ANÁLISIS DEL ESTADO DE LA CIBERSEGURIDAD EN LOS SISTEMAS SCADA EN EL SECTOR ELECTRICO COLOMBIANO.

MICHELLE DAYANNA CASTELLANOS FORERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUÉ
2022

ANÁLISIS DEL ESTADO DE LA CIBERSEGURIDAD EN LOS SISTEMAS SCADA EN EL SECTOR ELECTRICO COLOMBIANO.

MICHELLE DAYANNA CASTELLANOS FORERO

MONOGRAFÍA PRESENTADO PARA OPTAR POR EL TITULO DE ESPECIALISTA EN SEGURIDAD INFORMATICA

MSC. KATERINE MARCELES
DIRECTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUÉ
2022

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ibagué, 30 de Marzo del 2022

DEDICATORIA

A todo aquel que crea en sí mismo, que quiere luchar por mejorar su vida, por ampliar sus conocimientos, creen en sí mismo es el impulso más grande, el reto más fuerte pero que al final dará la satisfacción más placentera.

AGRADECIMIENTOS

A todos aquellos que con su tiempo, ánimo y comprensión me dieron apoyo para sacar esta meta personal y profesional adelante, el apoyo del entorno es una fuente de energía que impulsa para seguir y no desfallecer.

CONTENIDO

LISTA DE FIGURAS

Pág.

GLOSARIO

CPS (Cyber Physical Systems o Sistemas Ciberfísicos): integra capacidades de computación, almacenamiento y comunicación junto con capacidades de seguimiento y/o control de objetos en el mundo físico. Los sistemas ciberfísicos a menudo están interconectados y, a su vez, conectados al mundo virtual de una red digital global.

CIBERSEGURIDAD: también se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. Es la práctica de proteger computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes y datos de ataques maliciosos.

CREG (Comisión de Regulación de Energía y Gas): es una entidad regulatoria que tiene como objetivo permitir que los servicios de energía eléctrica, gas natural, gas licuado de petróleo (GLP) y combustibles líquidos sean prestados al mayor número posible de personas y en el menor costo posible para los usuarios y así mismo haya una retribución proporcionada para las empresas que se encargan de garantizar la calidad, cobertura y expansión de los servicios.

DELITO CIBERNÉTICO: son todos aquellos que se cometen haciendo uso equipos informáticos, internet y en ocasiones, también *software* malicioso o *malware* del tipo troyano.

DESENERGENIZACIÓN: corte parcial o total del suministro de energía eléctrica, normalmente efectuada con el fin de realizar reparaciones, adiciones o extensiones de los mismos de manera segura.

DISPOSITIVO ELECTRÓNICO: Consiste en un grupo de componentes electrónicos organizados en un circuito el cual está diseñado para controlar y explotar señales eléctricas. A diferencia de los dispositivos eléctricos, los dispositivos electrónicos usan electricidad para almacenar, transmitir o transformar información.

INFRAESTRUCTURA INFORMÁTICA: El conjunto de software y hardware del que dependen los servicios de una organización permiten responder eficazmente las necesidades de los consumidores, actualizar los planes de control o seguimiento y mejorar la colaboración con proveedores y clientes.

INTERFAZ: el conjunto de elementos de la pantalla que permiten al usuario realizar acciones sobre el Sitio Web que está visitando. Por lo mismo, se considera parte de la interfaz a sus elementos de identificación, de navegación, de contenidos y de acción.

RED ELECTRICA: es la que se encarga de suministrar electricidad a los consumidores. Sus inicios fueron durante la Revolución Industrial y a día de hoy dan

servicio a millones de hogares. Thomas Edison fue el que inventó el sistema de red eléctrico que suministraba energía para la iluminación.

RED FIBRA OPTICA: también conocidos como cables ópticos o cables de fibra óptica, la fibra óptica es la tecnología empleada para transmitir información en forma de pulsos de luz mediante hilos de fibra de vidrio o plástico, a través de largas distancias, debido a que no presenta componentes metálicos, no se ven afectados por la interferencia magnética (es decir, condiciones climatológicas), lo que puede reducir la velocidad de transmisión y se acoplan de manera correcta para trabajar cerca de tramos de red eléctricos, sin sufrir alteración en la trasmisión de información**.**

RED INTELIGENTE: Es una red de telecomunicaciones creada al agregar un entorno informático a una red conmutada tradicional, quedando esta con una infraestructura que permita la creación y prestación de servicios de valor agregado, permitiendo el fácil mantenimiento y administración de la misma.

SCADA: Proviene del inglés "Supervisory Monitoring and Data Collection". Esto significa que un sistema de este tipo que es destinado a la monitorización y control remoto de instalaciones puede integrar en un mismo lugar los datos recogidos de diferentes sensores, PLCs (PLCs) y dispositivos a través de diferentes protocolos. Estas lecturas se toman en tiempo real y se pueden registrar. Además de esto, SCADA también proporciona otras funciones como veremos más adelante.

SEGURIDAD INFORMÁTICA: Este es un sistema encargado de proteger la integridad y confidencialidad de la información almacenada en los sistemas informáticos. En ambos casos, no existe ninguna tecnología que garantice la inviolabilidad del sistema.

SISTEMA INFORMATICO: es una herramienta que permite el almacenamiento y el proceso de información, para lo cual se vale de un grupo de elementos que se relacionan entre sí. Estos elementos no son otros que el *hardware*, el *software* y finalmente el usuario, quien es el que requiere de la información procesada, y quien es también el que en definitiva tiene el control total de lo que sucede.

SMART GRID**:** son básicamente redes de distribución eléctrica combinadas con modernas tecnologías de información, que proporcionan datos tanto a las empresas distribuidoras de electricidad como a los consumidores. Este es un ganar-ganar para ambas partes, a pesar de la operación de esta red de distribución inteligente. Más complicado que la red eléctrica actual.

SUPLANTACION DE IDENTIDAD: Es una actividad perjudicial que incluye hacerse pasar por otros por varias razones, cometer algún tipo de fraude, obtener datos de manera ilegal, cometer acoso cibernético o *ciberbullying o grooming,* este último considero la manera de conseguir la confianza de un menor para poder abusar sexualmente de él.

TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC): Se centra en el papel de la comunicación de manera equiparada, la integración de las telecomunicaciones (líneas telefónicas y señales inalámbricas) y las computadoras, así como el software, el middleware, los sistemas de almacenamiento y los medios necesarios para que los usuarios puedan acceder, almacenar, transmitir y procesar la información.

TECNOLOGÍAS DE OPERACIÓN (TO): Tecnología basada en la optimización de procesos para obtener los mismos resultados que de manera que es el método más efectivo y/o eficiente

TELEOPERACION: indica la operación de un sistema o máquina a distancia. Es similar en significado a la frase "control remoto", pero generalmente se encuentra en entornos de investigación, académicos y técnicos.

RESUMEN

Esta monografía está enfocada en los delitos cibernéticos y amenazas que pueden estar presentes hoy en día en el sector eléctrico colombiano con la implementación en auge de sistemas *SCADA*, los cuales se están convirtiendo en una gran amenaza en varios países.

Esto requiere el desarrollo por parte de los operadores de redes eléctricas, de un mecanismo de defensa frente a estos ataques para tratar de evitarlos antes de que ocurran, poder mitigarlos cuando ocurren y evitar la posibilidad de ataques recurrentes, teniendo en cuenta que dicha infraestructura es catalogada como crítica, ya que una falla en su operación afecta a la comunidad en general, incluyendo sectores bancarios, transporte, salud, acueductos y demás. Inclusive, un ataque a este tipo de infraestructura podría llegar a dejar sin servicio al país completo.

Es así como el presente trabajo se centrará en conocer las vulnerabilidades en cuanto a ciberseguridad a las que se enfrentan las empresas de energía, para poder analizar las soluciones que se han brindado para subsanar dichas debilidades que puedan convertirse en ataques reales y que puedan afectar la infraestructura eléctrica.

Es importante recordar que las amenazas surgen con el desarrollo e implementación de nuevas tecnologías, por lo que se considera un problema nuevo y por lo que es difícil para las empresas de energía actuar, debido a la falta de experiencia y conocimiento sobre el tema.

El propósito de esta indagación es complementar los planes generales de ciberseguridad para el área de la industria de energía.

ABSTRACT

This monograph is focused on cyber crimes and threats that may be present today in the Colombian electricity sector with the booming implementation of SCADA systems, which are becoming a great threat in several countries.

This requires the development by power grid operators of a defense mechanism against these attacks to try to prevent them before they occur, to be able to mitigate them when they occur and to avoid the possibility of recurring attacks, taking into account that said infrastructure is cataloged as critical, since a failure in its operation affects the community in general, including banking, transportation, health, aqueducts and others. Even an attack on this type of infrastructure could leave the entire country without service.

This is how this work will focus on knowing the vulnerabilities in terms of cybersecurity that energy companies face, in order to formulate solutions for said attacks; planning some attacks that may affect the electrical infrastructure, analyzing vulnerabilities.

It is important to remember that this type of threat arises with the development and implementation of new technologies, which is why it is considered a new problem and therefore it is difficult for energy companies to act, due to the lack of experience and knowledge on the subject. .

The purpose of this inquiry is to complement the general cybersecurity plans for the energy industry area.

INTRODUCCIÓN

Los delitos informáticos han tenido un incremento considerable en los últimos años, esto debido a los avances significativos que ha experimentado las tecnologías de la información y la comunicación ocupando un lugar fundamental en las organizaciones, debido a este auge de los sistemas digitales se ha propiciado un ambiente para que los ciberdelincuentes aprovechen y logren ingresar ilícitamente a los sistemas de información confidencial de las empresas y así poder realizar sus ciberataques.

Es una realidad que el sector que se ha visto afectado por estos cibercrímenes en los últimos años es el eléctrico, por este motivo en la presente monografía busca examinar las amenazas y vulnerabilidades más usuales que tienen que afrontar las empresas de energía colombiana al implementar sistemas SCADA, analizando los ataques presentados en otras regiones y la manera adecuada de subsanar las vulnerabilidades, con el fin de evidenciar los riesgos de integridad a los que se pueden enfrentar las empresas.

Se plantea como objetivo general el analizar el estado de la ciberseguridad en los sistemas SCADA en el sector eléctrico colombiano teniendo en cuenta las recomendaciones internacionales de protección contra ataques cibernéticos que podrá implementar con el fin de mitigar el impacto de estos. Dentro de los objetivos específicos se pretende el poder llegar a determinar la importancia de la ciberseguridad aplicada en los sistemas SCADA, también examinar las amenazas y vulnerabilidades más usuales a las que están se afrontan las empresas de energía colombiana al implementar sistemas SCADA y finalmente proponer recomendaciones para la gestión de la seguridad.

De manera general el contenido de esta monografía incluye y define la problemática y su respectiva formulación, el marco referencial que está comprendido por el marco teórico y conceptual para continuar con el respectivo marco legal, el diseño metodológico, el desarrollo de los objetivos para culminar con las conclusiones y recomendaciones de la temática.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La Industria 4.0 y su objetivo de aumentar la competitividad de la industria manufacturera y la creciente integración con los sistemas Ciberfisico (CPS), donde este último se define como la integración de las máquinas inteligentes, la conexión a internet y la interacción humana, ha hecho que se implemente la conexión entre los objetos cotidianos y sistemas digitales a través de sensores inalámbricos, redes de fibra óptica e internet en general, permitiendo así que haya una transferencia de información de dichos objetos como su estado, entorno, procesamiento o hasta la necesidad de un mantenimiento.

Haciendo un recorrido histórico reciente de los ciberataques que han sido más representativos se puede mencionar el ocurrido contra: “la red eléctrica de Ucrania, el cual, fue víctima de una ataque tipo *malware*, no confirmado, denominado *Industroyer* (un juego de palabras que equivaldría a destructor de industrias). Diseñado para infiltrarse en un sistema y controlar los interruptores automáticos de potencia de una subestación eléctrica”[1].

“No se sabe con precisión como *Industroyer* logro llegar a las estaciones de trabajo por medio de las cuales se controlaba la infraestructura critica, en especial su sistema SCADA; pero un análisis del caso permitió identificar que *malware* encuentra hardware que pueda deshabilitar y utiliza un proceso bastante inteligente: envía datos a los servidores de control que se ocultan usando el ofuscador de identificación conocido como Tor y espera para comunicarse fuera del horario de trabajo”[2].

Ha salido a la luz que: “Un colectivos de hackers se ha apoderado de los ordenadores de un centro de control de energía para sumir a partes de Kiev (Ucrania) en la oscuridad. Todo indica que el hacker está enviando malware por correo electrónico a los trabajadores de las instalaciones, lo que les permitió robar sus contraseñas y desconectar las subestaciones de la red. Al final del ataque, como resultado dio lugar a un bloqueo de 200 megavatios de capacidad, que corresponde a aproximadamente del 20% del consumo eléctrico nocturno de la ciudad”.[3]

Se sabe que otro ataque realizado por Estados Unidos afectó la capacidad de Irán para disparar a los petroleros en el Golfo Pérsico. “El ataque se consideró ofensivo

[1] CONDLIFFE, Jamie. El virus del apagón en Ucrania es "la mayor amenaza" informática desde 2009. [Citado el 15 de noviembre de 2020] Disponible en Internet: https://www.technologyreview.es/s/7951/el-virus-del-apagon-en-ucrania-es-la-mayor-amenaza-informatica-desde-2009

[2] Ibid pág. 1.

[3] Ibid pág. 2

e interrumpió los sistemas informáticos de Irán, que se utilizan para controlar misiles y lanzamientos de misiles contra petroleros, y el ataque afectó la capacidad de Teherán para atacar el tráfico marítimo en el Golfo Pérsico, al menos temporalmente"[4].

Irán ha desatado ciberataques destructivos en el pasado. "En 2012, creó un virus llamado Shamoon, que casi destruyó más de 30.000 computadoras de la red corporativa de Saudi Aramco, una empresa estatal de petróleo y gas. Los virus pueden eliminar las copias de seguridad de los datos. El análisis de las operaciones de TI reveló un aumento en los intentos de robo a través de ataques de bayoneta, destinados a obtener acceso a los sistemas de TI en el sector de la energía.

