ANÁLISIS DE LOS RIESGOS DE SEGURIDAD INFORMÁTICA DE SISTEMAS SCADA EN SUBESTACIONES ELÉCTRICAS EN LA CIUDAD DE DUITAMA BOYACÁ

CARLOS EDUARDO OTERO MURILLO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA

ESPECIALIZACION EN SEGURIDAD INFORMATICA

DUITAMA

2016

ANÁLISIS DE LOS RIESGOS DE SEGURIDAD INFORMÁTICA DE SISTEMAS SCADA EN SUBESTACIONES ELÉCTRICAS EN LA CIUDAD DE DUITAMA BOYACÁ

CARLOS EDUARDO OTERO MURILLO

Trabajo de grado presentado para optar por el título de Especialista en Seguridad Informática

Asesor: Ing. Martin Camilo Cancelado Ruiz

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA

ESPECIALIZACION EN SEGURIDAD INFORMATICA

DUITAMA

2016

DEDICATORIA

A mi Esposa Liliana, a mis hijos Juan Camilo y Santiago por el gran apoyo, el tiempo y el espacio que me proporcionaron para cumplir con esta nueva meta en mi vida.

AGRADECIMIENTOS

Agradezco primero a Dios por darle un buen rumbo a mi vida y la fuerza necesaria para cumplir con este nuevo logro, también a mi familia y a todas las personas que me colaboraron para la realización de este proyecto.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

Lo que se buscó en el presente proyecto fue la recopilación de información sobre sistemas SCADA en el sector eléctrico, la interconexión entre subestaciones y central de mando, protocolos de comunicación y sistemas de control, de esta infraestructura critica que puede ser blanco de ataques informáticos y para minimizar el riesgo informático de sistemas SCADA en una subestación eléctrica.

Para esto, analizamos la forma en que son manejados los datos de supervisión y control a distancia (telemetría) de la subestación eléctrica, los medios de transmisión y comunicación, con el fin de mejorar la integridad, disponibilidad y el no repudio de los datos que se envían y reciben.

Con base en la información recopilada, se creó una matriz de riesgos, donde se evidenciaron vulnerabilidades, los respectivos controles y plan de mejora que se debe implementar y tener en cuenta para fortalecer la seguridad informática en el sistema.

Palabras Clave: Eléctrica, Informática, Infraestructura, SCADA, Riesgo, Seguridad, Subestación, Telecomunicaciones.

INTRODUCCIÓN

En la industria, los sistemas de control de máquinas y procesos se basan en accionamientos on-off (encendido y apagado) de elementos que conectan o desconectan sistemas de alimentación eléctrica, flujo hidráulico, calderas, radiadores entre otros y sensores de medida de variables físicas. Estos controles son basados en sistemas computacionales de control soportado por sistemas SCADA (supervisión, control y adquisición de datos) los cuales se programan en una computadora, la cual está conectada a un PLC (controlador lógico programable) que es el encargado de enviar y recibir las señales de control a actuadores, sensores e instrumentos. Este sistema antiguamente estaba aislado y supervisado por personal presente en la planta, hoy en día con el avance de la tecnología, estos sistemas se han ido interconectando a redes privadas internas e incluso vía internet, esto representa un ventaja al poder controlar y supervisar el proceso a distancia y más cuando se maneja elementos peligrosos para el ser humano, pero también conlleva un riesgo ya que al enviar información por la red, esta puede ser intervenida, robada o atacada poniendo en riesgo la integridad de los procesos e inclusive de la planta.

Para este proyecto se busca implementar controles de seguridad para minimizar el riesgo informático de sistemas SCADA en una subestación eléctrica, con el fin de disminuir las posibles vulnerabilidades y fallas de seguridad del sistema de control.

Para esto, analizaremos la forma en que son manejados los datos de supervisión y control a distancia (telemetría) de la subestación eléctrica, los medios de transmisión y comunicación, con el fin de garantizar la integridad, disponibilidad y el no repudio de los datos que se envían y reciben.

Se espera que este trabajo, brinde información necesaria para implementar una matriz de riesgo para identificar problemas en la seguridad de este tipo de plantas industriales, que son de vital importancia para el desarrollo regional, que prestan un servicio público indispensable para la comunidad

PLANTEAMIENTO DEL PROBLEMA

Los sistemas de interconexión de media tensión por medio de subestaciones, son el corazón que convierte la energía eléctrica a baja tensión y lleva la energía a los usuarios finales en las principales ciudades del país.

Estas subestaciones están siendo modernizadas según la norma internacional IEC 61850 en donde se establece una comunicación vía Ethernet para supervisión y control a distancia de estas subestaciones eléctricas, pudiéndose presentar riesgos de seguridad informática, que terminen en la explotación de vulnerabilidades del sistema y un inminente ataque informático como por ejemplo: alteración de las medidas de sensores de estado de la planta, envió de instrucciones falsas a los actuadores y controles de la planta, implantación de virus o malware informático que afectaría el sistema que maneja el PLC, que podría causar la falla del sistema de control SCADA que maneja la subestación, lo cual puede causar un corte indefinido del suministro eléctrico e incluso catástrofe por daño o explosión en el transformador reductor.

Este proyecto busca determinar si existe algún tipo de riesgo inherente al proceso de control y supervisión a distancia con telemetría de una subestación eléctrica, si el acceso a los equipos y a la red de telecomunicaciones es restringido a personal netamente autorizado y si los equipos y protocolos de comunicación presentan falencias en seguridad informática que puedan afectar el buen funcionamiento y la disponibilidad y optima operación del sistema SCADA.

JUSTIFICACIÓN

Los sistemas de interconexión eléctrica de alto voltaje así como las subestaciones eléctricas a nivel mundial están migrando hacia nuevas tecnologías como los sistemas Smart Grid que integra fuentes de energía renovable, con el inter-conexionado habitual, así como los sistemas de control industrial (ICS), junto con el modelo de supervisión, control y adquisición de datos SCADA, por medios computarizados, son en muchos casos el cerebro de las operaciones en muchas plantas y subestaciones eléctricas a nivel mundial y se hace necesario proteger y resguardar la comunicación entre la central y las subestaciones, así como administrar y controlar los protocolos que usan y como proteger estos sistemas ante amenazas.

En nuestro país, que por muchos años ha venido siendo víctima de la delincuencia organizada y grupos al margen de la ley, es necesario proteger las instituciones nacionales y las que prestan servicios públicos básicos y esenciales como la industria energética, acueductos y servicios de telecomunicaciones, contra la acción delictiva o terrorismo, ya que no solo pueden atacar físicamente, sino que también existe la posibilidad de ataques informáticos en contra de la plataforma energética en Colombia. En el sector industrial, existen riesgos muy grandes que pueden generar perdidas económicas y afectación a sectores vulnerables en todos los niveles, es por esto, que se propone a través de este proyecto, verificar los riesgo que existen para la seguridad física e informática, el control y automatización de sus comunicaciones, envío de información importante para su supervisión y manejo de procesos industriales, centrándonos en el sector energético en el territorio colombiano y más específicamente en subestaciones eléctricas en la ciudad de Duitama Boyacá.

OBJETIVOS

Objetivo General

Realizar una matriz de riesgos con sus respectivos controles a partir de la valoración de activos de información, que ayuden a minimizar los riesgos de seguridad informática que se puedan presentar en un sistema SCADA de una subestación eléctrica en la ciudad de Duitama Boyacá.

Objetivos Específicos

- Identificar los elementos que conforman un sistema de control SCADA de una subestación eléctrica.

- Reconocer los diferentes protocolos de telecomunicaciones que debe tener una subestación eléctrica.

- Desarrollar una matriz de riesgos a partir de la información recogida anteriormente, e implementar los respectivos controles de seguridad para el sistema SCADA de estudio.

- Proponer un plan de mejora y mitigación de riesgos que pueda ayudar a disminuir el riego informático que se pueda presentar eventualmente en el sistema SCADA.

1. MARCO CONCEPTUAL Y TEÓRICO

1.1. MARCO CONTEXTUAL

1.1.1 Subestaciones eléctricas en Colombia

En Colombia como en muchos países en vía de desarrollo el tema energético es de carácter primordial para el impulso de la economía de un país, y es necesario contar con sistemas de generación de energía que suplan las necesidades de la industria y de la sociedad civil y que a futuro sea sostenible y sobre todo segura, que tenga un nivel de disponibilidad óptimo para el buen funcionamiento de equipamiento, alumbrado y que pueda abastecer a la comunidad creciente de una región.

El propósito de todo sistema eléctrico de potencia es suministrar la energía necesaria para el desarrollo de un sector o país. Para alcanzarlo es necesario generar, trasmitir y distribuir la energía eléctrica desde los centros de generación, ubicados estratégicamente con base en la disponibilidad de fuentes primarias de energía como el gas, el carbón, el agua o la energía nuclear hasta los centros de distribución y consumo, considerando en todo momento las limitaciones económicas y condiciones de seguridad, de confiabilidad y de calidad del servicio requeridos.

Una subestación eléctrica es la muestra física de un nodo de un sistema eléctrico de potencia, en el cual se puede transformar la energía eléctrica a niveles adecuados de tensión para su transporte, distribución y consumo bajo determinados requerimientos técnicos de calidad, confiabilidad, flexibilidad y eficiencia[1].

Además, las subestaciones eléctricas están conformadas por un conjunto de equipos que permiten: a) controlar el flujo de energía a través de los

[1] GOMEZ, Fernando y VARGAS, Hermann. Planeamiento del diseño de subestaciones eléctricas. Revista Espsilon N° 16. Enero - Junio 20111 p. 79 - 112.

transformadores de potencia, convirtiendo la tensión de suministro a niveles de tensión más bajos o altos de acuerdo con la necesidad preestablecida, b) adelantar la interconexión de diferentes rutas del flujo de energía al mismo nivel de tensión.

Estas subestaciones eléctricas cuentan con sistemas de control sistematizados que son controlados en muchos casos por PLC's (Controlador Lógico Programable) o sistemas donde intervienen interfaces digitales susceptibles a errores de programación, transmisión, de control remoto o en dados casos virus informáticos que pueden afectar estos sistemas de control.

A continuación, veremos cómo se plantean los sistemas de comunicaciones y control en una subestación eléctrica en Colombia que es la parte que nos interesa profundizar y donde se pueden presentar vulnerabilidades de tipo informático que en resumidas cuentas es el objeto de estudio de este proyecto.

1.1.2 Sistema de comunicaciones

La selección del sistema de telecomunicaciones debe ser el más apropiado para la intercomunicación de la subestación con las otras subestaciones asociadas al proyecto y con el centro de control del sistema eléctrico. Para adelantar la selección se debe tener en cuenta el diseño mismo, la configuración, sus niveles de calidad, confiabilidad y seguridad, al igual que el desempeño dentro del sistema general de comunicaciones del sistema. Inicialmente debe identificarse el sistema de telecomunicaciones de la compañía propietaria del proyecto para luego proceder a seleccionarlo entre los siguientes tipos:

- Red de radio microondas.
- Sistema de fibra óptica.
- Enlace de onda portadora por línea de potencia.
- Estación satelital.
- Red de radio móvil.
- Red telefónica pública

Sistema de control Para la operación coordinada de los diferentes niveles de control de una subestación se emplean redes y medios de comunicación. Es de tener en cuenta además que pueden existir varios niveles de control dependiendo de las necesidades de operación en particular que se presenten, las cuales pueden ser:

- De operación local: Las que se adelantan en el propio equipo.

- De operación remota: Las que se adelantan desde un edificio de control ubicado dentro de la subestación o las que se realizan en un edificio de despacho alejado de ésta.

La estructura general del sistema de control de una subestación, por lo general, está dividida en tres niveles:

- Primer nivel de control (nivel de campo): se presenta en el ámbito de los equipos primarios de la subestación (seccionadores, interruptores, transformadores de corriente y tensión). La operación de los interruptores y seccionadores se hace, por lo general, en el mando del propio equipo. El control en este nivel reside en el propio mando del interruptor y seccionador y en la lógica de control implementada en el propio gabinete de mando.

- Segundo nivel (nivel de control de posición): conformado por elementos intermedios de la subestación como: armarios de agrupamiento, unidades de control de posición (unidades de control digital o control convencional mediante manetas, pulsadores y relés auxiliares, dependiendo de la tecnología de control empleada) y todos aquellos elementos encargados de las funciones asociadas al conjunto de la posición, como: control, supervisión, enclavamientos, regulación de voltaje, protección y medición.

- Tercer nivel de control: en éste se realizan las tareas de supervisión, maniobra y control del conjunto de toda la subestación, incluyendo todos los equipos y las posiciones de alta, media y baja tensión.

Lo anterior permite definir una estructura lógica del sistema de control, con dos niveles jerárquicos superiores:

- El nivel de control de posición, desde donde pueden ejecutarse órdenes y supervisar el sistema o parte de éste.

