Lineamientos de ciberseguridad para mejorar la protección de los sistemas de control industrial. Caso de estudio: ISA INTERCOLOMBIA

Claudia Patricia Pérez Arroyave

Trabajo de grado para optar al título profesional:

Maestría en Ciberseguridad y Ciberdefensa

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

2020

MINISTERIO DE DEFENSA NACIONAL

COMANDO GENERAL FUERZAS MILITARES
ESCUELA SUPERIOR DE GUERRA
MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA

LINEAMIENTOS DE CIBERSEGURIDAD PARA MEJORAR LA PROTECCIÓN DE LOS SISTEMAS DE CONTROL INDUSTRIAL. CASO DE ESTUDIO: ISA INTERCOLOMBIA

ALUMNO: CLAUDIA P. PÉREZ ARROYAVE

TUTOR: LUCAS ADOLFO GIRALDO RÍOS MBA, MsC

MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR EL TITULO DE MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA
BOGOTÁ – COLOMBIA
2020

Declaración de originalidad por parte del autor

Mediante la presente certifico que soy la única autora de esta monografía. Todos los materiales usados, referencias de literatura y estudios elaborados por otras personas han sido referenciados en el presente documento. Así mismo este proyecto de grado no se ha presentado para su examen en ningún otro lugar.

Autor: [CLAUDIA P. PÉREZ ARROYAVE]

Septiembre, 2020

Agradecimientos

A Dios por haber puesto dentro de mi plan de vida esta oportunidad de crecimiento profesional y personal, por la sabiduría que dio al escribir este trabajo. Sin él, nada hubiese sido posible.

A mis padres que no están conmigo, pero sembraron en mi los más altos principios y valores, la tenacidad y la perseverancia para lograr siempre lo impensable.

Mi familia quienes siempre me han brindado la fuerza y sus oraciones ayudándome en lo que fuera posible.

A Eric, por convertirse en gran parte de la motivación que requiero.

Agradezco a mi asesor el Doctor Lucas Adolfo Giraldo Rios, por la motivación durante el desarrollo de los estudios de esta maestría, por su paciencia, orientación, conocimiento, experiencia y el apoyo incondicional durante la realización de este trabajo, me oriento y encamino en todo momento para llegar a este punto que significa mucho para mí.

A mi empresa, por darme la oportunidad de crecer profesionalmente y brindarme todo el apoyo necesario para poder llegar hasta aquí.

Resumen

Lineamientos de Ciberseguridad para Mejorar la Protección de los Sistemas de Control Industrial. Caso de Estudio: ISA INTERCOLOMBIA

La protección de los Sistemas de Control Industrial (ICS) es una de las áreas críticas que permiten la correcta aplicación y operación de los servicios que operan las infraestructuras críticas nacionales. Esta monografía analiza las regulaciones, estándares y buenas prácticas, así como también algunos marcos en la gestión de riesgos, con el fin de identificar parámetros que permitan establecer lineamientos clave en la protección de los ICS. La descripción de algunos de los ataques dirigidos, software malicioso, campañas de intrusión e incidentes cibernéticos hacia las ICS en los últimos años, permite identificar algunas interrupciones, fallas y consecuencias más relevantes debido a la ausencia de regulaciones y recomendaciones aplicables al sector eléctrico.

El propósito de esta monografía es establecer lineamientos de ciberseguridad para mejorar la protección de los ICS, tomando como caso de estudio la compañía ISA INTERCOLOMBIA, la cual incluye la propuesta de un modelo de madurez de capacidades compuesto por cuatro niveles: (1) seguridad; (2) Defensa; (3) Aseguramiento; y, (4) Monitoreo, basados en seis pasos y cuatro principios fundamentales, mediante la obtención de información de fuentes primarias y secundarias, los estándares y enfoques ya existentes para el sector eléctrico, y el uso de la combinación de métodos cualitativos y cuantitativos y el análisis documental.

Palabras Claves: Ciberseguridad, Infraestructura Crítica, Sistemas de Control de Industrial y Modelo de Madurez de Capacidades, Lineamientos.

Abstract

Cybersecurity Guidelines to Enhance the Protection of Industrial Control Systems. Case Study: ISA INTERCOLOMBIA.

