Diseño de un modelo de defensa en profundidad para la infraestructura de medición avanzada en Colombia

Juan Camilo Gutiérrez Gallego

Trabajo de grado para optar al título profesional:

Maestría en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2020

Ministerio de Defensa Nacional
Comando General de las Fuerzas Militares
Escuela Superior de Guerra
Maestría en Ciberseguridad y Ciberdefensa

Diseño de un modelo de defensa en profundidad para la infraestructura de medición avanzada en Colombia.

Estudiante:

Juan Camilo Gutierrez Gallego

Maestría en Ciberseguridad y Ciberdefensa
Trabajo de grado
Bogotá – Colombia
2020

Ministerio de Defensa Nacional
Comando General de las Fuerzas Militares
Escuela Superior de Guerra
Maestría en Ciberseguridad y Ciberdefensa

Diseño de un modelo de defensa en profundidad para la infraestructura de medición avanzada en Colombia.

Director

Ing. Ivan Camilo Castellanos Romero

Maestría en Ciberseguridad y Ciberdefensa
Trabajo de grado
Bogotá – Colombia
2020

Agradecimientos

A la Escuela Superior de Guerra por ser la institución que me ha acogido en los estudios de Maestría De Ciberseguridad y Ciberdefensa, al ingeniero Ivan Camilo Castellanos Romero por los consejos y el tiempo invertido a la tutela y en su acompañamiento para la materialización de este proyecto, por último, un agradecimiento especial a los docentes y a los compañeros de la cohorte IV por todo el conocimiento impartido.

A EPM por permitir y patrocinar mi formación en la Maestría en Ciberseguridad y Ciberdefensa.

Dedicatoria

A mi esposa, compañera de triunfos y luchas por su apoyo y el amor que me dedica día a día, también a mi hija por ser una motivación en ser mejor todos los días. A mi papá y a mi mamá por su apoyo incondicional, a mi hermano y su familia, a mi Tía Mary y mi Abuelita, y a todas las personas que han permitido culminar este proyecto.

Resumen Ejecutivo

El crecimiento exponencial que presentan las tecnología de la información y las comunicaciones, ha permitido la materialización de las redes inteligentes y su diversidad de aplicaciones, comunicaciones y el alto volumen de dispositivos conectados, donde la incorporación de la infraestructura de medición avanzada en el sistema de energía eléctrica implica la actualización y modificación de parte de sus infraestructuras tecnológicas, en el cual la ciberseguridad debe tratarse ampliamente ya que la información que esta representa es crítica y puede carecer de una defensa por capas como control para prevenir, contener y mitigar los riesgos de un ciberataque que impacten la confidencialidad, integridad o disponibilidad de la infraestructura de medida avanzada, la presente monografía describe el diseño de un modelo de seguridad en profundidad para la infraestructura de medición avanzada en Colombia.

Palabras clave: *Conectividad, Ciberseguridad. Infraestructura de Medida Avanzada, Seguridad en Profundidad.*

Abstract

The exponential growth of information technology and communications has allowed the realization of smart grids and their diversity of applications, communications and the high volume of connected users, where the incorporation of the infrastructure of the advanced capacity in the electric power system implies the updating and modification of part of the technological infrastructures, in which cybersecurity must be treated until the information that is represented is critical and can be counted on as a control to prevent, contain and mitigate. This article describes the design of a security model in depth for the connectivity of the energy management infrastructure in Colombia.

Key words: *Connectivity, Cybersecurity Infrastructure of Advanced Measurement, Security in Depth.*

CONTENIDO

LISTA DE GRÁFICOS

LISTA DE TABLAS

LISTA DE ABREVIATURAS

CERT:	Equipos de Respuesta a Emergencias Informáticas
CONPES:	Consejo Nacional de Política Económica y Social
CVE:	Common Vulnerabilities and Exposures
DDoS	Ataques de Denegación de Servicios
DHS:	Seguridad Nacional de EE. UU.
DMZ:	Zona desmilitarizada
IDS	Intrusion Detection System
IoT	Internet de las Cosas
IPS:	Intrusion Prevention System
ITU	International Telecomunication Unit
NIST:	National Institute of Standards and Technology
OEA	Organización de los Estados Americanos
OTAN	Organización del Tratado del Atlántico Norte
ONU	Organización de Naciones Unidas
PKI	Public Key Infraestructure
SSO	Single Sign-On
TIC	Tecnologías de la Información y la Comunicación
TO	Tecnologías de Operación
VPN:	Red Virtual Privada
WAF:	Web Application Firewall

INTRODUCCIÓN

La transformación de la red eléctrica para dar cabida a los requisitos actuales ha llevado a la incorporación de capacidades de procesamiento de la información para el control y operación del sistema eléctrico, adquiriendo capacidades de redes inteligentes que ofrecen beneficios notables a los propietarios, operadores y usuarios finales (Hébert C., 2013). Donde su funcionamiento conduce a necesitar el despliegue de infraestructura tecnológica que soporten su automatización y conectividad. El incremento constante en el suministro de energía eléctrica en Colombia es un reto para el sistema eléctrico nacional, el cual necesita la implantación de nuevos proyectos de generación, transmisión y distribución para suplir las necesidades presentes y futuras del país, donde la red eléctrica inteligente es una estrategia que está en proceso consolidación (Giral , W. M., Celedón H. J., Galvis, E.,Zona, A., 2017).

Las redes inteligentes buscan brindar información y mejorar el servicio de energía por medio de diversas tecnologías de información, telecomunicaciones y dispositivos electrónicos (Enrique, S., Gary, R., Le,T., & Xiaoming, F., 2010). La infraestructura de la medición avanzada es uno de los sistemas que se conectan a las redes inteligente, incorporando a los consumidores al sistema eléctrico, así mismo, permite a los usuarios utilizar la electricidad de forma eficiente, y proporciona a los usuarios la capacidad de gestionar la demanda casi en tiempo real (Boal, J., & Larrauri, M.; 2011), además propicia un cambio en el modelo tradicional de consumo de energía.

Aunque, se han reportado pocos ciberincidentes en los servicios de energía eléctrica, se conocen algunos como el virus de gusano de arena, tipo Stuxnet, que tomó el control del sistema de Supervisión y Adquisición de Datos (SCADA) de una planta nuclear en Irán (Moreira, N., Molina, E., Lázaro, J., Jacob, E., & Astarloa, A. 2016); así mismo, el 23 de diciembre de 2015, se organizó y ejecutó un ataque coordinado y simultaneo en tres empresas de Ucrania, una de distribución de energía, otra empresa minera y otra ferroviaria, e impactaron aproximadamente 225,000 clientes (Smith, E., Corzine, S., Racey, D., Dunne P.,

Hassett, C., & Weiss, J. ;2016), contextos como los mencionados, hacen que las organizaciones que operan y mantienen las infraestructuras críticas planeen y se preparen para futuros ataques basados en sus propias estrategias de ciberseguridad.

En febrero de 2013, el presidente de los Estados Unidos emitió la orden ejecutiva 13636, donde se busca mejorar la ciberseguridad de las infraestructuras críticas, como respuesta, el Instituto Nacional de Estándares y Tecnología (NIST) creó su framework de ciberseguridad, (Webb, J & Hume, D., 2018), el cual trabaja en políticas y procedimientos genéricos de ciberseguridad. En Colombia la CREG (Comisión de Regulación de Energía y Gas) es un organismo que se dedica a regular las actividades de prestación de servicios públicos domiciliarios, entre los cuales está la energía eléctrica (CREG, 2018), definiendo resoluciones que impactan la ciberseguridad y la infraestructura de medición avanzada para las empresas de distribución de energía eléctrica en Colombia.

Tomando como referencia el Instituto de Investigación de Energía Eléctrica (EPRI), nos indica que los mayores retos que para el desarrollo de la infraestructura de medición avanzada es lo relacionado con su ciberseguridad, debido a la probabilidad cada vez mayor de eventos cibernéticos y los incidentes críticos en contra del sector, ya que se vuelve cada vez más interconectado (Metke & Ekl, 2010, p. 99). Las empresas de distribución de energía eléctrica están en constante planeación para impactar sus redes de datos con diferentes tecnologías, donde pretenden comunicar diferentes servicios operativos y corporativos, entre esos la infraestructura de medición avanzada, según lo anteriormente expresado el presente trabajo de grado a busca desarrollar una investigación que dé respuesta a la pregunta:

¿Cuál es la estrategia de defensa en profundidad para la infraestructura de medición avanzada de la energía eléctrica en Colombia?

METODOLOGÍA

La monografía se plantea un método de solución por etapas a partir de investigación descriptiva. La primera etapa desarrolla la recopilación de referencias, examinando la literatura vigente sobre sobre la infraestructura de medición avanzada de energía eléctrica en Colombia, describiendo y documentando un marco conceptual por medio de un enfoque técnico y funcional, posteriormente, en la segunda etapa se identifica los dispositivos y protocolos claves para el diseño de una estrategia de defensa en profundidad, y a partir de esta, se identifican infraestructuras de red segura enfocada en la infraestructura de medición avanzada. La tercera etapa, formula una estrategia de defensa en profundidad para la infraestructura de medición avanzada de energía eléctrica en Colombia.

El presente trabajo de grado busca ser una fuente de consulta en la biblioteca de la Escuela Superior de Guerra, en el cual se desarrolla el diseño de un modelo de seguridad en profundidad de la infraestructura de medición avanzada en empresas de energía eléctrica colombianas, además del desarrollo de diferentes conceptos como ciberespacio, redes inteligentes, defensa en profundidad, ciberseguridad, entre otros.

Las consultas se desarrollaron principalmente en fuentes documentales, bases de datos especializadas y redes académicas.

CAPÍTULO I.
FUNDAMENTOS TEÓRICOS SOBRE LA INFRAESTRUCTURA DE MEDICIÓN AVANZADA

La infraestructura de medición avanzada es una parte del ciberespacio de la red eléctrica inteligente, donde se realiza el flujo de datos bidireccional relacionados con la medición inteligente y los comandos de control de la energía eléctrica, monitoreando y controlando en tiempo real la red eléctrica (Gómez, V. A., Hernández, C., & Rivas, E, 2018). Para las empresas de energía eléctrica, la infraestructura de medición avanzada, es un habilitador que integra hardware (medidores inteligentes , concentradores, antenas entre otros), software, arquitecturas y redes de comunicaciones, que permiten la operación de la infraestructura y la gestión de los datos del sistema de energía eléctrica y los sistemas de medida, en este capítulo, se desarrolla referencias documentales sobre la infraestructura de medición avanzada de energía eléctrica en Colombia como se muestra a continuación.

1.1 Ciberespacio

La palabra ciberespacio se ha utilizado para describir lo relacionado con computadores, servidores, redes de datos o el campo de la ciberseguridad, dicha palabra se remonta cuando el escritor William Gibson introdujo ciberespacio en uno de sus libros de ciencia ficción llamado Neuromante, (Gibson, W., 1984) y a la fecha, la palabra ciberespacio se ha extendido a círculos profesionales y académicos. (Ottis, R. & Lorents, P., 2010).

El ciberespacio es una dimensión compleja que permite y deniega el tráfico de información en las redes de datos. (Huandong, W., Yong, L., Yang, C., Yue, W.; Jian, Y. & Depeng, J., 2016). Hoy en día existen varias definiciones sobre ciberespacio, por ejemplo, el Centro de Excelencia para la Ciberdefensa de la OTAN lo define como "un conjunto de sistemas de información interconectados, dependientes del tiempo, junto con los usuarios que interactúan con estos sistemas" (Ottis R. & Lorents, P., 2010, p. 268).

Por otro lado, El Departamento de Defensa de Estados Unidos describe el ciberespacio como un dominio globalizado dentro de un contexto de información, conformado por infraestructuras de tecnologías de la información y datos en una red interconectada, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores integrados (US.DoD, 2015). Así mismo, El Departamento de Energía de los Estados Unidos hace referencia al ciberespacio como un dominio mundial dentro del entorno de la información, el cual está conformado por una infraestructura de redes de datos interdependientes de tecnologías de la información y sistemas de control industrial, Internet, las redes de datos, los sistemas informáticos, controladores y procesadores integrados (US. Department of Energy, 2012).

En el ciberespacio, un usuario tiene que cruzar múltiples redes y sistemas interconectados antes de acceder al sistema de destino (Li, F., Li Z., Han, W., Wu, T., Chen, L., Guo, Y. & Chen, J, 2018). es decir, el ciberespacio revela la característica distintiva de que las personas pueden acceder al "sistema de sistemas" a través de "redes de redes" , sin embargo la ciberseguridad ha sido un tema pasado por alto para los operadores de infraestructuras críticas durante décadas, pero ahora, con las redes inteligentes y los ataques a los sistemas de control industrial, es imperativo que los operadores eléctricos entiendan que cumplir con los estándares de cumplimiento de ciberseguridad no es suficiente (Aitel, D., 2013), debido a que el cumplimiento de estándares y metodologías es el mínimo indispensable, donde un verdadero plan de ciberseguridad necesita ir mucho más allá.

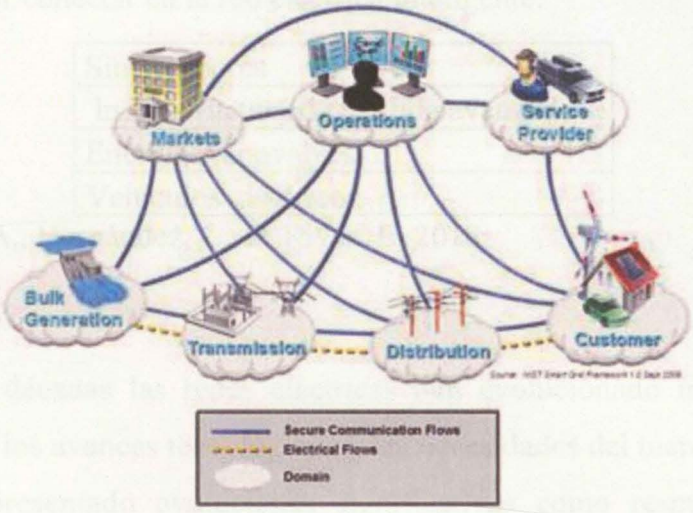
Consolidando las referencias de lo escrito anteriormente en el numeral 1.1, el autor de la monografía plantea el ciberespacio como una red de datos, constituida de infraestructura de tecnologías de la información y las comunicaciones interdependiente e interrelacionada, sistemas informáticos y sistemas que gestionan procesos de producción y control en sectores estratégicos conectados a la seguridad nacional.

1.2 Red eléctrica inteligente

La red eléctrica tradicional fue implementada con requerimientos de energía eléctrica simples, donde el gran porcentaje de los consumidores demandaban bajos niveles de potencia, así mismo la interacción entre los clientes y las empresas distribuidoras de energía eléctrica era en una sola vía (ESPE, 2017), dificultando los tiempos de respuesta a las variaciones y al incremento de la demanda energética. Actualmente el sector eléctrico en el mundo está cambiando por medio del concepto de las redes inteligentes; en Colombia las redes inteligentes se hacen realidad por medio de iniciativas sectoriales y su regulación al respecto, transformando su sistema eléctrico (Giral , W. M., Celedón H. J., Galvis, E.,Zona, A., 2017).

El concepto de red eléctrica inteligente hace referencia a la implantación de tecnologías, las cuales permitan modernizar la red eléctrica y aprovisionarla de características para la integración de diferentes técnicas de generación, almacenamiento y medición de energía eléctrica, permitiendo la participación activa del consumidor, donde se debe satisfacer las necesidades actuales del servicio de energía en cuanto a calidad, eficiencia, escalabilidad y ciberseguridad. (Enrique, S., Gary, R., Le,T., & Xiaoming, F., 2010). Esto tiene implícita la necesidad de disponer de una infraestructura tecnológica escalable, confiable y segura (Andrade, C. A. D., & Hernández, J. C., 2011), en la Ilustración 1 se muestra un modelo conceptual de la estructura del concepto de red inteligente.

Ilustración 1 : Modelo conceptual de la estructura de una red inteligente.



Fuente: (NIST, 2014)

La UIT y el NIST, indican que los requisitos de las redes inteligentes están clasificados en un modelo de tres áreas, los cuales son servicios, aplicaciones en redes inteligentes, por último están las comunicaciones y los equipos físicos (IEEE Std 802.11i, 2004), así mismo hay siete dominios que son mercado, clientes, proveedores de servicios, operaciones, generación, transmisión y distribución, donde las redes inteligentes hacen parte de muchos sistemas y subsistemas, es decir, sistemas con varios propietarios que están interconectados para proporcionar servicios de extremo a extremo entre las partes interesadas y entre dispositivos inteligentes. (International Telecommunication Union, 2011).

Las redes inteligentes se hacen realidad cuando se tiene dispone de una infraestructura tecnológica inteligente que brinde en todo momento el control y la información precisa sobre todos los puntos del sistema de los servicios que involucran la generación, transporte y suministro de energía eléctrica, identificando los sistemas se le van a conectar como se muestran en la Tabla 1.

Tabla 1. Sistemas por conectar en la red eléctrica inteligente.

Sincrofasores
Infraestructura de medida avanzada
Energías renovables
Vehículos eléctricos

Fuente: Gómez, V. A., Hernández, C., & Rivas, E, 2018

En las últimas décadas las redes eléctricas han evolucionado muy lentamente, sin embargo, a partir de los avances tecnológicos y las necesidades del mercado de los sistemas eléctricos se han presentado evoluciones significativas como respuesta a los nuevos requerimientos, cobrando importancia las infraestructuras y tecnologías que soportan la continuidad operativa de los datos que estos sistemas generan, y surgen nuevos conceptos como los contadores inteligentes, los sensores inteligentes o los dispositivos inteligentes, entre otros (Gómez, V. A., Hernández, C., & Rivas, E, 2018).

