Definición de una arquitectura de ciberseguridad para los sistemas de control industrial críticos de empresas de distribución de energía en Colombia

Sandra Milena Granados Correa

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

Definición de una arquitectura de ciberseguridad para los sistemas de control industrial críticos de empresas de distribución de energía en Colombia

Estudiante:

Sandra Milena Granados Correa

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

Definición de una arquitectura de ciberseguridad para los sistemas de control industrial críticos de empresas distribución de energía en Colombia

Director

Dr. Iván Camilo Castellanos

Maestría en Ciberseguridad y Ciberdefensa

Trabajo de grado

Bogotá – Colombia

2020

Agradecimientos

Agradezco a la Escuela Superior de Guerra por permitirme participar en este proceso educativo, y así facilitar la ampliación de conocimientos y visión del mundo de Ciberseguridad.

Adicionalmente agradezco al Ministerio de Tecnologías de la Información y Comunicaciones de Colombia, quién a través de su patrocinio logró hacer de esta meta una realidad.

Finalmente, agradezco a todos mis compañeros, por el apoyo recibido y todos los conocimientos adquiridos.

Dedicatoria

Este trabajo está dedicado a mi familia, quienes a través de los años me han apoyado con mucho amor, en cada uno de los pasos que he decido dar.

Resumen Ejecutivo

En la actualidad las organizaciones no prestan la suficiente atención a la definición de sus arquitecturas empresariales de ciberseguridad, por lo que determinan que definir una topología de red o un modelo de defensa en profundidad es suficiente para garantizar la protección de sus activos o ciberactivos críticos.

En un proceso de definición de una arquitectura de ciberseguridad para sistemas de control industrial o ICS, es importante conocer las necesidades y capacidades que se deben desarrollar, pero enmarcando estas necesidades en los riesgos a los que se expone la organización y con una visión de arquitectura empresarial, que permita realmente definir modelos adecuados que sirvan como base para el desarrollo de dichas capacidades en ciberseguridad.

Este trabajo es el resultado de la investigación realizada para obtener la información previa en el ámbito académico y de industria frente al diseño, análisis y modelamiento de arquitecturas empresariales de ciberseguridad para sistemas de control industrial, basadas en drivers de negocio.

Inicialmente se desarrollan los conceptos relevantes tales como frameworks, que permiten enmarcar las arquitecturas empresariales de ciberseguridad.

Luego se realizó una identificación de los elementos críticos relacionados con las empresas de distribución de energía, incluidas las personas, los procesos y las tecnologías. Este trabajo se basó en modelos genéricos de la industria.

Finalmente, se presenta una definición de requerimientos y drivers de negocio, legislación asociada a Ciberseguridad para empresas de distribución de energía en Colombia, y una

definición de riesgos asociado a infraestructuras críticas; todos estos elementos integrados mediante la aplicación del modelo de arquitectura SABSA, que es un marco y una metodología para la arquitectura de seguridad empresarial y la gestión de servicios, permiten concluir con la definición de una propuesta de arquitectura de ciberseguridad aplicado a empresas de distribución de energía.

Abstract

Nowadays, organizations do not pay enough attention to the definition of their cybersecurity business architectures, so they determine that defining a network topology or a depth defense model is enough to guarantee the protection of their critical assets or cyber-assets.

In a process of defining a cybersecurity business architecture for industrial control systems or ICS, it is important to know the needs and capabilities that must be developed, but articulating these needs according to the risks to which the organization is exposed, and integrating the vision of business architecture that really allows to define suitable models that serve as a basis for the development of capacities in cybersecurity.

This work is the result of investigation to obtain the previous information in the academic and industry field about the design, analysis and modeling of cybersecurity business architecture for industrial control systems, based on business drivers.

Initially, relevant concepts such as frameworks are developed, which allow framing cybersecurity business architectures.

Then an identification of the critical elements related to energy distribution companies including people, processes and technologies was made. This work was based in generic industry models.

Finally, a definition of business requirements and controllers, legislation associated with Cybersecurity for energy distribution companies in Colombia, and a definition of risks associated with critical infrastructure are presented; All these elements integrated through the application of the SABSA architecture model, which is a framework and methodology for enterprise security architecture and service management, may conclude with the definition of a proposed cybersecurity architecture applied to energy distribution companies.

CONTENIDO

Lista de Gráficos X

Lista de Tablas XII

Lista de Abreviaturas XIII

Introducción 15

Metodología 19

Capítulo I. Conceptos Relevantes y Mejores Prácticas en Arquitecturas de Ciberseguridad 21

1. Entorno ICS Energía – Definición y Modelos de Arquitectura 25
2. Arquitecturas y Frameworks de Ciberseguridad para ICS 32

Capítulo II. Identificación de Procesos, Personas y Tecnologías Relacionados con Empresas de Distribución de Energía 41

1. Procesos 42
2. Personas 45
3. Tecnologías 47

Capítulo III. Drivers de negocio, Legislación y Riesgos Asociados a Ciberactivos en las Empresas de Distribución de Energía 55

1. Requerimientos, Drivers de Negocio y Atributos de Ciberseguridad 56
2. Legislación aplicable 68
3. Flujos de información o Flujos de Bits 79
4. Escenarios de Riesgo 81

Capítulo IV. Modelo de Arquitectura de Ciberseguridad Enfocado en Infraestructuras Críticas de Empresas de Distribución de Energía 87

1. Principios de arquitectura usados para este modelo 87

2. Matriz de hallazgos y controles por cada capa 91

3. Priorización de Iniciativas 128

Conclusiones 137

Recomendación 139

Referencias 140

Lista de Gráficos

Ilustración 1:Transmission and Distribution Grid Structure within the Power Industry.[Estructura de la red de transmisión y distribución en la industria de energía]. Merchant & Thompson, 2010 25
Ilustración 2: A general architecture of a SCADA network based on remote substations. [Arquitectura general de un Sistema SCADA basada en subestaciones remotas]. (Alcaraz & Zeadally, 2014) 27
Ilustración 3: The ISA-95 architecture. [Arquitectura ISA]. Jiang, 2017 28
Ilustración 4: Purdue Model for Control Hierarchy logical framework.[Modelo Purdue para un modelo lógico jerárquico de control] Obregon,2015 29
Ilustración 5: ICS Security Reference Architecture. [Arquitectura de referencia de seguridad para ICS] (Ku et al., 2017) 33
Ilustración 6: IT/OT Architecture. [Arquitectura TI/TO]. (Challenges, 2018). 34
Ilustración 7. Modified Purdue Model for Control Hierarchy Architecture. [Arquitectura modificada del modelo de Purdue para control jerárquico]. (Obregon, 2015). 36
Ilustración 8. Modelo de referencia para el estándar IEC 62443. (International Electrotechnical Commission, 2009) 37
Ilustración 9. Ejemplo de conductos y zonas.(International Electrotechnical Commission, 2009) 39
Ilustración 10. Vistas del modelo SABSA. (Sherwood et al., 2005) 39
Ilustración 11. Direccionadores de la arquitectura (nivel estratégico). Elaboración propia. 41
Ilustración 12. Factores de riesgo e impacto en el modelo de negocio. (Cano, 2013) 41
Ilustración 13. Proceso General del sistema de distribución de energía. Elaboración propia 43
Ilustración 14. Proceso de Operación del sistema de distribución de energía. Elaboración propia 44
Ilustración 15. Proceso de Mantenimiento del sistema de distribución de energía. Elaboración propia 45

Ilustración 16. Componentes de un SCADA para un sistema de Distribución de Energía. (Siemens, 2014) 47
Ilustración 17. Arquitectura ICS modelo para subestaciones de energía. Elaboración propia 50
Ilustración 18. Direccionadores de arquitectura. Nivel estratégico y táctico + ciberseguridad. Elaboración propia 55
Ilustración 19. Flujos de información para un sistema de distribución de energía. Ilustración propia basada en (Dan, Sandberg, Bj, & Ekstedt, 2012). 79
Ilustración 20. Modelo de arquitectura de Ciberseguridad. Elaboración propia 87
Ilustración 21 Modelo de defensa en profundidad. Traducción del modelo de defensa en profundidad, tomado de la SANS. (SANS, 2015) 89
Ilustración 22. Priorización de iniciativas de Ciberseguridad 134

Lista de Tablas

Tabla 1. RACI Operación del sistema de distribución 46
Tabla 2. RACI Mantenimiento del sistema de distribución 46
Tabla 3. Requerimientos de Negocio para una empresa de distribución de energía 57
Tabla 4. Drivers de negocio para una empresa de distribución de energía 58
Tabla 5. Asociación de los drivers de negocio con Atributos de seguridad. Elaboración propia 61
Tabla 6 Integración de la legislación en Ciberseguridad para los sectores de infraestructuras críticas nacionales 71
Tabla 7. Fuentes de amenazas para un sistema de distribución de energía. 82
Tabla 8. Escenarios de riesgos para un sistema de distribución de energía 84
Tabla 9. Modelo de defensa en profundidad. Elementos de la estrategia 89
Tabla 10. Matriz de integración 92
Tabla 11. Matriz de hallazgos 113
Tabla 12. Matriz de priorización de iniciativas 130
Tabla 13. Orden de Implementación de iniciativas 135

Lista de Abreviaturas

AE: Arquitectura Empresarial

DHCP: Dynamic Host Configuration Protocol. Protocolo de configuración dinámica de host

DMZ: Demilitarized zone. Zona desmilitarizada

DNA: Distribution Network Application. Aplicaciones para la red de distribución.

DNS: Domain name server. Servidor de nombres de dominio.

DMS: Distribution Management System. Sistema de gestión de distribución.

HIS (Historian): Base de datos histórica.

HMI: Human Machine interface. Interfaces hombre-máquina (IHM)

ICS: Industrial Control Systems. Sistema de control industrial

ICCP: Inter-control Center Communications. Protocolo de comunicación entre centros de control.

IDS: Intrusion detection system. Sistema de detección de intrusos

OM – OMS: Outage Management System: Sistema para gestión de interrupciones

PLC: Controladores lógicos programables

RBAC: Role based Access control. Control de acceso basado en roles

RTU: Remote terminal unit. Unidad terminal remota

SCADA: Supervisory Control and Data Acquisition. Sistemas de supervisión de control y adquisición de datos

TI: Technology information. Tecnología de la información

TO: Technology operation. Tecnología de la operación

UI: User interface. Servidores de interfaz de usuario de SCADA

VPN: Virtual private network

Introducción

Los sistemas de control industrial (ICS por sus siglas en inglés: Industrial Control System) son los sistemas dedicados al control y monitoreo de sistemas electrónicos y eléctricos de un proceso industrial o servicios esenciales para la sociedad, y son llamados infraestructuras críticas si dichos servicios son indispensables para el funcionamiento de un país. (Bolívar, 2016).

El objetivo de un atacante en relación con los Sistemas de Control Industrial se encuentra orientado a lograr la pérdida de la supervisión y del control, o a la manipulación de los sensores e instrumentos en campo. (Bolívar, 2016)

En relación con los ICS, al manipular un controlador, un atacante puede modificar las señales de control enviadas a los actuadores. El gusano Stuxnet es un excelente ejemplo de un ataque a un controlador, en el cual se manipuló el código de configuración de un dispositivo de lógica programable para enviar comandos maliciosos a convertidores de frecuencia que directamente controlaron los rotores de una centrífuga. (Hahn et al., 2015). De igual forma, el ataque Aurora demostró que los generadores de energía eléctrica podrían sufrir daños físicos si su control de frecuencia no está sincronizado con el control de frecuencia de la red eléctrica. (Hahn, Thomas, Lozano, & Cardenas, 2015)

Lo anterior nos demuestra que la gran la mayoría de las infraestructuras críticas actualmente desplegadas en nuestra sociedad, dependen de sistemas de información para la gestión de información sensible. Esto significa que un evento no planificado sobre las infraestructuras cibernéticas puede conducir a graves consecuencias que pueden afectar el rendimiento, la confiabilidad y la seguridad crítica del sistema subyacente. (Alcaraz & Zeadally, 2014).

Por otro lado, la Arquitectura Empresarial (AE) se concibe hoy en día, como una actividad esencial de gestión para visualizar y evaluar la dirección futura de una organización u compañía. (Cáceres & Zea, 2014). Enmarcado en este concepto se encuentra la definición de la arquitectura de ciberseguridad empresarial.

Mientras la dimensión estratégica cobija a toda una organización y es un medio para alcanzar objetivos empresariales, las dimensiones táctica y operativa se orientan al mediano o corto plazo y buscan alcanzar metas inmediatas o resultados específicos.

En este sentido, la definición de una arquitectura de ciberseguridad empresarial permite desarrollar el concepto de alineación con la dimensión estratégica, integrando las necesidades de negocio con las tecnologías de información de una organización; su principal foco es el cumplimiento de las políticas de seguridad sin que sea vista como un factor de prohibición y su propósito fundamental es proteger el valor de la información generada desde los activos y ciberactivos críticos de una organización. (Flórez, Calvo, & Parada, 2011)

Sin embargo, la experiencia común en muchas organizaciones es que las soluciones de seguridad de la información y ciberseguridad a menudo se diseñan, adquieren e instalan tomando como base una dimensión táctica (por ejemplo a partir de diseños topológicos). En este proceso no hay oportunidad de considerar la dimensión estratégica lo que genera una mezcla de soluciones técnicas sobre una base ad hoc, cada una diseñada y especificada independientemente y sin garantía de que sean compatibles e interoperables en el tiempo. A menudo no hay un análisis de los costos a largo plazo y no existe una estrategia clara que esté siendo apoyada al tomar tales decisiones. (OpenGroup, 2011)

Adicionalmente, tanto como avanzan las tecnologías, las arquitecturas deben evolucionar y por lo tanto las organizaciones deben implementar nuevos servicios y capacidades,

incluidos los servicios mejorados de seguridad y capacidades de respuesta a nuevas amenazas, protegiéndose así de una manera ágil y oportuna. (OAS - Microsoft, 2018).

Tomando como base la necesidad de definición de una arquitectura de Ciberseguridad empresarial, surge la siguiente **pregunta de investigación**:

¿Cuál es el modelo de arquitectura de ciberseguridad adecuado para infraestructuras críticas pertenecientes a las empresas de distribución de energía?

Teniendo en cuenta la pregunta de investigación definida, la importancia de la adecuada definición de una arquitectura de ciberseguridad, y considerando que actualmente las empresas de distribución de energía no cuentan una arquitectura que logre direccionar de una manera adecuada los esfuerzos en ciberseguridad, se propone como **objetivo general** de este trabajo:

- **Proponer un modelo de arquitectura de ciberseguridad adecuado para infraestructuras críticas pertenecientes a las empresas de transmisión y distribución de energía.**

Para la realización de este trabajo y lograr el objetivo general planteado se desarrollaron los siguientes **objetivos específicos:**

- Establecer el estado del arte y las mejores prácticas en arquitecturas de ciberseguridad aplicables a empresas del sector eléctrico

- Identificar ciberactivos críticos pertenecientes a las empresas de transmisión y distribución de energía integrando personas, procesos y tecnologías relevantes.
- Analizar el estado actual y los riesgos asociados a los ciberactivos críticos que requieren ser protegidos por las empresas de transmisión y distribución de energía identificando requerimientos de negocio, flujos de información relevantes y legislación colombiana aplicable.
- Definir un modelo de arquitectura de ciberseguridad enfocado en la infraestructura crítica de las empresas de transmisión y distribución de energía.

Cada uno de estos objetivos es desarrollado a continuación como un capítulo, para finalmente, presentar una propuesta de arquitectura de ciberseguridad empresarial aplicada a empresas de distribución de energía en Colombia. El desarrollo de esta trabajo permitirá por lo tanto, direccionar los esfuerzos que se realicen en relación con la ciberseguridad, definir capacidades de ciberseguridad que orienten la toma de decisiones, generar marcos de referencia que direccionen la adquisición o implementación de nuevas soluciones y orientar el desarrollo unificado de la estrategia de Ciberseguridad empresarial.

Metodología

Como base del marco metodológico se utilizará un enfoque de investigación cuantitativa con un alcance descriptivo principalmente. Los estudios descriptivos miden, evalúan o recolectan datos sobre diversos conceptos (variables), aspectos, dimensiones o componentes del fenómeno a investigar. En un estudio descriptivo se selecciona una serie de cuestiones y se mide o recolecta información sobre cada una de ellas, para así (valga la redundancia) describir lo que se investiga. (Hernandez Sampieri, Fernandez Collado, & Baptista Lucio, 2010).

Como base del marco teórico se utilizará la metodología SABSA, la cual se integra con algunos elementos de TOGAF.

TOGAF es un marco de arquitectura que proporciona herramientas para facilitar la definición y mantenimiento de una arquitectura empresarial. El uso de este modelo se basa en un proceso iterativo que es respaldado por el uso de buenas prácticas, y objetos o activos de arquitectura que se definen una vez y luego son reutilizados. (OpenGroup, 2011).

SABSA es una metodología para desarrollar arquitecturas de seguridad empresariales y que permite entregar soluciones de infraestructura de seguridad. Es un estándar abierto, que comprende varios marcos, modelos, métodos y procesos y de uso gratuito. La idea fundamental detrás de SABSA es que la arquitectura de seguridad se crea para facilitar el cumplimento de los requerimientos de negocio lo cual está en línea con los conceptos TOGAF. (OpenGroup, 2011). El uso de SABSA permitirá tener en cuenta tanto los elementos requeridos en una arquitectura de ciberseguridad como la integración y uso del marco de referencia TOGAF en el cual se basa la arquitectura empresarial de muchos grupos empresariales.

Adicionalmente se hizo recolección y análisis de publicaciones de diferentes fuentes de información tales como:

- Publicaciones académicas (IEEE).
- Publicaciones comerciales y patrocinadas (Microsoft, IBM, SANS, TOGAF, Trend Micro, Gartner, entre otros).
- Publicaciones de organizaciones normativas (NIST).

Capítulo I. Conceptos Relevantes y Mejores Prácticas en Arquitecturas de Ciberseguridad

Qué es Ciberseguridad y Qué es una Arquitectura de Ciberseguridad

Concepto de Ciberseguridad

De acuerdo con lo definido por Richard J. Campbell en su artículo "Cybersecurity Issues for the Bulk Power System", la ciberseguridad puede definirse como la seguridad (es decir, protección contra intrusiones externas, corrupción u otros accesos no autorizados) de las redes de operación, computadoras, hardware y sistemas de software para procesos de control industrial y de negocio. (Campbell, 2016).

Adicionalmente, la Unión de Telecomunicaciones (UIT) define la ciberseguridad como 'La colección de herramientas, políticas, conceptos de seguridad, lineamientos, enfoques de gestión de riesgos, acciones, formación, mejores prácticas y tecnologías que puedan ser utilizadas para proteger los activos de la organización. Los activos de la organización incluyen dispositivos informáticos conectados, infraestructura, aplicaciones, servicios, sistemas de telecomunicaciones y la totalidad de la información transmitida y/o almacenada en el ciber-entorno. (Information Systems Audit and Control Association (ISACA), 2015).

Otro concepto relevante es el del Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST), quienes definen el "ciberespacio" como la red interdependiente de infraestructuras de sistemas de información, incluyendo internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores embebidos. Adicionalmente se define "Ataque cibernético" como un ataque orientado al uso del ciberespacio de una empresa con el propósito de interrumpir, deshabilitar, destruir, controlar

maliciosamente un entorno informático o infraestructura, destruir la integridad de los datos, o robo de información. En consecuencia, la ciberseguridad es definida como la capacidad para proteger o defender el uso del ciberespacio de ciberataques. (Information Systems Audit and Control Association (ISACA), 2015).

Para el presente trabajo se usará la definición de la UIT entendiendo la ciberseguridad como la colección de herramientas, políticas, conceptos de seguridad, lineamientos, mejores prácticas y tecnologías que puedan ser utilizadas para proteger los ciberactivos críticos de la organización, y por lo tanto no se incluye la protección de elementos que se encuentren fuera del perímetro de seguridad electrónica de la organización.

De acuerdo con el Comité nacional de operación de Colombia (CNO), los ciberactivos críticos son aquellos que presentan una o más de las siguientes particularidades:

- El ciberactivo usa un protocolo enrutable para comunicarse afuera del perímetro de seguridad electrónica, o,
- El ciberactivo usa un protocolo enrutable con un centro de control

Adicionalmente es importante precisar que el perímetro de seguridad electrónica se define como la frontera lógica y con acceso controlado, que envuelve una red aislada o con conectividad enrutable a otras redes, y dentro de la cual están conectados los ciberactivos críticos. (Consejo Nacional de Operación, 2015).

Arquitecturas de Ciberseguridad

En relación con las arquitecturas de Ciberseguridad, la definición hecha por Rob McMillan y Tom Scholtz en el artículo de Gartner, "Definition: Security Architecture", indica lo siguiente: Arquitectura de Seguridad es un término amplio que casi siempre significa diferentes cosas para diferentes personas, dependiendo del contexto.

Consecuentemente, el alcance o intención de una persona usando el término no es siempre claro para otros interlocutores. (McMillan & Scholtz, 2018)

Adicionalmente existen algunas fuentes de confianza que discuten el significado del término Arquitectura de Seguridad dentro del contexto de una arquitectura empresarial. Entre ellas se encuentra el framework y metodología para arquitecturas de seguridad empresarial y gestión de Servicios llamado Sherwood Applied Business Security Architecture o SABSA.

En relación con la metodología SABSA, y específicamente en el libro "Sherwood, J., Clark, A., and Lynas, D., "Enterprise Security Architecture: A Business-Driven Approach," CRC Press, primera edición, se encuentra la siguiente definición del término en cuestión: "Arquitectura de seguridad es el arte y ciencia de diseñar y supervisar la construcción de sistemas de negocio los cuales deben ser: libres de peligro y daños, libres de miedo y preocupación, en custodia segura, sin probabilidad de que fallen, y libres de ataques." (Sherwood, Clark, & Lynas, 2005).

Otra entidad que define el término de arquitectura de ciberseguridad es "The Open Group". En el documento "Integrating Risk and Security within a TOGAF Enterprise Architecture," se define el término arquitectura de seguridad de la siguiente forma: "Una arquitectura de seguridad es una estructura de componentes organizacionales, conceptuales, lógicos y físicos que interactúan de manera coherente para lograr y mantener un estado de riesgo gestionado. Es un driver de comportamiento seguro, a salvo, resiliente y confiable, y respetando la privacidad en áreas de riesgo de toda la empresa". (The Open Group, 2016).

Finalmente, la National Institute of Standards and Technology (NIST) entrega la siguiente definición: "Es una parte integrada e integral de la arquitectura empresarial que describe la estructura y comportamiento de los procesos de seguridad de una empresa, sistemas de

seguridad de la información, personal y subunidades organizativas, mostrando su alineación con la misión empresarial y planes estratégicos" (Dempsey, White, & Ricke, 2014).