- El nivel de campo desde donde se realiza la adquisición de datos fundamentales para la operación y control de la subestación, tales como el estado de los equipos de maniobra, las tensiones y corrientes en el sistema, la temperatura en los devanados de los transformadores, el nivel de aceite en los transformadores, el nivel de gas en los interruptores, etc. Para tener un sistema de control efectivo, todos sus niveles deben estar interconectados para lograr el mayor intercambio de información. En el diseño de los sistemas de control de una subestación se deben tener en cuenta los siguientes requerimientos:

    - Facilidad de expansión.

    - Automatización de las funciones con el objeto de tener la información disponible de la subestación, donde la acción que tomen los dispositivos de control pueda ser ordenada a control remoto e inclusive realizada localmente (ver Figura 1).

    - Establecer altos márgenes de seguridad: redundancia de equipos de control.

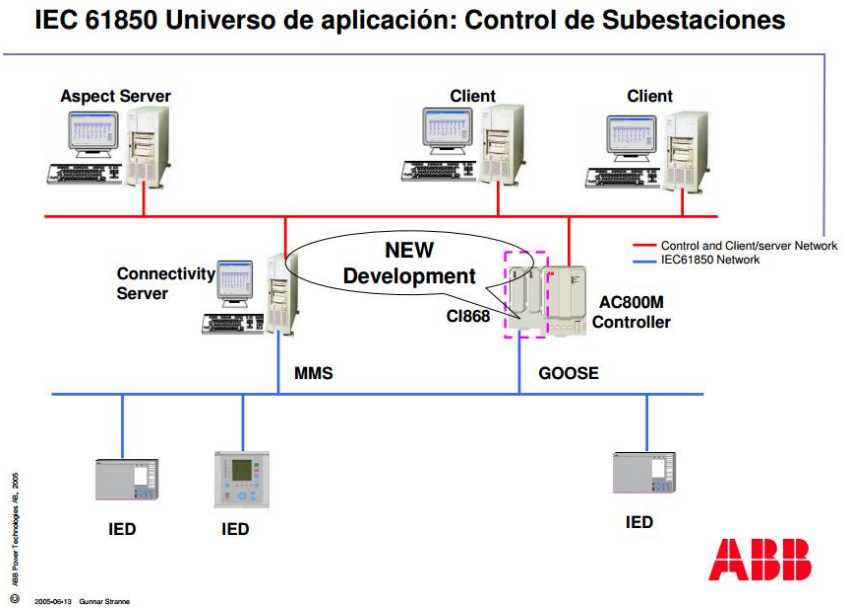
    - Prever un margen alto de disponibilidad de equipos para garantizar la redundancia del sistema de control, ya que ello implica un nivel alto de seguridad, lo que permitirá en caso de que se presente una falla total, se tengan equipos adicionales para asegurar que la falla se reduzca a proporciones tolerables por el sistema.

    - Establecer un alto margen de flexibilidad del sistema de control para que se pueda acomodar a las condiciones de contingencia de la subestación, lo anterior obliga a: Prever la extensión o modificación parcial del sistema de control; prever la posibilidad de intercambiar equipos de diferentes fabricantes; efectuar el diseño inicial de tal manera que se reduzcan gastos cuando se realicen ampliaciones o modificaciones futuras teniendo en cuenta los estándares de sistemas abiertos permitiendo que el sistema de control y los diferentes equipos puedan intercambiar información y compartir recursos entre diferentes tecnologías.

- Establecer para el sistema de control un alto grado de simplicidad en su diseño para aumentar su grado de confiabilidad, ya que éste debe coordinar el manejo de una gran cantidad de información de los equipos de patio y del manejo de la información de las señales de maniobra, para cambiar el estado de la subestación o proceder a aislar un sector de la misma cuando ésta se encuentre en falla.

Como lo vemos, los sistemas de comunicación no son la parte fuerte de la industria energética y de subestaciones en Colombia ya que por lo general se contrata una empresa prestadora de servicios de comunicación para la transmisión de información de monitoreo y control a distancia, dando solución de ultimo kilometro en donde se pueden presentar problemas de comunicación o fallas de transmisión, afortunadamente existen sistemas redundantes que respaldan esta comunicación y es allí donde vamos a mirar cuales son los problemas de seguridad informática a los que se enfrentan estos sistemas.

Figura. 1 Modelo de comunicación IEC 61850



Fuente: ABB

1.1.3 Que son Sistemas SCADA

Los sistemas de monitorización y control en tiempo real son elementos esenciales en el funcionamiento no sólo de la mayoría de los procesos industriales, sino además de gran parte de las tareas rutinarias en nuestra sociedad. A pesar de ello, tanto dichas tareas como estos sistemas son desconocidos por gran parte de los ciudadanos. Se trata de herramientas utilizadas para gestionar infinidad de procesos: desde el funcionamiento del sistema de aire acondicionado o calefacción en un edificio hasta la distribución de energía eléctrica en el territorio nacional.

Entre las diferentes clases de sistemas de monitorización y control existentes, los más utilizados son los denominados SCADA[2]. El acrónimo SCADA (*Supervisory Control And Data Acquisition)* se puede traducir como control de supervisión y adquisición de datos.

Es decir, se denomina sistema SCADA a aquel conjunto de redes, equipos y programas que monitorizan en tiempo real procedimientos industriales y tareas complejas, a partir de la información obtenida a través de sensores, comunicándose con los dispositivos actuadores para transmitirles las órdenes adecuadas y pudiendo controlar el proceso de forma automática mediante un software especializado.

Así pues, la frontera entre un sistema SCADA y un sistema de control remoto es muy difusa, pudiéndose incluir en esta denominación los ICS (*Industrial Control System,* sistema de control industrial), los DCS (*Distributed Control System,* sistema de control distribuido) o sistemas basados directamente sobre PLCs (*Programmable Logic Controllers,* controladores lógicos programables). Ofreciendo una descripción genérica que englobe a todos ellos, se les puede denominar sistemas de monitorización y/o control en tiempo real de forma, en mayor o menor medida, centralizada.

[2] PEREZ, Lizzette. Tendencias de seguridad para sistemas ICS y Scada. [En línea]. 2014. [Citado 10-0ct-2016]. Disponible en internet: http://searchdatacenter.techtarget.com/es/cronica/Tendencias-de-seguridad-para-sistemas-ICS-y-Scada

Tradicionalmente, los sistemas SCADA se referían a aquellos que supervisaban y controlaban procesos industriales, ciñéndose la gestión principalmente a válvulas, bombas, sensores, interruptores y demás elementos mecánicos. Se trataba de sistemas aislados que permitían una gestión centralizada y eficiente, ya que, al conocer el estado de todos los elementos del proceso industrial, la toma de decisiones se simplificaba de manera notable.

Sin embargo, este enfoque ha evolucionado y se ha ampliado a lo largo del tiempo. Por un lado, han aparecido sistemas SCADA para la monitorización y control de otro tipo de dispositivos, como cámaras de video vigilancia o sistemas de climatización. Por otro lado, se ha eliminado su aislamiento pasando a estar más expuestos y conectados a redes externas y públicas como Internet.

Todos estos cambios, unidos a las repercusiones que podría tener cualquier incidente de seguridad en muchos de estos sistemas, motivan la elaboración de esta Guía. En ella se exponen las características de los sistemas SCADA, sus componentes, su funcionamiento y los usos y aplicaciones actuales y futuros junto a los beneficios de dicho uso. Al mismo tiempo, se introduce la legislación aplicable y los estándares existentes, especialmente a nivel nacional. Pero sin duda el principal objetivo de esta Guía es exponer los posibles riesgos que afectan a estos sistemas y el modo de gestionarlos, al tiempo que se aporta una serie de recomendaciones y se señalan diferentes buenas prácticas a seguir.

1.1.4 Características y seguridad de SCADA

Para poder comprender los sistemas de monitorización y control en tiempo real y sus necesidades en cuanto a seguridad, es preciso conocer algunas de las características que los diferencian de las tecnologías estándar o de uso general. Los principales rasgos diferenciadores se refieren a su utilidad, su diseño inicial y a la evolución específica que han sufrido debido a sus peculiaridades. Estas características ubican dichos sistemas en una situación especial en cuanto a la seguridad.[3]

Estos rasgos son:

*Diseñados para su funcionamiento continuo***.** La principal característica diferenciadora de estos sistemas es su diseño, ya que fueron concebidos bajo la

[3] MATT, Kodama. 3 Important Security Trends for ICS/SCADA Systems. [En línea]. 2014. [Citado 5-Nov-2016] Disponible en internet: https://www.recordedfuture.com/ics-scada-trends/

prioridad absoluta del funcionamiento sin interrupción del proceso controlado frente a cualquier otra necesidad. Así pues, son sistemas diseñados para mantenerse en funcionamiento bajo cualquier circunstancia, lo cual puede producir deficiencias en otros aspectos. [4]Esto se debe a que, en sus inicios, estos sistemas se diseñaron para gestionar actividades de vital importancia para la sociedad, como la generación y distribución eléctrica o el control de embalses y plantas potabilizadoras.

*Actuación sobre el entorno físico***.** A diferencia de la mayoría de los sistemas informáticos, las acciones que se ejecutan en un sistema SCADA tienen, por lo general, un impacto directo sobre el mundo físico. Es decir, mientras que cuando se ejecuta un programa en un ordenador el único resultado es la visualización del mismo a través de una pantalla y el uso de su funcionalidad (por ejemplo, un visor de documentos PDF interpreta el fichero y lo muestra por pantalla), la ejecución o envío de una orden en un sistema SCADA puede suponer la apertura de una válvula de una tubería, la disminución de temperatura de un sistema de climatización o el corte del suministro eléctrico en una ciudad.

Automatización total o parcial de procesos complejos. Aunque esta característica podría considerarse propia de cualquier sistema informático, en este caso tiene un matiz diferente al tratarse de procesos más complicados y extensos. Un ejemplo de automatización de un proceso complejo es el sistema SCADA de una cadena de producción de coches, que controla los brazos robóticos, la velocidad de las cintas transportadoras, la presión aplicada para colocar las piezas, etc.

Paso del aislamiento a la conexión global. En un principio, este tipo de sistemas fueron diseñados para encontrarse en entornos aislados. Sin embargo, esta situación ha evolucionado hasta el escenario actual, en el que los sistemas de monitorización y control suelen encontrarse conectados con la red corporativa o redes públicas como Internet.

*Monitorización y control de Infraestructuras Críticas***.** Actualmente, muchas de las Infraestructuras Críticas se encuentran monitorizadas y controladas por sistemas SCADA, existiendo en muchos casos una dependencia prácticamente absoluta respecto a dichos sistemas. Esta dependencia provoca que el sistema SCADA pase a considerarse como crítico, con las necesidades de seguridad y protección que ello conlleva. Un ejemplo ilustrativo es el de una central nuclear. Estas centrales no pueden funcionar sin estos sistemas, ya que son los encargados de la gestión del proceso de generación de energía, así como de los mecanismos de seguridad que

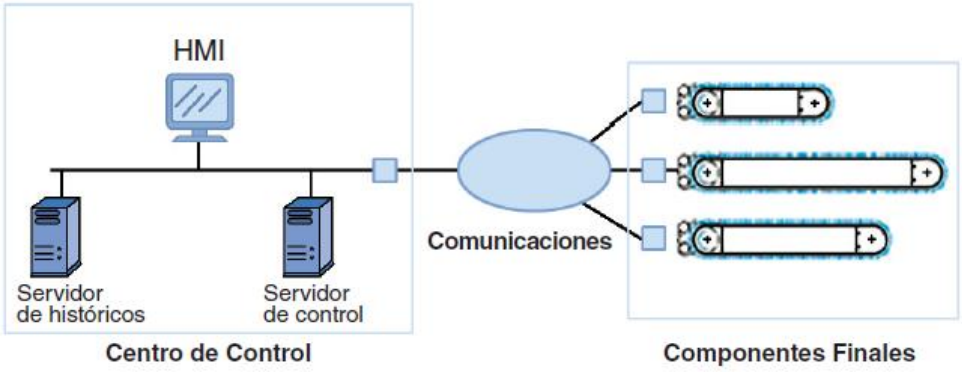
[4] PEREZ, Pablo y ALVAREZ, Eduardo. Estudio sobre la seguridad de los sistemas de monitorización y control de procesos e infraestructuras SCADA". En: Observatorio de la seguridad de la información INTECO. Edición, Marzo 2012 p. 17 - 30

evitan la materialización de riesgos que puedan poner en peligro la integridad de sus instalaciones.

Carencias en actualización de software. Otra característica propia de este tipo de sistemas es la escasa evolución de los mismos, debido principalmente a su aislamiento inicial y a los riesgos que podría implicar su actualización. El aislamiento para el cual fueron diseñados parecía asegurar en principio la imposibilidad de sufrir ataques informáticos, mientras que los posibles riesgos de su actualización se centran en la probabilidad de dejar sin servicio al sistema en caso de error. Estos dos factores han tenido como consecuencia la omisión de las actualizaciones que se han encontrado disponibles para los demás sistemas informáticos a medida que se han descubierto vulnerabilidades.