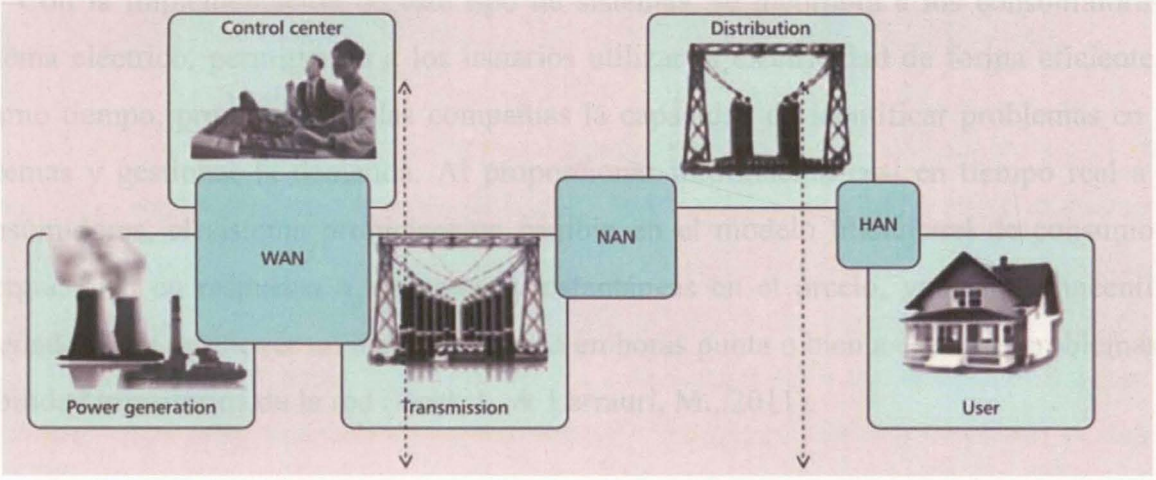
Las redes inteligentes han evolucionado de una visión a un objetivo de las naciones, el cual se está desarrollando lentamente, donde la tecnología ha servido de habilitador para el intercambio y control de la información por medio de arquitecturas integradas por el sistema de energía y las TICs, permitiendo que el sistema de energía eléctrica sea completamente flexible y controlable, además está orientada a la confiabilidad del suministro de energía eléctrica (Gómez, V. A., Hernández, C., & Rivas, E, 2018), donde la supervisión remota y la gestión automática de las redes inteligentes contribuye a la eficiencia principal.

Agrupando las referencias del presente numeral y según el autor de la monografía, la red eléctrica inteligente se considera como el conjunto que contiene a la infraestructura de medición avanzada entre sus diferentes sistemas y subsistemas, los cuales se encuentra interconectados con el objetivo de suministrar y monitorear el consumo de energía eléctrica, de una manera confiable, rentable, interoperable, seguro, con bajos costos de instalación y mantenimiento.

1.3 Infraestructura de telecomunicaciones en las redes inteligentes

La formación de redes eléctricas inteligentes se logra a través de la integración de diferentes tecnologías de telecomunicaciones a la infraestructura del sistema eléctrico. Las redes de telecomunicación, son un sistema de sistemas que combina una gran variedad de tecnologías, en dichos subsistemas se requieren interfaces físicas y lógicas bien definidas y armonizadas con los estándares existentes (Andrade, C. A. D., & Hernández, J. C., 2011), en la Ilustración 2 se muestra una visión general de la infraestructura de telecomunicación de un modelo jerárquico en las redes eléctricas inteligentes, describiendo los miembros y las tecnologías de cada zona:

Ilustración 2 : Infraestructura de telecomunicación para la red eléctrica inteligente.



Fuente: Yu, R., Zhang,Y., Gjessing, S., Yuen, Xie,C. S. & Guizani, M., (2011).

Las redes eléctricas inteligente segmentan sus usuarios en cinco partes (Generación, Trasmisión, Distribución, Centro de Control y Usuarios Finales), donde cada uno posee su infraestructura y protocolos, los dominios de comunicaciones son tres y se muestran la Tabla 2.

Tabla 2. Dominios de comunicaciones para las redes inteligentes.

Red para el hogar (Home Area Network HAN).
Red de área de vecindario - campo (Neighbourhood NAN).
Red de área amplia (Wide Area Nework WAN).

Fuente: Yu, R., Zhang,Y., Gjessing, S., Yuen, Xie,C. S. & Guizani, M., (2011).

La infraestructura de telecomunicaciones en las redes eléctricas inteligentes se debe diseñar bajo una arquitectura distribuida y escalable, al mismo tiempo debe ser una infraestructura que brinde ciberseguridad a la información que se transmite por medio de los canales de comunicaciones.

1.4 Infraestructura de medida avanzada.

Con la implementación de este tipo de sistemas, se incorpora a los consumidores al sistema eléctrico, permitiendo a los usuarios utilizar la electricidad de forma eficiente, al mismo tiempo, proporciona a las compañías la capacidad de identificar problemas en sus sistemas y gestionar la demanda. Al proporcionar información casi en tiempo real a los consumidores, el sistema propiciara un cambio en el modelo tradicional de consumo de energía, bien en respuesta a variaciones instantáneas en el precio, ya sea por incentivos diseñados para promover un menor consumo en horas punta o bien a causa de problemas de fiabilidad transitorios de la red (Boal, J., & Larrauri, M., 2011).

En Colombia, la demanda de energía eléctrica responde a variables como el crecimiento de la economía y su población; con respecto a la regulación, el Ministerio de Minas y Energía es la institución encargada de establecer los mecanismos para su implementación, operación y mantenimiento del servicio de energía eléctrica en el país (Giral , W. M., Celedón H. J., Galvis, E.,Zona, A., 2017).

1.4.1 Legislación en Colombia

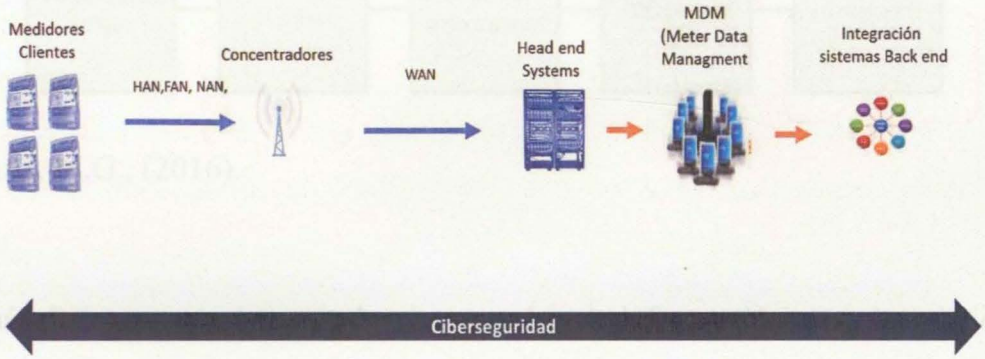
Actualmente en Colombia existe un marco legal que enmarca las infraestructuras de medición avanzada por medio de la resolución 40072 del 29 de enero de 2018 del Ministerio de Minas y Energía, así mismo estipula que los operadores de red serán los responsables de la instalación, administración, operación, mantenimiento y reposición de la infraestructura de medición inteligente, además, estipula que los operadores de red deben tener unos planes de implementación, considerando que por lo menos el 95% de los usuarios urbanos y 50% de los usuarios rurales deberán ser atendidos a más tardar en el año 2030 con funcionalidades para el almacenamiento, comunicación bidireccional, ciberseguridad, sincronización, actualización y configuración, acceso al usuario, lectura, medición horaria, prepago, calidad del servicio, registro de medición bidireccional, conexión, desconexión y limitación del suministro de energía eléctrica (Ministerio de Minas y Energía, 2018)., definiendo un contexto para el desarrollo de la infraestructura de medición avanzada, además de proyectar una hoja de ruta como país en su implementación.

De igual manera hay otras resoluciones que están relacionadas con la infraestructura de la medición avanzada como son la CREG 038 del 2014, la cual habla sobre el código de medida, o la resolución CREG 015 de 2018, en donde se incorpora el Artículo 25, precisando los compromisos de ajustes regulatorios relacionados con la infraestructura de medición avanzada, también se puede hacer referencia a la CREG 030, en la cual se regulan las actividades de autogeneración a pequeña escala y de generación distribuida en el sistema Interconectado Nacional, además de la circular 054 de 2018 orientada a la reglamentación de la infraestructura de medición avanzada, y por último el proyecto de resolución de la Superintendencia de Industria y Comercio para reglamento de medidores de energía, agua y gas (CREG, 2018).

1.4.2 Arquitectura

La arquitectura de la infraestructura de medición avanzada consta de equipos de medición inteligente, telecomunicaciones y centro de gestión de la medida, integrado a las aplicaciones de la operación y sistemas comerciales, en la Ilustración 3 se muestra una arquitectura funcional.

Ilustración 3 : Topología de la infraestructura de medición avanzada.



Fuente: Propia

La infraestructura de medida en el sistema de energía eléctrico se está transformando en un concepto que con el pasar de los días toma más vigencia, debido a que optimiza los consumos de energía por medio de una nueva base tecnológica interoperable, a continuación, se describen cada uno de los componentes funcionales de la infraestructura de medición avanzada:

1.2.1 Medidores Inteligentes.

Los medidores inteligentes están sustituyendo los medidores mecánicos y electrónicos porque posee características y funcionalidades adicionales, ya que es un dispositivo que mide y registra el suministro de energía eléctrica, tanto de la corriente como la del voltaje, el cual

tiene funciones como el almacenamiento de información de consumo de energía eléctrica, transmisión y recepción de información con la empresa proveedora de energía eléctrica por medio de una red de datos (Chris K., 2004), entre otras, en la Ilustración 4 se muestra un diagrama de bloques funcionales de un medidor inteligente, permitiendo la transferencia de información bidireccional sobre el consumo.

Ilustración 4 : Diagrama de bloques de un medidor inteligente

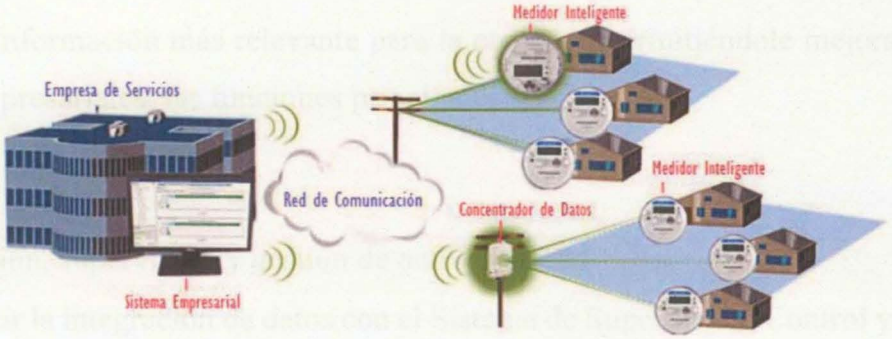
Fuente: Ruiz, M.G., (2016).

Además de las características sobre intercambio de información, permite adicionar otras funcionalidades en el medidor como una escala de tarifas, conexión y desconexión de cargas, facturación prepaga, facturación remota, desconexión y reconexión remota, detección de perdidas, notificación de corte de energía, entre otras.

1.4.3 Colectores de datos.

Estos dispositivos son conocidos como concentradores o gateways, los cuales extraen la información de los medidores inteligentes cercanos; deben estar diseñados para trabajar en ambientes de alta interferencia electromagnética y deben soportar la intemperie ya que se encuentran ubicados en lugares ambientalmente hostiles como se muestra en la Ilustración 5.

Ilustración 5 : Ubicación del concentrador de un medidor inteligente



Fuente: Gutierrez, M., (2011).

La recolección de datos en los colectores se da de forma controlada por medio de la programación de los dispositivos donde se define la recolección de datos cada un conjunto de minutos.

1.4.4 Sistema Head End.

El sistema Head End está compuesto por hardware y software, el cual hace referencia al concentrador o recolector principal de información de la medición, soportando altas tasas de concurrencia de datos, es un sistema con grandes capacidades de almacenamiento de información por lo que debe estar ubicado en un datacenter (Ruiz, M.G., 2016), además ponen los datos a disposición de otros sistemas al interior de las empresas de energía eléctrica para generar información técnica y comercial.

1.4.5 Meter Data Management (MDM)

Un MDM es una base de datos de medidores con herramientas analíticas para la gestión de energía, el cual se encarga de la administración y el almacenamiento de datos a largo plazo

para todos los datos de utilización de energía eléctrica y eventos que generan los servidores Head End, además se interactúa con aplicaciones del negocio (Galarza, D. I., 2017) para identificar la información más relevante para la empresa, permitiéndole mejorar la toma de decisiones empresariales, las funciones principales son:

- Medición, supervisión y gestión de activos de red.
- Permitir la integración de datos con el Sistema de Supervisión, Control y Adquisición de la Energía (SCADA), entre otros sistemas, lo que facilita las funciones de mantenimiento, operación y comerciales.
- Proporciona información para el pronóstico de carga y demanda, informes de gestión y métricas de servicio al cliente.

El sistema MDM importa y comprueba los datos del Sistema Head End, para hacerlos aptos en el análisis y la generación de información.

1.4.6 Red de telecomunicaciones

La red de telecomunicaciones de la infraestructura de medición avanzada se basará en la capacidad de colocar medidores en cualquier lugar que se necesiten, ya que los medidores podrían estar dispersos en las ciudades o en los campos; para satisfacer con las necesidades de la conectividad, diferentes tecnologías de corto, mediano y largo alcance se encuentran en el mercado de forma madura, además hay otras que se siguen desarrollando en términos de largo alcance y bajo consumo de energía que se describen a continuación:

1.4.6.1 Power Line Communications (PLC).

Es un sistema que permite la conectividad por medio de la infraestructura de la red eléctrica para transmitir datos a corta distancia, la cual incluye unidades concentradoras que se encuentran y unidades terminales de red ubicadas en el domicilio del usuario final, también

podría implementar en su arquitectura de red unidades repetidoras que incrementan la calidad de la conexión, más en redes eléctricas como las colombianas donde se presentan altos niveles de ruido.

Las soluciones iniciales basadas en PLC utilizaron la banda ultra estrecha que utilizó frecuencias inferiores a 3kHz, proporcionando velocidades de datos menores a 60bps. Con las necesidades de mayores anchos de banda impulsó el desarrollo de sistemas PLC de banda estrecha (NB PLC) en la banda de 3kHZ a 500kHz. Actualmente, los sistemas PLC de banda ancha operan en la banda de 1,8MHz a 250MHz y pueden alcanzar tazas de datos muy altas (Galarza, D. I., 2017).

1.4.6.2 LoRa.

LoRa es una solución diseñada para sistemas que requieren la capacidad de enviar y recibir cantidades bajas de datos en un rango de muchos kilómetros sin costos de energía elevados. Utiliza las bandas ISM de 868MHz y 900MHz, además puede transmitir a lo largo de varios kilómetros dependiendo del entorno. LoRa es una solución de espectro expandido que utiliza un ancho de banda amplio para ayudar a proteger contra interferencias deliberadas o ruido ambiental, proporcionando velocidades de datos de entre 0,3 kbps a 50 kbps, lo que varía según el rango requerido y la interferencia (Miller, R., 2016).

LoRa está diseñada para una topología de estrella de estrellas en la que una puerta de enlace actúa como un puente transparente que retransmite los mensajes entre los dispositivos finales y un servidor de servicios de fondo (Lee, G. M., Crespi, N., Choi J. K., & Boussard, M., 2013).

1.4.6.3 Sigfox.

SigFox es un sistema que permite que los dispositivos remotos se conecten utilizando la tecnología de banda ultra estrecha. Está dirigido a aplicaciones de machine to machine de bajo costo donde se requiere una cobertura de área amplia.

La topología general de la red SigFox se ha diseñado para proporcionar una red escalable de alta capacidad, con un consumo de energía muy bajo, al tiempo que mantiene una infraestructura basada en estrellas simple y fácil de implementar. SigFox permite hasta 140 mensajes por dispositivo por día, con una carga útil de mensajes de 12 bytes y un rendimiento inalámbrico de hasta 100 bits por segundo y potencia ultra baja. La red SigFox está basada en radio enlaces, los cuales usan frecuencias sin licencia, donde los datos no se entregan directamente al usuario desde el sistema de radio. Cuando se reciben datos de la red de radio, se envía un mensaje al servidor del usuario o un agregador que, a su vez, lo enviará al usuario (Lee, G. M., Crespi, N., Choi J. K., & Boussard, M., 2013).

1.4.6.4 Norrowband -IoT (NB-IoT).

El protocolo Narrowband-IoT, como su nombre lo indica, utiliza un ancho de banda de transmisión más pequeño en comparación con el LTE convencional: 200 KHz frente a 20 MHz. Una reducción en la potencia de transmisión mejora aún más la vida útil de la batería y admite una velocidad de datos de 200 kbit / s tanto para el enlace ascendente como para el enlace descendente, sintonizado para poder cubrir la mayoría de las necesidades de aplicaciones de IoT (Gresset, E., 2016).

NB-IoT es una red eficiente en el uso de la energía y tiene una profunda penetración en las ciudades, además posee una amplia cobertura y puede administrar grandes volúmenes de paquetes de datos pequeños. NB-IoT utiliza las características de seguridad y privacidad que

ya existen en las redes móviles, como el soporte para la confidencialidad de la identidad del usuario, la autenticación de la entidad, la confidencialidad, la integridad de los datos y la identificación del dispositivo (Lee, G. M., Crespi, N., Choi J. K., & Boussard, M., 2013).