The protection of Industrial Control Systems (ICS) is one of the critical areas that allow the correct application and operation of the services that operate the national critical infrastructures. This monograph analyzes the specific rules, regulations, modifications and good practices, as well as some frameworks of maturity models in risk management in order to identify parameters that establish key guidelines in the protection of ICS. The description of some of the targeted attacks, malicious software, intrusion campaigns and cyber incidents towards ICS in recent years, allows us to identify some of the most relevant interruptions, failures and consequences due to the absence of regulations and recommendations to the electricity sector.

The purpose of this monograph is to establish cybersecurity guidelines to improve the protection of ICS, taking the ISA INTERCOLOMBIA company as a case study, which includes the proposal of a capacity maturity model made up of four levels: (1) security; (2) Defense; (3) Safety; and, (4) Monitoring, based on six steps and four fundamental principles, by obtaining information from primary and secondary sources, existing standards and approaches for the electricity sector, and using the combination of qualitative and quantitative methods, and the documentary analysis.

Keywords: Cybersecurity, Critical Infrastructure, Industrial Control Systems and Capability Maturity Model, Guidelines.

Tabla de abreviaciones y términos

CIA	Confidencialidad, Integridad y Disponibilidad
CMM	Modelo de Madurez de Capacidades
CS	Sistemas de Control
DHS	Departamento de Seguridad Nacional
DCS	Sistemas de Control Distribuido
ES-C2M2	Modelo de Madurez de Capacidad de Ciberseguridad del Subsector de Electricidad
IC	Infraestrutura Crítica
ICC	Infraestrutura Crítica Cibernética
ISA	Sociedad Internacional de Automatización
IACS	Sistemas de Automatización y Control Industrial
TIC	Tecnologías de la Información y las Comunicaciones
ICS	Sistemas de Control Industrial
MIL	Niveles de Indicador de Madurez
NIST	Instituto Nacional de Estándares y Tecnología
PLC	Controlador Lógico Programable
RTU	Unidad Terminal Remota
SCADA	Sistemas de Control de Supervisión y Adquisición de Datos

Contenido

Pág.

Listas de Tablas

Pág.

Lista de Ilustraciones

Pág.

Introducción

En palabras del CONPES 3701,

> El uso de las tecnologías de la información y las comunicaciones trae consigo cambios y retos permanentes y se constituye como uno de los pilares del mundo globalizado. De manera simultánea el avance de estas tecnologías ha incrementado el uso de medios tecnológicos con fines delictivos alrededor del mundo. (Mintic, 2011, pág. 4)

Es así como la evolución de las amenazas ha llevado a una transformación digital o adaptación de los negocios a un nuevo entorno digital cambiando absolutamente todo el panorama empresarial.

En los últimos años, la conectividad ha ido ganando peso en todos los ámbitos, bajo el contexto en el que cada vez más dispositivos se encuentran conectados entre sí. Pero la digitalización, que abre enormes oportunidades, también implica riesgos que hay que saber gestionar. Uno de ellos es la Ciberseguridad (Martinez, 2018). Esta, conforma uno de los puntos claves en las estrategias de seguridad nacional de muchos países. Por lo anterior, los campos en los que se enfrenta la guerra han evolucionado de los tradicionales -aire, mar, tierra e inclusive el espacio- a una amplia variedad de amenazas que confluyen en el ciberespacio obligando a los Estados a tomar medidas que anteriormente no eran tenidas en cuenta (Instituto Español de Estudios Estratégicos; Instituto Universitario General Gutiérrez Mellado, 2011).

Las ciberamenazas afectan a todo tipo de organizaciones, desde empresas privadas a administraciones públicas, incluyendo sus infraestructuras críticas, las cuales están expuestas a múltiples amenazas donde puede verse afectada la disponibilidad del servicio.

La infraestructura crítica es un elemento esencial por el papel protagónico que tiene dentro del proceso productivo, de la economía, de la seguridad del Estado y de la prosperidad nacional, las cuales se encuentran expuestas a riesgos y amenazas cibernéticas, es importante tener en cuenta que el concepto de infraestructura critica está muy ligado al tema de ciberseguridad, en Europa el plan nacional de infraestructuras criticas estable el siguiente concepto:

> El elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población, cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones (Directiva Europea, 2008, pág. 3).

