de la Red.

Propuesta.

Como se observó en las muestras del analizador de tráfico las subredes comparten el mismo canal, al estar todas interconectadas el dominio de broadcast es amplio y ya sea un equipo de la red de comunicación, de la red de vigilancia o de la red DNP o PLA, todas comparten tráfico.

Se propone el empleo de Red de Área Local Virtual (VLAN), para ordenar la disposición de los equipos en el Centro de Control y en las Subestaciones, lo que permitirá identificar el tráfico de cada puerto, con la implementación de VLAN se mejora la utilización del ancho de banda pues se limitará el dominio de broadcast por VLAN. La revisión de actividad de puertos permitirá identificar si se conecta un dispositivo no autorizado.

La configuración planteada en el Conmutador (Switch) es la siguiente:

Dividir los puertos de los conmutadores (switches) instalados en la red del SCADA en tres VLAN: vigilancia, comunicaciones y SCADA Local DNP se elige 3 VLANS una por cada servicio o sistema presente;

Se propone realizar esta configuración con el fin de organizar la disposición de los equipos lo que ayudará a detectar si existen equipos sospechosos conectados a la red. En la Tabla 10, resumimos la disposición de las VLAN.

Configuración de VLAN en Switch de Subestaciones			
Número de VLAN	Nombre de VLAN	Puertos del Switch	Rango de sub red
20	Vigilancia	01 al 06	192.X.20.X
30	Comunicaciones	07 al 12	192.X.30.X
101	Red DNP o SCADA	13 al 23	192.X.101.X
Troncal	Todas	24	Todas

Tabla 10.- *Detalle de la configuración de VLAN propuesta para conmutador (switch) de Subestaciones,*

Con la ayuda de la herramienta libre Packet Tracer de Cisco se ha simulado la configuración de las VLANs en el conmutador (switch) de Subestaciones a continuación se indica la configuración.

```
Switch>enable
Switch#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 20
Switch(config-vlan)#name Vigilancia
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name Comunicaciones
Switch(config-vlan)#vlan 101
Switch(config-vlan)#name PLA
Switch(config-vlan)#exit
Switch(config)#interface range fa0/1-6
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
Switch(config)#interface range fa0/7-12
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#exit
Switch(config)#interface range fa0/13-23
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 101
Switch(config-if-range)#exit
Switch(config)#interface range fa0/24
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#exit
Switch(config)#exit

%SYS-5-CONFIG_I: Configured from console by console
Switch(config)#copy runnig-config star.
```

La Figura 24, indica la disposición de los equipos por VLAN en la Subestaciones y su conexión hacia el conmutador (Switch) principal o troncal.

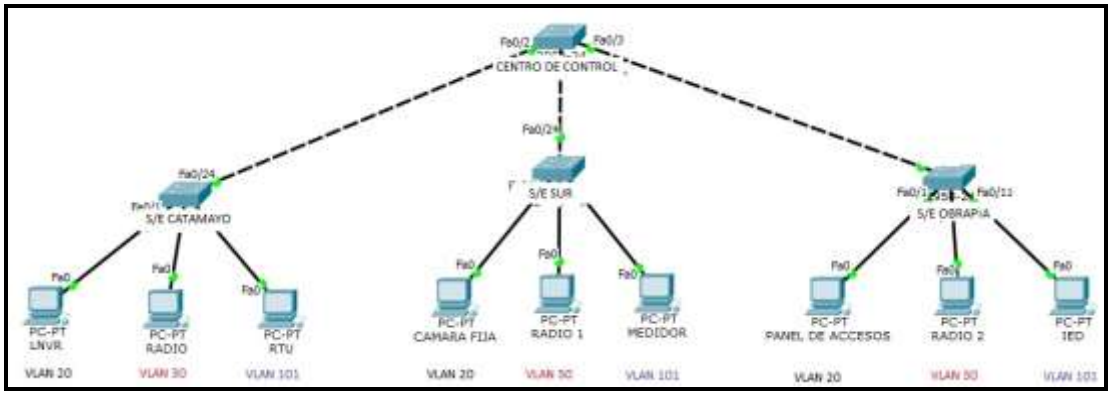

Figura 24.- *Configuración de VLAN en conmutador (Switch) de Subestación.*

El empleo de VLAN ayudará a monitorear el tráfico por puertos del conmutador (Switch), y al ejecutar una herramienta de monitoreo de tráfico será más fácil determinar si existe una dirección sospechosa.

Adicional a la ordenación lógica de los hosts en los diferentes dispositivos no se debe olvidar etiquetar los cables adecuadamente y llevar un registro, esto ayudará al personal en campo cuando requieran asistencia remota, en sus inspecciones o labores de mantenimiento.

5.1.2 Análisis de la Dirección de Acceso Remoto

Propuesta.

La dirección de mantenimiento está conectada directamente a la red corporativa por ello, se propone el empleo de (Access Control Lists – ACLs) Listas de Control de Acceso las cuales pueden limitar el tráfico que ingresa a un determinado equipo de red, evitando que dispositivos no autorizados tengan acceso a determinado segmento de red o a un host, así la dirección destino se encuentre dentro del mismo segmento de red.

Esto ayudará a mejorar la seguridad ya que algún intruso que quiera ingresar debe conocer exactamente la dirección de acceso a la ACL.

La propuesta consiste en configurar una ACL estándar, que permita el ingreso al equipo con la dirección IP de mantenimiento configurada, es decir las solicitudes que provengan de la dirección del equipo del Administrador de la red y rechace todas las otras posibles solicitudes.

A continuación se presenta un ejemplo de configuración de una ACL estándar que puede ser implementada en un enrutador; en el ejemplo se limita el acceso por dirección IP al servidor o host conectado desde la red corporativa a la red SCADA Local de EERSSA.

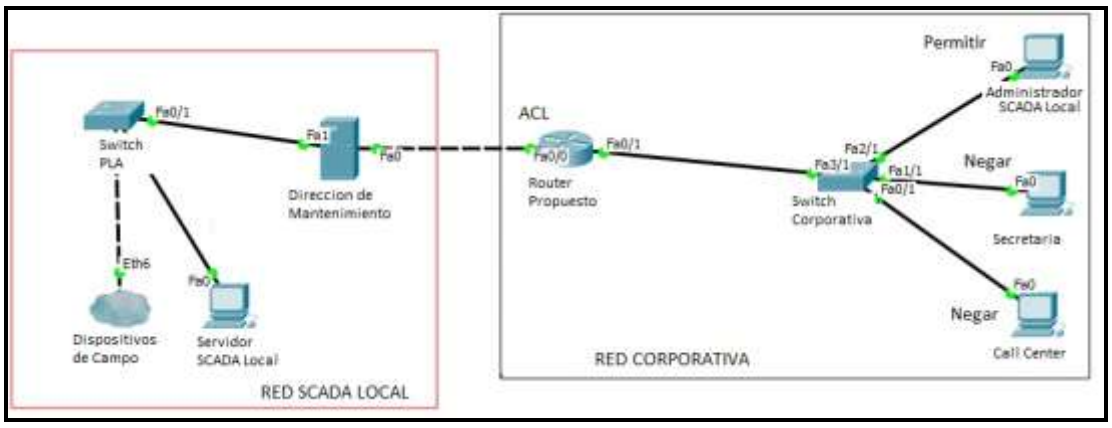

Figura 25.- *Ejemplo de aplicación de ACL*

La configuración del router es la siguiente:

Router#
Router#config term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 10 permit host 172.X.55.X4X
Router(config)#access-list 10 deny any
Router(config)#Interface fa0/0
Router(config-if)#ip access-group 10 out
Router(config)#exit

Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK].

Con la implementación de esta ACL, el acceso será permitido sólo al dispositivo con la dirección 172.X.55.X4X, perteneciente al Administrador de la red SCADA Local, los otros equipos de la red no podrán ejecutar ninguna solicitud.

Adicionalmente se propone implementar un servidor o el router con sistema AAA (Autenticación, Autorización, Auditoria), esto permitirá gestionar de manera ordenada los accesos de administración e ingresos remotos y llevar un registro que facilite identificar si existe amenazas de accesos no autorizados, además limitar el acceso a servicios por usuario.[35]

A Continuación se describen los componentes del sistema AAA.

Autenticación.- Los usuarios deben probar que son ellos los que están requiriendo acceder al sistema, este proceso se realiza empleando métodos de combinación de: usuario y contraseña, preguntas de desafío y respuesta, adicionalmente incluir cifrado.

Autorización.- Luego de identificar el usuario, los servicios de autorización determinan los recursos y operaciones a los que el usuario tiene acceso, es decir el nivel de acceso determinado por roles de usuario por ejemplo: Observado, Administrador, Operador.
La autorización se puede limitar por tiempo, ubicación física, o número de acceso por usuario.

Auditoría.- Se registra lo que realiza el usuario, los recursos a los que accede, tiempo que permanece conectado, cambios que ejecuta; recolecta y reporta información con estampa de tiempo y estadísticas de uso de paquetes, permite identificar la dirección IP desde donde se conecta el usuario.

Entre las bondades de emplear un sistema AAA se encuentra la flexibilidad y configuración de los controles de acceso, manejan protocolos estandarizados como RADIUS y TACACS+. [35]

Protocolo RADIUS.- Remote Autentication Dial In User Service .- en un estándar abierto, emplea protocolo UDP, tiene contraseña y cifrado, no autoriza comandos, combina autenticación y autorización separa auditoría.

Protocolo TACACS.- Terminal Access Controller Access Control System Plus.- es un protocolo soportado por CISCO, soporta protocolo TCP, permite paquetes totalmente cifrados, separa autenticación y auditoría.

A continuación se presenta una configuración para ingreso desde una dirección remota a la configuración de un Router a través de un servidor AAA con protocolo Radius.

Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname router1
router1(config)#int fa0/0
router1(config-if)#ip address 172.19.55.254 255.255.0.0
router1(config-if)#duplex auto
router1(config-if)#speed auto
router1(config-if)#no shutdown

router1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
exit
router1(config)#int fa0/1
router1(config-if)#ip address 192.168.100.130 255.255.255.0
router1(config-if)#duplex auto
router1(config-if)#speed auto
router1(config-if)#no shutdown

router1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
exit
router1#
%SYS-5-CONFIG_I: Configured from console by console

router1#
router1#config t
Enter configuration commands, one per line. End with CNTL/Z.
router1(config)#int fa0/1
router1(config-if)#exit
router1(config)#aaa new-model
router1(config)#aaa authentication login modelo1 group radius local
router1(config)#aaa authentication login modelo2 local
router1(config)#aaa authentication enable default group radius
router1(config)#aaa authorization exec modelo1 if-authenticated
router1(config)#aaa authorization exec modelo2 if-authenticated
router1(config)#radius-server host 192.168.100.100 key admin
router1(config)#username local password admin
router1(config)#line vty 0 4
router1(config-line)#login authentication modelo1
router1(config-line)#session-limit 3
router1(config-line)#exec-timeout 30
router1(config-line)#exit
router1(config)#line console 0
router1(config-line)#login authentication modelo1
router1(config-line)#exit
router1(config)#ip domain-name aaa.com
router1(config)#crypto key generate rsa
The name for the keys will be: router1.aaa.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

router1(config)#ip ssh version 2
**mar 1 0:15:47.144: RSA key size needs to be at least 768 bits for ssh version 2*
**mar 1 0:15:47.144: %SSH-5-ENABLED: SSH 1.5 has been enabled*
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
router1(config)#line vty 0 4
router1(config-line)#transport input ssh
router1(config-line)#exit
router1(config)#exit
router1#
%SYS-5-CONFIG_I: Configured from console by console

router1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]

5.1.3 Contraseñas.

Se debe concientizar al personal involucrado en la operación y administración del sistema SCADA Local de la EERSSA que el objetivo del empleo de la contraseña es evitar que un tercero acceda al sistema con credenciales de los Operadores.[12]

Se propone que se realice cambios periódicos de contraseñas, los Operadores deben cambiar su contraseña mínimo cada tres meses [1][13], para evitar que el cambio de contraseña afecte el normal funcionamiento del Centro de Control se deberá seguir los siguientes lineamientos.