1.4.6.5 LTE-M.

La primera opción para un protocolo celular IoT basado en LTE es Cat-M, este está diseñado para aplicaciones que exigen un índice de datos alto en comparación con otros protocolos de IoT, ya que Cat-M soporta datos de 1Mbit / s tanto para los datos ascendentes como para los descendentes mediante la comunicación halfdúplex. Aunque se basa en LTE, el protocolo Cat-M emplea un esquema de transmisión simple que reduce la complejidad del módem en comparación con la implementación de redes LTE para telefonía celular (Gresset, E., 2016).

Para soportar la operación de baja potencia, Cat-M reduce la frecuencia de los ciclos de actualización utilizados para mantener el contacto con una estación base. Es posible lograr diez años de funcionamiento con dos baterías del tamaño AA si la frecuencia del ciclo se reduce a una vez cada diez minutos. Para muchas aplicaciones de IoT que son relativamente insensibles al retardo, como la medición, esta compensación proporciona un buen equilibrio entre el rendimiento y el consumo de energía. (Gresset, E., 2016).

1.4.6.6 ZigBee.

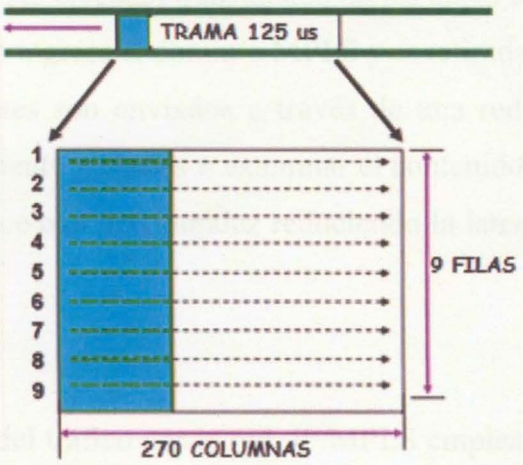
Es un sistema de comunicación inalámbrica de bajo consumo de energía, corto alcance y baja velocidad de datos, la cual fue desarrollado por ZigBee Alliance para la automatización y domótica. Opera en las bandas de radio no licenciadas ISM, 868 MHz en Europa, 915 en Estados Unidos y 2,4 GHz ofreciendo 16 canales cada uno con un ancho de banda de 5 MHz,

además funciona bajo seguridad de encriptación de datos AES de 128 bits, (Ruiz, M.G., 2016). permitiendo la autenticación de las comunicaciones.

1.4.6.7 Jerarquía Digital Sincrónica (SDH).

SDH (Synchronous Digital Hierarchy) son las siglas en inglés de las redes de Jerarquía Digital Sincrónica, también es un sistema de transporte digital diseñado para proveer una infraestructura de redes de telecomunicaciones que usa multiplexación en el dominio del tiempo, el cual es estandarizado por la ITU, el cual se especificó originalmente para el transporte de múltiples conexiones PDH (Plesiochronous Digital Hierarchy), también tiene la habilidad de soportar mecanismos de conmutación ante fallos de manera ágil, combinado con sus características de monitoreo de desempeño han logrado proporcionar un sistema de transporte resistente y confiable (Brito, J., 2015), en la Ilustración 6 se muestra la trama de una señal STM-N.

Ilustración 6 : Trama de una señal STM-N



Fuente: Brito, J., (2015).

SDH basa el transporte de servicios sus servicios en circuitos tal como la voz en plantas telefónicas tradicionales; así mismo tienen anchos de banda fijos y con granularidad alta. El crecimiento de los servicios y aplicaciones soportadas por protocolos con tecnología de paquetes, especialmente los servicios con contenido de video y en contraste el decremento de los servicios de telefonía fija, pusieron de manifiesto la necesidad por parte de las redes de transporte de tener la habilidad de transferir paquetes de manera nativa. Con Ethernet como el estándar de facto para las redes de datos empresariales, el estándar SDH tuvo que evolucionar a NG-SDH (Next-Generation SDH), tecnología que transforma las redes SDH orientadas a la voz en un mecanismo de transporte universal donde se optimiza tanto los servicios de voz como de datos.

1.4.6.8 IP/MPLS

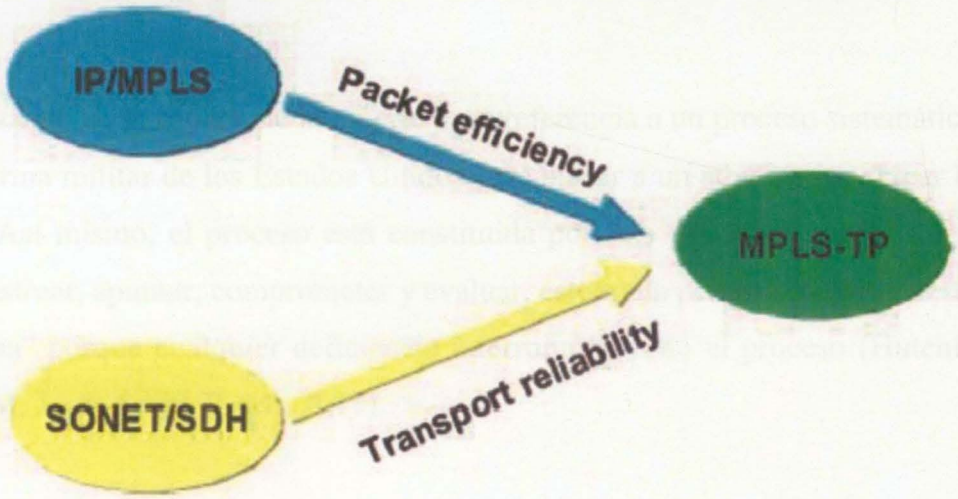
IP/MPLS (Internet Protocol/Multiprotocol Label Switching) es un sistema de transición de datos estandarizada por el IETF (Internet Engineering Task Force), el cual es un protocolo diseñado para dar solución a la gran demanda de recursos y calidad de servicio que tienen las nuevas aplicaciones, basando su conectividad empleando el concepto de conmutación de etiqueta, donde los enrutadores ejecutan transmisión de los datos basado en una etiqueta que se adjunta al paquete cuando ingresa al dominio MPLS y es retirada cuando sale del dominio. De esta manera, los paquetes son enviados a través de una red MPLS sin necesidad de consultar tablas de enrutamiento globales o examinar el contenido del paquete, permitiendo que la conectividad se realice con más rapidez reduciendo la latencia total de cada servicio (Brito, J., 2015).

Para controlar el flujo del tráfico por la red, IP/MPLS emplea un plano de control en el que todos los dispositivos necesitan conocer la topología del dominio, razón por la cual aún depende de IP, por lo anterior se conoce como IP/MPLS. De esta manera, a través de protocolos de enrutamiento, se determinan las rutas a los diferentes destinos.

1.4.6.9 MPLS-TP

MPLS-TP (Multiprotocol Label Switching – Transport Profile) es una tecnología optimizada para el transporte de paquetes, la cual proporciona servicios de transporte orientado a la conexión para las tecnologías y servicios de conmutación de paquetes (IP) y de conmutación de circuitos (TDM) como se muestra en la Ilustración 7, el cual se derivada de IP/MPLS y está siendo desarrollada en conjunto por IETF e ITU-T, con la cual se adicionan y retiran funcionalidades para simplificar el IP/MPLS en las redes de transporte (García, L. E., Pedraza, L. F., & Parra, O. S., 2013). , sin embargo MPLS-TP aún se encuentra en proceso de estandarización por parte de IETF e ITU-T, lo cual implica que la interoperabilidad entre las soluciones existentes en el mercado aún no está garantizada.

Ilustración 7 : Arquitectura general de MPLS-TP.



Fuente: García, L. E., Pedraza, L. F., & Parra, O. S., (2013).

La idea tras MPLS-TP es la de mantener la funcionalidad básica de IP/MPLS como una tecnología de networking para el transporte de paquetes orientada a la conexión, eliminando el plano de control dinámico y adicionando funcionalidades de AOM típicas de las redes de transporte tradicionales (García, L. E., Pedraza, L. F., & Parra, O. S., 2013).

CAPÍTULO II.
CONCEPTOS, DISPOSITIVOS Y PROTOCOLOS PARA EL DISEÑO DE UNA ESTRATEGIA DE CIBERSEGURIDAD.

Los eventos de ciberseguridad que impactan las empresas públicas y privadas, representan millones de dólares en pérdidas a nivel mundial cada año, además del impacto en su reputación, razón por la cual, se deben desarrollar estrategias preventivas y correctivas que eviten o mitiguen posibles ataques y fallos de seguridad (Muñoz & Rivas,2015), el capítulo II inicia describiendo la cadena de la muerte cibernética y que etapas la componen, posteriormente se desarrolla el concepto de ciberseguridad y se termina el capítulo documentando diferentes conceptos, dispositivos y protocolos que permiten diseñar una estrategia de ciberseguridad.

2.1 Cadena de la muerte cibernética

El concepto de la cadena de la muerte hace referencia a un proceso sistemático definido por la doctrina militar de los Estados Unidos para atacar a un adversario y crear los efectos deseados. Así mismo, el proceso está constituida por seis pasos los cuales son encontrar, arreglar, rastrear, apuntar, comprometer y evaluar, este es un proceso integral, descrito como una "cadena" porque cualquier deficiencia interrumpirá todo el proceso (Hutchins, E. M., Cloppert, M. J., & Amin, R. M., 2011).

En 2011, los analistas de Lockheed Martin Eric M. Hutchins, Michael J. Cloppert y Rohan M. Amin crearon el marco de referencia conocido como cadena de la muerte cibernética, con el objetivo de apoyar el proceso de toma de decisiones para detectar y responder mejor a las intrusiones no deseadas en el ciberespacio de los individuos, empresas o gobiernos, este modelo no es directamente aplicable a la naturaleza de los ciberataques, (Assante, M. J. & Lee, R. L., 2015) pero sirve como una gran base y concepto sobre el cual construir una hoja de ruta para crear una estrategia de ciberseguridad.

La cadena de la muerte cibernética define el flujo de un ciber-ataque en un modelo de siete capas, donde cada capa es crítica, a continuación, se describe en términos generales cada etapa de la cadena de la muerte cibernética.

2.1.1 Reconocimiento

Es donde se recopila información sobre el objetivo potencial a través de la observación u otros métodos de detección, enfocándose en la identificación, selección y perfilado de objetivos en el ciberespacio, proporcionando el conocimiento para los posibles objetivos.

El objetivo de la fase de reconocimiento es revelar debilidades e identificar información que apoye a los atacantes en sus esfuerzos para atacar, entregar y explotar elementos de un sistema, los tipos de información que pueden ser útiles para un atacante pueden incluir información sobre humanos, redes, hosts, cuentas y protocolos, así como información sobre políticas, procesos y procedimientos (Assante, M. J. & Lee, R. L., 2015). El reconocimiento enfocado en la infraestructura de medición avanzada puede incluir actividades tales como investigar las vulnerabilidades y sus características técnicas u obtener una comprensión de cómo el proceso y el modelo operativo pueden ser susceptibles de explotación Rawat, D.B., Bajracharya, C. (2015).

3.1.1 Militarizar

Hoy en día, la interacción a través de los datos digitalizados está evolucionando y se consumen más datos que nunca a través de los objetos distribuidos en las redes eléctricas inteligentes, militarizar incluye la modificación de por lo menos un archivo, con el fin de permitir el siguiente paso del adversario, diseñando una puerta trasera y un plan de penetración, utilizando la información obtenida del reconocimiento, para permitir la entrega

exitosa de la puerta trasera, técnicamente tiene como alcance unir las aplicaciones con una herramienta de acceso remoto (Assante, M. J. & Lee, R. L., 2015), implicando la adquisición de un botnet para preparar un malware y/o APT.

2.1.2 Entrega

La entrega es una parte crítica, ya que esta etapa el adversario usa un método para interactuar con la red del defensor (Assante, M. J. & Lee, R. L., 2015), es decir, en esta etapa del proceso el ataque cibernético debe ser eficiente y efectivo, así mismo es una tarea de alto riesgo para el atacante porque la entrega deja rastros.

2.1.3 Explotación

Después de entregar, el objetivo del ataque se complementa activando un fragmento de software, dato, secuencia de comandos o acciones, los cuales se implantan aprovechando las brechas de ciberseguridad o utilizando la vulnerabilidad de los softwares o los errores del software que resulta una amenaza potencial para el sistema (Assante, M. J. & Lee, R. L., 2015).

2.1.4 Instalación

Esta parte del proceso hace referencia al despliegue de por lo menos de un vector de infección por medio de un ejecutable de malware en una ubicación inusual, en donde se modifique las configuraciones existentes de registro o inicio del software, permitiendo que el ejecutable del malware se implante en los dispositivos, (Assante, M. J. & Lee, R. L., 2015), alterando el funcionamiento tradicional de los mismo, por el contrario, los defensores deben enfocar sus esfuerzos en encontrar y comprender la amenaza, debido a que no siempre deben suponer que la amenaza está basada en malware.

2.1.5 Comando y Control

Con una intrusión cibernética exitosa, el adversario pasa a la siguiente fase, aquí el actor establecerá el sistema de Comando y Control (C&C), el cual se usa para dar instrucciones remotas a máquinas comprometidas o como el lugar donde todos los datos pueden ser exfiltrados. El sistema C&C a menudo se establece por medio de múltiples rutas para garantizar que la conectividad no se interrumpa si se detecta o elimina parte de ellas, además es importante tener en cuenta que los métodos de comando y control no siempre requieren una conexión directa que admita una alta frecuencia de comunicación bidireccional (Assante, M. J. & Lee, R. L., 2015),. Con el acceso administrado y habilitado, el atacante ahora puede comenzar a lograr su objetivo.

2.1.6 Actuar en el objetivo

Después de obtener la configuración de comunicación con el sistema objetivo, el atacante ejecuta los comandos, los cuales dependen del interés del ataque; sin embargo, las actividades comunes incluyen el descubrimiento de nuevos sistemas o datos, movimiento lateral alrededor de la red, instalación y ejecución de capacidades adicionales, lanzamiento de esas capacidades, captura de comunicaciones transmitidas como credenciales de usuario, recopilación de datos deseados, exfiltración de esos datos fuera del medio ambiente y las técnicas anti forenses, como limpiar los rastros de la actividad de ataque o defender su punto de apoyo cuando se encuentra con defensores, como respondedores de incidentes (Assante, M. J. & Lee, R. L., 2015).

2.2 Ciberseguridad.

La evolución de las tecnologías de información y las comunicaciones, ha o va a impactar en la forma en que utilizamos y adquirimos la mayoría de los servicios en nuestra vida diaria, donde el funcionamiento de las TICs y la operación de las infraestructuras críticas como el transporte, las comunicaciones, el comercio electrónico, los servicios financieros, los servicios de emergencia y servicios públicos se sustentan en la ciberseguridad de la información que fluye a través de estas infraestructuras. En el año 2011, un equipo de trabajo bilateral del EastWest Institute (EWI) y la Universidad de Moscú desarrolló un marco de terminología internacional, en el cual definieron la ciberseguridad como "una propiedad del ciberespacio, que tiene la capacidad de resistir las amenazas intencionales y no intencionales, responder y recuperarse" (Leiva, E, 2015, p. 2).

En Colombia se consolidó en el documento CONPES 3701 los lineamientos nacionales de una política en Ciberseguridad, los cuales buscan el desarrollo de una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan al país y se define la Ciberseguridad como "la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética" (MinTic, 2014, p.4).

La ciberseguridad juega un papel clave en el control y seguimientos de los procesos físicos y lógicos del ciberespacio, en particular cuando se hace referencia al ciberespacio que impacta las infraestructuras críticas como son los sistemas eléctricos, ya que presentan un potencial significativo de vulnerabilidades en su infraestructura tecnológica que pone en riesgo la continuidad de los servicios de energía bajo condiciones de operación, las cuales también están sujetas a incidentes cibernéticos. Las vulnerabilidades cibernéticas van desde el software de la aplicación, la red de comunicación y/o los dispositivos de campo, representando riesgos en los procesos físicos de las redes eléctricos, en la Tabla 3 se muestran las vulnerabilidades más comunes enfocadas en las redes eléctricas. (Li, Z., Shahidehpour, M., & Aminifar, F; 2017)

Tabla 3. Las vulnerabilidades más comunes en las TO de las redes eléctricas.

Dominio	Vulnerabilidades comunes
Software de la aplicación	Mala calidad del código
	Inadecuada gestión de la configuración
	Pobres permisos y gestión de acceso
	Comprobación de integridad de datos inadecuada
	Inadecuada gestión de parches
	Manejo inadecuado de errores
	Inadecuada protección de la base de datos
Red de comunicaciones	Inadecuada segregación y segmentación
	Control de acceso inadecuado
	Detección y prevención de intrusiones débiles
	Mecanismo de cifrado débil
	Protección inadecuada de datos confidenciales
	Monitoreo y auditoría inadecuados de la red.
	Seguimiento de anomalías inadecuado
Dispositivos de campo	Acceso físico desprotegido
	Configuración incorrecta del dispositivo
	Protección de firmware inadecuada
	Falta de hardware resistente a la manipulación
	Débil autenticación y autorización

Fuente: Li, Z., Shahidehpour, M., & Aminifar, F. (2017).

Los dispositivos que conforman el ciberespacio enfocado en las infraestructuras críticas han recibido un impulso tecnológico considerable durante los últimos años, y se espera que se desarrolle aún más, donde de forma paralela se ha creado un escenario paralelo el cual muestra un incremento en los riesgos de ciberseguridad sobre la confidencialidad, integridad y disponibilidad de su información, conceptos que se explican en la Tabla 4.