La estructura básica de un sistema SCADA típica podría ser la siguiente:

Figura 2 Diagrama genérico de SCADA



Fuente: Forrester

Como se observa, un sistema SCADA se puede dividir físicamente en 3 conjuntos principales:

*Centro de control***.** Es el lugar donde se ubican los componentes centrales de un sistema SCADA. Los principales elementos con que cuenta son:

Servidor de control. Es el núcleo del sistema. Se encarga de la monitorización y del control de componentes. Recibe la información proveniente de los componentes

finales y envía las órdenes pertinentes en caso de necesitarse algún tipo de cambio en los elementos controlados.

Servidor de Históricos. Es el elemento encargado del almacenamiento y consolidación de la información recolectada por los sensores que forman parte del sistema.

HMI *(Human Machine Interface).* Son los equipos y aplicaciones informáticas empleadas por el personal encargado de la gestión del sistema SCADA para poder desarrollar sus tareas de una forma más visual y sencilla. En muchas ocasiones se utilizan páginas web, interfaces gráficas de usuario o incluso pantallas táctiles sobre las que se muestran un diagrama del sistema gestionado con información relativa a su estado.

Es importante señalar que estos tres componentes no tienen por qué estar separados físicamente, ya que en sistemas de monitorización y control de tamaño reducido pueden encontrarse en un único equipo informático.

*Comunicaciones***.** Se trata de comunicaciones entre el centro de control y los componentes finales, es decir, entre el centro de mando y los sensores y elementos a manipular. Estas comunicaciones pueden abarcar pequeñas o grandes distancias, y utilizan un amplio abanico de tecnologías: redes locales, redes telefónicas, conexiones vía satélite o radio, redes públicas, etc. La información transmitida en estas comunicaciones contiene datos de monitorización de los componentes finales, así como órdenes de control remoto.

*Componentes finales***.** Son los sensores que proporcionan los datos al sistema y los dispositivos que se manipulan a través del mismo. Por ejemplo, cámaras de video vigilancia, sensores de temperatura, elementos de climatización, etc.

Es importante señalar que esta separación física puede resultar bastante difusa en sistemas de tamaño reducido, pudiendo estar todos los componentes en una misma instalación o incluso en una única sala.

1.1.5 Evolución de sistemas SCADA

Estos sistemas han sufrido una evolución distinta a la del resto de los sistemas TIC. Esta diferenciación se centra en dos aspectos principales: el tipo de tecnologías utilizadas y la interconexión con otros sistemas.

*Tecnología propietaria y específica vs. Tecnología de uso general***.** Un aspecto destacable de estos sistemas en sus orígenes era el uso de tecnología propietaria de escasa difusión (y por tanto poco conocimiento público) en la práctica totalidad de sus componentes. Con el transcurso del tiempo y la evolución de las TIC, estos sistemas comenzaron a emplear elementos de uso general, como ordenadores con sistema operativo Windows, Sistemas de Gestión de Bases de Datos de amplia difusión, etc.

*Interconexión***.** Con el paso del tiempo, y en muchas ocasiones por necesidades de negocio, se establecieron conexiones entre los sistemas de monitorización y control y otras redes, rompiendo así su aislamiento inicial. En la mayoría de los casos, las conexiones se realizaron con redes semi-confiables, como por ejemplo la red corporativa de la propia empresa, mientras que en otros casos se llevaron a cabo con redes públicas, como Internet, lo cual da lugar a una gran exposición a diferentes riesgos.

Estos dos factores han supuesto un cambio sustancial respecto a la preocupación sobre la seguridad. Mientras que inicialmente los sistemas eran considerados seguros debido a su aislamiento y al uso de tecnologías poco conocidas, actualmente se encuentran conectados con otras redes y, al emplear elementos de uso general, mucha más gente tiene conocimiento sobre los mismos, especialmente sobre sus debilidades en seguridad.

1.1.6 Madurez de sistemas SCADA

El grado de madurez de los sistemas de monitorización y control en tiempo real se refiere al nivel de sofisticación y fiabilidad al que ha llegado el desarrollo de estos elementos.

A continuación, se describirá brevemente el grado de madurez de los diferentes componentes de estos sistemas en cuanto a seguridad física, seguridad informática o lógica y funcionalidad.

1.1.6.1 Centros de control

*Seguridad física***.** Al tratarse del núcleo de este tipo de sistemas, estos centros han contado históricamente con unas medidas de protección físicas muy robustas, por lo que en este aspecto se considera que su nivel de madurez es alto.

*Seguridad informática***.** El nivel de madurez es en general escaso, debido a que el escenario en el cual se encuentran actualmente los sistemas de monitorización y control en tiempo real no se contempló en su diseño.

*Funcionalidad***.** Este requisito ha sido cubierto de una forma muy eficaz desde el inicio del uso de este tipo de sistemas. Se basa en dos pilares fundamentales que son la robustez de los sistemas y equipos empleados y la redundancia, es decir, la duplicación de componentes críticos para el funcionamiento del sistema, de modo que, si el componente original deja de funcionar, la réplica pueda realizar las mismas funciones.

1.1.6.2 Comunicaciones

*Seguridad física***.** En general, el nivel de madurez es medio-bajo, debido en gran medida al uso de tecnologías inalámbricas y a las distancias cubiertas en ocasiones por estas comunicaciones.

*Seguridad informática***.** La seguridad informática en las comunicaciones es muy dependiente de la tecnología empleada, si bien es cierto que en los últimos años la preocupación por la seguridad ha fomentado la implantación de medidas como el cifrado de estas comunicaciones. Por ello, el grado de madurez en este aspecto se puede considerar medio.

*Funcionalidad***.** El grado de madurez en este caso también depende de la tecnología empleada, aunque en general se puede considerar que su nivel es alto.

1.1.6.3 Componentes finales

Seguridad física. En general, el nivel de seguridad es muy dependiente de la dispersión geográfica del sistema. Mientras que en entornos reducidos (por ejemplo, un edificio) la seguridad física generalmente es razonable, en sistemas que tienen componentes en zonas distantes, éstos suelen contar con escasas medidas de protección física.

*Seguridad informática***.** En general, su nivel de seguridad es escaso, al tratarse de componentes cuyo diseño no ha tenido en cuenta este aspecto. Además, suelen contar con programas informáticos obsoletos o configuraciones por defecto, hechos que incrementan notablemente su inseguridad.

*Funcionalidad***.** Al igual que en la inmensa mayoría de componentes y dispositivos de un sistema de monitorización y control en tiempo real, el grado de madurez en términos funcionales es muy elevado.

A modo de resumen, globalmente el nivel de madurez respecto a la funcionalidad se puede considerar elevado, aunque en cuanto a seguridad es escaso. No obstante, el nivel de seguridad informática se encuentra en evolución positiva.

1.1.7 Protocolos de comunicaciones industriales

Los protocolos de comunicación más usados para el control de procesos industriales a nivel en sistemas SCAD son:

Protocolo DNP3: es un protocolo de red distribuido basado en telemetría por medio de radio dispersión diseñado en 1993 y usado especialmente en USA y Canadá y está encaminado al sector eléctrico, es un protocolo de 4 capas (Enlace, Aplicación y de pseudo-transporte y física), este es el protocolo que se ha estado usando en subestaciones eléctricas en Colombia y el cual vamos a ver más a fondo.

ModBus: es un protocolo de comunicaciones industriales serial para interaccionar con PLC, es uno de los más antiguos y tuvo que migrar a la versión TCP/IP en la década de los 90, hoy en día es ampliamente usado en control industrial, trabaja en la capa de transporte y proporciona comunicación en modo cliente/servidor, actualmente no es muy usado en aplicaciones de subestaciones eléctricas.

Profibus: (Process Field Bus) Creado en 1989 pro Siemens en Alemania, es un protocolo muy usado en instalaciones que integran esta marca en sus equipos de

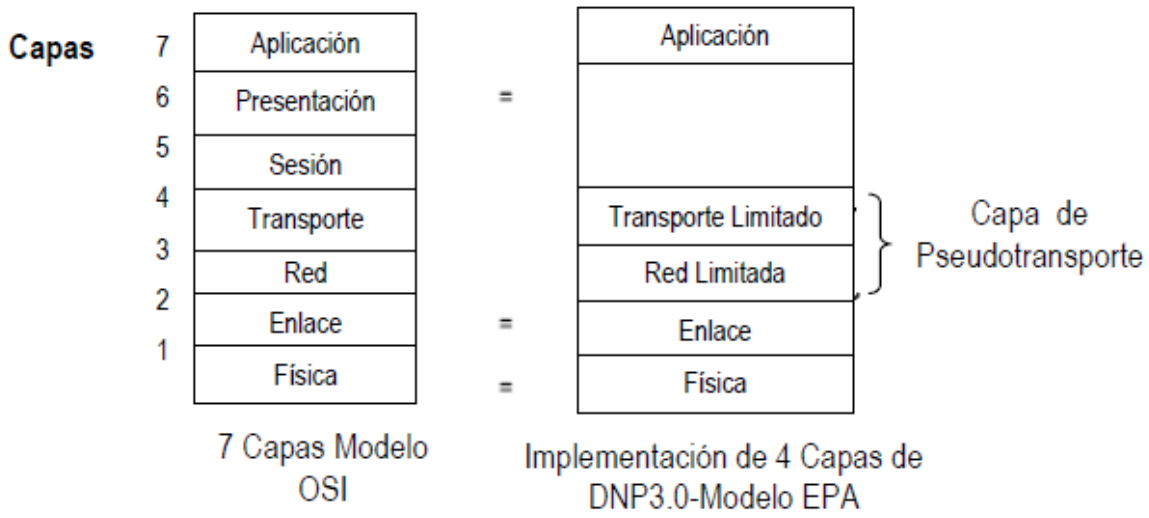
control industrial, y se basa en la comunicación serie con soporte sobre cable (rs-484. MBP) sobre fibra óptica, en la actualidad ha evolucionado a 2 variantes, Profibus DP (periféricos descentralizados) se usa en operación de sensores y actuadores y Profibus PA (Automatización de procesos) usado para monitorear equipos de medida en sistemas de control de procesos, en algunas plantas eléctricas que usan esta marca está presente el protocolo profibus y es necesario usar adaptadores de protocolo.

1.1.7.1 Protocolo DNP3 (Distributed Network Protocol 3.0)

Protocolo de red distribuido basado en telemetría por medio de radio dispersión que define la comunicación entre estaciones maestras, RTUs (Remote Terminal Unit), y otros dispositivos como IEDs (Intelligent Electronic Devices). Fue diseñado para dar interoperabilidad entre distintos sistemas como generación eléctrica, agua y gas y seguridad industrial.

Este protocolo fue diseñado específicamente para aplicaciones SCADA, para usarse en la adquisición de datos y envío de comandos de control entre una estación Maestra y una estación esclava, y se encarga de transmitir paquetes de datos de forma confiable, usando mensajes con secuencia determinística, y trabaja con tres capas del modelo OSI

Fig. 3 Relación del modelo OSI vs DNP3



Fuente: Practical Modern-Scada-Protocols[5]

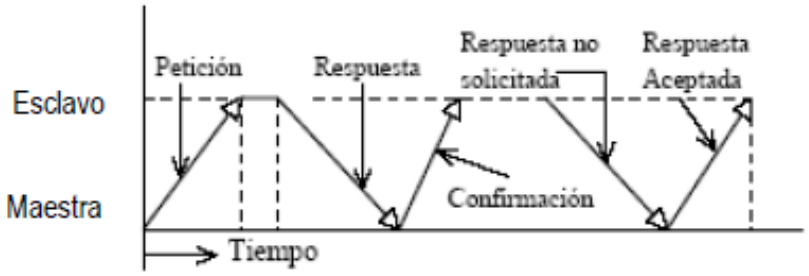
[5] Gordon Clarke, Deon Reynders. Practical Modern-Scada-Protocols: Dnp3 e IEC 60870.5 and Related-Systems. Publicación 2004. British Library. ISBN 07506 7995

Capa de aplicación DNP3:[6] Los datos de usuario son los datos que vienen desde la aplicación de usuario, se pueden ver en una aplicación tipo software puede ser en C++o un software especializado como Citect o Intelution como el HMI (Human Machine Interface). Los datos enviados pueden ser de tipo alarma o eventos asíncronos, datos digitales, datos analógicos, o un paquete de configuración desde una estación maestra MTU a una estación esclava RTU.

El tamaño total de la trama de datos no es limitado por el protocolo, se forman bloques de datos administrables llamados ASDU (Application Service Data Units). Seguidamente la capa aplicación crea la APDU (Application Protocol Data Units), El protocolo tiene cabecera de 2 bits para un mensaje de requerimiento y 4 bits para un mensaje de respuesta, para el cas de los comandos solo tiene una cabecera.

Cuando los bloques de ASDU a transmitir son grandes para un mensaje en la capa de aplicación, se crean múltiples fragmentos de tipo APDU con tamaños de 2048 bytes.