Propuesta de política de cambio de contraseñas.

- Las contraseñas deben ser de mínimo 7 caracteres.
- Las contraseñas deben contener símbolos.
- Las contraseñas no deben usar el mismo término dos veces.
- Las contraseñas no deben contener nombres propios.
- Las contraseñas no deben ser datos como fechas de nacimiento, código postal, número de identificación personal, direcciones, etc.

Es importante contar con la colaboración del personal que labora en forma directa con los equipos del SCADA Local ya que no se debe:

- Enviar la contraseña por correo.
- Anotarla en cuadernos o papeles, deben ser memorizadas.

- Conservar las contraseñas por defecto que viene en los dispositivos nuevos.

Para evitar contratiempos con contraseñas que por cualquier motivo quedan expuestas se debe cambiar de contraseña a los Operadores:

- Cada tres meses.
- Cuando exista cambio de personal encargado de la operación o administración.
- Cuando quede expuesta debido a una operación de emergencia.

Estas consideraciones deben ser socializadas con todo el personal involucrado para obtener resultados favorables, y deben contar con el apoyo del personal de administración de EERSSA.

Las políticas deben ser aprobadas por el comité de seguridad, el mismo que se encargará de verificar su implementación.

El Administrador de la red es el encargado de ejecutar o llevar a cabo la política de cambio de contraseñas ya que habilita el sistema para asignación de roles y edición de contraseñas.

Entre el personal que debe realizar sus actualizaciones de contraseñas se encuentran: Administrador de vigilancia, Operadores y Administrador de red.

Si el incidente se presenta en el sistema SCADA PLA, se reportaran al Ingeniero de operación y mantenimiento.

La dirección IP de mantenimiento con el acceso a través de IP pública debe modificarse, se plantea acceder a la dirección de mantenimiento a través de la máquina asignada en la red corporativa al Administrador de la red SCADA, de esta manera el intercambio de información será seguro.

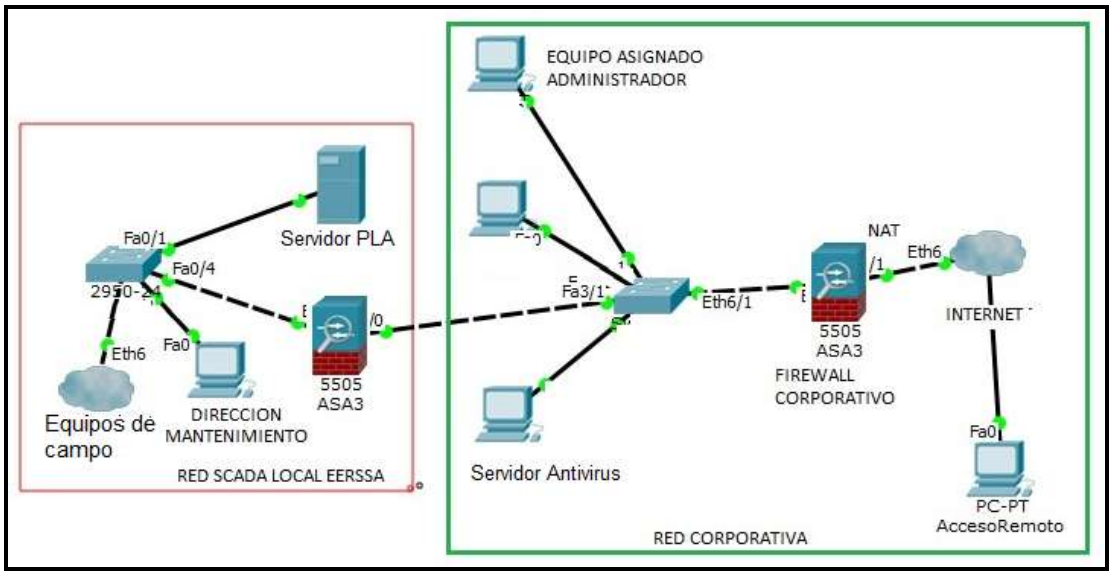

Figura 26.- *Propuesta para acceso de manera segura a la dirección de mantenimiento.*

La configuración expuesta en la Figura 26, proporciona seguridad de acceso ya que el usuario deberá ingresar por escritorio remoto a dos ambientes y cada uno de ellos con protección de contraseña.

5.1.4 Acceso físico.

El acceso a la sala de servidores, se encuentra ubicado en la parte interna del Centro de Control, la puerta de acceso se encuentra en el área de sistemas, con quienes se comparte las instalaciones, la administración del control de accesos lo realiza el Administrador del sistema de vigilancia. Al área de sistemas se le asignó dos tarjetas de ingreso,

Se debe considerar que los ingresos a la sala de servidores son frecuentes, de los que tiene cierto registro es de los autorizados por el Administrador de la Red del SCADA Local de la EERSSA.

Como se mencionó en el capítulo 4, existen equipos de otras empresas instalados en la Sala de servidores y en otras instalaciones a lo largo del área de concesión, se debe llenar un registro por cada intervención de terceros que se autorice. El registro debe contener los siguientes parámetros.

- Nombre de la empresa que hace el requerimiento de acceso.
- Nombres y Apellidos del personal que se autoriza a ingresar
- Número de credencial de la empresa o número de cédula
- Descripción de los trabajos a realizar
- Sitio al que ingresa.
- Horario de entrada
- Horario de Salida
- Contar con la autorización de la Superintendencia de Subestaciones y Comunicaciones de la EERSSA.

EMPRESA ELECTRICA REGIONAL DELSUR

GERENCIA DE OPERACIÓN Y MANTENIMIENTO

SUPERINTENDENCIA DE SUBESTACIONES Y COMUNICAIONES

Registro de Acceso a las Instalaciones de la EERSSA. Personal de otras empresas								
Fecha de ingreso	Nombre de la empresa	Nombres y Apellidos	Número de credencial o número de cédula	Descripción de los trabajos a realizar	Sitio al que ingresa.	Hora de entrada	Hora de Salida	Cuenta con autorización

Tabla 11.- *Formato para registro de ingreso de personal de otras empresas a instalaciones de la EERSSA donde se dispone de equipos de la red*

SCADA Local de la EERSSA.

Además de este registro se debe disponer a una persona de confianza del Administrador de la red SCADA Local; es decir de una persona que conozca sobre el sistema e identifique apropiadamente los dispositivos que son de la EERSSA y los que corresponden a terceros el cual debe estar informado sobre el trabajo a realizarse por el personal de la empresa que solicita el ingreso, con el fin de evitar que por errores involuntarios confundan los dispositivos o se desconecte un equipo, se evitaría que instalaran software malicioso o que conectaran un equipo de almacenamiento para descargar un archivo contaminado o extraer información.

Control Biométrico Para el Acceso Físico.-

Para garantizar que sólo personal autorizado ingrese a las instalaciones de del Centro de Control y Cuarto de Servidores del Sistema SCADA Local, se recomienda el empleo de control biométrico para el acceso físico.

La biometría es un método automático de reconocimiento de personas en base a características anatómicas, lo que garantiza la identificación. Las muestras de los patrones que se almacenan en la memoria de los equipos biométricos se toman con la ayuda de sensores, esta información es contrastada cada vez que el personal quiere ingresar y si no consta en la base de datos el acceso es denegado.

El empleo de elementos biométricos permite eliminar la suplantación de identidad de las personas, aumentando los niveles de seguridad, además evita problemas que se pueden presentar por robo de: llaves, tarjetas de ingreso, o claves.

Actualmente existen varios tipos de lectores biométricos basados en los indicadores de individualidad podemos citar algunos:

Huella digital
Rostro
Geometría de la mano

Iris

Voz

Para el acceso al centro de control se recomienda el empleo del indicador biométrico de rostro, ya que es uno de los más aceptados al no requerir contacto físico con el equipo lector y no se considera invasivo.

El control biométrico permite gestionar automáticamente los accesos al emitir reportes periódicos.

5.1.5 Almacenamiento y Respaldo de información crítica.

Mantener una copia o respaldo de las configuraciones de los dispositivos que forman parte de la red SCADA Local de la EERSSA, ayudará a gestionar de mejor manera la administración y a minimizar tiempos de recuperación de equipos en caso de fallas de funcionamiento sea por error de hardware o porque haya sufrido un ataque de virus que comprometa su configuración.

Para garantizar que las copias sean confiables se debe adjuntar por cada archivo de respaldo generado un registro que identifique el objetivo de la configuración o actualización, esto con la finalidad que si se debe regresar a un respaldo anterior se tenga certeza de los cambios que se debe realizar para volver a mantener el sistema funcionando.

Registro de Configuración de respaldo de proyecto PLA			
Fecha	Nombre de Archivo	Almacenamiento	Motivo de actualización

Tabla 12.- *Tabla propuesta para registro de configuraciones que se realicen en el Sistemas SCADA Local PLA.*

Registro de Configuración de respaldo de proyecto de RTU			
Fecha	Nombre de Archivo	Almacenamiento	Motivo de actualización

Tabla 13.- *Tabla propuesta para registro de configuraciones que se realicen en los dispositivos remotos.*

Por cada equipo configurado, se debe llevar un detalle documentado de los cambios que se generen, se debe registrar cada vez que se realice un cambio o actualización, como ejemplo se presentan las Tablas 12 y 13 para las configuraciones de las RTU (Unidad Terminal Remota) y Proyecto SCADA Local (PLA PowerLink Advantage), configuraciones que se modifican en forma permanente ya sea porque se integra un nuevo IED (Dispositivo Electrónico Inteligente) o equipo de campo. Los registros de estas configuraciones deben ser llenados con la fecha en la que entran en funcionamiento.

Para realizar las copias o respaldos de los equipos del Centro de Control se debe considerar.

- La información a respaldar.
- Medios de Almacenamiento.
- Frecuencia con la que se debe hacer el respaldo.

En la Tabla 14, se presenta la frecuencia y el medio de almacenamiento que se propone para garantizar copias confiables.