Tabla 4. Las vulnerabilidades más comunes en las TO de las redes eléctricas.

Pilares de ciberseguridad	
Confidencialidad	hace referencia a que los datos solo sean accesibles e interpretados por el destino autorizado, y que no se produzcan divulgaciones intencionales o no intencionadas de los datos.
Integridad	es que los datos sean auténticos, sin modificaciones, para que la información no se falsee o corrompa, como ejemplo se hace referencia a ley 527 de 1999 donde se reglamentó el comercio electrónico en Colombia
Disponibilidad	es acceder a los datos cuando se necesiten, sin embargo no se puede hacer referencia a una disponibilidad en el ciberespacio del 100 % ya que los dispositivos electrónicos tienen elementos físicos que definen su tiempo medio de reparación y su tiempo medio de falla.

Fuente: Cleveland, F. M. (2008).

La seguridad en el ciberespacio es un desafío para las infraestructuras críticas, sin embargo, las empresas de energía eléctrica están enfocando sus esfuerzos en el desarrollo de estrategias de ciberseguridad flexibles y coordinadas, donde se permita reducir los riesgos de un ciberataque que impacte la continuidad operativa, por lo que es muy importante contar con una convergencia en las tecnologías de información y las comunicaciones con protocolos, dispositivos y arquitecturas tecnológicas que le apunten a la disponibilidad, confiabilidad e integridad extremo a extremo en la prestación de los servicios de energía eléctrica como pilares de su funcionamiento (Puthal, D., Mohanty, S. P., Nanda, P.& Choppali, U, 2017), así mismo, deben contar con características de control para determinar la interacción y trazabilidad con los datos del sistema eléctrico.

2.3 Arquitecturas, dispositivos y protocolos para una estrategia de ciberseguridad.

En el mundo de hoy los datos juegan un papel muy importante en el desarrollo de las sociedades, donde la mayoría de los dispositivos electrónicos tienen la capacidad de almacenamiento y comunicar de datos, donde se presentan vulnerabilidades que permiten la materialización de ciberataques. Los ciberataques no van a desaparecer; de hecho, aumentarán, se intensificarán y se volverán cada vez más sofisticados (Thakur, M. A., 2019), por lo que se debe desplegar estrategias de ciberseguridad coordinadas para que las personas, las empresas y los gobiernos puedan avanzar en el objetivo común de hacer que el ciberespacio sea más seguro.

En una estrategia de ciberseguridad no se crea un escudo cibernético impenetrable, más bien, minimiza el riesgo y mantiene a las organizaciones un paso por delante de los cibercriminales, para esto los dispositivos y protocolos enfocados en la ciberseguridad deben estar integrados en la realización de la función de controlar y proteger los ciberactivos de las empresas, donde si un atacante o un usuario no autorizado penetra las primeras capas de defensa en un sistema, otros puedan responder de inmediato para tomar medidas preventivas.

2.3.1 Firewall.

Un firewall es un sistema que permite ejercer políticas de control de acceso entre redes de datos, definiendo los servicios que pueden accederse por medio de sus funcionalidades para bloquear el tráfico y otro para permitirlo (Suarez, D. E., 2016), representando un mecanismo de defensa para la conectividad por medio de reglas.

Hay firewalls basados en hardware y otros en software, pero lo que resulta importante es la forma como gestionan sus recursos lógicos done se permite filtrar el tráfico TCP, UDP,

ICMP, IP, entre otros, (Guijarro, A. A., Yepes Holguin, J. M., Peralta Guaraca, T, J & Ortiz Zambrano, C. ,2018), lo más relevante es definir si un paquete pasa, se modifica, se convierte o se descarta, por último es importante definir la velocidad con la que se requiere que se ejecute esta funcionalidad en las redes de datos, debido a que hay diferentes sistemas que requieren una exigencia ajustada para su disponibilidad operacional.

Cuando la prioridad es el filtrado rápido de paquetes, se sacrifica seguridad, ya que profundizar en el paquete IP para su inspección requiere tiempo y recursos de máquina, de igual modo, los firewalls permiten conectar a las empresas al ciberespacio con una sola dirección IP por medio del RFC1918 Network Address Translation (NAT), lo cual enmascara direcciones IP en otra IP privadas, permitiendo ocultar el direccionamiento real de los ciberactivos, y es una buena práctica en ciberseguridad, así mismo, la mayoría de los ISP le dan a una compañía un cierto número de destinatarios de IP cuando se registran para el servicio de Internet. Para superar esta limitación, los firewalls y enrutadores pueden usar NAT (SANS Institute, 2003), a continuación, se muestran tres segmentos de direccionamiento IP que se pueden utilizar para configurar NAT con el siguiente rango de direcciones privadas:

- 10.0.0.0 - 10.255.255.255 (prefijo 10/8)
- 172.16.0.0 - 172.31.255.255 (prefijo 172.16 / 12)
- 192.168.0.0 - 192.168.255.255 (prefijo 192.168 / 16)

Los rangos de IP privadas no se enrutan a través de Internet, debido a que todos los ISP bloquean estos rangos en sus enrutadores. Una empresa debe elegir un rango de direcciones IP privadas que se ajuste a su demanda actual y permita el crecimiento futuro. Como se dijo anteriormente, un firewall permite el tráfico solo si cumple con una regla definida en su conjunto de reglas, de igual manera debería usar la filosofía de denegación predeterminada que dicta la configuración de enrutadores y firewalls para bloquear protocolos que no están expresamente permitidos. Los expertos dicen que la mayoría de los segmentos de red solo

necesitan servicios básicos como SMTP para correo electrónico (puerto 25) DNS (puerto 53), HTTP para web (puerto 80) y SSL (puerto 443). Todos los demás puertos pueden cerrarse a menos que sea requerido por alguna aplicación o necesidad comercial. La política de denegación es más difícil de administrar, pero evitará el tráfico no deseado (SANS Institute, 2003), sin embargo, cada entidad define su mejor estrategia.

Como puede ver, el firewall es un dispositivo muy importante en una estrategia de defensa en profundidad para la red, por lo que es necesario proteger este dispositivo con los últimos parches y actualizaciones de servicio, algunas soluciones instalan mas de un firewall para mejorar los niveles de disponibilidad.

2.3.2 VPN.

Algunos dispositivos tienen redes privadas virtuales (VPN) integradas en ellos, esto brinda una conexión segura a la red, donde por medio de un canal de comunicaciones, permite conectarse desde redes remotas como si estuvieran en la red LAN o en la misma tabla de enrutamiento, por medio de una conexión cifrada a la red. La VPN apalanca a la privacidad, seguridad e integridad de la información, las cuales pueden utilizar diferentes protocolos de encriptación para combatir una amenaza cambiante y a menudo desconocida (Fornero, F., 2019), si bien el número continúa aumentando con el tiempo, hay dos tipos de protocolos principales:

2.3.2.1 Point--to--Point Tunneling Protocol (PPTP).

Fue desarrollado por un consorcio fundado por Microsoft para crear una VPN a través de redes de acceso telefónico en julio de 1999 como una característica regular de Windows 95. PPTP se puede configurar y ejecutar como un servicio sin la necesidad de instalar un nuevo software. Dado que el protocolo en sí no tiene ninguna seguridad incorporada, la

confidencialidad del túnel VPN se basa en el cifrado de su tráfico desde otra fuente, MS-CHAP v2 es el más popular de estos tipos de cifrado y permite que incluso las versiones modernas de los sistemas operativos de Microsoft implementen múltiples niveles de autenticación de forma nativa en la pila PPTP de Windows (Fornero, F., 2019).

Cuando salió por primera vez, diferentes investigadores en el mundo han publicado artículos que describen fallas de seguridad con PPTP y la autenticación MS-CHAP v2, algunos de estos hallazgos permitirían a un adversario descifrar el cifrado en dos días, sin embargo, Microsoft ha reparado la falla y emitió una recomendación de que los usuarios de VPN deberían usar L2TP / IPsec o SSTP, a pesar de esta recomendación y las numerosas publicaciones de fallas, el protocolo PPTP y la autenticación MS-CHAP v2 sigue siendo uno de los métodos de autenticación y túnel VPN utilizados en la actualidad (Fornero, F., 2019).

2.3.2.2 L2TP/IPsec

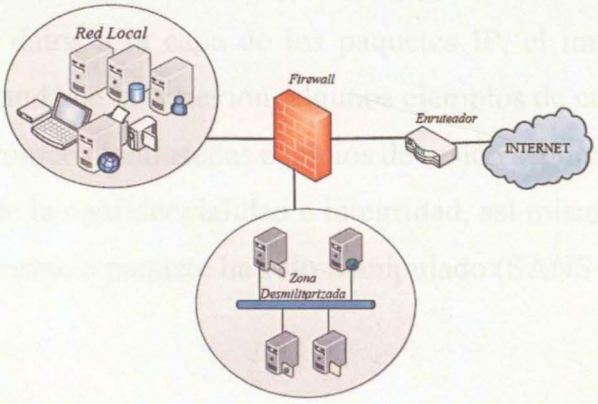
L2TP (Layer 2 Tunnel Protocol with Internet Protocol Security) es un protocolo de túnel utilizado para admitir conexiones de red privada virtual, sin embargo, no proporciona ningún cifrado a los datos que transporta, debido a esto, el protocolo casi se debe implementar junto con IPsec. L2TP / IPsec está integrado en los sistemas operativos modernos y dispositivos con capacidad VPN (Fornero, F., 2019).

L2TP / IPsec funciona envolviendo el paquete de datos original dentro de un nuevo paquete, este nuevo paquete puede tener nueva información de enrutamiento y direcciones IP de origen / destino. Este tipo de envoltura protege la información potencialmente confidencial de la compañía al atravesar la red pública o privada de cualquiera que escuche el tráfico. En este momento, el cifrado IPsec no tiene vulnerabilidades conocidas importantes, y si se implementa correctamente puede ser seguro (Fornero, F., 2019).

2.3.3 DMZ.

Dentro de una organización se cuenta con ciberactivos que suministran las funcionalidades en el ciberespacio necesarias para el correcto funcionamiento de los servicios, parte de los ciberactivos suministran información confidencial, la cual debe ser protegida de usuarios externos e internos no permitidos, para esto se implementa una DMZ o zona desmilitarizada, la cual es una subred en la que están disponibles los servicios protegida al menos por un firewall que define las reglas de acceso a los ciberactivos de la DMZ para los usuarios (Zura, A. Y., 2015), en la Ilustración 8, se muestra una representación gráfica de una DMZ.

Ilustración 8 : DMZ.



Fuente: Zura, A. Y. (2015).

En conclusión, si una empresa va a alojar un servidor ante el ciberespacio, debe configurar una DMZ ya que este segmento de red está protegido por el firewall y está separado de su segmento de red interna. Si un atacante irrumpe en la subred de su pantalla, su red interna sigue siendo segura y esto agrega otro nivel de protección. También puede configurar una DMZ para que se permita de forma controlada que se conecten a su red de

forma segura y explícita desde redes que están filtradas, esto significa que se va a confiar en que su red es segura en su lado del firewall, no se debe permitir entrar a toda la red y luego ya que tendrían un camino limpio hacia la totalidad de los ciberactivos sin controles, se debe configurar una subred filtrada y solo dar acceso y abrir puertos que sean necesarios para realizar las operaciones (SANS Institute, 2003).

2.3.4 Cifrado.

El tráfico que cruza por el ciberespacio por defecto no es seguro, se envía en texto plano, cuando se usa cifrado en las redes de datos o en Internet, generalmente se utiliza el puerto TCP 443 o la capa de conexión segura (SSL), agregando una capa que el atacante necesitaría romper (SANS Institute, (2003).

Cuando se usa el cifrado de datos, se impacta negativamente el rendimiento del servicio, debido que se agregan datos a la capa de los paquetes IP, el impacto en el rendimiento depende del ancho de banda de la conexión, algunos ejemplos de cuándo usar el cifrado son VPN, PKI, correo electrónico, contraseñas e inicios de sesión seguros. El cifrado asegura que se respeten los pilares de la confidencialidad e integridad, así mismo, por medio del cifrado se puede saber si un mensaje o paquete ha sido manipulado (SANS Institute, (2003).

2.3.5 Syslog.

Con cualquier infraestructura tecnológica, es prudente monitorear los registros de su sistema, por lo que se debe configurar un syslog en un servidor separado y monitorearlo diariamente. Al usar un servidor syslog, descarga el procesador y el almacenamiento de otros dispositivos además de tener un recurso dedicado para manejar los históricos de lo que pasa en la red (SANS Institute, 2003).

2.3.6 Balanceador de carga.

Es un dispositivo de hardware o software que se encarga de distribuir las solicitudes que llegan de los usuarios u otros dispositivos en los servidores disponibles por medio de un algoritmo, buscando el óptimo desempeño de las aplicaciones, así mismo incluye técnicas informáticas y técnicas de resolución de problemas para completar las actividades de procesamiento de solicitudes.

2.3.7 IPS e IDS.

Un sistema de detección o protección de intrusos son programas utilizado para detectar y/o prevenir acceso no autorizado a una red, utilizando patrones o firmas de ataques conocidos en un análisis del tráfico de la red, verificando en los paquetes por medio de firmas la búsqueda de software malicioso basadas en anomalías comportamentales de la red, de acuerdo a políticas que la plataforma y a las normas establecidas (Suarez, D. E., 2016). Los beneficios básicos de los sistemas IPS e IDS son los siguientes:

- Eficiencias operativas para reducir la necesidad de reaccionar a los registros de eventos para su protección.
- Detección o protección proactiva de la infraestructura de la red.
- Mayor cobertura contra ataques de paquetes y ataques de día cero
- Detectar actividades maliciosas normales e intrusivas.

En la Tabla 5, se hace un breve resumen de la clasificación de los IDS/IPS

Tabla 5. Clasificación de los IDS/IPS

<table>
<tr><td colspan="3">Clasificación</td></tr>
<tr><td rowspan="2">Según el modo de análisis</td><td colspan="2">Detectores de usos indebidos</td></tr>
<tr><td colspan="2">Detectores de anomalías</td></tr>
<tr><td rowspan="3">Según el tipo de sensores</td><td rowspan="3">De máquina</td><td>Sistema Operativo</td></tr>
<tr><td>De aplicación</td></tr>
<tr><td>Hardware</td></tr>
<tr><td rowspan="2">Según el tiempo de ejecución</td><td colspan="2">Periódicos</td></tr>
<tr><td colspan="2">De tiempo real</td></tr>
<tr><td rowspan="2">Según el tipo de respuesta</td><td colspan="2">Activos</td></tr>
<tr><td colspan="2">Pasivos</td></tr>
<tr><td rowspan="2">Según la arquitectura</td><td colspan="2">Centralizados</td></tr>
<tr><td colspan="2">Distribuidos</td></tr>
</table>

Fuente: Suarez, D. E., (2016).

Estos dispositivos ayudan a obtener una visión general de su red por medio de la supervisión o control de la red por medio de la búsqueda de firmas, monitoreando los segmentos de la red, sin estos dispositivos, la mayoría de los ataques pasarían desapercibidos.

2.3.8 Anti-virus (Antimalware)

Una de las defensas más utilizadas en las capas profundas de una estrategia de ciberseguridad de defensa en profundidad es el software anti-virus, el cual debe instalarse en todos los servidores y computadoras de escritorio de las organizaciones, ya que si se tiene un

software anti-virus en sus servidores y escritorios, esto ayudará a detener algunos ataques; el software antivirus establece una capa significativa en un perímetro de seguridad reforzado (SANS Institute, (2003), a continuación se muestran varias de sus fortalezas:

- Es efectivo ante números Male-Wares
- Tiene una tasa relativamente baja de falsos positivos.
- Recibe actualizaciones y el cliente no lo verá ejecutándose en segundo plano
- El software antivirus es asequible

Todas las compañías antivirus tienen actualizaciones que deben aplicarse a sus servidores y equipos de escritorio. La mayoría de las empresas de antivirus empresariales tienen una consola central que puede programar sus actualizaciones que deben enviarse a los clientes, sin embargo, si se libera un virus de día cero en la naturaleza, deberá aplicar una revisión a su software de virus y eliminarlo de inmediato. La consola ayuda a realizar un seguimiento de qué usuario tiene male-ware, también facilita la realización de informes y hacer que su equipo de soporte de desktop intente limpiar el male-ware del dispositivo (SANS Institute, 2003), este software es importante para la estabilidad de los dispositivos en el ciberesapcio.

2.3.9 Manejo de parches.

Los administradores de sistemas deben parchar sus sistemas. Microsoft es uno de los sistemas más difíciles de mantener actualizado, debido a que Microsoft sale con una nueva solución de seguridad muy frecuentemente. Los administradores de sistemas deben mantenerse al día con todas las actualizaciones y cuáles deben aplicar, una forma es suscribirse a una lista de vulnerabilidades o grupo de noticias como los sitios web CERT o SANS donde se puede obtener las últimas noticias sobre los parches a los que debe prestar atención. ¿Cómo saber si su empresa necesita la actualización o pueden esperar el próximo

parche de servicio?, Fred Avolid tiene un proceso de seis pasos para parches prácticos (SANS Institute, 2003).

1. Desarrollar una base de datos actualizada de todos los sistemas de producción que tenga datos como el sistema operativo, niveles de paquete de soporte, aplicación, tipo de hardware, entre otros.
2. Diseñe un plan para estandarizar los sistemas de producción a la misma versión del sistema operativo o software de aplicación.
3. Haga una lista de todos los controles de seguridad que tiene en su lugar, como enrutadores, firewalls, IDS, IPS, entre otros, así como su configuración.
4. Compare las vulnerabilidades reportadas con su inventario.
5. Clasificar el riesgo evalúa la vulnerabilidad y si está en riesgo.
6. Aplicar el parche.