Fig. 4 Secuencia de comunicación entre un MTU y un RTU en la capa de aplicación

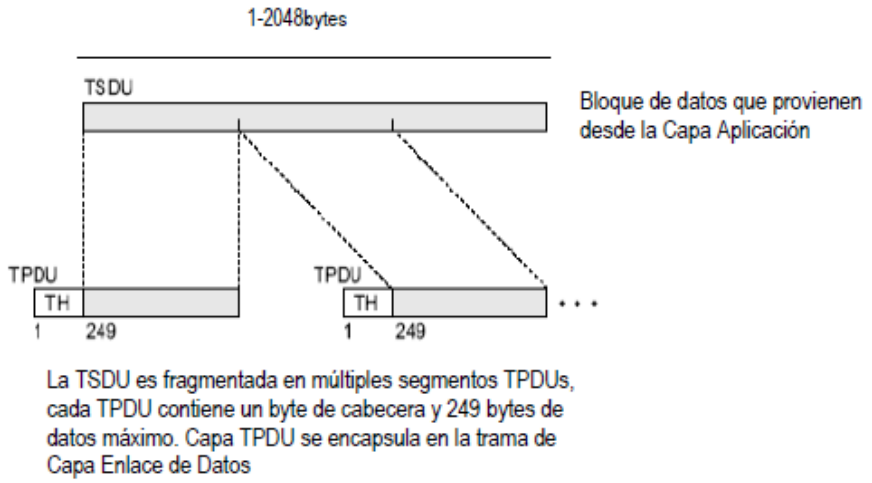


Fuente: ABB

Capa de Pseudotransporte: EL fragmento APDU de la capa de aplicación es encapsulado como la unidad de datos de servicio de transporte TSDU al interior de la capa de Pseudotransporte. Esta capa se divide en unidades mas pequeñas de datos llamados TPDU o unidades de protocolo, estas constan de un byte de cabecera, y un tamaño máximo de 249 bytes. En conclusión el tamaño total de encapsulamiento de las TPDU es de 250 bytes.

[6] VILLALBA, Julian Alejandro. Estudio y pruebas del protocolo de comunicación DNP3.0 sobre TCP/IP para la comunicación entre la central de generación de Cumbaya de la empresa eléctrica de Quito S.A y el Canace. 2010 .Pag. 59 - 61

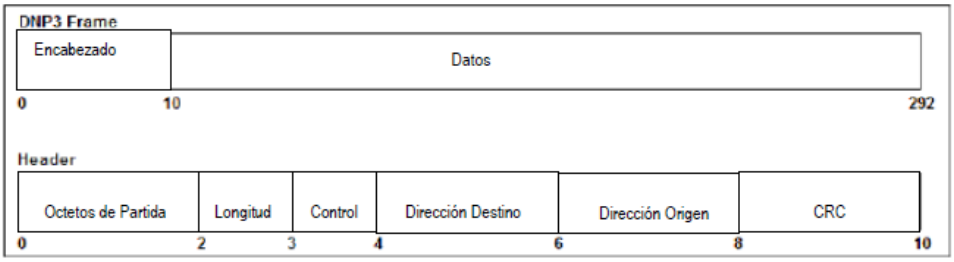
Fig. 5 Segmentación de la TSDU en varios TPDUs



Fuente: *Practical Modern-Scada-Protocols*[7]

Capa de enlace de Datos: Esta capa toma las TPDU desde la capa de Pseudotransporte y añade 10 bytes de cabecera. La capa de enlace tambien es la encargada de la detección de errores y funciones de corrección por medio de CRC (código de redundancia cíclica) de 16 bits, es decir cada TPDU es convertida a una trama LPDU de 292 bytes. Este formato de trama es conocida como FT3, que es un protocolo de comunicación industrial.

Fig. 6 Cabecera y datos de la trama en la capa enlace DPN3

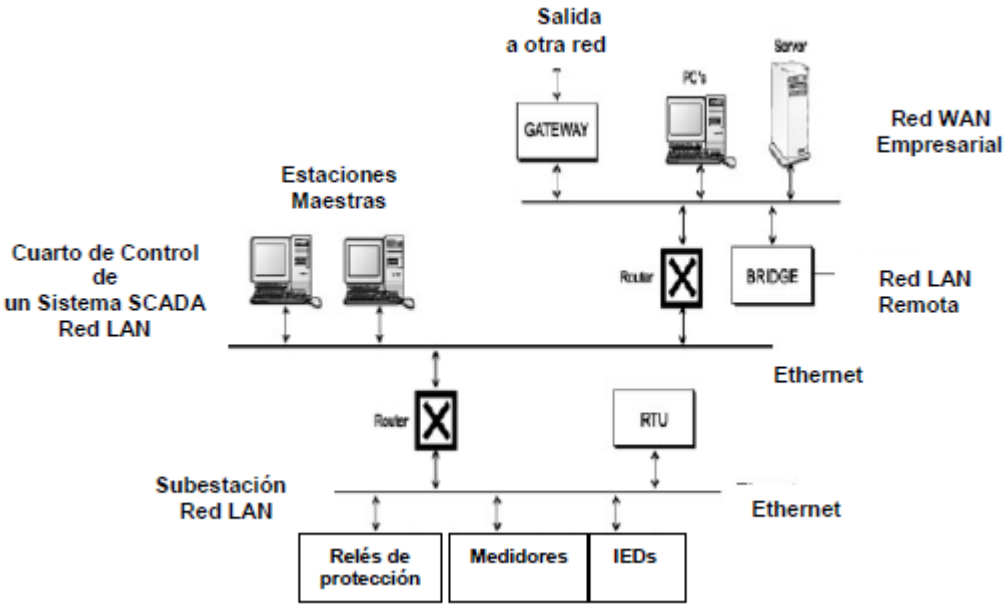


Fuente: ABB

[7] GORDON Clarke, DEON Reynders. Practical Modern-Scada-Protocols: Dnp3 e IEC 60870.5 and Related-Systems. Publicación 2004. British Library. ISBN 07506 7995

Capa Física: Esta capa convierte cada trama en una cadena de bits sobre el medio físico. Originalmente el protocolo DNP3 fue serial, con un formato de trama de 8 bits, con 1 bit de inicio, un bit de parada y sin paridad. Actualmente, el protocolo es usado sobre TCP/IP para el transporte de mensajes sobre red Ethernet, mediante encapsulamiento de datos en redes LAN, MAN y WAN, tiene velocidades de transmisión del orden de 10/100/1000Mbps.

Fig. 7 Topología típica de una red DNP3 sobre TCP/IP



Fuente: ABB

2. MARCO LEGAL

2.1. Norma y estándares de Seguridad informática

Para la matriz de riesgos y controles de seguridad informática se tendrá en cuenta apartes que puedan aplicarse a este proyecto de la norma ISO/IEC27001:2013.

2.2. Norma Internacional IEC 65850

IEC 61850 es la nueva norma internacional para la comunicación en subestaciones. Permite integrar todas las funciones de protección, control, medición y supervisión en una subestación; y proporciona los medios necesarios para aplicaciones de protección de subestaciones de alta velocidad, enclavamiento y arrastre. Combina la comodidad de Ethernet con el rendimiento y la seguridad, fundamentales en las subestaciones de la actualidad.

Fig. 8 Historia IEC 61850

Fuente: Introduction to the IEC 61850 substation comunication standard [8]

2.3. Otras Disposiciones legales

La prestación del servicio público de Energía Eléctrica en Colombia, está regido por las siguientes leyes y reglamentaciones, basadas principalmente en:

- La Ley 142 de Servicios Públicos Domiciliarios de 1994.
- La Ley 143 o Ley Eléctrica de 1994.
- Las Resoluciones expedidas por la Comisión de regulación de Energía y Gas CREG.
- El REGLAMENTO TÉCNICO DE INSTALACIONES ELÉCTRICAS – RETIE mediante el cual se fijan las condiciones técnicas que garantizarán la seguridad en los procesos de generación, transmisión, transformación, distribución y utilización de la energía eléctrica en Colombia.

[8] K. Hubert, K; Introduction to the IEC 61850 substation comunication standard. Jornada de Automación de Subestaciones Eléctricas con la Norma IEC 61850, p. 18, Bogotá, 2008.

Leyes y normas sobre seguridad informática y digital en Colombia

- Ley 1273 de 2009. De la protección de la información y de los datos

3. METODOLOGÍA

El presente proyecto se inscribe dentro del área de telecomunicaciones, específicamente en la línea de infraestructura tecnológica y seguridad en redes.

El Universo son todas las subestaciones eléctricas modernas que pueden manejar sistemas SCADA e interconexión con el HMI principal de la EBSA a nivel Duitama, para nuestro caso hay 3 subestaciones eléctricas, la subestación Higueras, que se encuentra ubicada en la entrada sur de la ciudad, otra la subestación es San Antonio a la salida oriente y por último la subestación Maranta en el centro de la ciudad, cada una cuanta con diferente carga y transformadores de diferente tamaño, pero el sistema de control y comunicación SCADA es idéntico, así que tomaremos por comodidad la Subestación de oriente a la cual se tuvo acceso y fue en donde realizamos el estudio del presente proyecto.

El instrumento de recolección de información que se usó inicialmente fue las entrevistas con personal a cargo de la subestación principal de Duitama Boyacá, en donde se recogió información sobre los sistemas de comunicación y control de la subestación, que normas internacionales está sujeta y que protocolos de seguridad tienen, para eventuales fallas del sistema informático de comunicación y control. (Por ser una entidad privada con políticas de confidencialidad, esta información no será lo suficientemente profunda ni nutrida, así que será complementada con información técnica consultada).

La metodóloga que se aplicó a este proyecto fue una mezcla entre los métodos empíricos, basados en la observación y la entrevista y los métodos teóricos, basados en hipótesis como el planteamiento del problema el cual es revisar si es posible que se puedan presentar fallas de seguridad informática en los sistemas SCADA y deductivos basados en la recolección de información se generan conclusiones y recomendaciones para evitar que estas fallas se puedan presentar.

También de estudio de la norma internacional IEC 61850, la cual es la norma que rige los sistemas de comunicación de subestaciones eléctricas y verificar si la están aplicando en las subestaciones actuales o tiene planes para su implementación a futuro y protocolo DNP3.0, para comunicación de RTU por medio de radiofrecuencia en la subestación eléctrica.

Se realizará una matriz de riesgos de seguridad informática, basado en la metodóloga de la presente investigación, para evidenciar las posibles vulnerabilidades que se podrían presentar y una valoración del riesgo en los activos de la información.

Según los resultados encontrados, procederá a la realización de plan de tratamiento de riegos y controles de seguridad informática que permitan mitigar las diferentes vulnerabilidades de seguridad informática en la subestación eléctrica, y

posteriormente se propondrá un plan de mejora, para la seguridad en los sistemas de comunicación y la información transmitida de la subestación a los centros de control y a otras subestaciones eléctrica, basados en los hallazgos que se observaron y el estudio de las normas vistas anteriormente.

4. RESULTADOS

Se realizó la visita a las instalaciones de GENSA S.A en donde se encuentra la subestación de oriente (Figura 3), esta es la que alimenta el circuito del municipio de Duitama y San Antonio Belencito con una carga de 115 kV, en un patio de elevación para envió al inter-conexionado oriente del departamento y Santander

Figura 9 Subestación de Oriente

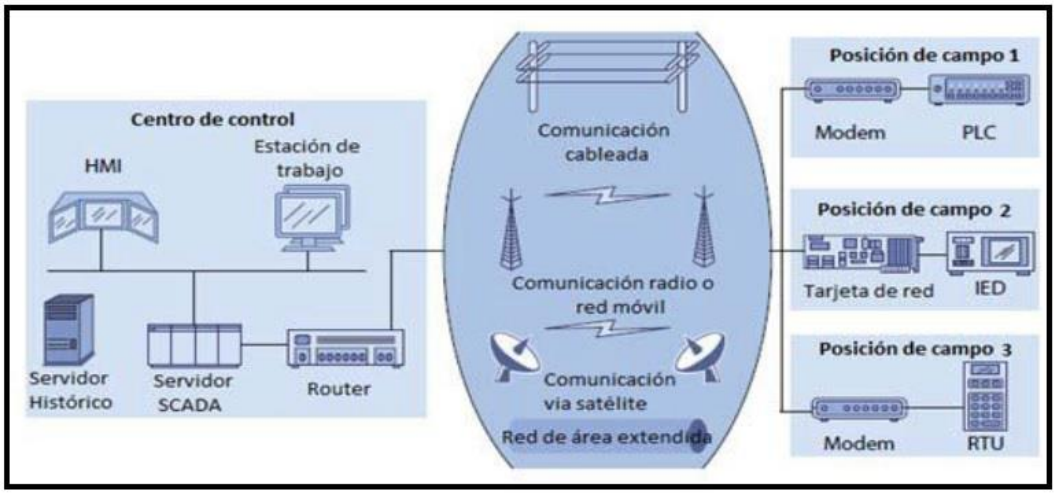
Fuente: GENSA

Esta Subestación esta monitoreada y controlada mediante telemetría, con el sistema SCADA central que se comunica con protocolos DNP 3.0 sobre TCP/IP y IEC 870-5-104, el cual puede intercambiar el protocolo a través del software sin necesidad de adicionar o cambiar tarjetas del controlador del re-conectador, cuenta con un puerto Ethernet RJ-45 para conexión a MODEM celular o canal privado de datos (comunicación de respaldo), y un (1) puerto Ethernet MT-RJ fibra óptica para conexión con la central de monitoreo HMI en la EBSA Tunja. En los equipos de comunicación usados los protocolos de comunicación DNP e IEC, son nativos en el control sin convertidores de protocolo.