Propuesta para Registros de Respaldo			
Configuración	Requiere Respaldo	Almacenamiento	Frecuencia
Proyecto PLA	Si	NAS	Cada actualización
Remota	Si	NAS	Cada actualización
Servidor Principal	Si	DVD/NAS	Anual
Servidor Respaldo	Si	DVD/NAS	Anual
Servidor Históricos	Si	DVD/NAS	Anual
Servidor de Vigilancia	Si	DVD/NAS	Anual
Servidores ICCP	Si	DVD/NAS	Anual
Firewall	Si	NAS	Actualización
Switch	Si	NAS	Actualización
Switch de Subestación	Si	NAS	Actualización
Grabadores de video	Si	NAS	Actualización
Consola de Operación PLA	Si	DVD/NAS	Anual
Consola de vigilancia	Si	DVD/NAS	Anual
Consola de Comunicaciones	Si	DVD/NAS	Anual
Consola EMS	Si	DVD/NAS	Anual

Tabla 14.- *Propuesta para adquisición de respaldos*

Para obtener las imágenes de los discos duros, se debe emplear un software que permita elegir el destino de la copia de seguridad, que reallice copias totales, incrementales o diferenciales, entre los Software disponibles se encuentran entre otros:

- Acronis True Image
- Norton Ghost
- Cobian Backup

Para almacenar esta información se debe contar con medios que garanticen la confiabilidad de la información respaldada y que está estará disponible cuando se la requiera, para contar con un respaldo las imágenes de disco de los equipos del Centro de Control y de las Subestaciones se deben almacenar en DVD debido a que ofrecen gran capacidad de almacenamiento, también se propone concentrar las copias en un mismo dispositivo de almacenamiento denominada NAS (Network Attached Storage) que permite concentrar en un solo equipo todas las copias de las configuraciones y proteger su acceso con contraseñas, su conexión a la red permite que la obtención de los respaldos sea directa a cada uno de los equipos.

Si se opta por el empleo de un dispositivo NAS, esté debe ser gestionado por el Ingeniero Administrador del sistema, las claves de acceso serán manejadas por el Ingeniero Superintendente de Subestaciones y el Administrador de la red. Estará instalado en el cuarto de servidores y las copias se almacenaran según la propuesta presentada en la Tabla 14. la revisión de los respaldos se realizará cada mes. Para la elección del dispositivo NAS se tomará en cuenta la capacidad de almacenamiento y velocidad del procesador, su empleo será exclusivo para almacenamiento de archivos de respaldo de dispositivos conectados en red.

La obtención de las copias de seguridad se realizará con el software de NAS, tratando en lo posible que sea lo más automático posible a fin de evitar errores humanos, en el caso de los respaldo de los proyectos PLA y configuraciones de RTU se conectaran los dispositivos portátiles a la red para obtener los archivos de las últimas configuraciones.

El acceso a estas copias de seguridad debe ser gestionada por la Superintendencia de Subestaciones y comunicaciones de la EERSSA y por el ingeniero de telecomunicaciones que es el encargado de administrar la red SCADA Local.

5.1.6 Software malicioso (Virus).

Debido a que la recomendación del proveedor del sistema fue no instalar antivirus en los servidores, se debe tratar de evitar exponer la red a contaminación para ello se debe contar con el compromiso pleno de todos los usuarios de los equipos de la red SCADA de la EERSSA.

Para evitar que archivos maliciosos ingresen por medios extraíbles de entrada USB, por ejemplo Pen Drive o también llamadas flash memory, se debe bloquear el acceso de estos dispositivos en las consolas del Centro de Control y en los grabadores de video instalados en las Subestaciones.

Se debe comprometer al personal de la Superintendencia de Subestaciones y Comunicaciones a emplear los computadores portátiles, destinados para configuración de RTU y proyecto SCADA Local, solamente para estas actividades, lo que evitará que los equipos se carguen con software que debe actualizar periódicamente por internet se evitará también el empleo de dispositivos de almacenamiento para el intercambio de archivo entre estos computadores y hosts de la red corporativa. Estos equipos portátiles serán los únicos autorizados a conectarse temporalmente en los Switch de las Subestaciones en un puerto asignado por el Administrador de la red.

Cuando se integra un nuevo dispositivo o se adiciona señales de monitoreo al Sistema SCADA se emplea el computador portátil de desarrollo el cual se conecta directamente a campo y luego de realizar las pruebas respectivas se aprueba el proyecto para ser actualizado en los servidores, esto se realiza a través de un pen drive. Este pen drive se debe emplear sólo para este propósito, con el fin de que no contamine de malware los servidores.

Para completar el análisis de introducción de virus, se consultó con Autotrol, (compañía que implementó el sistema SCADA Local de la EERSSA), si existen actualizaciones del Software que permitan la instalación de antivirus en los equipos que conforman la red SCADA, contestaron que para la

versión PLA que maneja la EERSSA aún no se aconseja instalar en los servidores antivirus pero si en los clientes incluido la consola de mantenimiento.

En la actualidad se encuentran a disposición varios antivirus para aplicación en sistemas de control industrial los cuales trabajan a la par con empresas proveedoras de sistemas SCADA Local, entre los antivirus desarrollados para sistemas de control industrial se puede citar a McAfee, Eset.

5.2 POLITICAS DE SEGURIDAD

Observada la estructura de red del sistema SCADA Local de la EERSSA, y realizadas las pruebas de acceso proponemos considerar la implementación de políticas y procedimientos a llevar a cabo para mejorar la seguridad del sistema.

Basados en RFC 1244, se debe suponer varios aspectos para determinar una política de seguridad, se debe considerar la operación del sistema y el personal involucrado [26].

Para establecer las políticas de Seguridad los aspectos a considerar son:

- Considerar que se va a proteger la integridad y disponibilidad del sistema SCADA Local de la EERSSA.
- Considerar que se debe proteger de accesos no autorizados y denegaciones de servicio.
- Determinar las amenazas y sus probabilidades de ataque.
- Buscar una manera rentable de poner en práctica las medidas de seguridad considerando que la disponibilidad no debe verse afectada.
- Revisar continuamente los procesos para evidenciar debilidades y tomar correctivos.

En base a la norma ISO 27002 se proponen las políticas de seguridad a implementarse con la intención de mejorar la Seguridad del Sistema SCADA Local de la EERSSA, como referencia se consideran las cláusulas para adaptarlas al Sistema SCADA Local.

1. Política de Seguridad de la Información. [45]
2. Organización de la Seguridad de la Información.
3. Gestión de Activos de Información.
4. Seguridad de los Recursos Humanos.
5. Seguridad Física y Ambiental.
6. Gestión de las Comunicaciones y Operaciones.
7. Control de Accesos.
8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
9. Gestión de Incidentes en la Seguridad de la Información.
10. Gestión de Continuidad del Negocio.
11. Cumplimiento.

Antes de iniciar con las políticas de seguridad se identificará la misión, según el Manual de Clasificación de Puestos de la EERSSA [29], de los Directivos involucrados.

Gerente de Operación y Mantenimiento.- *Programación organización, dirección, supervisión y control de las actividades relacionadas con la producción, transporte y distribución de energía eléctrica. Supervisado por el Presidente Ejecutivo.*

Superintendente de Subestaciones y Comunicaciones*.- Programación organización, dirección, supervisión y control de las actividades de operación y mantenimiento de las subestaciones del Sistema y de los Equipos de Comunicación. Supervisado por el Gerente de Operación y Mantenimiento.*

Superintendente de Líneas y Redes Zona 1 y Zona 2.- *Programación organización, dirección, supervisión y control de Trabajos de operación y mantenimiento de los sistemas de Subtransmisión y Distribución. Supervisado por el Gerente de Operación y Mantenimiento.*

Superintendente de Sistemas.- *Programación, organización, dirección y control de las actividades informáticas de la Empresa. Supervisado por el Presidente Ejecutivo.*

Adicionalmente identificamos a los Ingenieros que laboran en la Superintendencia de Subestaciones y Comunicaciones, departamento que tiene a cargo la Administración del sistema SCADA Local y están supervisados por el Superintendente de Subestaciones y Comunicaciones.

Ingeniero 1 Telecomunicaciones.- Se encarga del sistema de comunicación de voz, sistema de comunicación de datos del Sistema SCADA Local, adicionalmente es el Administrador de la red SCADA Local de la EERSSA.

Ingenieros 1 de Operación y Mantenimiento.- Se encargan de las funciones operativas del sistema eléctrico de potencia y de la Administración del sistema de Vigilancia e integraciones de nuevos equipos de campo.

Operadores del Centro de Control.- Personal encargado del monitoreo y operación del sistema eléctrico de potencia a través del sistema SCADA Local, laboran en horario de turnos para cubrir la disponibilidad 24/7.

5.2.1 Políticas de Seguridad.

5.2.1.1 Documento de la Política de Seguridad de la Información.

- **Objetivos de la Políticas de Seguridad**

I.- Proteger los recursos del Sistema SCADA Local de la EERSSA, la tecnología para su operación garantizando su disponibilidad, confidencialidad e integridad, frente a amenazas internas o externas, intencionadas o accidentales.

II.- Asegurar que la políticas se implementen adecuadamente con la colaboración de la administración de la EERSSA y el personal involucrado en su operación.

III.- Vigilar que las políticas se encuentren actualizadas a fin de evitar acciones que pongan en riesgo la disponibilidad del sistema.

5.2.1.2 Revisión de la Política de Seguridad.

La revisión de estas políticas debe realizarse según la Norma ISO 27000, cumpliendo con las etapas de planificación, implementación, seguimiento y mejora continua.

La revisión de estas políticas se realizará en un periodo de 12 meses, tiempo en el cual se irá registrando las incidencias que se presenten y realizando pruebas de hacking con el fin de detectar las posibles vulnerabilidades.

En la figura 27, se presenta un esquema de implantación de las políticas para el sistema SCADA Loca de la EERSSA.