Luego de analizar estas definiciones se observa como elemento común que no existe una única definición en relación con el término en cuestión. También se puede determinar que una arquitectura de empresarial no define el detalle de implementación de un sistema específico; es una metodología que permite en el proceso de estrategia e ingeniería, enmarcar el diseño y asegurar consistencia con la arquitectura empresarial.

Las arquitecturas empresariales incluyen entre algunos factores:

- La necesidad de integración entre los sistemas empresariales disminuyendo costos y tiempos para esta necesidad.
- Tienen en cuenta misión y valor del negocio para la toma de decisiones técnicas que permitan la sostenibilidad del negocio.
- Tendencias en arquitecturas de sistemas distribuido, multisitios, sitios aislados e incluso tendencias de nube.

Todos estos elementos enmarcados en el contexto ciber pueden ser integrados en una definición como la siguiente: una arquitectura de ciberseguridad debe definir conceptos que permitan satisfacer los requisitos específicos de los sistemas y debe poner estos conceptos dentro de un contexto que guíe la implementación e integración de ciber capacidades. Una sola arquitectura debe estar en la capacidad de servir como base para múltiples arquitecturas de sistemas específicos que soporten necesidades de negocio relacionadas.

1. Entorno ICS Energía – Definición y Modelos de Arquitectura

Para dar un contexto general en relación con el término ICS Energía y tomando como base el artículo "The Electric Power Transmission and Distribution Industry", se encuentra el siguiente diagrama que descompone de forma general, la estructura de un sistema de transmisión y distribución de energía (Merchant & Thompson, 2010) y busca explicar de manera simple el proceso en general:

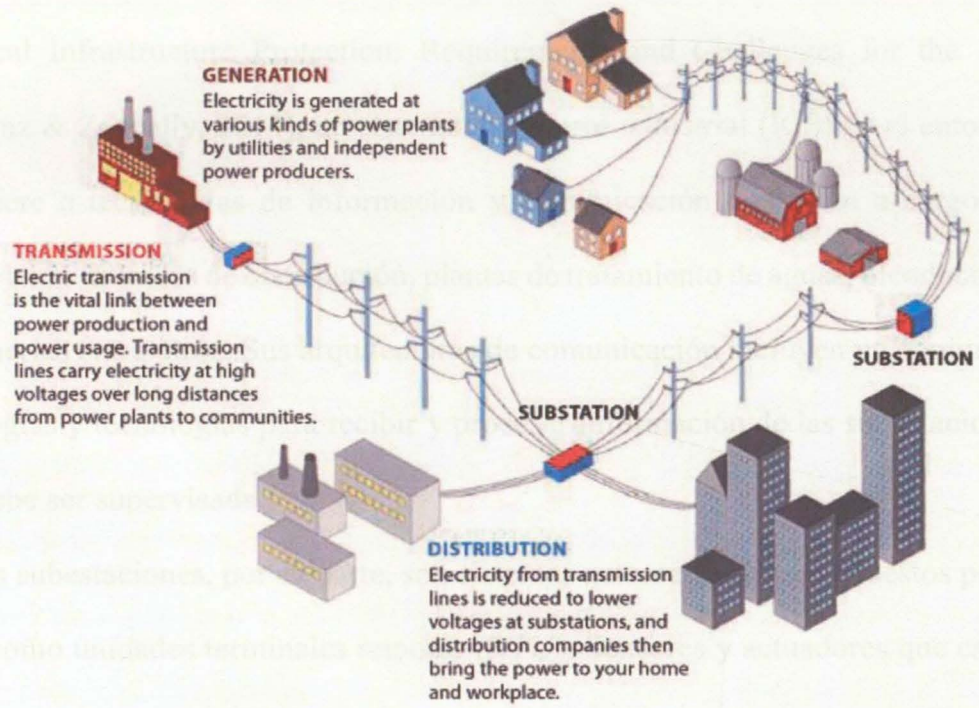

Ilustración 1:Transmission and Distribution Grid Structure within the Power Industry.[Estructura de la red de transmisión y distribución en la industria de energía]. Merchant & Thompson, 2010

En la etapa inicial de este proceso se convierte la energía de una fuente de generación (carbón, nuclear, eólica, etc.) a un formato eléctrico de alto voltaje que se puede transportar utilizando la red eléctrica, ya sea por aire o de forma subterránea. Este proceso de conversión o transformación ocurre muy cerca de la fuente de generación de energía.

La segunda etapa se produce cuando esta potencia de alto voltaje se "reduce" mediante el uso de engranajes de conmutación y luego se controla mediante el uso de interruptores automáticos y pararrayos para protegerse contra sobretensiones.

Esta energía eléctrica de media tensión puede distribuirse de manera segura en áreas urbanas o pobladas. La etapa final implica reducir la potencia a un voltaje utilizable para el cliente comercial o residencial.

En relación con los modelos de arquitectura de un ICS, y de acuerdo con el documento "Critical Infrastructure Protection: Requirements and Challenges for the 21st Century" (Alcaraz & Zeadally, 2014), un sistema de control industrial (ICS) en el entorno de energía se refiere a tecnologías de información y comunicación que están a cargo del control y supervisión de líneas de distribución, plantas de tratamiento de aguas, oleoductos, gasoductos y refinerías entre otros. Sus arquitecturas de comunicación incluyen un conjunto de enlaces, topologías y tecnologías para recibir y procesar información de las subestaciones remotas y que debe ser supervisada.

Las subestaciones, por su parte, son sistemas automatizados compuestos por dispositivos tales como unidades terminales remotas (RTU), Sensores y actuadores que están a cargo de recopilar y enviar el estado relacionado con la infraestructura controlada. Esto se envía a un nivel de supervisión o SCADA (Supervisory Control And Data Acquisition), quien a su vez puede tener comunicación bidireccional con dichos elementos.

Esto se ilustra mediante la siguiente arquitectura que incluye los elementos de las subestaciones, el sistema SCADA e incluye adicionalmente integración con la red corporativa.

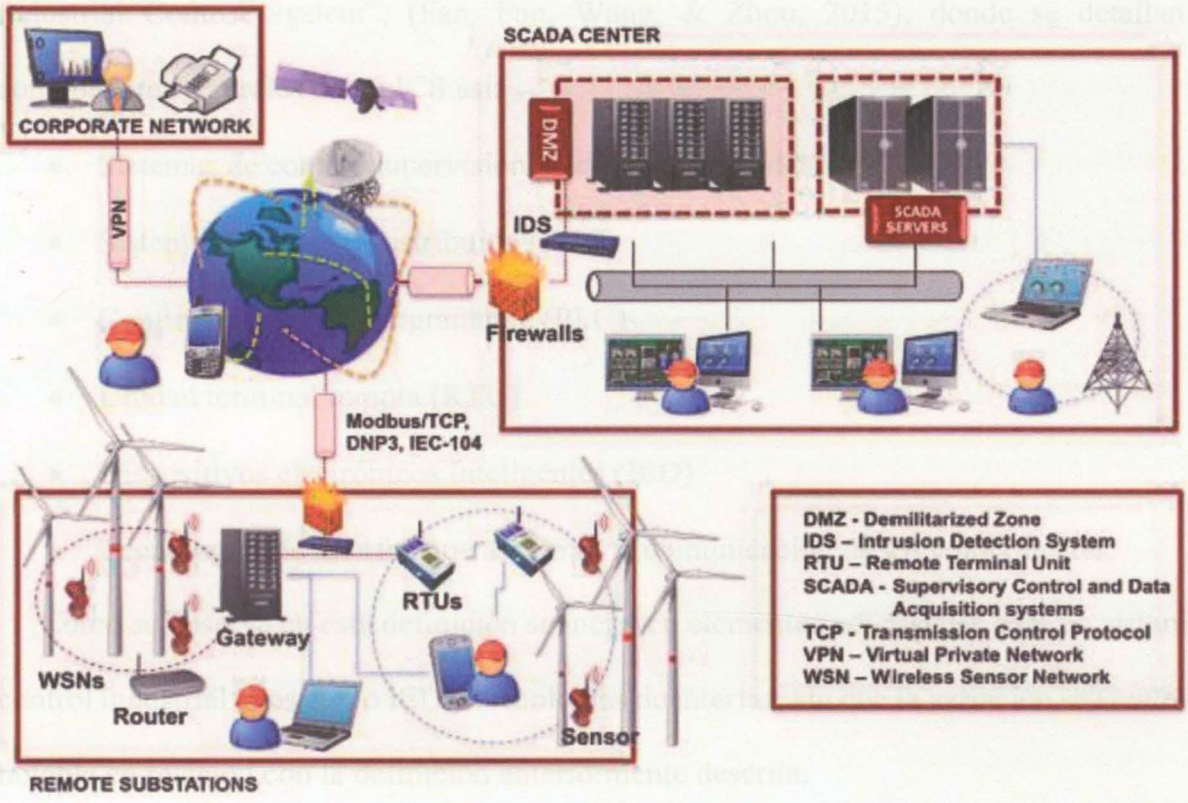

Ilustración 2: A general architecture of a SCADA network based on remote substations. [Arquitectura general de un Sistema SCADA basada en subestaciones remotas]. (Alcaraz & Zeadally, 2014)

También se encuentra el concepto de ICS en la definición realizada en "Trend Micro Cybersecurity Reference Architecture for Operational Technology", (Ku et al., 2017), en el cual se detalla que los ICS se componen de los siguientes elementos principales:

- Sistemas de supervisión de control y adquisición de datos (SCADA)
- Sistemas de control distribuido (DCS)
- Sistemas de control como Controladores lógicos programables (PLC)
- Unidades terminales remotas (RTU).

Otra definición de los elementos que componen un modelo de arquitectura para un sistema de control industrial o ICS es la realizada en el artículo "Overview of Cyber-security of

Industrial Control System", (Fan, Fan, Wang, & Zhou, 2015), donde se detallan los componentes centrales de un ICS así:

- Sistemas de control supervisión y adquisición de datos (SCADA)
- Sistema de Control Distribuido (DCS)
- Controlador lógico programable (PLC)
- Unidad terminal remota (RTU)
- Dispositivos electrónicos Inteligentes (IED)
- Tecnologías de interfaz que aseguran la comunicación de los componentes.

Como se observa en esta definición se incluyen elementos adicionales para un sistema de control industrial tales como IED y tecnologías de interfaz, sin que la variación sea realmente notable en relación con la definición anteriormente descrita.

Un punto de vista adicional es el propuesto en ISA95, descrito en An Improved Cyber-Physical Systems Architecture for Industry 4.0 Smart Factories (Jiang, 2017) que se detalla a continuación:

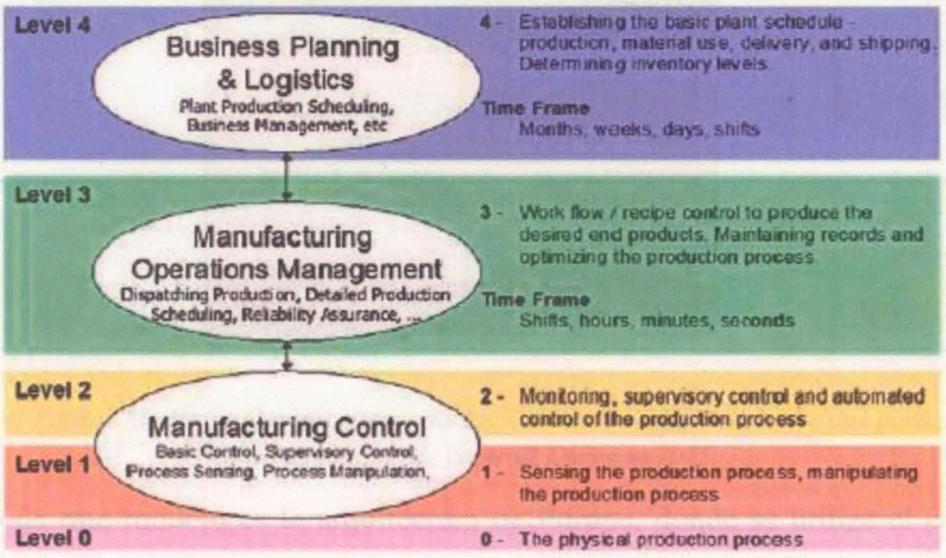

Ilustración 3: The ISA-95 architecture. [Arquitectura ISA]. Jiang, 2017

Para describir estos elementos y cada una de las capas que componen la arquitectura ISA-95, se muestra la definición en cada uno de los niveles. El nivel 0 define los procesos físicos de producción. El nivel 1 define las acciones relacionadas con sensado y maniobra del proceso físico. El nivel 2 define las acciones de monitoreo, supervisión y control automatizado del proceso físico. En este nivel es donde se encuentran elementos como el SCADA, los DCS y PLC. El nivel 3 define las acciones asociadas al flujo que permite producir los productos finales y el nivel 4 define acciones afines al negocio y necesarias para gestión de la organización.

Como complemento a la definición realizada en ISA95, se puede analizar la descripción de arquitecturas para sistemas de control industrial, detallada por la SANS en el artículo "Secure Architecture for Industrial Control Systems", (Obregon, 2015) la cual es la siguiente:

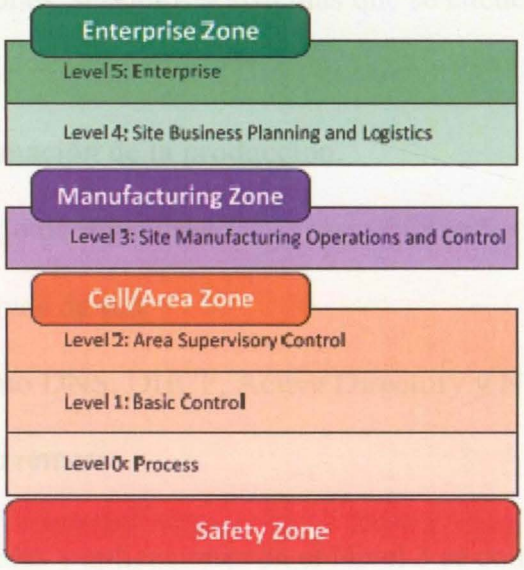

Ilustración 4: Purdue Model for Control Hierarchy logical framework.[Modelo Purdue para un modelo lógico jerárquico de control] Obregon,2015.

La base de este modelo es la arquitectura de Purdue, donde se utiliza el concepto de zonas para subdividir una red empresarial e ICS en segmentos lógicos compuestos por sistemas que realizan funciones similares o tienen funciones similares.

Zona empresarial - Nivel 5: Empresa. El nivel 5 es donde existen los sistemas y aplicaciones corporativas de infraestructura de TI. Por lo general, allí se encuentra el acceso remoto a la VPN y los servicios corporativos de acceso a Internet.

Zona empresarial - Nivel 4: Planificación de negocios y logística. Puede ser visto como una extensión del nivel 5, y es donde se encuentran los sistemas de TI que se ocupan de la generación de informes, programación, gestión de inventarios, planificación de capacidad operativa, gestión de mantenimiento, y servicios transversales tales como correo electrónico y comunicaciones. Estos son los servicios y sistemas normalmente administrados y operados por la organización de TI.

Zona de fabricación - Nivel 3: Operaciones y control. Los sistemas en el Nivel 3 son responsables de administrar la planta de control de operaciones para generar el producto deseado. Algunas aplicaciones, servicios y sistemas que se encuentran en este nivel son:

- Historiador
- Sistemas de programación de la producción.
- Estaciones de trabajo de ingeniería.
- Servidores de archivos de red
- Servicios de TI como DNS, DHCP, Active Directory y NTP
- Servicios de acceso remoto.

Normalmente, los sistemas y aplicaciones en el Nivel 3 se comunican con los sistemas de la Zona Empresarial a través de una DMZ.

Zona primaria - Nivel 2: Control de supervisión de área. Incluyen los equipos para la operación. Este nivel incluye típicamente los HMI. Los sistemas de alertas o alarmas y las estaciones de trabajo ubicadas en las salas de control

Zona primaria - Nivel 1: Control básico. Incluye los equipos de control de proceso que reciben la entrada de sensores, procesan los datos y los envían a un elemento final. Algunos dispositivos de este nivel son los DCS o sistemas de control distribuido, los PLCs y las RTU.

Estos dispositivos ejecutan sistemas operativos específicos del proveedor y son programados y configurados a través de estaciones de trabajo de ingeniería

Zona primaria - Nivel 0: Proceso. Incluye los sensores y elementos de instrumentación que se conectan directamente y permiten controlar el proceso de fabricación o producción. Son controlados por dispositivos que se encuentran en el Nivel 1.

Zona segura. Los sistemas en la zona de seguridad monitorean los procesos para validar anomalías y permiten regresar automáticamente a procesos seguros si se supera un umbral definido.

En relación con los elementos de seguridad que deben ser tenidos en cuenta en los entornos ICS es importante agregar que dichas infraestructuras están compuestas en gran parte por componentes con sistemas operativos (SO) personalizados y protocolos de red específicos, y, por lo tanto, las herramientas para abordar los problemas de ciberseguridad no son comunes en el mercado, especialmente en aquellos elementos de la arquitectura más cercanas al campo y dispositivos de entrada / salida (E / S). Por esto es importante que la arquitectura definida tenga en cuenta todos estos elementos y que su definición permita ayudar a mitigar los posibles ataques en un entorno de ICS. (Hurd & McCarty, 2017).

Como se puede evidenciar los modelos de arquitectura tampoco son conceptos únicos y determinados, pero tienen una base común que es ISA95. Es importante aclarar que uno u otro modelo no son verdades absolutas, y se deja como deber de cada organización determinar cuál es la base que más se adapta a su realidad y documentar la arquitectura, sus componentes e interrelaciones buscando entregar modelos de referencia.

2. Arquitecturas y Frameworks de Ciberseguridad para ICS

En el apartado anterior se detalló de forma general los componentes de un modelo de arquitectura para ICS. A continuación se explorará de manera general las diferentes concepciones de arquitecturas de ciberseguridad para ICS y como ellas pueden combinarse para lograr un mejor acercamiento al tema propuesto.

Arquitectura de Ciberseguridad propuesta por Trend Micro

Una referencia en arquitectura de seguridad es la proveída por Trend Micro, (Ku et al., 2017), donde se definen los requisitos funcionales típicos de las redes ICS existentes. La recomendación de este autor en cuanto a seguridad es separar las redes de TI y de TO tal como lo definen la SANS y la NIST. Para esto, se debe establecer una zona DMZ y un firewall con mecanismos de control de ciberseguridad entre las zonas. (Nota: una DMZ es un segmento de red separado). Cuando se realiza la implementación de la segmentación de red, se minimizan los métodos y niveles de acceso a información sensible y recursos del sistema, y adicionalmente se evitan movimientos laterales.

Los controles de seguridad de bordes pueden incluir gateways, routers, firewalls, IPS, IDS, VPNs entre otros. A continuación se muestra una gráfica que ilustra estos conceptos:

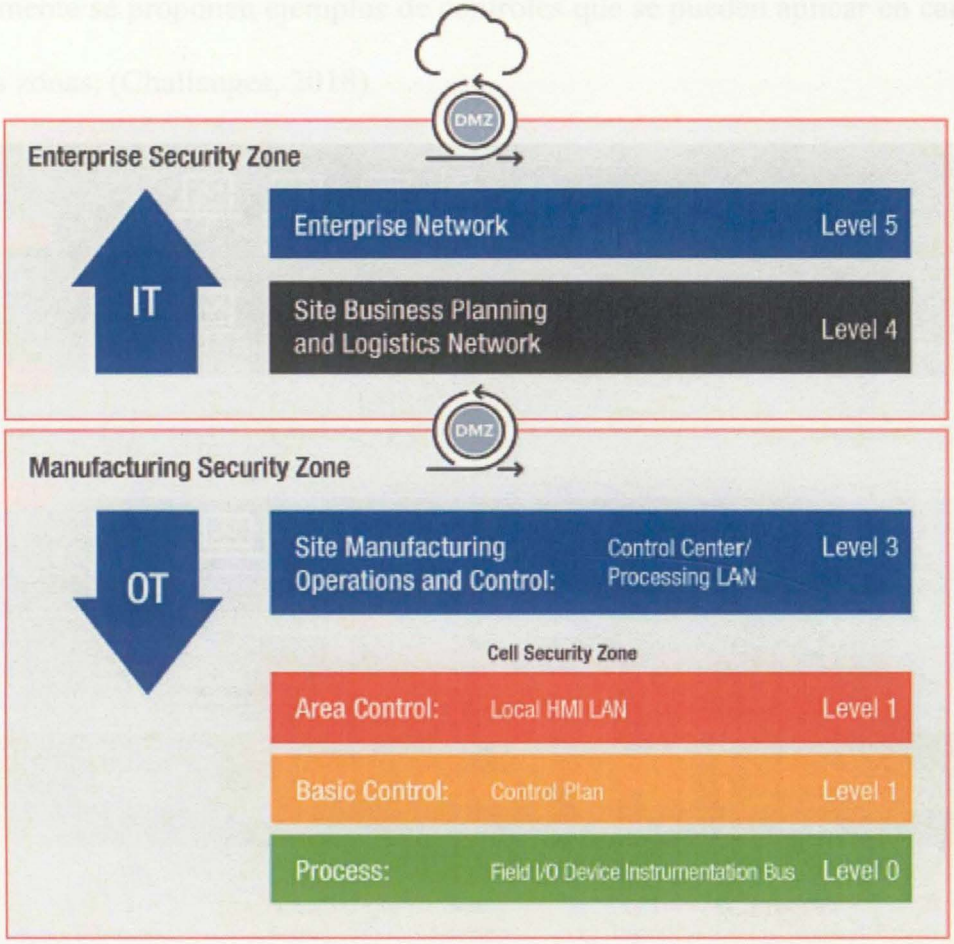

Ilustración 5: ICS Security Reference Architecture. [Arquitectura de referencia de seguridad para ICS] (Ku et al., 2017)

Arquitectura de Ciberseguridad propuesta por Gartner

En este modelo de arquitectura el autor recomienda usar el modelo de Purdue como framework de referencia de arquitectura. En esta arquitectura propuesta empezamos a validar la inclusión de conceptos y definiciones de seguridad, tomando como base un modelo de arquitectura de industria para los sistemas de control industrial tal como lo es Purdue.

Este modelo entrega una segmentación del sistema, detallando las diferentes zonas entre TI y TO que deben ser aseguradas. Con este modelo se puede realizar una mejor identificación de los controles que deben ser desplegados entre los diferentes niveles y

adicionalmente se proponen ejemplos de controles que se pueden aplicar en cada una de las diferentes zonas, (Challenges, 2018).