Según Cesar Calderon funcionario de la EBSA entrevistado, la interfaz de comunicación al módulo de control, permite ser utilizado por una computadora remota para monitorear y controlar la subestación, por aplicaciones de SCADA de Centro de Control a distancia por medio de estaciones de trabajo del operario de la red de distribución o la conexión a un sistema de automatización de redes de distribución (DSA) para el control automático por una computadora de supervisión HMI desde el centro de control.

Se puede apreciar el modelo de comunicación que se está implementando en la subestación eléctrica (Figura. 4), en donde interviene el HMI (Interfaz Hombre Maquina) (Figura. 5) que se encuentra en el centro de control de la EBSA Tunja, en este centro de control, operarios están al tanto de los datos que llegan de las diferentes subestaciones y monitorean constantemente el estado de las redes eléctricas para garantizar la prestación del servicio eléctrico con calidad.

Figura 10 Comunicaciones en subestaciones con SCADA



Fuente: EBSA

El medio de comunicación, que en este caso es por fibra óptica con redundancia por red móvil de radio frecuencia, es el medio por donde los datos recogidos de la subestación y las variables de medida y acción a posibles fallos, viajan de un extremo a otro proporcionando una comunicación bidireccional y en tiempo real de los datos digitales, que son medidos y no calculadas sobre el control del sistema SCADA, esto se hace mediante un rack de comunicaciones ubicado en la casa de control de la subestación (figura. 6)

Figura 11 HMI EBSA

Fuente: EBSA

Figura 12 Rack comunicaciones Subestación Oriente

Fuente: GENSA

La subestación se adapta a las siguientes interfaces físicas sin que exista un límite la instalación de módulos futuros para expansión de los puertos de comunicaciones (Figura. 7), y en caso de falla se pueden usar cualquiera de las siguientes interfaces:

- Un puerto Ethernet RJ45
- Dos Puertos seriales RS-232 DB9.
- Un Puerto Ethernet de fibra Óptica MT-RJ

Figura 13 Montaje comunicaciones EBSA Tunja

Fuente: EBSA

Los equipos de campo que manejan el sistema SCADA de la subestación como son el PLC (Controlador Lógico Programable) (Figura. 8) el cual es el encargado de controlar los actuadores de la subestación y medir las diferentes variables como

corriente de línea, voltaje de línea, temperatura del transformador entre otros, el IED (Dispositivo Electrónico Inteligente) o el RTU (Unidad Terminal Remota) (Figura. 9) Son los elementos inteligentes que controlan todo el proceso y además se comunican con el HMI para la supervisión y control a distancia, por medio del Gateway (Figura. 10) de comunicaciones especializado en subestaciones.

Figura 14 PLC Subestación de oriente

Fuente: GENSA

Figura 15 RTU Subestación de oriente

Fuente: GENSA

Figura 16 Gateway Subestación

Fuente: GENSA

Además del Gateway se utilizan módems con las siguientes características:

- Enrutador GPRS/EDGE Grado industrial.
- Control de flujo de información mediante Firewall y VPN.
- Interfaz Ethernet 10/100 Base T.
- Puerto de comunicación RJ45 para transferencia de datos.
- Cuatro bandas: 850/900/1800/1900 MHz
- Velocidades de conexión clase 12 para GPRS y clase 10 para EDGE
- Garantía de estabilidad del enlace y el servicio GPRS 7 días x 24 horas.
- Temperatura de operación: 0-70ºC
- Administración remota vía Web, Telnet y FTP.

Para el caso del canal de datos privado se usan equipos con protección contra interferencias, con 1 interfaz Ethernet 10/100 Base T, con firewall, con VPN, con administración remota vía Web, Telenet y FTP, lo cual garantiza la estabilidad del canal en un 99.6%, estos están implementados por fibra óptica o radio enlaces de microondas, los cuales tienen respaldo de energía eléctrica por medio de plantas de emergencia y UPS con autonomía de 8 horas. Para la implementación de radio enlaces se hace uso de frecuencias licenciadas lo cual impide interferencias a otros sistemas.

No se considera viable el esquema de conectividad al Centro de Control SCADA por medio de canales de Internet debido a los riesgos de seguridad informática inherentes a este sistema, por lo tanto por ahora, no está considerado dentro del esquema de comunicación.

4.1 IDENTIFICACIÓN DE ACTIVOS

Los activos que se tendrán en cuenta a la hora de realizar la identificación de riesgos en la información (Disponibilidad, Integridad, Confidencialidad y no repudio, trazabilidad), son los elementos que conforman el sistema SCADA como: HMI principal (HMI P), HMI en subestación eléctrica (HMI SE), RTU, Protocolos (PT), Sistema de telecomunicación (ST) teniendo en cuenta la siguiente tabla:

Tabla 1 Colores Valoración activos

Extremo
Alto
Moderado
Bajo

Tabla 2 Matriz de Identificación de activos de información

Activo	Disponibilidad		Integridad		Confidencialidad		No repudio		Trazabilidad	
	Valoración	Justificación	Valoración	Justificación	Valoración	Justificación	Valoración	Justificación	Valoración	Justificación
HMI P	Extremo	El monitoreo y control del sistema eléctrico no se podría realizar.	Alto	Si no funciona se puede enviar cuadrilla para maniobra manual.	Moderado	Información operativa convencional que no necesariamente es confidencial	Bajo	Los ajustes al HMI son realizaos por expertos, responsabilizados y registrados.	Extremo	Se deben registrar los cambios para futuras adecuaciones del sistema a nuevos elementos.
HMI SE	Alto	La supervisión y control de la SE es muy dispendiosa, la información no esta disponible	Moderado	Si no funciona se puede hacer manual.	Moderado	Información operativa convencional que no necesariamente es confidencial	Bajo	Los ajustes al HMI son realizaos por expertos, responsabilizados y registrados.	Extremo	Se deben registrar los cambios para futuras adecuaciones del sistema a nuevos elementos.
RTU	Moderado	La supervisión del elemento no está disponible inaccesible	Extremo	Por ser un elemento base para la transmisión y recepción de información, su integridad es indispensable	Moderado	Información operativa convencional que no necesariamente es confidencial	Bajo	Los ajustes al RTU son realizaos por expertos, responsabilizados y registrados.	Extremo	Se deben registrar los cambios para futuras adecuaciones del sistema a nuevos elementos.

PT	Bajo	Los protocolos no están disponibles	Bajo	Los protocolos son altamente confiables	Bajo	Protocolos usados son standard	Bajo	Los protocolos no aplican repudio	Bajo	Logs de estos protocolos no son necesarios
ST	Extremo	El monitoreo y control del sistema eléctrico no se podría realizar.	Alto	Si no funciona se puede enviar cuadrilla para maniobra manual.	Moderado	Información operativa convencional que no necesariamente es confidencial	Bajo	Los ajustes al sistema de telecomunicación son realizaos por expertos, responsabilizados y registrados.	Extremo	Se deben registrar los cambios para futuras adecuaciones del sistema a nuevos elementos.

4.2 VALORACIÓN DE RIESGOS

Así como los activos se pueden valorar en una escala cualitativa, también los riesgos pueden ser valorados teniendo en cuenta los pilares fundamentales de la seguridad informática como son: disponibilidad, confidencialidad, integridad, trazabilidad, (no repudio se excluye ya que, en el anterior matiz, presento riesgo moderado y bajo)

En este caso, con base en las vulnerabilidades que pueden ser explotadas por diferentes amenazas a las que se exponen los activos, se pueden determinar los riesgos de forma tal, que sean identificables fácilmente y así poder realizar un control optimo del proceso.

Para este caso nos basaremos en la siguiente tabla para calificar el riesgo:

Tabla 3 Colores valoración riesgo

IA	Inaceptable
ID	Inadmisible
TO	Tolerable
AC	Aceptable

Tabla 4 Valoración del riesgo en perdida de disponibilidad del activo

Vulnerabilidad	Amenaza	RTU	HMI SE	HMI P	ST	PT
Controles Inadecuados de acceso físico/lógico	Abuso de privilegios	IA	IA	IA		
	Acceso no autorizado	ID	ID	ID		
	Denegación de servicios	ID	ID	ID		
	Ataque dirigido		ID	ID	ID	
Configuración incorrecta o inadecuada	Acceso no autorizado	ID	ID	ID		
	Ataque dirigido		ID	ID	ID	
	Caída del servicio por agotamiento de recurso.		ID	IA	ID	
	Denegación de servicios	ID	ID	ID	ID	
Insuficiente protección contra virus y código malicioso	Fallas en el software		ID	ID		
	Vulnerabilidad de los programa		ID	ID		
	Denegación de servicios		ID	ID		
Punto único de fallo	Fallas de hardware				ID	
	Caída del servicio por agotamiento de recurso.				ID	
	Ataque dirigido				ID	
Mantenimientos predictivos o correctivos inadecuados	Fallas de hardware				ID	
	Denegación de los soportes de almacenamiento				ID	
	Avería de origen físico/lógico				ID	

Tabla 5 Valoración del riesgo en perdida de confidencialidad del activo

Vulnerabilidad	Amenaza	RTU	HMI SE	HMI P	ST	PT
Controles Inadecuados de acceso físico/lógico	Abuso de privilegios	IA		TO	TO	
	Acceso no autorizado	IA		IA	IA	
	Escaneos de red	IA			IA	
	Análisis de trafico			IA		
Configuración incorrecta o inadecuada	Abuso de privilegios	IA		TO	IA	
	Acceso no autorizado	IA	IA	IA	IA	
	Escaneos de red	IA			ID	
	Análisis de trafico		IA	IA		
	Escapes de información			IA		
Poca conciencia sobre seguridad de la información	Divulgación de información			IA		
	Ataque de ingeniería social			IA		
	Fuga o robo de información		IA	IA		
Inadecuado procedimiento de actualizaciones de seguridad y antivirus	Errores de administrador		TO	IA		
	Vulnerabilidad de programas		IA	IA		
	Difusión de software dañino					

Tabla 6 Valoración del riesgo en perdida de integridad del activo

Vulnerabilidad	Amenaza	RTU	HMI SE	HMI P	ST	PT
Controles Inadecuados de acceso físico/lógico	Abuso de privilegios	IA	IA	IA		TO
	Acceso no autorizado	IA	ID	ID		IA
	Ataque dirigido	IA	ID	ID		
	Manipulación de la configuración.		ID	ID	ID	TO
	Manipulación de programas		IA	IA		
Configuración incorrecta o inadecuada	Errores de administrador	IA	ID	ID		IA
	Abuso de privilegios	IA	IA	IA	IA	
	Acceso no autorizado	IA		IA		
	Difusión software dañino		ID	ID		IA
	Fallas del software		ID	ID		
	Errores de los usuarios			IA		
	Fallas de hardware				ID	
	Ataque dirigido				ID	
	Vulnerabilidad de programas					IA
Inadecuado esquemas de reposición de activos antiguos	Acceso no autorizado		ID	ID	ID	
	Abuso de privilegios		ID	ID		
	Ataque dirigido		ID	ID	ID	ID
	Difusión software dañino		ID	ID		
Mantenimientos predictivos o correctivos inadecuados	Fallas de hardware				ID	
	Denegación de los soportes de almacenamiento				ID	

Tabla 7 Valoración del riesgo en perdida de trazabilidad del activo

Vulnerabilidad	Amenaza	RTU	HMI SE	HMI P	ST	PT
Escasos registros de Logs o variables auditables	Fallas de hardware	IA				
	Errores de administrador	IA	IA	ID	IA	IA
	Acceso no autorizado	IA			IA	
	Ataque dirigido				IA	
	Abuso de privilegios				IA	
	Manipulación de la configuración.		IA			IA
	Errores de configuración					IA
	Errores de monitorización					IA
	Destrucción de información		IA	ID		
Pocos mecanismos de control y monitoreo	Errores de administrador	IA	IA	ID	IA	
	Errores de configuración	IA			IA	
	Ataque dirigido	IA	IA	ID		
	Errores de monitorización		ID	ID		