En cuanto a ataques de ciberseguridad contra Colombia se puede mencionar que: "La Guardia Civil Española en el año 2010, desmanteló a una de las mayores redes de computadores Zombis conocida con el nombre de *BootNet* Mariposa compuesta por más de 13 millones de direcciones IP infectadas, distribuidas en 190 países alrededor del mundo. Colombia ocupo el quinto puesto entre los países más afectados por esta red".[5]

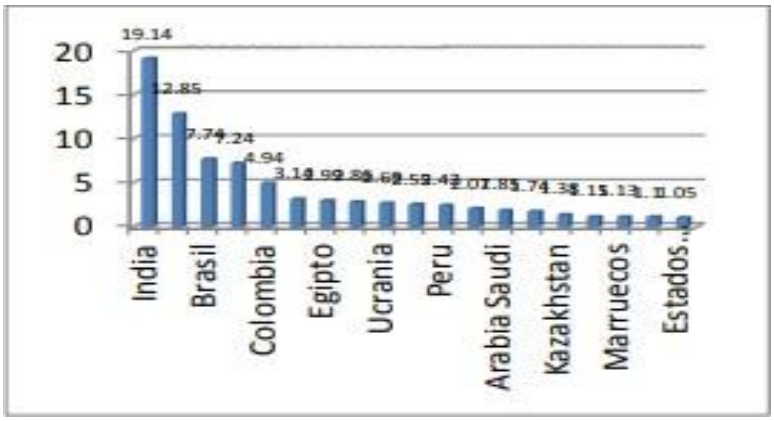
"Latinoamérica encabeza el top 20 en países más afectados, conformados por: México con el 12.85%, Brasil con el 7.74%, Colombia con el 4,94%, Perú con el 2,42%, Chile con el 1,74% y Argentina con el 1.10% del total"[6] resultados que se pueden observar en la figura 1.

[4] INFOBAE. Un ataque cibernético de Estados Unidos afectó la capacidad de Irán de disparar contra buques petroleros en el Golfo Pérsico. [Citado el 15 de Noviembre de 2020] Disponible en Internet: https://webcache.googleusercontent.com/search?q=cache:EL-jUiDW5FIJ:https://www.infobae.com/america/mundo/2019/08/28/un-ataque-cibernetico-de-estados-unidos-afecto-la-capacidad-de-iran-de-disparar-contra-buques-petroleros-en-el-golfo-persico/+&cd=8&hl=es-419&ct=clnk&gl=co

[5] REINERIO, Camacho. Ciberseguridad y Ciberdefensa en Colombia. [Citado el 25 de Noviembre de 2020] Disponible en internet: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2984/Trabajo%20de%20grado.pdf?sequence=1

[6] Universidad Piloto de Colombia, Ciberseguridad y Ciberdefensa en Colombia. [En línea] http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2984/Trabajo%20de%20grado.pdf?sequence=1

Figura 1. Países más afectados por BootNet Mariposa



Fuente Universidad Piloto de Colombia, Ciberseguridad y Ciberdefensa en Colombia. [En línea] http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2984/Trabajo%20de%20grado.pdf?sequence=1

Los ataques a los sistemas SCADA se contemplan como ataques de alto riego, debido a la implicaciones económicas que pueden conllevar. En Colombia, los sistemas SCADA permite la operación de los sistemas de generación, trasmisión y distribución eléctrica, una falla en dichos sistemas de información, podría provocar la parálisis de la industria manufacturera e industrializada además de afectar otro sectores de la económica.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo incide en las empresas de energía eléctrica colombianas la implementación de guías, marcos de trabajo y estándares internacionales para la evaluación de la seguridad en sus sistemas SCADA, si se tienen en cuenta aspectos como las recomendaciones, amenazas y vulnerabilidades que presentan regularmente en el campo de la ciberseguridad?

2 JUSTIFICACIÓN

El sistema de información SCADA gestiona procesos muy importantes en diferentes industrias e infraestructura crítica del país, tales como, el sistema eléctrico. Los sistemas eléctricos se consideran infraestructura crítica, según lo definido por la directiva europea 2008/114/CE del Consejo de 8 de diciembre de 2008, donde se indica que una interrupción y/o destrucción de sus redes, servicios, bienes y equipos tendrían un impacto a nivel salud, La seguridad y el bienestar económico de los ciudadanos, también afectan el funcionamiento efectivo de las instituciones estatales. Hay que tener presente que la red eléctrica va encaminada a volverse una red inteligente, mejor conocida como Smart Grid, cuyo objetivo es mejorar la capacidad, confiabilidad y eficiencia del servicio a través de la cooperación entre los usuarios finales, la integración de la tecnología de la información y la red existente[7].

Los sistemas SCADA: "Son herramientas robustas, estables, administrables y que facilitan la automatización de procesos complejos y delicados como la desenergización de las redes eléctricas a través de la tele operación, compuesto de sensores, actuadores, controladores y medidores además de líneas de comunicación con interfaces, protocolos con controladores lógicos programables (PLC) y dispositivos electrónicos inteligentes" [8].

Sin embargo, este tipo de sistema de información tiene un ciclo de actualización muy largo, ya que originalmente no fueron diseñados para conéctarse a redes como Internet o redes públicas, en sus inicios, contaban con protocolos de comunicación propios, sin capas de seguridad, tipo autenticación o encriptación.

Además, que la modernización de la industria, la automatización y el internet de las cosas IoT, son acciones que juntas pueden conllevar a la pérdida de la seguridad, eso sumado a la implementación de Ethernet, TCP/IP y sistemas SCADA en infraestructura crítica como las redes eléctricas ha permitido el aumento sobre la exposición de todo tipo de amenazas.

Todo esto hace que conocer el estado actual de la seguridad de los sistemas de supervisión, control y adquisición de datos sea una prioridad, con el fin de poder tomar decisiones que permitan optimizar y proteger a la infraestructura critica de amenazas o ataques cibernéticos. Lo que se busca con esta monografía es conocer cómo se implementa unas directrices básicas para la evaluación de la seguridad en sus sistemas SCADA, teniendo en cuenta aspectos como las recomendaciones, amenazas y vulnerabilidades que presentan regularmente en el campo de la ciberseguridad.

[7] Directiva Europea, DIRECTIVA 2008/114/CE DEL CONSEJO. Disponible en: https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/DirectivaEuropea2008-114-CE.pdf
[8] Ibid Pág. 282

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Analizar el estado de la ciberseguridad en los sistemas SCADA en el sector eléctrico colombiano teniendo en cuenta las recomendaciones internacionales de protección contra ataques cibernéticos con la finalidad de proponer recomendaciones para la gestión de la seguridad informática.

3.2 OBJETIVOS ESPECÍFICOS

Determinar la importancia de la ciberseguridad aplicada en los sistemas SCADA en las empresas del sector eléctrico colombiano para una adecuada gestión del riesgo cibernético en su operación, basado en la revisión documental y los estándares establecidos a nivel internacional

Examinar las amenazas y vulnerabilidades más usuales que tienen que afrontar las empresas de energía colombiana al implementar sistemas SCADA, analizando los ataques presentados en otras regiones y la manera adecuada de subsanar las vulnerabilidades.

Proponer recomendaciones para la gestión de la seguridad para las empresas de energía eléctrica colombiana con el fin de prevenir y asegurar su infraestructura eléctrica de ataques cibernéticos y logren una disminución del nivel de riesgo cibernético en su operación.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

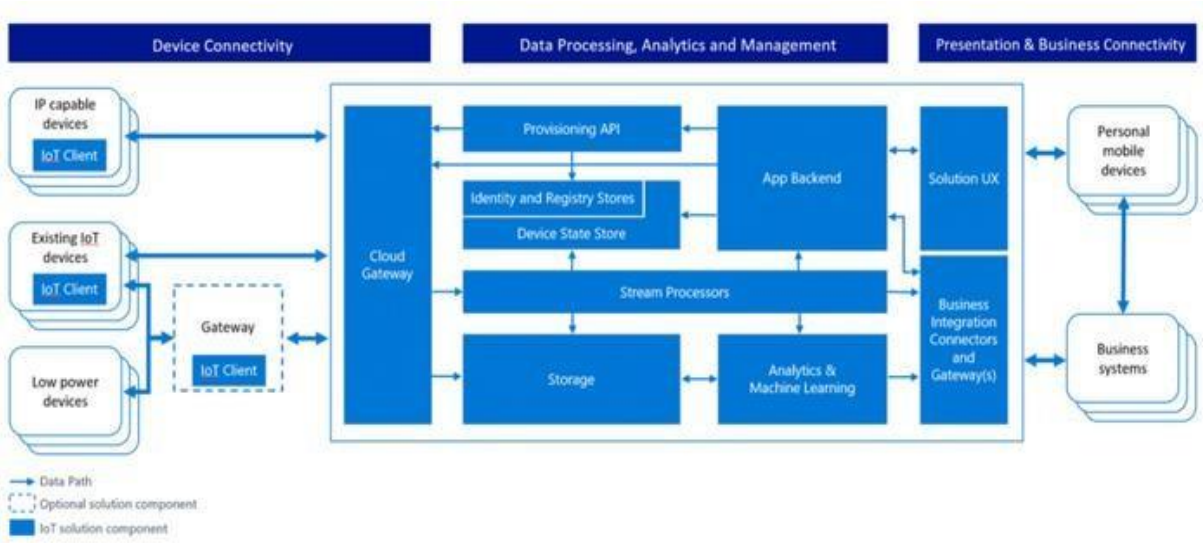
4.1.1 Arquitectura de Iot. Una arquitectura IoT se caracteriza por estar integradas por capas compuestas por una serie de tecnologías, servicios y protocolos. El siguiente autor presenta una arquitectura compuesta por cinco capas[9]**:**

- Recolección de datos: Esta capa está diseñada para permitir capturar datos de varios dispositivos al mismo tiempo, de manera ordenada y sincronizada, generando un volumen significativo de información, “casi que en tiempo real”.
- Transmisión de datos: La escalabilidad de la información es la base para la toma de decisiones, ya sea automatizadas o manuales; por los tanto, la trasmisión de datos es la encargada de garantizar la integridad de la información recolectada y que esta llegue a su lugar de almacenamiento ideal. Esta capa además, deberá esta resguarda mediante protocolos de comunicación que garanticen la estabilidad y legalidad de la data.
- Almacenamiento de datos en la nube o base de datos: El almacenamiento de la información emitida por los dispositivos IoT, están entornos distribuidos que constan de uno o más servidores, con el fin de garantizar la disponibilidad de la misma para su análisis.
- Análisis de datos: Esta capa recoge los eventos o datos emitidos, transportados y almacenados, proporcionando la posibilidad de procesarlos y con el fin de tomar decisiones y poder actuar sobre estos. Esta capa además, facilita el almacenamiento de los resultados en BBDD.
- Presentación y/o visualización de resultado: La capa final, permite a través de dispositivos administrativos o *dashboard* verificar el resultado final.

La integración de estas capas se puede evidenciar en la figura 2, donde se muestran la interacción de cada una de ellas.

[9] Microsoft, Modelado de riesgos de la arquitectura de referencia de Azure IoT [Citado el 25 de Noviembre de 2020]. Disponible en internet: https://docs.microsoft.com/es-es/azure/iot-fundamentals/iot-security-architecture

Figura 2. Capas de la arquitectura de IoT



Fuente Microsoft, Modelado de riesgos de la arquitectura de referencia de Azure IoT [En línea] https://docs.microsoft.com/es-es/azure/iot-fundamentals/iot-security-architecture

Como indica Joyanes Aguilar[10], Los sistemas SCADA son herramientas robustas, estables, administrables y que facilitan la automatización de procesos complejos y delicados como la desenergización de las redes eléctricas a través de la tele operación de elementos como los equipos de corte, que se componen de sensores, actuadores, controladores y medidores además de líneas de comunicación con interfaces, protocolos. Con controladores lógicos programables (PLC) y dispositivos electrónicos inteligentes.

Los sensores y actuadores son parte de la detección y recopilación de datos, porque los sensores son dispositivos físicos que están conectados al entorno y detectan o miden cantidades físicas y devuelven sus valores en forma de manera digital. Esta conexión puede ser de entrada o salida; los sensores de entrada pueden medir variables de manera similar, como temperatura y humedad, o variables binarias (sí / no), como alta temperatura sí / no.

Por otra parte, están los actuadores, que son dispositivos que accionan ante una solicitud para controlar el estado de una variable y normalmente son del tipo si/no. Un ejemplo claro son los equipos de corte en la red de energía como los

[10] AGUILAR Joyanes, Luis Industria 4.0 La cuarta revolución industrial, Cap. 10 Pág. 282. Editorial AlfaOmega 2019

seccionadores, los cuales atienden señales de abierto o cerrado para energizar o desenergizar a la red. [11]

4.1.2 Sistema SCADA. El sistema SCADA (sistema de supervisión, control y adquisición de datos) está compuesto por elementos que permiten el control industrial, la automatización de procesos y controlar remotamente equipos o elementos de una red. Consiste en la infraestructura compuesta por diferentes entes amenazantes con atractivo para perpetrar infiltraciones al sistema, con el propósito de recolectar información sensible como instalación, diseño, uso, umbrales críticos o configuraciones de dispositivos con el fin de generar ataques cibernéticos, y por consiguiente, operaciones de sabotaje, dentro de las cuales se incluyen: interrupción del servicio, situaciones peligrosas o incluso fatales, que representan situaciones extremadamente desagradables, tal como lo indica Samuel Moya en su publicación del 2017. [11]

4.1.3 Tipos de redes SCADA. Los tipos de redes SCADA se dividen en dos grupos principales: El primero de ellos se denomina la Red Corporativa que tiene como función: “Desarrollar un sistema que cuyo objetivo sean las actividades de monitoreo de usuarios, de modo que lo que esta red quiere es un proceso de autenticación y autorización muy detallado y preciso para acceder a la información en la base de datos (historial, alertas, etc.) y en los sistemas críticos del servidor. "

El segundo tipo de red SCADA se llama la Red de Control que desarrolla: “Las actividades configuración, mantenimiento y operación; como los mandos a actuadores, lectura de variables, monitoreo del proceso, etc. La comunicación entre dispositivos en una red de control utiliza protocolos específicos, como Modbus / TCP (Protocolo de control de transmisión basado en Modbus). DNP (Protocolo de Red Distribuida). En caso de requerirse deben soportar tecnologías como: líneas telefónicas, satélite, microondas, fibra óptica, *wireless*, seguridad de intrusión entre otros”. [12]

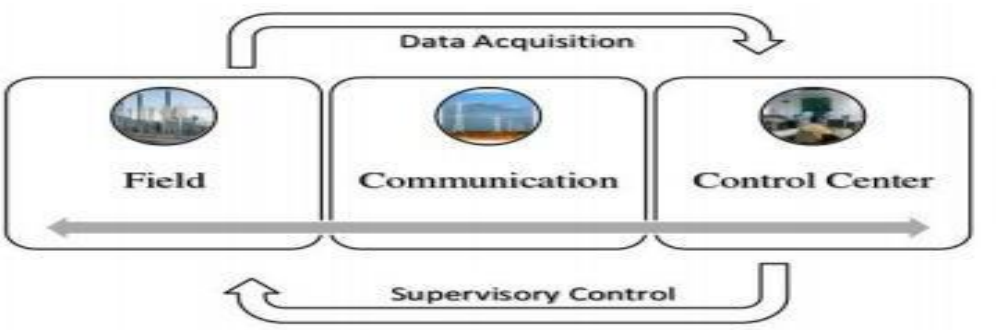
En la red de control interactúa una multitud de protocolos propios de automatización industrial basados en TCP/IP para el control remoto o todos aquellos pertenecientes a la familia del Protocolo Industrial Común CIP, mantenido por la *organización Open DeviceNet Vendors Association* (ODVA), como: *Ethernet/IP, DeviceNet, CompoNet* y *ControlNet*. No obstante, la mayoría de ellos presentan altas vulnerabilidades al carecer de mecanismos de protección. [13]

La seguridad en los sistemas SCADA. El objetivo principal de los sistemas SCADA es el de facilitar la retroalimentación en tiempo real del sistema, utilizando datos de

[11] MOYA Samuel. Ciberseguridad en Redes de Control Industrial (SCADA). [Citado el 21 de Noviembre de 2021] Disponible en Internet: https://www.isamex.org/intechmx/index.php/2017/09/22/ciberseguridad-en-redes-de-control-industrial-scada/
[12] Ibíd., Pág 1
[13] ibíd., Pág 1

los diferentes sensores que lo componen para controlar automáticamente el proceso. De manera similar, proporciona datos en tiempo real sobre el estado del proceso y puede obtener información sobre el control de calidad, los niveles de producción y otras variables que ayudan a administrar el proceso[14]. Como se muestra en la Figura 3, la comunicación es entre los elementos dispuesto en campo y centro de control, permitiendo la adquisición de datos y la supervisión.