Si sigue los pasos anteriores, se tiene una lista actualizada de todos los dispositivos y si sale un nuevo parche, se pueden tomar decisiones con información si se necesita aplicarlo o no. Si mantiene los dispositivos parcheados, evitará que las numerosas vulnerabilidades conocidas comprometan sus sistemas. La gestión de parches es un área en la que las deben dedicar tiempo porque es algo que ya deberíamos estar haciendo. Esta área también es donde deberíamos dedicar tiempo y esfuerzo si no puede obtener fondos para nuevos firewalls o sistemas IDS.

2.3.10 Arquitectura de tres capas

Esta arquitectura busca garantizar el funcionamiento autónomo del sistema por medio de la reutilización y distribución del código, segmentando el modelo en tres capas:

- Capa de presentación.
- Capa de aplicación.
- Capa de datos.

Las tres capas están conectadas por una red de área local de alta velocidad, donde cada nivel se debe implementar en forma de capas independientes, donde el funcionamiento de las tres permita un mejor rendimiento de las aplicaciones.

2.3.11 Security Information and Event Management (SIEM).

A medida que los ataques cibernéticos están evolucionando y apuntando a las empresas, lo que puede causar la discontinuidad de sus servicios, la filtración de sus datos y afectar su reputación, las empresas buscan reforzar sus capacidades de ciberseguridad para protegerse contra las amenazas de seguridad cibernética, por lo que adoptan estrategias de seguridad de múltiples capas que incluyen el uso de una solución SIEM, el cual representa un sistema con capacidades de análisis en tiempo casi real de alertas de seguridad y registros generados a partir de varios conjuntos de fuentes dentro de la infraestructura tecnológica de una organización. Sin embargo, implementar una solución SIEM no es solo una fase de instalación que se adapta a cualquier escenario dentro de cualquier organización; El mejor sistema SIEM para una organización puede no ser adecuado para otra (Mokalled, H., Catelli, R., & Casola, V., 2019).

Un sistema SIEM cada día se convierte en un requisito cada vez más recurrente para cualquier tipo de organización que tenga un Sistema de Información, debido a que es el sistema adecuado para la detección de actividades maliciosas.

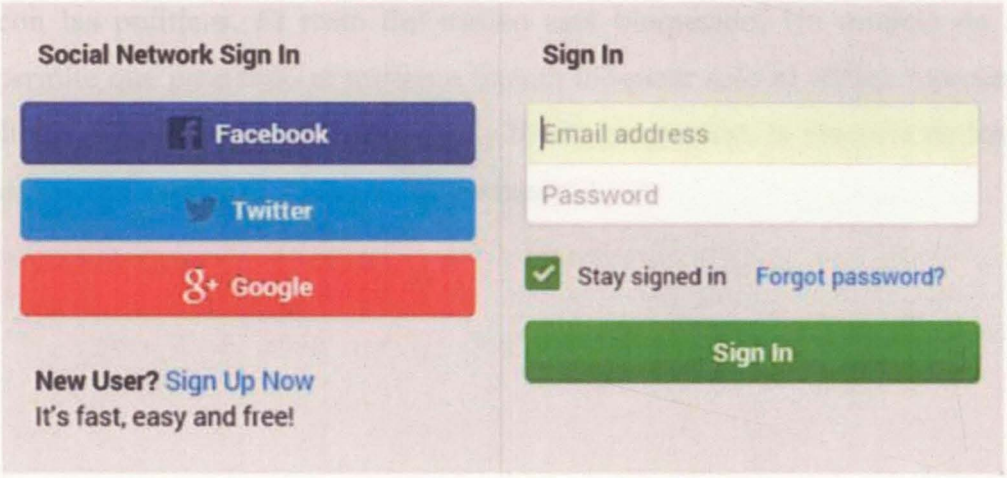
2.3.12 Single Sign-On (SSO)

Es un proceso que permite a un usuario autenticarse solo una vez con una credencial y luego tener acceso a todos los recursos autorizados y múltiples aplicaciones dentro de una empresa, siendo efectivo, ya que los usuarios no tienen la carga de completar los registros

para nuevas cuentas (Scott, C.; Wynne, D., & Boonthum, C, 2016). Estos beneficios podrían incluir minimizar la cantidad de contraseñas y nombres de usuario, y la facilidad para suscribirse a las aplicaciones.

SSO permite a los usuarios disminuir la carga de registrar varias cuentas en línea y recordar contraseñas como se muestra en la Ilustración 9.

Ilustración 9 : Ejemplo de página de inicio de SSO



Fuente: Scott, C.; Wynne, D., & Boonthum, C (2016)

La conveniencia que este tipo de esquema brinda a nuestras vidas en el ciberespacio es importante, sin embargo, de forma paralela se debe comprender que las mismas herramientas que hacen que nuestras vidas sean más convenientes también tienden a ser menos seguras. A medida que avanzamos tecnológicamente más, se hace evidente que debemos pensar cuidadosamente sobre los esquemas y dispositivos utilizados a diario. Si estamos tan dispuestos a enviar nuestra información a herramientas como los SSO, conociendo las posibles vulnerabilidades de seguridad.

2.3.13 Firewalls de aplicaciones web (WAF).

Los WAF se implementan para proteger las aplicaciones web y ofrecen una seguridad profunda, realizando una inspección profunda de paquetes del tráfico de red que ocurre entre el cliente y el servidor. Al analizar los datos transferidos entre el cliente y el servidor, WAF puede identificar posibles ataques incluso si a la implementación le falta esa detección.

WAF puede tener dos tipos de modelos de seguridad basados en el tipo de política: positivo o negativo. Un modelo de seguridad positivo solo permite el paso del tráfico que coincide con las políticas. El resto del tráfico está bloqueado. Un modelo de seguridad negativo permite que pase todo el tráfico e intenta bloquear solo el tráfico representado por reglas maliciosas (Clincy, V. & Shahriar, H., 2018), en general, la mayoría de los firewalls usan reglas positivas o negativas, rara vez ambas.

CAPÍTULO III.
PROPUESTA DE UN MODELO DE SEGURIDAD EN PROFUNDIDAD PARA LA INFRAESTRUCTURA DE MEDICIÓN AVANZADA EN EMPRESAS DE ENERGÍA ELÉCTRICA COLOMBIANAS.

Las brechas en ciberseguridad de las infraestructura de medición avanzada y los dispositivos asociados facilitan un escenario para el uso malicioso de los dispositivos del servicios de energía eléctrica, lo cual conduce al espionaje de datos, daños físicos a los dispositivos, denegación intencional del servicio y explotación de vulnerabilidades con fines de lucro, el capítulo III inicialmente describe una estrategia de ciberseguridad llamada defensa en profundidad y las cinco capas que la componen para luego formular una estrategia de defensa en profundidad enfocada en la infraestructura de medición avanzada de energía eléctrica en Colombia, con una infraestructura tecnológica y arquitecturas maduras e implantadas en las empresas públicas y privadas de nuestro país, por último se describe el impacto de la infraestructura de medición avanzada en el modelo de negocio de las empresas de energía eléctrica en Colombia .

3.1 Defensa en profundidad.

La defensa en profundidad es un concepto, el cual se desarrolló para defender inicialmente activos militares o estratégicos del mundo real mediante la creación de capas de defensa que obligan al atacante a gastar una gran cantidad de recursos, al tiempo que agotan las líneas de suministro, de este modo el objetivo táctico es retrasar y hacer que el ataque enemigo sea insostenible. Esta estrategia resulta en dejar al atacante vulnerable para el contraataque, y de esta manera el defensor puede entonces contraatacar al enemigo y eliminar la amenaza (Small, P., 2019), algunas adaptaciones adicionales de defensa en profundidad se muestran a continuación:

• *Prevención de incendios*: Requiere el despliegue de alarmas de incendio, extintores, planes de evacuación, rescate móvil y equipo contra incendios

• *Energía nuclear*: Hace referencia a la práctica de tener múltiples, redundantes y capas independientes de sistemas de seguridad para el único punto crítico de falla: el núcleo del reactor

• *Ingeniería*: Se enfatiza en la redundancia, donde un sistema que sigue funcionando cuando falla un componente.

Para la ciberseguridad, la defensa en profundidad se enfoca en proteger una red de ciberactivos con una serie de mecanismos defensivos de tal manera que si un mecanismo falla, ya habrá otro para frustrar un ataque, ya que hay tantos atacantes potenciales con una variedad tan amplia de métodos de ataque disponibles, además no existe un método único para proteger con éxito a un sistema en el ciberespacio, y utilizar la estrategia de defensa en profundidad reduce el riesgo de tener un ataque exitoso y probablemente muy costoso en una entidad pública o privada (McGuiness, T.,2019).

El Departamento de Seguridad Nacional de EE. UU. (DHS) propuso una estrategia de "defensa en profundidad" del sistema de control industrial y dividió la red de control industrial en diferentes zonas de seguridad (Ning, P., Cui, Y., & D.S. Reeves, 2002), al proponer diferentes capas en el sistema de seguridad como firewalls, la detección de intrusiones, el análisis de vulnerabilidades y otras medidas de seguridad para buscar una protección integral por capas, en la Ilustración 10 se muestra el modelo de defensa en profundidad, el cual para el presente trabajo de grado está enfocado en cinco capas funcionales (perímetro, segmentos, servidores y estaciones, aplicaciones y datos), donde cada capa tiene un alcance definido para su segmento.

Ilustración 10 : Modelo de defensa en profundidad.

Fuente: ETEK, (2019).

El modelo de defensa en profundidad que se desarrollará en el presente de grado es el basado en la figura anterior, donde la defensa en profundidad es una estrategia funcional, la cual busca asegurar la información y administrar el riesgo de los elementos que hacen parte de la infraestructura de una red por medio de capas en una estructura definida para filtrar, evitar y detener amenazas a las que están expuesto los recursos físicos y los servicios que son prestados a los usuarios, y donde cada capa cuenta con diferentes controles de seguridad (Suarez, D. E., 2016), y las cuales se explican a continuación:

3.1.1 Perímetro.

La defensa perimetral es una parte importante de la estrategia de defensa en profundidad, donde se protege las conexiones antes de ingresar a la infraestructura tecnológica de la empresa por medio de reglas estrictas y complejas para la conectividad. Las redes de datos en las tecnologías de operación emplean dispositivos para separar y segmentar las comunicaciones al igual que las redes basadas en Ethernet que ejecutan TCP / IP (Jiang, N.,

& Zhenyu, H. L., 2017), generalmente en esta capa se utilizan dispositivos como Balanceador, Firewall, IPS, entre otros.

3.1.2 Segmento.

La existencia de servicios compartidos en la red, como el de históricos de datos, por contextos como el anteriormente expresado, la capa de segmente tiene un impacto significativo en la implementación de la protección de las conexiones existentes entre los servidores y estaciones de trabajo, donde se debe examinar el tráfico permitido en la red, así mismo bloquear el que no es necesario.

3.1.3 Servidores y/o Estaciones de Trabajo.

Esta capa hace referencia al aseguramiento de los servidores y estaciones de trabajo, por medio del cumplimiento criterios de un conjunto de actividades que son realizadas para fortalecer la seguridad de los servidores y estaciones de trabajo, por medio de las políticas aplicadas para el aseguramiento de los servicios en el ciberespacio (Rico, I. E., 2015), así mismo en esta capa se implementan configuraciones en el sistema operativo, recomendaciones de expertos y fabricantes que nos guían con buenas prácticas, retardando la acción de un atacante y disminuyendo la probabilidad de explotar vulnerabilidades.

3.1.4 Aplicación.

En esta capa se debe incorporar la seguridad en las aplicaciones, manteniendo la protección de acceso y ejecución de software no habilitados, por lo anterior en esta capa se revisa y controla la ejecución de los servicios y aplicaciones para que estas operen con los privilegios óptimos, por último, la seguridad en la capa de aplicación se debe implementarse desde el código de la aplicación por medio de buenas prácticas en el desarrollo seguro,

canales de comunicación seguros y arquitecturas que permitan la separación de ambientes en modelos de tres o 2 capas por medio de un ente de control y gestión (Guijarro, A. A., Yepes Holguin, J. M., Peralta Guaraca, T, J & Ortiz Zambrano, C. ,2018).

3.1.5 Datos.

Consientes que el activo más importante de las empresas son los datos (Guijarro, A. A., Yepes Holguin, J. M., Peralta Guaraca, T, J & Ortiz Zambrano, C. ,2018), en esta capa, se define la forma en cómo se administra el dato desde su creación, clasificación, transmisión y la eliminación con el objetivo de proteger los datos por medio de un esquema que reduzca significativamente los niveles de vulnerabilidades en las empresas, aplicando una estructura jerárquica para mejorar la ciberseguridad de los datos.

3.2 El sistema eléctrico, la infraestructura de la medición avanzada y la defensa en profundidad.

El sistema eléctrico de los países contienen una multitud de dispositivos desplegados para medir, observar y controlar su proceso físico, así mismo, los sistemas de energía están experimentando una evolución similar a la que atravesó el sector de telecomunicaciones hace varias décadas. La transformación de la red eléctrica incorpora capacidades tecnológicas para la medición, el control y operación del sistema eléctrico, transformándolo en redes inteligentes (Hébert C., 2013),donde los sistemas analógicos y cableados son reemplazando por sistemas automatizados.

La red inteligente es una revolución que ha permitido la distribución de energía de una manera más eficiente; la infraestructura de la medición avanzada es un subsistema que conforma las redes inteligentes, (Boal, J., & Larrauri, M.; 2011), además propicia un cambio en el modelo tradicional de consumo de energía, ya que permiten operaciones inteligentes

como la conmutación de control de carga, la gestión de datos del medidor y la demanda mediante la creación de una red de comunicación bidireccional para contadores inteligentes, sin embargo, el pronóstico de la carga, la gestión de la respuesta a la demanda y el perfil preciso de la carga del consumidor basados en los datos generados por los medidores inteligentes continúan siendo un desafío para el sistema eléctrico y los problemas de investigación en la academia, por lo anteriormente expresado, se selecciona la infraestructura de la medición avanzada enfocada en las redes eléctricas como uno de los pilares de la presente monografía.

La afectación en la prestación del servicio de energía eléctrica puede ser catastrófica en la seguridad y la economía de las naciones, los activos críticos, los dispositivos electrónicos inteligentes, las comunicaciones y su interdependencia, hacen que las empresas prestadores del servicio de energía tengan el reto de fortalecer continuamente sus sistemas de ciberseguridad (Ten, C. W., Govindarasu, M., & Liu, C. C., 2007); debido a que de forma paralela a los beneficios que nos trae las infraestructuras de medida avanzada, el uso de estándares abiertos, la obsolescencia tecnológica, entre otros elementos, permite que sus vulnerabilidades incrementen el riesgo de afectar la operación de los servicio de energía eléctrica (Byres, E., & Lowe, J. ;2004), y traer como consecuencia desafíos en la disponibilidad, estabilidad y rendimiento para la gestión de riesgos de ciberseguridad en la continuidad operativa.

Después de los ciberataques en Irán y Ucrania, la ciberseguridad sobre las infraestructuras críticas, especialmente aquellas que controlan procesos estratégicos en las naciones, han adquirido una importancia vital para los gobiernos, es en este escenario que la implementación de estrategias de ciberseguridad para la infraestructura tecnológica en las empresas de energía eléctrica toma una mayor relevancia (Smith, E., Corzine, S., Racey, D., Dunne P., Hassett, C., & Weiss, J. ;2016), así mismo, el modelo de defensa en profundidad fue propuesto como una estrategia de ciberseguridad por parte del Departamento de Seguridad Nacional de Estados Unidos para los sistemas de control industrial (Ning, P., Cui, Y., & D.S. Reeves, 2002), debido a que estos deben estar separados de cualquier impacto

externo como Internet, y los cambios en el sistema, como las actualizaciones, deben seguir un protocolo de cadena de suministro de hardware y software cuidadosamente examinado para proteger contra malware o spyware, por lo anteriormente, la defensa en profundidad es una estrategia funcional óptima que se seleccionó para la ciberseguridad la infraestructura de medición avanzada.

3.3 Diseño de una estrategia de defensa en profundidad para la infraestructura de medición avanzada.

La infraestructura de medición avanzada debe estar estrictamente protegida para garantizar operaciones confiables y seguras de la red inteligente, debido a que un ciberataque para el sistema de medición puede conducir a la fuga de privacidad del usuario o incluso al compromiso de los sistemas de medición avanzada. Así mismo, es importante hacer referencia que la infraestructura de medición avanzada está ubicada dentro de un área de suministro de energía en las ciudades y las regiones, sin embargo, algunos nodos son de difícil acceso debido a que están geográficamente retirados de las urbes, lo que representa un esfuerzo mayor para la ciberseguridad, operación y mantenimiento (Zhiguo, W., Guilin, W. Yanjiang Yang, & Shenxing, Shi. ;2014).

En la topología para la infraestructura de medición avanzada propuesta, la ciberseguridad no se puede lograr solamente confiando en soluciones y tecnologías de seguridad. Por lo tanto, debemos integrar estrategias que permitan mejorar la capacidad de ciberseguridad general del servicio. Con el fin de buscar mejorar los niveles de la confiabilidad, disponibilidad e integridad del servicio de la medición avanzada para el servicio de energía eléctrica y hacerla modular, se hace necesario diseñarla de manera jerárquica, de tal manera que interactúan los protocolos, servicios, aplicaciones, dispositivos, entre otros bajo el marco de referencia seguridad en profundidad (Abercrombie, R. K., Schlicher, B. G., Sheldon, F. T., 2014).