4.3 CONTROLES.

Activo	Riesgo	Amenaza	Vulnerabilidad	Controles
ST	Perdida de disponibilidad de hardware	DNS	Incorrecta configuración	Entrenamiento al personal a cargo
		Caída de sistema por agotamiento de recursos		Análisis de rendimiento y capacidad del sistema
		Ataque dirigido		- Implementación de un IDS o Host IPS - Uso de protocolos seguros - Segmentación de red en VLANS - Implementación de un Firewall - Uso de un control de acceso a la red NAC
		Ataque dirigido	Controles débiles de acceso lógico o físico a un activo de información	- Implementación de un IDS o Host IPS - Líneas base de seguridad. - Implementación de un Firewall
		Daño de tipo físico o lógico	Mantenimiento preventivo y correctivo deficiente	Renovación de equipamiento tecnológico
		Falla de hardware		Programas de mantenimiento continuos
		Denegación de los soportes de almacenamiento		Programa de mantenimiento preventivo y correctivo
		Falla de hardware	Punto de falla único	Sistemas
		Ataque dirigido		- Implementación de un IDS o Host IPS - Líneas base de

				seguridad. - Implementación de un Firewall
		Caída del sistema por agotamiento de recursos		Análisis de rendimiento y capacidad del sistema
		Ataque dirigido	Falta de control en el acceso físico y lógico a un activo de información	- Implementación de un IDS o Host IPS - Líneas base de seguridad. - Implementación de un Firewall
RTU	Perdida de disponibilidad de hardware	DNS	Incorrecta configuración	Entrenamiento al personal
		Acceso no autorizado		- Administración de privilegio y roles - Sistema de Autenticación eficientes - Control de acceso físico al hardware
		DNS	Controles débiles de acceso lógico o físico a un activo de información	- Implementación de un IDS o Host IPS - Líneas base de seguridad. - Implementación de un Firewall
		Acceso no autorizado		- Administración de privilegio y roles - Sistema de Autenticación - Control de acceso físico al hardware
HMIP	Perdida de disponibilidad de software	Acceso no autorizado	Incorrecta configuración	- Administración de privilegio y roles - Sistema de Autenticación

		Ataque dirigido		- Implementación de un IDS o Host IPS - Líneas base de seguridad. - Implementación de un Firewall
		DNS		- Implementación de un IDS o Host IPS - Líneas base de seguridad. - Implementación de un Firewall
		Acceso no autorizado	Controles débiles de acceso lógico o físico a un activo de información	- Administración de privilegio y roles - Sistema de Autenticación eficientes
		Ataque dirigido		- Implementación de un IDS o Host IPS - Líneas base de seguridad. - Implementación de un Firewall
		DNS		- Implementación de un IPS o Host IPS - Líneas base de seguridad. - Implementación de un Firewall
		Ausencia de software certificado	Falta de protección contra virus y código malicioso	- Adquisición de sistemas detectores de malware - Pruebas y control de cambios en el software
		Programas sin los respectivos parches de seguridad		- Adquisición de sistemas detectores de malware - Pruebas y control de

				cambios en el software - Aplicación de parches y actualización de software
		DNS		- Adquisición de sistemas detectores de malware
HMI S-E	Perdida de disponibilidad de software	Acceso no autorizado	Incorrecta configuración	- Administración de privilegio y roles - Sistema de Autenticación
		Ataque dirigido		- Implementación de un IDS o Host IPS - Líneas base de seguridad. - Implementación de un Firewall
		DNS		- Implementación de un IDS o Host IPS - Líneas base de seguridad. - Implementación de un Firewall
		Acceso no autorizado	Controles débiles de acceso lógico o físico a un activo de información	- Administración de privilegio y roles - Sistema de Autenticación
		Ataque dirigido		- Implementación de un IDS o Host IPS - Líneas base de seguridad. - Implementación de un Firewall
		DNS		- Implementación de un IDS o Host IPS - Líneas base de seguridad.

				- Implementación de un Firewall
		Ausencia de software certificado	Falta de protección contra virus y código malicioso	- Adquisición de sistemas detectores de malware - Pruebas y control de cambios en el software
		Programas sin los respectivos parches de seguridad		- Adquisición de sistemas detectores de malware - Pruebas y control de cambios en el software - Aplicación de parches y actualización de software
		DNS		- Adquisición de sistemas detectores de malware
ST	Perdida de confidencialidad del Hardware	Escaneo de la red	Incorrecta configuración	- Implementación de un IDS o Host IPS - Uso de protocolos seguros - Segmentación de red en VLANS - Implementación de un Firewall - Uso de un control de acceso a la red NAC
RTU	Perdida de confidencialidad del Hardware	Acceso no autorizado	Controles débiles de acceso lógico o físico a un activo de información	- Sistema de Autenticación eficientes - Control de acceso físico al hardware
		Escaneo de red		
		Abuso de privilegios		- Administración de privilegio y roles
		Acceso no autorizado	Incorrecta configuración	- Sistema de Autenticación eficientes - Control de acceso

				físico al hardware
		Escaneo de red		- Implementación de un IDS o Host IPS - Uso de un control de acceso a la red NAC
		Abuso de privilegios		- Administración de privilegio y roles
HMIP	Perdida de confidencialidad del Software	Acceso no autorizado	Controles débiles de acceso lógico o físico a un activo de información	- Capacitación de personal - Líneas base de seguridad. - Implementación de un Firewall
		Análisis de trafico		- Implementación de un IDS o Host IPS - Uso de un control de acceso a la red NAC
		Acceso no autorizado	Incorrecta configuración	- Capacitación de personal - Líneas base de seguridad. - Implementación de un Firewall
		Análisis de trafico		- Implementación de un IDS o Host IPS - Uso de un control de acceso a la red NAC
		Robo o fuga de información	Falta de conciencia sobre seguridad de la información	- Capacitación de personal - Líneas base de seguridad.
		Ataque ingeniera social		- Capacitación de personal - Líneas base de seguridad.
		Divulgación de		- Capacitación de

		información		personal - Líneas base de seguridad.
		Falla del software	Falta de protección contra virus y código malicioso	- Pruebas y control de cambios en el software - Sistema redundantes
		Programas sin los respectivos parches de seguridad		- Adquisición de sistemas detectores de malware - Pruebas y control de cambios en el software - Aplicación de parches y actualización de software
		Fallas del Administrador		- Capacitación de personal - Líneas base de seguridad. - Implementación de un Firewall
HMI S-E	Perdida de confidencialidad del Software	Acceso no autorizado	Incorrecta configuración	- Capacitación de personal - Líneas base de seguridad. - Implementación de un Firewall
		Análisis de trafico		- Implementación de un IDS o Host IPS - Uso de un control de acceso a la red NAC
		Fallas del Administrador	Falta de protección contra virus y código malicioso	- Capacitación de personal - Líneas base de seguridad. - Implementación de un Firewall

		Falla del software		- Pruebas y control de cambios en el software - Sistema redundantes
ST	Perdida de integridad del Hardware	Manipulación de la configuración	Controles débiles de acceso lógico o físico a un activo de información	- Pruebas y control de cambios en el hardware
		Falla de hardware	Incorrecta configuración	- Mantenimiento predictivo y correctivo
		Ataque dirigido		- Implementación de un IDS o Host IPS - Líneas base de seguridad.
		Acceso no autorizado	Esquemas deficientes de actualización de activos obsoletos	- Administración de privilegio y roles - Sistema de Autenticación eficientes - Control de acceso físico al hardware
		Ataque dirigido		- Implementación de un IDS o Host IPS - Líneas base de seguridad. - Implementación de un Firewall
		Falla de hardware	Falta de mantenimiento predictivo, preventivo y/o correctivo,	- Mantenimiento predictivo y correctivo
		Degradación de soportes de almacenamiento		- Renovación del activo actualización.
HMIP	Perdida de integridad del Software	Manipulación de la configuración	Controles débiles de acceso lógico o físico a un activo de información	- Pruebas y control de cambios en el software
		Acceso no autorizado		- Administración de privilegio y roles - Sistema de Autenticación eficientes
		Manipulación de		- Pruebas y control de

		programas		cambios en el software
		Ataque dirigido		- Implementación de un IDS o Host IPS - Líneas base de seguridad. - Implementación de un Firewall
		Falla del software	Incorrecta configuración	- Pruebas y control de cambios en el software - Sistema redundantes
		Fallas del Administrador		- Capacitación de personal - Líneas base de seguridad. - Implementación de un Firewall
		Software Dañino		- Adquisición de sistemas detectores de malware
		Acceso no autorizado		- Administración de privilegio y roles - Sistema de Autenticación eficientes
		Software Dañino	Esquemas deficientes de actualización de activos obsoletos	- Adquisición de sistemas detectores de malware
		Acceso no autorizado		- Administración de privilegio y roles - Sistema de Autenticación eficientes
		Ataque dirigido		- Implementación de un IDS o Host IPS - Líneas base de seguridad. - Implementación de un Firewall
HMI S-	Perdida de	Manipulación de la	Controles débiles de	- Pruebas y control de

E	integridad del Software	configuración	acceso lógico o físico a un activo de información	cambios en el software
		Acceso no autorizado		- Administración de privilegio y roles - Sistema de Autenticación eficientes
		Ataque dirigido		- Implementación de un IDS o Host IPS - Líneas base de seguridad. - Implementación de un Firewall
		Falla del software	Incorrecta configuración	- Pruebas y control de cambios en el software - Sistema redundantes
		Fallas del Administrador		- Capacitación de personal - Líneas base de seguridad. - Implementación de un Firewall
		Software Dañino		- Adquisición de sistemas detectores de malware
		Software Dañino	Esquemas deficientes de actualización de activos obsoletos	- Adquisición de sistemas detectores de malware
		Acceso no autorizado		- Administración de privilegio y roles - Sistema de Autenticación eficientes
		Ataque dirigido		- Implementación de un IDS o Host IPS - Líneas base de seguridad. - Implementación de un Firewall

PT	Perdida de integridad del Software	Ataque dirigido	Inadecuado esquemas de reposición de activos antiguos	- Implementación de un IDS o Host IPS - Líneas base de seguridad. - Implementación de un Firewall
HMIP	Perdida de Trazabilidad del Software	Fallas del Administrador	Pocos registros en logs o variables auditables	- Capacitación de personal - Líneas base de seguridad. - Implementación de un Firewall
		Destrucción de información		- Capacitación de personal - Aplicación de revisiones y auditorias
		Fallas del Administrador	Escasos mecanismos de monitoreo y control	- Capacitación de personal - Aplicación de revisiones y auditorias - Implementación de Sistema SOC y correlacionado de eventos
		Errores de monitoreo		- Capacitación de personal - Aplicación de revisiones y auditorias - Implementación de Sistema SOC y correlacionado de eventos
		Ataque dirigido		- Implementación de un IDS o Host IPS - Líneas base de seguridad. - Implementación de un Firewall

HMI S-E	Perdida de Trazabilidad del Software	Fallas del Administrador	Pocos registros en logs o variables auditables	- Capacitación de personal - Líneas base de seguridad. - Implementación de un Firewall
		Manipulación de la configuración		- Pruebas y control de cambios en el software
		Perdidas de información		- Servidor de respaldo y sistemas redundantes
		Falla de Administrador	Escasos mecanismos de monitoreo y control	- Capacitación de personal - Aplicación de revisiones y auditorias - Implementación de Sistema SOC y correlacionado de eventos
		Errores de monitoreo		- Capacitación de personal - Aplicación de revisiones y auditorias - Implementación de Sistema SOC y correlacionado de eventos
		Ataque dirigido		- Implementación de un IDS o Host IPS - Líneas base de seguridad. - Implementación de un Firewall
RTU	Perdida de Trazabilidad del Hardware	Fallas de hardware	Pocos registros en logs o variables auditables	- Mantenimiento predictivo y correctivo
		Fallas del Administrador		- Capacitación de personal - Líneas base de seguridad.

		Acceso no autorizado		- Administración de privilegio y roles - Sistema de Autenticación eficientes
		Fallas del Administrador	Escasos mecanismos de monitoreo y control	- Capacitación de personal - Aplicación de revisiones y auditorias - Implementación de Sistema SOC y correlacionado de eventos
		Errores de configuración		- Uso de un control de acceso a la red NAC
		Ataque dirigido		- Implementación de un IDS o Host IPS - Líneas base de seguridad.
PT	Perdida de Trazabilidad del Software	Fallas del Administrador	Escasos mecanismos de monitoreo y control	- Capacitación de personal - Aplicación de revisiones y auditorias - Implementación de Sistema SOC y correlacionado de eventos
		Manipulación de la configuración		- Pruebas y control de cambios en el software
		Error de configuración		- Uso de un control de acceso a la red NAC
		Errores de monitoreo		- Capacitación de personal - Aplicación de revisiones y auditorias - Implementación de Sistema SOC y correlacionado de eventos
	Perdida de	Fallas del	Pocos registros en	- Capacitación de

ST	Trazabilidad del Hardware	Administrador	logs o variables auditables	personal - Líneas base de seguridad.
		Acceso no autorizado		- Administración de privilegio y roles - Sistema de Autenticación eficientes
		Ataque dirigido		- Implementación de un IDS o Host IPS - Líneas base de seguridad. - Implementación de un Firewall
		Abuso de privilegios		- Administración de privilegio y roles - Sistema de Autenticación eficientes
		Fallas del Administrador	Escasos mecanismos de monitoreo y control	- Capacitación de personal - Aplicación de revisiones y auditorias - Implementación de Sistema SOC y correlacionado de eventos
		Error de configuración		- Uso de un control de acceso a la red NAC

4.4 PLAN DE MEJORA Y MITIGACIÓN DE RIESGOS

Tomando la información sobre los controles propuestos en la tabla anterior, explicaremos como estos podrían ayudar a mitigar los riesgos detectados tanto en los sistemas de transmisión y comunicación y los inherentes al manejo por parte del personal del sistema SCADA de la subestación.