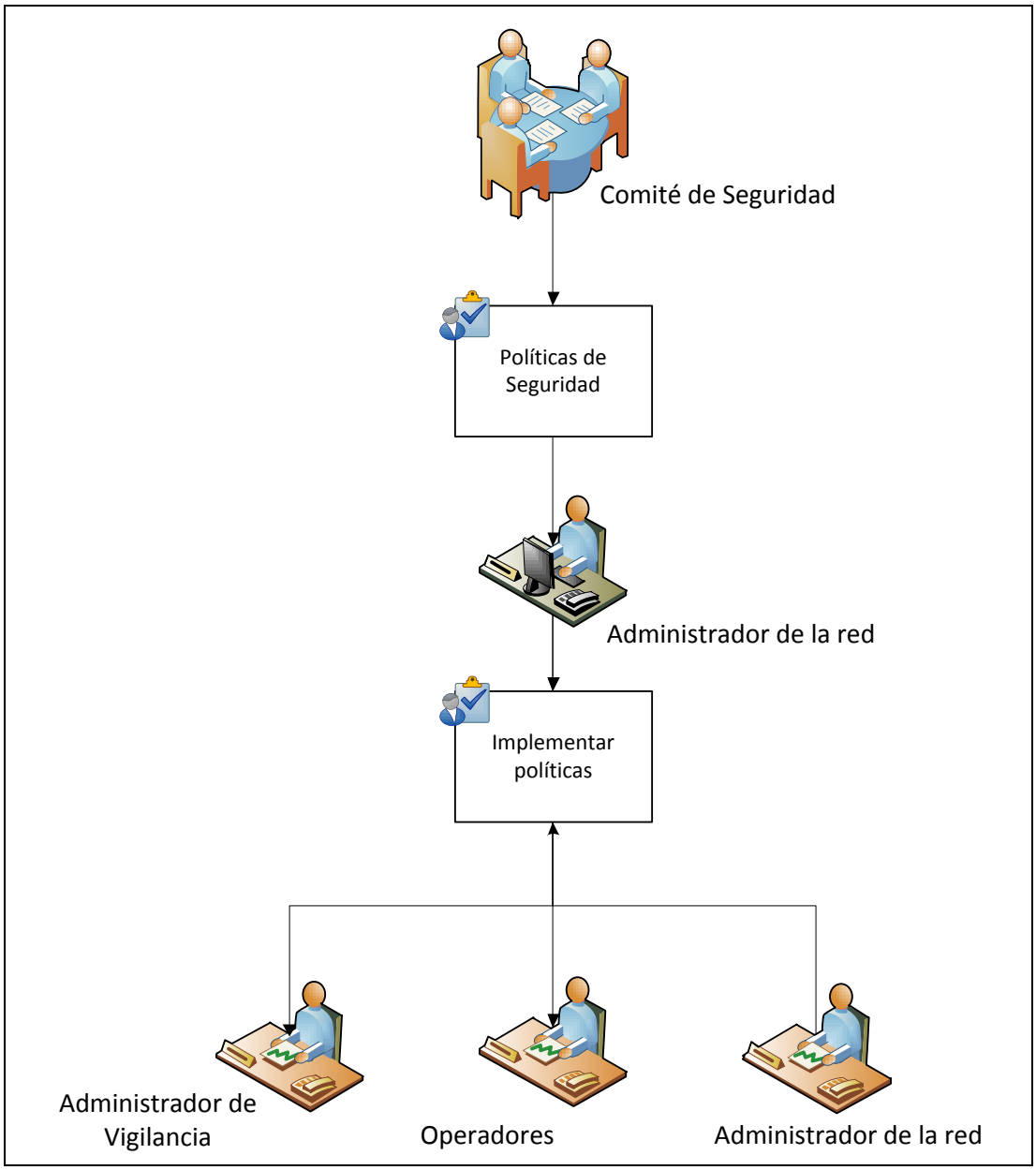

Figura 27.- *Esquema de procedimiento a seguir para la implantación de políticas para el sistema SCADA Local de la EERSSA.*

5.2.2 Política de Aspectos Organizativos de la Seguridad.

5.2.2.1 Infraestructura de Seguridad del Sistema SCADA Local de la EERSSA

Comité de Seguridad.- Debe estar integrado por el Administrador de la red, el Superintendente de Subestaciones y comunicaciones, Superintendente de las Zona 1 y Zona 2 de Operación y Mantenimiento.

Este comité tiene como funciones:

I.- Revisar y proponer al Gerente de operación y mantenimiento y a los directivos de EERSSA, las políticas de seguridad a implementarse en el Centro de Control de la EERSSA

II.- Monitorear los riesgos o posibles amenazas, sean internas o externas, que afecten la disponibilidad del sistema SCADA Local de la EERSSA.

III.- Conocer sobre los incidentes que se presenten en la seguridad del sistema SCADA, aprobar y supervisar la aplicación de procesos para solventarlos.

IV.- Promocionar las políticas de seguridad y comprometer al personal de su aplicación.

5.2.2.2 Asignación de responsabilidades.

Dentro del comité de Seguridad se plantean las responsabilidades de sus miembros.

El Administrador de la red SCADA Local se encargará de difundir las políticas a los usuarios directos del sistema SCADA Local, estará pendiente de su ejecución y a él se le reportarán las incidencias. Estará a cargo de asignar los accesos autorizados, por roles a los usuarios del Sistema SCADA.

Los roles definen las responsabilidades y alcances dentro de la configuración y operación del sistema SCADA Local.

Los Roles son:

Rol de Administrador.- Permite acceder a la configuración del proyecto SCADA, por ejemplo integrar o eliminar señales de monitoreo, habilitar y deshabilitar las solicitudes de interrogación a los dispositivos de campo, asignar roles.

Usuarios con rol de Administrador

Sistema SCADA Local,

- Superintendente de Subestaciones y Comunicaciones.
- Ingeniero 1 de Operación y Mantenimiento, Subestaciones
- Ingeniero 1 de Telecomunicaciones

Sistema Vigilancia.

- Superintendente de Subestaciones y Comunicaciones.
- Ingeniero 1 de Operación y Mantenimiento, Vigilancia

Sistema Monitoreo de Subestaciones,

- Superintendente de Subestaciones y Comunicaciones.
- Ingeniero 1 de Telecomunicaciones

Rol de Operador: Este rol permite operar el sistema, reconocer alarmas, enviar comandos, permitir accesos. No interviene en la configuración de los sistemas.

Usuarios con rol de Operador.

Sistema SCADA Local.

- Operadores el Centro de Control.

Sistema Vigilancia

- Operadores del Centro de Control.

Sistema Monitoreo de Subestaciones,

- Operadores del Centro de Control.

Estos roles se asignan a los Operadores del Centro de Control que laboran con disponibilidad 24/7, los cuales cumplen horarios de turnos rotativos de 8 horas.

Rol de Observador: Este rol permite al usuario observar el comportamiento de los sistemas, no tiene acceso a operación alguna, ni a configuración de los dispositivos.

Usuarios con rol de Observador.

Rol de Observador:

- Superintendente de Zona 1 de Operación y Mantenimiento
- Superintendente de Zona 2 de Operación y Mantenimiento

5.2.2.3 Información entregada a Terceros

La información que se almacena en los históricos del sistema SCADA Local es fundamental para el análisis del comportamiento del Sistema Eléctrico de Potencia por ende es requerida por otros departamentos de la EERSSA.

- La información de históricos se descargará semanalmente cada domingo en formato .csv, Cada archivo contendrá la información de valores analógicos de los últimos 15 días.
- Estos archivos se almacenarán en el servidor de históricos y existirá una conexión a la consola de gestión de protecciones.
- Estos archivos se copiaran cada lunes a las 08h00 a través de red a un computador conectado a la red corporativa desde donde cualquier dependencia de la EERSSA pueda consultar la información; esta acción la realizará el Ingeniero 1 de Operación y Mantenimiento de Subestaciones.

5.2.3 Política de Gestión de Activos.

5.2.3.1 Responsabilidad sobre los activos.

La gestión de los conmutadores, cortafuegos, servidores PLA estará a cargo del ingeniero administrador del sistema, será el que maneje las claves de acceso a las configuraciones y administre las VLAN y ACL.

Las consolas de operación del Centro de Control permanecerán activas en disponibilidad 24/7, estas consolas serán de uso estricto del Sistema SCADA Local.

Cada Operador contará con una clave de acceso e ingresará cada vez que inicie el turno,

En las consolas y en los servidores no se debe instalar software que no corresponda a los sistemas del SCADA Local.

Los portátiles de desarrollo contendrán el software correspondiente al sistema SCADA Local, y se empleará un equipo pen drive exclusivo para la transferencia de información entre los servidores y las portátiles.

5.2.3.2 Etiquetado.

Todos los activos que forman parte de la red SCADA Local de la EERSSA deben estar identificados adecuadamente, en el Centro de Control las consolas deben contener una etiqueta que las identifique para evitar confusiones operativas.

En el cuarto de servidores se tendrá identificado los racks que pertenecen al Sistema SCADA Local y los armarios que corresponden a la Superintendencia de Sistemas, del mismo modo se solicitará a las empresas que instalen equipos en el cuarto de servidores que estos se encuentren debidamente etiquetados para evitar confusiones.

En las subestaciones se tendrá identificados adecuadamente los equipos de Red (Networking) y los equipos de maniobra de Campo. (Interruptores, Seccionadores, etc)

Los conmutadores y cortafuego (switches y firewall) deben tener identificadas las conexiones en cada uno de los puertos con una nomenclatura clara la cual debe estar registrada en una base de datos que será administrada por el Ingeniero de Telecomunicaciones.

5.2.4 Política de Seguridad del Personal.

5.2.4.1 Antes del empleo.

La Gerencia de Operación y Mantenimiento realizará las solicitudes para contratación de personal o creación de partidas nuevas. La Superintendencia Administrativa conjuntamente con el departamento de Asesoría son los encargados de la selección del personal y la elaboración de los contratos de trabajo.

Antes de la contratación el personal postulante deberá cumplir con los requisitos y evaluaciones que constan en el reglamento interno de la EERSSA.

Cuando este habilitado para integrarse a sus funciones se le asignará el horario a cumplir, las claves de acceso al sistema y la tarjeta de acceso al Centro de Control.

5.2.4.2 Durante el empleo.

La Superintendencia de Subestaciones, encargada de la administración del Sistema SCADA Local de la EERSSA, asignará las funciones del personal en base a los requerimientos de operación del Sistema SCADA Local, realizará la inducción de las funciones a realizar y lo presentará con el personal que labora en el Centro de Control, y la Superintendencia.

El personal de Subestaciones Ingeniero 1 de Operación y Mantenimiento en conjunto con el Ingeniero 2 de Protecciones y el Superintendente, elaboraran y revisaran cada 6 meses los procedimientos de operación del Sistema Eléctrico de Potencia. Estos procedimientos serán entregados a los compañeros Operadores y a los Superintendentes de Operación y Mantenimiento Zona 1 y Zona 2; encargados del monitoreo y operación del Sistema Eléctrico de Potencia de la EERSSA.

El comité de Seguridad coordinará capacitaciones de concientización sobre seguridad, cada año o cuando se tenga ingreso de personal nuevo, donde se abarque temas de responsabilidades en el cumplimiento de las políticas de seguridad y los riesgos legales que conlleva su incumplimiento.

Se solicitará al departamento médico que se realice chequeos psicológicos anuales al personal que labora en turnos rotativos con el fin de identificar posibles resentimientos laborables que pongan en riesgo la seguridad del Sistema SCADA Local.

5.2.4.3 Cese del Empleo.

Si por causas operativas del sistema se necesita prescindir de un recurso humano, o si personal que se encuentra laborando presenta su renuncia sea porque realiza un cambio administrativo (es decir laborará en otra área de la EERSSA), cambiará de empresa (laborará fuera de la Institución), o se acoge al beneficio de la jubilación, se tomarán las siguientes acciones.

- Se realizarán los procedimientos de separación o cese de funciones vigentes en el reglamento interno de la EERSSA
- Se notificará mediante correo y mensajero institucional, el cambio de dependencia o retiro de la empresa, para que todo el personal de la EERSSA tenga conocimiento. Además en la próxima reunión de seguridad Industrial se indicará a los trabajadores de la EERSSA, la separación del recurso humano de la operación del SCADA Local.
- Se retirará los accesos autorizados, para ello se retirará la tarjeta de acceso y se comunicará a todo el personal que si el personal que acaba de retirarse requiere acceder a las instalaciones debe solicitar autorización siguiendo los procesos de ingreso a particulares indicados en la política de acceso físico.
- Se cancelará el usuario y clave de acceso de los sistemas de Monitoreo y control SCADA Local (PLA), sistema de Vigilancia, de Gestión de comunicaciones, de los Switch, firewall.