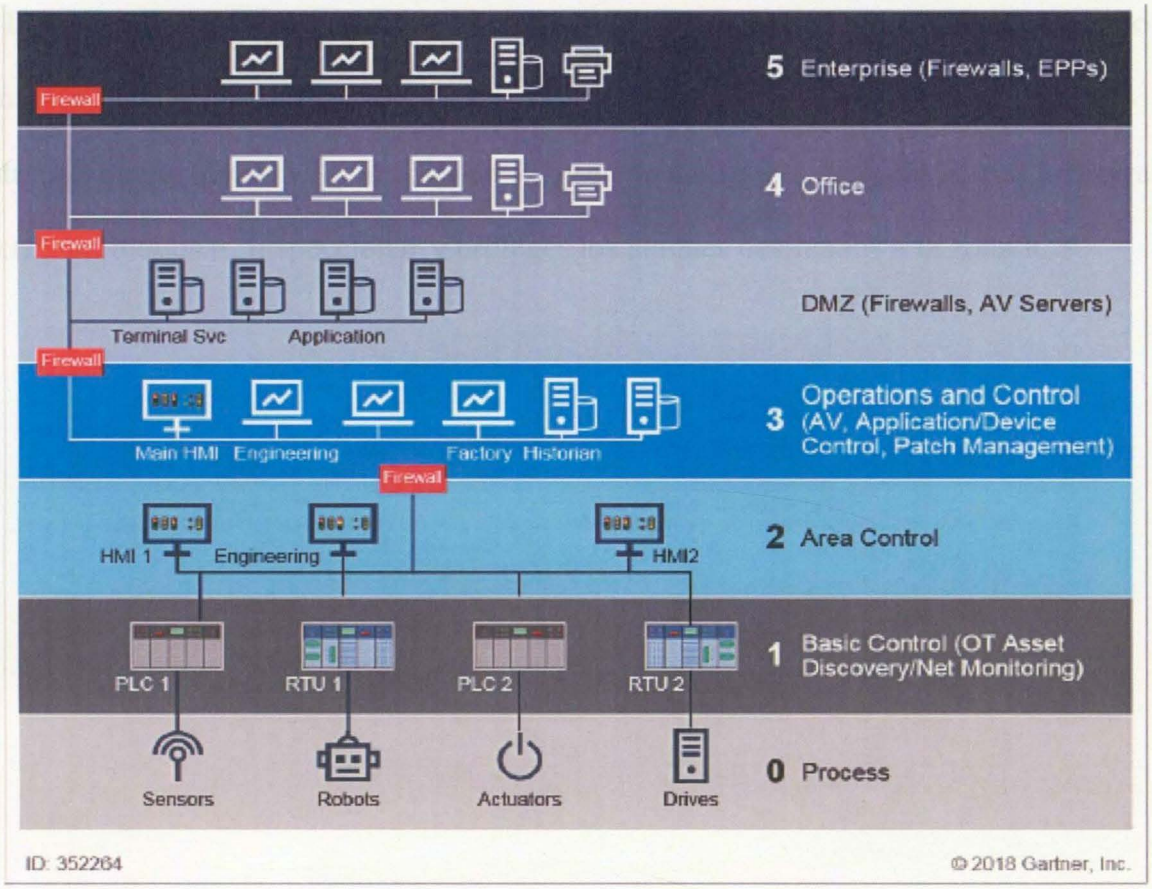

Ilustración 6: IT/OT Architecture. [Arquitectura TI/TO]. (Challenges, 2018).

Arquitectura de Ciberseguridad NIST

Mediante este modelo, el autor ilustra una arquitectura de referencia en ciberseguridad para ICS. Esta arquitectura al igual que las anteriores, utiliza el concepto de zonas para dividir la red en entornos más pequeños donde se puedan aplicar controles de seguridad más enfocados. (Obregon, 2015).

En este modelo se puede apreciar que su base principal es Purdue al igual que otras arquitecturas de ciberseguridad para ICS, y como elementos relevantes de seguridad propuestos se encuentra lo siguiente:

El nivel 5 se divide en una DMZ empresarial (para la salida a internet, VPN, Servidor web, SFTP, etc.) y una subzona interna donde residen las aplicaciones empresariales.

El IDS se muestra como parte de cada una de las capas, ya que se encuentra sensando la información que es transmitida por la red.

Entre la zona empresarial y la zona de ICS se encuentra una zona DMZ con 2 firewalls que permiten bloquear, inspeccionar y proteger los ataques destinados a la zona ICS

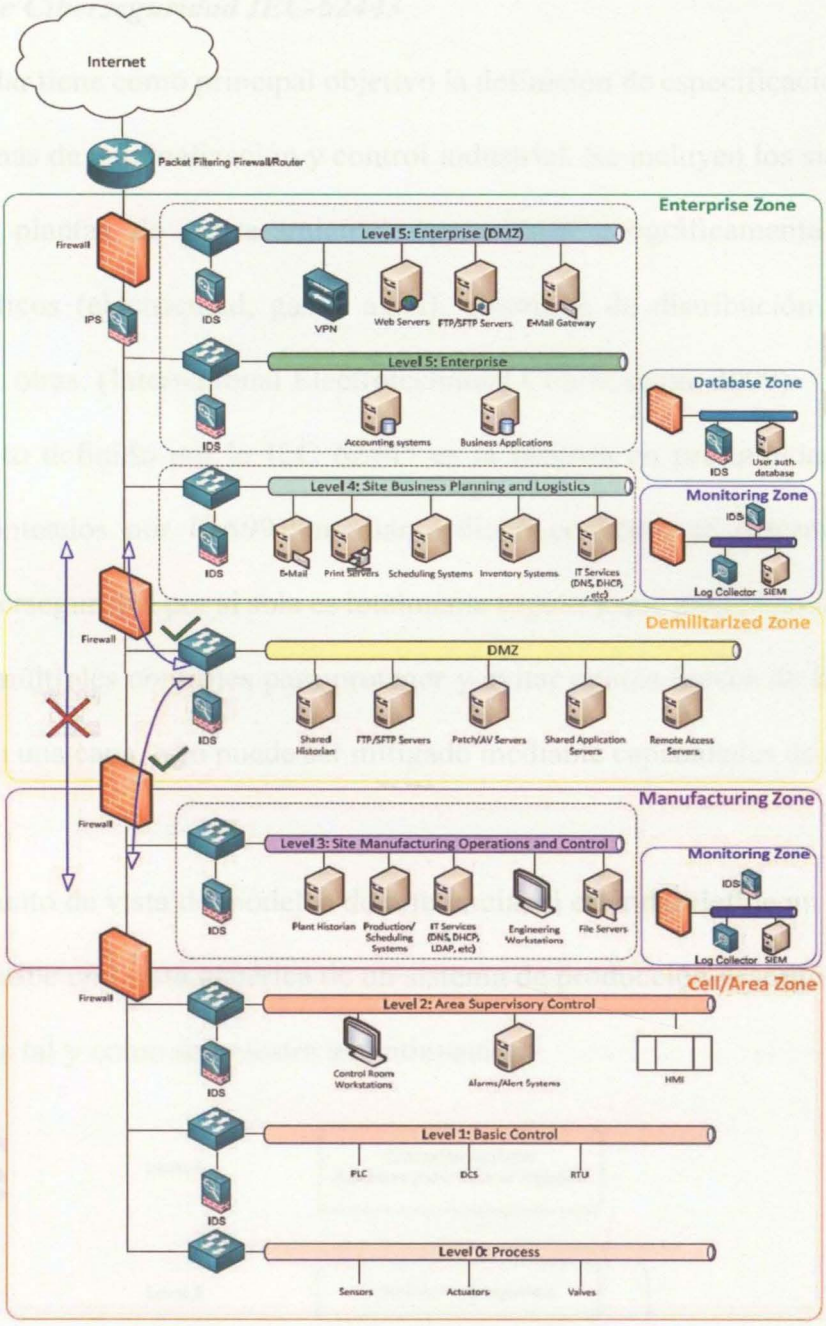

Ilustración 7. Modified Purdue Model for Control Hierarchy Architecture. [Arquitectura modificada del modelo de Purdue para control jerárquico]. (Obregon, 2015).

Framework de Ciberseguridad IEC-62443

Este estándar tiene como principal objetivo la definición de especificaciones de seguridad para los sistemas de automatización y control industrial. Se incluyen los sistemas de control utilizados en plantas de procesamiento, operaciones geográficamente dispersas como servicios públicos (electricidad, gas y agua), empresas de distribución y producción de petróleo, entre otras. (International Electrotechnical Commission, 2009)

Un concepto definido por la IEC 62443 es la defensa en profundidad (a partir de los conceptos planteados por ISA99); mediante dicho concepto se determina que ninguna medida de ciberseguridad por si sola es totalmente segura y que para reducir riesgos se deben implementar múltiples controles para proteger y evitar puntos únicos de fallas. Así en caso de intrusión en una capa, esto puede ser mitigado mediante capacidades de ciberseguridad de otras capas.

Desde el punto de vista de modelos de referencia, el estándar define un modelo mediante el cual se describe una vista genérica de un sistema de producción descrito a través de niveles lógicos tal y como se muestra a continuación:

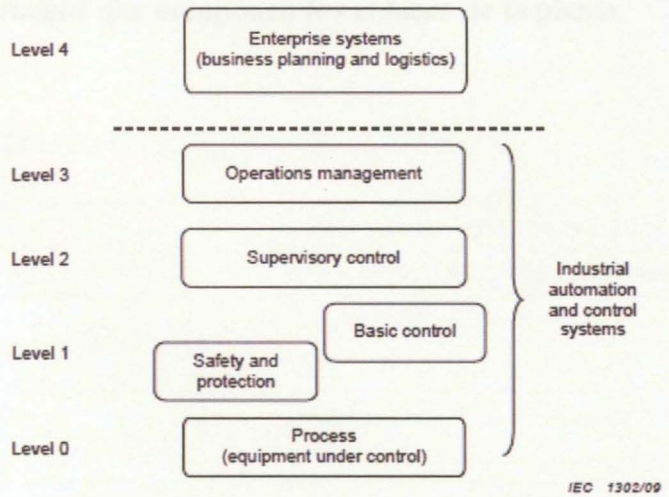

Figure 12 – Reference model for IEC 62443 standards

Ilustración 8. Modelo de referencia para el estándar IEC 62443. (International Electrotechnical Commission, 2009)

Mediante el anterior modelo se segmentan por capas las funciones y actividades que van desde los procesos (nivel 0) hasta el nivel de empresa (nivel 4).

A partir del concepto de defensa en profundidad y desde el punto de vista de su implementación, IEC 62443 define conceptos adicionales como zonas de seguridad y conductos. Las zonas de seguridad permiten dividir o agrupar los activos de acuerdo con su funcionalidad, criticidad y ubicación física, generando así una agrupación que relaciona requerimientos de seguridad comunes. En relación con las zonas de seguridad se desarrolla el concepto de conducto. Los conductos pueden ser vistos como un tipo de zona de seguridad que agrupa las comunicaciones entre zonas o internamente dentro de una zona y puede ser un único servicio (red ethernet) o estar compuesto por múltiples portadores de datos.

Para ejemplificar estos conceptos, a continuación se muestra una gráfica en la cual se pueden diferenciar la zona empresarial, las zonas de cada planta (A, B y C) y las respectivas zonas de control de cada planta. También se ejemplifican los conductos a través de los cuales se conecta cada planta a la zona empresarial y adicionalmente se muestran algunos de los conductos dentro de cada planta. En el conducto se incluyen todos los equipos de comunicaciones y cortafuegos que componen los enlaces de la planta.

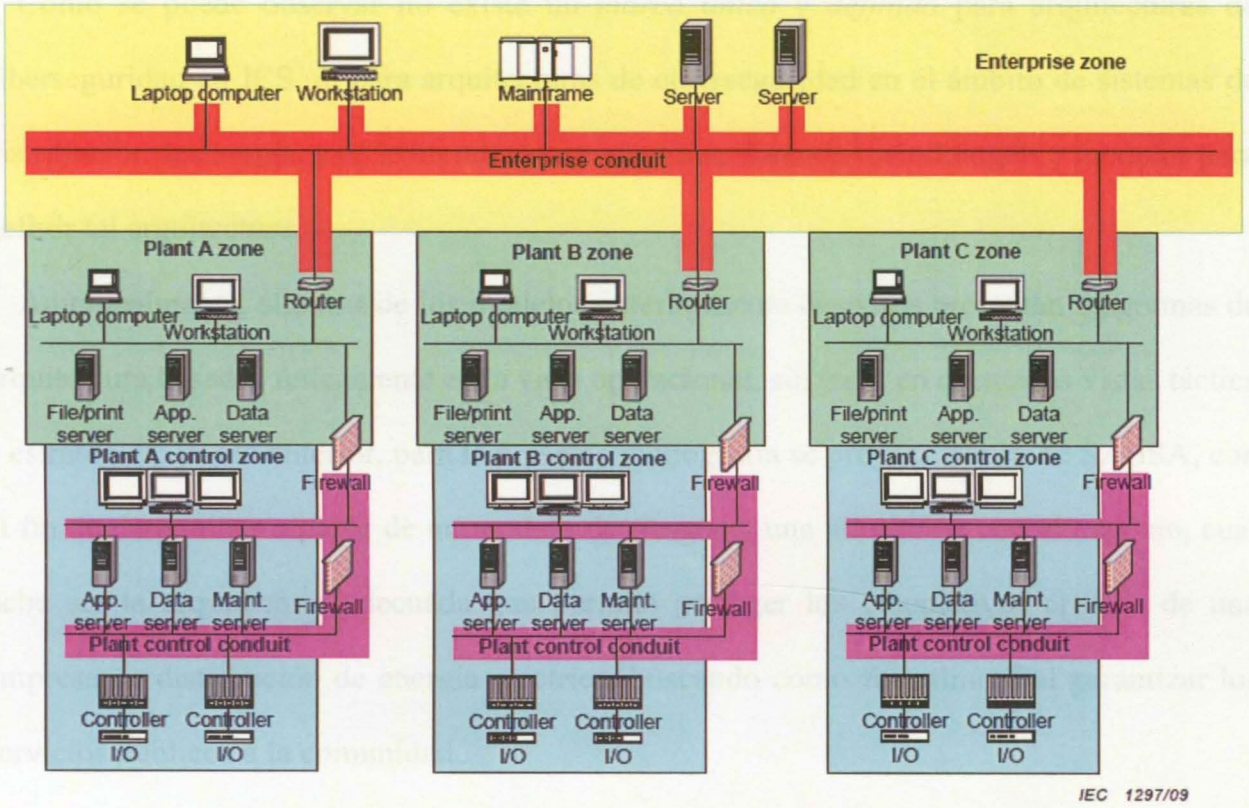

Ilustración 9. Ejemplo de conductos y zonas.(International Electrotechnical Commission, 2009)

Arquitectura de Seguridad Modelo SABSA

SABSA o Sherwood Applied Business Security Architecture, permite establecer a través de un modelo de capas, como se crea una arquitectura de seguridad. Este modelo fue adaptado de la arquitectura propuesta por Zachman, agregando una visión de seguridad. Consta de seis capas y cada capa incorpora la vista de un rol diferente para los procesos de especificar, diseñar, construir y utilizar un sistema (Sherwood et al., 2005).

The Business View	Contextual Security Architecture
The Architect's View	Conceptual Security Architecture
The Designer's View	Logical Security Architecture
The Builder's View	Physical Security Architecture
The Tradesman's View	Component Security Architecture
The Facilities Manager's View	Operational Security Architecture

Ilustración 10. Vistas del modelo SABSA. (Sherwood et al., 2005)

Como se puede observar no existe un *marco único y definido* para arquitecturas de ciberseguridad en ICS, ni para arquitecturas de ciberseguridad en el ámbito de sistemas de distribución de energía, y en la literatura se encuentran diversas metodologías y modelos para definir tal arquitectura.

Adicionalmente, algunos de los modelos anteriormente descritos presentan diagramas de arquitectura basados únicamente en la vista operacional, sin tener en cuenta las vistas táctica y estratégica. Por lo anterior, para la presente monografía se propone el uso de SABSA, con el fin de determinar a partir de un modelo de riesgos y una alineación con el negocio, cuál debe ser la arquitectura adecuada que permita proteger los ciberactivos críticos de una empresa de distribución de energía eléctrica, buscando como fin primordial garantizar los servicios públicos a la comunidad.

Para el presente trabajo y a través del marco de SABSA, se definirá la arquitectura desde las vistas de negocio y del arquitecto que nos llevan a una definición de arquitectura contextual y conceptual. **Esta aclaración debe realizarse ya que el framework de SABSA permite definir una arquitectura desde 6 diferentes vistas, pero tal alcance no es el objetivo de este trabajo (al ser una arquitectura empresarial), y por lo tanto no debe esperarse que se entreguen modelos topológicos.**

Capítulo II. Identificación de Procesos, Personas y Tecnologías Relacionados con Empresas de Distribución de Energía

En este capítulo se detallará con más precisión los siguientes elementos asociados a las empresas de distribución de energía:

- Procesos
- Personas
- Tecnologías

Esta identificación es parte de los insumos requeridos para la definición de la arquitectura empresarial.

Ilustración 11. Direccionadores de la arquitectura (nivel estratégico). Elaboración propia

Como parte esencial para la definición de una arquitectura empresarial de ciberseguridad se encuentra el entendimiento del negocio que se desea proteger, y por lo tanto el detalle de sus procesos, personas y tecnologías inherentes.

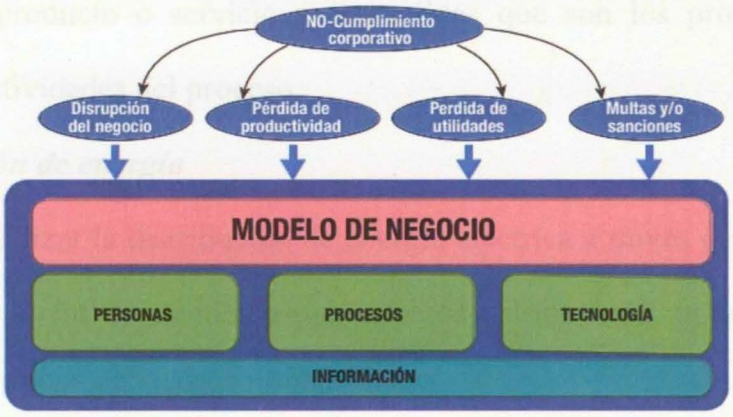

Ilustración 12. Factores de riesgo e impacto en el modelo de negocio. (Cano, 2013)

"Se debe desarrollar la competencia de ver desde las posibilidades de falla, las relaciones estructurales entre la tecnología, los procesos y las personas para condensar escenarios de potenciales amenazas que muestren acciones, que anticipen situaciones de excepción, y no solamente adviertan el incumplimiento normativo inherente a los hechos, sino que construya la capacidad de pronóstico que le debe asistir, frente a su contexto de negocio y la responsabilidad frente a sus grupos de interés" (Cano, 2013)

A continuación se describen estos 3 componentes de la estrategia empresarial

1. Procesos

Para una empresa de distribución de energía el dominio de procesos se convierte en uno de los principales elementos del modelo de arquitectura empresarial, ya que su principal enfoque es la generación de valor para los clientes a través del cumplimiento de la estrategia empresarial y busca lograr un objetivo global a nivel de empresa, facilitando el flujo de la información y el desarrollo de modelos de mejoramiento y excelencia operacional.

Los procesos tienen como parte de su definición 3 principales componentes. Las entradas que son los insumos que se transforman en el proceso, las actividades que se realizan para poder obtener un producto o servicio y las salidas que son los productos o servicios resultantes de las actividades del proceso.

Proceso Distribución de energía

Su objetivo es realizar la distribución de energía eléctrica a través de la operación de su infraestructura, con el fin de atender requerimientos del mercado, brindando continuidad, seguridad y confiabilidad del sistema. (EPM, 2016)

Dentro de los subprocesos se encuentra la planeación, la operación, el mantenimiento del sistema, seguimiento y mejora.

Ilustración 13. Proceso General del sistema de distribución de energía. Elaboración propia

Como parte de la planeación se identifican, presupuestan y asignan los recursos para los proyectos, planes de mejoramiento y planes operacionales alineados con el direccionamiento estratégico. En relación con el seguimiento y mejora como parte de un proceso, se analizan las acciones y datos relacionados con la ejecución de las actividades que permiten la optimización de resultados.

A continuación se detallan las entradas y salidas para los principales subprocesos que son la operación y el mantenimiento.

Operación del sistema de distribución

Con este subproceso se realizan las maniobras operativas necesarias por los niveles tácticos y operativos en la infraestructura del sistema, para mantener la disponibilidad y continuidad del sistema tanto en condiciones normales como de contingencia, asegurando que el sistema se encuentre dentro los parámetros establecidos como normales y dando

cumplimiento a los planes establecidos por el área de planeación empresarial que es parte del nivel estratégico de la empresa.

Ilustración 14. Proceso de Operación del sistema de distribución de energía. Elaboración propia

Actividades del proceso

- Planeación de la operación del sistema de distribución de energía eléctrica.
- Programación de la operación del sistema de distribución de energía eléctrica
- Ejecución de la operación del sistema de distribución de energía eléctrica
- Análisis Post-operativo

Mantenimiento del sistema de distribución

Con este subproceso se realizan las acciones de mantenimiento correctivas y preventivas por los niveles tácticos y operativos en la infraestructura del sistema, para mantener la disponibilidad y continuidad del sistema acorde con los objetivos del negocio que son determinados por el nivel estratégico de la empresa.

Ilustración 15. Proceso de Mantenimiento del sistema de distribución de energía. Elaboración propia

Actividades del proceso

- Programación del mantenimiento
- Ejecución del mantenimiento
- Verificación y Control del mantenimiento

2. Personas

Matriz RACI

A continuación se muestra la matriz RACI de acuerdo con las actividades definidas para cada uno de los subprocesos de operación y mantenimiento del sistema de distribución de energía.

R: Responsable, A: Aprobador, C: Consultado, I: Informado

Tabla 1. *RACI Operación del sistema de distribución*

		Roles		
		Estratégico	Táctico	Operativo
Actividades	Planeación de la operación del sistema de distribución	A/I	R	I
	Coordinación y Supervisión de la operación del sistema de distribución		A/R	I
	Ejecución de la operación del sistema de distribución.		A/C/I	R
	Análisis Post-operativo	I	I	R

Tabla 2. *RACI Mantenimiento del sistema de distribución*

		Roles		
		Estratégico	Táctico	Operativo
Actividades	Planeación y Programación del mantenimiento	I	R/A	I
	Ejecución del mantenimiento		A/C/I	R
	Verificación y Control del mantenimiento	I	I	R

3. Tecnologías

En el capítulo anterior, en el apartado número 2, se describieron de manera general los elementos más relevantes en el ámbito de empresas de energía; sin embargo, es importante detallar que tipos de elementos componen dichas arquitecturas y cuál es su funcionamiento general, con el fin de entender con más profundidad que tipos de tecnología y ciberactivos se desean proteger.