Figura 3. Esquema Componentes SCADA



Fuente BAQUERO, German Dario. Seguridad de la Información en los Sistemas SCADA. [En línea] http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/3009/Trabajo%20de%20grado1512.pdf?sequence=1

4.1.4 Sistemas SCADA y los Smart Grids: Los sistemas SCADA en las empresas de energía se emplean para la toma de medidas, cambios de estado y registro de operación de elementos telecontrolados, telemedidos y teleoperados, los cuales representan una vulnerabilidad cibernética en las redes eléctricas, esto debido a que las señales emitidas por los actuadores conectados a dichos elementos, viajan por Fibra Óptica, redes 3G y/o 4G, provocando la energización o desenergización de la red.

Según los estándares internaciones, los sistemas SCADA se componen de PLCs, DCSs y el *software* como tal denominado SCADA además de los profesionales del sector eléctrico que tiene la tarea de monitorizar todo el sistema eléctrico y las señales que emiten los dispositivos “mapeados” en el sistema. El objetivo de la automatización de las redes eléctricas es implementar una solución que permita a los Operadores de Red mejorar el desempeño de la red eléctrica actual, con el objetivo de atender de manera eficiente al elevado número de consumidores

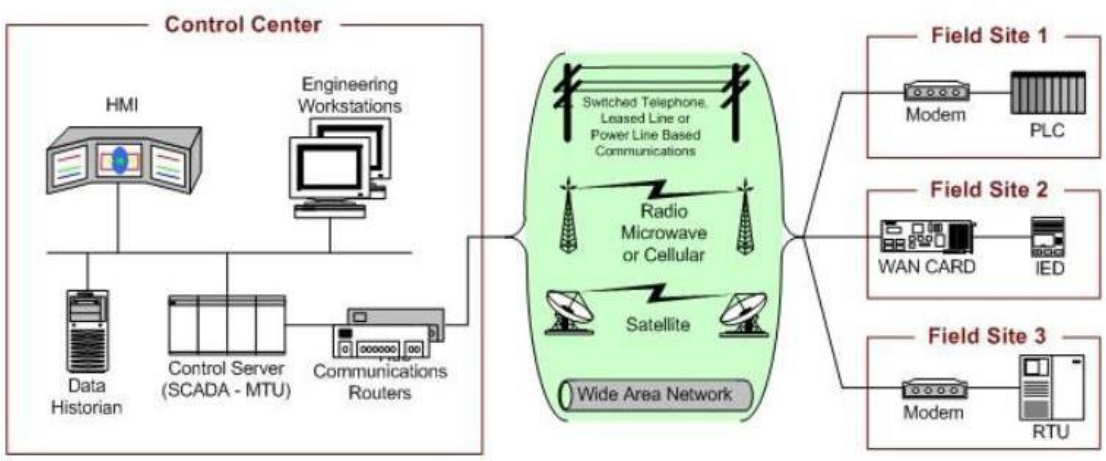
[14] BAQUERO Salamanca, Germán Darío. Seguridad de la Información en Sistemas SCADA. Universidad Piloto de Colombia. [Citado el 21 de octubre de 2021]. Disponible en Internet: http://polux.unipiloto.edu.co:8080/00001512.pdf

actuales y los esperados en el futuro, buscando que la red eléctrica se convierta en una Smart Grid [15]

Energía y Sociedad define la *Smart Grid* como la red que permite integrar de manera perspicaz los comportamientos de los usuarios (generadores, consumidores y usuarios que están en línea al mismo tiempo) conectados a ella, para así realizar un control, monitorización y operación desde un sistema SCADA, garantizando así el suministro de energía eficiente, seguro y sostenible.

Según lo indicado por Guía de seguridad de los sistemas de control industrial (ICS)[16] se plantea el siguiente esquema para la implementación de sistemas SCADA, el cual se muestra en la Figura 4.

Figura 4. Diseño general de un sistema SCADA



Fuente STOUFFER, Keith. PILLITTERI, Victoria [Imagen]. Guide to Industrial Control Systems (ICS) Security. 2da Edición. Washington: NIST 2015. pp 21

[15] GIRAL, William -RAMÍREZ, Hugo. Smart grids in the colombian electric system: Current situation and potential opportunities. [Citado el 10 de Noviembre de 2020] Disponible en Internet: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-921X2017000300119

[16] Guide to Industrial Control Systems (ICS) Security, p21. [Citado el 25 de Octubre de 2020]. Disponible en internet: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

4.1.5 Qué son los Sistemas de Control Industrial. Los estándares ISA99, además de ser utilizados por la Comisión Electrotécnica Internacional (IEC) para la producción de los Estándares IEC62443, definen que los Sistemas de Control Industrial son: "Una colección de personal, hardware y software que pueden afectar o influir en la operación segura, la seguridad y la confiabilidad de los procesos industriales. El estándar ISA-62443-3-3, define que los sistemas de control industrial son una colección de personal, hardware, software y políticas involucradas en la operación del proceso industrial y que pueden afectar o influenciar su operación segura y confiable".[17]

El Instituto Nacional de Estándares y Tecnología (NIST) del Departamento de Comercio del gobierno norteamericano, establece que: "Los Sistemas de Control Industrial es un término general que abarca varios sistemas de control, incluidos sistemas de supervisión y adquisición de datos (SCADA), sistemas de control distribuido y otras configuraciones de sistema de control como controladores lógicos programables (PLC) que a menudo se encuentran en los sectores industriales y en las infraestructuras críticas. Un sistema de control industrial consiste en combinaciones de componentes de control (por ejemplo: eléctricos, mecánicos, hidráulicos, neumáticos) que actúan conjuntamente para lograr un objetivo industrial". [18]

4.1.5 Transmisión de datos y redes de comunicación. Los registros generados o adquiridos por todos los sensores y actuadores de los equipos teleoperados son enviados a una base de datos o repositorio de almacenamiento para su análisis y toma de decisiones, su almacenamiento puede ser distribuido o centralizado, según las disposiciones de los Operadores de Red. En esta capa, se necesita una red de comunicación para que puedan enviar la información capturada.

En sistemas antiguos se tenía una conexión tipo M2M (Máquina a Maquina) y normalmente realizadas por medio de redes cableadas. Luego se evolucionó a la comunicación por satélite hasta llegar a la actualidad, donde se cuenta con redes inalámbricas y alámbricas tipo WAN, MAN, LAN y PAN e incluso WiFi[19].

Los estándares de comunicación han ido aumentando las velocidades de las redes de comunicación y, por consiguiente, ahora se puede transmitir grandes volúmenes de información en poco tiempo. Ahora todo puede estar conectado, operarse remotamente y tener reportes de comportamiento en tiempo real, esto incluye los activos de las redes eléctricas que permiten la tele operación.

---

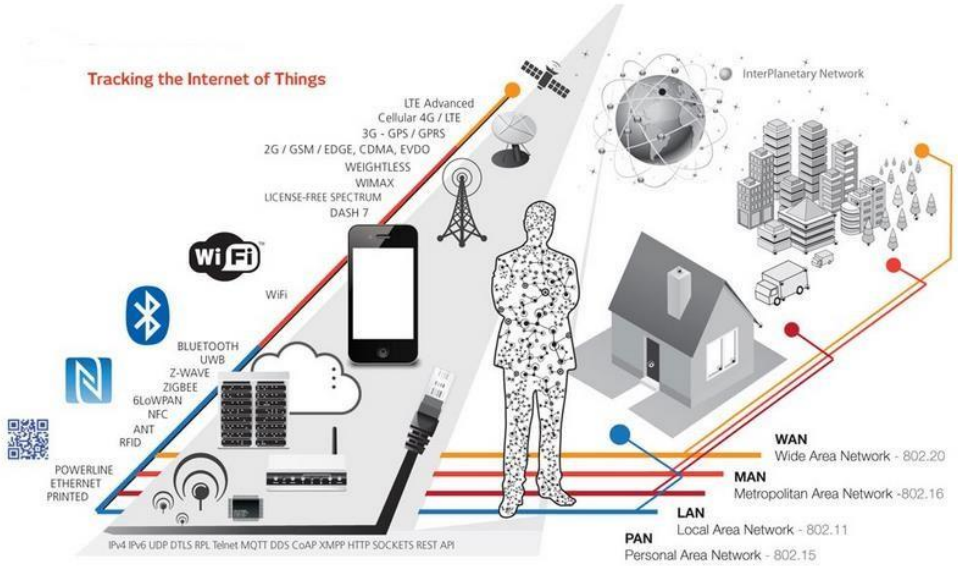
[17] GARCIA, Julián Andrés. Trabajo final de Master: Investigación de la Ciberseguridad aplicada a los Sistemas de Control Industrial con Énfasis en el sector energético. [Citado el 2 de Noviembre de 2020]. Disponible en internet: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72749/6/jgarciaariasTFM0118Memoria.pdf

[18] ibíd. Pág 8

[19] LANGNER, Ralph. Robust Control System Networks: How to Achieve Reliable Control After Stuxnet. New York: Momentum Press, 2012.

Para los sistemas de control industrial, enviar y recibir información es la parte más importante del proceso de control. Para ello, se utilizan protocolos de comunicación. Algunos de estos protocolos están diseñados para propósitos específicos, mientras que otros están diseñados para utilizar tecnología de medios de transmisión más moderna y garantizar de interoperabilidad entre diferentes fabricantes de equipos de control como se ve en la Figura 5.

Figura 5. Redes de comunicación



Fuente Dr. Rajiv Desai Blog: Internet of things (IoT) 19/07/2026. http://drrajivdesaimd.com/2016/07/19/internet-of-things-iot/

Aquí están los detalles de algunos de los protocolos de comunicación más utilizados en los sistemas SCADA:

*Modbus Serie***:** Utiliza comunicación serie y protocolos como HDLC, RS232 y RS485 para transmitir datos, y MODBUS utiliza TCP/IP, que utiliza la pila de protocolos TCP/IP para transmitir información. MODBUS no realiza ninguna función de seguridad en la capa de transporte o capa de aplicación, sin embargo, las medidas de seguridad basadas en TCP / IP solo se pueden aplicar a la implementación usando MODBUS TCP / IP[20].

Powerlink Ethernet: Protocolo de comunicación en tiempo real, se caracteriza por transferir información de manera sincronizada y precisa a intervalos de tiempo configurados, Evitar la colisión de información, a través de un proceso de software

[20] NI, Información Detallada sobre el Protocolo Modbus. [Citado el 25 de Noviembre de 2020]. Disponible en internet: https://www.ni.com/es-co/innovations/white-papers/14/the-modbus-protocol-in-depth.html

anidado conocido como gestión de red de medios de ranura (SCNM), que garantiza que solo los equipos de red puedan acceder a los medios de transmisión.

Opcua: Es un protocolo de comunicación *opensource* desarrollado por la Fundación OPC y liberado en el 2006, Se utiliza para conectarse entre dispositivos, y realizando la recopilación de datos y de sistemas de control de datos., es multiplataforma y basado en una Arquitectura Orientada a Servicios (SOA por su sigla en inglés). Tiene una gran seguridad, incluida la autenticación a nivel de aplicación, el cifrado y la autenticación de mensajes. Utiliza los puertos TCP 80 y 443, lo que facilita la configuración del firewall.

Sin embargo, esta integración de comunicación y redes, da a lugar a una serie de nuevas vulnerabilidades provocadas por la intrusión y la corrupción de la red de comunicación, que pueden provocar efectos físicos destructivos así como enormes pérdidas económicas, ya que no solo es la interrupción de un servicio esencial sino que la misma infraestructura provee interconexión con otras industrias críticas: transporte, las telecomunicaciones, la salud pública, banca y finanza, suministro de agua, servicios de seguridad, entre otros.

4.2 MARCO CONCEPTUAL

4.2.1 Redes de uso general. Según el Concepto 2938 de 2004 de la Comisión de Energía y Gas son: "La red compartida es aquellos que usan dos o más personas naturales o más (usuarios del servicio de usuario) no forman parte de las instalaciones de usuario no vivas o internos que no pertenecen a la compañía de terceros"

Los propietarios de estas redes tienen las siguientes opciones:

· Convertirse en un OR
· Venderlos
· Tome posesión de él y reciba el pago del OR que lo usa.

En el caso de que los propietarios de la red decidan conservar la propiedad de los activos, conviene señalar que la empresa, además de recompensar a los propietarios, también es responsable de administrar los activos, operar y mantener estos activos.

Los nuevos estándares de gestión de activos se convertirán en un gran desafío para muchas organizaciones relacionadas con la industria de las redes eléctricas. Aunque la industria y los organismos reguladores y de financiación relacionados se beneficiarán enormemente, los principales proveedores de equipos también se beneficiarán. Los fabricantes y contratistas de mantenimiento de los principales

activos de servicios públicos también enfrentan sus propios desafíos de gestión de activos tal como lo indica Cornelec [21].

4.2.2 Activos en operación. Componentes eléctricos que se utilizan permanentemente para actividades de distribución de energía en el sistema, incluidos los que normalmente están abiertos. Un sistema normalmente abierto debe entenderse como un sistema que puede usarse inmediatamente cuando sea necesario.
A nivel empresarial todo activo es una inversión, para amortizar las actividades de la empresa. Éstos son divididos en aquellos que representan inversión líquida, dentro de los cuales se encuentran los inventarios, los deudores comerciales, pagos por anticipado. Los anteriores representan un grupo de cuenta al que denominamos CAPITAL DE TRABAJO. Dentro de los activos de baja líquidez se encuentran 2 grupos, el primero EL CAPITAL FIJO, en el cual se encuentra la propiedad planta y equipo, la depreciación y las valorizaciones de los mismos. El segundo grupo se denomina OTROS ACTIVOS OPERATIVOS, los cuales son activos intangibles como las licencias, las patentes y los diferidos no corrientes. La suma de las combinaciones descritas anteriormente se resume en un grupo denominado activos operativos.