Por lo anterior, se puede observar que una afectación en términos de ciberseguridad en las IC y especialmente en el sector eléctrico (tal como se abordará con mayor detalle en la problemática y el objetivo 1), Puede comprometer la vida de los mismos ciudadanos de un territorio. Estos fenómenos de ciberseguridad están asociados a elementos de procesos, personas y tecnologías, las cuales, son abordadas en las respuestas del capítulo 7 del presente documento.

Para abordar esta problemática, se identificaron marcos, guías, estándares nacionales e internacionales y buenas prácticas existentes para la protección de los sistemas de control industrial y en el sector eléctrico, para el aseguramiento de sus componentes, con el fin de reducir y mitigar los riesgos en las Infraestructuras Criticas, los documentos analizados tienen similitudes las cuales son tomadas como referencia para el desarrollo de los lineamientos de ciberseguridad que pueden ser implementos en una organización para la construcción de un ambiente confiable en las operación de los Sistemas de Control Industrial (ICS por sus siglas en inglés) .

Adicionalmente, las organizaciones deben avanzar en la alineación entre las áreas de tecnología de la Información (IT) y Tecnologías de Operación (OT) de las empresas, con el fin de crear oportunidades para el desarrollo de un país desde las empresas del sector energético, garantizando el funcionamiento de las ICS. Los lineamientos propuestos en este trabajo servirán como referencia para orientar a las organizaciones en los pasos a seguir en el momento que se requiera integrar las dos áreas y especialmente para ISA INTERCOLOMBIA.

Este trabajo pretende, por medio de un proceso sistemático y el cumplimiento de los objetivos trazados, proponer unos lineamientos de ciberseguridad para mejorar la protección de los sistemas de control industrial y se encuentra organizado de la siguiente forma:

Identificación de los marcos, guías, estándares nacionales e internacionales, buenas prácticas o herramientas aplicadas en el aseguramiento de los sistemas de control.

Análisis de los estándares, políticas e información académica del sector eléctrico que permita identificar las ventajas y desventajas, junto con las mejores prácticas en la protección de los sistemas de control industrial.

Proponer un análisis conceptual de los requerimientos mínimos para definir los lineamientos en el aseguramiento de los sistemas de control industrial.

A partir de un análisis conceptual y teórico del estado actual de ciberseguridad del sector energía, se identificaron las mejores prácticas en la protección de los ICS, así mismo se describen los estándares, políticas e información académica del sector eléctrico que permita identificar las ventajas y desventajas, junto con las mejores prácticas en la protección de los ICS. A su vez se presentan algunos ataques cibernéticos que se han realizado a estos sistemas, lo cual permite tener un entendimiento de los riesgos y efectos a los cuales se enfrentan los ICS. Igualmente se abordan los atributos de la información (Confidencialidad, Integridad y Disponibilidad) desde un entorno de IT y OT, donde la disponibilidad juega un papel relevante en la continuidad de las operaciones de las infraestructuras críticas, porque permite ofrecer a continuidad del servicio (Knowles, 2015).

Para un mejor entendimiento de los estándares estos fueron definidos y clasificados dentro de una serie características y elementos según la función y gestión que cumplen con el fin de entender su propósito y su funcionalidad dentro del contexto del análisis. Lo anterior permitió realizar un análisis de cuáles estándares podrían cubrir en mayor medida lo tipos de ataques cibernéticos, sin embargo, los estándares son utilizados como un punto de partida

para desarrollar iniciativas en la protección de los ICS, facilitando la implementación de estos de acuerdo con las condiciones y necesidades propias de cada organización.

El desarrollo de lineamientos adaptados a las necesidades de los sectores o empresas mejoraría significativamente la gestión de la ciberseguridad. La implementación de lineamientos, estándares o normas es una práctica que continúa teniendo validez para mitigar los riesgos asociados al uso de ciberespacio.

La evaluación de los lineamientos de Ciberseguridad en una empresa del sector eléctrico es un proceso que debe realizarse de manera cíclica y evaluarse a través de herramientas de medición, tales como: los Indicadores Clave de Rendimiento (KPI por sus siglas en inglés), modelos de madurez de capacidades, auditorias, pruebas de penetración o diagnóstico, inclusive la Guía de Ciberseguridad del acuerdo No. 1241 del 30 de septiembre de 2019 donde propone en su anexo 2 un listado de cumplimiento de la guía de ciberseguridad.

