UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Tecnura

https://revistas.udistrital.edu.co/ojs/index.php/Tecnura/issue/view/1024

DOI: 10.14483/22487638.15388

INVESTIGACIÓN

Identificación de activos y ciberactivos críticos en sistemas de transmisión de energía eléctrica

Identification of assets and cyber critical assets in electric power transmission systems

Alvaro Espinel Ortega[1], Juan Carlos Carreno Perez[2]

Fecha de recepción: 20 de Noviembre de 2019 **Fecha de aceptación:** 6 de Mayo de 2020

Cómo citar: Espinel-Ortega., A., y Carreño-Perez., J.C. (2020). Identificación de activos y ciberactivos críticos en sistemas de transmisión de energía eléctrica. *Tecnura*, *24*(65)27-38. DOI: 10.14483/22487638.15388

Resumen

Objetivo: Presentar una propuesta para la identificación de activos y ciberactivos críticos, facilitando a los agentes del sector conocer su planta tecnológica instalada, clasificar sus activos y ciberactivos, para que posteriormente se valore el estado de vulnerabilidad cibernética y se tomen las acciones necesarias para mantener su sistema en un nivel operativamente seguro.

Metodología: Debido al avance de los sistemas de comunicaciones y tecnologías electrónicas, se ha promulgado durante los últimos 18 años la implementación de estos beneficios tecnológicos a los sistemas de potencia eléctrica abarcando toda la cadena productiva de energía eléctrica, es decir, generación, transmisión, distribución, comercialización e incluso en proyectos de generación distribuida, con el propósito de brindar confiabilidad, selectividad y controlar de manera centralizada la información y gestión de todas las variables eléctricas. En consecuencia, la investigación se construyó a partir de modelar el funcionamiento desde la perspectiva de ciberseguridad e identificando los servicios, arquitecturas y topologías de operación del sistema de transmisión de energía eléctrica.

Resultados: Anteriormente en los sistemas eléctricos, las únicas fallas que podrían producir una pérdida del suministro de energía eran las ocasionadas por descargas atmosféricas, sobrecargas de los circuitos o fallas en los activos del sistema, como conductores, transformadores, interruptores, bujes entre otros. Ahora, con la integración de redes de comunicación en los sistemas energéticos, a estos imprevistos se suman problemas de seguridad cibernética como lo son la seguridad e integridad de la información, así como el control de acceso para la manipulación de los dispositivos de maniobras del sistema eléctrico.

Con base en este nuevo aspecto que puede ocasionar fallas y daños en la infraestructura eléctrica, se necesita conocer detalladamente los activos que pueden ser afectados y que a su vez su intervención maliciosa llegue a alterar el sistema de transmisión de energía eléctrica. Por tal razón, en este documento se presenta una propuesta para la identificación de activos y ciberactivos críticos, facilitando a los

1 Ingeniero electricista, magíster en Teleinformática, doctor en Ingenieria de Software, docente de Planta Facultad de ingenieria. Universidad Distrital Francisco Jose de Caldas Bogota D.C. Contacto: aespinel@udistrital.edu.co

2 Ingeniero en Distribución y Redes Eléctricas, especialista en Teleinformática, magíster en Ingenieria, magíster en Ciencias de la Información y las Comunicaciones. Grupo de Investigación GESETIC. Bogota D.C. Contacto: jccarrenop@correo.udistrital.edu.co

agentes del sector conocer su planta tecnológica instalada, clasificar sus activos y ciber activos.

Conclusiones: En este trabajo presenta una propuesta para la identificación de activos y ciberactivos críticos, facilitando a los agentes del sector conocer su planta tecnológica instalada, clasificar sus activos y ciberactivos En este artículo se presenta una propuesta para la identificación de activos y ciberactivos críticos de la infraestructura eléctrica de transmisión de energía, con el propósito de realizar posteriormente una valoración del estado de vulnerabilidad cibernética y se tomen las acciones necesarias para mantener su sistema en un nivel operativamente seguro.

Palabras clave: ciberseguridad, energía eléctrica, infraestructura crítica, tecnologías de operación, vulnerabilidades.

Abstract

Objective: Submit a proposal for the identification of critical assets and cybernetic assets, which makes it easier for the agents of the sector to know their installed technological plant, classify their cybernetic assets and assets, so that the cyber vulnerability status is subsequently evaluated and take the necessary measures to keep your system at an operationally safe level.

Methodology: Due to the advance of communications and technology systems, the implementation of these technological benefits to electric power systems has been promulgated over the last 18 years, covering the entire production chain of electric energy, that is, generation, transmission, distribution, commercialization and even in distributed generation projects, with the purpose of providing reliability, selectivity and centrally controlling the information and management of all electrical variables. Consequently, the research was built from functional modeling from the perspective of cybersecurity and identifying the services, architectures and operational topologies of the electric power transmission system.

Results: Previously in electrical systems, the only failures that could cause a loss of energy supply were those caused by atmospheric discharges, circuit overloads or failures in system assets such as conductors, transformers, switches, bushings, among others. Now, with the integration of communication networks in the energy systems, to these unforeseen are added cyber security problems such as information security, data integrity and access control for the manipulation of the system maneuvering devices electric.

Based on this new aspect that can cause failures and damage to the electrical infrastructure, it is necessary to know in detail the assets that may be affected and that in turn their malicious intervention can affect the electric power transmission system. For this reason, this document presents a proposal for the identification of critical assets and cyber assets, which makes it easier for sector agents to know their installed technology plant, classify their cyber assets and assets,

Conclusions: In this document, a proposal for the identification of critical assets and cybernetic assets is presented, which makes it easier for the agents of the sector to know their installed technological plant, classify their cybernetic assets and assets, so that the state of cyber vulnerability is evaluated and may take the necessary measures to keep their system at an operationally safe level.