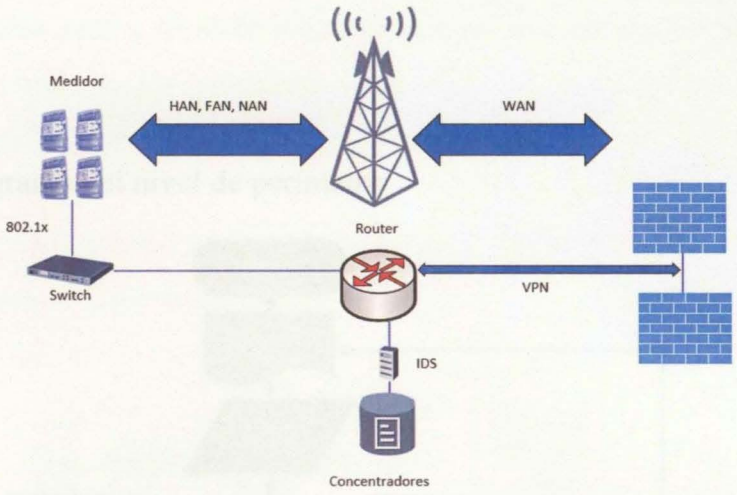
A continuación, se presenta la estrategia de ciberseguridad basada en el modelo de seguridad en profundidad para la infraestructura de medición avanzada en empresas de energía eléctrica colombianas, la construcción de la estrategia se ha generado con el propósito de proteger parte de las infraestructuras críticas de Colombia, a sus ciudadanos, su economía y aprovechar el acceso al ciberespacio para mejorar el desempeño económico y la prestación de servicios públicos, extrayendo lecciones aprendidas y útiles que pueden tenerse en cuenta por los países de América Latina y el Caribe y por la OEA, como base para la construcción de las estrategias de Ciberseguridad y Ciberdefensa a implementar en la región (ETEK, 2019).

La estrategia funcional plantea por medio de cinco capas (perímetro, segmentos, servidores y estaciones, aplicaciones y datos) los controles mínimos de ciberseguridad para la infraestructura de medición avanzada, donde se busca asegurar la información y administrar el riesgo de sus elementos, definiendo diferentes controles de seguridad como se muestra a continuación:

3.3.1 Diseño del nivel de perímetro

Esta capa permite definir el primer nivel de ciberseguridad en la infraestructura de medición avanzada, la cual enfoca sus esfuerzos en proteger la infraestructura de ataques externos, por lo que se propone proteger los medidores en el acceso físico hacia el lugar en donde se alojan, con el propósito de mantenerlos seguros físicamente por medio de un bloqueo mecánico o con un candado de seguridad (Viveros, J, 2015), en la Ilustración 11 se muestra el diagrama del nivel de perímetro y los dispositivos que están involucrados en su arquitectura topológica.

Ilustración 11 : Diagrama del nivel de perímetro



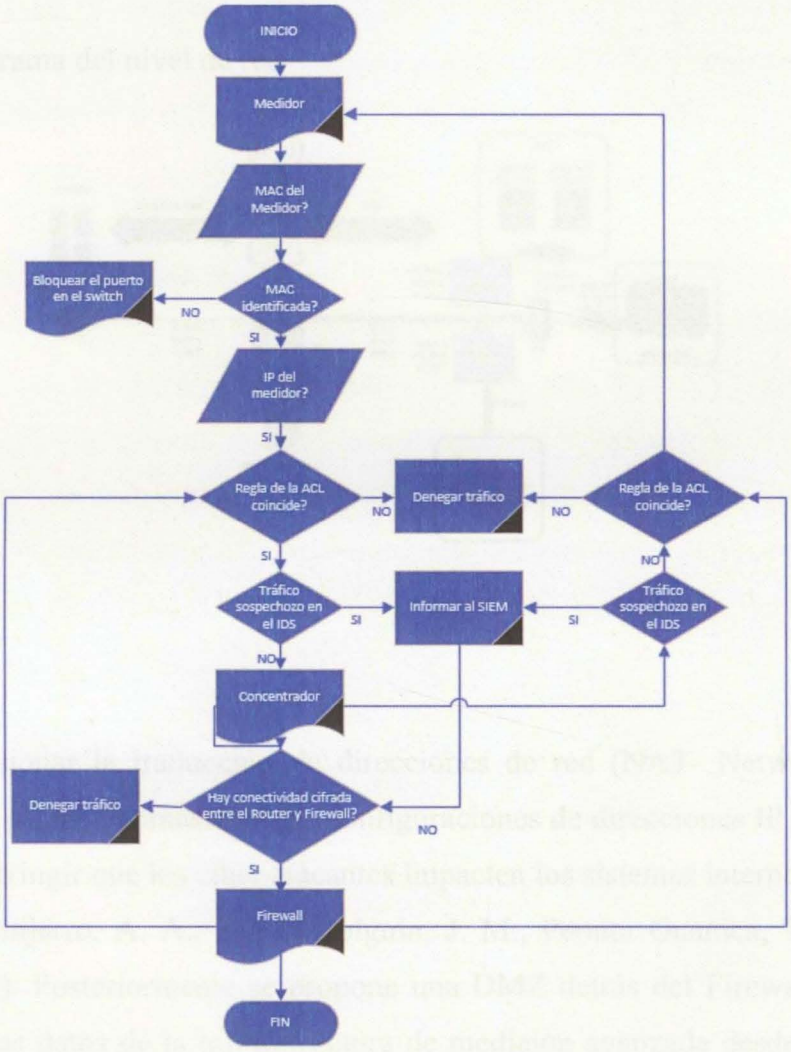
Fuente: Propia

En el nivel de red HAN, FAN, NAN se encuentran las comunicaciones entre los medidores y concentradores, la cual puede ser de manera inalámbrica, (Lora, SigFox, NOB-IoT, entre otras) o por PLC, por lo que se propone implementar un sistema autenticación en la red usando el protocolo 802.1x, con el propósito de garantizar seguridad perimetral, y una correcta identificación de la MAC en la red de los medidores inteligentes en el switch de acceso, los cuales tendrán comunicación con un router, el cual posibilita aprovisionar todos los medidores dentro de rangos de IPs controlados, permitiendo o denegando el tráfico que se genere desde estos por medio de listas de control de acceso (ETEK, 2019).

Además, se propone implementar IDS, con el objetivo de monitorear, analizar e informar ante cualquier desviación no autorizada y anómala de la red, buscando fortalecer un sistema confiable de medición, rastreando e identificando los ataques a la red que detectan a través de los registros de los IDSs. Para las redes WAN (Zura, A. Y., 2015), el firewall representa un rol con gran impacto, ya que es el dispositivo establece las VPNs de los routers que recogen la conectividad de los concentradores y medidores inteligentes, implementar una topología de alta disponibilidad, con por lo menos dos dispositivos tipo firewall configurados

en alta disponibilidad (Guijarro, A. A., Yepes Holguin, J. M., Peralta Guaraca, T, J & Ortiz Zambrano, C., 2018), en la Ilustración 12 se muestra el diagrama de flujo para el nivel de perímetro.

Ilustración 12 : Flujograma del nivel de perímetro



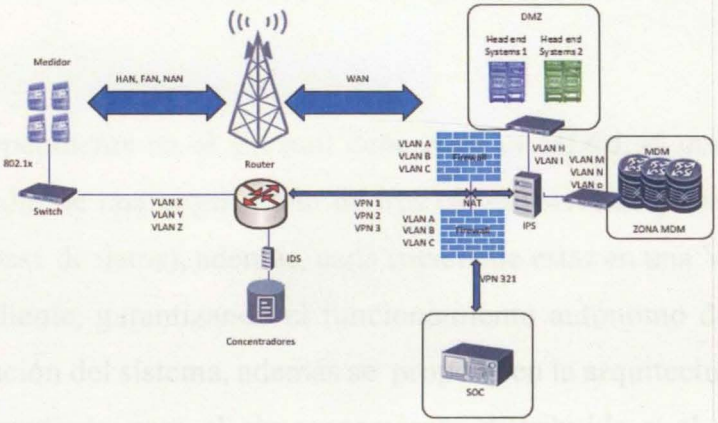
Fuente: Propia

3.3.2 Diseño del nivel de segmento

Las configuraciones en el firewall permiten controlar la comunicación de acuerdo a unas políticas de enrutamiento definidas, donde se debe segmentar la red por medio de segmentos

de broadcast independientes con máscaras de red cerradas entre el firewall y los concentradores con VLANs independientes, de esta manera se debe supervisar, controlar y filtrar el tráfico entre las redes, además busca garantizar una independencia lógica de los datos en tránsito por medio de las comunicaciones entre los dos dispositivos (Guijarro, A. A., Yepes Holguin, J. M., Peralta Guaraca, T, J & Ortiz Zambrano, C., 2018).

Ilustración 13 : Diagrama del nivel de red



Fuente: Propia

Se debe aprovisionar la traducción de direcciones de red (NAT- Network Address Translation), lo cual permite enmascarar las configuraciones de direcciones IP y de puertos TCP y UDP para restringir que los ciber atacantes impacten los sistemas internos y externos de forma directa (Guijarro, A. A., Yepes Holguin, J. M., Peralta Guaraca, T, J & Ortiz Zambrano, C., 2018). Posteriormente se propone una DMZ detrás del Firewall, donde se acceda o deniegue los datos de la infraestructura de medición avanzada desde y hacia los servicios de Head End System, controlando la conectividad y los datos de los usuarios internos y externos.

La infraestructura de medición avanzada es un sistema crítico por sus datos confidenciales y estrictas regulaciones de cumplimiento, por lo que se propone implementar

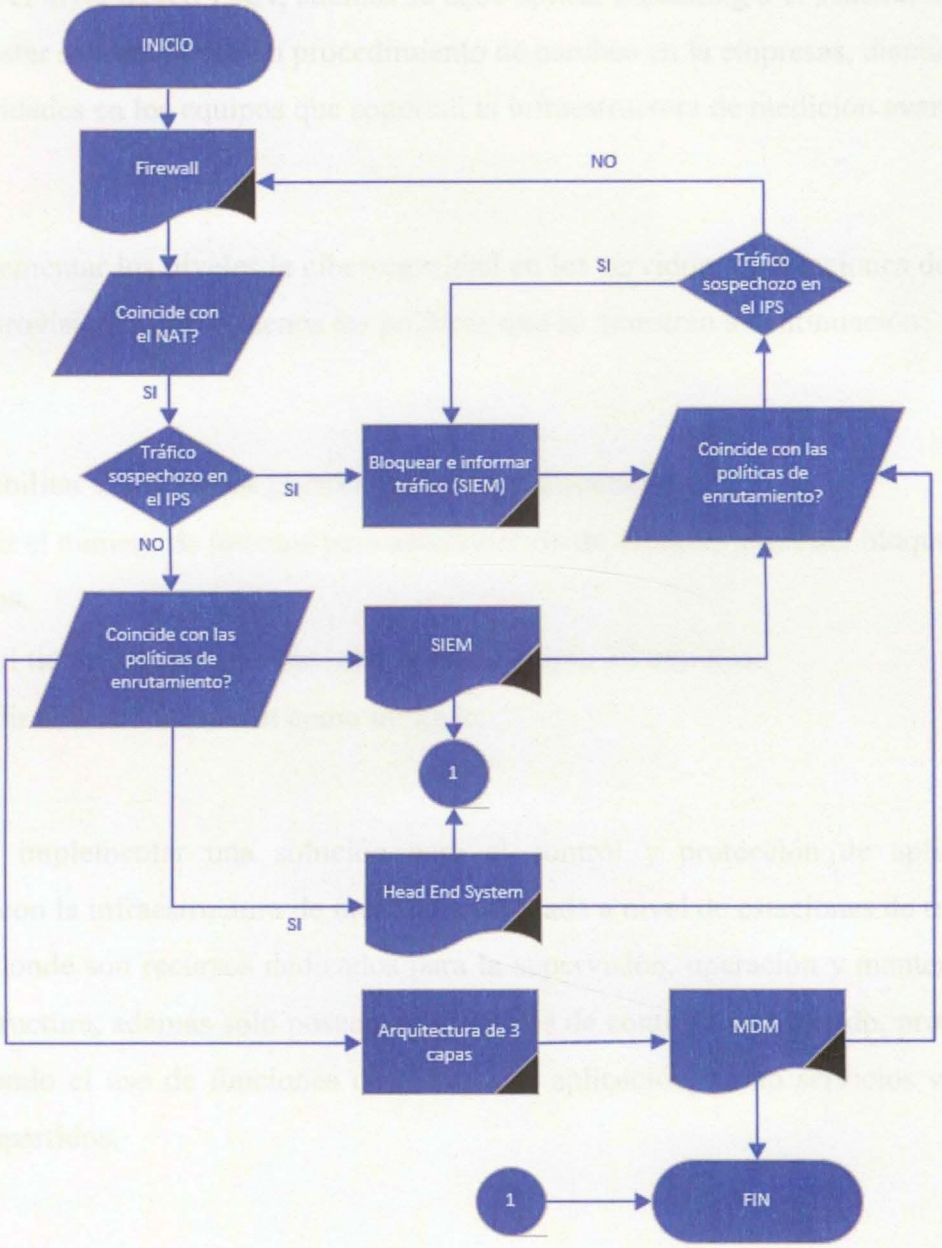
la funcionalidad de un sistema de protección de intrusos (IPS), para rastrear, identificar y proteger la infraestructura de los ciberataques por medio de firmas, detectando y controlando el acceso no autorizado (Suarez, D. E., 2016).

Considerando las funcionalidades de firewall e IPS se implementa controles de ciberseguridad a nivel de las tramas, paquetes y puertos TCP/UDP, reduciendo el riesgo de un ciberataque, así mismo, deben ser complementadas por medio de la implementación de rutas explicitas publicadas en la red interna y externa (Viveros, J, 2015).

En una zona independiente en el firewall debe estar el MDM, el cual, se sugiere esté implementado por medio de una arquitectura de tres capas (nivel de presentación, nivel de aplicación y nivel de base de datos), además, cada capa debe estar en una VLAN y segmento de broadcast independiente, garantizando el funcionamiento autónomo del sistema para la reutilización y distribución del sistema, además se propone en la arquitectura un balanceador de carga sensible al contexto para el almacenamiento distribuido y el procesamiento de consultas en el sistema Head End (Guijarro, A. A., Yepes Holguin, J. M., Peralta Guaraca, T, J & Ortiz Zambrano, C., 2018).

Las empresas de energía eléctrica colombianas deben implementar una solución de gestión de eventos e incidentes de seguridad (SIEM), garantizando buenos controles de gestión para evitar resultados inesperados y mantener la disponibilidad, integridad y confidencialidad de los servicios relacionados con la prestación del servicio, con un enfoque estructurado para administrar tareas, que soporte las decisiones enfocado en tareas de ciberseguridad, valorando las entradas y detectando la presencia de amenazas, ataques cibernéticos, anomalías, protegiendo los ciberactivos críticos para lo cual se propone un Secure Office Center (SOC) con conectividad a una zona, VLAN y VPN independiente del firewall (Mokalled, H., Catelli, R., & Casola, V., 2019) , en la Ilustración 14 se muestra el diagrama de flujo para el nivel de segmento.

Ilustración 14 : Flujograma del nivel de segmento.



Fuente: Propia

3.3.3 Diseño del nivel de servidores y estaciones.

El hardening o endurecimiento está definido por un conjunto de procedimientos que son implementadas para fortalecer la seguridad de los servidores, routers, swiches y estaciones

con el objetivo de mitigar el riesgo de incidentes de ciberseguridad. Para incrementar la protección en el nivel de red LAN, además se debe aplicar hardening a el sistema operativo el cual debe estar soportado por un procedimiento de parcheo en la empresas, disminuyendo las vulnerabilidades en los equipos que soportan la infraestructura de medición avanzada.