Las normas, estándares, buenas prácticas, entre otros analizados, coinciden con las temáticas que deberían incluirse en la elaboración de lineamientos de Ciberseguridad para protección de los ICS en las empresas. Finalmente se tuvieron presente los siguientes estándares por su cobertura en cada uno de las características y elementos evaluados:

ISO/IEC 27001 – Anexo

21 pasos para mejorar la seguridad cibernética de las redes SCADA - The U.S. Department of Energy

Controles de seguridad y privacidad para sistemas y organizaciones federales de información. NIST SP 800-53

Adicionalmente a los estándares, se tuvieron presente los marcos en la gestión de riesgos, para el establecimiento de los lineamientos claves en la protección de los ICS, los cuales nos permiten identificar y analizar actividades involucradas en el proceso de gestión de riegos.

Cómo último punto, si bien no era un compromiso del presente trabajo, debido a su desarrollo se pudo construir y proponer un modelo de madurez para los ICS que está compuesto por cuatro elementos: (1) seguridad; (2) Defensa; (3) Aseguramiento; y, (4) Monitoreo, en este trabajo se presentan unas consideraciones que permiten elevar los índices de evaluación de los niveles de madurez para la protección de los ICS, basados en seis pasos, los cuales se encontrarán al final del mismo.

Siendo ISA INTERCOLOMBIA un actor clave del sector energético nacional y teniendo en cuenta que sus políticas y lineamientos plasmados en los documentos de Informe Integrado de Gestión y el Reporte Integrado Gestión de ISA INTERCOLOMBIA e ISA respectivamente, evidencian la importancia al desarrollar una aproximación de los lineamientos de ciberseguridad para mejorar la protección de los sistemas de control industrial.

1. Delimitación del trabajo de investigación

Hasta hace algunos años se consideró que, cuando los Sistemas de Control Industrial (ICS, por sus siglas en inglés Industrial Contol System) no están conectados a Internet, sus componentes y procesos podrían no estar expuestos a las amenazas cibernéticas. No obstante, el programa maligno "Stuxnet" en el año 2010 demostró que la posibilidad de un ciber ataque a un operador de infraestructura crítica, no se genera únicamente por la falta de tecnología o la ausencia absoluta de esta, sino a través del factor humano (Langher, 2011).

Factores como el comportamiento humano, que en algunas ocasiones no son el resultado de una acción intencional o malicioso, pero que su efecto podría ser tan negativo como el de un ciber ataque, permiten generar vulnerabilidades difíciles de detectar. Igualmente, los intereses geopolíticos de países potencialmente enemigos, como fue el caso de ciber ataque a la infraestructura eléctrica de Ucrania, permitió que un atacante externo afectará la disponibilidad del sistema (Liang, 2016).

Para contrarrestar estas acciones, las industrias del sector eléctrico han adquirido e implementado tecnologías digitales, y una variedad de sistemas de información para mejorar el aseguramiento de la productividad y eficiencia de sus procesos. En algunas ocasiones, no se han establecido estrategias nacionales o lineamientos institucionales adecuados que permitan mejorar el aseguramiento de sus activos de acuerdo con las características particulares de las Tecnologías de Operación (OT – por su acrónimo en inglés, Operation Technologies).

Los sistemas de control de supervisión y adquisición de datos (SCADA por sus siglas en inglés Supervisoy Control And Data Acquisition) y los sistemas de control distribuido (DCS por sus siglas en inglés Distributed Control System) se relacionan con procesos muy vitales de los que dependen otras infraestructuras críticas, estos serán descritos con mayor detalle en el apartado 7, los ICS cuentan con características específicas "exclusivas" para gestionar las plantas industriales (redes de distribución de agua y energía, infraestructuras aeronáuticas, entre otros); los cuales fueron adaptados para gestionar los procesos físicos de las operaciones de negocio, pero no están diseñados para monitorear las posibles ciberamenazas como las del entorno de Tecnologías de Información (IT – por su acrónimo en inglés, Information Technologies).