Keywords: cybersecurity, critical infrastructure, electric power, operation technologies, vulnerabilities.

INTRODUCCIÓN

Durante los últimos años, la difusión e implementación de las tecnologías de la información y las comunicaciones (TIC) han producido un fenómeno con profunda influencia política, social y económica, que aporta aspectos positivos como la globalización del conocimiento.

Al incorporar las TIC en los sistemas de control, supervisión y protección de la infraestructura

eléctrica, se crea una vulnerabilidad a nivel de seguridad informática, en la cual un agente inescrupuloso pueda generar ataques cibernéticos que ocasionen pérdidas de suministro de energía o fallas en el sistema eléctrico. Con base en este nuevo aspecto que puede ocasionar fallas y daños en la infraestructura eléctrica, y evaluando la situación actual mundial en cuanto a la seguridad y condición social, se evalúa que existe gran probabilidad de ataques cibernéticos organizados a los sistemas energéticos. En consecuencia, a nivel sistémico eléctrico es muy importante identificar los activos que se pueden ver afectados ante cualquier tipo de ataque cibernético.

En consecuencia, a nivel sistémico eléctrico es muy importante identificar los activos que se pueden ver afectados ante cualquier tipo de ataque cibernético; por esta razón, en este documento se presenta una propuesta de identificación de los activos y ciberactivos para sistemas de transmisión de energía eléctrica.

ANTECEDENTES

De acuerdo con lo propuesto en DeSmit, Elhabashy, Wells y Camelio (2017), como primer paso, las empresas deben comprender cómo sus sistemas podrían verse comprometidos por ataques ciberfísicos. Sin embargo, antes de esto se debe tener claridad de la manera en que funciona el sistema para determinar todos los posibles vectores de ataque, al que dicho sistema se puede ver expuesto.

Con el propósito de entender el funcionamiento del sistema de transmisión de energía eléctrica, en términos generales una subestación cuenta con cuatro niveles jerárquicos de operación.

- *Nivel 0*: Patio en el caso de subestaciones aisladas en aire, y GIS, en el caso de subestaciones encapsuladas aisladas en SF6.
- *Nivel 1:* Controlador de Bahía/Selectores de respaldo (mímicos de operación de emergencia para control de equipos de patio).
- *Nivel 2:* Estación de operación y gateway o controladores de subestación.
- *Nivel 3:* Centros de control.

La filosofía de operación establece que, si un nivel jerárquico está habilitado para operación, los niveles superiores a este se encontrarán bloqueados. Así, si el nivel 0 se encuentra habilitado, no se podrá operar desde los niveles 1, 2 y 3; de igual manera para los niveles superiores.

Los sistemas de automatización y protección de las subestaciones eléctricas del sistema de transmisión de energía eléctrica colombiano están conformados, en su mayoría, por un equipo de control de subestación de nivel 2; por su parte, los sistemas de control y protección de bahías de nivel 1 son realizados por dispositivos numéricos programables e integrados en el mundo de la tecnología de las comunicaciones.

La automatización y protección de las subestaciones de transmisión de energía cumple de manera integral con las siguientes tareas: adquisición y distribución de la información en tiempo real, señalización local (nivel 1 y nivel 2), señalización remota (nivel 3), supervisión, control local y remoto, control con enclavamientos, control bajo secuencias de mando, protección eléctrica de la bahía, selectividad de la operación de protecciones eléctricas de la subestación, conexión decentralizada o centralizada mediante protocolos de comunicación con dispositivos de protección eléctrica, controladores de bahía y estaciones esclavas, registro y archivo de la información del proceso.

Por la forma modular en que, en la actualidad, se diseñan las subestaciones eléctricas de transmisión, el sistema de automatización y protección es escalable y expandible en la medida que se puede implementar en un rango amplio de tipos, tamaños, con diferentes aplicaciones y requerimientos, permitiendo adaptarse a la medida de las necesidades que el sistema de transmisión lo vaya necesitando.

Por su parte, estos sistemas digitales se integran a la tecnología de las comunicaciones IT aprovechando las ventajas actuales, sus desarrollos y todas sus posibilidades futuras. Mediante las posibilidades de comunicación de los equipos de automatización y protección es posible crear los enlaces necesarios para el intercambio de información dentro del sistema y con los centros de control de nivel superior, IED (*intelligent electronic device*), controladores de bahía y otros dispositivos o sistemas. Lo anterior, teniendo en cuenta que dentro de su diseño e implementación no se comprometa la disponibilidad del sistema, el cual es un factor que puede afectar la operación del sistema eléctrico (Carreño, 2012).

La investigación realizada por Hyunguk y Taeshik (2015), menciona que de acuerdo con la revisión, no se tienen estudios sobre los tipos de nuevas vulnerabilidades de seguridad y los requisitos de seguridad que se requieren en un entorno de protocolo heterogéneo basado en IEC 61850. En este documento, se examina la red eléctrica en Corea y analiza las vulnerabilidades de seguridad, los requisitos de seguridad y arquitecturas de seguridad en dicho entorno.

Las comunicaciones en las subestaciones son basadas en IEC 61850, entre las subestaciones y el Centro de Control del sistema de control de potencia de Corea, se usan los protocolos IEC 61850, DNP3 y IEC 61970.

Cuando se conectan protocolos heterogéneos, como en este caso, un punto de conversión de protocolo es requerido y se convierte en un punto de ruptura de la seguridad de extremo a extremo, en este punto se basa la metodología propuesta por Hyunguk y Taeshik (2015). Por lo que determinan que las amenazas de seguridad que pueden ocurrir en un entorno donde se conectan protocolos heterogéneos basados en IEC 61850, se clasifican en seis tipos: vulnerabilidad de protocolo, asignación inadecuada de protocolos, mapeo de servicio de seguridad incorrecta, herramienta de configuración insegura, sistema Gateway inseguro y debilidad de diseño de red.