4.2.3 Control. Este término se puede analizar desde diferentes perspectivas una de ellas es una perspectiva limitada y una perspectiva amplia.
Desde una perspectiva limitada, el control es la verificación realista de los resultados obtenidos observando las metas establecidas y controlando los gastos de inversión operacional a través de las operaciones El nivel de gestión del desempeño, y por lo tanto está estandarizado cuantitativamente, forma parte central de la acción de control. Desde una perspectiva limitada, el control es la verificación realista de los resultados obtenidos observando las metas establecidas y controlando los gastos de inversión operacional a través de las operaciones El nivel de gestión del desempeño, y por lo tanto está estandarizado cuantitativamente.
Este enfoque enfatiza los elementos sociales y culturales en el contexto institucional, desde la parte del principio de que el último comportamiento individual determina la efectividad de los métodos de control controlados.

De igual manera el planteamiento de las definiciones de control es variadas como se puede leer a continuación:

Para Henry Farrol, el control incluía verificar que todo saliera de acuerdo con el plan aprobado (AP), los lineamientos emitidos y los principios establecidos. Su propósito es señalar las debilidades y fallas para que puedan ser abordadas y evitar que

[21] CORNELEC. Gestión Estratégica de Activos En las Redes Eléctricas. [Citado el 5 de Noviembre de 2020]. Disponible en internet: https://cornelec.cl/2015/10/23/gestion-estrategica-de-activos-en-las-redes-electricas/

vuelvan a ocurrir. El pequeño Roberto B. Bushell afirma que se trata de medir los resultados actuales contra el plan, diagnosticar las causas de las desviaciones y tomar las medidas correctivas necesarias. jorge r Terry: El proceso de identificar y evaluar lo que se está haciendo y, si es necesario, tomar medidas correctivas para que la implementación vaya de acuerdo con el plan. Buró K. Scanlan afirma que el control tiene como objetivo cerciorarse de que los hechos vayan de acuerdo con los planes establecidos, en cuanto a la definición de Robert Eckles, Ronald Carmel y Bernard Kate argumentan que las regulaciones sobre las actividades, según un plan creado para lograr ciertos objetivos. De manera similar, Harold Kitzz y Cyril O'Neil controlan las medidas para lograr las brechas y las medidas de reparación para garantizar que los planes se basen en los planes.

4.2.4 Operación. Este concepto aplicado en el área empresarial incluye: “Todas las actividades relacionadas con la creación de productos o servicios prestados a los clientes. Se puede decir que es una “forma de hacer negocios” tal que sus actividades permiten la prestación de un servicio o la fabricación de un producto para ser suministrado o entregado al cliente para cumplir con sus expectativas.

Por lo tanto, dentro de los objetivos de las operaciones en el sector empresarial se encuentran llegar a ser competitivo, rentable y aumentar la productividad.

Dentro de los fundamentos de programación las operaciones se hacen posibles al: “Combinar operadores y operandos, es decir acciones que conduzcan a disponer de variables con valores que pueden obtenerse ya sea por parte de los usuarios de los programas o a su vez como resultado de la ejecución de una expresión”[22]

Las operaciones más comunes son las dirigidas hacia la lectura, la escritura y la asignación.

La operación de lectura, significa que una variable tomará un valor que será ingresado por el usuario a través de un dispositivo externo de entrada, generalmente un teclado. En la forma más sencilla se utilizan los verbos: Leer o Ingresar junto al nombre de la variable que se desea obtener. La operación de escritura, a su vez expresa la necesidad de visualizar el valor que tiene una variable a través de un dispositivo de salida, ya sea una pantalla en la mayoría de casos, o una impresora. Al igual que en la operación de lectura se utilizan verbos: Escribir o Imprimir junto al nombre de la variable que se desea visualizar y la operación de asignación es una manera diferente que se utiliza para que una variable reciba un valor de forma directa sin intervención del usuario, o como resultado de la evaluación de una expresión. Para esta operación se utiliza un operador que varía

[22] CERVANTES, Nancy. Operaciones. [Citado el 15 de Noviembre de 2020]. Disponible en internet: http://www.utn.edu.ec/reduca/programacion/fundamentos/operaciones.html

de acuerdo al lenguaje, pero que de forma básica puede ser una flecha con dirección hacia la izquierda[23]

4.2.5 Seguridad. Este concepto relacionado con la informática es el área de la computación que se enfoca en Protección y privatización de su régimen, en el que existen dos tipos:

La seguridad lógica se centra en proteger su contenido e información. La seguridad física se aplica a este tipo de dispositivos, porque el ataque no está estrechamente relacionado con estos programas informáticos sino también con el hardware. Pueden aparecer amenazas externas e internas, y una forma común de ataque es el uso de virus, que son archivos que pueden modificar información o datos de otros archivos sin el consentimiento del usuario; El camino exterior es el camino que se lleva desde fuera y no tiene mucha seguridad por lo que es más fácil de pelear, y por tanto más difícil para el autor dar el golpe, que el camino interior, que es más capital. Peligroso porque la computadora no necesita una conexión de red para recibir el ataque

En lo que respecta a la seguridad aplicada en el sector energético la seguridad de abastecimiento abarca dos conceptos diferentes, por un lado están los hechos económicos y por otro el concepto psicológico de seguridad, estos dos conceptos permiten mantener un precio determinado basado en la percepción. Cabe aclarar que además de la seguridad de suministro, la seguridad energética tiene otros aspectos importantes que suelen pasarse por alto, como la seguridad de las instalaciones (en caso de accidente o atentado), la seguridad ambiental o social tal y como lo indica Gonzalo Escribano en su ponencia sobre seguridad energética[24]

4.2.6 Sistema. El concepto de sistemas ha sido utilizado por dos líneas de pensamiento diferentes, la primera es la teoría general del sistema, que es una tendencia iniciada por Von Bertalanffy y que continúa siendo desarrollada por Bouldffig donde el esfuerzo principal es lograr la integración científica. El segundo movimiento es más práctico y se conoce como ingeniería de sistemas o ciencia de sistemas iniciada por la investigación de operaciones, seguida de la gestión científica (ciencia de la gestión) y, finalmente, el análisis de sistemas. Otra definición agrega algunas características adicionales, lo que indica que un sistema es un conjunto de partes y objetos que interactúan y que forman un todo o se ven afectados por fuerzas en alguna relación definida, tal y como lo explica Rafael

[23] Ibid pág. 3

[24] ESCRIBANO, Gonzalo. Seguridad Energética: concepto, escenarios e implicaciones para España y la UE (DT). [Citado el 25 de Noviembre de 2020]. Disponible en: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/dt33-2006
http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/dt33-2006

Lapiedra en su ponencia sobre la Introducción a la Gestión de Sistemas de Información En la Empresa[25].

El concepto también se encuentra ligado al entorno informático y consiste en una interconexión compleja de un gran número de componentes hardware y software, que son básicamente sistemas deterministas y formales, de tal manera que siempre se obtiene la misma salida para una determinada entrada. El sistema de información es un sistema social cuyo comportamiento está influenciado en gran medida por los objetivos, valores y creencias de los individuos y grupos, así como por el desempeño técnico. Por tanto, el comportamiento del sistema de información no es determinista ni se ajusta a la representación de ningún modelo de algoritmo formal[26].

4.3 ANTECEDENTES O ESTADO ACTUAL

Dentro de los antecdentes más relevantes se encuentra el ataque cibernético a la infraestructura eléctrica de Ucrania ocurrido 23 de diciembre del 2015, donde las plantas eléctricas no habían recibido ningún reporte de sus elementos telecontrolados, ningún daño se reportó y aparentemente la red funcionaba con normalidad; sin embargo, el llamado de usuarios a reportar la falta de suministro eléctrico alertó a los ingenieros a cargo.

Tiempo después, los ingenieros encontraron la causa: La planta de energía sufrió un ciberataque, aparentemente coordinado por piratas informáticos rusos, y por medio del cual, se dio a conocer el *malware* denominado "*Black Energy*" [27], La historia se convierte en el primer avance exitoso en la red energética global. Pero fue solo el primero, en 2017, al menos doce compañías eléctricas en las que está la planta nuclear Wolf Creek, En Kansas, EE. UU., también se coordinó un ataque informático, según el FBI, por una "red de saboteadores".[28], lo que convierte a estos tipos de ataques en una herramienta de guerra mundial.

Esto plantea preocupaciones razonables y dudas sobre la seguridad de los sistemas eléctricos a nivel mundial, aunque en Colombia no se ha producido ataques de este tipo, con la automatización de las redes eléctricas en auge, es fundamental mostrar a los Operadores de Red las nuevas vulnerabilidades a las que se enfrentan.

[25] SÁNCHEZ, Daniel. Que es un Sistema. [Citado el 25 de Noviembre de 2020]. Disponible en Internet: https://www.academia.edu/31110664/Qu%C3%A9_es_un_sistema

[26] LAPIEDRA, Rafael. DEVECE, Carlos. Introducción a la Gestión de Sistemas de Información En la Empresa. [Citado el 25 de Noviembre de 2020]. Disponible en internet: https://libros.metabiblioteca.org/bitstream/001/193/8/978-84-693-9894-4.pdf

[27] INCIBE_CERT, BlackEnergy y los sistemas críticos. [Citado el 25 de Noviembre de 2020].Disponible en internet: https://www.incibe-cert.es/blog/blackenergy-sistemas-criticos

[28] LIOMAN Lima, BBC - Estados Unidos vs Rusia: cómo el hackeo de las redes eléctricas se convirtió en un nuevo campo de batalla entre Washington y Moscú. [Citado el 25 de Noviembre de 2020] Disponible en: https://www.bbc.com/mundo/noticias-internacional-48668879

Describir las amenazas y ataques cibernéticos principales que pueden generar una afectación en la seguridad y confiabilidad de la red eléctrica es uno de los grandes retos.

En este mismo sentido para el desarrollo de este trabajo se tuvo como referencia tres investigaciones que tienen una temática similar a la de esta monografía y en las cuales se describen los datos básicos de cada una de ellas, el resumen y las conclusiones a las que llegaron los autores de estos trabajos.

La primera investigación es un trabajo final de master titulado: "Investigación sobre ciberseguridad aplicada a los sistemas de control industrial con foco en el sector energético" por Julien Andrés García Arias, presentada ante la Universidad Oberta de Catalunya en Diciembre de 2017[29]. En resumen el internet permite que se genere una productividad considerable en todos los países, incentivando los ingresos de las personas pues se genera empleo, a pesar de estas ventajas la tecnología digital presenta algunos vacíos que son aprovechados por los hackers para lograr sus acciones ilícitas. La importancia que ha adquirido la ciberseguridad a nivel industrial ha sido notoria en los últimos años catalogándose como infraestructuras de tipo crítico. Por este motivo los gobiernos de todas las naciones se han fijado dentro de sus objetivos plantear soluciones en el campo de la ciberseguridad que protejan a la sociedad de los delitos informáticos para aumentar el progreso de los países utilizando herramientas como la comunicación y las tecnologías de la información. En esta investigación se hace un estudio directamente en las empresas de tipo industrial que tienen implementado los sistemas SCADA, analizando su funcionamiento y las estrategias que se pueden realizar para prevenir, mitigar riesgos y vulnerabilidades.
Por lo anterior, se puede concluir que los sistemas de control Industrial contienen variedad de procedimientos que manejan los procesos a través de los diferentes componentes que posee su infraestructura, el cual maneja un grado de complejidad considerable por lo que cuenta con sistemas que se han utilizado durante años y miles de unidades, dado que es complicado llegar a controlarlos en su totalidad.

En la tabla 1 se realiza un análisis comparativo entre las Tecnologías de la Información y la Comunicación (TIC) y las Tecnologías de Operación (TO), se presentan una diferencia notable y es el grado de impacto que podrían producir cuando se presente un problema de seguridad en un Sistema de Control Integral, se puede indicar que, cuando se compromete la seguridad de redes empresariales tipo TIC podría desencadenar consecuencias a nivel financiero, se afectaría también la imagen que tienen los clientes de esta entidad y sus datos personales quedarían al descubierto, mientras que cuando se presenta un problema de

[29] GARCÍA Arias, Julián Ándres. Trabajo final de master: Investigación de la ciberseguridad aplicada a los sistemas de control industrial con énfasis en el sector energético. Universidad Oberta de catalunya. [Citado el 22 de Octubre de 2021]. Disponible en Internet: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72749/6/jgarciaariasTFM0118Memoria.pdf

seguridad en un Sistema de Control Industrial, las consecuencias se verían reflejadas en la destrucción de los recursos físicos, personas que mueren o quedan heridas[30].

Cuadro 1. Comparativo TIC y TO

	Tecnologías de la Información y de la Comunicación (TIC)	**Tecnologías de Operación (TO)**
Objetivo	Aplicable en equipos de telecomunicación, esta tecnología es más empleada en ámbito empresarial y de los negocios	Tecnología implementada para la detección de cambios en procesos físicos mediante la monitorización y control remoto de dispositivos haciendo de su aplicación más industrial.
Necesidad Tecnológica	Depende por lo general, de la cantidad de profesionales activos ya que requieren de un control personal	El despliegue es mas amplio en cuanto a los dispositivos, ya que su aplicación es mas autónoma, por lo tanto, la cantidad puede ser superior al número de trabajadores.
Conservación	Son tecnologías frágiles que requiere de cambios nulos o muy pocos además de controlados y de mantenimiento permanente	El entorno de estas tecnologías es mas rudo, soportan temperaturas mas fuertes, humedad y ataques climatológicos con mayor resistencia
Protocolo y Normativa	Cuanta con mayor flexibilidad en la aplicación de protocolos y normativas, ya que no requiere relación estrecha	Depende del sector industrial en el cual se implemente ya que no existe una normativa generalizada.
Seguridad	Su enfoque está en el siguiente orden: 1. Confidencialidad 2. Integridad	Su enfoque está en el siguiente orden: 1. Disponibilidad 2. Integridad

[30] MENDOZA Villamil, Pedro Julio. Ataques informáticos a la infraestructura crítica del sector eléctrico colombiano. [Citado el 22 de octubre de 2021].Disponible en Internet: https://repository.unad.edu.co/bitstream/handle/10596/27757/%09pjmendozav.pdf?sequence=1&isAllowed=y

	3. Disponibilidad	3. Confidencialidad
Datos y procesos	Las vías de comunicación deben de garantizar el flujo de información y datos de manera continua, debido al volumen de la misma.	La infraestructura de comunicación es más básica haciendo del mantenimiento y la administración algo mínimo.
Actualización	Al presentar actualizaciones constantes hace que los sistemas sean mas vulnerables pero al mismo tiempo que los errores sean detectados mas fácilmente y subsanados de igual forma, de manera ininterrumpida.	Al ser dispositivos de larga vida útil, sus actualización o parcheo son nulos o requieren de un pare de actividades, lo que ocasiona que en la industria se encuentre dispositivos obsoletos.