A continuación se detalla un modelo del sistema SCADA, el cual representa gran parte de los componentes de un sistema ICS para empresas de distribución. Éste es un sistema de adquisición de datos que permite la integración con sistemas que entregan datos o señales y sistemas que permiten realizar el monitoreo y control de diversas señales.

Mediante la siguiente gráfica se pueden ver detalles de los componentes de un SCADA de industria para la gestión de la distribución de energía:

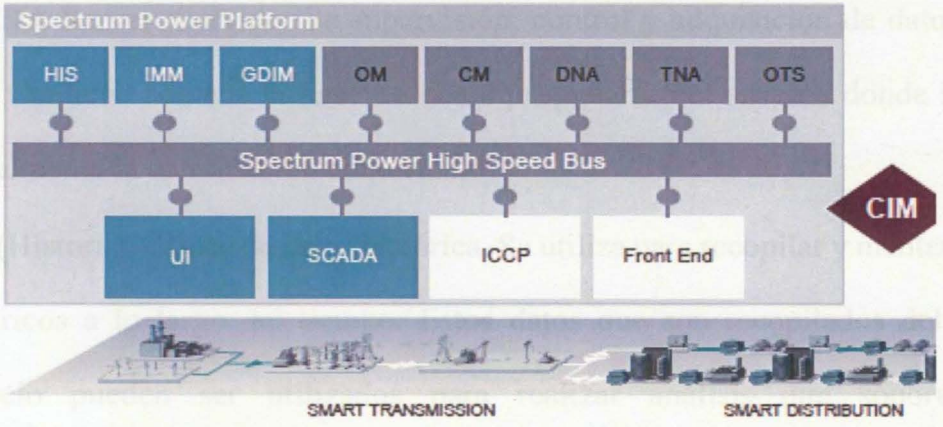

Ilustración 16. Componentes de un SCADA para un sistema de Distribución de Energía. (Siemens, 2014)

El objetivo principal de un sistema SCADA es la adquisición de datos a través de la integración con un sistema de transmisión de datos. Adicionalmente a través de los componentes como HMI o UI se proporciona un sistema de monitoreo y control centralizado para las entradas y salidas del proceso.

Los sistemas SCADA permiten la recopilación de información de campo, que luego es mostrada al operador a través de una interfaz gráfica. Esto le permite a un operado gestionar, monitorear o controlar el sistema desde una ubicación centralizada y en tiempo casi real.

El centro de control también es responsable de mostrar las alarmas de forma centralizada y permite la generación de análisis de tendencias o informes. Los dispositivos de campo son quienes realizan el control local de los actuadores y supervisan los sensores, sin embargo estos equipos definen una capacidad de acceso remoto para permitir a los operadores realizar diagnósticos remotos y reparaciones, generalmente a través de una conexión WAN independiente o acceso telefónico de acuerdo con la antigüedad y diseño de comunicaciones de los elementos de campo.

De estos componentes, es relevante describir los principales elementos que componen el sistema SCADA y que se muestran a continuación:

- SCADA Server: Servidor de supervisión, control y adquisición de datos en tiempo real. Contiene además la base de datos propietaria del sistema donde se almacena inicialmente la información adquirida.
- HIS (Historian): Base de datos histórica. Se utiliza para recopilar y mantener los datos históricos a lo largo del tiempo. Estos datos que son recopilados del proceso de negocio pueden ser utilizados para realizar análisis que soporten por ej. optimizaciones del proceso, de costos, y adicionalmente como soporte para la documentación requerida de acuerdo con las regulaciones propias del país. Teniendo en cuenta su criticidad estas bases de datos no permiten la ejecución de procesos que demanden alta capacidad de procesamiento en tiempo real. (IEC, 2019)

- IMM: Gestión del modelo de información. Este componente permite la gestión y transformación de la información para lograr comunicación e integración de los elementos que conforman el sistema.
- GDIM: Gestión de importación de datos del GIS. Esta es la base para el despliegue de todos los diagramas y modelos presentados por el SCADA
- UI: Servidores de interfaz de usuario del SCADA
- ICCP: Protocolo de comunicación entre centros de control. Adicionalmente puede ser un servidor, elemento físico o lógico dentro la arquitectura de un SCADA que cumple la función definida por el protocolo al integrar diversos centros de control.
- DNA: Aplicaciones para la red de distribución. En este grupo se encuentra el OM – OMS (Outage Management System) que es el sistema para gestión de interrupciones y permite determinar donde ocurrió un daño o evento que impida la entrega del servicio y dependiendo del tipo de evento, restaurar el servicio. También se encuentra el DMS (Distribution Management System) que permite analizar y optimizar la entrega del servicio de energía eléctrica.
- TNA: Aplicaciones para la red de transmisión
- OTS: Sistema de entrenamiento del operador
- OM – OMS: Outage Management System: Sistema para gestión de interrupciones

Como parte de estos elementos, es relevante indicar cuales son los protocolos usados por este tipo de sistemas. Para el sistema de energía los protocolos comúnmente usados son ICCP, IEC 61850 y DNP3. Dado que estos protocolos se utilizan para controlar dispositivos remotos y subestaciones, una vez que un atacante pueda obtener acceso a la red, puede manipular las comunicaciones para inyectar controles y estados maliciosos del

sistema. Por lo tanto, la red requiere versiones seguras de estos protocolos que no solo brinden garantías de seguridad, sino que también cumplan con las garantías de latencia y confiabilidad requeridas por las aplicaciones de la red. (Montanari & Querzoni, 2014).

Anteriormente se describieron los elementos que componen un sistema SCADA de industria. A continuación, se describe el resto de los elementos que son primordiales en un sistema de control industrial ICS asociado a empresas de distribución de energía y que permiten la conectividad y funcionamiento correcto entre los elementos del sistema.

El siguiente gráfico detalla tres tipos de subestaciones. Estos tipos de subestaciones son ilustrativos y no significa que un sistema de ICS para distribución de energía necesariamente contenga todos estos elementos. La clasificación se realiza con el fin de describir los posibles elementos comunes en una arquitectura de una subestación y su diseño de conectividad.

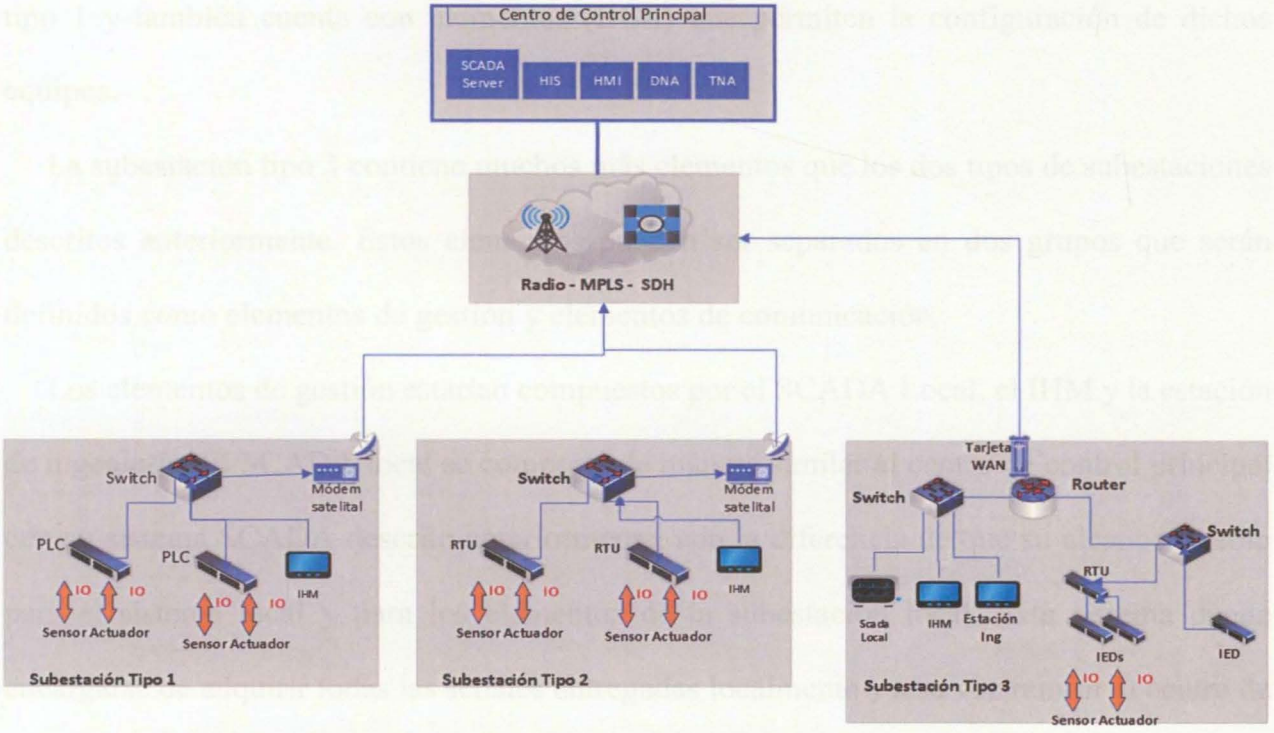

Ilustración 17. Arquitectura ICS modelo para subestaciones de energía. Elaboración propia

Como puede observarse en la ilustración 16, se describen 3 tipos de subestación que a través de algún medio de conectividad (Radio, MLPS, SDH o incluso una combinación de

ellos) envían o reciben información de un Centro de control Principal, el cual contiene el sistema SCADA.

La subestación tipo 1 se encuentra compuesta principalmente por elementos de tipo PLC, a través de los cuales se envían o reciben señales a dispositivos de campo tales como sensores o actuadores. Estos dispositivos se comunican a través de un suiche capa 2, el cual a su vez a través de un módem satelital envía la información al centro de control principal. En este modelo también se cuenta con un elemento de tipo (IHM o HMI) que es quien permite la operación local y configuración de dichos elementos.

La subestación tipo 2 se encuentra compuesta principalmente por elementos de tipo RTU, a través de los cuales también se pueden enviar o recibir señales a los dispositivos de campo. En relación con el esquema de comunicación se comporta exactamente igual a la subestación tipo 1 y también cuenta con elementos (IHM) que permiten la configuración de dichos equipos.

La subestación tipo 3 contiene muchos más elementos que los dos tipos de subestaciones descritos anteriormente. Estos elementos pueden ser separados en dos grupos que serán definidos como elementos de gestión y elementos de comunicación.

Los elementos de gestión estarían compuestos por el SCADA Local, el IHM y la estación de ingeniería. El SCADA local se comporta de manera similar al centro de control principal con su sistema SCADA descrito anteriormente, con la diferencia de que su alcance es solo para el sistema local y para los elementos de la subestación local. Este sistema puede encargarse de adquirir todas las señales entregadas localmente y a su vez remitir al centro de control principal únicamente las señales requeridas. Adicionalmente como parte de la gestión se encuentran el IHM para las configuraciones de equipos locales (por ej. RTUs) y las

estaciones de ingeniería que pueden contener software especializado para tareas de programación más detalladas o complejas.

Como parte de los elementos de comunicación se encuentran las RTUs, IEDs, suiches y routers. Para sistemas de distribución de energía se utilizan normalmente IED tales como relés de protección orientados principalmente a la detección de fallas tales como sobrecorriente, sobretensión y fallos de tierra entre otros. Estos dispositivos pueden comunicarse directamente con el centro de control o con RTUs que concentran las comunicaciones de diversos IEDs tal como se muestran en la gráfica. En el esquema de conectividad propuesto para este tipo de subestación se realiza conexión de los elementos a través suiches, un router y el uso de la red MPLS para la conexión con el centro de control principal.

A continuación se detallan los principales elementos descritos en las arquitecturas tipo de las subestaciones:

IHM o HMI (Human Machine Interface). Es el software y Hardware a través de los cuales los operadores interactúan con un controlador. Físicamente puede ser definido como un panel de control físico con botones y leds indicadores o incluso puede llegar a ser un computador industrial con un software especializado. Esta interfaz le permite a un operador humano monitorear y modificar configuraciones, y en caso de una emergencia sobrescribir funciones que pudieron ser enviadas automáticamente para lograr así una operación local. (Stouffer, Lightman, Pillitteri, Abrams, & Hahn, 2014)

Estación de Ingeniería. Es un Computador que usa un sistema operativo común (Windows o Linux principalmente) y que contiene el software necesario para configurar por ejemplo un IED, RTU, PLC o aplicaciones adicionales requeridas para realizar monitoreos o

análisis locales. Adicionalmente con estos computadores se pueden realizar actualizaciones de firmware. Los trabajos realizados en estas estaciones se almacenan localmente.

PLC (Programmable logic controller). Un controlador lógico programable es un componente de control que provee gestión local de procesos. Tiene una memoria programable que permite almacenar instrucciones para implementar funciones tales como control de entrada, salida, funciones lógicas, de tiempo y de comunicación, entre otras. Puede incluso ser accedido desde un HMI y físicamente presenta una fuente de alimentación, un microprocesador, módulos de entrada/salida e interfaz de comunicaciones.

IED (Intelligent Electronic Device). Los dispositivos electrónicos inteligentes están compuestos por uno o varios procesadores que permiten recibir o enviar datos o señales de control desde o hacia una fuente externa. Un IED provee una interfaz directa para monitorear y/o controlar equipos y/o sensores. Estos dispositivos también cuentan con programación local que les permite actuar sin necesidad de tener comunicación con un centro de control. (Stouffer et al., 2014)

Aunque conceptualmente es muy similar a un PLC, el término IED se utiliza comúnmente para sistemas de energía y específicamente para automatización de subestaciones. Un IED recibe mediciones del equipo de potencia (por ejemplo, transformadores, interruptores y circuitos) y ejecuta lógica de control o funciones de protección. (IEC, 2019)

Los IEDs igual que los PLCs pueden ser configurados a través de una estación de ingeniería y utilizando un software especializado. La diferencia con los PLCs es que los IED permiten directamente a través de una interfaz de usuario propia del dispositivo, la ejecución de funciones esenciales, por lo que estos dispositivos funcionan correctamente aún sin comunicación por fuera de la subestación o incluso sin comunicación con otros IEDs o

elementos de la subestación. Los IED modernos utilizan protocolos basados en Ethernet y TCP / IP para comunicarse con los niveles superiores y similar a los PLC, los IED deben cumplir con los requisitos de alta integridad y disponibilidad en tiempo real.

RTU (Remote terminal Unit). Se utilizan principalmente para comunicación con equipos remotos en campo. Los PLCs con comunicación vía radio también pueden cumplir las funciones de una RTU. Estos dispositivos también están equipados con diversas capacidades para comunicación por red alámbrica con el controlador de supervisión. son elementos cruciales en los sistemas SCADA ya que son responsables de adquisición de los datos en las subestaciones y ejecución de los comandos enviados por el sistema central.(Shirali, Ensafi, & Naseri, 2010)

Capítulo III. Drivers de negocio, Legislación y Riesgos Asociados a Ciberactivos en las Empresas de Distribución de Energía

En el capítulo anterior se describieron los procesos, tecnologías y personas asociadas al proceso de distribución de energía eléctrica. A partir de estos elementos se definirá lo siguiente:

- Requerimientos de negocio, drivers de negocio y atributos de ciberseguridad
- Requerimientos regulatorios o legales
- Flujos de información
- Escenarios de riesgos

Estas son las principales entradas y direccionadores para la definición de la arquitectura empresarial de ciberseguridad y por lo tanto, será el desarrollo de este capítulo tal y como se muestra a continuación.

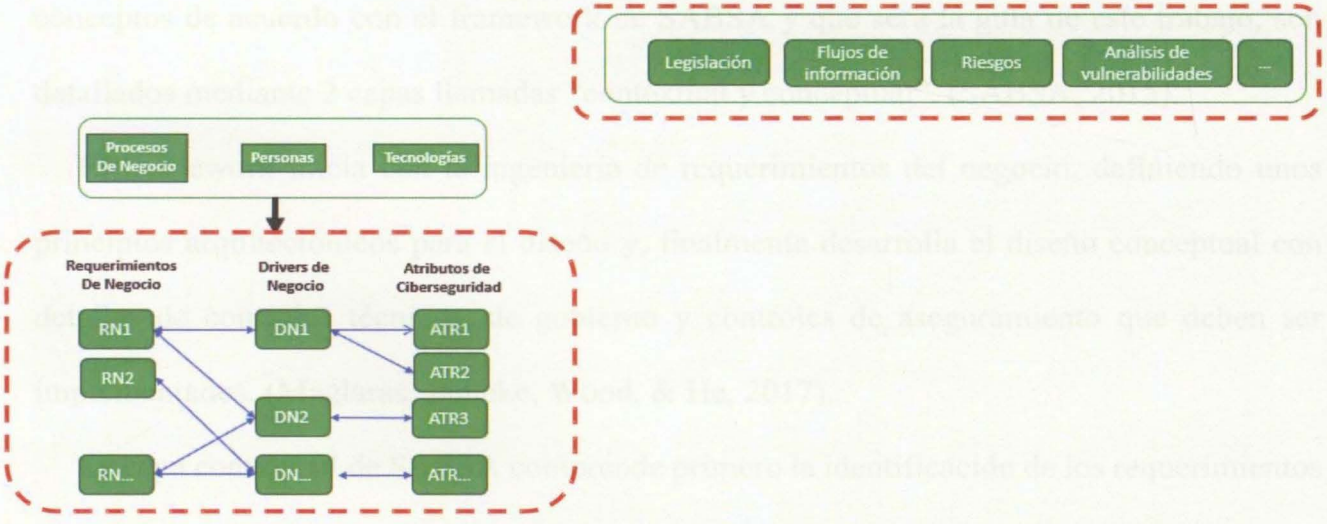

Ilustración 18. Direccionadores de arquitectura. Nivel estratégico y táctico + ciberseguridad. Elaboración propia

Para iniciar es relevante indicar que en los ambientes de operación de TO, cualquier cuestionamiento acerca de vulnerabilidades potenciales se debate y se justifica a través de la falta de conocimiento de la tecnología de la operación (concepto de seguridad por oscuridad)

y adicionalmente el personal de TO confía en la falta de conectividad con el exterior. (Michael Horkan, 2015)

La situación actual asociada a los sistemas de control industrial se encuentra enmarcada por el uso de protocolos propietarios en los diferentes elementos de la red, estaciones de control y sistemas SCADA. Este tipo de redes y el uso de dichos protocolos cumple una función específica y están orientados para permitir la comunicación de la información necesaria y suponen que dicha información es siempre verdadera, por lo que la situación normal no es solicitar autenticación. (Michael Horkan, 2015).

1. Requerimientos, Drivers de Negocio y Atributos de Ciberseguridad

Como paso inicial para determinar cuál debería el estado deseado en ciberseguridad para una empresa de distribución de energía, deben quedar entonces claramente definidos los requerimientos y drivers de negocio que guiarán el desarrollo de esta arquitectura. Estos conceptos de acuerdo con el framework de SABSA y que será la guía de este trabajo, son detallados mediante 2 capas llamadas "contextual y conceptual". (SABSA, 2015).

El framework inicia con la ingeniería de requerimientos del negocio, definiendo unos principios arquitectónicos para el diseño y, finalmente desarrolla el diseño conceptual con detalles de controles técnicos, de gobierno y controles de aseguramiento que deben ser implementados. (Maglaras, Janicke, Wood, & He, 2017).

La capa contextual de SABSA comprende primero la identificación de los requerimientos de negocio y a continuación la identificación de los drivers de negocio enfocados en seguridad. La motivación para la definición de ciberseguridad puede ser determinada al analizar adicionalmente la regulación y los factores de riesgo asociados con los drivers de negocio. (Shore & Deng, 2010).

Requerimientos de Negocio

Los requerimientos de negocio para una empresa de distribución de energía están asociados especialmente a la disponibilidad del sistema, más que a los otros atributos de seguridad. La disponibilidad es el factor más esencial para un sistema de control ya que el servicio no debe interrumpirse ni por un momento. (Kim, Kang, Na, Chung, & Work, 2016).

La disponibilidad es una característica fundamental en este tipo de sistemas, ya que la perdida de la misma puede generar pérdidas financieras, multas por entes regulatorios, e incluso pérdida de vidas humanas. A continuación se detallan los requerimientos típicos propuestos en términos del negocio:

Tabla 3. *Requerimientos de Negocio para una empresa de distribución de energía*

Nro. Req	Descripción del requerimiento
RN1	Se debe garantizar una operación confiable del sistema eléctrico nacional con disponibilidad del 99,8% del tiempo y evitando una caída que pueda impactar al usuario final. (Araghi & Fardi, 2018)
RN2	El sistema SCADA debe permitir tanto operación local como remota.
RN3	El sistema debe permitir conexiones remotas en caso de ser requerido únicamente para el soporte entregado por el fabricante.
RN4	Los sistemas deben entregar la información requerida para realizar analíticos y minería de datos. También deben entregar la información para otros sistemas que la requieran con el fin de optimizar los costos y la operación del negocio.

RN5	El servicio debe ser monitoreado con el fin de detectar posibles intrusiones, mal uso o fallos
RN6	Se debe garantizar el acceso a los sistemas que componen el servicio solo para el personal autorizado
RN7	Se debe prevenir la fuga de información
RN8	El sistema debe estar protegido contra fuentes de amenazas conocidas
RN9	El sistema debe estar protegido contra fuentes de amenazas internas
RN10	El sistema de estar protegido de forma que se evite que una falla o ataque en una parte del sistema genere daño a todo el sistema
RN11	Se debe garantizar el cumplimiento regulatorio

Drivers de Negocio

Los drivers de negocio soportan los requerimientos de negocio. Permiten definir requerimientos más específicos enfocados en seguridad y desarrollar los requerimientos de negocio de una forma medible. A continuación se describen los drivers de negocio y su relación con los requerimientos de negocio.