Las protocolos que se manejan en la infraestructura de red sobre los sistemas de transmisión energía eléctrica generalmente son basados en TCP/IP, DeviceNet, ControlNet, PROFIBUS, MODBUS, DNP3, IEC61850, IEC61870-5-104, IEC61870-5-101 Serial, IEC61870-5-103 Serial (Cherdantseva *et al.*, 2016).

En Colombia se están desarrollando constantemente proyectos de expansión de energía eléctrica, como se presenta en UPME (2018) con proyección al 2031, en los cuales se están vinculando tecnologías modernas que implementan tendencias IP y específicamente aplicaciones con IEC 61850; adicionalmente, se realizan modernizaciones de sistemas existentes contemplando el cambio de plataforma y migrando a sistemas inteligentes, automatizando procesos e integrando gestión energética. Por tanto, se requiere establecer una metodología que brinde a las empresas del sector los mecanismos necesarios para tener un sistema seguro.

Adicionalemente, en Colombia las empresas encargadas de proveer el servicio de energía eléctrica tienen la obligación de mantener altos estándares de calidad, dentro de ellas la disponibilidad y confiabilidad del sistema como se especifican en los marcos regulatorios (Mora, Carrillo y Jaimes, 2004). Con esto toma mayor relevancia la identificación de activos y ciberactivos críticos en sistemas de transmisión de energía eléctrica, con el proposito de que los diferentes agentes del sector tomen las medidas de mitigación correspondientes garantizando los estádares de calidad que ellos deben mantener.

MODELO DE FUNCIONAMIENTO

Con la intención de representar el funcionamiento y los elementos principales que componen el sistema de transmisión de energía eléctrica desde la perspectiva de ciberseguridad, en la figura 1 se muestra un modelo de funcionamiento en donde se proporciona la estructura del sistema desde la

perspectiva de ciberseguridad propuesta en esta investigación.

En este trabajo se considera *infraestructura crítica* (IC) las redes de transmisión de energía eléctrica. Como se presenta en la figura 1, estas redes a su vez se definen como sistemas complejos debido a las múltiples interacciones entre sus componentes, dadas principalmente por el diseño que está orientado a brindar un rendimiento óptimo, una operación confiable y una funcionalidad segura. El problema radica en que los métodos clásicos de análisis de vulnerabilidad y evaluación del riesgo no pueden abarcar la complejidad de la IC (estructura y dinamismo; topología y funcionalidad, estática y dinámica).

Esta complejidad dificulta el análisis de una falla o mal funcionamiento; comportamientos emergentes pueden surgir en el sistema por una respuesta colectiva de componentes fundamentales, que se traduce en la incapacidad de predecir y administrar un evento en el sistema. Como consecuencia, existe una mayor incertidumbre en la caracterización de escenarios de falla de la infraestructura crítica (Zio, 2016).

La estructura compleja hace referencia a la heterogeneidad, y esta última a las diferencias en los elementos, sus interconexiones y roles dentro de la estructura del sistema, frecuentemente con alta conectividad hacia los elementos del núcleo y baja conectividad hacia los nodos periféricos (Zio, 2016).

Figura 1. Modelo del funcionamiento desde la perspectiva de ciberseguridad

Fuente: elaboración propia.

La complejidad dinámica se manifiesta mediante eventos inesperados en el comportamiento del sistema, en respuesta a cambios locales en el entorno y a las condiciones operacionales de sus componentes. El sistema eléctrico de potencia a mostrado dentro sus antecedentes a nivel mundial comportamientos emergentes, en donde fallas locales han producido efectos envolventes inesperados transformándose en fallas en cascada sobre todo el sistema (Zio, 2016).

ARQUITECTURA DE COMUNICACIONES EN SISTEMAS DE TRANSMISIÓN

Con la intención de dar una descripción de los diferentes componentes que intervienen en el sistema de control, protección y medida en la transmisión de energía eléctrica, la arquitectura de comunicaciones de este tipo de sistemas está formada por uno o más centros de control y un número de dispositivos de campo como RTU (*remote terminal unit*), IED (*intelligent electronic device*), PLC (*programmable logic controller*), *gateway* (controladores basados en *software* y sistemas operativos), conectados por una infraestructura de comunicaciones. Estos dispositivos reciben información desde los componentes de campo y convierten esta información en datos digitales, los cuales a su vez son enviados a los centros de control, y también son capaces de recibir comandos digitales desde los centros de control y manejar grupos de alarmas y ajustes de variables de campo (Cherdantseva *et al.*, 2016).

Las RTU, PLC y *gateway* son dispositivos digitales que monitorean sensores y variables de campo, con las cuales toman decisiones basadas en programas de control realizadas por el usuario con lo que dependiendo de estas controlan válvulas, interruptores, tiristores, IGBT, entre otros. Dentro de la arquitectura de control, la mayoría de las instalaciones cuenta con una interfaz hombre-maquina (IHM) que permite almacenar, controlar y operar de manera local el sistema a partir de una interfaz gráfica y despliegues de operación.

Por otra parte, las IHM proporcionan un sistema de supervisión y control centralizado para numerosas entradas y salidas de proceso. Están diseñadas para recopilar información de campo, transferirla a un centro informático central y mostrar la información al operador gráfica o textualmente (Santander, 2017).

La comunicación se basa en el intercambio de mensajes entre los dispositivos maestros o clientes, con los dispositivos de control esclavos o servidores los cuales envían información y aceptan instrucciones de operación que transmiten hacia los elementos de campo (Cherdantseva *et al.*, 2016).