Fuente NetCloud, Tecnologías de la información IT vs. tecnologías de la operación OT. Disponible en https://netcloudengineering.com/tecnologia-informacion-it-operacion-ot/

Hasta el momento se puede asegurar que no existe una estrategia, normas ni elementos de tipo tecnológico que sean eficaces y que puedan brindar garantía de seguridad a los activos ni tampoco que se puedan evitar problemáticas en un futuro próximo, más bien se deben tener en cuenta aspectos como el papel fundamental de los directivos de una organización, la respectiva asignación de recursos, y darle el lugar primordial que tiene la ciberseguridad en muchos campos de la industria eléctrica.

La adopción de buenas prácticas, normas y estándares constituyen una hoja de ruta de gran valor, pero los desafíos a la hora de aplicarlas son la transformación del “qué hacer” al “cómo hacerlo”, se deben interpretar las necesidades de la organización, conseguir el apoyo gerencial, obtener los recursos, gestionar los riesgos, diseñar métricas para tomar decisiones y demostrar el entorno de las inversiones en ciberseguridad industrial.

Es una realidad que se ha generado un crecimiento importante de los estándares, la evolución y practica de todo tipo de tecnologías y las correspondientes amenazas que pueden presentarse en el sector industrial todo con el fin de lograr una protección considerable, aun así, falta mucho más que simplemente adoptar las buenas prácticas y cumplir con los estándares establecidos.

La segunda investigación es un artículo titulado: “Seguridad en la Información en los Sistemas SCADA” cuyo autor es German Dario Baquero Salamanca, presentado

ante la Universidad Piloto de Colombia en el año 2014[31]. En este escrito se muestra lo fundamental que es la seguridad en los sistemas de tipo SCADA, iniciando con la introducción donde se hace una explicación sobre lo que significa los sistemas SCADA, su importancia, controles para la respectiva protección, riesgos con los que cuenta y sus amenazas, culminando con unas pautas que se pueden aplicar con el fin de beneficiar la seguridad de toda la información que se maneja. A manera de conclusión los Sistemas de Control Industrial (SCI) actualmente están presentando varias clases de vulneraciones, pues son el blanco perfecto para recibir ataques informáticos, los protocolos que se manejan TCP/IP son un riesgo considerable, por eso se deben poner en marcha estrategias de seguridad que se manejen de forma permanente y realizar las respectivas actualizaciones del software.

La tercera y última investigación es un artículo de revista llamado: "Predicción de ciberataques en sistemas industriales SCADA a través de la implementación del filtro Kalman" cuyos autores son: Stephen Quiroz Tascón, Julián Zapata Jiménez y Héctor Fernando Vargas Montoya, presentado ante el Instituto Tecnológico Metropolitano de Medellín, Colombia en Marzo 21 de 2020[32]. En dicho artículo se realiza un modelo de predicciones de los más probables ciberataques del sistema SCADA utilizando un filtro de tipo Kalman que contiene un sistema que detecta intrusos generando de esta manera una proyección a futuro de las posibles probabilidades de que se produzca un ataque. Con la información que se logra recopilar el administrador de los sistemas tendrá las bases para poder tomar decisiones de cómo actuar frente a cada uno de estos ataques cibernéticos. Poder predecir posibles eventos de seguridad les permitirá las organizaciones gestionar de manera más proactiva los riesgos en sus sistemas industriales. La prevención como elemento fundamental en los planes de tratamiento de riesgos permitirá establecer diferentes rutas de actuación para lograr mitigar posibles ciberataques. A partir de la medición de los 3 ataques informáticos generados, se puede establecer una predicción temprana con una reducción del error tendiente a cero (0) para los ataques de escritura y lectura, tenga permitir que el porcentaje de predicción una tendencia hacia el logro del objetivo (llegar al 100%), siendo el ataque 514 el de mejor convergencia.

Con ello, las personas pueden visualizar los posibles impactos generados en los sistemas industriales, por lo que el uso del filtro Kalman, en una primera aproximación, puede apoyar la identificación de posibles eventos de seguridad que puedan impactar negativamente la seguridad. Con ello, los administradores podrán

[31] BAQUERO Salamanca, Germán Darío. Seguridad de la Información en Sistemas SCADA. Universidad Piloto de Colombia. [Citado el 22 de octubre de 2021]. Disponible en Internet: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/3009/Trabajo%20de%20grado1512.pdf?sequence=1

[32] Stephen Quiroz Tascón, Julián Zapata Jiménez y Héctor Fernando Vargas Montoya. Predicción de ciberataques en sistemas industriales SCADA a través de la implementación del filtro Kalman. [Citado el 22 de octubre de 2021]. Disponible en Internet: https://revistas.itm.edu.co/index.php/tecnologicas/article/view/1586/1639

visualizar diferentes estrategias que le ayuden a actuar si el evento identificado se materializa o, mejor aún, establecer mecanismos de control para que no se materialicen. En comparación con otros procesos investigativos y sus resultados, y considerando que el uso del filtro Kalman se aplicó en una red real, obtener un 98% en la predicción con tendencia de error a cero (0) ataques sobre en línea, es un valor muy relevante (solo 1 punto porcentual por debajo de algunos resultados ejecutados con datos estáticos). Esto puede permitir establecer un método funcional que sea afinado y utilizado para actuar frente a posibles eventos de seguridad.

Contar con sistemas de detección de intrusos (IDS) que pueden identificar ataques a través de reglas o alertas en los sistemas industriales SCADA en tiempo real, permite tener las entradas necesarias hacia el filtro Kalman y así contar con una herramienta de predicción. La efectividad de la respuesta depende de la afinación misma de la entrada (el IDS) y de cómo las reglas configuradas permiten esa identificación de ataques informáticos.

Si bien el *honeypot* utilizado en las diversas implementaciones de sistemas SCADA simulados, con el fin de realizar análisis de vulnerabilidad tiene diferentes limitaciones con respecto a los SCADA reales, los resultados permitieron establecer las reglas para la configuración ideal de los IDS y la programación del filtro Kalman.

4.3.1 Predicciones de seguridad para el 2017 – 2020. En los últimos años se ha incrementado el uso de plataformas tecnológicas en la industria eléctrica como la nube y el IoT (Internet de los objetos), pero esto a echo que aumenten las amenazas a la ciberseguridad de las empresas. Un informe entregado por McAfee Labs[33] publicado en el 2016 y basado en las amenazas a *Cloud Computing IoT* demuestra las múltiples oportunidades que hay para robar datos, denegar servicios o provocar daños, son abundantes. Dentro de sus conclusiones sobre los *malware* indica que hoy más que nunca, los *hackers* tienen más posibilidades y facilidades para entrar por las puertas trasera ya que vivimos en un mundo hiperconectado, no solo a nivel personal, sino industrial.

Los *hackers* están más activos que nunca, los incentivos económicos y la posibilidad de causar daños a gran escala, los motivan, los retan. Dentro de las predicciones se indica que los ataques serán enfocados a nivel económico, la desestabilización de empresas y países, esto utilizando ataques tipo *ransomware* y *hacktivismo*, *imponiendo* desafíos a los fabricantes de dispositivos conectados.

[33] McAfee Labs, Predicciones sobre amenazas para 2017. Noviembre 2016 [en Línea] disponible en: https://mcafee.app.box.com/v/2017predictionsSP

Dentro de un punto de vista práctico, McAfee Labs en su informe enumera diez predicciones catalogadas como las más destacadas y probables para un periodo de cuatro años (2017-2020):

Amenaza de ataque al IoT, aunque no se considera aun que se puedan producir como parte de una motivación económica, se pueden presentar para generar reconocimiento en el mundo de los hackers:

- *Ransomware* considerada la principal amenaza.
- Hacktivismo catalogado como el riego más importante.
- Ataques a infraestructura crítica serán un motivo de preocupación constante.
- La pérdida de privacidad con el uso de IoT.
- Los equipos IoT se consideran vectores útiles de ataques dirigidos a sistemas de control, vigilancia y operación.
- Las fallas en los dispositivos provenientes de fábrica.
- El control de dispositivos IoT será uno de los objetivos principales.
- Los puntos de recopilación de información de los dispositivos IoT.
- Todos los dispositivos IoT con conexión estable, sufrirán ataques tipo *Ransomware* o *DoS.*

4.4 MARCO LEGAL

Dentro del marco legal y estándares, se pueden resaltar los siguientes el cual aportan al proceso de aseguramiento de la información en estos sistemas, entre ellos:

ISO/IEC27001:2013[34] Sistemas de gestión de seguridad de la información. La información es un activo valioso que puede hacer o deshacer su organización. Cuando se administra correctamente, le permite operar con confianza. Administrar la seguridad de la información le brinda la libertad de crecer, innovar y expandir su base de clientes sabiendo que toda su información confidencial permanecerá igual.

[34] ISO 27001:2013 [Citado el 22 de octubre de 2021]. Disponible en Internet: https://normaiso27001.es/

Al hacer esto, ayuda a identificar los riesgos para su información confidencial y a implementar los controles apropiados para ayudar a reducirlos.

Dentro de los beneficios de la Gestión de la Seguridad de la Información se encuentran:

- Identifica los riesgos y coloque controles en el sitio para gestionarlos o eliminarlos.
- Flexibilidad para adaptar controles a todas las áreas o áreas seleccionadas de su organización.
- Gane la confianza de los interesados y de los clientes de que sus datos están protegidos.
- Demuestre cumplimiento y gane estatus como proveedor preferido.
- Satisfaga más expectativas de licitaciones al demostrar cumplimiento.

ISO/IEC27002:2013[35] definido como lista de buenas prácticas de seguridad de la información, la lista se desarrolla en base a la experiencia de implementación del control de seguridad de la información aceptada por las empresas y organizaciones más importantes del mundo.

Por lo tanto, se recomienda utilizar la Norma 27002 como guía para implementar medidas de control y seguridad. Esta guía debe utilizarse en forma de LISTA DE VERIFICACIÓN para seleccionar las medidas de control aplicables a partir de los resultados del análisis o la evaluación de riesgos, lo que no solo determinará qué medidas de control se aplican, sino que también determinará el alcance o los recursos de las medidas de control aplicables.

Resolución CREG 015 del 2018[36]. Por la cual se establece la metodología para la remuneración de la actividad de distribución de energía eléctrica en el Sistema Interconectado Nacional. Ítem 5.2.11.2 Registro de la información de los eventos

Reglamento Técnico de Instalaciones Eléctricas (RETIE)[37] cuyo objetivo es determinar las estrategias que brinden una garantía de seguridad a todas las personas, a los recursos animales y vegetales, preservando los recursos naturales y logrando eliminar, prevenir y minimizar los riesgos que se puedan ocasionar por las actividades realizadas en empresas eléctricas.

[35] ISO 27002:2013 [Citado el 05 de diciembre de 2022]. Disponible en Internet: https://normaiso27001.es/

[36] Resolución CREG 015 / 2018. Comisión de Regulación de Energía y Gas CREG. Citado el 22 de octubre de 2021]. Disponible en Internet:http://apolo.creg.gov.co/Publicac.nsf/1c09d18d2d5ffb5b05256eee00709c02/65f1aaf1d57726a90525822900064dac/$FILE/Creg015-2018.pdf

[37] Reglamento Técnico de Instalaciones Eléctricas – RETIE. [Citado el 22 de octubre de 2021]. Disponible en Internet: https://www.minenergia.gov.co/retie

La Ley 1273 de 2009[38] Con la modificación del Código Penal, se crea un nuevo bien jurídico protegido - denominado "Protección de la Información y los Datos" - y se protegen los sistemas que utilizan las TIC. completamente completo, entre otras disposiciones, comprende:

Artículo 269A: Acceso abusivo a un sistema informático.
Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.
Artículo 269C: Interceptación de datos informáticos.
Artículo 269D: Daño Informático.
Artículo 269E: Uso de software malicioso.
Artículo 269F: Violación de datos personales.
Artículo 269G: Suplantación de sitios web para capturar datos personales.
Artículo 269H: Circunstancias de agravación punitiva.
Artículo 269I: Hurto por medios informáticos y semejantes.
Artículo 269J: Transferencia no consentida de activos

[38] Ley 1273/2009 [Citado el 22 de octubre de 2021]. Disponible en Internet: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

5 DESARROLLO DE LOS OBJETIVOS

5.1 OBJETIVO 1: DETERMINACION DE LA IMPORTANCIA DE LA CIBERSEGURIDAD APLICADA EN LOS SISTEMAS SCADA EN LAS EMPRESAS DEL SECTOR ELÉCTRICO COLOMBIANO PARA UNA ADECUADA GESTIÓN DEL RIESGO CIBERNÉTICO EN SU OPERACIÓN, BASADO EN LA REVISIÓN DOCUMENTAL Y LOS ESTÁNDARES ESTABLECIDOS A NIVEL INTERNACIONAL

La creciente interconectividad y la dependencia de las plataformas y servicios basados en internet han aumentado considerablemente la exposición al riesgo de los gobiernos, las empresas y los ciudadanos, a toda una gran variedad de actos relacionados con la delincuencia, el espionaje y la seguridad cibernética. De acuerdo con un estudio de la Organización de Estados Americanos (OEA), los datos disponibles indican que los incidentes y los ataques cibernéticos, en particular aquellos que se realizan con intenciones criminales, están aumentando en frecuencia y en los niveles de sofisticación. Los gobiernos y las empresas reconocen la necesidad de tener políticas y estrategias nacionales de seguridad cibernética, cultura cibernética, educación, formación y competencias de seguridad, marcos jurídicos, reglamentarios y normatividad, así como también contar con cooperación e intercambio de información. [39]

Los incidentes que han ocurrido en los últimos años han ocasionado que las organizaciones sean más conscientes de la importancia de la ciberseguridad en los sistemas de control industrial. El número de incidentes que han sido reportados al Equipo de Respuesta ante emergencias Informáticas (CERT) de la Directiva Europea, ha aumentado tanto en los últimos años que, a partir del año 2003, el CERT dejo de contar los incidentes, ya que los números ascendían a cifras considerables, tanto así que durante el año 2003 se alcanzaron a reportar más de ciento veinte mil incidentes. No solo aumentó el número de ataques, sino que también sus niveles de sofisticación.[40]

En la industria energética, se puede observar que las redes eléctricas, desde la generación hasta la trasmisión, la distribución y comercialización están experimentando altos niveles de trasformación en sus arquitecturas y una mayor convergencia entre las tecnologías de la operación (TO) y las tecnologías de la información y la comunicación TIC. En las redes futuras, aparecerán cientos o miles de millones de dispositivos de energía distribuidos, paneles solares, nuevos medidores inteligentes para medición avanzada, nuevos generadores de energía,

[39] GARCIA, Julián Andrés. Trabajo final de Master: Investigación de la Ciberseguridad aplicada a los Sistemas de Control Industrial con Énfasis en el sector energético. [Citado el 20 de Noviembre de 2020]. Disponible en internet : http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72749/6/jgarciaariasTFM0118Memoria.pdf