Tabla 4. *Drivers de negocio para una empresa de distribución de energía*

Nro. Driver	Descripción del Driver	Relación con RN
DN1	Mantener la capacidad operacional y disponibilidad del sistema en un n%	RN1
DN2	Se deben identificar y proteger los perímetros de seguridad electrónica dentro de los cuales residen los	RN1,RN8,RN9

	ciberactivos críticos. (Consejo Nacional de Operación, 2015)	
DN3	Definir procedimientos e implementación de controles tecnológicos sobre los ciberactivos con el fin de tener un estándar mínimo de gestión de seguridad. (Consejo Nacional de Operación, 2015)	RN1,RN7.RN10
DN4	Administrar el acceso físico a los ciberactivos que permita la protección de los ciberactivos críticos en contra de situaciones que puedan llevar a una mala operación o inestabilidad en el sistema interconectado Nacional. (Consejo Nacional de Operación, 2015)	RN2, RN6, RN7
DN5	Proveer un mecanismo para conectarse al sistema SCADA de forma remota segura y solo por el personal autorizado	RN2, RN3
DN6	Proveer un mecanismo para que el sistema SCADA pueda entregar la información que se requiera a otros sistemas autorizados	RN4
DN7	Identificar y detener ataques de fuentes conocidas y desconocidas	RN8,RN9
DN8	Disponer de mecanismos de monitoreo pasivos que permitan determinar si existe un comportamiento anómalo o sospechoso en la red del sistema	RN5, RN10

DN9	Implementar capas de defensa en profundidad con controles de contención para proteger ciberactivos críticos.	RN10
DN10	Implementar mecanismos seguros para intercambio de información entre los elementos del sistema	RN4
DN11	Se debe asegurar que los privilegios de acceso son diseñados e implementados de tal forma que se minimice el riesgo de que una sola persona tenga poder excesivo que pueda ser abusado sin ser fácilmente detectado	RN6, RN9
DN12	Proteger la reputación de la empresa, asegurando que es percibida como competente en el sector	RN1
DN13	Mantener la entrega continua del servicio cumplimento con los requerimientos de acuerdos de niveles de servicio	RN1
DN14	Se debe asegurar que el enfoque de ciberseguridad de los sistemas apoye el cumplimiento legal	RN11

Asociación de los drivers de negocio con atributos de seguridad

En el negocio de distribución de energía los principales atributos de seguridad están asociados a la disponibilidad y en segunda medida a la integridad. El control de la operación se otorga a los sitios de campo de forma remota, donde el tiempo real y los datos precisos son muy importantes para el control. El flujo de información retrasado puede causar, por ejemplo, el apagado del sistema y / o poner en peligro la vida humana. La disponibilidad e integridad de los datos de control es un requisito previo para una red SCADA segura y protegida. (Katam, 2015)

Tabla 5. *Asociación de los drivers de negocio con Atributos de seguridad. Elaboración propia*

Nro. Driver	Descripción del Driver	Atributos de Seguridad	Nro. Atributo	Detalle del atributo
DN1	Mantener la capacidad operacional y disponibilidad del sistema en un n%	Disponibilidad	ATR1	La información y los servicios deben estar disponibles de acuerdo con el nivel de servicio requerido para el servicio de energía eléctrica establecido en un 99.8975% (Araghi & Fardi, 2018)
DN2	Se deben identificar y proteger los perímetros de seguridad electrónica dentro	Integridad	ATR2	El proceso debe estar monitoreado en línea o por lo menos de forma constante, con el fin de alertar en caso

Nro. Driver	Descripción del Driver	Atributos de Seguridad	Nro. Atributo	Detalle del atributo
	de los cuales residen los ciberactivos críticos (CNO)			de cambios del comportamiento del mismo y garantizar la integridad de la información.
DN3	Definir procedimientos e implementación de controles tecnológicos sobre los ciberactivos con el fin te tener un estándar mínimo de gestión de seguridad (CNO)	Disponibilidad	ATR3	Los ciberactivos asociados a los servicios de TO deben estar plenamente identificados y caracterizados con el fin de garantizar el conocimiento mínimo de la infraestructura a proteger y su comportamiento en condiciones normales, lo cual permitirá garantizar el funcionamiento del sistema.
			ATR4	Los ciberactivos deben ser actualizados y parchados de acuerdo con recomendación del fabricante, con el fin de evitar explotación por vulnerabilidades conocidas.
			ATR5	Los ciberactivos deben configurarse de acuerdo con prácticas adecuadas de ciberseguridad dentro de las

Nro. Driver	Descripción del Driver	Atributos de Seguridad	Nro. Atributo	Detalle del atributo
				cuales se encuentran deshabilitar puertos y servicios no utilizados y gestión de uso de dispositivos autorizados.
DN4	Administrar el acceso físico a los ciberactivos que permita la protección de los ciberactivos críticos en contra de situaciones que puedan llevar a una mala operación o inestabilidad en el sistema interconectado Nacional (CNO)	Disponibilidad	ATR6	Cada solicitud de ingreso al sistema debe ser verificada a través de un procedimiento que permita validar que efectivamente, quien realiza la solicitud es quien dice ser, evitando la inestabilidad o mala operación del sistema.
		Integridad	ATR7	Todas las acciones realizadas sobre el sistema deben ser en lo posible registradas, entregando un nivel de detalle requerido por el negocio
DN5	Proveer un mecanismo para conectarse al sistema SCADA de forma remota	Disponibilidad	ATR8	Cada solicitud de ingreso al sistema debe ser verificada a través de un procedimiento que permita validar que efectivamente quien realiza la solicitud es quien dice

Nro. Driver	Descripción del Driver	Atributos de Seguridad	Nro. Atributo	Detalle del atributo
	segura y solo por el personal autorizado			ser, evitando la inestabilidad o mala operación del sistema.
		Integridad	ATR9	Todas las acciones realizadas sobre el sistema deben ser en lo posible registradas, entregando un nivel de detalle requerido por el negocio
DN6	Proveer un mecanismo para que el sistema SCADA pueda entregar la información que se requiera a otros sistemas autorizados	Integridad	ATR10	El sistema debe interoperar con otros sistemas que adicionalmente pueden tener diversos protocolos industriales, con el fin de compartir información requerida de forma segura e integra.
DN7	Identificar y detener ataques de fuentes conocidas y desconocidas	Disponibilidad	ATR11	Los eventos relevantes y/o reconocidos por su calificación negativa, deben ser detectados, reportados y en lo posible deben detenidos de forma automática para evitar indisponibilidad del sistema

Nro. Driver	Descripción del Driver	Atributos de Seguridad	Nro. Atributo	Detalle del atributo
DN8	Disponer de mecanismos de monitoreo pasivos que permitan determinar si existe un comportamiento anómalo o sospechoso en la red del sistema	Disponibilidad, Integridad	ATR12	El proceso debe estar monitoreado en línea o por lo menos de forma constante, con el fin de alertar en caso de cambios del comportamiento del mismo y garantizar la integridad de la información y disponibilidad del sistema
DN9	Implementar capas de defensa en profundidad con controles de contención para proteger ciberactivos críticos.	Disponibilidad	ATR13	El sistema debe estar diseñado mediante el uso de capas de ciberseguridad, de forma que existan controles para que caso de una intrusión, no se permita el acceso a todo el sistema de forma indiscriminada causando indisponibilidad del mismo.
DN10	Implementar mecanismos seguros para intercambio de	Integridad	ATR14	El sistema debe disponer de mecanismos seguros, no propietarios, que permitan compartir información garantizando la integridad de la misma.

Nro. Driver	Descripción del Driver	Atributos de Seguridad	Nro. Atributo	Detalle del atributo
	información entre elementos del sistema			
DN11	Se debe asegurar que los privilegios de acceso son diseñados e implementados de tal forma que se minimice el riesgo de que una sola persona tenga poder excesivo que pueda ser abusado sin ser fácilmente detectado	Disponibilidad	ATR15	Se debe garantizar un diseño de ciberseguridad basado en el mínimo privilegio, para evitar que un actor malintencionado o no, pueda generar indisponibilidad del sistema.
DN12	Proteger la reputación de la empresa, asegurando que es percibida como competente en el sector	Disponibilidad	ATR16	La información y los servicios deben estar disponibles de acuerdo con los niveles de servicio requeridos, generando confiabilidad tanto en los usuarios y clientes como en el sector en general.

Nro. Driver	Descripción del Driver	Atributos de Seguridad	Nro. Atributo	Detalle del atributo
DN13	Mantener la entrega continua del servicio, cumplimento con los requerimientos de acuerdos de niveles de servicio	Disponibilidad	ATR17	La información y los servicios deben estar disponibles de acuerdo con los niveles de servicio requeridos, generando confiabilidad tanto en los usuarios y clientes como en el sector en general.
DN14	Se debe asegurar que el enfoque de ciberseguridad de los sistemas apoye el cumplimiento legal	Disponibilidad	ATR18	Los sistemas deben garantizar el cumplimiento regulatorio Colombiano en relación con ciberseguridad, garantizando el cumplimiento de las condiciones exigidas desde el punto de vista legal, y que están orientadas a la prestación y disponibilidad del servicio.

2. Legislación aplicable

En el ámbito colombiano, y en relación con el cumplimiento normativo relacionado con requerimientos de Ciberseguridad, se encuentra la política Nacional de seguridad Digital o CONPES 3854, en la cual, además de promover la defensa y seguridad nacional en el entorno digital. se incluyen las infraestructuras críticas cibernéticas nacionales como actor relevante.

Esta política es la guía para la construcción de estrategias que permiten desarrollar la ciberseguridad en diferentes sectores nacionales. Específicamente en el plano de infraestructuras críticas se determina que el Ministerio de Defensa Nacional a partir de la guía para la identificación de infraestructura crítica cibernética, llevará a cabo la actualización periódica del catálogo de infraestructuras críticas cibernéticas nacionales y establecerá los planes de protección para las mismas.(MinTIC, MDN, DNI, & DNP, 2016).

Otra parte del marco regulatorio, asociado a infraestructuras críticas y a tecnologías de la operación es la RESOLUCIÓN 40072 DE 29 DE ENERO DE 2018, relacionada con la implementación de infraestructura de Medición Avanzada en el servicio público de energía eléctrica. En dicha resolución y desde el punto de vista de ciberseguridad se determina que la Comisión de Regulación de Energía y Gas (CREG) establecerá los requisitos de ciberseguridad, manejo, uso y protección de datos que garanticen un adecuado funcionamiento de la infraestructura de medición avanzada y privacidad de la información. Así mismo la CREG 038 que legisla código de la medida, determina requerimientos mínimos de seguridad e integridad en las lecturas de medidas, transporte de información y configuración de los equipos involucrados.

Finalmente, y como parte de la regulación más fuerte en el ámbito de este trabajo, se encuentra el acuerdo 1241 de 2019 definido por el Comité Nacional de Operación, en el cual se define la Guía de Ciberseguridad, la cual hace referencia al cumplimiento de la

normatividad NERC-CIP, y de la cual se extractaron los aspectos aplicables a las empresas del sector eléctrico en Colombia y relacionados con definición de activos críticos, controles asociados a la gestión de ciberseguridad, personal y entrenamiento, perímetros de seguridad electrónica, seguridad física, gestión de sistemas de seguridad, reporte de incidentes, planes de respuesta y planes de recuperación de ciberactivos críticos. (Consejo Nacional de Operación, 2015).

En relación con el cumplimiento del acuerdo de ciberseguridad previamente definido por el CNO (Consejo Nacional de Operación, 2015), se encuentra que empresas como Celsia tienen identificado como uno de los riesgos estratégicos la Ciberseguridad, entendida como ataques o fallas cibernéticas que pongan en peligro la prestación de los servicios o la entrega de los productos, con impacto reputacional y/o económico, y para lo cual se ejecutan acciones de mitigación tales como implementación de herramientas para detección de eventos asociados a ciberseguridad con el fin de aislar las operaciones comprometidas. (Celsia, 2018)

Otra empresa analizada fue ISA, la cual muestra dentro de su marco estratégico y como parte de los riesgos emergentes los ataques cibernéticos. Ellos determinan como impacto en relación con este riesgo, sobrecostos para la compañía y definen como acciones de mitigación, la implementación de mecanismos de protección para los ciberactivos a través de monitoreo en tiempo real, procedimientos de seguridad física y definición de planes de recuperación. (ISA, 2017).

ENEL muestra dentro de su informe anual la participación en las mesas de infraestructura crítica y su participación en la actualización del acuerdo 788. Como acciones concretas asociadas a este acuerdo se definió la política de gestión de eventos de ciberseguridad y se implementaron herramientas de monitoreo en tiempo real para supervisar y analizar el tráfico

de la red, además de funciones de supervisión para la navegación corporativa.(Codensa S.A.S., 2018).

Por último, EPM con base en lo dispuesto en el acuerdo mencionado, lineamientos generales para la estrategia de gobierno en línea y el cumplimiento de la Política de seguridad de la información y ciberseguridad del Grupo empresarial, define lineamientos normativos para el cumplimiento de los requerimientos de ciberseguridad, la protección de información, activos y ciberactivos críticos, mantenimiento del inventario de los mismos, repuesta a incidentes, continuidad del negocio y elementos de concienciación.(EPM, 2017)

Como puede analizarse en estos informes, estas empresas están guiando la definición de su estrategia de Ciberseguridad principalmente en elementos de cumplimiento legal. El enfoque propuesto en este trabajo incluye además del marco regulatorio, obtener como parte de los drivers que soportan la definición de la arquitectura empresarial de ciberseguridad, los requerimientos de negocio, con el fin de guiar el ejercicio de arquitectura en pro del cumplimiento de la estrategia empresarial.

A continuación se realiza una matriz de requerimientos en Ciberseguridad para los sectores de infraestructuras críticas nacionales, asociando la legislación con los atributos de ciberseguridad afectados. Esta matriz se fundamenta en lo determinado por la propuesta de guía de ciberseguridad creada por el CNO en 2019 (Consejo Nacional de Operación, 2019).

Adicionalmente también se analizará el plan de protección para infraestructuras críticas que contiene la definición de marco de gobierno, roles y responsabilidades generales de cada uno de los grupos definidos, así como el detalle de clasificación de alertas, actuación, notificación, escalamiento y respuesta en eventos de Ciberseguridad contra las ICCN, fundamentados en cinco principios y alineados a unos objetivos nacionales en materia de protección y resiliencia.(Ministerio de Defensa Nacional & Gobierno Nacional, 2017).

Tabla 6 *Integración de la legislación en Ciberseguridad para los sectores de infraestructuras críticas nacionales*

ID	CNO- Guía de Ciberseguridad 2019	Plan de protección para infraestructuras críticas de Colombia 2017	Atributo
L1	Usando la lista de activos críticos desarrollada, cada entidad responsable identificará y documentará sus ciberactivos críticos, esenciales para la operación de los activos críticos	Elaborar y mantener actualizado el inventario de centros de IT/OT, dispositivos y sistemas físicos, software y aplicaciones; mapas de comunicación, flujos de datos y redes, mapa y catálogo de sistemas/ servicios de información interna/externa o de terceros, estableciendo como mínimo su criticidad, función y responsable.	Disponibilidad
L2	Cada entidad responsable deberá implementar actividades de administración de acceso lógico y físico	Identificar y gestionar todas las identidades, credenciales y conexiones remotas, no remotas y físicas a los sistemas IT/OT de la ICCN	Integridad

ID	CNO- Guía de Ciberseguridad 2019	Plan de protección para infraestructuras críticas de Colombia 2017	Atributo
L3	Cada entidad responsable deberá verificar al menos una (1) vez cada semestre calendario que las personas con acceso electrónico activo o acceso físico sin escolta tengan registros de autorización.		Confidencialidad
L4	Cada entidad responsable deberá verificar al menos una (1) vez cada año que el acceso electrónico y/o físico para todas las cuentas de usuario, grupos de cuentas de usuario o categorías de roles de usuario, y sus privilegios asociados específicos sean correctos y que sean los que la entidad responsable determine que sean necesarios.		Confidencialidad

ID	CNO- Guía de Ciberseguridad 2019	Plan de protección para infraestructuras críticas de Colombia 2017	Atributo
L5	Cada entidad responsable implementará y documentará los procedimientos organizacionales y los mecanismos técnicos para el control de acceso en todos los puntos de acceso electrónico al perímetro de seguridad electrónica	Construir o configurar infraestructuras dedicadas o aisladas para los sistemas de control de procesos de seguridad crítica de otros (ej.: IT), siempre que sea posible, minimizando los números de conexiones a estas, garantizando los requerimientos del negocio.	Disponibilidad
L6	La entidad responsable debe implementar un sistema de control intermedio para todas las conexiones remotas interactivas que permita monitorear, cifrar y controlar la autorización con controles de doble factor de autenticación.	Proteger adecuadamente las conexiones entre los sistemas de control de procesos y otros sistemas, con Cortafuegos, protección perimetral, zona neutral, entre otros; así como someter estos controles a adecuados procesos de gestión y supervisión.	Integridad

ID	CNO- Guía de Ciberseguridad 2019	Plan de protección para infraestructuras críticas de Colombia 2017	Atributo
L7	La entidad responsable establecerá, documentará e implementará procedimientos de administración de conexiones temporales dentro del perímetro de seguridad electrónica.	Implementar los procesos y mecanismos para habilitar y deshabilitar las conexiones de acceso remoto, restringiendo las mismas de acuerdo con el máximo requerido; así como llevar a cabo auditorías periódicas de seguridad, junto con las de todos los terceros.	Disponibilidad
L8	La entidad responsable establecerá, documentará e implementará un procedimiento para garantizar que solamente aquellos puertos y servicios requeridos para las operaciones normales y de emergencia	Identificar los puertos protocolos y/o servicios usados por los dispositivos (especialmente dispositivos tales como PLCs y UTR), a fin para deshabilitar los que sean no sean requeridos.	Disponibilidad

ID	CNO- Guía de Ciberseguridad 2019	Plan de protección para infraestructuras críticas de Colombia 2017	Atributo
	sean habilitados en cada punto de acceso de los perímetros de seguridad electrónica.		
L9	La entidad responsable implementará y documentará procedimientos para el monitoreo y registro de accesos lógicos permitidos y denegados en puntos de acceso al (los) perímetro(s) de seguridad electrónica veinticuatro (24) horas al día, siete (7) días por semana.	Monitorear en tiempo real los sistemas IT/OT, los sistemas de seguridad física de la ICCN y las actividades de personal interno y externo, para determinar un comportamiento inusual que podría ser el resultado de un incidente cibernético, entendiendo el vector de ataque y sus métodos, así como evaluar su impacto	Disponibilidad
L10	La entidad responsable deberá utilizar herramientas de prevención contra software malicioso ("malware"), donde sea	Proteger los sistemas de control de procesos con software antivirus en las estaciones de trabajo y los servidores.	Integridad

ID	CNO- Guía de Ciberseguridad 2019	Plan de protección para infraestructuras críticas de Colombia 2017	Atributo
	técnicamente factible, para detectar, prevenir, disuadir y mitigar la introducción, exposición y propagación de malware a todos los ciberactivos dentro del (los) perímetro(s) de seguridad electrónica.	Donde el software no pueda desplegarse, deben ser aplicadas otras medidas de protección (ej., uso de pasarelas o gateways con antivirus o control manual).	
L11	La entidad responsable establecerá y documentará un procedimiento de evaluación de vulnerabilidades para garantizar periódicamente la implementación adecuada de los controles de seguridad electrónica en ciberactivos críticos y perímetros de seguridad electrónica.	Diseñar y realizar gestión de vulnerabilidades a todos los sistemas IT/OT de la ICCN, retroalimentando los resultados en la gestión del riesgo, estableciendo el impacto y medidas de mitigación	Integridad

ID	CNO- Guía de Ciberseguridad 2019	Plan de protección para infraestructuras críticas de Colombia 2017	Atributo
L12	La entidad responsable establecerá y documentará un procedimiento para control de ciberactivos transitorios y medios extraíbles los cuales son usados temporalmente.	Gestionar los dispositivos removibles, sistemas de acceso y demás activos críticos.	Disponibilidad
L13	La entidad responsable deberá implementar y mantener un procedimiento de actualizaciones y parches de seguridad donde sea técnicamente factible.	Implementar los procesos para el despliegue y auditoría de parches de seguridad a los sistemas de IT/OT. Cuando los parches de seguridad no sean posibles o prácticos, deben considerarse medidas alternativas apropiadas de protección	Integridad
L14	La entidad responsable, donde sea técnicamente factible, establecerá un		Integridad

ID	CNO- Guía de Ciberseguridad 2019	Plan de protección para infraestructuras críticas de Colombia 2017	Atributo
	procedimiento para identificar y monitorear eventos del sistema relacionados con ciberactivos.		

3. Flujos de información o Flujos de Bits

Como parte de los flujos de información de un sistema de distribución de energía, y en relación con los procesos de operación y mantenimiento se ilustra el siguiente diagrama mediante el cual se muestra el flujo de información y los sistemas o elementos involucrados y que son objeto de protección en una arquitectura empresarial de ciberseguridad.

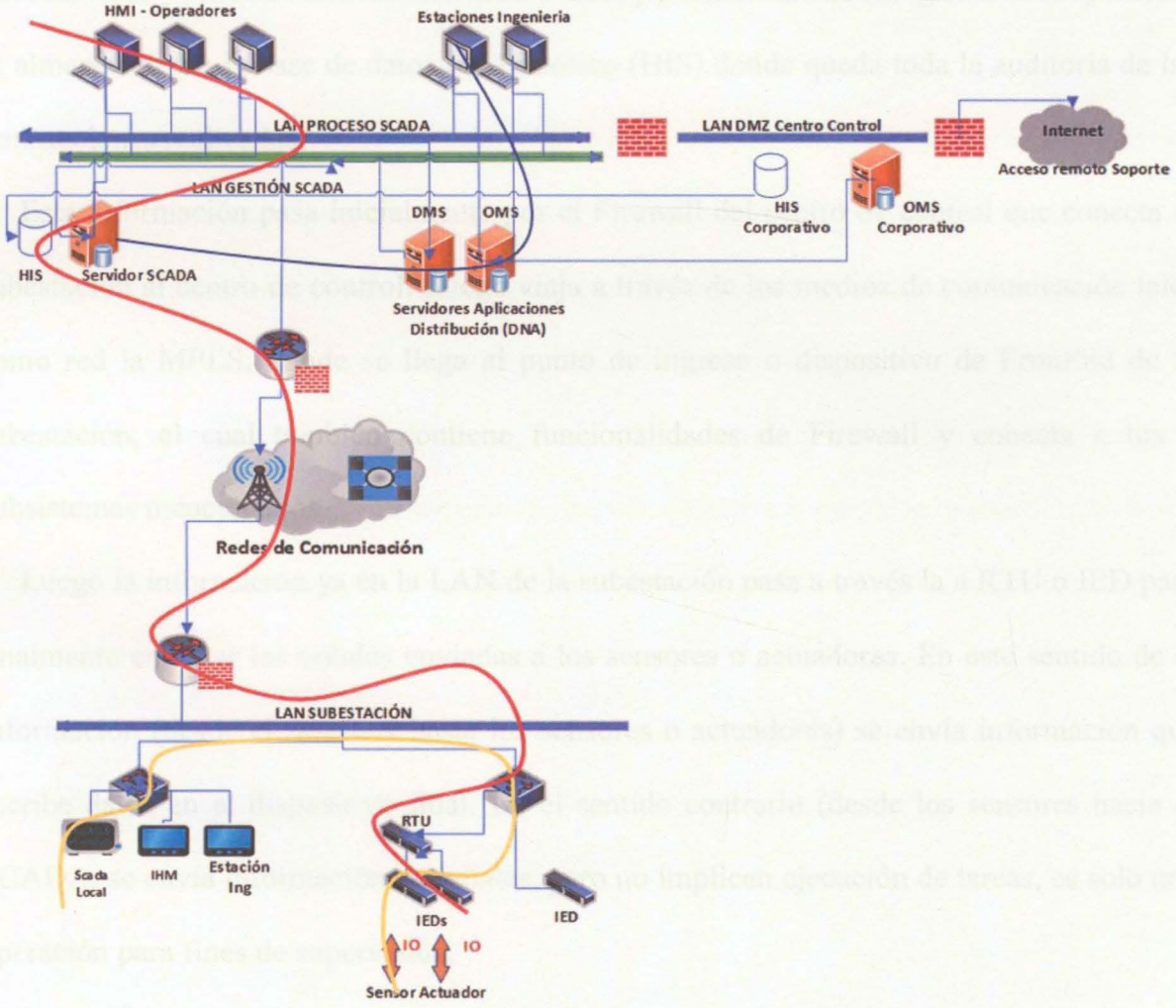

Ilustración 19. Flujos de información para un sistema de distribución de energía. Ilustración propia basada en (Dan, Sandberg, Bj, & Ekstedt, 2012).