Dentro de este marco y tomando las funcionalidades definidas anteriormente, estas se soportadan físicamente en arquitecturas de comunicaciones que se resumen en a figura 2; este diagrama se desarrolló con el objeto de ilustrar las comunicaciones y enlaces de los casos más comunes que podemos encontrar en un sistema de transmisión de energía eléctrica.

Uno de los tipos más importantes de infraestructura de información crítica son los sistemas de control industrial (ICS) que supervisan y controlan procesos en infraestructuras industriales, como sistemas de generación de energía, sistemas de distribución y transmisión eléctrica, sistemas de tratamiento de agua, oleoductos y gasoductos, plantas químicas y refinerías (Alcaraz y Zeadally, 2015). Estos sistemas incorporan arquitecturas de comunicaciones como la presentada en la figura 2, para conectar centros de control a subestaciones remotas ubicadas en las infraestructuras que se controlan. Las subestaciones incorporan sistemas automatizados llamados unidades terminales remotas (RTU), *gateway* o controladores de subestación, que alojan sensores para recopilar y enviar datos de estado al centro de control, y actuadores para realizar acciones de control (Alcaraz y Zeadally, 2015).

Teniendo en cuenta la importancia del sector energético, se necesita una tecnología principal para asegurar la coordinación de todos los

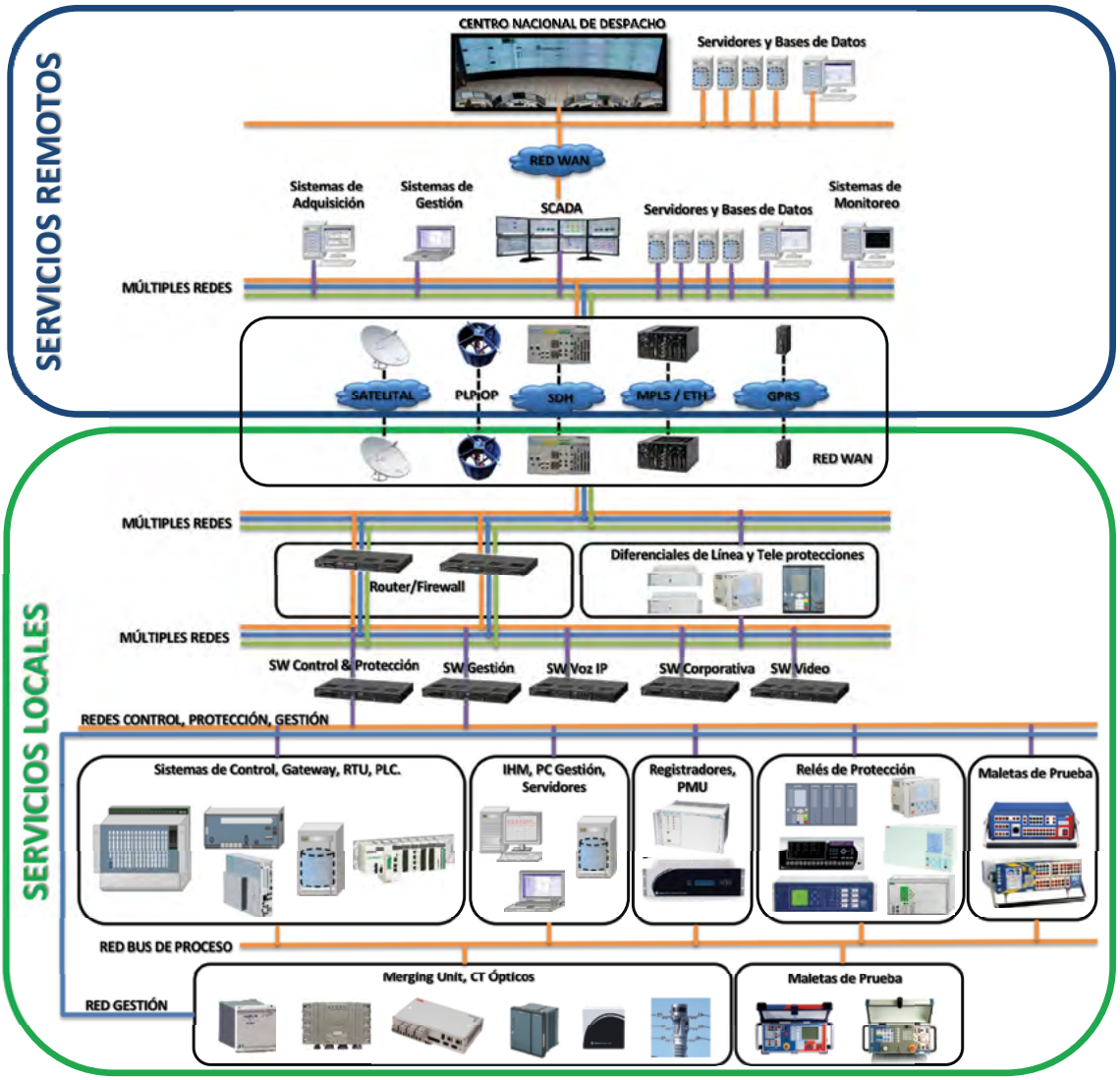

Figura 2. Esquema de arquitectura de comunicaciones en sistemas de transmisión

Fuente: elaboración propia.

componentes de la tecnología de operación (OT) desde un único centro, la cual se denomina *sistemas de supervisión y adquisición de datos* (SCADA). Los SCADA deben brindar alta disponibilidad e integridad de la información. En el caso particular del sector de energía, su importancia está dada en el garantizar el suministro de energía eléctrica a toda la población y a diferentes industrias (Santander, 2017).