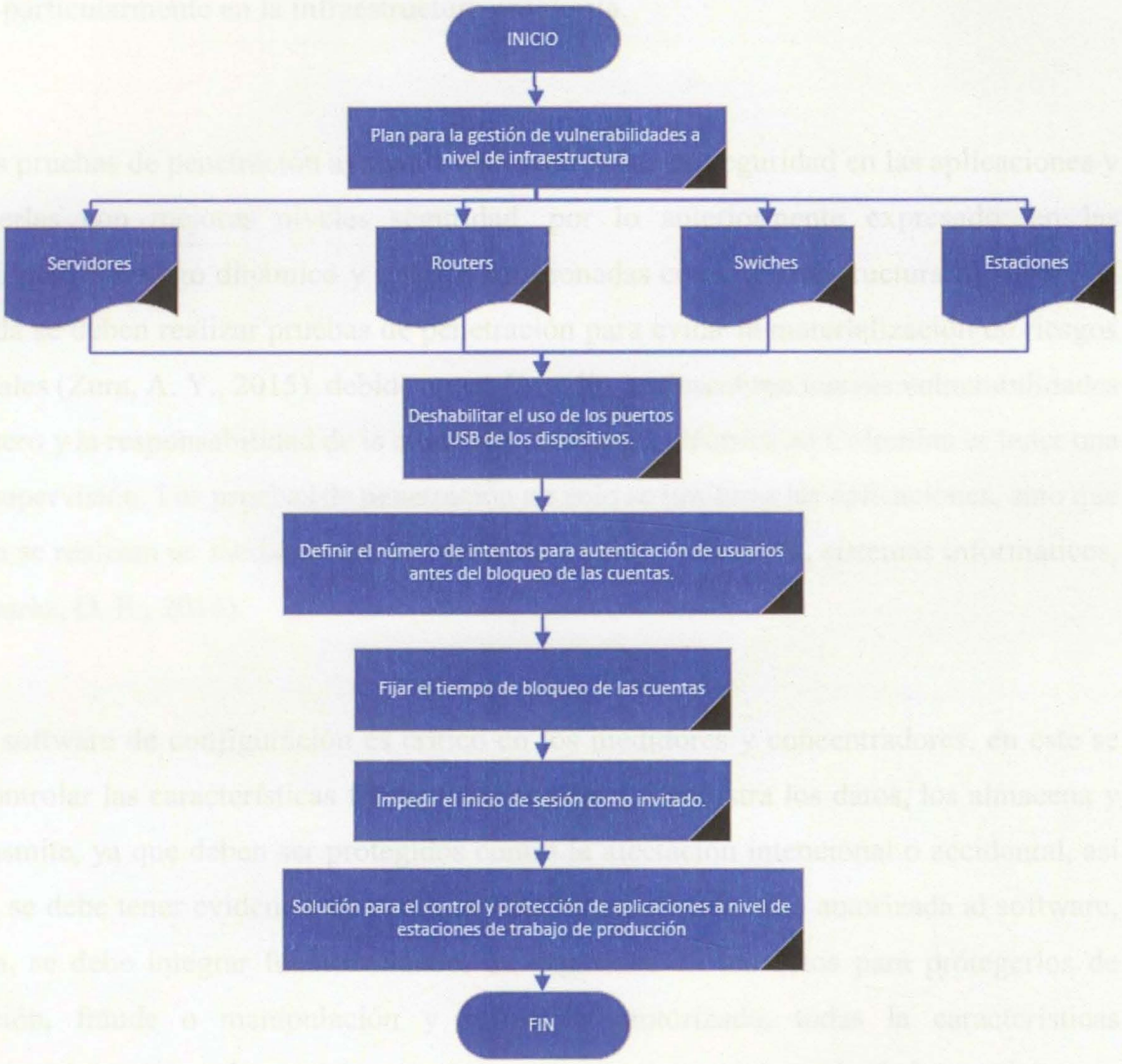
Para incrementar los niveles la ciberseguridad en los servidores y estaciones de trabajo se propone aprovisionar por lo menos las políticas que se muestran a continuación:

- Deshabilitar el uso de los puertos USB de los dispositivos.
- Definir el número de intentos para autenticación de usuarios antes del bloqueo de las cuentas.
- Fijar el tiempo de bloqueo de las cuentas, ejemplo 30 minutos.
- Impedir el inicio de sesión como invitado.

Se debe implementar una solución para el control y protección de aplicaciones relacionadas con la infraestructura de medición avanzada a nivel de estaciones de trabajo de producción, donde son recursos dedicados para la supervisión, operación y mantenimiento de la infraestructura, además sólo poseen aplicaciones de control, controlando, protegiendo y/o restringiendo el uso de funciones de la capa de aplicación, como servicios web y de archivos compartidos.

En general, las vulnerabilidades sobre las infraestructuras de medición avanzada se han multiplicado debido que es una infraestructura con una red de varios sistemas interconectados, por lo anterior, se debe desarrollar un plan para la gestión de vulnerabilidades a nivel de infraestructura, en la Ilustración 15 se muestra el diagrama de flujo para el nivel de servidores y estaciones.

Ilustración 15 : Flujograma del nivel de servidores y estaciones.



Fuente: Propia

3.3.4 Diseño del nivel de aplicación.

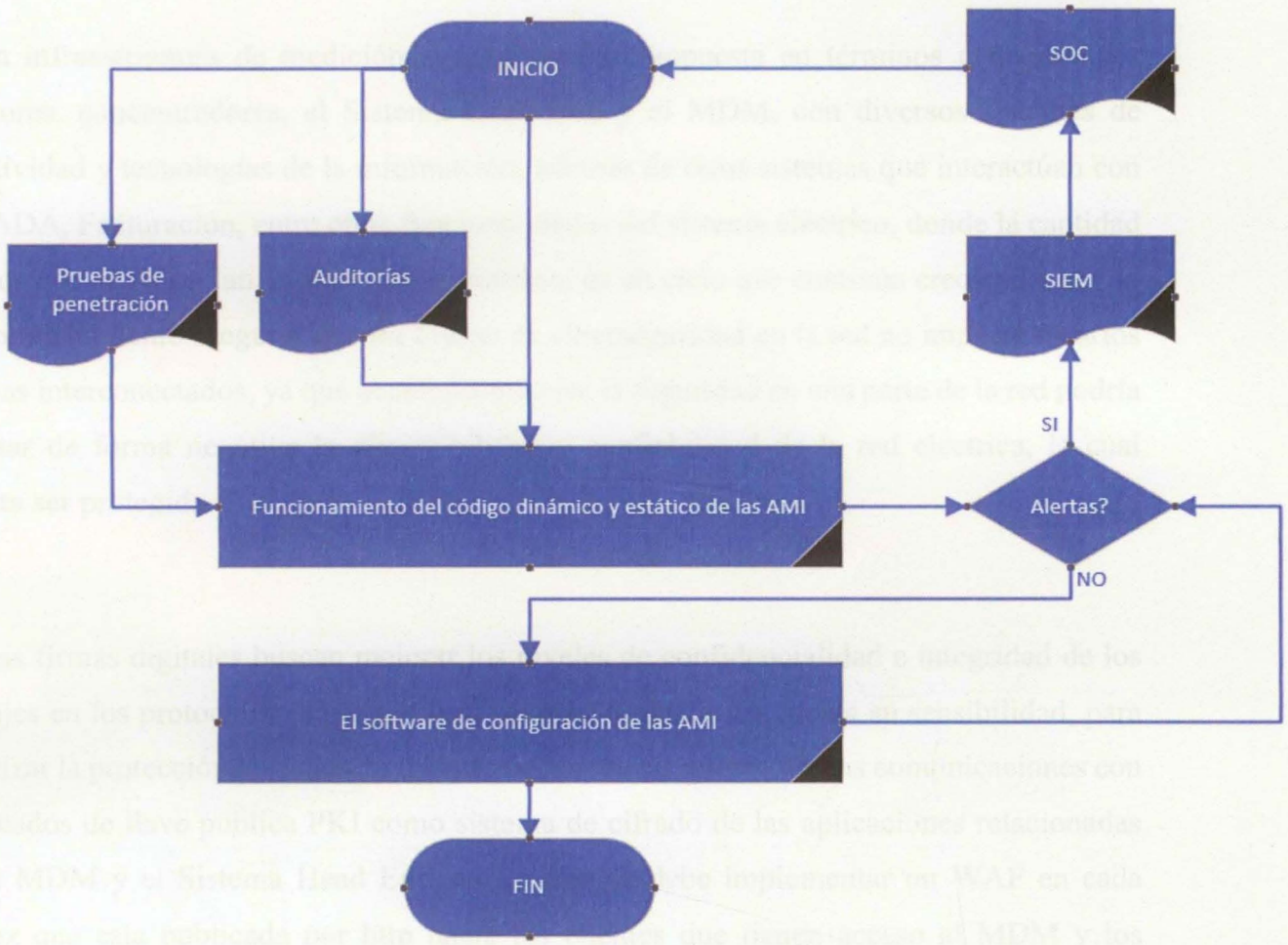
Las vulnerabilidades del software que está involucrado con la infraestructura de medición avanzada son brechas de software que exponen debilidades de la disponibilidad, integridad y confidencialidad del sistema, por lo que se convierte en un componente necesario de la gestión de la infraestructura de medición avanzada. Para mejorar la

protección, se propone auditorías y activadores de alertas, que notifican a los administradores sobre actividades sospechosas, priorizando el orden en el que se investigan los tipos de alertas, particularmente en la infraestructura propuesta.

Las pruebas de penetración ayudan a encontrar fallas de seguridad en las aplicaciones y mantenerlas con mejores niveles seguridad, por lo anteriormente expresado, en las aplicaciones, el código dinámico y estático relacionadas con la infraestructura de medición avanzada se deben realizar pruebas de penetración para evitar la materialización de riesgos potenciales (Zura, A. Y., 2015), debido a que día a día, se descubren nuevas vulnerabilidades de día cero y la responsabilidad de la empresas de energía eléctrica en Colombia es tener una buena supervisión. Las pruebas de penetración no solo se limitan a las aplicaciones, sino que también se realizan en medidores, concentradores, equipos de redes, sistemas informáticos, etc, (Suarez, D. E., 2016).

El software de configuración es crítico en los medidores y concentradores, en este se debe controlar las características funcionales de como administra los datos, los almacena y los transmite, ya que deben ser protegidos contra la afectación intencional o accidental, así mismo, se debe tener evidencia de una intervención autorizada o no autorizada al software, también, se debe integrar funcionalidades de seguridad en los datos para protegerlos de corrupción, fraude o manipulación y acceso no autorizado, todas la características anteriormente mencionadas permiten tener control de acceso y operación de los medidores y los concentradores, además de un sistema de cifrado para evitar el robo de contraseñas y datos en reposo (EPSA, 2018), en la Ilustración 16 se muestra el diagrama de flujo para el nivel de aplicación.

Ilustración 16 : Flujograma del nivel de aplicación.



Fuente: Propia

Los tomadores de decisiones en empresas de energía eléctrica colombianas, involucrados en el proceso de administración de parches enfocados en la infraestructura de medición deben definir una adecuada priorización de parches, maximizando los beneficios de los recursos disponibles al abordar primero los ciberactivos más críticos y, por lo tanto, minimizar el riesgo inherente de manera efectiva a las brechas de seguridad que estén en los medidores y concentradores (Rico, I. E., 2015).

3.3.5 Diseño del nivel de datos.

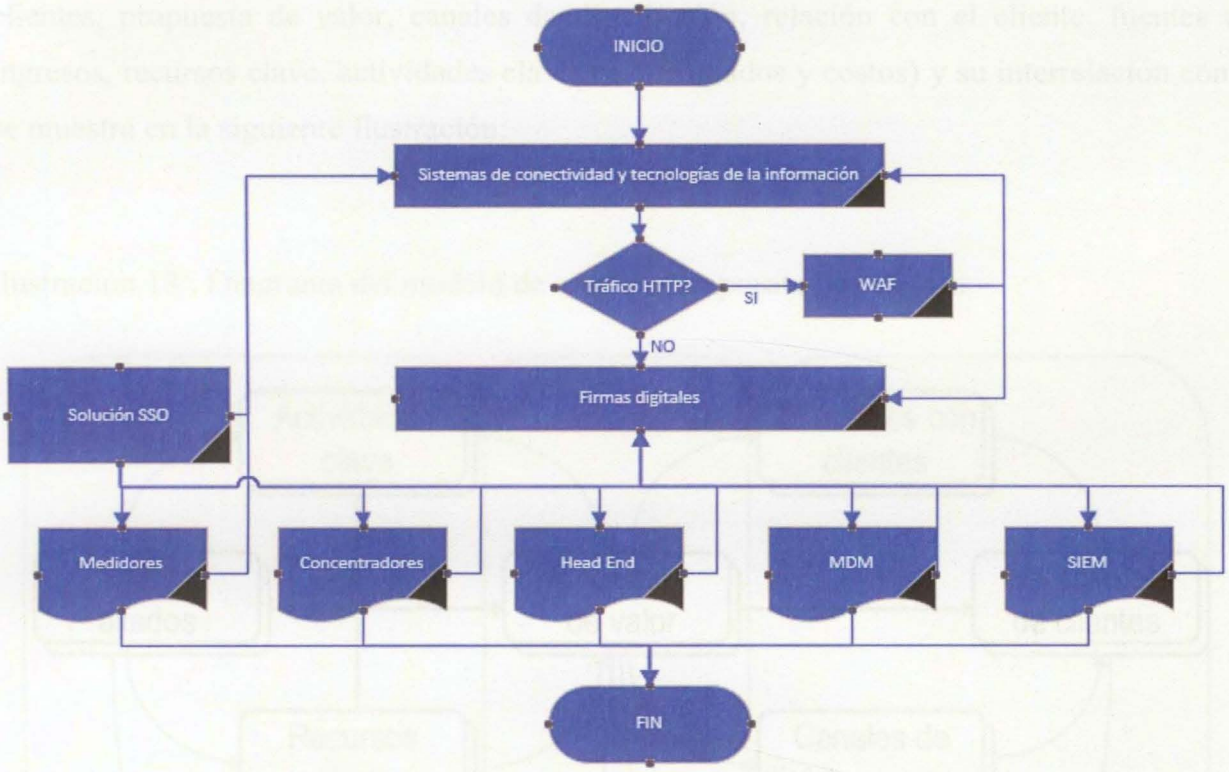
La infraestructura de medición avanzada está compuesta en términos generales por medidores, concentradores, el Sistema Head End y el MDM, con diversos sistemas de conectividad y tecnologías de la información, además de otros sistemas que interactúan con el SCADA, Facturación, entre otras funcionalidades del sistema eléctrico, donde la cantidad de datos que se recopilan, almacenan y procesan, es un ciclo que continúa creciendo, por lo anterior es prudente asegurar que un evento de ciberseguridad en la red no impacte a varios sistemas interconectados, ya que al comprometerse la seguridad en una parte de la red podría impactar de forma negativa la disponibilidad y confiabilidad de la red eléctrica, la cual necesita ser protegida.

Las firmas digitales buscan mejorar los niveles de confidencialidad e integridad de los mensajes en los protocolos criptográficos, además, teniendo en cuenta su sensibilidad, para garantizar la protección los datos en tránsito se propone implementar las comunicaciones con certificados de llave pública PKI como sistema de cifrado de las aplicaciones relacionadas con el MDM y el Sistema Head End, así mismo se debe implementar un WAF en cada interfaz que esta publicada por http hacia los clientes que tienen acceso al MDM y los sistemas Head End.

Se propone implementar sistemas de autenticación para tener el control de los usuarios, el cual permita una administración de los usuarios privilegios para la administración y operación en los recursos tecnológicos , desarrollando una solución SSO por medio de un repositorio único y común de usuarios orientados en la operación y mantenimiento de la infraestructura operativa, utilizándolo para intercambiar datos de autenticación y autorización en los usuarios según el nivel de privilegios en los dispositivos, de modo que la seguridad de SSO se pueda verificar de principio a fin, donde se supervise y controle las actividades de administración que se realizan en el ciberespacio (Scott, C.; Wynne, D., &

Boonthum, C, 2016), en la Ilustración 17 se muestra el diagrama de flujo para el nivel de datos.

Ilustración 17 : Flujograma del nivel de datos.



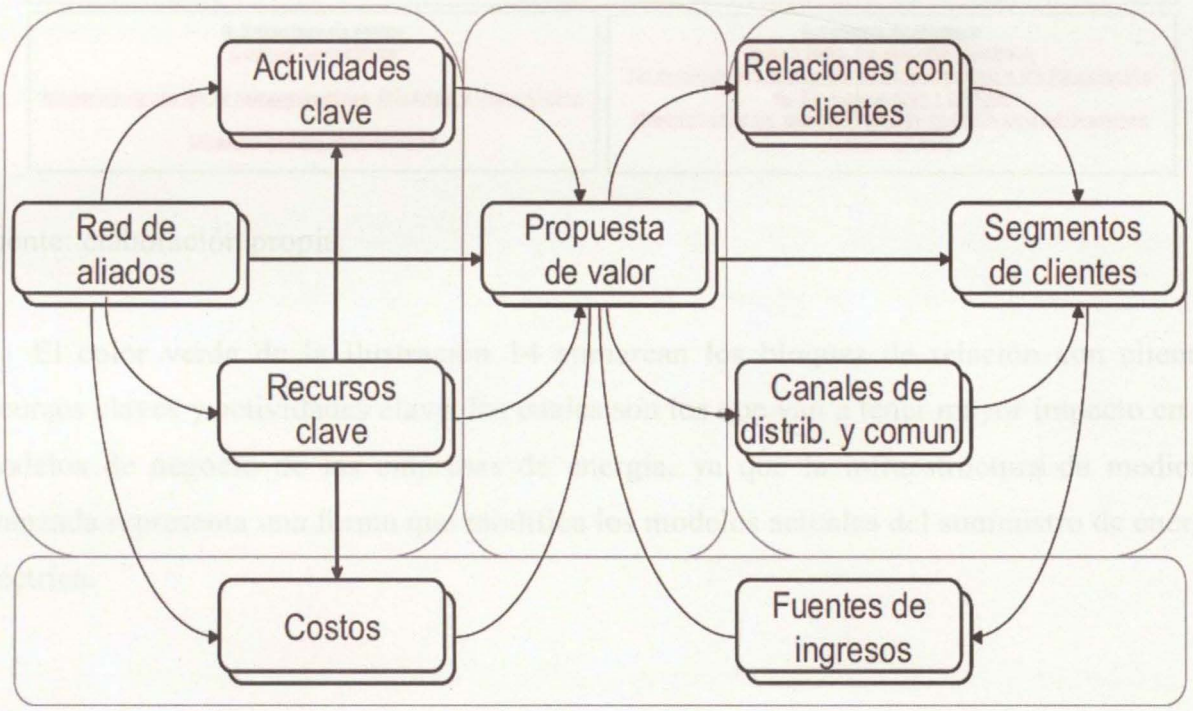
Fuente: Propia

3.4 Impacto de la infraestructura de medición avanzada en el modelo de negocio de las empresas de energía eléctrica en Colombia

Una forma metódica de llevar a cabo las actitudes emprendedoras es por medio del diseño de un modelo de negocio, en el cual se representa tanto la estructura holística para un producto o servicio como sus flujos de información, que tenga en cuenta la interacción de los diferentes actores involucrados en el negocio, al igual que sus roles y la descripción de las fuentes de ingresos y de los beneficios potenciales para cada uno de ellos (Timmers, 2000).