- Se cambiará la clave de acceso del correo y del mensajero institucional genéricos que es de dominio de todos los que laboran en el Centro de Control.
- Se realizará una actualización de contraseñas según se indica en la Política de control de Accesos.

5.2.5 Política de Seguridad de Acceso físico.

5.2.5.1 A las instalaciones de la EERSSA.

Los controles de acceso al Centro de Control y sala de servidores estarán a cargo del Administrador del sistema de vigilancia, pero el Administrador de la red SCADA Local será el que autorice los ingresos a las instalaciones donde se disponga de equipo de networking correspondiente al Sistema SCADA Local.

Para la autorización del ingreso de personal propio de la EERSSA, se debe solicitar por parte del Operador del Centro de Control el siguiente registro.

- Nombres y Apellidos del personal que ingresa.
- Nombre de área que autoriza el ingreso.
- Descripción del trabajo a realizar
- Sitio al que ingresa
- hora de entrada
- hora de salida

Si personal de otras instituciones o particulares desean ingresar a las instalaciones de la EERSSA, deben presentar una solicitud al Administrador de la red, con 48 horas de anticipación a la fecha de ingreso, el cual analizará los trabajos a realizarse y evaluará si se procede con la autorización, además alertará a los Superintendentes de Zona 1 y 2 de los trabajos que se ejecutaran a fin de no obstaculizar tareas que estén realizando.

En base a ese análisis el Gerente de Operación y Mantenimiento autorizará el ingreso, se llevará un registro que contendrá la siguiente información.

- Nombre de la empresa Solicitante.
- Nombre y Apellidos del personal que ingresa
- Número de cédula
- Descripción de los trabajos.
- Sitio al que ingresa.
- Hora de entrada
- Hora de Salida
- Número de autorización de la EERSSA.

Estos formatos serán registrados por los Operadores del Centro de Control, los cuales recibirán, con 24 horas de anticipación, de parte del Administrador de la red la autorización del ingreso y constatarán que coincida con el registro de entrada.

Los ingresos autorizados contarán además con el nombre del personal de confianza designado por el Ingeniero de Telecomunicaciones (Administrador del Sistema SCADA Local), para que asista o acompañe a la realización de los trabajos.

5.2.5.2 Al Centro de Control

Debido a que la función principal del Centro de Control es el monitoreo y control del Sistema Eléctrico de Potencia de la EERSSA, y con el objetivo de no entorpecer esta actividad y no incrementar tiempos de operación el acceso al Centro de Control se limitará a: los Operadores que estén de turno, al Superintendente de Subestaciones que está a cargo del sistema, a los Administradores de la red SCADA Local y Administrador de Vigilancia.

Si otra área de la empresa necesita información del sistema en tiempo real deberá solicitarla por medio de correo electrónico.

5.2.5.3 Al Cuarto de Servidores.

El ingreso al cuarto de Servidores se realizará en común acuerdo entre las dependencias de las Superintendencias de Subestaciones y Superintendencia de Sistemas.

Si se requiere el ingreso de personal interno de la EERSSA se llevará un registro que contendrá:

- Nombres y Apellidos del personal que ingresa.
- Nombre de área que autoriza el ingreso.
- Descripción del trabajo a realizar
- Sitio al que ingresa
- hora de entrada
- hora de salida.

La solicitud debe presentarse mínimo 5 horas antes de la intervención y será autorizada por la Superintendencia que no solicita el ingreso, este registro será archivado y administrado por las dos dependencias.

Si personal de otras instituciones o particulares requieren ingresar al cuarto de servidores se pondrá a disposición de las dos Superintendencias la solicitud para ello se debe presentar una solicitud con 72 horas de anticipación, la autorización se realizará en 48 horas y la aprobación se dará a conocer con 24 horas a la empresa solicitante y al Centro de Control, se registrarán los siguientes datos.

- Nombre de la empresa Solicitante.
- Nombre y Apellidos del personal que ingresa
- Nombre y Apellidos del Personal de EERSSA (asistencia)
- Número de cédula
- Descripción de los trabajos.
- Sitio al que ingresa.
- Hora de entrada
- Hora de Salida
- Número de autorización de la EERSSA

El personal de confianza que acompañe a este personal durante su trabajo será designado por la Superintendencia que administra el convenio con la institución solicitante ya que es la dependencia que lleva el convenio de cooperación o alquiler de servicios y tiene conocimiento de los equipos en los que deben intervenir.

5.2.6 Política de Gestión de Comunicaciones y Operaciones.

5.2.6.1 Procedimientos de Operación.

Para el adecuado funcionamiento del Sistema Eléctrico de Potencia se elaborarán los manuales de procedimientos de operación.

- Manual de Procedimiento para un Colapso parcial del sistema
- Manual de Procedimiento para un Colapso total del sistema
- Manual de Procedimiento de Operación normal del sistema SCADA Local.
- Manual de Procedimiento de revisión del sistema de vigilancia en operación normal.
- Manual de Procedimiento de revisión del sistema de vigilancia en caso de contingencia.

- Manual de Procedimiento de revisión del sistema de telecomunicaciones en operación normal.
- Manual de Procedimiento de revisión del sistema de telecomunicaciones en caso de contingencia.
- Manual de procedimiento para cambio de turno.

Estos manuales se revisarán cada seis meses, en caso de actualización se cambiará el documento el cual será identificado por el número de revisión.

Estos manuales serán elaborados por los Ingenieros de cada sistema, se revisaran por el Superintendente y su aprobación la realizará el Gerente de Operación y Mantenimiento.

En estos manuales se especificarán todas las funciones asignadas a los Operadores, Ingenieros de Turno y Administradores de Sistemas de SCADA Local, Vigilancia y Telecomunicaciones.

5.2.6.2 Servicios prestados por terceros.

De Mantenimiento.

El mantenimiento de los dispositivos del Centro de Control estará a cargo de los administradores de cada sistema (PLA, Vigilancia, Telecomunicaciones).

Si se requiere la asistencia de personal especializado el administrador del sistema será el que gestione ante la Superintendencia de Sistemas para una revisión de los elementos informáticos, la asistencia se realizará en el sitio de instalación del dispositivo y se coordinará oportunamente para realizarla junto con el Administrador de la red.

Si se necesita dar mantenimiento con personal técnico especializado particular, se solicitará en lo posible que se realice dentro de las instalaciones de la EERSSA en compañía de personal de sistemas que

solicitó la revisión para ello se coordinará las autorizaciones de acceso previas.

De Transmisión de Datos.

En sitios donde la EERSSA no dispone de infraestructura propia de telecomunicaciones se cuenta con servicio prestado por otras compañías.

Se llevará un registro de la disponibilidad de los canales de comunicación para verificar si cumplen con los estándares para garantizar la continuidad del servicio, estos registros será administrados por el ingeniero de Telecomunicaciones, se debe mantener reuniones permanentes con los suministradores de servicio para revisar las configuraciones de seguridad.

5.2.6.3 Protección contra código malicioso.

Las consolas de operación serán de uso exclusivo para operación del sistema, la actualización de información entre Servidor de sistemas y Clientes debe realizarse a través de red que se encuentra aislada de la corporativa.

La computadora de gestión de protecciones que tiene conexión a la red corporativa contará con la instalación del antivirus institucional, esta computadora tendrá restringido el acceso a internet, sólo accederá a las páginas del CENACE para envío de información de centrales, los puertos USB estarán bloqueados.

Los Operadores tendrán usuarios restringidos en esta máquina no podrá compartir archivos por red sólo los que el administrador autorice, el correo también estará restringido al dominio de CENACE, EERSSA, CELEC para envío y recepción de información.

5.2.6.4 Almacenamiento de Respaldos.

Se debe guardar respaldos de las configuraciones de los siguientes equipos**.**

- Firewall.
- Switch.
- Unidades terminales remotas (RTU).
- Proyecto SCADA Local PLA.
- Radios de comunicación de datos

Los respaldos deben realizarse inmediatamente luego de poner en operación la configuración del dispositivo.

Con asistencia de personal del área de sistemas, respaldar con imágenes de disco:

- Servidor Principal y Respaldo PLA.
- Servidor de Históricos y de Monitoreo de Comunicaciones.
- Servidor de Vigilancia
- Consolas de operación
- Grabadores Video

Cada respaldo debe registrase con una nota adscrita en donde se describa los cambios que se realizaron, a fin de llevar un registro de cambios.

Estos respaldos deberán almacenarse en unidades DVD o en una unidad NAS (Network Attached Storage), el acceso a estos respaldos será restringido con contraseña. Administraran la unidad NAS el Superintendente de Subestaciones y Comunicaciones y el Administrador de la Red SCADA.

Se debe revisar periódicamente, cada 3 meses, el estado de estos archivos, así, si en caso de emergencia se necesita recurrir a ellos, estén disponibles y funcionales.

5.2.6.5 Seguridad de Redes.

El Ingeniero de Telecomunicaciones revisará permanentemente la configuración de la red, cada vez que se autorice un acceso monitoreará la actividad de los puertos de los switch (conmutadores) y firewall (cortafuegos).

Se implementarán VLANs (Virtual Local Area Networks) y ACLs (Access Control Lists) para limitar el acceso no autorizado a través de red a los sistemas y permitirá gestionar de mejor manera el tráfico de red estas configuraciones serán administradas por el Ing. de Telecomunicaciones.

5.2.6.6 Política de contraseñas.

Definidos los roles se debe proceder a cambiar las contraseñas por defecto en los servidores del SCADA Local, de Vigilancia, de monitoreo de Comunicaciones e Históricos, de igual manera en las consolas de operación de los sistemas antes mencionados. Además se debe proteger con contraseñas las configuraciones de cortafuegos, conmutadores, paneles de Acceso, grabadores de video, computadores portátiles de configuración de RTU y SCADA PLA

Las contraseñas deben seguir los siguientes lineamientos.

- ✓ Contener como mínimo 7 caracteres.
- ✓ Contener por lo menos un símbolo de puntuación.
- ✓ No deben contener nombres del usuario.
- ✓ No deben contener fechas de nacimiento, números de cédula, direcciones.

Cada sistema (PLA, Vigilancia What Up) y equipo (conmutador, firewall, servidores, Consolas) tendrá una contraseña por usuario, definidos privilegios por el rol que desempeñen,

Las contraseñas son de uso personal, y se deben cambiar mínimo cada 3 meses, o cuando exista cambio de personal de administración u operación. el cambio de la contraseña estará a cargo del administrador de la red y supervisada por el Ing. Superintendente de Subestaciones y Comunicaciones.

Cada usuario tendrá que mantener seguros los mecanismos de control de acceso que se le proporcione, esto incluye Nombre de Usuario, Contraseña para acceder a las consolas de monitoreo del Sistema SCADA. Es de total responsabilidad del usuario el buen uso y confidencialidad de su control de acceso, no debe compartirlo, divulgarlo o remitirlo por correo, debe estar consiente que toda actividad registrada por su usuario y contraseña será cargado a su historial de operación.

El nombre del usuario para el acceso a las consolas será único es decir cada usuario tendrá un nombre de usuario diferente.