Con la información de planeación y programación definida, con el detalle de activos involucrados y análisis de requerimientos para la operación, los operadores proceden a ejecutar las tareas programadas. Los operadores que se encuentran en la LAN del proceso

del SCADA, analizan las solicitudes en el sistema SCADA, analizan el comportamiento del sistema, tales como restricciones y variables del sistema y en caso de que todo funcione adecuadamente, se procede a ejecutar la tarea respectiva.

La ejecución de la tarea implica el ingreso de la información por parte del operador desde las consolas de operación en el sistema SCADA. Esta información es inicialmente procesada en el servidor y base de datos del sistema SCADA y posteriormente el registro de la operación es almacenado en la base de datos del Histórico (HIS) donde queda toda la auditoría de las transacciones realizadas.

Esta información pasa inicialmente por el Firewall del centro de control que conecta la subestación al centro de control. Luego viaja a través de los medios de comunicación tales como red la MPLS, donde se llega al punto de ingreso o dispositivo de FronEnd de la subestación, el cual también contiene funcionalidades de Firewall y conecta a los 2 subsistemas mencionados.

Luego la información ya en la LAN de la subestación pasa a través la a RTU o IED para finalmente entregar las señales enviadas a los sensores o actuadores. En este sentido de la información (desde el SCADA hasta los sensores o actuadores) se envía información que escribe datos en el dispositivo final. En el sentido contrario (desde los sensores hacia el SCADA, se envía información de señales, pero no implican ejecución de tareas, es solo una operación para fines de supervisión.

Otra opción de operación es la local, que sucede en la subestación, sin intervención de operadores desde el centro de control. Esta operación se ejecuta en caso de desconexión con el centro de control, o para tareas específicas de mantenimiento o de operación que deban ser llevadas a cabo localmente. Para esto los operadores a través de la HMI de la subestación operan el SCADA Local y a través de la LAN de la subestación se envían las señales a los

dispositivos o elemento requeridos. Esta información al no salir de la LAN de la subestación no pasa por ningún elemento de seguridad tal como un Firewall, y solo pasa por los elementos de comunicación al interior de la subestación.

El tercer flujo de información presentado en la gráfica anterior hace referencia a la información que se ingresa al sistema desde las estaciones de ingeniería hacia el DMS y OMS, y que finalmente entrega las tareas para ser ejecutadas por los operadores en el SCADA.

El DMS permiten analizar y optimizar las maniobras realizadas, y adicionalmente permite generar informes para proponer acciones de mejora provenientes de los análisis Post-operativos, mientras que el OMS se encarga de toda la gestión asociada a la restauración del servicio. Las funciones de estos módulos pueden o no estar integradas al SCADA de forma directa para su ejecución, pero suponiendo un escenario donde no lo están, las solicitudes, análisis de comportamientos del sistema (como restricciones y variables relevantes), trabajos programados y requerimientos para restaurar el servicio, son analizados y gestionados por estos subsistemas y a partir de estos se genera la programación respectiva de operación.
En relación con los flujos de información, es relevante decir que para este caso la información viaja directamente a través de la VLAN del SCADA y por lo tanto no hay comunicación con elementos externos a esta VLAN.

4. Escenarios de Riesgo

En años recientes se han realizado diversos estudios asociados a la definición de modelos y gestión de riesgos para sistemas ICS, entre estos están los mencionados por (Maglaras et al., 2017) y por (Xie et al., 2013), en los cuales se mencionan algunos de los riesgos relevantes

para sistemas ICS de forma general y se realiza un análisis de vulnerabilidades y una cuantificación de acuerdo con los tipos de acceso y conocimientos ciber requeridos.

Los sistemas de control industrial asociados a la distribución de energía, pueden ser objeto de diversas fuentes de amenazas. De acuerdo con Alexey Poletykin, como parte del establecimiento del contexto para determinar las posibles amenazas en un sistema ICS, las fuentes reales de amenazas cibernéticas pueden ser: terrorista, hacker, virus específico para una computadora objetivo y sabotaje realizado por el hombre. (Poletykin, 2018)

Tomando como base estas definiciones, a continuación se detallan las características de algunas de estas fuentes de amenaza y se clasifican de acuerdo con su capacidad de hacer daño, que es determinada por el conocimiento y posibilidad de ejecutar una acción; luego se determinan los posibles escenarios de riesgos asociados a un sistema de distribución de energía.

Tabla 7. *Fuentes de amenazas para un sistema de distribución de energía.*

ID	Fuente de amenaza	Capacidad para hacer daño	Justificación de la capacidad
F1	Empleados molestos	Alta	Tienen gran conocimiento de la empresa y de la infraestructura
F2	Competidores	Media	No tiene los conocimientos y perfiles avanzados en ciber, pero pueden contratar estos servicios.
F3	Estados enemigos	Alta	Conocimientos y perfiles avanzados en ciber
F4	Hackers	Media	Aunque tiene conocimientos avanzados en Ciber, tienen poca

ID	Fuente de amenaza	Capacidad para hacer daño	Justificación de la capacidad
			experiencia en el campo de las tecnologías de operación.
F5	Terroristas	Media	Pueden no tener directamente los conocimientos requeridos, pero tienen el dinero para contratar los perfiles requeridos
F6	Hacktivistas	Baja	Tiene bajan habilidades en el ciber, se centran en realizar "defacement" de sitios web.
F7	Grupos criminales organizados	Baja	No tienen el conocimiento suficiente para realizar ataques en sistemas de control industrial, se enfocan en otro tipo de sistemas tales como el financiero
F8	Comportamiento de usuario final	Alta	Tienen conocimientos avanzados de sistemas y pueden ejecutar acciones sin intención de realizar daño.

Escenarios de Riesgos

A continuación se proporciona un análisis de escenarios de riesgos a alto nivel, y de manera general para un sistema de control industrial de distribución de energía.

Tabla 8. *Escenarios de riesgos para un sistema de distribución de energía*

ID	Escenario del Riesgo	Fuente de Amenaza	Probabilidad	Impacto
R 1	Falta de monitoreo en la red que permita identificar una posible intrusión	F1,F2,F3,F4,F5,F8	Alta	Alta
R2	Poca o nula actualización de los sistemas o de firmware que genere vulnerabilidades	F3,F4,F5	Alta	Alta
R3	Ejecución no deseada de malware por usuario final	F8	Alta	Alta
R4	Ejecución de amenazas avanzadas persistentes	F3,F5,F8	Media	Alta
R5	Falta de zonificación en la red que habilite la contención de un ataque	F1,F2,F3,F4,F5,F8	Media	Media
R6	Conexión de equipos no autorizados tales como portátiles, dispositivos móviles, y otros similares que permitan acceso a los sistemas de control	F1,F2,F3,F4,F5,F7,F8	Media	Alta
R7	Abuso de privilegios por falta de una de gestión adecuada de	F1,F8	Media	Alta

ID	Escenario del Riesgo	Fuente de Amenaza	Probabilidad	Impacto
	identidades o exceso de los mismos			
R8	Fallos en la configuración o configuraciones por defecto que habiliten el acceso a los sistemas	F2,F3,F4,F5	Media	Alta
R9	Acceso no autorizado a los sistemas de control a través de internet	F2,F3,F4,F5	Media	Alta
R10	Falta de conciencia situacional en ciberseguridad asociada a los sistemas de control industrial para distribución de energía	F1,F2,F3,F4,F5,F8	Media	Media
R11	Envío de información de comandos y medidas en la comunicación en ambas vías entre IED o RTU con el centro de control, en texto claro	F2,F3,F4,F5	Media	Media
R12	Acceso al sistema de control de control a través de la red de TI	F1,F3,F4,F5	Media	Alta
R13	Poco o nulo análisis de vulnerabilidades sobres los sistemas de control industrial	F2,F3,F4,F5	Media	Media

ID	Escenario del Riesgo	Fuente de Amenaza	Probabilidad	Impacto
R14	Intrusión al sistema a través de los canales establecidos con los fabricantes para soporte	F2,F3,F4,F5	Alta	Alta
R15	Intrusión al sistema por desprotección de la infraestructura crítica, al no tener un inventario actualizado de la misma.	F1,F2,F3,F4,F5	Alta	Alta

Capítulo IV. Modelo de Arquitectura de Ciberseguridad Enfocado en Infraestructuras Críticas de Empresas de Distribución de Energía

Desde el punto de vista del framework de arquitectura SABSA, la forma adecuada de generar una arquitectura de ciberseguridad empresarial incluye como entradas la visión y estrategia del negocio representada a través de tecnologías, personas y procesos; la legislación vigente aplicable en términos de ciberseguridad, y desde el punto de vista de los stakeholders la definición de requerimientos y drivers de negocio representados en términos de ciberseguridad. Estos elementos fueron desarrollados en los capítulos 2 y 3 de este trabajo.

A continuación se explica cómo todas estas entradas serán la base para desarrollar el modelo de arquitectura de ciberseguridad propuesto, orientado al cumplimiento de los requerimientos propios de Negocio, como se muestra a continuación:

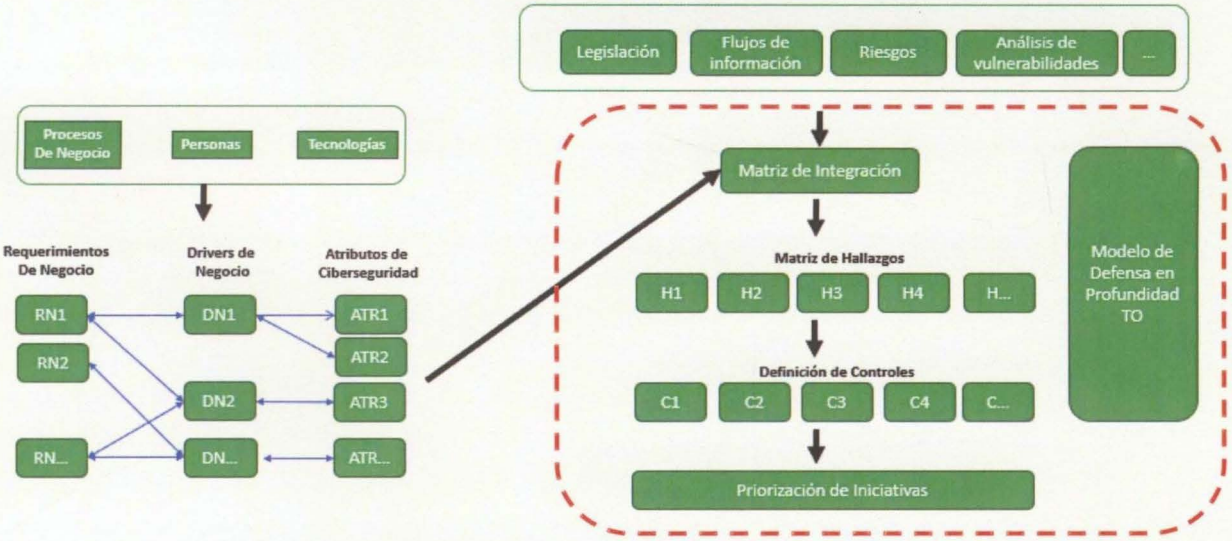

Ilustración 20. Modelo de arquitectura de Ciberseguridad. Elaboración propia

1. Principios de arquitectura usados para este modelo

La defensa en profundidad como concepto se originó en la estrategia militar para proporcionar barreras que impiden el progreso de los intrusos para alcanzar sus objetivos, mientras monitorean su progreso y desarrollan e implementan respuestas al incidente para

repelerlos. En el paradigma de ciberseguridad, la defensa en profundidad se asocia con las medidas de detección y protección diseñadas para impedir el progreso de un intruso cibernético, mientras se habilita a la organización para que detecte y responda a la intrusión con el objetivo de reducir y mitigar las consecuencias de una violación. (Homeland Security, 2016). Adicionalmente desde el estándar IEC 62443 también se define este concepto como relevante en seguridad de sistemas de control industrial y en resumen, como ya fue explicado el capítulo I, se determina que ninguna medida de ciberseguridad por si sola es totalmente segura y que para reducir riesgos se deben implementar múltiples controles para proteger y evitar puntos únicos de fallas.(International Electrotechnical Commission, 2009)

Como principio de arquitectura para este modelo se tomará el definido por la SANS como defensa en profundidad para ICS. (SANS, 2015)

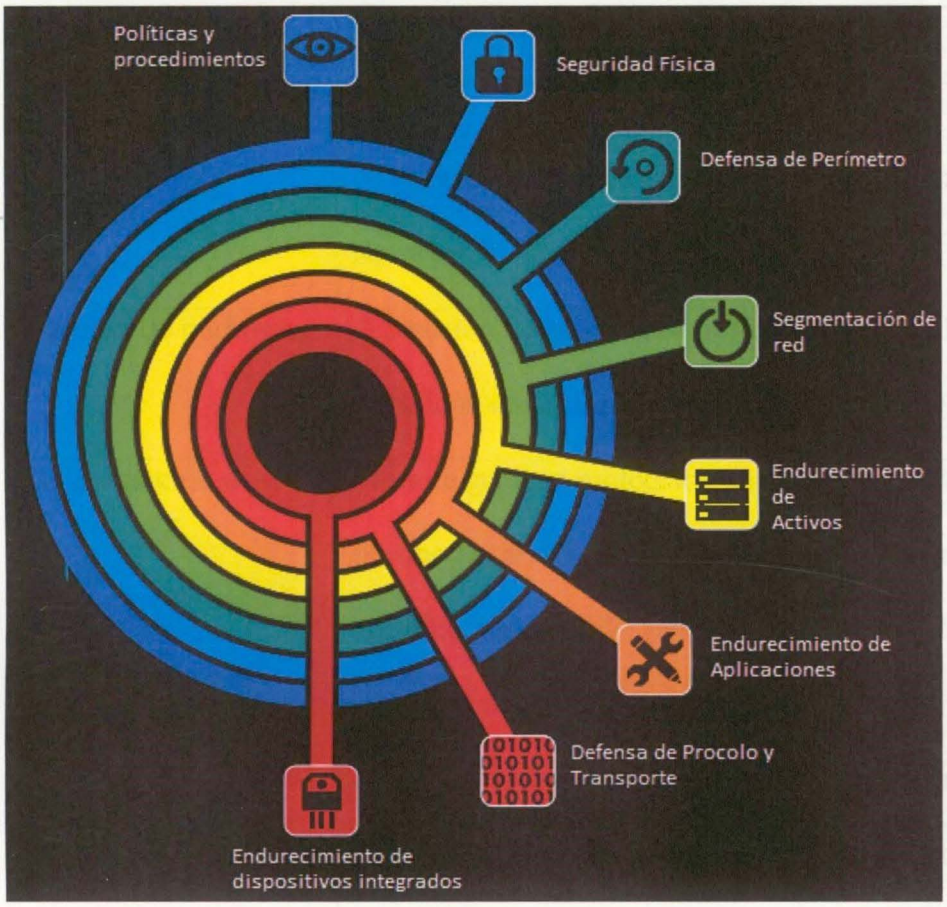

Ilustración 21 Modelo de defensa en profundidad. Traducción del modelo de defensa en profundidad, tomado de la SANS. (SANS, 2015)

A continuación para describir un ejemplo de lo que desarrollará por cada capa, se describen algunos elementos que pueden ser definidos como parte de la estrategia, específicamente para un ICS.

Tabla 9. *Modelo de defensa en profundidad. Elementos de la estrategia.*

Capa	**Elementos de la estrategia**
Políticas y procedimientos	Se encuentra asociada a la creación de recomendaciones, estándares, políticas y procedimientos específicamente para cibserseguridad. (Homeland Security, 2016)

Capa	Elementos de la estrategia
Seguridad Física	Asociado a controles de acceso para centros de control, controles de acceso, barreras, sistemas de videovigilancia. (Homeland Security, 2016)
Defensa de perímetro	Protección de las conexiones que ingresan al perímetro de seguridad electrónica. Por ejm Firewalls, IDS o IPS.
Segmentación de red	Permite generar protección entre los elementos que componen el perímetro de seguridad electrónica. Por ej. microsegmentración, zonificación o DMZ. (Homeland Security, 2016)
Endurecimiento de activos	Aseguramiento de los activos que componen el sistema tales como servidores, estaciones de trabajo y consolas, a través de definición de líneas base, antimalware o control de movimientos laterales.
Endurecimiento de aplicaciones	Separación de aplicaciones por capas, firewall de aplicación, separacion de ambientes, gestión de vulnerabilidades, autenticación, autorización y monitoreo.
Defensa de protocolos y transporte	Integrado con la defensa de perímetro, pueden integrarse controles de tipo IDS para determinar comportamientos anómalos en protocolos de ICS, integrado con monitoreo.
Endurecimiento de dispositivos integrados	Teniendo en cuenta que estos dispositivos no poseen capacidades de ciberseguridad tal como lo permite una estación de trabajo, las posibles acciones a tomar en estos dispositivos

Capa	Elementos de la estrategia
	son deshabilitar puertos o servicios no requeridos o usados y restringir acceso físico. (Homeland Security, 2016)

Nota: Elaboración propia basada en (Abdelghani, 2019)

2. Matriz de hallazgos y controles por cada capa

Como parte fundamental para determinar los hallazgos, y como parte de la metodología de SABSA, a continuación se realiza la matriz de integración entre la legislación aplicable, atributos de seguridad derivados de los drivers de negocio, riesgos y capa del modelo de defensa en profundidad. Adicionalmente todos los ítems que apoyan las variables anteriores son priorizados, ya que al definir controles se mejorará la situación de ciberseguridad de la empresa en mayor proporción, y por lo tanto para dichos elementos se determina que capa de la arquitectura es soportada.

A partir de dicha matriz se determinarán los hallazgos más relevantes que darán lugar a la definición de los controles requeridos.

Tabla 10. *Matriz de integración*

ID Legislación	CNO- Guía de Ciberseguridad Propuesta 2019	Plan de protección para infraestructuras críticas de Colombia 2017	ID Atri-buto	Atributos de Seguridad asociados a Drivers de Negocio	ID Riesgo	Riesgos	Capa
L1	Usando la lista de activos críticos desarrollada, cada entidad responsable identificará y documentará sus ciberactivos críticos, esenciales para la operación de	Elaborar y mantener actualizado el inventario de centros de IT/OT, dispositivos y sistemas físicos, software y aplicaciones; mapas de comunicación, flujos de datos y redes, mapa y catálogo de sistemas/servicios	ATR3	Los ciberactivos asociados a los servicios de TO deben estar plenamente identificados y caracterizados con el fin de garantizar el conocimiento mínimo de la infraestructura a proteger y su	R15	Intrusión al sistema por desprotección de la infraestructura crítica, al no tener un inventario actualizado de la misma.	Defensa de Perímetro

ID Legislación	CNO- Guía de Ciberseguridad Propuesta 2019	Plan de protección para infraestructuras críticas de Colombia 2017	ID Atri-buto	Atributos de Seguridad asociados a Drivers de Negocio	ID Riesgo	Riesgos	Capa
	los activos críticos	de información interna/externa o de terceros. Estableciendo como mínimo su criticidad, función y responsable.		comportamiento base para garantizar el correcto funcionamiento del sistema			
L2	Cada entidad responsable deberá implementar actividades de administración	Identificar y gestionar todas las identidades, credenciales y conexiones remotas, no remotas y físicas a los sistemas	ATR10	El sistema debe interoperar con otros sistemas que adicionalmente pueden tener diversos	R7	Abuso de privilegios por falta de una de gestión adecuada de identidades o	Endurecimiento de activos

ID Legislación	CNO- Guía de Ciberseguridad Propuesta 2019	Plan de protección para infraestructuras críticas de Colombia 2017	ID Atri-buto	Atributos de Seguridad asociados a Drivers de Negocio	ID Riesgo	Riesgos	Capa
	de acceso lógico y físico	IT/OT de la ICCN (infraestructura crítica cibernética nacional)		protocolos industriales, con el fin de compartir información requerida de forma segura e integra.		exceso de los mismos	
L3	Cada entidad responsable deberá verificar al menos una (1) vez cada semestre		ATR6	Cada solicitud de ingreso al sistema debe ser verificada a través de un procedimiento			Seguridad física

ID Legislación	CNO- Guía de Ciberseguridad Propuesta 2019	Plan de protección para infraestructuras críticas de Colombia 2017	ID Atri-buto	Atributos de Seguridad asociados a Drivers de Negocio	ID Riesgo	Riesgos	Capa
	calendario que las personas con acceso electrónico activo o acceso físico sin escolta tengan registros de autorización.			que permita validar que efectivamente quien realiza la solicitud es quien dice ser, evitando la inestabilidad o mala operación del sistema.			
L4	Cada entidad responsable deberá verificar al menos una (1) vez cada año		ATR14	El sistema debe disponer de mecanismos seguros, no propietarios, que	R7	Abuso de privilegios por falta de una de gestión adecuada de	Endurecimiento de activos

ID Legislación	CNO- Guía de Ciberseguridad Propuesta 2019	Plan de protección para infraestructuras críticas de Colombia 2017	ID Atri-buto	Atributos de Seguridad asociados a Drivers de Negocio	ID Riesgo	Riesgos	Capa
	que el acceso electrónico y/o físico para todas las cuentas de usuario, grupos de cuentas de usuario o categorías de roles de usuario, y sus privilegios asociados específicos sean correctos y que sean los que la			permitan compartir información garantizando la integridad de la misma.		identidades o exceso de los mismos	
			ATR15	Se debe garantizar un diseño de ciberseguridad basado en el mínimo privilegio, para evitar que un			