Por otro lado, y teniendo en que lo que expresan Osterwalder y Pigneur (2010), donde un modelo de negocios es la descripción lógica de cómo una organización crea, entrega, y captura valor, así mismo, Osterwalder y Pigneur también desarrollaron la formulación de un modelo de negocio conocidos como Canvas, el cual se basa en 9 bloques (segmentos de clientes, propuesta de valor, canales de distribución, relación con el cliente, fuentes de ingresos, recursos clave, actividades clave, red de aliados y costos) y su interrelación como se muestra en la siguiente Ilustración:

Ilustración 18 : Diagrama del modelo de negocio propuesto por Canvas

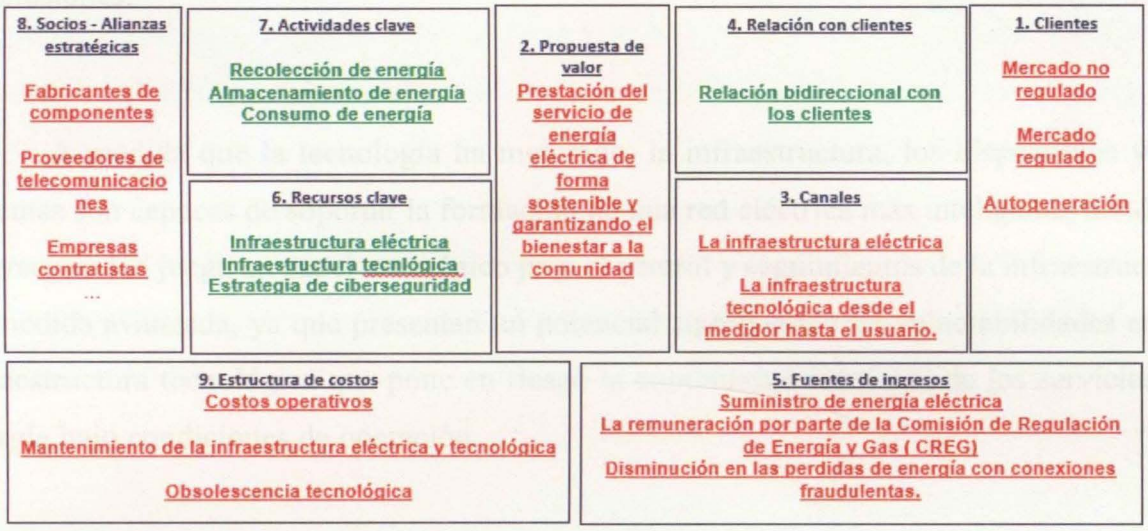


Fuente: elaboración propia, a partir de Osterwalder y Pigneur (2010)

Tomando como referencia la metodología anteriormente expuesta, estableciendo el impacto en cada uno de sus componentes, donde se muestra en la Ilustración 19 un modelo canvas enfocado en el servicio de medición avanzada para las empresas de energía eléctrica

colombianas, para lo cual, la disponibilidad, integridad y confidencialidad de la operación forman parte transversal del modelo de negocio de las empresas de energía eléctricas.

Ilustración 19 : Canvas del AMI para las empresas de energía eléctrica colombianas



Fuente: elaboración propia.

El color verde de la Ilustración 14 enmarcan los bloques de relación con clientes, recursos claves y actividades clave, los cuales son los que van a tener mayor impacto en los modelos de negocio de las empresas de energía, ya que la infraestructura de medición avanzada representa una forma que modifica los modelos actuales del suministro de energía eléctrica.

CONCLUSIONES

Con base en la información y reflexión de la monografía, el presente trabajo de investigación logró diseñar una estrategia de defensa en profundidad para la infraestructura para medición avanzada de la energía eléctrica en Colombia, donde se llegó a las siguientes conclusiones:

A medida que la tecnología ha mejorado, la infraestructura, los dispositivos y los sistemas son capaces de soportar la formación de una red eléctrica más inteligente, donde la ciberseguridad juega un papel estratégico para el control y seguimientos de la infraestructura de medida avanzada, ya que presentan un potencial significativo de vulnerabilidades en su infraestructura tecnológica que pone en riesgo la continuidad funcional de los servicios de energía bajo condiciones de operación.

La monografía presenta la exploración de referencia documentales sobre la infraestructura de medición avanzada de energía eléctrica en Colombia, así mismo, se desarrolla la red eléctrica inteligente de Colombia, que contiene la implementación de la medición inteligente a través de una infraestructura de medición avanzada, la cual debe planificarse cuidadosamente sobre el ciberespacio del servicio de energía eléctrica, asegurando una buena adaptación de la tecnología a lo largo de su vida útil.

En este trabajo de grado se identifican arquitecturas, dispositivos y protocolos, los cuales son claves para una estrategia de ciberseguridad, la cual permite adaptarse dinámicamente al entorno de un ciberespacio cambiante por medio de una estrategia por capas conocida como defensa en profundidad.

La estrategia de ciberseguridad propuesta en el presente trabajo de grado formula una estrategia de defensa en profundidad para la infraestructura de medición avanzada de energía

eléctrica en Colombia, eliminando o mitigando diferentes amenazas por medio de un modelo por capas de diferentes infraestructuras y protocolos altamente maduros y difundidos en el mercado para lograr la interoperabilidad que las normas vigentes exigen.

Por otro lado, como continuación de la presente monografía quedan distintas líneas futuras de investigación que se dejan abiertas y en las que es prudente continuar trabajando; algunas de ellas, es la implementación de la estrategia de ciberseguridad planteada en el desarrollo del trabajo de grado, por otro lado, las redes eléctricas inteligentes tienen otros elementos que la componen a diferencia de la infraestructura de medición avanzada y sería interesante investigar sobre movilidad eléctrica, sincrofasores o autogenerados, por último, una investigación futura puede ser investigar sobre otras estrategias de ciberseguridad diferentes a defensa en profundidad.

REFERENCIAS BIBLIOGRÁFICAS

Abercrombie, R. K., Schlicher, B. G., Sheldon, F. T., (2014). Security Analysis of Selected AMI Failure Scenarios Using Agent Based Game Theoretic Simulation. 47th Hawaii International Conference on System Science, 978-1-4799-2504-9.

Aitel, D. (2013). Cybersecurity Essentials for Electric Operators. The Electricity Journal, 26(1), 52–58. doi:10.1016/j.tej.2012.11.014.

Andrade, C. A. D., & Hernández, J. C. (2011). Smart Grid: Las TICs y la modernización de las redes de energía eléctrica–Estado del Arte. Sistemas & Telemática, 9(18), 53-81.

Assante, M. J., & Lee, R. L., (2015). The Industrial Control System Cyber Kill Chain. SANS Institute Reading Room

Brito, J. (2015). Diseño de una red switching redundante para la provisión de servicios ethernet sobre la red de transporte de CELEC EP – TRANSELECTRIC. Universidad de la Fuerzas Armadas ESPE, Sangolqui, Ecuador.

Boal, J., & Larrauri, M. (2011). Comunicaciones Industriales Avanzadas. Universidad Pontificia Comillas, Escuela Tecnica Superior de Ingenieria (ICAI).

Byres, E., & Lowe, J. (2004). The myths and facts behind cyber security risks for industrial control systems. Proceedings of the VDE Kongress 116, 213-218.

Chen, M., Miao, Y., Jian, X., Wang, X., Humar, I. (2018). Cognitive-LPWAN: Towards Intelligent Wireless Services in Hybrid Low Power Wide Area Networks. IEEE Transactions On Green Communication And Networking.

Chris, K. (2004). Advanced Metering Infrastructure AMI Overview of System Features and Capabilities. eMeter Corporation.

Clincy, V. & Shahriar, H. (2018). Web Application Firewall: Network Security Models and Configuration. 2018 42nd IEEE International Conference on Computer Software & Applications.

Cleveland, F. M. (2008). Cyber security issues for advanced metering infrasttructure (AMI). In Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, IEEE. 1-5.

CREG, (2018) Circular 054. Comisión de Regulación de Regulación de Energía y Gas.

Enrique, S., Gary, R., Le,T., & Xiaoming, F., (2010). Getting Smart. IEEE Power & Energy Magazine, vol. 8, num. 2, pp. 41-48.

EPSA, (2018). Norma técnica de medición y acometidas. Gerencia de distribución. Recuperado 14 de Mayo,2019.

ETEK, (2019). Framework para el desarrollo de una Arquitectura de Seguridad. [Diapositivas de PowerPoint]. Recuperado 23 de Agosto, 2019.

Fornero, F. (2019). Extending your BusinessNetwork through a Virtual Private Network (VPN). SANS Institute Reading Room site

Galarza, D. I., (2017). Estudio y diseño de una infraestructura de medición avanzada ami para la empresa eléctrica quito. Tesis Pregrado. Universidad de la Fuerzas Armadas.

García, L. E., Pedraza, L. F., & Parra, O. S. (2013). Estado del arte mpls-tp conmutación multiprotocolo mediante etiquetas - perfil de transporte. Revista Electrónica Redes De Ingeniería, 449-65.

Gibson, W., (1984), Neuromante.

Giral , W. M., Celedón H. J., Galvis, E.,Zona, A., (2017). Redes inteligentes en el sistema eléctrico colombiano: revisión de tema. Revista Tecnura, 21(53), 119-137, doi: 10.14483/22487638.12396

Gómez, V. A., Hernández, C., & Rivas, E, (2018). Visión General, Características y Funcionalidades de la Red Eléctrica Inteligente (Smart Grid). Información Tecnológica, 29(2), 89-102..

Gresset, E. (2016). TECH FOCUS: IoT Protocols For The Wide-Area IoT. ECN: Electronic Component News, 60 (9), 26-28.

Guijarro, A. A., Yepes Holguin, J. M., Peralta Guaraca, T, J & Ortiz Zambrano, C. (2018). Defensa en profundidad aplicado a un entorno empresarial. Espacios, 39(42), 19-27

Gutierrez, M., (2011). Estudio para la implementación del sistema de infraestructura de medición avanzada (AMI) en la empresa eléctrica Regional Centro Sur(tesis de pregrado). Universidad Politécnica Salesiana, Cuenca, Ecuador.

Hébert, C. (2013). The Most Critical of Economic Needs (Risks): A Quick Look at Cybersecurity and the Electric Grid. The Electricity Journal, 26(5), 15–19. doi:10.1016/j.tej.2013.05.009.

Huandong, W., Yong, L., Yang, C., Yue, W.; Jian, Y. & Depeng, J. (2016). Co-location social networks: Linking the physical world and cyberspace. IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), 295 – 298.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M., (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research, vol. 1, 2011.

International Telecommunication Union, (2011). Deliverable on Requirements of communication for smart grid, pp. 1{81, 2011.

Jiang, N., & Zhenyu, H. L. (2017). Research of Paired Industrial Firewalls in Defense-inDepth Architecture of Integrated Manufacturing or Production System. Proceedings of the 2017 IEEEInternational Conference on Information and Automation (ICIA) Macau SAR, China, July 2017

Kozik, R. & Choras, M. (2019). Improving Web Application Firewalls through Anomaly Detection. Proceedings - 17th IEEE International Conference on Machine Learning and Applications, ICMLA 2018 8614149, pp. 779-784

Lee, G. M., Crespi, N., Choi J. K., & Boussard, M., (2013). Internet of things security guidelines (p.p. 257-282). IoT Alliance Australia. https://doi.org/10.1007/978-3-642-41569-2_13

Leiva, E. (2015). Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. Revista Latinoamericana de Ingenieria de Software, 3(4), 161-176.

Li, F., Li Z., Han, W., Wu, T., Chen, L., Guo, Y. & Chen, J (2018). Cyberspace-Oriented Access Control: A Cyberspace Characteristics based Model and its Policies. IEEE Internet of Things Journal, Year:, (Early Access), Pages: 1 – 1

Li, Z., Shahidehpour, M., & Aminifar, F, (2017). Cybersecurity in distributed power systems. Proceedings of the IEEE 105 (7), 1367-1388

McGuiness, T., (2019). Defense In Depth. SANS Institute Informaction Security Reading Room

Miller, R. (2016). LoRa securit: building a secure LoRa solution. MWR Labs Whitepaper. MWR Labs Whitepaper.

Ministerio de Tecnologías de Información y las Comunicaciones [MinTic], (2014). Agenda Estratégica de Innovación: Ciberseguridad. Recuperado el 29 de marzo del 2019 de mantic: https://www.mintic.gov.co/portal/604/articles-6120_recurso_2.pdf

Mokalled, H., Catelli, R., & Casola, V., (2019). The applicability of a SIEM solution: Requirements and Evaluation. 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)

Moreira, N., Molina, E., Lázaro, J., Jacob, E., & Astarloa, A. (2016). Cyber-security in substation automation systems. Renewable and Sustainable Energy Reviews, 54, 1552–1562. doi:10.1016/j.rser.2015.10.124.

NIST, 2014. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0. Recuperado el 29 de junio de 2019. http://www.nist.gov/smartgrid/upload/NIST-SP-1108r3.pdf

Ostewalder, A., y Pigneur, Y. (2010). Business Model Generation.Amsterdam. A Handbook for visionaries, game changers, and challengers.

Ottis, R. & Lorents, P. (2010). Cyberspace: Definition and Implications. In Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April. Reading: Academic Publishing Limited, pp 267-270.

Pilipovic, D., 1998. Energy risk: valuing and managing energy derivates. New York: Mc-Graw Hill.

Puthal, D., Mohanty, S. P., Nanda, P.& Choppali, U, (2017), Building Security Perimeters to Protect Network Systems Against Cyber Threats. IEEE Consumer Electronics Magazine, Volume: 6, Issue: 4. 24 – 27

Rawat, D.B., Bajracharya, C. (2015), Cyber security for smart grid systems: Status, challenges and perspectives. In: SoutheastCon 2015, Fort Lauderdale, FL, pp. 1–6

Raza, U., Kulkarni, P, & Sooriyabandara, M. (2017). Low Power Wide Area Networks: An Overview. IEEE Communications Surveys & Tutorials, VOL. 19(2), 855-872.

Rico, I. E., (2015). Defensa en profundidad basada en servidores. Bogotá: Universidad Piloto de Colombia.

Ruiz, M.G., (2016). Diseño de un sistema hibrido inalámbrico-fibra para transmisión de datos de medidores inteligentes de energía en redes Smart Grid (tesis de maestría). Pontificia Universidad Católica del Ecuador, Quito, Ecuador

SANS Institute, (2003). Global Information Assurance Certification Paper. GIAC Certification.

Scott, C.; Wynne, D., & Boonthum, C (2016). Examining the Privacy of Login Credentials Using Web-Based Single Sign-On: Are We Giving up Security and Privacy for Convenience?. IEEE. Cybersecurity Symposium. (CYBERSEC)

Small, P., (2019) Defense in Depth: An Impractical Strategy for a Cyber World. SANS Institute Informaction Security Reading Room

Smith, E., Corzine, S., Racey, D., Dunne P., Hassett, C., & Weiss, J. (2016). Going Beyond Cybersecurity Compliance: What Power and Utility Companies Really Need To Consider. IEEE Power and Energy Magazine, 14, (5), 48-56. doi: 10.1109/MPE.2016.2573898

Suarez, D. E. (2016). Diseño de una arquitectura de red basado en un modelo de defensa en profundidad utilizando estandares de las normas ISO 27000 y COBIT 5.0 (tésis pregrado). Bogotá: Universidad Fransisco José de Caldas

Ten, C. W., Govindarasu, M., & Liu, C. C. (2007). Cybersecurity for electric power control and automation systems. In 2007 IEEE International Conference on Systems, Man and Cybernetics, IEEE. 29-34.

Thakur, M. A., (2019). A Survey of Directory and Database Protocols for Data Extraction. Information and Communication Technology for Sustainable Development pp 315-325

Timmers, P. (2000). Electronic Commerce: Strategies and models for business to business trading. Chichester, England: John Wiley & Sons Inc.

US. Department of Energy, (2012). Electricity subsector cybersecurity. Risk management process.

US.DoD, (2015). Joint Publication 1-02. Dictionary of Military and Associated terms. http://www.dtic.mil. Fecha consulta 03.06.2015.

Viveros, J, (2015). Defensa en profundidad para proteger la información de la red corporativa. Universidad Piloto de Colombia.

Webb, J & Hume, D. (2018). Campus IoT Collaboration and Governance using the NIST Cybersecurity Framework. In Campus IoT collaboration and governance using the NIST cybersecurity framework (pp. 1-7). London, UK: IET

Yu, R., Zhang,Y., Gjessing, S., Yuen, Xie,C. S. & Guizani, M., (2011).Cognitive Radio Based Hierarchical Communications Infrastructure for Smart Grid. IEEE Network, vol. 25,num. 5, pp. 614,

Zhiguo, W., Guilin, W. Yanjiang Yang, & Shenxing, Shi. (2014). SKM: Scalable Key Management for Advanced Metering Infrastructure in Smart Grids. IEEE Transactions on industrial electronics, VOL. 61, NO. 12, 7055 - 7066

Zura, A. Y. (2015). Diseño del modelo de seguridad de defensa en profundidad en los niveles de usuario, red interna y red perimetral, aplicando políticas de seguridad en base a la norma ISO/IEC 27002 para la red de datos del GAD Municipal de Otavalo. (tesis de pregrado). Universidad Técnica del Norte, Ibarra, Ecuador.