[40] Ibid. pág. 11

otros medios de trasporte eléctrico, ciudades y edificios inteligentes, nuevos tipos de almacenamiento de energía; así como otros sistemas electrónicos de diversas magnitudes. Todos estos elementos adquirirán nuevas capacidades y soportarán nuevos servicios, lo que llevará a las redes y medios de comunicación a brindar acceso e interconectividad en lugares donde antes no había el acceso, porque no existía o simplemente porque no se concebía. Aparecerán nuevas formas de generar y consumir energía y se utilizara de forma más flexible y en ese mismo sentido aparecerán nuevas vulnerabilidades y riesgos cibernéticos.[41]

La información de una empresa es considerada en la actualidad como uno de los factores más importantes correspondientes a su competitividad. El uso de sistemas de automatización que permitan la supervisión y el control y adquisición de datos (SCADA, del inglés *Supervisory Control And Data Acquisition*) son necesarios. Las organizaciones emplean este tipo de sistemas para mejorar no solo la eficiencia y eficacia en los procesos, sino adicionalmente para cuidar su seguridad industrial, denotando que con la competitividad acrecentada también se presentan de manera consecuente riesgos que ponen en peligro el actuar de la organización.[42]

Concretamente el sistema SCADA permite que un operador logre realizar procesos industriales tales como: ajustes y cambios, al igual que paradas de emergencia y arranque de equipos desde una estación de programación remota a través de una interfaz amigable, permitiendo una integración hombre máquina. Los sistemas SCADA se desarrollaron para trabajar en redes siempre aisladas, por lo que la seguridad de la información nunca le dió importancia. Sin embargo, durante los últimos años, estos sistemas se han venido integrando a la misma red física de las redes de TI (Tecnología Informática) y a campos como la IoT (*Internet de los Cosas*) en procesos industriales que tienen rápido crecimiento, permitiendo mayor flexibilidad y conectividad entre dispositivos y sensores. Estas integraciones logran reducir costos de instalación y posibilitan la conexión desde fuera de la empresa, ya sea para generar control de rutina, gestión de alarmas o simplemente soporte técnico.[43]

Se puede concluir que debido a la información que transmite y procesa los sistemas automatizados, es de vital importancia que las empresas de energía Colombia diseñen, implementen y mantenga los sistemas SCADA basado en una estimación de recursos adecuada, buscando apoyo de entidades que les guíen en la elaboración e implementación de estándares acorde a su tamaño y que facilite la actualización constante de los equipos y sistemas., a fin de garantizar la

[41] Ibid pág. 11.
[42] TORRES, Ricardo. MEDINA, Fabián. Propuesta metodológica para la auditoría de ciberseguridad aplicada a un sistema SCADA. . [Citado el 21 de Noviembre de 2020]. Disponible en Internet: https://revistas.usb.edu.co/index.php/IngUSBmed/article/download/4307/3735/.
[43] Ibid pág. 63

minimización de factores de vulnerabilidad y riesgo, que puede conllevar a perdida de eficiencia y eficacia de sus procesos.

5.2 OBJETIVO 2: EXAMINAR LAS AMENAZAS Y VULNERABILIDADES MÁS USUALES QUE TIENEN QUE AFRONTAR LAS EMPRESAS DE ENERGÍA COLOMBIANA AL IMPLEMENTAR SISTEMAS SCADA, ANALIZANDO LOS ATAQUES PRESENTADOS EN OTRAS REGIONES Y LA MANERA ADECUADA DE SUBSANAR LAS VULNERABILIDADES.

5.2.1 Amenazas y vulnerabilidades más usuales que tienen que afrontar las empresas de energía colombiana al implementar sistemas SCADA. La evolución tecnológica en los sistemas energéticos ha traído consigo la implementación de diversos equipos digitales especialmente aquellos sistemas que combinan ciertos tipos de automatización y control de acceso remoto son vulnerables a los ciberataques; por ejemplo los sistemas eléctricos que incluyen redes inteligentes. Especialmente frente a los nuevos métodos de terrorismo, utilizan esta estrategia para lograr objetivos políticos o ideológicos y atacar sistemas clave como sistemas de comunicación, sistemas de energía, plantas de tratamiento de agua, centros de mando y control militar[44].

Es importante entender que: “La interconexión de sistemas informáticos empresariales con sistemas de control industrial, implica que las fallas de seguridad de los sistemas informáticos tradicionales (Windows, Linux, Unix, protocolos TCP/IP, etc.) impactarán los sistemas de control que hasta la fecha se encontraban centralizados y aislados”[45]

Los antiguos dispositivos de control e instrumentación industrial (SCADA, EMS) no fueron diseñados para soportar medidas de seguridad tales como: antivirus, detectores de intrusos, mecanismos de autenticación y de control de acceso. Anteriormente, los fraudes en medidores de energía eran muy sencillos; se instalaban servicios directos, se soltaban, se corrían las anclas de tensión y se aislaban con esmalte o cinta, cuando el ancla estaba en la parte exterior del medidor. Con base en esto, se implementaron las primeras cuadrillas que con sólo inspección visual, detectaban dichos fraudes; procedían a abrir los sellos de seguridad, con el fin de intervenir internamente el medidor; ya sea la señal de tensión, los pivotes del imán de freno, puentes entre entrada y salida o el integrador; dichas empresas implementaron la prueba de tiempo-potencia, que

[44] UPME. Seguridad energética para Colombia. . [Citado el 21 de Noviembre de 2020]. Disponible en Internet: https://bdigital.upme.gov.co/bitstream/001/1314/1/Seguridad%20Energ%C3%A9tica%20UPME-CIDET%20Entrega%20Final.pdf

[45] JARAMILLO, Santiago. Amenazas cibernéticas al sistema eléctrico son una realidad en Colombia y el mundo. [Citado el 26 de Noviembre de 2020]. Disponible en Internet: https://www.ventasdeseguridad.com/2017100310190/noticias/empresas/amenazas-ciberneticas-al-sistema-electrico-son-una-realidad-en-colombia-y-el-mundo.html

consta de una resistencia y un cronómetro, tomando diferentes datos para con estos determinar si el medidor se encuentra frenado o intervenido.[46]

Los sistemas de interconexión de media tensión por medio de subestaciones, son el corazón que convierte la energía eléctrica a baja tensión y lleva la energía a los usuarios finales en las principales ciudades del país. Estas subestaciones están siendo modernizadas según la norma internacional IEC 61850 en donde se establece una comunicación vía Ethernet para supervisión y control a distancia de estas subestaciones eléctricas, pudiéndose presentar riesgos de seguridad informática, que terminen en la explotación de vulnerabilidades del sistema y un inminente ataque informático como por ejemplo: alteración de las medidas de sensores de estado de la planta, envió de instrucciones falsas a los actuadores y controles de la planta, implantación de virus o *malware* informático que afectaría el sistema que maneja el Control Lógico Programable (PLC), que podría causar la falla del sistema de control SCADA que maneja la subestación, lo cual puede causar un corte indefinido del suministro eléctrico e incluso catástrofe por daño o explosión en el transformador reductor[47]

Dentro de las características que pueden ser vulnerables de los sistemas SCADA en las empresas de energía en Colombia se pueden mencionar:

Monitorización y control de Infraestructuras Críticas. Actualmente, muchas de las Infraestructuras Críticas se encuentran monitorizadas y controladas por sistemas SCADA, existiendo en muchos casos una dependencia prácticamente absoluta respecto a dichos sistemas. Esta dependencia provoca que el sistema SCADA pase a considerarse como crítico, con las necesidades de seguridad y protección que ello conlleva. Un ejemplo ilustrativo es el de una central nuclear. Estas centrales no pueden funcionar sin estos sistemas, ya que son los encargados de la gestión del proceso de generación de energía, así como de los mecanismos de seguridad que evitan la materialización de riesgos que puedan poner en peligro la integridad de sus instalaciones[48]

Otra de las vulnerabilidades identificadas son las carencias en actualización de software. En ese mismo sentido se encuentra la escasa evolución de los mismos, debido principalmente a su aislamiento inicial y a los riesgos que podría implicar su actualización. El aislamiento para el cual fueron diseñados parece asegurar la imposibilidad de sufrir ataques informáticos, mientras que los posibles riesgos de su actualización se centran en la probabilidad de dejar sin servicio al sistema en caso de error. Estos dos factores han tenido como consecuencia la omisión de las

[46] Ibid pág 1
[47] OTERO, Carlos Eduardo. Análisis de los Riesgos de Seguridad Informática de sistemas SCADA en subestaciones eléctricas en la ciudad de Duitama Boyacá.
[Citado el 28 de Noviembre de 2020]. Disponible en Internet:
https://repository.unad.edu.co/bitstream/handle/10596/14419/74374246.pdf?sequence=1
[48] Ibid pág. 22

actualizaciones que se han encontrado disponibles para los demás sistemas informáticos a medida que se han descubierto vulnerabilidades[49]

Otros de los riesgos y amenazas que presentan los sistemas SCADA se pueden analizar según un estudio realizado por *Positive Technologies* en las cuales hace unas afirmaciones muy serias al respecto:

> Indican que el 40% de los sistemas de monitorización y control en tiempo real SCADA disponibles en internet, pueden ser hackeados fácilmente, la mitad de las vulnerabilidades encontradas permiten la ejecución de código arbitrario en los sistemas destino, un tercio de las vulnerabilidades son debido a malas configuraciones y el uso de contraseñas por defecto y una cuarta parte están relacionados con los administradores de sistema por no instalar actualización de seguridad[50]

Al conocer las amenazas se debe tratar de establecer sus motivaciones para poder responder ante ellas. Dentro de la identificación de posibles amenazas, estaría: "Denegación de servicio, ataques dirigidos, ataques accidentales, acceso y controles no autorizados, código malicioso instalado en las máquinas (gusanos, virus, troyanos, *spam*, *phishing*, *bots*, etc".[51]

Las fuentes de las amenazas o de los atacantes potenciales para una organización incluyen: "Hackers y delincuentes, *Malware* de propagación automática, atacantes internos, personal descontento, personal realizando acciones no autorizadas, acciones accidentales, inteligencia corporativa, contratistas, servicios de inteligencia extranjeros, crimen organizado, terroristas y manifestantes y activistas medioambientales, políticos, etc".[52]

5.2.2 Ataques informáticos a las Infraestructuras Criticas. Según el plan nacional de protección de infraestructura crítica, la definición es la siguiente: "Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas".

Dentro de las infraestructuras criticas se definen los siguientes sectores: Energía, Agua, Finanzas, TIC, Transportes entre otros. En otras palabras, todas estas son infraestructuras, y sus sistemas, métodos y servicios son la base del progreso

[49] Ibid pág. 22
[50] ARIAS, Javier Eduardo. Riesgos a los sistemas SCADA en empresas Colombianas. [Citado el 28 de Noviembre de 2020]. Disponible en Internet: http://polux.unipiloto.edu.co:8080/00001601.pdf
[51] Ibid pág. 5
[52] Ibid pág. 5

social. Y servicios para asegurar el normal funcionamiento de los servicios prestados por el estado y la administración pública.

El enfoque en la seguridad de la red es garantizar la continuidad de las actividades y los servicios prestados a los ciudadanos. La interrupción más pequeña del servicio puede tener un gran impacto en la organización por lo tanto, en un gran número de personas. A su vez, los objetivos de los ciberataques también han cambiado, los beneficios económicos que buscan los ciberdelincuentes han pasado a segundo plano. Sus intenciones van mucho más allá de la obtención de dinero a través de actividades ilícitas. Los ciberdelincuentes actuales buscan vulnerabilidades en los sistemas de infraestructura crítica con el fin de obtener información relevante, controlar una actividad o toda la organización, y pueden empeorar la situación, paralizar o finalizar la actividad. Por consiguiente, en un entorno cada vez más complejo, interconectado y en evolución, las medidas de seguridad y protección se han vuelto críticas.

La ciberseguridad está restringida por factores internos y externos, buscando asegurar la calidad y continuidad de los servicios y el cumplimiento de la normativa vigente, llevando a la infraestructura crítica a repensar su estrategia de ciberseguridad. Dentro de las problemáticas más comunes están:

- Sistemas obsoletos o inseguros.
- *Hardware* obsoleto.
- Falta de talento.
- Agujeros de seguridad en el diseño.
- El número de dispositivos conectados aumenta.
- Protección de la red.
- Falta de preparación y conciencia.
- Requisitos legales más altos.

Los sistemas SCADA están presentes en varias industrias. Sin embargo, su principio de aplicabilidad es igual en todos los sectores productivos, se busca la automatización de procesos como la operación y el mantenimiento.

Ejemplos reales de ataques cibernéticos efectuados a infraestructura critica

La empresa Open Data Security (ODS) realiza un compilatorio sobre los ataques cibernéticos que se han realizado a infraestructura critica a lo largo de los años en diversas empresas alrededor del mundo[53]

[53] ODS. Ciberseguridad en las infraestructuras críticas. Disponible en internet: https://opendatasecurity.io/ciberseguridad-en-las-infraestructuras-criticas/

2000 – Sistema de bombeo, Morrochy Shire Town, Queensland, Australia+

En abril del 2000, en la planta de tratamiento de aguas residuales en Morrochy Shire Town, Queensland, Australia, sufrió un ataque por un exempleado, el cual afecto las 142 estaciones de bombeo y los servidores que controlaban la frecuencia de radio.
El sistema SCADA implementado en la planta de aguas residuales fue ejecutado por la compañía Hunter Watertech Pty Ltda empleando tecnología PDS Compact 500 para la gestión, el control y supervisión de las estaciones de bombeo, por medio de la cual se monitoreaba utilizando portadoras con un enlace de radio analógico y bidireccional. El ataque consistió en modificar las tramas de comunicación de las bombas, como consecuencia de esta intrusión maliciosa el sistema presento errores de funcionamiento haciendo que las bombas no encendieran en su ciclo normal, el sistema de alarmas local en las estaciones de bombeo perdió comunicación con la estación central y se iniciaron constates pedidas del enlace de comunicación entre los diferentes dispositivos. [54]

2006 – 2011 Ataques chinos y *Utilities* vulnerables

McAfee detecto e investigo el ataque conocido como *Night Dragon* generado por China y dirigido a compañías de *Utilities*, su principal objetivo era el de acceder a información sensible y así espiar las actividades en las compañías de *Utilities*. El plan ejecutado por fases logro legar a su objetivo. Su primer paso fue vulnerar los servidores públicos (sitios web) lo que les abrió un puente hacia la red interna de las organizaciones. Es decir, emplearon una serie de ataques que les permitió vulnerar más de 71 organizaciones.