ID Legislación	CNO- Guía de Ciberseguridad Propuesta 2019	Plan de protección para infraestructuras críticas de Colombia 2017	ID Atri-buto	Atributos de Seguridad asociados a Drivers de Negocio	ID Riesgo	Riesgos	Capa
	entidad responsable determine que sean necesarios.			actor malintencionado o no, pueda generar indisponibilidad del sistema.			
L5	Cada entidad responsable implementará y documentará los procedimientos organizacionales y los mecanismos	Construir o configurar infraestructuras dedicadas o aisladas para los sistemas de control de procesos de seguridad crítica de otros (ej.: IT),	ATR13	El sistema debe estar diseñado mediante el uso de capas de ciberseguridad, de forma que existan controles para que caso de	R5	Falta de zonificación en la red que habilite la contención de un ataque	Segmentación de red

ID Legislación	CNO- Guía de Ciberseguridad Propuesta 2019	Plan de protección para infraestructuras críticas de Colombia 2017	ID Atri-buto	Atributos de Seguridad asociados a Drivers de Negocio	ID Riesgo	Riesgos	Capa
	técnicos para el control de acceso en todos los puntos de acceso electrónico al perímetro de seguridad electrónica	siempre que sea posible, minimizando los números de conexiones a estas, garantizando los requerimientos del negocio.		una intrusión, no se permita el acceso a todo el sistema de forma indiscriminada causando indisponibilidad del mismo.			
		Proteger adecuadamente las conexiones entre los sistemas de control de procesos y otros			R9	Acceso no autorizado a los sistemas de control a través de internet	

ID Legislación	CNO- Guía de Ciberseguridad Propuesta 2019	Plan de protección para infraestructuras críticas de Colombia 2017	ID Atri-buto	Atributos de Seguridad asociados a Drivers de Negocio	ID Riesgo	Riesgos	Capa
		sistemas, con Cortafuegos, protección perimetral, zona neutral, entre otros; así como someter estos controles a adecuados procesos de gestión y supervisión			R12	Acceso al sistema de control de control a través de la red de TI	

ID Legislación	CNO- Guía de Ciberseguridad Propuesta 2019	Plan de protección para infraestructuras críticas de Colombia 2017	ID Atri-buto	Atributos de Seguridad asociados a Drivers de Negocio	ID Riesgo	Riesgos	Capa
L6	La entidad responsable debe implementar un sistema de control intermedio para todas las conexiones remotas interactivas que permita monitorear, cifrar y controlar						Defensa de perímetro

ID Legislación	CNO- Guía de Ciberseguridad Propuesta 2019	Plan de protección para infraestructuras críticas de Colombia 2017	ID Atri-buto	Atributos de Seguridad asociados a Drivers de Negocio	ID Riesgo	Riesgos	Capa
	la autorización con controles de doble factor de autenticación.						
L7	La entidad responsable establecerá, documentará e implementará procedimientos de administración de conexiones	Implementar los procesos y mecanismos para habilitar y deshabilitar las conexiones de acceso remoto, restringiendo las mismas de acuerdo	ATR6	Cada solicitud de ingreso al sistema debe ser verificada a través de un procedimiento que permita validar que efectivamente	R14	Intrusión al sistema a través de los canales establecidos con los fabricantes para soporte	Defensa de Perímetro

ID Legislación	CNO- Guía de Ciberseguridad Propuesta 2019	Plan de protección para infraestructuras críticas de Colombia 2017	ID Atri-buto	Atributos de Seguridad asociados a Drivers de Negocio	ID Riesgo	Riesgos	Capa
	temporales dentro del perímetro de seguridad electrónica.	con el máximo requerido; así como llevar a cabo auditorías periódicas de seguridad, junto con las de todos los terceros.		quien realiza la solicitud es quien dice ser, evitando la inestabilidad o mala operación del sistema.			
L8	La entidad responsable establecerá, documentará e implementará un procedimiento	Identificar los puertos protocolos y/o servicios usados por los dispositivos (especialmente dispositivos tales	ATR5	Los ciberactivos deben configurarse de acuerdo con prácticas adecuadas de	R8	Fallos en la configuración o configuraciones por defecto que habiliten el	Endurecimiento de activos

ID Legislación	CNO- Guía de Ciberseguridad Propuesta 2019	Plan de protección para infraestructuras críticas de Colombia 2017	ID Atri-buto	Atributos de Seguridad asociados a Drivers de Negocio	ID Riesgo	Riesgos	Capa
	para garantizar que solamente aquellos puertos y servicios requeridos para las operaciones normales y de emergencia sean habilitados en cada punto de acceso de los perímetros de seguridad electrónica.	como PLCs y UTR), a fin para deshabilitar los que sean no sean requeridos.		ciberseguridad dentro de las cuales se encuentran deshabilitar puertos y servicios no utilizados y gestión de uso de dispositivos autorizados.		acceso a los sistemas	

ID Legislación	CNO- Guía de Ciberseguridad Propuesta 2019	Plan de protección para infraestructuras críticas de Colombia 2017	ID Atri-buto	Atributos de Seguridad asociados a Drivers de Negocio	ID Riesgo	Riesgos	Capa
L9	La entidad responsable implementará y documentará procedimientos para el monitoreo y registro de accesos lógicos permitidos y denegados en puntos de acceso al (los)	Monitorear en tiempo real los sistemas IT/OT, los sistemas de seguridad física de la ICCN y las actividades de personal interno y externo, para determinar un comportamiento inusual que podría ser el resultado de	ATR2	El proceso debe estar monitoreado en línea o por lo menos de forma constante, con el fin de alertar en caso de cambios del comportamiento del mismo y garantizar la integridad de la información.	R1	Falta de monitoreo en la red que permita identificar una posible intrusión	Defensa de Perímetro

ID Legislación	CNO- Guía de Ciberseguridad Propuesta 2019	Plan de protección para infraestructuras críticas de Colombia 2017	ID Atri-buto	Atributos de Seguridad asociados a Drivers de Negocio	ID Riesgo	Riesgos	Capa
	perímetro(s) de seguridad electrónica veinticuatro (24) horas al día, siete (7) días por semana.	un incidente cibernético, entendiendo el vector de ataque y sus métodos, así como evaluar su impacto	ATR11	Los eventos relevantes y/o reconocidos por su calificación negativa, deben ser detectados, reportados y en lo posible deben detenidos de forma automática para evitar indisponibilidad del sistema			

ID Legislación	CNO- Guía de Ciberseguridad Propuesta 2019	Plan de protección para infraestructuras críticas de Colombia 2017	ID Atri-buto	Atributos de Seguridad asociados a Drivers de Negocio	ID Riesgo	Riesgos	Capa
L10	La entidad responsable deberá utilizar herramientas de prevención contra software malicioso ("malware"), donde sea técnicamente factible, para detectar, prevenir, disuadir y	Proteger los sistemas de control de procesos con software antivirus en las estaciones de trabajo y los servidores. Donde el software no pueda desplegarse, deben ser aplicadas otras medidas de protección (ej., uso de pasarelas o gateways con	ATR11	Los eventos relevantes y/o reconocidos por su calificación negativa, deben ser detectados, reportados y en lo posible deben detenidos de forma automática para evitar indisponibilidad del sistema	R3	Ejecución no deseada de malware por usuario final	Endurecimiento de activos
					R4	Ejecución de amenazas avanzadas persistentes	

ID Legislación	CNO- Guía de Ciberseguridad Propuesta 2019	Plan de protección para infraestructuras críticas de Colombia 2017	ID Atri-buto	Atributos de Seguridad asociados a Drivers de Negocio	ID Riesgo	Riesgos	Capa
	mitigar la introducción, exposición y propagación de malware a todos los ciberactivos dentro del (los) perímetro(s) de seguridad electrónica.	antivirus o control manual).					

ID Legislación	CNO- Guía de Ciberseguridad Propuesta 2019	Plan de protección para infraestructuras críticas de Colombia 2017	ID Atri-buto	Atributos de Seguridad asociados a Drivers de Negocio	ID Riesgo	Riesgos	Capa
L11	La entidad responsable establecerá y documentará un procedimiento de evaluación de vulnerabilidades para garantizar periódicamente la implementación adecuada de los controles de seguridad	Diseñar y realizar gestión de vulnerabilidades a todos los sistemas IT/OT de la ICCN, retroalimentando los resultados en la gestión del riesgo, estableciendo el impacto y medidas de mitigación	ATR4	Los ciberactivos deben ser actualizados y parchados de acuerdo con recomendación del fabricante, con el fin de evitar explotación por vulnerabilidades conocidas.	R13	Poco o nulo análisis de vulnerabilidad es sobres los sistemas de control industrial	Endurecimiento de Aplicaciones

ID Legislación	CNO- Guía de Ciberseguridad Propuesta 2019	Plan de protección para infraestructuras críticas de Colombia 2017	ID Atri-buto	Atributos de Seguridad asociados a Drivers de Negocio	ID Riesgo	Riesgos	Capa
	electrónica en ciberactivos críticos y perímetros de seguridad electrónica.						
L12	La entidad responsable establecerá y documentará un procedimiento para control de ciberactivos transitorios y	Gestionar los dispositivos removibles, sistemas de acceso y demás activos críticos.	ATR5	Los ciberactivos deben configurarse de acuerdo con prácticas adecuadas de ciberseguridad dentro de las	R6	Conexión de equipos no autorizados tales como portátiles, dispositivos móviles, y otros similares	Endurecimiento de activos

ID Legislación	CNO- Guía de Ciberseguridad Propuesta 2019	Plan de protección para infraestructuras críticas de Colombia 2017	ID Atri-buto	Atributos de Seguridad asociados a Drivers de Negocio	ID Riesgo	Riesgos	Capa
	medios extraíbles los cuales son usados temporalmente.			cuales se encuentran deshabilitar puertos y servicios no utilizados y gestión de uso de dispositivos autorizados.		que permitan acceso a los sistemas de control	
L13	La entidad responsable deberá implementar y mantener un	Implementar los procesos para el despliegue y auditoría de parches de seguridad a los	ATR5	Los ciberactivos deben configurarse de acuerdo con prácticas	R2	Poca o nula actualización de los sistemas o de firmware que genere	Endurecimiento de activos

ID Legislación	CNO- Guía de Ciberseguridad Propuesta 2019	Plan de protección para infraestructuras críticas de Colombia 2017	ID Atri-buto	Atributos de Seguridad asociados a Drivers de Negocio	ID Riesgo	Riesgos	Capa
	procedimiento de actualizaciones y parches de seguridad donde sea técnicamente factible.	sistemas de IT/OT. Cuando los parches de seguridad no sean posibles o prácticos, deben considerarse medidas alternativas apropiadas de protección		adecuadas de ciberseguridad dentro de las cuales se encuentran deshabilitar puertos y servicios no utilizados y gestión de uso de dispositivos autorizados.		vulnerabilidades	

ID Legislación	CNO- Guía de Ciberseguridad Propuesta 2019	Plan de protección para infraestructuras críticas de Colombia 2017	ID Atri-buto	Atributos de Seguridad asociados a Drivers de Negocio	ID Riesgo	Riesgos	Capa
L14	La entidad responsable, donde sea técnicamente factible, establecerá un procedimiento para identificar y monitorear eventos del sistema relacionados con ciberactivos.		ATR7	Todas las acciones realizadas sobre el sistema deben ser en lo posible registradas, entregando un nivel de detalle requerido por el negocio	R1	Falta de monitoreo en la red que permita identificar una posible intrusión	Defensa de Perímetro

A continuación se describen, a manera de ejemplo, algunos posibles hallazgos y los controles propuestos para cada capa impactada del modelo de defensa en profundidad, de acuerdo con el análisis realizado en la matriz anterior. Se priorizan los ítems que permiten obtener cumplimiento tanto de la legislación, como de los atributos de seguridad y riesgos evaluados.

Tabla 11. *Matriz de hallazgos*

Capa	**Hallazgo**	**Riesgo por hallazgo**	**Atributo afectado**	**Control propuesto**
Defensa de perímetro	No se cuenta con un inventario actualizado de los ciberactivos críticos de TO que permitan su identificación, conocimiento de sus características y comportamiento básico	*Intrusión al sistema por falta de protección adecuada de los ciberactivos o desconocimiento de los mismos	Disponibilidad	Solución de gestión de seguridad para OT, que permita visibilidad del inventario. Algunas soluciones de este tipo entregan tanto el inventario de activos, como el monitoreo de seguridad integrados. Para el despliegue de este control se propone una consola centralizada en la zona de control de proceso, y un sensor que entrega la información de cada subestación integrada al sistema

Capa	Hallazgo	Riesgo por hallazgo	Atributo afectado	Control propuesto
				SCADA. Este es un control de tipo Pasivo. El enfoque pasivo de recopilación y análisis de datos tiene dos fases principales. En la primera fase los datos de tráfico de la red deben capturarse de forma segura. En la segunda fase el tráfico capturado es cargado en herramientas de análisis para identificar: activos en la red, debilidades en seguridad y configuración, y posibles amenazas activas.(Janesko, 2019)

Capa	Hallazgo	Riesgo por hallazgo	Atributo afectado	Control propuesto
	No se cuenta con un mecanismo tecnológico que permita habilitar o deshabilitar accesos de forma temporal de las conexiones con empresas de soporte o Partners	*Ingreso no autorizado al sistema por falta de gestión adecuada de identidades (por ej. ingreso por parte del proveedor)	Disponibilidad	Los proveedores deben ser configurados para tener el mínimo de privilegios. La conexión de los proveedores debe ingresar inicialmente a través del Firewall de TI, y debe realizarse a través de una VPN, utilizando un mecanismo fuerte de autenticación multifactor. Adicionalmente el proveedor debe utilizar otro mecanismo de autenticación multifactor para ingresar a la red de control. El uso de estas cuentas debe ser temporal y estar monitoreado. (NERC, 2011)

Capa	Hallazgo	Riesgo por hallazgo	Atributo afectado	Control propuesto
	No existe un control que permita analizar y monitorear el tráfico entrante al sistema, permitiendo ataques por vulnerabilidades o debilidades existentes	*Posible modificación de los protocolos industriales, para inyectar tráfico malicioso *Posible explotación de vulnerabilidades conocidas permitiendo acceso al sistema *Posible envío de	Disponibilidad	Teniendo en cuenta que los ICS usan protocolos tales como ICCP, DNP3 y Modbus, los IPS e IDS tradicionales del mundo de TI no responden a la necesidad de monitoreo de los eventos maliciosos en la red. (Drias, Serhrouchni, & Vogel, 2015). Por lo tanto se debe contar con IDS específico para sistemas ICS basado en firmas, detección de anomalías, y especificación del comportamiento

Capa	Hallazgo	Riesgo por hallazgo	Atributo afectado	Control propuesto
		tráfico a través de puertos innecesariamente abiertos lo que puede llevar desde un mal funcionamiento en el sistema hasta un ataque que habilite comando y control.		normal de los componentes y protocolos de un ICS.
Segmentación de red	*No existe una definición adecuada de VLANs que permita segmentar y aislar las funciones del proceso de acuerdo con su prioridad e importancia.	*Ingreso no autorizado a segmentos de red que faciliten la ejecución de procesos y acceso administrativo al sistema causando	Disponibilidad	El propósito de la segmentación es proporcionar limitación del flujo de comunicación entre los procesos del sistema.(Nelson, 2019) Entre las principales razones para segmentar las redes se encuentra

Capa	Hallazgo	Riesgo por hallazgo	Atributo afectado	Control propuesto
	No existe una adecuada separación entre la red de TI y la red de TO, incluyendo carencia de zonas funcionales tales como una DMZ y elementos de protección tales como firewall /UTM (Javier & Bertolín, 2012)	captura de tráfico, interrupción en el servicio o daños catastróficos. *Posible propagación de malware o amenazas avanzadas persistentes *Ingreso no autorizado al sistema desde la red de TI *Ingreso no autorizado desde internet a la red de TI, y luego de la red de TI a la red de TO *Ingreso directo desde		reducir la exposición o el ingreso del tráfico de red a un sistema de control y reducir la propagación o salida del tráfico de red de un sistema de control.(IEC, 2019) Para este propósito se proponen controles como ACL, VLAN, IDS, servicios de VPN y servicios Proxy. Se deben crear zonas independientes de acuerdo con las funciones de proceso, donde se debe separar por ej. la VLAN de proceso de la VLAN de gestión. Luego de creada esta segmentación deben crearse las

Capa	Hallazgo	Riesgo por hallazgo	Atributo afectado	Control propuesto
		la red de TI a la red de TO, y no a través de una DMZ		reglas de Firewall que limiten la visualización entre las subredes. Otra aproximación para la segmentación de la red es la definición de zonas y conductos. Una zona es una colección de entidades definida de acuerdo con un base funcional, lógica o física. Un conducto es una agrupación lógica de canales de comunicación entre 2 zonas con requerimientos de seguridad similares.(Machii et al., 2015). De igual manera este concepto de zonas y conductos también es definido desde el estándar IEC

Capa	Hallazgo	Riesgo por hallazgo	Atributo afectado	Control propuesto
				62443.(International Electrotechnical Commission, 2009)
Endurecimiento de activos	No se cuenta con un sistema que permite realizar una gestión adecuada de credenciales locales	*Posible rompimiento de contraseñas por fuerza bruta, debido a contraseñas débiles, o políticas no adecuadas que no obliguen a cambiar de contraseña y no controlen reintento.(Javier & Bertolín, 2012)	Integridad	En la mayoría de las redes ICS, varios usuarios utilizan sistemas diferentes y se debe poder acceder a los sistemas rápidamente según lo requieran las operaciones del sistema. La autenticación corporativa, la autorización y las prácticas de administración de cuentas pueden ser problemáticas para los ICS, porque los ICS están

Capa	Hallazgo	Riesgo por hallazgo	Atributo afectado	Control propuesto
		*Ingreso no autorizado por usuarios que no son autenticados y autorizados antes de obtener acceso. (Obregon, 2015) *Ingreso al sistema utilizando cuentas compartidas lo que no permite un adecuado monitoreo de las acciones en el sistema		"siempre encendidos", por lo que no es una opción viable detener el sistema para que los usuarios cierren sesión y vuelvan a iniciarla.(Homeland Security, 2016) Para los hallazgos asociados con contraseñas débiles, el control debe incluir primero concientización y luego establecimiento de políticas de contraseña fuertes, donde sea técnicamente factible. Adicionalmente para ingreso local o remoto para gestión de dispositivos remotos tales como IED, se propone

Capa	Hallazgo	Riesgo por hallazgo	Atributo afectado	Control propuesto
				la implementación de una solución que le permite a los operadores gestionar a través de conectividad remota un IED. Este tipo de soluciones son comúnmente conocidas como "Secure Access manager" o "SAM" para IEC y permiten además de la autenticación, la autorización a través del modelo RBAC (Control de acceso basado en roles).
	Los usuarios autorizados en el sistema cuentan con privilegios que no requieren para sus funciones o cuentan	*Acceso a funciones no requeridas para un perfil específico que puedan desencadenar en mal	Disponibilidad	Igual que en el caso anterior, se propone acceso basado en roles (RBAC).

Capa	Hallazgo	Riesgo por hallazgo	Atributo afectado	Control propuesto
	con usuarios administradores sin que esa sea su función	funcionamiento del sistema o daños en el sistema. *Movimientos laterales a través del acceso a cuentas administradoras.		
	No se encuentra un software antimalware instalado en los dispositivos que lo soportan (Servidores, estaciones de ingeniería)	*Ejecución de malware o APTs por parte del usuario final, que puede darse por error del usuario. *Posibilidad de propagación de malware o APTs a	Integridad	Los controles propuestos incluyen: *Restringir los privilegios de usuario para asignar solo los necesarios para el rol de cada persona. *Seguimiento de logs de auditoría *Uso de controles de seguridad tipo antimalware donde sea técnicamente factible.(Stouffer et al., 2014)

Capa	Hallazgo	Riesgo por hallazgo	Atributo afectado	Control propuesto
		través de los dispositivos de la red de TO		
	Se encuentran dispositivos con puertos abiertos o servicios disponibles que no son requeridos para la ejecución del proceso	*Posible acceso al sistema a través de los puertos o servicios abiertos, conexión de dispositivos móviles u otros similares, lo que podría permitir acceso de tipo administrador,	Disponibilidad	Los controles propuestos incluyen: *Deshabilitar todos los puertos y servicios no utilizados *Restringir los privilegios de usuario para asignar solo los necesarios para el rol de cada persona.(Stouffer et al., 2014)

Capa	Hallazgo	Riesgo por hallazgo	Atributo afectado	Control propuesto
		captura de tráfico o inestabilidad en el sistema		
	Se encuentran dispositivos configurados por defecto o con cuentas por defecto	*Acceso a dispositivos o sistemas a través de cuentas por defecto o por fallos en la configuración.	Disponibilidad	Auditar configuraciones para evitar cuentas y configuraciones por defecto. Esto puede ser realizado manualmente, pero se sugiere la utilizando de una herramienta de escaneo pasivo que determine esta condición.
	El firmware o software de los ciberactivos críticos no cuenta con versiones actualizadas o parches de seguridad requeridos	*Acceso a dispositivos o sistemas a través de explotación de vulnerabilidades conocidas posibilitando	Integridad	Los controles propuestos incluyen: *Implementar parches de seguridad luego de haberlos probado en un ambiente que simule la realidad

Capa	Hallazgo	Riesgo por hallazgo	Atributo afectado	Control propuesto
		ataques de dominio público. (Homeland Security, 2016)		*Deshabilitar todos los puertos y servicios no utilizados *Restringir los privilegios de usuario para asignar solo los necesarios para el rol de cada persona. *Seguimiento de pistas de auditoría.(Stouffer et al., 2014)
Endurecimiento de aplicaciones	No se cuenta con un análisis de vulnerabilidades sobre los ciberactivos críticos que componen el sistema	*Acceso a dispositivos o sistemas a través de explotación de vulnerabilidades conocidas posibilitando ataques de dominio público. (Homeland Security, 2016)	Disponibilidad Integridad	• Validación del Sistema a través de servicios tales como SHODAN. • Ejecutar herramientas de análisis pasivo. (Samtani, Yu, Zhu, Patton, & Chen, 2016) • En caso de contar con un ambiente de pruebas, ejecutar

Capa	Hallazgo	Riesgo por hallazgo	Atributo afectado	Control propuesto
				sobre dicho ambiente un análisis de vulnerabilidades activo. • Solicitar al proveedor o fabricante inicialmente la solución de los hallazgos críticos o proponer controles complementarios de acuerdo con cada situación presentada.