ACTIVOS Y CIBERACTIVOS CRÍTICOS

En este artículo se considera infraestructura crítica (IC) las redes de transmisión de energía eléctrica. Estas a su vez se definen como *sistemas complejos* debido a la multiples interacciones entre sus componentes, dadas por el diseño que está orientado a brindar un rendimiento óptimo, una operación confiable y una funcionalidad segura.

Para la identificación de activos críticos dentro del sistema de transmision de energia electrica, se utilizó el método de identificarlos dando respuestas a las siguientes preguntas (Zio, 2016):

- ¿Cuáles son sus componentes críticos que si fallan causarían grandes consecuencias?
- ¿Cuáles son los mecanismos de propagación en toda la infraestructura crítica?
- ¿Cuáles son los eventos iniciales locales que pueden evolucionar a fallas en cascada globales?

En este orden de ideas, la definición de los componentes eléctricos del sistema de transmisión de energía se da en dos grandes grupos: subestaciones eléctricas y las líneas de transmisión que conectan las subestaciones al resto de la cadena energética.

En consecuencia, a nivel sistémico eléctrico los activos que se pueden ver afectados son subestaciones y líneas de transmisión; así, la identificación de los activos que en este trabajo se denominan activos primarios corresponde, por un lado, a la propia línea de transmisión y por otro, a los elementos que constituyen una unidad constructiva que abarca dentro de este un conjunto de elementos y equipos utilizados para dirigir el flujo de energía, lo que se denomina *grupo subestación eléctrica*.

La definición de estos activos primarios depende de la configuración de la subestación, esta hace referencia al arreglo de equipos electromecánicos consecutivos de un patio de conexión, que se traduce en la manera en que permite su operación con diferentes grados de confiabilidad, seguridad y flexibilidad.

Por consiguiente, los activos utilizados en el presente trabajo se definen en las figuras 3, 4, 5 y 6, en donde se muestra la tipificación de los activos primarios para las configuraciones de subestaciones existentes en Colombia, y que a su vez son identificados como los elementos del sistema de transmisión que pueden verse afectados ante un ataque de cualquier índole y origen.

Identificando estos activos primarios, se definen los activos secundarios que pueden afectar el activo primario, entendiéndose *afectar* como no permitir el flujo de energía a través de él, en condiciones del sistema en el que debería admitirlo. Los activos secundarios, para cada activo primario se presentan en la figura 7, los cuales fueron definidos a partir del modelo funcional y del esquema de arquitectura desarrollado al inicio de esta sección, y teniendo en cuenta que por su funcionalidad afectan directamente el activo primario de nuestro sistema de transmisión de energía.

Estos activos secundarios al ser conectados directamente a redes de comunicaciones y

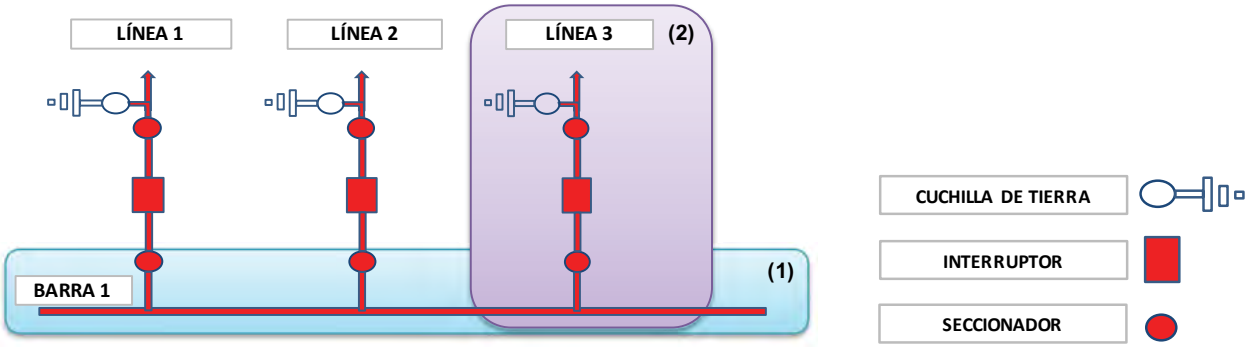

Figura 3. Activos primarios subestación barra sencilla en sistemas de transmisión

Fuente: elaboración propia.