2017 – Ciberataque con Triton en Arabia Saudí

Los ciber terroristas asumieron el control remoto de una estación de trabajo ampliamente conocida que estaba en Arabia Saudita, emplearon el *malware* denominado Triton, tomando el control del sistema de seguridad instrumentado (SIS por sus siglas en inglés). Sin embargo, este *malware* no solo ataco esta empresa, alcanzo a propagarse por varias, según lo documentado en el 2019.[55]

2015- 2016 Las redes eléctricas de Ucrania y el *Black Energy*

[54] Malicious Control System Cyber Security Attack Case Study–Maroochy Water Services,Australia.{En línea}. {12 diciembre 2018}.Disponible en:http://www.scadahackr.com/library/Documents/Case_Studies/Case%20Study%20-%20NIST%20-%20Maroochy.pdf

[55] Davis Ariel, MIT Technology Review. Así se propaga Triton, el malware que amenaza a la industria mundial. Disponible en https://www.technologyreview.es//s/11009/asi-se-propaga-triton-el-malware-que-amenaza-la-industria-mundial

Considerado uno de los primeros ciberataques y/o casos cuyo alcance afectó a un servicio crítico imprescindible. En Ucrania miles de hogares se quedaron sin energía eléctrica durante el invierno de 2016 en pleno invierno. Empleando un *malware* de negación de servicio, los ciberdelincuentes lograron afectar más de 30 plantas eléctricas parando la generación de energía en dichas instalaciones. Los investigadores de este ataque apuntaron a un claro caso de *phishing*, mediante el cual se propagó el programa malicioso que hizo posible aquel apagón. [56]

2010 – Fallas sospechosas en Natanz, Irán

En enero de 2010, en la planta de energía nuclear de Natanz en Irán, las centrifugadoras de uranio comenzaron a funcionar mal. Les tomó 5 meses darse cuenta de que se trataba de un ciberataque llevado a cabo por un virus informático malintencionado. El virus puede atacar el controlador lógico programable del PLC y controlar el equipo, provocando fallos de funcionamiento o invalidando la centrífuga. Además de hacer que la planta de energía nuclear de Natanz estuviera inactiva por un tiempo, el ataque cibernético también afectó hasta mil centrifugadoras.

2017 – Otros ataques a Ucrania y sus infraestructuras críticas.

En 2017, Ucrania quedó paralizada. Las actividades diarias de los vehículos de transporte son anormales, el aeropuerto no muestra información sobre el vuelo y la máquina de pago en el metro deja de funcionar. El gobierno registró fallas en sus computadoras, incapaces de medir la radiación de Chernobyl, y el Banco Central de Ucrania también fue atacado. Un escenario aparentemente imposible, pero ya sucedió y ha desencadenado malware, es decir, virus informáticos.

2019 – América del Sur y el *malware* “Machete”

El *malware* denominado “Machete” y descubierto en 2010 no ha dejado de propagarse. Diseñado específicamente para robar datos sobre sus tropas del ejército latinoamericano y según los expertos en ciberataques, el virus se propagó a través del *phishing*, y después de 9 años de vida, sigue propagándose e infectando los equipos del gobierno latinoamericano. [57]

Como se puede ver, los ataques que se han detectado y documentado en los últimos años, han conllevado a la perdida de información valiosa y fallas en la prestación de servicios esenciales como es los cortes o perdida de suministro de la energía eléctrica, dejando como enseñanza que los sistemas industriales deben de

[56] ESET, BlackEnergy y el corte energético de Ucrania: ¿qué sabemos realmente? Disponible en https://www.welivesecurity.com/la-es/2016/01/13/blackenergy-corte-energetico-de-ucrania-que-sabemos/

[57] Kavantic, ‘Machete’, la ‘ciberamenaza’ que afecta gobiernos en Latinoamérica. Disponible en https://www.kavantic.com/machete-la-ciberamenaza-que-afecta-gobiernos-en-latinoamerica/

estar separados o segmentados de los sistemas TI y que las organizaciones deben de implementar equipos de respuesta a incidentes de seguridad informáticas (CSIRT) para que se pueda de manera interna, con el fin de que pueda coordinar y respaldar la respuesta a un evento o incidente de seguridad informática

5.3 OBETIVO 3: PROPONER RECOMENDACIONES PARA LA GESTIÓN DE LA SEGURIDAD PARA LAS EMPRESAS DE ENERGÍA ELÉCTRICA COLOMBIANA CON EL FIN DE PREVENIR Y ASEGURAR SU INFRAESTRUCTURA ELÉCTRICA DE ATAQUES CIBERNÉTICOS

Según estudios de la empresa Positive Technologies donde se indica que el 40% de los sistemas SCADA pueden ser atacados fácilmente por ciberdelicuentes, identificando que las vulnerabilidades más frecuentes son aquellos que permiten la ejecución de código arbitrario y la principal vulnerabilidad es debido a configuraciones mal realizadas, el uso de contraseñas sin nivel de protección (por defecto) o por la falta de actualización de los sistemas.[58]

Todo experto en seguridad informática, sabe que al conocer las amenazas se debe establecer primero las motivaciones del atacante con el fin de saber como responder a ellas. Como se indica en el punto anterior, dentro de las posibles amenazas están:

- Denegación del sistema
- Ataques dirigidos
- Ataques accidentales
- Accesos y control no autorizados
- Código malicioso instalado en las maquinas

Y dentro de las amenazas potenciales se incluyen:

- *Hackers*
- *Malware* de propagación automática y sistemática
- Amenazas internas
- Personal descontento o realizando acciones no autorizadas
- Servicios de inteligencias extranjeras
- Crimen organizado o terroristas

La función principal de un sistema SCADA es el acceso a la información en tiempo real, que permita la toma de decisiones y la operación automatizada, por lo que una indisponibilidad del mismo, puede acarrear problemas operacionales.

[58] V. MOTOS, «HACK PLAYERS,» 13 NOVIEMBRE 2012. [En línea]. Disponible en http://www.hackplayers.com/2012/11/informe-alerta-seguridad-scada.html. [Último acceso: 20 mayo del 2021]

Dentro de las estrategias para aseguramiento de los sistemas SCADA se podrían indicar, las siguientes:

Principios básicos: En el estudio de la presente monografía se ha analizado la aplicación de sistemas SCADA, permitiendo identificar los tres principios básicos de aseguramiento, los cuales buscan: Proteger, Detectar y Responder. Estos principios pretenden básicamente, implementar medidas de protección para prevenir y desalentar los ataques, también, el establecer mecanismos que permitan identificar de manera oportuna los ataques que intenten entra al sistema así mismo, que cuando algún ataque llegue al sistema, se tengan medidas de respuesta.

Es importante dentro de los principios básicos, el diseño de un marco de seguridad para cualquier sistema de control no se debe limitar al despliegue de medidas de protección, también es importante ser capaz de detectar posibles ataques y responder de forma adecuada para minimizar su impacto. [59]

Medidas de reducción de riesgo: Las medidas de reducción de riesgo permiten disminuir el costo de operación, medir la eficacia de las medidas, verificar la dificultad de la implementación de una medida así mismo deberá verificar las soluciones existentes y crear grupos de atención ante emergencias.

Buenas prácticas: La buenas prácticas de la seguridad informática que se deben tener en cuenta a la hora de analizar y formular estrategias para la gestión de la seguridad son: el estudiar el riesgo con el fin de comprender los sistemas con los que se va a trabajar, comprender las amenazas a las que se expone, percibir el impacto que puede haber al materializarse un incidente, entender las vulnerabilidades a través de evaluaciones, auditorias y verificaciones a los diferentes sistemas, tanto físicos como lógicos.

Otra buena práctica es el de realizar el análisis y estudio continuo riesgo en función de la amenaza, los impactos y las vulnerabilidades para identificar cualquier cambio, reevaluar el riesgo y poner en marcha las mejoras de seguridad que se requieran.

Diseño e implementación de arquitecturas seguras:

Según la Guía de Seguridad de las TIC el diseño de una arquitectura segura para empresas que requieren de sistemas de monitorización y control en tiempo real, debe de incluir:

- Arquitectura de la red
- Sistemas Cortafuegos

[59] CCN, GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-480) SEGURIDAD EN SISTEMAS SCADA, 2010. Disponible en https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/205-ccn-stic-480-seguridad-en-sistemas-scada/file.html

- Acceso Remoto
- Software Anti Virus
- Correo electrónico
- Acceso a internet
- Fortalecimiento del sistema
- Fortalecimiento de la Plataforma Tecnológica
- Copias de seguridad y recuperación Seguridad Física
- Seguridad Lógica
- Monitoreo de los sistemas
- Monitoreo de la Plataforma Tecnológica
- Redes Alámbricas e Inalámbricas.
- Actualizaciones y/o parches de seguridad
- Verificación de antecedentes del personal con acceso y control a los sistemas SCADA.
- Contraseñas, cuentas y perfiles de usuario
- Control documental
- Infraestructura e instalaciones adecuadas
- Gestión de vulnerabilidades
- Rotación de personal
- Gestión del cambio
- Pruebas de seguridad
- Análisis de conectividad de nuevos dispositivos
- Capacitación de personal
- Verificación de Terceros
- Verificación de Proveedores

El objetivo de proteger el entorno de OT puede parecer angustioso a simple vista; sin embargo, hay que tener en cuenta que la mitigación de los riesgos se realiza de manera gradual, lo primero es contar o preparar un ambiente resiliente y seguro, optimizando los recursos con el fin de poder responder a las necesidades sin dejar a un lado las amenazas de TI y OT. Aunque se recomienda que las empresas, sin importar el sector, adopten siempre nuevas tecnologías que permitan la actualización constante de sus sistemas operativos, antivirus y demás componentes de software, con el fin de mejorar la seguridad, prestando especial atención a no implementar soluciones técnicas y operativas, sino soluciones estratégicas e integrales.

6. CONCLUSIONES

Con el desarrollo de esta monografía se han identificado los diferentes riesgos y amenazas asociados a los sistemas SCADA, así como también permitió determinar pautas de buenas prácticas para implementar a dichos sistemas con el fin de salvaguardar el activo de información; para este propósito, las empresas de energía eléctrica en Colombia se les propone tener en cuenta cada recomendación que se plantea en este trabajo, dado que les permitirá minimizar el riesgo en caso de ser atacados por una amenaza y ésta no logre causar daños económicos y físicos con un impacto muy alto al sistema ni a la organización.

En ese mismo sentido, es importante resaltar que brindar aseguramiento es una tarea compleja para todas las empresas de energía de Colombia, ya que al momento de adquirir cualquier sistema de monitoreo en tiempo real (SCADA), deben solicitar al proveedor que garantice que el producto cumple con los requisitos mínimos de seguridad. Sin embargo, aún si éstos garantizan esos requisitos no significa que la organización va estar segura sino que van a mantener un riesgo residual el cual el impacto será menor en caso de llegarse a presentar un incidente de seguridad que no se tenga identificado.

Es por ello, que los ataques a los sistemas SCADA pueden repercutir a nivel económico y social en la comunidad y hasta el momento, Colombia no tiene un marco regulatorio, estándares y/o pautas para la correcta implementación de sistemas de monitoreo y control en tiempo real; sin embargo, a nivel mundial se han podido establecer algunos como es el CCN (Centro Criptológico Nacional). Guía CCN- STIC-480 en materia de Seguridad en Sistemas SCADA, IEEE (Institute of Electrical and Electronics Engineers) IEEE PC37.1™ Draft Standard for SCADA and Automation Systems y ENISA (European Network and Information Security Agency) “Protecting Industrial Control Systems. Recommendations for Europe and Member States. Estos estándares mundiales permiten tener las bases para una buena práctica de implementación.

Es preciso indicar que a pesar de esto, no existe una fórmula para garantizar la seguridad de todos los activos clave en sistemas de infraestructura critica, tampoco puede haber estándares o componentes técnicos que garanticen que todo saldrá bien factores como el apoyo y compromiso de la alta dirección, recursos la importancia de la distribución y la ciberseguridad industrial deben de estar siempre presentes en la agenda. La adopción de buenas prácticas, normas y estándares constituye una valiosa hoja de ruta, pero el desafío en la aplicación es la transición de "qué hacer" a "cómo hacer". Tener que explicar las necesidades, obtener apoyo de la gerencia, obtener recursos, gestionar riesgos, diseñar indicadores para tomar decisiones y demostrar el retorno de la inversión son algunos de los retos que tiene que pasar la implementación de las guías de ciberseguridad sugeridas a nivel mundial.

Como apreciación final, es importante que se comprenda la importancia de los sistemas de infraestructura crítica y sus sistemas de monitorización (SCADA) además de que se identifique y conozca las vulnerabilidades a las cuales se están exponiendo los sistemas de infraestructura critica Colombia al implementar este tipo de controles automatizados, tambien de identificar el soporte que estos sistemas brindan al desarrollo de la sociedad.

7. RECOMENDACIONES

Para terminar, se presentan cuatro (4) recomendaciones fundamentales que deben de ser abordados por las empresas de energía con el fin de elevar el nivel de ciberseguridad al momento de implementar infraestructura critica, específicamente sistemas de información SCADA:

- Segmentar la red: Este es uno de los conceptos más efectivos en cuanto a arquitectura, que permite lograr el objetivo de mejorar la seguridad para los sistemas SCADA, la segmentación se debería diseñar e implementar para ser dinámica. Un framework que se podría aplicar es la ISA/IEC-62443, la cual, dicta guía practicas para lograr una segmentación de red adecuada, dándole a cada zona un nivel de seguridad, evaluado entre 0 y 4, donde 0 indica lo mas bajo en cuanto a seguridad y 4 el más alto.

- Monitorear tráfico: Permite conocer si la información que se trasmite cuenta con el ancho de banda suficiente para garantizar su correcta recepción y trasmisión, además de alertar de manera temprana la presencia de una amenaza conocida, identificar anomalías de tráfico y de usabilidad que pudiesen ser antecedentes a un ataque cibernético.

- Control de Acceso y dispositivos: Considerar la mejor manera de limitar el acceso a un sistema o a recursos físicos o virtuales. Iniciativas de NAC (Network Access Control), RBAC (Role Based Access Control) y de Gestión de Accesos se alinean con este objetivo.

- Proteger puntos de acceso: Es necesario que los dispositivos, sensores y demás dispositivos o componentes de la infraestructura critica, cuenten con seguridad por diseño, y que sean administrados desde una interfaz central en lugar de manera particular.