Como se sabe es indispensable asegurar el sistema SACDA, ante los peligros informáticos lo cual es proceso continuo y permanente, ya que cada día evolucionan nuevas amenazas que explotan las vulnerabilidades del sistema las cuales deben ser analizadas para implementar nuevas alternativas de seguridad que permitan que el sistema sea más confiable y menos susceptible a fallas.

También es conocido, que la aplicación de estos controles al sistema de control SCADA, debe ser paulatina, repartida en fases, para que el proceso sea gradual y se acomode a las necesidades de seguridad, tanto en el plazo inmediato, como al corto y mediano plazo.

Para este plan de mejora se proponen las siguientes Fases:

- Aseguramiento de la red: Como se vio anteriormente en la tabla de controles es necesario que la red que maneja la supervisión y tráfico de variables de medidas y actuadores entre la subestación y el centro de mando debe estar aislado lógicamente de la red administrativa de la empresa de energía, así mismo como la aplicación de control de acceso a las subestación y manejo de credenciales de acceso fuertes, esto lo veremos con más detalle en el apartado 4.4.1

- Entrenamiento al personal y auditorias de seguridad informática y física: Para esta fase se propone realizar un plan de mejoramiento en donde se envíe periódicamente por correo píldoras o tips sobre la seguridad informática como parte esencial de protección a la información de la organización así como realizar charlas y capacitaciones al personal sobre el buen manejo de los sistemas y los riesgos a los que se está expuesto, así mismo programar Auditorias anuales para la verificación de los requisitos mínimos en cuanto a seguridad informática, esto lo ahondaremos en el ítem 4.4.2

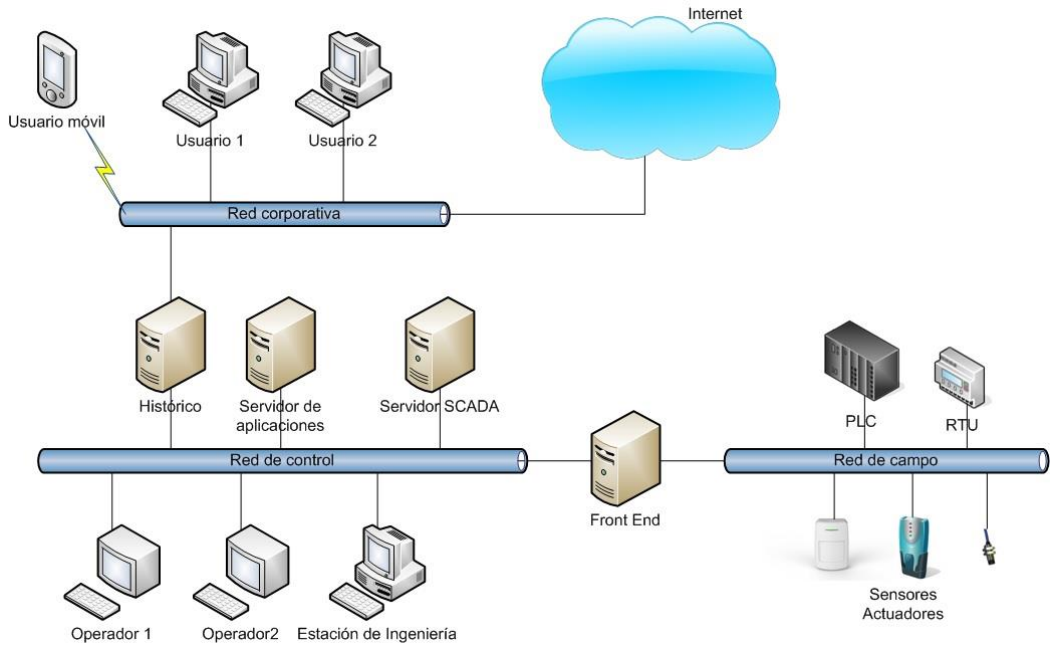
- Procedimientos y mecanismos de protección del sistema SCADA: en este ítem realizaremos las respectivas recomendaciones en cuanto a configuración y adquisición de equipos para la protección del activo informático que maneja el sistema de control de la subestación, y cual protocolo de comunicación es más confiable, esto lo veremos en el numeral 4.4.3

4.4.1 Aseguramiento de la red SCADA

El sistema SCADA debe estar conectado a la red únicamente por medio de accesos lógicos necesarios y aislados de otras dependencias, es decir aplicar una arquitectura, basa en segmentación de red, esto permite que cada subred tenga un uso específico y asegurar que los usuarios de otras redes, tengan las restricciones de acceso no autorizado a los elementos vitales de funcionamiento como RTU o PLC que controla la subestación.

Actualmente, la empresa EBSA maneja una red básica para las subestaciones como se muestra en la Fig 17, como no se han presentado incidentes de tipo informático en la región, ni ataques dirigidos a la seguridad informática a sus instalaciones, no se le ha dado la suficiente importancia a este tema por lo que se propone la implementación de una segmentación de red más avanzada con la inclusión de firewall entre cada dependencia para asegurar la red SCADA de la subestación.

Fig. 17 Red de control de la subestación sin segmentar



Fuente: Instituto nacional de ciberseguridad

También es conveniente que se configure el firewall de los equipos de la red corporativa, estos firewall pueden ser de aplicación es decir, software que aísle las dependencias de la red internet y de la red de control y de campo, para esto, se propone que se adquiera la suit de McAfee Enterprise Security Manager, que posee un potente firewall así como protección antivirus y excelente soporte para empresas.

Otro tipo protección que se propone es la inclusión de un firewall físico entre el HMI o estación de control y el RTU/PLC de manera que habilite únicamente al trafico especifico de medidas y variables de control entre la subestación y el centro de control y desvíe cualquier otro tráfico no autorizado, para este caso se recomienda el firewall industrial DPI referencia Eagle Tofino de la marca Hirschmann

Fig. 18 Firewall industrial Eagle Tofino

Fuente: Industrial Cibersecurity

Este dispositivo cuanta con las siguientes ventajas para su aplicación en ambientes industriales:

- Se han diseñado de forma específica pensando en los entornos ambientales y operación de las redes industriales.
- Su instalación y despliegue no es intrusiva ni invasiva.
- Su configuración y módulos de gestión de reglas son fáciles de utilizar.
- Incorporan funcionalidades específicas que permiten incrementar la seguridad de las redes OT.
- Es un firewall que se despliega físicamente entre los sistemas SCADA, HMI (nivel II de la ISA95) y los dispositivos de campo como los PLCs, DCSs, RTUs (nivel I de la ISA95).
- Bloquea malware construido sobre protocolos típicamente IT. Es decir, la mayoría del malware no está construido sobre protocolos industriales. Al poder definir reglas de segmentación específicas por protocolo industrial (Modbus, Profinet, OPC, Ethernet/IP, DNP3) este tráfico no estaría permitido.
- Segmenta tráfico que no es conforme al “estándar” del protocolo industrial seleccionado.
- Permite definir reglas de segmentación por Function Codes específicas de protocolos como Modbus, DNP3 o Ethernet IP.

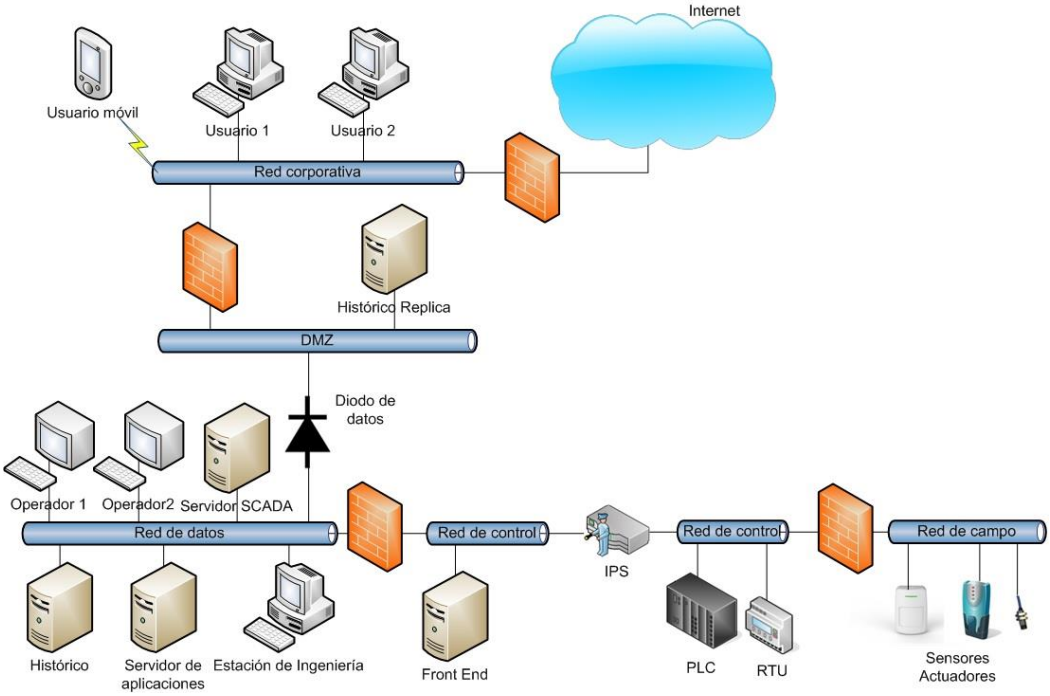
También se propone la instalación de IDS/IPS (Sistema de detección de intrusos y/o

Sistema de Prevención de intrusos)[9] el cual permite detectar patrones anormales basado en el funcionamiento de la red SCADA, se recomienda usar un IPS que se adapte a las características de la red como el sensor NGIPS (Next Generation intrusión prevention system) Cisco FirePower 8000 Series Appliance, Fig. 19 el cual es un dispositivo de hardware dedicado que permitirá la restricción de acceso a la red, como se muestra en la Fig 20.

Fig. 19 NGIPS Cisco FirePower 8000

Fuente: Cisco Products & Services

Fig. 20 Configuración de red apropiada para el sistema SCADA de la subestación



Fuente: Instituto nacional de ciberseguridad

[9] PADILLA, Jhon Jairo. Ciber Seguridad en redes industriales. [En línea] 2014. Disponible en:http://jpadilla.docentes.upbbga.edu.co/redes_industriales/Ciber%20Seguridad%20en%20Redes%20Industriales.pdf

Es necesario aplicar como políticas de seguridad informática la continua revisión parches en el sistema operativo tanto de computadores de trabajo, como de los servidores, esta revisión se puede realizar mensualmente así actualización periódica de antivirus semanalmente programada en el servidor principal que maneja el dominio de la red y que administra los diferentes terminales de la red, llevar un control de recursos usados y dispositivos conectados a la red.

Los esquemas de mantenimiento predictivo y correctivo, deben realizarse periódicamente por lo menos 1 vez cada 6 meses, para evitar cualquier daño o avería de un activo que perjudique el buen funcionamiento del sistema SCADA, que controla la subestación, así mismo, en caso de falla imprevista, se debe contar con sistemas redundantes paralelos de alta disponibilidad, para evitar perdida de información, si ocurre un fallo lógico o físico, con esto se busca disminuir el riesgo de puntos críticos únicos de fallo y asegurar los activos eficientemente. Se recomienda contar con un sistema SOC (Security Operation Center) y un correlacionador de eventos, aunque es un servicio que se puede contratar externamente, sería necesario incluirlo dentro del presupuesto de funcionamiento del departamento de seguridad informática si es posible, el cual sirve, para monitorear el acceso a activos de la red SCADA de forma centralizada y estandarizada, con los protocolos de comunicación y a su vez la relación que existe con los logs para obtener mayor eficiencia en la identificación y manejo de incidentes de seguridad.

Algunas empresas en Colombia prestan este servicio de monitoreo (SOC remoto) o se puede adquirir el paquete de software especializado (SOC en Sitio), para este servicio a nivel interno de la organización como lo es SOC Colombia. La gestión del SOC está basada en Ticket que permiten registrar las anomalías registradas, por otro lado, hay un equipo de personas que analizan de manera detallan los eventos recolectados por la plataforma.