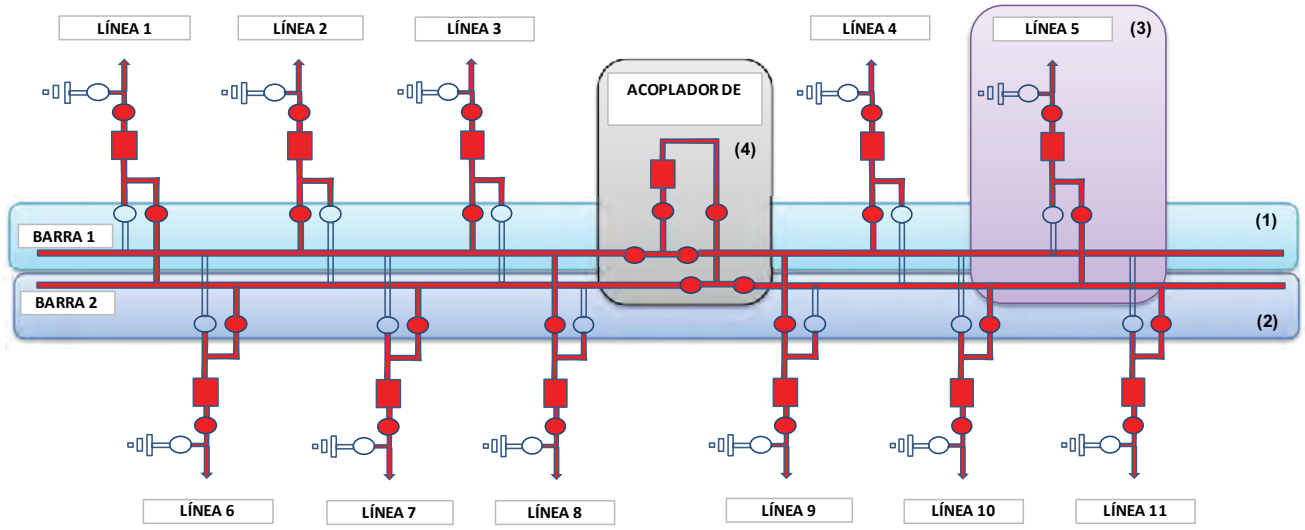

Figura 4. Activos primarios subestación doble barra en sistemas de transmisión

Fuente: elaboración propia.

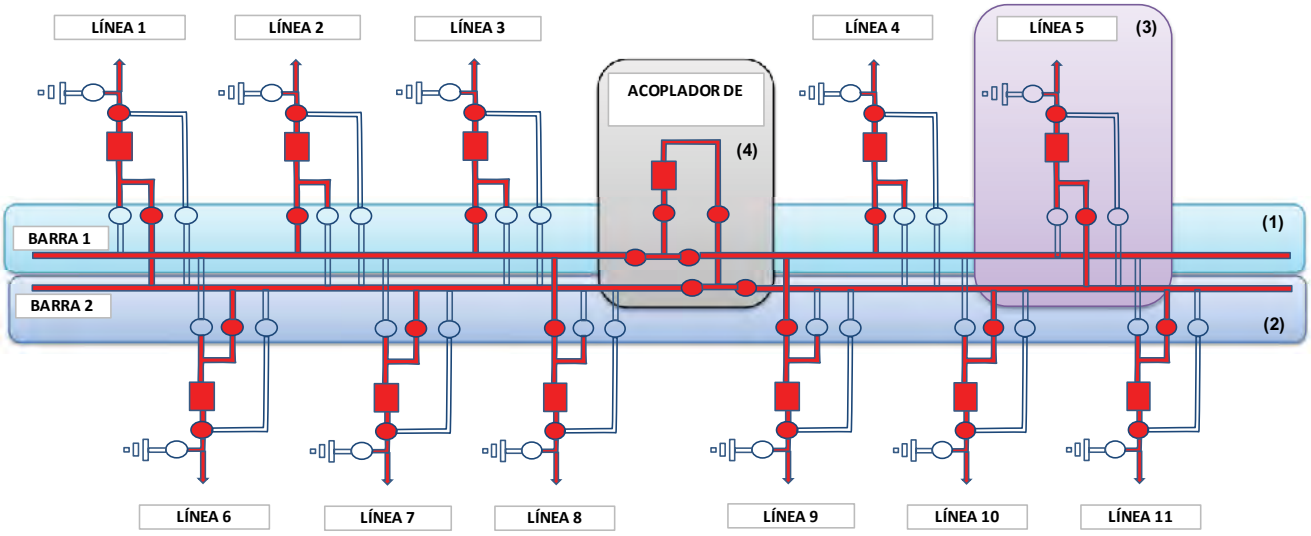

Figura 5. Activos primarios subestación doble barra + transferencia en sistemas de transmisión.

Fuente: elaboración propia.

sistemas de información, que en conjunto permiten la toma de decisión ante eventos y contingencias sobre el sistema de transmisión, pueden ser afectados por otros, a los que en este documento denominamos *activos terciarios*, dado que por medio de estos se pueden alterar, manipular y eliminar información relevante, modificando los resultados que se obtienen en lo que en el modelo de funcionamiento del sistema desarrollado se definió como las capas de sistemas e inteligencia operacional. En la figura 8 se presentan los activos terciarios y la manera indirecta en la que puede afectar el funcionamiento de un activo primario.