Si bien, los ciberataques en gran proporción son dirigidos a los sistemas de información mediante técnicas y/o explotación de vulnerabilidades, tales como: día cero, desbordamientos de búfer, scripts, denegación de servicio, entre otros. Estos ataques por lo general tienen como propósito un reconocimiento financiero y la obtención de información sensible. Sin embargo, existen casos específicos de ciberataques contra los ICS, donde la ausencia de políticas, guías, buenas prácticas, lineamientos y estrategias han permitido la explotación de vulnerabilidades sobre las características propias de diseño de los componentes o sistemas (Jarmakiewicz J. a., 2017).

Por lo anterior, este trabajo contribuirá a mejorar la protección cibernética de los ICS de ISA INTERCOLOMBIA, así como también de las empresas del sector eléctrico que tienen las mismas características.

2. Planteamiento del problema

2.1 Descripción del Problema

Las infraestructuras críticas son 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 en una realidad geográfica específica o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas (Fundación In-Nova Castilla La Mancha, 2019). La generación, transporte y distribución de la energía eléctrica son considerados como infraestructuras críticas y han iniciado un proceso de transformación hacia la automatización de sus procesos a través de la aparición de nuevas tecnologías. Estas Tecnologías de Operación (OT) dependen en gran medida de la manipulación segura de los ICS, además una interrupción en uno de sus sistemas no sólo ocasionaría el colapso del subsector eléctrico, sino también una crisis socioeconómica (Knowles, 2015), toda vez que las infraestructuras críticas están interconectadas unas con otras produciéndose unas relaciones de interdependencias especiales. Las relaciones expresan el hecho de que una infraestructura critica podría depender de los productos y servicios prestados por otra infraestructura crítica y la segunda infraestructura critica también puede depender de los productos y servicios de la primera (Cristina Alcaraza, 2014). Esta interrelación puede tener efectos en cascada en una o varias infraestructuras críticas causando la interrupción de uno o varios de sus productos o servicios.

Para proteger los componentes de los ICS, tales como: SCADA y los DCS (los cuales serán abordados y explicados con mayor detalle en los capítulos 6 y 7) en las organizaciones

del sector de energía se deben identificar y perfilar las principales amenazas de OT, y así establecer lineamientos y buenas prácticas para el aseguramiento del servicio de acuerdo con la demanda de los usuarios (Li, Cybersecurity in distributed power systems, 2017), garantizando la resistencia, estabilidad, seguridad de suministro y calidad de energía para los usuarios finales de electricidad.

Los ICS incluyen componentes de hardware y software que son utilizados para operar y automatizar procesos industriales. Sin embargo, estos sistemas no operan de manera aislados, hoy en día se conectan a otras redes de datos, sistemas de información y dispositivos electrónicos que utilizan protocolos IP (IP – por su acrónimo en inglés, Internet protocol) para su comunicación; lo que ha permitido obtener no sólo beneficios para su administración, sino también una serie de riesgos que son heredados de las Tecnologías de la Información (IT) (Jarmakiewicz J. a., 2017).

Hechos ocurridos como el de Ucrania en Diciembre de 2015 al sistema interconectado nacional de energía eléctrica; donde un ciberataque deshabilitó por más de 9 horas el servicio eléctrico en 30 subestaciones de 110 y 35 kV, afectando a más de 225 mil usuarios; ha demostrado la importancia de establecer protocolos, lineamientos y políticas en ciberseguridad para mejorar el aseguramiento y disponibilidad de estos servicios críticos (Liang, 2016).

El número de incidentes de seguridad cibernética reportados en los ICS han incrementado exponencialmente a medida que interactúan con otros componentes de IT conectados a Internet. Una gran ventaja de las IT es el grado de desarrollo en normas,

estándares y recomendaciones implementadas en los sistemas de información, sin embargo, estas mismas condiciones en su gran mayoría no son aplicables a las OT. Por tal razón, la materialización de un riesgo en uno de sus componentes no sólo ocasionaría daños ambientales, mala reputación institucional y consecuencias económicas, sino también la pérdida de vidas humanas (Chaves, 2017) debido a la dependencia que tienen otras infraestructuras críticas, como: hospitales, aeropuertos, represas, entre otras; con el suministro de energía eléctrica.