5.2.7 Política de Seguridad en los procesos de Desarrollo.

Cuando se habilite una nueva función en los equipos de protección o se instale dispositivos de campo se debe actualizar el proyecto SCADA Local o PLA

- Se debe respaldar el proyecto vigente, para tenerlo de respaldo.
- Se instalará el proyecto en la computadora de desarrollo de PLA.
- Se integrarán las señales nuevas al sistema.
- Se realizarán las pruebas respectivas en campo con la computadora de desarrollo.
- Luego de probado el proyecto se trasladará a los servidores.

Los procedimientos anteriores también se aplicarán a las actualizaciones de configuración del conmutador y cortafuegos.

5.2.8 Política de Gestión de Incidentes.

Cuando se presente un incidente que genere retardo en la operación o pérdida de comunicación con cualquier dispositivo, se debe informar inmediatamente al Administrador

Debe informarse de manera concreta y con estampa de tiempo, solamente se coordinará las acciones a tomar con los administradores a fin de no acrecentar el inconveniente por manipulación errada.

Los incidentes que se deben reportar según ISO 27002 son: [45]

a) pérdida del servicio, equipo o medios;
b) mal funcionamiento o sobrecarga del sistema;
c) errores humanos;
d) incumplimientos de las políticas o lineamientos;
e) violaciones de los acuerdos de seguridad física;
g) mal funcionamiento del software o hardware;
h) violaciones de acceso.

Si el incidente se presenta en el sistema SCADA PLA, se reportaran al Administrador de la red el cual luego del análisis lo asignará a operación del SCADA Local, Telecomunicaciones o Vigilancia.

Todo el personal involucrado en la operación del sistema tiene que reportar los eventos de seguridad o de vulnerabilidades del sistema.

Se debe llevar un registro por cada evento a fin de contar con un histórico de consulta en caso de ocurrir o presentarse nuevamente el incidente, además se debe socializar con todos los involucrados en la operación luego de solucionarlo.

Para llevar un mejor control de los incidentes se propone la creación de un Equipo de Respuesta a Incidentes de Seguridad CSIRT (Computer Security Incident Response Team). El equipo CSIRT requiere de estudio de la tecnología, de procesos y personal que conformen un grupo de trabajo de conocimiento científico y legal

La conformación de un CSIRT permite:

- Disponer de una coordinación especializada que ayuda a mitigar y evitar incidentes graves dentro del correcto funcionamiento del Sistema SCADA Local de la EERSSA.
- Mejorar el tiempo de respuesta en la solución de incidentes presentados en el Sistema SCADA Local de la EERSSA.

El CSIRT interno estará conformado por el administrador de la red SCADA Local de la EERSSA como Director. Con el apoyo del personal de la Superintendencia de Sistemas se conformará el equipo de técnicos investigadores.

Este equipo tendrá a su cargo la elaboración de:

- Plan de respuesta a incidentes.
- Reporte de recolección de evidencia forense de un incidente.
- Plan de Contingencia

- **Plan de respuesta a incidentes.-** Basados en la gestión de incidentes abarca la recepción de notificaciones de parte de los usuarios del sistema para ordenar y responder según la importancia de los eventos, con acciones que permitan mitigar las amenazas.
  Para ello realizará una valoración de:

- **Recolección de evidencia forence.-** Se considera evidencia forence a cualquier archivo u objeto encontrado en un sistema que pudiera ser parte de una amenaza o ataque. [33].

El grupo de técnicos investigadores serán los encargados de recopilar la información a ser analizada por el CSIRT interno de la EERSSA, así mismo será su responsabilidad su adecuado almacenamiento a fin de no comprometer o adulterar la evidencia.

- **Plan de contingencia.-** Permite iniciar el proceso de recuperación y prevención de futuros incidentes. Se elabora luego de la evaluación de la información presentada en la denuncia del incidente y la evidencia forence encontrada.

5.2.9 Política de Gestión de la continuidad del Negocio.

Cada mes se realizará un mantenimiento general de las consolas y servidores de los sistemas.

Este mantenimiento tendrá como objetivo monitorear la carga de los procesadores y el uso de la memoria, esto permitirá diagnosticar si los equipos son blancos de ataques.

Para garantizar un correcto funcionamiento de los equipos instalados en el cuarto de servidores se debe realizar mantenimientos anuales a los respaldos de energía y al aire acondicionado de precisión.

5.2.10 Política de Cumplimiento.

El comité de Seguridad estará pendiente de las normas adoptadas por el Instituto Ecuatoriano de Normalización INEN. Para la elaboración de las presentes políticas se ha tomado como referencia la Norma Técnica Ecuatoriana NTE ISO/IEC 27002

Con el compromiso de la administración de la EERSSA se deben poner en práctica las políticas y garantizar su aplicación.

Se revisará en forma continua, junto con el departamento jurídico, que estás políticas se mantengan dentro de los parámetros de la legislación vigente.

CAPITULO VI.

6. CONCLUSIONES Y RECOMENDACIONES.

6.1 Conclusiones.

Luego de concluir este trabajo sobre el sistema SCADA Local de la EERSSA se presentan las siguientes conclusiones.

- En los sistemas SCADA lo que se prioriza es la disponibilidad del sistema, el mismo, que debe ser constante y en caso de interrupciones reponerse en tiempos cortos.

- La EERSSA no dispone de procedimientos, ni políticas de Seguridad que se apliquen a la operación del Sistema SCADA Local.

- La implementación de VLANS, ACL y ARP estáticas en el sistema SCADA de la EERSSA, son configuraciones que ayudarán a ordenar los hosts y llevar un mejor control de tráfico, pues se determina los equipos que pertenecen a cada subred y permiten identificar las direcciones que tienen permiso para ingresar a la red del SCADA Local.

- El mejoramiento de la seguridad del sistema SCADA Local de la EERSSA involucra la configuración de equipos de red (conmutadores y firewall) así como el compromiso del personal que labora en la administración y operación del sistema, la conjunción de estos elementos lograrán resultados favorables para evitar vulnerabilidades.

- Los cambios de contraseñas deben realizarse también en los equipos de campo, como IED (Dispositivo Electrónico Inteligente), pues son dispositivos que se encuentran en diferentes distribuidoras y sus contraseñas de fábrica están al alcance de todos, pues están publicadas en las guías o manuales de los fabricantes que se pueden obtener en internet.

- Las revisiones de vulnerabilidades son necesarias para determinar puntos de ingresos no autorizados, las pruebas deben realizarse periódicamente y llevar un registro de las mismas. Luego de implementar las políticas se debe realizar pruebas de ingreso desde diferentes puntos para probar su eficiencia.

- El sistema SCADA no dispone de antivirus instalado, por ello es necesario el compromiso de los usuarios, para mantener el máximo aislamiento de los dispositivos extraíbles que pueden estar infectados de virus.

- Debe existir una sala de servidores exclusiva para los equipos de la red SCADA, la política de accesos será exitosa cuando una sola dependencia administre los ingresos. Al ser compartida la sala de equipos el ingreso no es restringido y los controles pueden vulnerarse lo que puede ocasionar robo o destrucción de datos o hardware, o desconexiones no autorizadas de equipos.

6.2 Recomendaciones.

- La implementación de políticas de seguridad debe ser un compromiso de todos los actores que intervienen dentro del Sistema SCADA Local de la EERSSA. Se debe contar con el apoyo de la administración ya que la continuidad en el suministro del servicio eléctrico se garantiza con la información de este sistema.

- Se debe llevar un registro de incidencias, de los eventos que se presenten en los equipos que conforman el sistema SCADA de la EERSSA, esto ayudará a analizar las medidas a tomar para solventarlas, se debe realizar un seguimiento para determinar si la solución que se implementó fue satisfactoria, consiguiendo con ello cumplir con el criterio de mejora continua.

- Se debe mantener continuamente contacto con la compañía AUTOTROL, si existe una actualización del sistema que soporte el empleo de antivirus, algunas empresas proveedoras de Sistemas SCADA trabajan conjuntamente con empresas desarrolladoras de antivirus, ofreciendo garantía al empleo de estas aplicaciones.

- La prioridad del Centro de Control es monitorear el Sistema Eléctrico de Potencia, por eso se restringe el acceso del personal, se sugiere que si es necesario realizar una visita de grupo se construya una sala continua que permita visualizar las instalaciones sin la necesidad de interferir en la operación del sistema, ni distraer a los Operadores.

- El dispositivo de almacenamiento de información crítica, debe almacenarse en un lugar ventilado para que los archivos e imágenes de disco no vayan a comprometerse, de ser posible se debe realizar pruebas de carga para verificar su estado y se garantice una copia segura, en caso de requerir recuperar un proyecto o una consola de operación.

- El recurso humano es un elemento primordial a considerar dentro de la implementación de políticas de seguridad, se debe realizar campañas constantes para difundir las medidas de seguridad que se implementen a fin de crear conciencia de su importancia.

- Los equipos nuevos, que se deseen integrar al sistema SCADA Local, pueden ser revisados en la página de acceso libre del NVE (National Vulnerability Database) perteneciente al NIST (National Institute of Standards and Technology) en la que se enlistan las vulnerabilidades de dispositivos lo que permitirá elegir de mejor manera el hardware. https://web.nvd.nist.gov/view/vuln/search.,

- Para un mejor funcionamiento del equipo CSIRT interno, se recomienda contar con consultores externos como el ECUCERT,[34] (Centro de Respuesta a Incidentes informáticos del Ecuador), perteneciente a la Agencia de Regulación y Control de las Telecomunicaciones del Ecuador, cuyo objetivo es “Brindar a su comunidad Objetivo, (Instituciones del Estado Ecuatoriano o instituciones de sector privado) el apoyo en la prevención y resolución de incidentes de seguridad informática a través de la coordinación, capacitación y soporte técnico”

GLOSARIO.

AAA.- Autenticación, Autorización , Auditoría.

ACL.- Access Control List**.**

ARP.- Address Resolution Protocol

CELEC.- Corporación Eléctrica del Ecuador.

CENACE.- Centro Nacional de Control de Energía

COBIT.- Los Objetivos de Control para la Información y la Tecnológia relacionada.

CSIRT.- Computer Security Incident Response Team.

CNT.- Corporación Nacional de Telecomunicaciones.

DNP.- Distributed Network Protocol

EERSSA.- Empresa Eléctrica Regional del Sur

IED.- Dispositivo Eléctronico Inteligente

NAS .- Network Attached Storage

NIST.- National Institute of Standards and Technology

NVE.- National Vulnerability Database

OWASP.- The Open Web Application Security Project

PLA.- PowerLink Advantage

RADIUS.- Remote Autentication Dial In User Service.

RTU.- Unidad Terminal Remota.

SCADA.- Sistema de Control y Adquisición de Datos.

TACACS.- Terminal Access Controller Access Control System Plus.

TCP.- Protocolo de control de Transmisión

TRANSELECTRIC.- Empresa Transmisora de Electricidad unidad de Negocio de CELEC

UDP.- Protocolo de Datagrama de Usuario.

VLAN.- Red de Área Local Virtual.

BIBLIOGRAFIA.

[1] Kaeo M., ***Diseño de seguridad de redes.*** CISCO PRESS, Pearson Educación S.A.