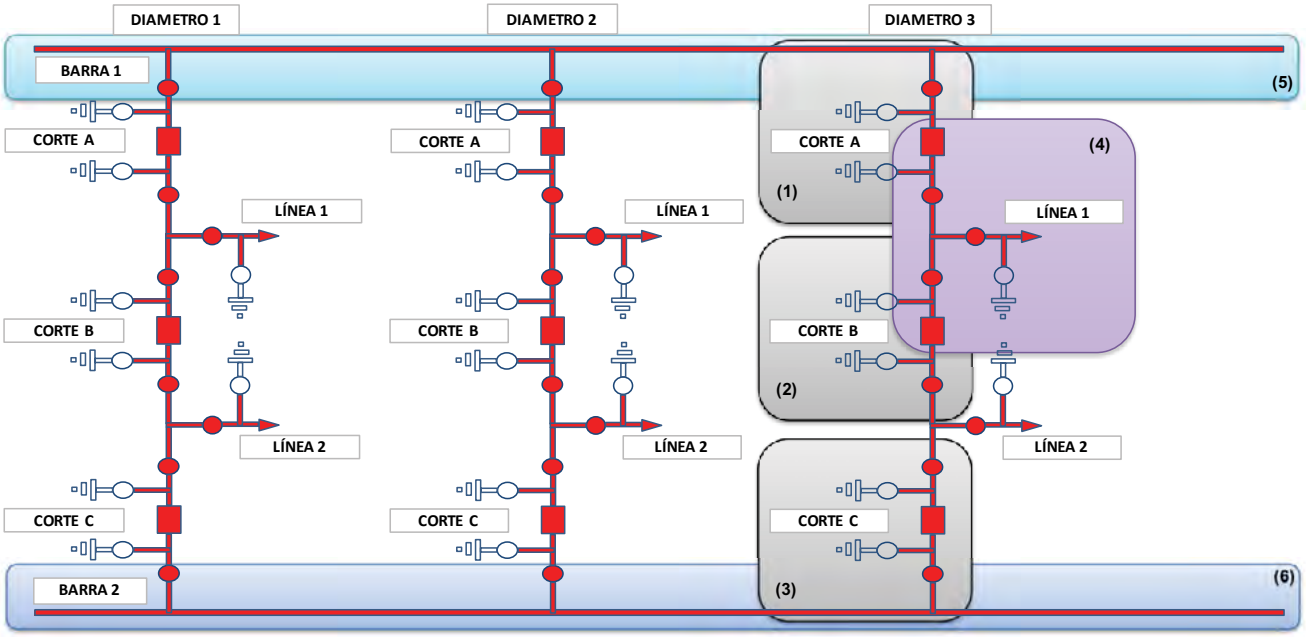

Figura 6. Activos primarios subestación interruptor y medio en sistemas de transmisión

Fuente: elaboración propia.

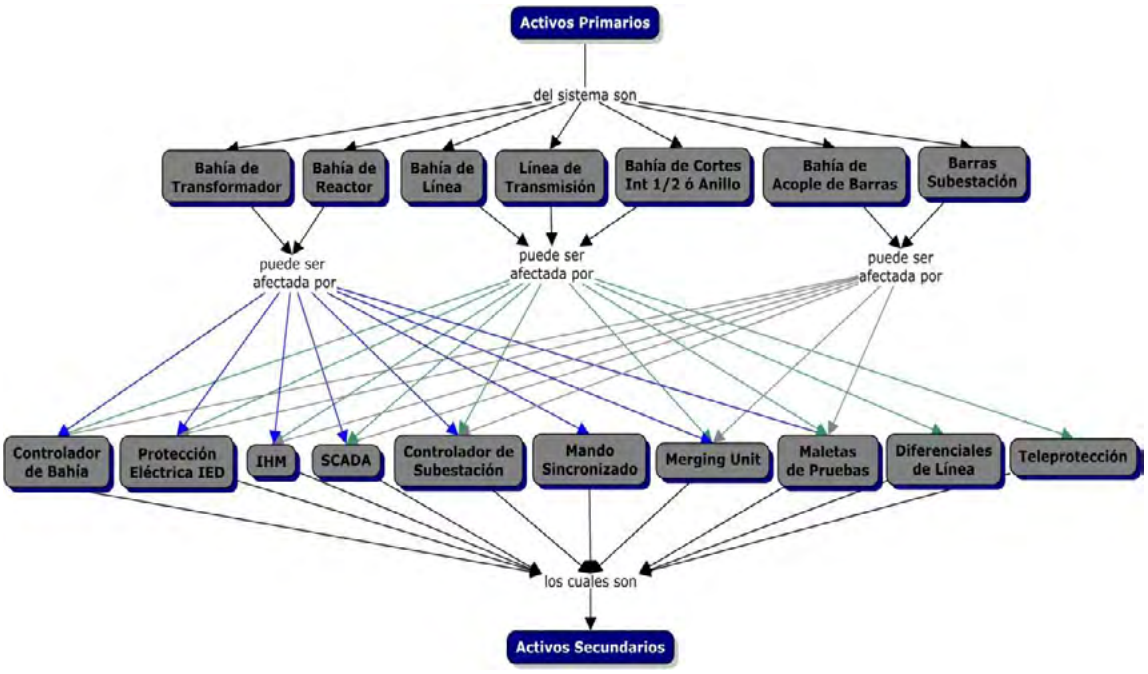

Figura 7. Activos secundarios que pueden afectar los activos primarios del sistema de transmisión

Fuente: elaboración propia.

Los sistemas de potencia funcionan frecuentemente cerca de los limites operacionales debido al incremento de la demanda de electricidad, donde pequeños disturbios en la red pueden producir disparos y efectos de mayor escala como *blackouts*. En general, estos resultan de fallas en cascada en el sistema de transmisión de energía, los disparos de fallas en cascada son múltiples y principalmente incluyen casos aleatorios y ataques maliciosos (Zhu *et al.*, 2015).

Por medio de la identificación de activos propuesta en este documento, se visualizan las fuentes de posibles vectores de ataque que en determinado momento pueden ser objetivo, para afectar el suministro de energía eléctrica y que finalmente desencadenen en *blackout* afectando diferentes sectores estratégicos y vitales para las naciones.

CONCLUSIONES

Se desarrolló un modelo de funcionamiento del sistema de transmisión de energía eléctrica desde la perspectiva de ciberseguridad presentado en la figura 1, que permite conocer el funcionamiento sistemico y evidenciar los posibles vectores de vulnerabilidad que pueden presentarse en los diferentes puntos de operación.

Se elaboró la arquitectura general de comunicación de sistemas de transmisión de energía eléctrica mostrado en la figura 2, donde se representan las comunicaciones y enlaces que se pueden encontrar en sistemas reales, facilitando la comprensión del funcionamiento del sistema y permitiendo a los diferentes agentes del sector diseñar los perímetros de seguridad lógica para mitigar posibles