8. BIBLIOGRAFÍA

AGUILAR Joyanes, Luis Industria 4.0 La cuarta revolución industrial, Editorial AlfaOmega 2019

ARIAS, Javier Eduardo. Riesgos a los sistemas SCADA en empresas Colombianas. [Citado el 28 de Noviembre de 2020]. Disponible en Internet: http://polux.unipiloto.edu.co:8080/00001601.pdf

BAQUERO Salamanca, Germán Darío. Seguridad de la Información en Sistemas SCADA. Universidad Piloto de Colombia. [Citado el 21 de octubre de 2021]. Disponible en Internet: http://polux.unipiloto.edu.co:8080/00001512.pdf

CABRERA, Elibeth. Control. [Citado el 15 de Noviembre de 2020]. Disponible en internet: https://www.monografias.com/trabajos14/control/control.shtml

CERVANTES, Nancy. Operaciones. [Citado el 15 de Noviembre de 2020]. Disponible en internet: http://www.utn.edu.ec/reduca/programacion/fundamentos/operaciones.html

COBB, Stephen. Aumentan los ataques a infraestructuras críticas. 1 ed. ESET, pp.11-13. [Citado el 15 de Noviembre de 2020]. Disponible en internet: https://www.welivesecurity.com/wp-content/uploads/2017/12/Tendencias_2018_ESET.pdf

CHEREPANOV, Anton. Industroyer: la mayor amenaza para sistemas de control industrial desde Stuxnet. En línea. 09 de mayo de 2018. Disponible en: https://www.welivesecurity.com/la-es/2017/06/12/industroyer-amenaza-control-industrial/

COLOMBIA. COMISION DE REGULACION DE ENERGIA Y GAS. Concepto 2938 de 2004. Bogotá. 2004 Disponible en internet: https://www2.javerianacali.edu.co/sites/ujc/files/normas_icontec.pdf

COMISIÓN REGULADORES DE ENERGÍA YGAS- CREG, Resolución CREG 015 del 2018, Numeral 5.2.11.2 Registro de la información de los eventos. Disponible en http://apolo.creg.gov.co/Publicac.nsf/1c09d18d2d5ffb5b05256eee00709c02/65f1aaf1d57726a90525822900064dac/$FILE/Creg015-2018.pdf

CONDLIFFE, Jamie. El virus del apagón en Ucrania es "la mayor amenaza" informática desde 2009. [Citado el 15 de Noviembre de 2020] Disponible en Internet:

https://www.technologyreview.es/s/7951/el-virus-del-apagon-en-ucrania-es-la-mayor-amenaza-informatica-desde-2009

CONSEJO NACIONAL DE POLITICA ECONOMICA Y SOCIALCOLOMBIA. Política nacional de seguridad digital. p. 44. [Citado el 10 de Noviembre de 2020] Disponible de: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

CORNELEC. Gestión Estratégica de Activos En las Redes Eléctricas. [Citado el 5 de Noviembre de 2020]. Disponible en internet: https://cornelec.cl/2015/10/23/gestion-estrategica-de-activos-en-las-redes-electricas/

CSIT-CV, Centro de Seguridad de la comunidad Valencina, 2014. [Citado el 25 de Noviembre de 2020]. Disponible en Internet: https://www.csirtcv.gva.es/sites/all/files/downloads/%5BCSIRT-CV%5D%20Informe-Internet_de_las_Cosas.pdf

Directiva Europea, DIRECTIVA 2008/114/CE DEL CONSEJO. Disponible en: https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/DirectivaEuropea2008-114-CE.pdf

Energía y Sociedades, Smart Grid, 2010. [Citado el 12 de Noviembre de 2020]. Disponible en Internet: http://www.energiaysociedad.es/manenergia/4-5-smart-grids/

ESCRIBANO, Gonzalo. Seguridad Energética: concepto, escenarios e implicaciones para España y la UE (DT). [Citado el 25 de Noviembre de 2020]. Disponible en: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/dt33-2006

GARCIA, Julián Andrés. Trabajo final de Master: Investigación de la Ciberseguridad aplicada a los Sistemas de Control Industrial con Énfasis en el sector energético. [Citado el 2 de Noviembre de 2020]. Disponible en Internet: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72749/6/jgarciaariasTFM0118Memoria.pdf

GIRAL, William -RAMÍREZ, Hugo. Smart grids in the colombian electric system: Current situation and potential opportunities. [Citado el 10 de Noviembre de 2020] Disponible en Internet: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-921X2017000300119

GÓMEZ, Emilio. ¿Qué son las Operaciones en una Empresa? [Citado el 25 de Noviembre de 2020]. Disponible en internet: http://impconsultores.com/que-son-las-operaciones-en-una-empresa/

Guide to Industrial Control Systems (ICS) Security, p21. [Citado el 25 de Octubre de 2020]. Disponible en internet: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

HudsonAnalytix, Inc, Glosario de Seguridad Cibernética Para La Comisión Interamericana de Puertos, Organización de los Estados Americanos. [Citado el 16 de Octubre de 2020]. Disponible en internet: http://portalcip.org/wp-content/uploads/2019/12/HA-CIP-Glosario-de-Seguridad-Cibern%C3%A9tica-ESP.pdf

INCIBE_CERT, BlackEnergy y los sistemas críticos. [Citado el 25 de Noviembre de 2020]. Disponible en internet: https://www.incibe-cert.es/blog/blackenergy-sistemas-criticos

INFOBAE. Un ataque cibernético de Estados Unidos afectó la capacidad de Irán de disparar contra buques petroleros en el Golfo Pérsico. [Citado el 15 de Noviembre de 2020] Disponible en Internet: https://webcache.googleusercontent.com/search?q=cache:EL-jUiDW5FIJ:https://www.infobae.com/america/mundo/2019/08/28/un-ataque-cibernetico-de-estados-unidos-afecto-la-capacidad-de-iran-de-disparar-contra-buques-petroleros-en-el-golfo-persico/+&cd=8&hl=es-419&ct=clnk&gl=co

INFORMATIZARTE. Conceptos básicos de Seguridad Informática. [Citado el 25 de Noviembre de 2020]. Disponible en internet: http://informatizarte.com.ar/blog/?p=2731

JARAMILLO, Santiago. Amenazas cibernéticas al sistema eléctrico son una realidad en Colombia y el mundo. [Citado el 26 de Noviembre de 2020]. Disponible en Internet: https://www.ventasdeseguridad.com/2017100310190/noticias/empresas/amenazas-ciberneticas-al-sistema-electrico-son-una-realidad-en-colombia-y-el-mundo.html

KUNBUS, Ethernet POWERLINK. [Citado el 15 de Noviembre de 2020]. Disponible en internet: https://www.kunbus.com/ethernet-basics.html

KASPERSKY, El origen de Stuxnet, 2014. [Citado el 5 de Noviembre de 2020]. Disponible en internet: https://www.kaspersky.es/blog/el-origen-de-stuxnet/4887/

LANGNER, Ralph. Robust Control System Networks: How to Achieve Reliable Control After Stuxnet. New York: Momentum Press, 2012.

LAPIEDRA, Rafael. DEVECE, Carlos. Introducción a la Gestión de Sistemas de Información En la Empresa. [Citado el 1 de Noviembre de 2020]. Disponible en internet: https://libros.metabiblioteca.org/bitstream/001/193/8/978-84-693-9894-4.pdf

LIOMAN Lima, BBC - Estados Unidos vs Rusia: cómo el hackeo de las redes eléctricas se convirtió en un nuevo campo de batalla entre Washington y Moscú. [Citado el 25 de Noviembre de 2020] Disponible en: https://www.bbc.com/mundo/noticias-internacional-48668879

MANTILLA, Alexandra. Activos Operacionales. [Citado el 8 de Noviembre de 2020]. Disponible en internet: http://mariamantilla.blogspot.com/2009/04/dias-de-pago.html
McAfee Labs, Predicciones sobre amenazas para 2017. Noviembre 2016 [en Línea] disponible en: https://mcafee.app.box.com/v/2017predictionsSP

MENDOZA, Pedro Julio. Ataques informáticos a la infraestructura crítica del sector eléctrico colombiano. [Citado el 29 de Noviembre de 2020]. Disponible en Internet: https://repository.unad.edu.co/bitstream/handle/10596/27757/%09pjmendozav.pdf?sequence=1&isAllowed=y

Microsoft, Modelado de riesgos de la arquitectura de referencia de Azure IoT [Citado el 25 de Noviembre de 2020]. Disponible en internet: https://docs.microsoft.com/es-es/azure/iot-fundamentals/iot-security-architecture

NetCloud, Tecnologías de la información IT vs. tecnologías de la operación OT. Disponible en https://netcloudengineering.com/tecnologia-informacion-it-operacion-ot/

NI, Información Detallada sobre el Protocolo Modbus. [Citado el 25 de Noviembre de 2020]. Disponible en internet: https://www.ni.com/es-co/innovations/white-papers/14/the-modbus-protocol-in-depth.html

ORTIZ, Antonio. Ciberseguridad en Redes de Control Industrial. [Citado el 28 de Octubre de 2020]. Disponible en Internet: https://www.isamex.org/intechmx/index.php/2017/09/22/ciberseguridad-en-redes-de-control-industrial-SCADA/

OTERO, Carlos Eduardo. Análisis de los Riesgos de Seguridad Informática de sistemas SCADA en subestaciones eléctricas en la ciudad de Duitama Boyacá. [Citado el 28 de Noviembre de 2020]. Disponible en Internet: https://repository.unad.edu.co/bitstream/handle/10596/14419/74374246.pdf?sequence=1

Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia, 2019. Recuperado de: https://www.ccoc.mil.co/ciberdefensa_maquetacion_biblioteca_publica_conpes.

REINERIO, Camacho. Ciberseguridad y Ciberdefensa en Colombia. [Citado el 25 de Noviembre de 2020] Disponible en internet: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2984/Trabajo%20de%20grado.pdf?sequence=1

SÁNCHEZ, Daniel. Que es un Sistema. [Citado el 5 de Noviembre de 2020]. Disponible en internet: https://www.academia.edu/31110664/Qu%C3%A9_es_un_sistema

TORRES, Ricardo. MEDINA, Fabián. Propuesta metodológica para la auditoría de ciberseguridad aplicada a un sistema SCADA. [Citado el 17 de Noviembre de 2020] Disponible en internet: https://revistas.usb.edu.co/index.php/IngUSBmed/article/download/4307/3735/.

UPME. Seguridad energética para Colombia. . [Citado el 21 de Noviembre de 2020]. Disponible en Internet: https://bdigital.upme.gov.co/bitstream/001/1314/1/Seguridad%20Energ%C3%A9tica%20UPME-CIDET%20Entrega%20Final.pdf

9. ANEXO

9.1 RESUMEN ANALÍTICA ESPECIALIZADO - RAE

Fecha de Realización:	22/10/2021
Programa:	Especialización en Seguridad Informática
Línea de Investigación:	Gestión de sistemas
Título:	Análisis del estado de la ciberseguridad en los sistemas SCADA en el sector eléctrico colombiano
Autor(es):	Michelle Dayanna Castellanos Forero
Palabras Claves:	Ciberseguridad, Infraestructura Critica, SCADA, Energía Eléctrica
Descripción:	Esta monografía está enfocada en los delitos cibernéticos y amenazas que pueden estar presentes hoy en día en el sector eléctrico colombiano con la implementación en auge de sistemas SCADA, los cuales se están convirtiendo en una gran amenaza en varios países. Se centrará en conocer las vulnerabilidades en cuanto a ciberseguridad a las que se enfrentan las empresas de energía, para poder analizar las soluciones que se han brindado para subsanar para dichos ataques; analizando además los ataques que puedan afectar la infraestructura eléctrica. Es importante recordar que este tipo de amenazas surge con el desarrollo e implementación de nuevas tecnologías, por lo que se considera un problema nuevo y por lo que es difícil para las empresas de energía actuar, debido a la falta de experiencia y conocimiento sobre el tema.
Fuentes bibliográficas destacadas: ARIAS, Javier Eduardo. Riesgos a los sistemas SCADA en empresas Colombianas. [Citado el 28 de Noviembre de 2020]. Disponible en Internet: http://polux.unipiloto.edu.co:8080/00001601.pdf	

BAQUERO Salamanca, Germán Darío. Seguridad de la Información en Sistemas SCADA. Universidad Piloto de Colombia. [Citado el 21 de octubre de 2021]. Disponible en Internet: http://polux.unipiloto.edu.co:8080/00001512.pdf
GARCIA, Julián Andrés. Trabajo final de Master: Investigación de la Ciberseguridad aplicada a los Sistemas de Control Industrial con Énfasis en el sector energético. [Citado el 2 de Noviembre de 2020]. Disponible en Internet: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72749/6/jgarciaariasTFM0118Memoria.pdf
JARAMILLO, Santiago. Amenazas cibernéticas al sistema eléctrico son una realidad en Colombia y el mundo. [Citado el 26 de Noviembre de 2020]. Disponible en Internet: https://www.ventasdeseguridad.com/2017100310190/noticias/empresas/amenazas-ciberneticas-al-sistema-electrico-son-una-realidad-en-colombia-y-el-mundo.html
TORRES, Ricardo. MEDINA, Fabián. Propuesta metodológica para la auditoría de ciberseguridad aplicada a un sistema SCADA. [Citado el 17 de Noviembre de 2020] Disponible en internet: https://revistas.usb.edu.co/index.php/IngUSBmed/article/download/4307/3735/.

Contenido del documento:	Planteamiento del problema Objetivo General Objetivos específicos Justificación Marco Teórico Marco Conceptual Marco Legal Desarrollo de los objetivos Conclusiones
Conceptos adquiridos:	Después del desarrollo del trabajo de grado queda claro que la implementación de nuevas tecnologías como IoT en los diversos sectores de la economía y en especial, en el sector eléctrico, debe de ir acompañado de un análisis detallado de las vulnerabilidades a las que se podía quedar expuesto, para así poder tener un plan de acción que permita minimizar la afectación física y económica de las empresas. La tecnología implementada: sensores, actuadores, códigos QR y BiDi, además de las redes 3G, 4G y 5G debe de ser de vanguardia, que permita la actualización constante. IoT se considera un pilar fundamental de la industria 4.0 y los

	sistemas de automatización SCADA hace parte de él, es por ello que la ciberseguridad es un aspecto vital en la implementación de los mismos.
Conclusiones:	Es importante que se comprenda la importancia de los sistemas de infraestructura crítica y sus sistemas de monitorización (SCADA) además de que se identifique y conozca las vulnerabilidades a las cuales se están exponiendo los sistemas de infraestructura critica Colombia al implementar este tipo de controles automatizados, además de identificar el soporte que estos sistemas brindan al desarrollo de la sociedad. A lo largo del documento, se identifica los riesgos y las amenaza que hay para los sistemas SCADA, pero también que a nivel mundial se han planteado guía de buenas prácticas para implementar este tipo de sistemas de manera segura y confiable; para ello, es esencial que las empresas de energía colombiana al diseñar, implementar y mantener Sistema SCADA realicen un análisis correcto sobre la estimación de recursos y otros factores, con el fin de evitar que estos, al ser atacados con éxito, no causen daños económicos y físicos al sistema ni a la organización Los ataques a los sistemas SCADA pueden repercutir a nivel económico y social en la comunidad y hasta el momento, Colombia no tiene un marco regulatorio, estándares y/o pautas para la correcta implementación de sistemas de monitoreo y control en tiempo real, sin embargo, a nivel mundial se han podido establecer algunos. Es preciso indicar que a pesar de esto, no existe una fórmula para garantizar la seguridad de todos los activos clave en sistemas de infraestructura critica, tampoco puede haber estándares o componentes técnicos que garanticen que todo saldrá bien Factores como el apoyo y compromiso de la alta

	dirección, recursos La importancia de la distribución y la ciberseguridad industrial deben de estar siempre presentes en la agenda. La adopción de buenas prácticas, normas y estándares constituye una valiosa hoja de ruta, pero el desafío en la aplicación es la transición de "qué hacer" a "cómo hacer". Tiene que explicar las necesidades, obtener apoyo de la gerencia, obtener recursos, gestionar riesgos, diseñar indicadores para tomar decisiones y demostrar el retorno de la inversión son algunos de los retos que tiene que pasar la implementación de las guías de ciberseguridad sugeridas a nivel mundial.