Las OT son el pilar fundamental para garantizar la disponibilidad y la continuidad de los servicios en las IC, por lo tanto, al estar estas cada vez más permeadas por las IT, se exponen a riesgos heredados de estas últimas, incluyendo penetraciones de agentes maliciosos, acciones del malware, ataques de denegación de servicio, piratería, perturbación electromagnética, entre otras. Este tipo de amenazas se pueden englobar en aquellas relacionadas con los activos de información, hardware, software de base, aplicaciones, servicios y usuarios autorizados (Luiijf, 2006).

El riesgo principal de estos sistemas es el desconocimiento por parte del propietario de las interconexiones reales de los sistemas SCADA, la ausencia de buenas prácticas de seguridad, como la realización de actualizaciones periódicas o una adecuada gestión de las contraseñas, y las deficiencias en la configuración de los diferentes dispositivos que proporcionan muchas posibilidades de realizar acciones remotas que permiten el control de los mismos (Perez San Jose, 2012).

Por lo anterior se evidencia que al fallar una IC, la cual comprende sistemas y activos físicos y virtuales, que proporcionan funciones y servicios esenciales para el funcionamiento de una nación, la interrupción en uno de sus servicios, podrían tener un serio impacto en la seguridad nacional, el bienestar, la salud económica o la seguridad pública, o cualquier combinación de los mismos (Cristina Alcaraza, 2014).

A pesar de la creciente inversión en seguridad de tecnologías de la información, las amenazas de ataques de origen cibernético continúan creciendo, a consecuencia que la sociedad, en todos sus niveles y sectores, subestiman los riesgos de origen cibernético y continúan ejecutando medidas de control para defenderse de las ciberamenazas del pasado, en cambio los ciberdelincuentes usan las últimas tecnologías y están enfocados en innovar, desarrollar, investigar, estudiar, y aprovechar las vulnerabilidades del futuro.

Los riesgos de seguridad digital están estrechamente relacionados con el uso de las tecnologías de la información y comunicaciones enfocada a los activos digitales, las operaciones y la información.

De acuerdo con lo publicado en el documento "Ciberseguridad una guía de Supervisión" del Instituto de Auditores Internos de España, los principales riesgos cibernéticos a los que se exponen todos los usuarios del ciberespacio se pueden clasificar de la manera presentada en la Tabla 1.

Tabla 1. Riesgos Cibernéticos. Fuente: Adaptado del documento "Ciberseguridad una guía de Supervisión" del Instituto de Auditores Internos de España (Instituto de Auditores Internos de España, 2016, pág. 9 y 10)

Riesgo Cibernético	Descripción
Fraude Financiero	Las instituciones y entidades financieras son uno de los principales objetivos de los ciberdelincuentes. El robo económico representa una de las principales motivaciones de la gran mayoría de ciberatacantes.
Robo de información	La información de carácter personal o documentos clasificados son algunos de los principales activos de información que deben ser especialmente protegidos. La filtración pública o pérdida de la información confidencial es un riesgo elevado, cuyos impactos o pérdidas pueden resultar especialmente significativos.
Indisponibilidad de servicios	Es la interrupción puntual o prolongada de los servicios ofrecidos en línea como por ejemplo correos, pagos financieros, cobro de impuestos, registros públicos, entre otros.
Sabotaje de infraestructuras	Son los ataques contra los servicios o infraestructuras críticas de un país o estado, provocando desabastecimientos, o interrupciones de comunicaciones, etc. con el objetivo de provocar una paralización puntual o prolongada de los mismos.
Pérdida de reputación	Es una de las principales consecuencias de las agresiones cibernéticas y el objetivo de gran parte de los ciberataques, cuyos efectos pueden resultar altamente significativos.

Por todo lo anterior, debido a las vulnerabilidades de las OT, se puede inferir que una falla en la IC energética puede poner en riesgo la supervivencia de una sociedad; la literatura evidenció que hay una ausencia de lineamientos en temas de ciberseguridad para los ICS como primer eslabón de protección de estos últimos. Al ser ISA INTERCOLOMBIA un actor del Sistema Energético Nacional, el no abordar esta problemática, enunciando los riesgos previamente mencionados, podrían comprometer el negocio de Transporte de Energía en Colombia, Chile, Perú, Brasil y Bolivia, lo que acarrearía penalizaciones económicas, reputacionales (toda vez que se pierde credibilidad de la estabilidad del sistema de operación y manejo) e incluso el comprometimiento de vidas, ya que la IC apoyada por la empresa

soporte otras IC como salud, transporte, entre otros, razón por la cual está presentado en el Informe Integrado de Gestión (2019).