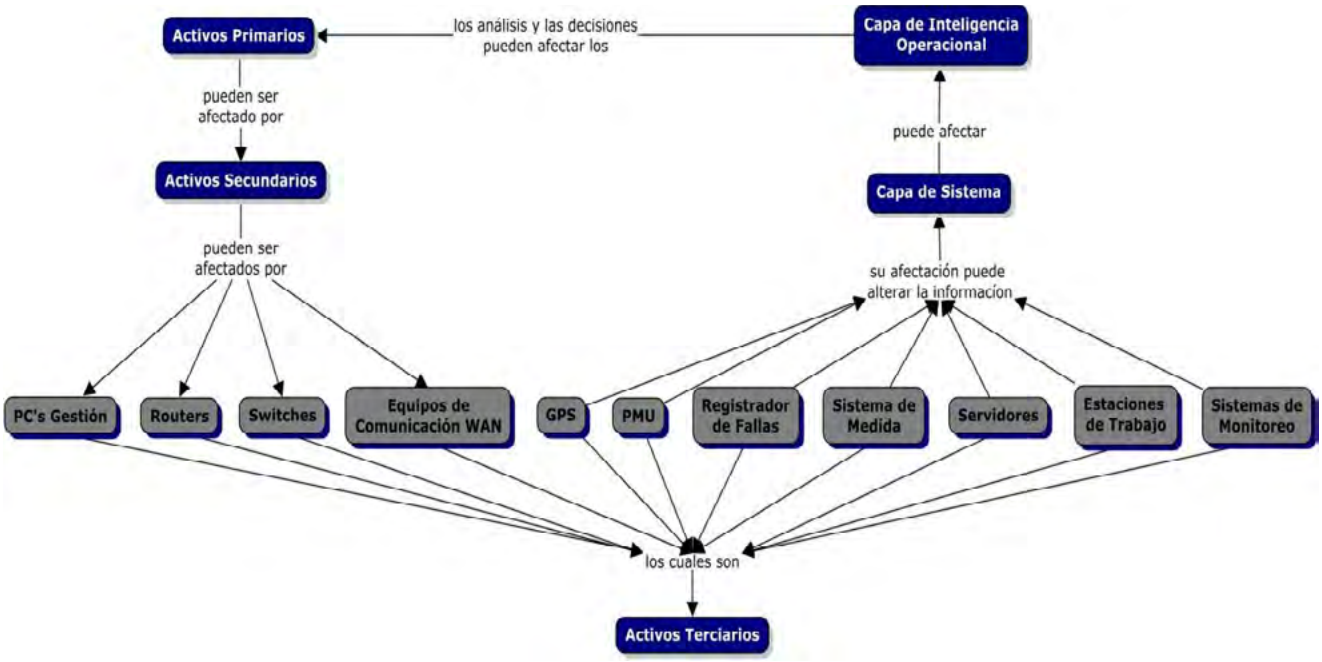

Figura 8. Activos terciarios que pueden afectar los activos primarios del sistema de transmisión de manera indirecta

Fuente: elaboración propia.

intrusiones en los diferentes ciberactivos de la infraestructura.

Se definieron tres tipos de activos para el análisis: primarios, secundarios y terciarios, con su posible afectación en el servicio de energía eléctrica. Adicionalmente, se definieron los posibles activos que se encuentran en los sistemas de transmisión, dependiendo de su topología eléctrica, funcionalidades y servicios tecnológicos presentes en la instalación.

Finalmente, este trabajo presenta una propuesta para la identificación de activos y ciberactivos críticos, facilitando a los agentes del sector clasificarlos y conocer su planta tecnológica instalada, para que posteriormente se valore el estado de vulnerabilidad cibernética y se tomen las acciones necesarias para mantener su sistema en un nivel operativamente seguro.

REFERENCIAS

Alcaraz, C. y Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, 8, 53-66. https://doi.org/10.1016/j.ijcip.2014.12.002

Carreño, J. (2012). Criterios y consideraciones metodológicas y tecnológicas a tener en cuenta en el diseño e implementación del protocolo iec 61850 en la automatización y protección de sistemas de potencia eléctrica. *Redes de Ingenieria, 3*(1), 23-40. https://revistas.udistrital.edu.co/index.php/REDES/article/view/6405 https://doi.org/10.14483/2248762X.6405

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H. y Stoddart, K. (2016). A review of cyber security risk assessment methods for 5SCADA6 systems. *Computers & Security*, 56, 1-27. https://doi.org/10.1016/j.cose.2015.09.009

DeSmit, Z., Elhabashy, A., Wells, L. y Camelio, J. (2017). An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems. *Journal of Manufacturing Systems*, 43, 339-351. https://doi.org/10.1016/j.jmsy.2017.03.004

Hyunguk, Y. y Taeshik, S. (2015). Challenges and research directions for heterogeneous cyber-physical system based on 5IEC6 61850: Vulnerabilities, security requirements, and security architecture. Future Generation Computer Systems.

Hyunguk, Y., Taeshik, S. (2015). Challenges and research directions for heterogeneous cyber-physical system based on 5IEC6 61850: Vulnerabilities, security requirements, and security architecture. *Future Generation Computer Systems*.

Mora, J., Carrillo, G. y Jaimes, J. (2004). Reducción de la indisponibilidad durante fallas en subestaciones de transmision de energía eléctrica. *Tecnura*, 15, 77-83.

Santander, M. (2017). Entendiendo los sistemas SCADA. *Boletín Ciberespacio, 1*(1), 32-39.

UPME. (2018). Plan de Expansión de Referencia Generación - Transmisión 2017-2031. https://www1.upme.gov.co/Energia_electrica/Plan_GT_2017_2031_PREL.pdf

Zhu, Y., Yan, J., Tang, Y., Sun, L. y He, H. (2015). Joint Substation-Transmission Line Vulnerability Assessment Against the Smart Grid. *IEEE Transactions on Information Forensics and Security, 10*(5), 1010-1024. https://doi.org/10.1109/TIFS.2015.2394240

Zio, E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures. ELSEVIER. https://doi.org/10.1016/j.ress.2016.02.009

Zio, E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliability Engineering & System Safety. ELSEVIER,* 152, 137-150. https://doi.org/10.1016/j.ress.2016.02.009