3. Priorización de Iniciativas

En la matriz descrita anteriormente, se determinó por cada capa de modelo de defensa en profundidad para TO, cuáles son los controles propuestos para fortalecer la arquitectura de ciberseguridad de acuerdo con el análisis realizado. En este punto se determinará cuál debe ser la priorización de dichas iniciativas teniendo en cuenta el impacto desde el punto de vista de soporte para la mitigación del riesgo, los atributos de ciberseguridad y la complejidad de implementación evaluada desde el punto de vista técnico, tiempo de implementación y costos. La priorización generará como resultado la implementación de las iniciativas que tengan mayor impacto y baja complejidad.

El impacto será calificado de 1 a 5, de acuerdo con el aporte de la iniciativa para mitigar el riesgo, donde 1 indica un aporte bajo a la mitigación del riesgo y 5 un aporte fundamental para este fin.

El atributo de Ciberseguridad será calificado con los valores 8, 4, 2 de acuerdo con la importancia del atributo para los sistemas de TO, donde la Disponibilidad tiene un valor de 8, la Integridad tiene un valor de 4 y la Confidencialidad tiene un valor de 2.

La complejidad será calificada de acuerdo con las siguientes variables:

Técnica

- 1: Fácil implementación, no requiere personal adicional, el equipo de ciberseguridad puede realizarlo de manera independiente
- 2: Tiene algunos componentes técnicos complejos, pero son pocos dentro del proyecto de implementación, el equipo de ciberseguridad puede realizarlo de manera independiente

- 3: Tiene elementos de complejidad, el equipo de ciberseguridad no puede realizarlo de manera independiente y requiere el apoyo de personal de soporte del negocio.
- 4: Es compleja, para la implementación el equipo de ciberseguridad requiere el acompañamiento de consultores y de personal de soporte del negocio
- 5: Alta complejidad, para la implementación el equipo de ciberseguridad requiere además del acompañamiento de consultores y personal de soporte, solicitar autorización para mantener durante algún tiempo el sistema por fuera de disponibilidad.

Tiempo

- 1: Tiempo de implementación: inferior a 6 meses
- 2: Tiempo de implementación : 7 a 12 meses
- 3: Tiempo de implementación: 13 a 24 meses
- 4: Tiempo de implementación 25 a 48 meses
- 5: Tiempo superior de implementación a 49 meses

Costos (para una empresa con más de 50 subestaciones):

- 1: Costos de implementación inferiores a 100.000 USD
- 2: Costos de implementación entre 100.000 y 200.000 USD
- 3: Costos de implementación entre 200.000 y 500.000 USD
- 4: Costos de implementación entre 500.000 y 1.000.000 USD
- 5: Costos de implementación superiores a 1.000.000 USD.

Tabla 12. *Matriz de priorización de iniciativas*

ID	Iniciativa	Atributo Ciberseguridad	Impacto	Valor Atributo Ciberseguridad	Total Atributo x Impacto	Complejidad			
						Técnica	**Tiempo**	**Costo**	**Complejidad**
1	Implementación de solución para gestión de seguridad de activos y dispositivos	Disponibilidad	5	8	40	5	4	4	80
2	Configuración de VPN con proveedores y otros externos	Disponibilidad	4	8	32	1	1	2	2
3	Implementación de doble factor para autenticación con proveedores	Disponibilidad	5	8	40	2	2	2	8
4	Implementación de solución IDS para	Disponibilidad	5	8	40	5	4	4	80

ID	Iniciativa	Atributo Ciberseguridad	Impacto	Valor Atributo Ciberseguridad	Total Atributo x Impacto	Complejidad			
						Técnica	**Tiempo**	**Costo**	**Complejidad**
	monitoreo de ciberactivos críticos								
5	Definición e Implementación de ACLs	Disponibilidad	3	8	24	2	1	1	2
6	Definición e implementación de VLANs o zonas	Disponibilidad	5	8	40	3	2	3	18
7	Implementación de RBAC para gestión de usuarios	Integridad	3	4	12	4	3	3	36
8	Implementación de soluciones antimalware	Integridad	5	4	20	3	2	3	18

ID	Iniciativa	Atributo Ciberseguridad	Impacto	Valor Atributo Ciberseguridad	Total Atributo x Impacto	Complejidad			
						Técnica	**Tiempo**	**Costo**	**Complejidad**
	para ICS (donde sea técnicamente factible)								
9	Análisis y gestión asociada a puertos y servicios que no estén en uso para los dispositivos de TO	Disponibilidad	5	8	40	2	2	1	4
10	Gestión de cuentas y configuración por defecto en los dispositivos de TO	Disponibilidad	5	8	40	2	2	1	4
11	Implementación de parches de seguridad y actualización de	Integridad	5	4	20	3	3	3	27

ID	Iniciativa	Atributo Ciberseguridad	Impacto	Valor Atributo Ciberseguridad	Total Atributo x Impacto	Complejidad			
						Técnica	**Tiempo**	**Costo**	**Complejidad**
	Firmware donde sea técnicamente factible								
12	Implementación de soluciones de escaneos de vulnerabilidades pasivas	Disponibilidad	5	8	40	3	1	2	6

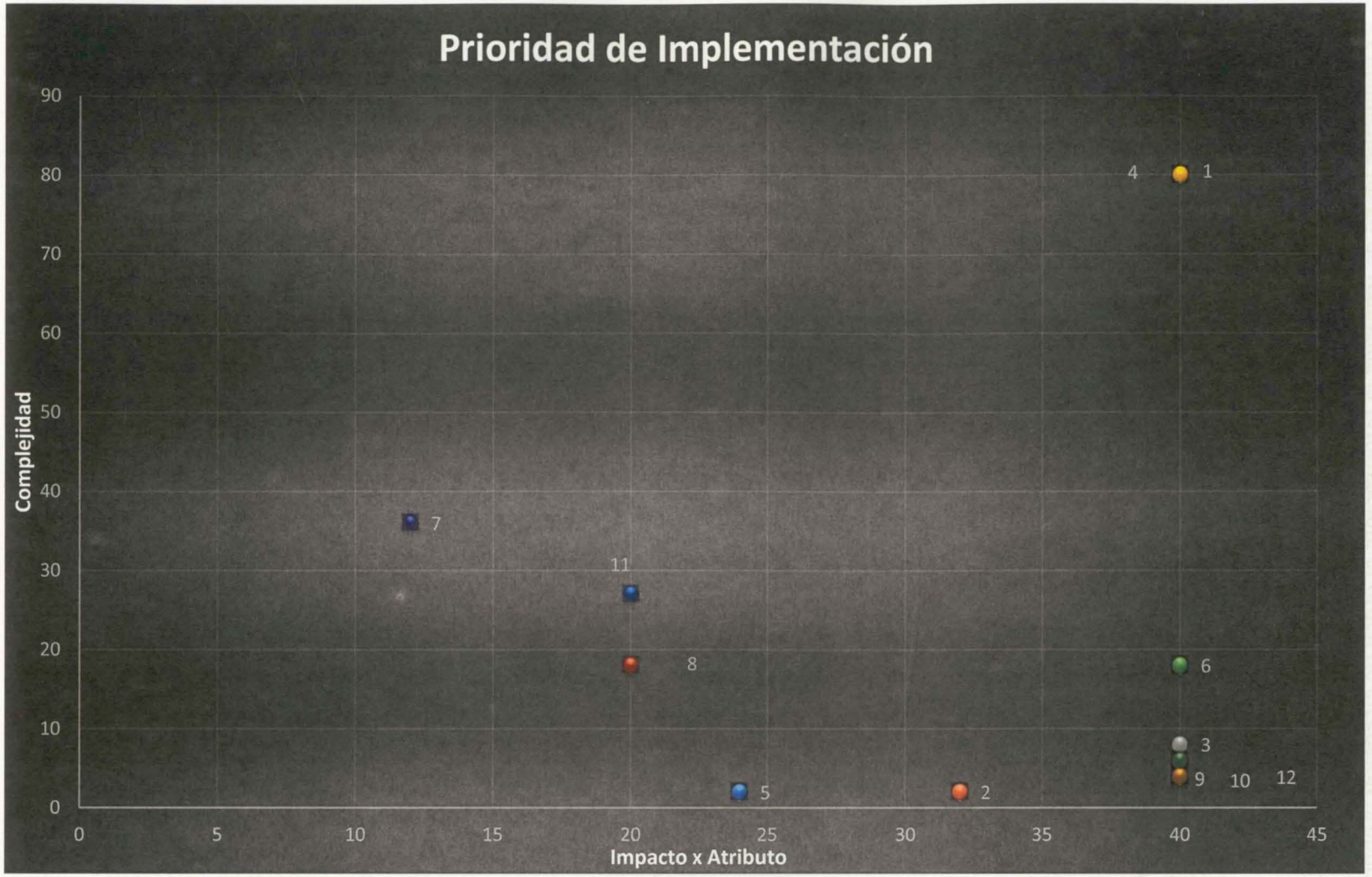

Ilustración 22. Priorización de iniciativas de Ciberseguridad

Finalmente luego de realizada la priorización, el orden de ejecución propuesto de iniciativas con mayor impacto x atributo (mayor a 30) y menor complejidad (menor de 40) sería el siguiente:

Tabla 13. *Orden de Implementación de iniciativas*

ID	Iniciativa	Impacto x Atributo	Complejidad
9	Análisis y gestión asociada a puertos y servicios que no estén en uso para los dispositivos de TO	40	4
10	Gestión de cuentas y configuración por defecto en los dispositivos de TO	40	4
12	Implementación de soluciones de escaneos de vulnerabilidades pasivas	40	6
3	Implementación de doble factor para autenticación con proveedores	40	8
6	Definición e implementación de VLANs o zonas	40	18
2	Configuración de VPN con proveedores y otros externos	32	2

El resto de las iniciativas puede ser ejecutadas en el siguiente orden:

1	Implementación de solución para gestión de seguridad de activos y dispositivos	40	80
4	Implementación de solución IDS para monitoreo de ciberactivos críticos	40	80
5	Definición e Implementación de ACLs	24	2

ID	Iniciativa	Impacto x Atributo	Complejidad
8	Implementación de soluciones antimalware para ICS (donde sea técnicamente factible)	20	18
11	Implementación de parches de seguridad y actualización de Firmware donde sea técnicamente factible	20	27
7	Implementación de RBAC para gestión de usuarios	12	36

Conclusiones

Durante el desarrollo de este trabajo se logró identificar los diferentes tipos de arquitecturas para sistemas de control industrial (ICS) y diferentes tipos de arquitectura de ciberseguridad para los sistemas mencionados; con esto se pudo comprobar que muchos de estos modelos se enfocan principalmente en tecnología sin tener en cuenta los drivers del negocio y otras variables relevantes para la toma de decisiones empresariales.

Adicionalmente se realizó una identificación de los procesos, personas y tecnologías asociadas a empresas de distribución de energía, integrando los anteriores componentes con el fin de obtener un entendimiento del tipo de negocio que se desea proteger y dar prioridad a los ciberactivos críticos relevantes como parte de la arquitectura de Ciberseguridad. Se logró determinar que los componentes de los sistemas de infraestructuras críticas tienen unas condiciones importantes que deben ser tenidas en cuenta a la hora de desarrollar el modelo de arquitectura, tales como la relevancia del atributo de disponibilidad para la prestación del servicio y la especificidad de protocolos y componentes tecnológicos (muy diferentes a los de TI), por lo cual este tipo de arquitecturas no deben ser definidas a la ligera o sin tener en cuenta todos estos factores y variables.

A continuación se realizó una definición de requerimientos y drivers de negocio, que luego fueron mapeados a atributos de seguridad. Esta definición de atributos de seguridad enfocados en la disponibilidad, más la integración de la legislación aplicable a empresas de infraestructuras criticas colombianas, principalmente el acuerdo 1241 del CNO, la visión de riesgos y flujos de información que fueron generados a partir de los principales componentes del sistema, permitieron determinar los insumos requeridos para la definición de arquitectura empresarial de ciberseguridad.

Finalmente, el modelo de arquitectura de Ciberseguridad se desarrolló a partir de la definición de los principios de arquitectura, las matrices de hallazgos que determinaron los controles

propuestos de acuerdo con el modelo de defensa en profundidad y la definición del orden de priorización para implementación de los controles para la protección de las infraestructuras críticas para empresas de distribución de energía.

Con el desarrollo de este trabajo se logró entonces responder a la pregunta de investigación definiendo un modelo de arquitectura de ciberseguridad que tiene en cuenta factores relevantes además de la tecnología, tales como la visión del negocio, los requerimientos de tipo regulatorio y otras variables que permiten visualizar de manera integral todos los componentes y drivers relevantes para una organización. Adicionalmente, se logró establecer un mapa de ruta objetivo que permitió determinar las iniciativas que generan mayor valor para el logro de los objetivos empresariales.

También se pudo determinar que los modelos de arquitectura son artefactos vivos que deben ser actualizados constantemente, y aunque históricamente para las infraestructuras críticas estas actualizaciones se realizaban cada 20 años, los requerimientos de negocio, la legislación vigente y las crecientes amenazas en el ámbito cibernético obligan a su revisión y actualización constante con el fin de ofrecer una protección adecuada.

Recomendación

Como trabajo propuesto para dar continuidad a lo planteado, se plantea la implementación de la segunda parte del modelo SABSA, donde se determinarán detalles de las capas lógica, física y de componentes que entregarán un diseño detallado y que permitirán la implementación de la arquitectura propuesta.

Referencias

Alcaraz, C., & Zeadally, S. (2014). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, *8*(2006), 53–66. https://doi.org/10.1016/j.ijcip.2014.12.002

Araghi, S., & Fardi, M. (2018). *Consideration of the reliability of the SCADA System of North Area Operating Center (NAOC) of Iran*. 1–6.

Cáceres, C. E., & Zea, O. M. (2014). Propuesta de un marco de referencia de gestión de organizaciones usando Arquitectura Empresarial. *Enfoque UTE*, Vol. 5, pp. 70–88. Retrieved from http://ingenieria.ute.edu.ec/enfoqueute/index.php/revista/article/view/48

Campbell, R. J. (2016). Cybersecurity issues for the bulk power system. *Electricity Delivery and Security: Federal Oversight, Activities and Funding*, 63–108.

Cano, J. (2013). La Inseguridad de la Información : Motivador de la Práctica de Cumplimiento Corporativo. *Journal Online Isaca*, *6*, 1–5. Retrieved from http://www.isaca.org/spanish/Pages/default.aspx

Celsia. (2018). *Celsia Reporte integrado 2018*. Retrieved from https://www.celsia.com/Portals/0/Documentos/Reporte_ Integrado_ Celsia_2018.pdf

Challenges, K. (2018). *OT Security Best Practices*. (September).

Codensa S.A.S. (2018). *CODENSA Memoria Anual 2018*. 144. Retrieved from https://www.enel.com.co/content/dam/enel-co/español/accionistas_e_inversionistas/distribución/información_financiera/memorias_anuales/2018/Memoria-anual-Codensa-2018.pdf

Consejo Nacional de Operación. (2015). *Guía de Ciberseguridad.* (788), 21. Retrieved from https://www.cno.org.co/sites/default/files/documentos/acuerdos/ACUERDO 788.PDF

Consejo Nacional de Operación. (2019). *Propuesta Guía de ciberseguridad.* Retrieved from https://cnostatic.s3.amazonaws.com/cno-public/archivosAdjuntos/propuesta_guia_de_ciberseguridad_para_comentarios.pdf

Dan, G., Sandberg, H., Bj, G., & Ekstedt, M. (2012). *Challenges in Power System Information Security*. 1–13.

Dempsey, K., White, G., & Ricke, D. (2014). Summary of NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. *NIST Computer Security Division*. https://doi.org/10.6028/NIST.SP.800-53r4

Drias, Z., Serhrouchni, A., & Vogel, O. (2015). *Analysis of Cyber Security for Industrial Control Systems*. (January 2016). https://doi.org/10.1109/SSIC.2015.7245330

EPM. (2016). *Modelo de Procesos Grupo EPM.* Retrieved from https://www.epm.com.co/site/Portals/0/documentos/modelo-procesos -grupo-epm-n1-n2-publicado.pdf?ver=2017-10-12-164738-650

EPM. (2017). *Lineamiento 2017-lingg-20 Sistema de Gestión Seguridad de la Información y Ciberseguridad.* 2–3. Retrieved from https://www.epm.com.co/site/Portals/0/documentos/politicas/lineamientos-sgsi-ciberseguridad-gg(20170503).pdf?ver=2018-11-16-164429-763

Fan, X., Fan, K., Wang, Y., & Zhou, R. (2015). Overview of cyber-security of industrial control system. *2015 International Conference on Cyber Security of Smart Cities, Industrial Control*

System and Communications, SSIC 2015 - Proceedings. https://doi.org/10.1109/SSIC.2015.7245324

Flórez, A., Calvo, J. A., & Parada, D. J. (2011). *MODELO DE ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN – MASI*.

Hahn, A., Thomas, R. K., Lozano, I., & Cardenas, A. (2015). A multi-layered and kill-chain based security analysis framework for cyber-physical systems. *International Journal of Critical Infrastructure Protection*. https://doi.org/10.1016/j.ijcip.2015.08.003

Hernandez Sampieri, R., Fernandez Collado, C., & Baptista Lucio, M. del P. (2010). Metodología de la investigación. In *Metodología de la investigación*. https://doi.org/- ISBN 978-92-75-32913-9

Homeland Security. (2016). Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies. *Ics-Cert*, (September), 1–48. Retrieved from https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf%0Ahttps://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf

Hurd, C. M., & McCarty, M. V. (2017). *A Survey of Security Tools for the Industrial Control System Environment*. https://doi.org/10.2172/1376870

IEC. (2019). *Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components*.

Information Systems Audit and Control Association (ISACA). (2015). Developing a Common Understanding of Cybersecurity. *Isaca Journal*, *6*. Retrieved from

https://www.isaca.org/Journal/archives/2015/volume-6/Pages/developing-a-common-understanding-of-cybersecurity.aspx

International Electrotechnical Commission. (2009). *IEC/TS 62443-1-1 Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*.

ISA. (2017). *Reporte integrado de gestión 2015*. 45–51. https://doi.org/10.1017/CBO9781107415324.004

Janesko, J. (2019). Passive Analysis of Process Control Networks. *SANS Institute*.

Javier, P., & Bertolín, A. (2012). *Mejora de la protección de la seguridad de los sistemas SCADA utilizados en el control de procesos industriales*. 60–70.

Jiang, J. R. (2017). An improved Cyber-Physical Systems architecture for Industry 4.0 smart factories. *Proceedings of the 2017 IEEE International Conference on Applied System Innovation: Applied System Innovation for Modern Technology, ICASI 2017*, 918–920. https://doi.org/10.1109/ICASI.2017.7988589

Katam, I. (2015). Applicability of Domain Based Security Risk Modeling to SCADA Systems. *2015 World Congress on Industrial Control Systems Security (WCICSS)*, 66–69. https://doi.org/10.1109/WCICSS.2015.7420327

Kim, B., Kang, D., Na, J., Chung, T., & Work, A. R. (2016). Abnormal Traffic Filtering Mechanism for Protecting ICS Networks. *2016 18th International Conference on Advanced Communication Technology (ICACT)*, 436–440. https://doi.org/10.1109/ICACT.2016.7423422

Ku, R., Vp, S., Iot, C., Development, M., Kam, W., & Manager, T. M. (2017). *Trend Micro Cybersecurity Reference Architecture for Operational Technology*. 1–13.

Machii, W., Kato, I., Koike, M., Matta, M., Aoyama, T., & Naruoka, H. (2015). Dynamic Zoning Based on Situational Activitie for ICS Security. *2015 10th Asian Control Conference (ASCC)*, 1–5. https://doi.org/10.1109/ASCC.2015.7244717

Maglaras, L. A., Janicke, H., Wood, A., & He, Y. (2017). A security architectural pattern for risk management of industry control systems within critical national infrastructure. *International Journal of Critical Infrastructures*, *13*(2/3), 113. https://doi.org/10.1504/ijcis.2017.10009242

McMillan, R., & Scholtz, T. (2018). *Definition : Security Architecture*. (April).

Michael Horkan. (2015). Challenges for IDS / IPS Deployment in Industrial. *Information Security Reading Room*.

Ministerio de Defensa Nacional, & Gobierno Nacional. (2017). *Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia PNPICCN V 1 . 0*. 1–51.

MinTIC, MDN, DNI, & DNP. (2016). *Consejo Colombiano de la Politica Ecnomica y Social-Politica Nacional de Seguridad Digital CONPES 3584*.

Montanari, L., & Querzoni, L. (2014). Critical Infrastructure Protection : Threats , Attacks and Countermeasures. *Tenace*.

Nelson, N. (2019). The Impact of Dragonfly Malware on Industrial Control. *SANS Institute*.

NERC. (2011). *Guidance for Secure Interactive Remote Access*. (July).

Obregon, L. (2015). Secure Architecture for Industrial Control Systems. *SANS Institute*.

Poletykin, A. (2018). Cyber security risk assessment method for scada of industrial control systems. *2018 International Russian Automation Conference, RusAutoCon 2018*, 1–5. https://doi.org/10.1109/RUSAUTOCON.2018.8501811

SABSA. (2015). *SABSA Chartered Architect Security Strategy & Planning*. 1–166.

Samtani, S., Yu, S., Zhu, H., Patton, M., & Chen, H. (2016). Identifying SCADA Vulnerabilities Using Passive and Active Vulnerability Assessment Techniques. *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, 25–30. https://doi.org/10.1109/ISI.2016.7745438

SANS. (2015). *The Sliding Scale of Cyber Security*.

Sherwood, J., Clark, A., & Lynas, D. (2005). Enterprise Security Architecture: A Business-Driven Approach. In *Computer Security Journal*.

Shirali, S., Ensafi, S., & Naseri, M. (2010). RTU Hardware Design for SCADA Systems Using FPGA. *2010 International Conference on Computer Applications and Industrial Electronics*, (Iccaie), 115–119. https://doi.org/10.1109/ICCAIE.2010.5735058

Shore, M., & Deng, X. (2010). Architecting Survivable Networks using SABSA. *2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)*, 1–7. https://doi.org/10.1109/WICOM.2010.5601323

Siemens. (2014). *Intelligent control center technology*.

Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., & Hahn, A. (2014). *NIST Special Publication 800-82 Revision 2 Initial Public Draft Guide to Industrial Control Systems (ICS) Security Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems*

(DCS), and Other Control System Configurations such as. 255. Retrieved from https://goo.gl/JRArRW

The Open Group. (2016). Open Group Guide Integrating Risk and Security within a TOGAF ® Enterprise Architecture. *Security Forum (a Forum of The Open Institute Group)*.

Xie, F., Lu, T., Guo, X., Liu, J., Peng, Y., & Gao, Y. (2013). Security analysis on cyber-physical system using attack tree. *Proceedings - 2013 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP 2013*, 429–432. https://doi.org/10.1109/IIH-MSP.2013.113