[2] INTECO, INSTITUTO NACIONAL DE TECNOLOGIAS DE LA COMUNICACIÓN Gobierno de España**.** ***Estudio sobre la seguridad de los sistemas de monitorización y control de procesos e infraestructuras*** **(SCADA)**.2012

[3] INTECO, INSTITUTO NACIONAL DE TECNOLOGIAS DE LA COMUNICACIÓN Gobierno de España**.** ***Guía para empresas: Seguridad de los Sistemas de Monitorización y control de los procesos e infraestructuras (SCADA*****)**. 2012

[4] **Disso, J.P. Jones, K. ; Bailey, S.** *A Plausible Solution to SCADA Security Honeypot Systems*

[5] Puliadi, A., Jo,J., Kim,Yoohwan., ***Application of NTRU Cryptographic Algorithm for SCADA Security.*** Department of Computer Science University of Nevada, Las Vegas, NV, USA.

[6] Alcaraz, C., Fernández G., Román R., Balastegui Á., López J., ***Gestión Segura de Redes SCADA***, Departamento de Lenguajes y Ciencias de la Computación, Universidad de Málaga

[7] Tanenbaum, A., Wetherall, D**.,** ***Redes de computadoras,*** Quinta edición

[8] Office of Energy Assurance U.S. Department of Energy**,** ***21 Steps to Improve Cyber Security of SCADA Networks***

[9] http://sas-origin.onstreammedia.com/origin/isaca/LatinCACS/cacs-lat/forSystemUse/papers/113.pdf

[10] NIST Special Publication 800-82. DRAFT **- Guide to Industrial Control Systems (ICS) Security. 2015**

[11] National Institute of Standards and Technology. www.nist.gov

[12] Johannson, Erick; Sommestad, Teodor; Ekstedt, Mathias, **Security Issues for SCADA Systems within Power Distribution,** Dept. of Industrial Information and Control System Royal Institute Of Technology, Stockholm, SWEDEN.

[13] Sater D., McCauley-Bell P., Malone L., DeMara R., ***Evaluation of the Human Impact of Password Authentication Practice on Information Security.*** Florida Institute of Technology, University of Central Florida, Orlando, USA

[14] Hassell L., Wiedenbeck S., ***Human Factors and Information Security.*** Drexel University

[15] https://www.microsoft.com/es-ES/download/details.aspx?id=6185

[16] https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4250

[17] norfipc.com/virus/eliminar/-virus-conficker.html

[18] http://technet.microsof.com/library/security/MS10-46

[19] Naedele, M., Vahldieck R., **SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN**

[20] ***Cryptographic Protection of SCADAComunications***, Part 1: Background, Policies and Test Plan.(AGA 12, Part 1).

[21] http:// cve.mitre.org/index.html.

[22] https://www.microsoft.com/es-ES/download/details.aspx?id=6185

[23] https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4250

[24] http://www.dlink.com//media/Files/B2B%20Briefs/ES/dlinklaalternativanas.pdf

[25] https://es.wikipedia.org/wiki/Request_for_Comments

[26] https://tools.ietf.org/html/rfc1244#section-1.6

[27] Stalling, William. ***FUNDAMENTOS DE SEGURIDAD DE REDES APLICACIONES Y STANDARES***, 2da Edición

[28] Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información ISO/IEC 27000.

[29] **Manual de Clasificación de Puestos**, Empresa Eléctrica Regional del SUR.

[30] **OWASP Top 10 – 2013**, Los diez riesgos más críticos en aplicaciones Web.

[31] **Código verde.com,** Consultoría especializada.

[32] Ramos, Jorge. **Pruebas de Penetración o Pent Test,** Universidad Mayor de San Andrés.

[33] Uyana, Mónica. "**Propuesta de diseño de un área informática forence para un equipo de respuestas ante incidentes de seguridad informáticos,CSIRT"**, Tesis de grado de Maestría en Gerencia de Seguridad y Riesgo. ESPE 2014.

[34] www.ecuacert.gob.ec.

[35] Andreu, Eduardo. **Seguridad Informática y Alta Disponibilidad – Resumen Capítulo 3 – CCNA Security – AAA**.

[36] Stallings, William., **Fundamentos de Seguridad en Redes Aplicaciones y Estándares**, 2004, Pearson Educación S.A.

[37] https://es.wikipedia.org/wiki/Intel_Security

[38] www.cioal.com/2014/05/08/mcafee-y-schneider-electric-se-alian-para-proporcionar-soluciones-de-seguridad/

[39] https://es.wikipedia.org/wiki/Kaspersky_Lab

[40] https://studentclubidatnet.wordpress.com/2010/09/17/kaspersky-y-microsoft-vs-stuxnet.

[41] NIST Special Publication 800-53.**- Security and Privacy Controls for Federal Information Systems and Organizations**. April 2013.

[42] ESTÁNDAR ISO/IEC INTERNACIONAL 17799. **Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información.** Segunda edición 2005.

[43] "*Previniendo Ataques DDoS con Redes Cisco que Se Autodefienden***"**

[44].- COBIT 5, Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa

[45] www.iso27002.es.

ANEXO A

is often subdivided into organizational units that should work together to reduce vulnerabilities. The scope and hierarchical relationship among policies and procedures needs to be managed for maximum effectiveness.

Certain controls in SP 800-53 and the ICS overlay in Appendix G specify responsibilities and requirements for the organization, while others focus on the capabilities and operation of the various systems within the organization. For example, the control AC-6, Least Privilege, states "The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions." The organization has to make decisions that get codified in policy and procedures. Some resulting artifacts, such as job descriptions that include roles, responsibilities, and authority, remain in a form suitable for people, while other artifacts, such as attributes, privileges, and access control rules, are implemented in IT.

Note that the ICS overlay follows SP 800-53 in employing the term "organization" very flexibly so that its guidance can be used by all sizes of organizational entities up and down an organization chart. Specific organizations should be identified, starting with the organization responsible for issuing and maintaining the policy or procedure.

Table C-2 presents examples of observed policy and procedure vulnerabilities for ICS.

Table C-2. Policy and Procedure Vulnerabilities and Predisposing Conditions

Vulnerability	Description
Inadequate security policy for the ICS	Vulnerabilities are often introduced into ICS due to inadequate policies or the lack of policies specifically for control system security. Every countermeasure should be traceable to a policy. This ensures uniformity and accountability. Policy must include portable and mobile devices used with ICS.
No formal ICS security training and awareness program	A documented formal security training and awareness policy and program is designed to keep staff up to date on organizational security policies and procedures as well as threats, industry cybersecurity standards, and recommended practices. Without training on specific ICS policies and procedures, staff cannot be expected to maintain a secure ICS environment.
Absent or deficient ICS equipment implementation guidelines	Equipment implementation guidelines should be kept up to date and readily available. These guidelines are an integral part of security procedures in the event of an ICS malfunction.
Lack of administrative mechanisms for security policy enforcement	Staff responsible for enforcing security should be held accountable for administering documented security policies and procedures.
Inadequate review of the effectiveness of the ICS security controls	Procedures and schedules should exist to determine the extent to which the security program and its constituent controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the ICS. The examination is sometimes called an "audit," "evaluation," or "assessment." Policy should address the stage of the life-cycle, purpose, technical expertise, methodology, and level of independence.
No ICS-specific contingency plan	A contingency plan should be prepared, tested and available in the event of a major hardware or software failure or destruction of facilities. Lack of a specific plan for the ICS could lead to extended downtimes and production loss.
Lack of configuration management policy	Lack of policy and procedures for ICS configuration change management can lead to unmanageable and highly vulnerable inventory of hardware, firmware, and software.

Vulnerability	Description
Lack of adequate access control policy	Access control enforcement depends of policy the correctly models roles, responsibilities, and authorizations. The policy model must enable the way the organization functions.
Lack of adequate authentication policy	Authentication policies are needed to define when authentication mechanisms (e.g., passwords, smart cards) must be used, how strong they must be, and how they must be maintained. Without policy, systems might not have appropriate authentication controls, making unauthorized access to systems more likely. Authentication policies should be developed as part of an overall ICS security program taking into account the capabilities of the ICS and its personnel to handle more complex passwords and other mechanisms.
Inadequate incident detection and response plan and procedures	An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring ICS services. Establishing a successful incident response capability includes continually monitoring for anomalies, prioritizing the handling of incidents, and implementing effective methods of collecting, analyzing, and reporting data.
Lack of redundancy for critical components	Lack of redundancy in critical components could provide single point of failure possibilities

System Vulnerabilities and Predisposing Conditions

Security controls must clearly identify the systems to which they apply. Systems range widely in size, scope, and capability. At the small end of the spectrum, a system may be an individual hardware or software product or service. At the other end of the spectrum we find large complex systems, systems-of-systems, and networks, all of which incorporate hardware architecture and software framework (including application frameworks), where the combination supports the operation of the ICS.

System vulnerabilities can occur in the hardware, firmware, and software used to build the ICS. Sources of vulnerabilities include design flaws, development flaws, misconfigurations, poor maintenance, poor administration, and connections with other systems and networks. Many of the controls in the SP 800-53 and the ICS overlay in Appendix G specify what the system must do to mitigate these vulnerabilities.

The potential vulnerabilities and predisposing conditions commonly found within ICS systems are categorized with the following tables:

- Table C-3. Architecture and Design Vulnerabilities and Predisposing Conditions.
- Table C-4. Configuration and Maintenance Vulnerabilities and Predisposing Conditions.
- Table C-5. Physical Vulnerabilities and Predisposing Conditions.
- Table C-6. Software Development Vulnerabilities and Predisposing Conditions.
- Table C-7. Communication and Network Configuration Vulnerabilities and Predisposing Conditions.

Table C-3. Architecture and Design Vulnerabilities and Predisposing Conditions

Vulnerability	Description
Inadequate incorporation of security into architecture and design.	Incorporating security into the ICS architecture, design must start with budget, and schedule of the ICS. The security architecture is part of the Enterprise Architecture. The architectures must address the identification and authorization of users, access control mechanism, network topologies, and system configuration and integrity mechanisms.
Insecure architecture allowed to evolve	The network infrastructure environment within the ICS has often been developed and modified based on business and operational requirements, with little consideration for the potential security impacts of the changes. Over time, security gaps may have been inadvertently introduced within particular portions of the infrastructure. Without remediation, these gaps may represent backdoors into the ICS.
No security perimeter defined	If the ICS does not have a security perimeter clearly defined, then it is not possible to ensure that the necessary security controls are deployed and configured properly. This can lead to unauthorized access to systems and data, as well as other problems.
Control networks used for non-control traffic	Control and non-control traffic have different requirements, such as determinism and reliability, so having both types of traffic on a single network makes it more difficult to configure the network so that it meets the requirements of the control traffic. For example, non-control traffic could inadvertently consume resources that control traffic needs, causing disruptions in ICS functions.
Control network services not within the control network	Where IT services such as Domain Name System (DNS), and Dynamic Host Configuration Protocol (DHCP) are used by control networks, they are often implemented in the IT network, causing the ICS network to become dependent on the IT network that may not have the reliability and availability requirements needed by the ICS.
Inadequate collection of event data history	Forensic analysis depends on collection and retention of sufficient data. Without proper and accurate data collection, it might be impossible to determine what caused a security incident to occur. Incidents might go unnoticed, leading to additional damage and/or disruption. Regular security monitoring is also needed to identify problems with security controls, such as misconfigurations and failures.