4.4.2 Entrenamiento al personal y auditorias de seguridad

En la seguridad informática intervienen muchos actores, principalmente el talento humano, por ello la importancia de un adecuado entrenamiento del personal que maneja el SCADA, este entrenamiento debe abarcar los temas de informática y telecomunicaciones, seguridad lógica y física de los activos que intervienen en el proceso de manejo cotidiano. Se sugiere antes de comenzar las actividades, realizar reuniones, donde se culturice sobre la seguridad en el entorno de trabajo, actuación frente a posibles fallos y mecanismos de contingencia en caso de problemas, Esta acción se realizará en 2 etapas:

- *Plan se sensibilización*, ya que la mayoría de las personas del común, desconoce temas como la seguridad de la información, el 80% de los ataques informáticos provienen del interior de la misma organización (ingeniería social, empleados

descontentos, carencia de entrenamiento etc..), por esto es necesario crear una conciencia sobre el manejo de contraseñas, de dispositivos extraíbles y sobre los peligros que asechan en el internet.

Las alternativas que se tiene para esta sensibilización son:

- Carteles o posters situados en lugares estratégicos y de fácil visualización por parte de los empleados de la empresa.
- Folletos que se pueden repartir en la portería a todos los empleados en donde se muestre información relevante sobre seguridad de la información.
- Uso de la tecnología, por medio de fondos de pantalla en donde semanalmente se cambien con información o tips de seguridad informática, así mismo como correos institucionales con píldoras que ayuden a sensibilizar la importancia de la seguridad informática en la empresa EBSA.

- *Plan de Capacitación*: es importante, la realización de capacitaciones y cursos al personal sobre seguridad informática y ética profesional, ya que el personal de apoyo es el responsable de la operación y buen funcionamiento de la red SACDA, debe ser idóneo y de absoluta confianza, aplicando los protocolos de seguridad necesarios para evitar inconvenientes, para esto se propone capacitar por lo menos 1 vez al año y una duración no menos a 16 horas (2 días), a los funcionarios que tienen contacto directo con los sistemas informáticos que controlan las subestaciones así como sistemas de transmisión y telecomunicaciones entre HMI y RTU en los siguientes temas:

  - Gestión en seguridad de la información, en donde se aborden temas de SGSI y normas ISO/IEC 27001.
  - Estándares de seguridad de la información, con temáticas sobre ITIL, ISO 27000, COBIT, entro otros.
  - Plan de continuidad del negocio BDP/DRP, esta ayudara a los gerentes o encargados de la seguridad informática a organizar de una mejor forma el proceso de implementación de un plan para la protección efectiva de la información de la empresa.

Otro aspecto que no vamos a realizar en el presente proyecto, pero que se debe tener en cuenta a futro inmediato, y de gran importancia para la seguridad del sistema SCADA es la implantación de políticas y procedimientos de seguridad a partir de los controles ya establecidos, y la realización auditoria y monitorización tanto del sistema SCADA, como de los elementos de red y de telecomunicaciones, también formalizar el procedimiento para la revisión de registros de auditoria con el fin de una detección temprana de anomalías tanto de seguridad como de funcionalidad. En este punto, es necesario resaltar la importancia de tomar las medidas necesarias, para la protección de archivos tanto de uso diario como la de los registros de auditoria.

4.2.3 Procedimientos recomendados en el sistema SACADA

Se hace necesario aplicar los debidos procedimientos para la administración de roles y privilegios, que realiza de acuerdo a las funciones y responsabilidades específicas de cada empleado, esto con el fin de minimizar ataques internos y errores humanos lo cual facilita la trazabilidad de las acciones, en caso de algún incidente de seguridad que se presente en la planta.

Para el caso anterior es perentorio realizar procedimientos de control de accesos físicos del personal encargado y debe contar con los requisitos mínimos para acceder a las instalaciones como: identificación de personal mediante el registro de datos, personal encargado de autorización de acceso y periodo de validez de la autorización. Preferiblemente las redes SCADA deben permanecer aisladas al personal no autorizado, se recomiendo asegurar los accesos remotos por medio de protocolos seguros con cifrado de las comunicaciones con algoritmos robustos y aplicando claves complejas que pueda proporcionar mayor confiabilidad al sistema también se sugiere la implementación de una VPN para tunelizar el trafico relativo al acceso remoto y emplear un mecanismo de acceso y autenticación fuerte de doble factor.

También son de suma importancia los procedimientos de prueba y control de cambios, los cuales se deben hacer en entornos similares a los de operación para detectar problemas a la hora de realizar cambios en los activos informáticos y muestra el camino mediante una serie de pasos que validaran el proceso y minimizar el riesgo de incompatibilidad o des configuración del nuevo activo a la hora de incorporarlo al sistema.

En materia de software y debido a la constante evolución de los sistemas informáticos, específicamente a la aparición de nuevas amenazas relativas a infecciones con malware, se deben realizar procedimientos continuos de actualizaciones o aplicación parches de seguridad, implementación de sistemas antimalware y actualización de firmas de los antivirus, en los equipos informáticos que manejan el sistema SCADA, también es recomendable realizarlos en entornos de prueba, para detectar conflictos con el sistema y verificar la compatibilidad de firmas, antes de aplicarlos al sistema de operación.

Antes de realizar la instalación de un sistema operativo o de una aplicación o la inclusión de un equipo en el entorno productivo, se deben aplicar medidas para el aseguramiento de dicho elemento mediante su correcta configuración, para el aseguramiento del activo, esto se conoce como líneas base de seguridad y tiene como objetivo que el elemento cuente con un nivel de seguridad razonable, sin que esto perjudique o afecte la funcionalidad. Esto se puede realizar con la eliminación o desactivación de servicios innecesarios o que comprometan la seguridad, usar siempre cuentas personales de acceso, activación de mecanismos y controles de seguridad, configuración de la ejecución de actualizaciones automáticas, política de contraseñas robustas, alterar la configuración por defecto para agregar la configuración de seguridad en el equipo.

Para la implementación de las líneas base de seguridad, se puede usar como base las guías de buenas prácticas y seguridad que ofrecen organizaciones especializadas,

teniendo en cuenta las necesidades específicas de la operación de sistemas SCADA[10].

Y finalmente debido al desarrollo continuo de la tecnología es necesario implementar programas de renovación tecnológica tanto en hardware como en software que permitan mayor funcionalidad, seguridad y expansión o escalabilidad, esta renovación será producto del análisis de capacidad y rendimiento de los equipos que deben realizarse con el fin de que se cumpla con los requerimientos de producción y transmisión de energía provistos en el sistema SCADA de la subestación.

[10] CENTRO CRIPTOGRAFICO NACIONAL DE ESPAÑA. Guía de seguridad de las TIC (CCN-STIC-480A) Seguridad en el control de proceso y SCADA, Guía de buenas prácticas. Febrero de 2010. p 11 - 29

CONCLUSIONES

Se identificaron todos los elementos que intervienen en el funcionamiento de una subestación eléctrica, basada en el control SCADA, como son los HMI, RTU, protocolos de comunicación y sistemas de transmisión, PLC, transformadores y actuadores, y como estos son manejados y controlados por computadoras ,las cuales están interconectas y deben tener un mínimo nivel de seguridad para que operen de forma óptima y confiable, ya que son estas las que suministran la energía a los diferentes sectores productivos de la región.

Las matrices de riesgo, proporcionaron una visión clara sobre ciertas vulnerabilidades inherentes a los activos que intervienen en el sistema SCADA y aplicando los pilares de seguridad de la información (disponibilidad, confidencialidad, integridad y trazabilidad), se obtuvo una aproximación sobre los riesgos que pueden presentar y da una idea de cómo abordar las posibles soluciones.

Los controles, que se proponen para disminuir el riesgo informático sobre los activos, proporcionan una solución, para mejorar el proceso de producción y transmisión de energía en la subestación, asegurando los activos informáticos, las comunicaciones y la información que se trasmite, así mismo de proporcionar a los operadores del sistema de capacitación, actualización en procedimientos y herramientas que permitan mejorar la seguridad de la información, que se maneja en el sistema SCADA.

Se determinaron los respectivos controles y se generó un plan de mejora y mitigación de riesgos en el sistema SCADA, lo cual vislumbra una dirección hacia el continuo perfeccionamiento de los procesos de generación y trasmisión de energía lo que permite el aseguramiento informático de la subestación, para evitar posibles saboteos o ataques tanto externos como internos, que puedan afectar el suministro eléctrico, tan importante para la comunidad e industria del municipio de Duitama.

RECOMENDACIONES

Se recomienda a la empresa EBSA, con sede ubicada en la ciudad de Tunja Boyacá, que tenga en cuenta el presente proyecto para fortalecer la seguridad informática en sus sistemas de comunicación y control SCADA de subestaciones eléctricas, se enviara copia al Ingeniero Cesar Calderon, director del centro de datos y telecomunicaciones.

Los sistemas de comunicación y protocolos usados en las comunicaciones SCADA son muy robustos y presentan un alto grado de confiabilidad, pero es necesario la capacitación de los operadores y funcionarios que tienen contacto con esta infraestructura, con el fin evitar posibles errores humanos que ocasionen fallas o accesos no autorizados que puedan perjudicar el funcionamiento de la subestación.

Aunque los sistemas SCADA en subestaciones eléctricas, no son el blanco preferido de hackers o piratas informáticos, no se debe bajar la guardia, ya que por ser infraestructura critica, se debe tener muy bien resguardado y con las medidas de seguridad necesarias, para evitar posibles intrusiones y daños que puedan afectar a los usuarios de la red eléctrica.

Cuando se vaya a realizar alguna modernización de algún elemento del sistema SCADA como el HMI o el PLC es necesario que se tenga en cuenta la seguridad informática, ya que cada vez más los sistemas interconectados se irán migrando a lo que se llama actualmente a nivel mundial SMART GRID, que es una interconexión total de sistemas industriales y monitoreados a través internet, lo cual presentara inmensos desafíos de seguridad, con protocolos aún más sofisticados y seguros que puedan garantizar el funcionamiento de dicha infraestructura.

BIBLIOGRAFIA

Principal

CORREA, Gabriel Jaime y YUSTA, Jose Maria, Seguridad energética y protección de infraestructuras críticas. Medellín Colombia, Lámpsakos. No 10. Julio – diciembre 2012. p 92 – 108.

DIAZ, Carlos Andres y HERNANDEZ, Juan Carlos. Smart Grid: Las TICs y la modernización de las redes de energía eléctrica – Estado del arte. Cali Colombia. Revista S&T, 9(18). 2011. P 53.81

GOMEZ, Fernando y VARGAS, Hermann. Planeamiento del diseño de subestaciones eléctricas. Revista Espsilon N° 16. Enero - junio 2011 p. 79 - 112.

FLORES, Pepe. Stuxnet y el nacimiento de la ciberguerra. [En línea]. Julio de 2013 Disponible en internet: http://www.gore.com/articulos/6560/Stuxnet-y-el-nacimiento-de-la-ciberguerra.

MATT, Kodama. 3 Important Security Trends for ICS/SCADA Systems. [En línea]. 2014. [Citado 5-Nov-2016] Disponible en internet: https://www.recordedfuture.com/ics-scada-trends/

PEREZ, Lizzette. Tendencias de seguridad para sistemas ICS y Scada. [En línea].2014. [Citado 10-0ct-2016]. Disponible en internet: http://searchdatacenter.techtarget.com/es/cronica/Tendencias-de-seguridad-para-sistemas-ICS-y-Scada

PEREZ, Pablo y ALVAREZ, Eduardo. Estudio sobre la seguridad de los sistemas de monitorización y control de procesos e infraestructuras SCADA". En: Observatorio de la seguridad de la información INTECO. Edición, marzo 2012 p. 17 - 30

PUGLIESE. German. IEC 61850 El estándar de la integración eléctrica del futuro. ABB Power Technogies. Gunnar Stranne, junio de 2005 p. 11- 38

Complementarias

CENTRO CRIPTOGRAFICO NACIONAL DE ESPAÑA. Guía de seguridad de las TIC (CCN-STIC-480) seguridad en sistemas SCADA. Marzo de 2010. p 30 - 41

Cepeda, F. (2013). *Seguridad informática para la seguridad física*. Recuperado de: http://searchdatacenter.techtarget.com/es/opinion/Seguridad-informatica-para-la-seguridad-fisica

COMANDO CONJUNTO CIBERNETICO, Infraestructura critica cibernética, guía de infraestructura critica cibernética para Colombia, Comando general fuerzas militares. Bogotá, Colombia. Febrero 2016. p. 1 – 40

CONSEJO NACIONAL DE POLITICA ECONOMICA Y SOCIAL COLOMBIA. política nacional de seguridad digital. Enero de 2016. p. 41 -76

LOPEZ DE VERGARA MENDEZ, Jorge Enrique, Análisis de las normas de seguridad para los controles, las comunicaciones y otros equipos críticos de la red de energía. Proyecto fin de carrera. Madrid España Universidad autónoma de Madrid. Departamento de tecnología Electrónica y de las comunicaciones. 2014. 147p.