Table C-4. Configuration and Maintenance Vulnerabilities and Predisposing Conditions

Vulnerability	Description
Hardware, firmware, and software not under configuration management.	The organization doesn't know what it has, what versions it has, where they are, or what their patch status is, resulting in an inconsistent, and ineffective defense posture. A process for controlling modifications to hardware, firmware, software, and documentation should be implemented to ensure an ICS is protected against inadequate or improper modifications before, during, and after system implementation. A lack of configuration change management procedures can lead to security oversights, exposures, and risks. To properly secure an ICS, there should be an accurate listing of the assets in the system and their current configurations. These procedures are critical to executing business continuity and disaster recovery plans.
OS and vendor software patches may not be developed until significantly after security vulnerabilities are found	Because of the tight coupling between ICS software and the underlying ICS, changes must undergo expensive and time-consuming comprehensive regression testing. The elapsed time for such testing and subsequent distribution of updated software provides a long window of vulnerability

Vulnerability	Description
OS and application security patches are not maintained or vendor declines to patch vulnerability	Out-of-date OSs and applications may contain newly discovered vulnerabilities that could be exploited. Documented procedures should be developed for how security patches will be maintained. Security patch support may not even be available for ICS that use outdated OSs.
Inadequate testing of security changes	Modifications to hardware, firmware, and software deployed without testing could compromise normal operation of the ICS. Documented procedures should be developed for testing all changes for security impact. The live operational systems should never be used for testing. The testing of system modifications may need to be coordinated with system vendors and integrators.
Poor remote access controls	There are many reasons why an ICS may need to be remotely accessed, including vendors and system integrators performing system maintenance functions, and also ICS engineers accessing geographically remote system components. Remote access capabilities must be adequately controlled to prevent unauthorized individuals from gaining access to the ICS.
Poor configurations are used	Improperly configured systems may leave unnecessary ports and protocols open, these unnecessary functions may contain vulnerabilities that increase the overall risk to the system. Using default configurations often exposes vulnerabilities and exploitable services. All settings should be examined.
Critical configurations are not stored or backed up	Procedures should be available for restoring ICS configuration settings in the event of accidental or adversary-initiated configuration changes to maintain system availability and prevent loss of data. Documented procedures should be developed for maintaining ICS configuration settings.
Data unprotected on portable device	If sensitive data (e.g., passwords, dial-up numbers) is stored in the clear on portable devices such as laptops and mobile devices and these devices are lost or stolen, system security could be compromised. Policy, procedures, and mechanisms are required for protection.
Passwords generation, use, and protection not in accord with policy	There is a large body of experience with using passwords in IT that is applicable to ICS. Password policy and procedure must be followed to be effective. Violations of password policy and procedures can drastically increase ICS vulnerability.
Inadequate access controls applied	Access controls must be matched to the way the organization allocates responsibilities and privilege to its personnel. Poorly specified access controls can result in giving an ICS user too many or too few privileges. The following exemplify each case: • System configured with default access control settings gives an operator administrative privileges • System improperly configured results in an operator being unable to take corrective actions in an emergency situation
Improper data linking	ICS data storage systems may be linked with non-ICS data sources. An example of this is database links, which allow data from one database to be automatically replicated to others. Data linkage may create a vulnerability if it is not properly configured and may allow unauthorized data access or manipulation.
Malware protection not installed or up to date	Installation of malicious software, or malware, is a common attack. Malware protection software, such as antivirus software, must be kept current in a very dynamic environment. Outdated malware protection software and definitions leave the system open to new malware threats.
Malware protection implemented without sufficient testing	Malware protection software deployed without sufficient testing could impact normal operation of the ICS and block the system from performing necessary control actions.
Denial of service (DoS)	ICS software could be vulnerable to DoS attacks, resulting in the prevention of authorized access to a system resource or delaying system operations and functions.

Vulnerability	Description
Intrusion detection/prevention software not installed	Incidents can result in loss of system availability and integrity; the capture, modification, and deletion of data; and incorrect execution of control commands. IDS/IPS software may stop or prevent various types of attacks, including DoS attacks, and also identify attacked internal hosts, such as those infected with worms. IDS/IPS software must be tested prior to deployment to determine that it does not compromise normal operation of the ICS.
Logs not maintained	Without proper and accurate logs, it might be impossible to determine what caused a security event to occur.

Table C-5. Physical Vulnerabilities and Predisposing Conditions

Vulnerability	Description
Unauthorized personnel have physical access to equipment	Physical access to ICS equipment should be restricted to only the necessary personnel, taking into account safety requirements, such as emergency shutdown or restarts. Improper access to ICS equipment can lead to any of the following: • Physical theft of data and hardware • Physical damage or destruction of data and hardware • Unauthorized changes to the functional environment (e.g., data connections, unauthorized use of removable media, adding/removing resources) • Disconnection of physical data links • Undetectable interception of data (keystroke and other input logging)
Radio frequency and electro-magnetic pulse (EMP)	The hardware used for control systems is vulnerable to radio frequency and electro-magnetic pulses (EMP). The impact can range from temporary disruption of command and control to permanent damage to circuit boards.
Lack of backup power	Without backup power to critical assets, a general loss of power will shut down the ICS and could create an unsafe situation. Loss of power could also lead to insecure default settings.
Loss of environmental control	Loss of environmental control (e.g., temperatures, humidity) could lead to equipment damage, such as processors overheating. Some processors will shut down to protect themselves; some may continue to operate but in a minimal capacity and may produce intermittent errors, continually reboot, or become permanently incapacitated.
Unsecured physical ports	Unsecured universal serial bus (USB) and PS/2 ports could allow unauthorized connection of thumb drives, keystroke loggers, etc.

Table C-6. Software Development Vulnerabilities and Predisposing Conditions

Vulnerability	Description
Improper Data Validation	ICS software may not properly validate user inputs or received data to ensure validity. Invalid data may result in numerous vulnerabilities including buffer overflows, command injections, cross-site scripting, and path traversals.
Installed security capabilities not enabled by default	Security capabilities that were installed with the product are useless if they are not enabled or at least identified as being disabled.
Inadequate authentication, privileges, and access control in software	Unauthorized access to configuration and programming software could provide the ability to corrupt a device.

Table C-7. Communication and Network Configuration Vulnerabilities and Predisposing Conditions

Vulnerability	Description
Flow controls not employed	Data flow controls, based on data characteristics, are needed to restrict which information is permitted between systems. These controls can prevent exfiltration of information and illegal operations.
Firewalls nonexistent or improperly configured	A lack of properly configured firewalls could permit unnecessary data to pass between networks, such as control and corporate networks, allowing attacks and malware to spread between networks, making sensitive data susceptible to monitoring/eavesdropping, and providing individuals with unauthorized access to systems.
Inadequate firewall and router logs	Without proper and accurate logs, it might be impossible to determine what caused a security incident to occur.
Standard, well-documented communication protocols are used in plain text	Adversaries that can monitor the ICS network activity can use a protocol analyzer or other utilities to decode the data transferred by protocols such as telnet, File Transfer Protocol (FTP), and Network File System (NFS). The use of such protocols also makes it easier for adversaries to perform attacks against the ICS and manipulate ICS network activity.
Authentication of users, data or devices is substandard or nonexistent	Many ICS protocols have no authentication at any level. Without authentication, there is the potential to replay, modify, or spoof data or to spoof devices such as sensors and user identities.
Use of unsecure industry-wide ICS protocols	Distributed Network Protocol (DNP) 3.0, Modbus, Profibus, and other protocols are common across several industries and protocol information is freely available. These protocols often have few or no security capabilities, such as authentication and encryption, to protect data from unauthorized access or tampering. Additionally protocols such as DNP and OPC have had numerous vulnerabilities in their implementation.
Lack of integrity checking for communications	There are no integrity checks built into most industrial control protocols; adversaries could manipulate communications undetected. To ensure integrity, the ICS can use lower-layer protocols (e.g., IPsec) that offer data integrity protection.
Inadequate authentication between wireless clients and access points	Strong mutual authentication between wireless clients and access points is needed to ensure that clients do not connect to a rogue access point deployed by an adversary, and also to ensure that adversaries do not connect to any of the ICS's wireless networks.
Inadequate data protection between wireless clients and access points	Sensitive data between wireless clients and access points should be protected using strong encryption to ensure that adversaries cannot gain unauthorized access to the unencrypted data.

Incidents

A threat event is an event or situations that could potentially cause an undesirable consequence or impact to the ICS resulting from some threat source. In NIST SP 800-30 Rev 1, Appendix E identifies a broad set of threat events that could potentially impact information systems. The properties of an ICS may also present unique threat events, specifically addressing how the threat events can manipulates the process of the ICS to cause physical damage. Table C-8 provides an overview of potential ICS threat events.

Table C-8. Example Adversarial Incidents

Threat Event	Description
Denial of Control Action	Control systems operation disrupted by delaying or blocking the flow of information, thereby denying availability of the networks to control system operators or causing information transfer bottlenecks or denial of service by IT-resident services (such as DNS)
Control Devices Reprogrammed	Unauthorized changes made to programmed instructions in PLCs, RTUs, DCS, or SCADA controllers, alarm thresholds changed, or unauthorized commands issued to control equipment, which could potentially result in damage to equipment (if tolerances are exceeded), premature shutdown of processes (such as prematurely shutting down transmission lines), causing an environmental incident, or even disabling control equipment
Spoofed System Status Information	False information sent to control system operators either to disguise unauthorized changes or to initiate inappropriate actions by system operators
Control Logic Manipulation	Control system software or configuration settings modified, producing unpredictable results
Safety Systems Modified	Safety systems operation are manipulated such that they either (1) do not operate when needed or (2) perform incorrect control actions that damage the ICS
Malware on Control Systems	Malicious software (e.g., virus, worm, Trojan horse) introduced into the system.

In addition, in control systems that cover a wide geographic area, the remote sites are often not staffed and may not be physically monitored. If such remote systems are physically breached, the adversaries could establish a connection back to the control network.

Sources of Incidents

An accurate accounting of cyber incidents on control systems is difficult to determine. However, individuals in the industry who have been focusing on this issue see similar growth trends between vulnerabilities exposed in traditional IT systems and those being found in control systems. ICS-CERT is a DHS organization that focuses on reducing the risk across critical infrastructure by identifying threats and vulnerabilities, while also providing mitigation strategies. ICS-CERT provides a trusted party where system owners and operators can report information about incidents within their ICS and obtain advice on mitigating their risk. As part of this effort ICS-CERT also performs onsite deployments to an ICS to analyze and respond to incidents. Additionally, they publish advisories of new security vulnerabilities discovered in common ICS platforms. Figure C-1 demonstrates (1) the number of ICS incidents reported, (2) the number of onsite ICS deployments taken by ICS-CERT, and (3) number of ICS vulnerabilities reported between years 2010 and 2013[25].

Other sources of control system impact information show an increase in control system incidents as well. This information should not be assumed to contain all ICS related incidents or discovered vulnerabilities as some information may go unreported.

[25] https://ics-cert.us-cert.gov/