2.2 Pregunta de Investigación:

¿Cuáles son los lineamientos de ciberseguridad para mejorar la protección de los ICS, para ISA INTERCOLOMBIA?

3. Objetivos de la investigación

3.1 Objetivo General

Establecer los lineamientos de ciberseguridad para mejorar la protección de los sistemas de control industrial. Caso de estudio: ISA INTERCOLOMBIA.

3.2 Objetivos Específicos

1. Identificar los marcos, guías, estándares nacionales e internacionales, buenas prácticas o herramientas aplicadas en el aseguramiento de los sistemas de control industrial.

2. Analizar estándares, políticas e información académica del sector eléctrico que permita identificar las ventajas y desventajas, junto con las mejores prácticas en la protección de los sistemas de control industrial.

3. Proponer un análisis conceptual y comparativo de los requerimientos mínimos para definir los lineamientos en el aseguramiento de los sistemas de control industrial. Caso de estudio: ISA INTERCOLOMBIA.

4. Alcances y limitaciones

4.1 Alcance

Este trabajo es orientado a los ICS, que se tienen en la empresa ISA INTERCOLOMBIA S.A. E.S.P., empresa de servicios públicos mixta, del orden nacional, que contempla dentro de su objeto social, la actividad de la transmisión de la energía eléctrica, representando, administrando, operando y manteniendo los activos de transmisión de energía eléctrica, que constituyen infraestructura crítica para la nación. Nuestras redes de transporte de energía se extienden a través de la diversa geografía nacional, aportando al desarrollo y a la competitividad de los colombianos. El trabajo se implementará en la empresa ISA INTERCOLOMBIA y sus filiales.

Este trabajo enmarcará la convergencia de las tecnologías de IT y OT, en los ICS dentro del contexto de ciberseguridad los cuales son apoyo a los servicios de la infraestructura crítica del país.

4.2 Limitaciones

Debido a que ISA INTERCOLOMBIA es una empresa de orden nacional y que hace parte de la infraestructura crítica del País, podrá tener limitación en cuanto al acceso a personas, organizaciones o documentos y por cualquier razón, el acceso podrá ser limitado, de alguna manera solo se presentará la información e imágenes que se pueda acceder de manera pública, debido a que en caso de ser conocida o utilizada por alguien no autorizado

no impactaría a la empresa del grupo, para este trabajo como ejemplo se tomara información de referencia de la página principal WEB de la organización. El documento por desarrollar será de tipo táctico – operativo el cual definirá y proporciona unas directrices y recomendaciones específica sobre lo que debe hacerse para la ciberseguridad para mejorar la protección de los ICS, aplicada al sector eléctrico de la empresa.

El trabajo se desarrolla tomando en cuenta algunos marcos internacionales y nacionales de gobernanza y seguridad relacionados con los sistemas ICS.

ISA en su Política de Información afirma que: "Declarar las decisiones corporativas orientadoras de la gestión de la información y el conocimiento como activos críticos y estratégicos, para el desarrollo de los negocios en sus necesidades presentes y futuras, que requieren ser conservados, protegidos en procura de la sostenibilidad, la construcción de sinergias y la continuidad de la operación de ISA y sus empresas" (ISA, 2020).

Igualmente, en su Política de Gestión Integral de Riesgo dice: "Declarar las decisiones corporativas orientadoras de la Gestión Integral de Riesgos, a través de la cual se busca generar y proteger el valor de ISA y sus empresas, la integridad de los recursos empresariales, la continuidad y sostenibilidad de los negocios." (ISA, 2020).

En el Informe Integrado de Gestión 2019 presenta: "Para ISA INTERCOLOMBIA la gestión Integral de Riesgos es el vehículo que transforma realidades; contando con un proceso sistemático y homologado, orientado por la Política Corporativa" (Isa Intercolombia, 2019, pág. 47), se cuenta con un mapa de riesgos empresariales, donde se identifican los recursos: reputación, humano y financiero; y se monitorean 15 categorías de

riesgos, en el cual se encuentra el riesgo llamado Tecnología de Información y Comunicación (TIC). "Conscientes de los impactos positivos y negativos inherentes a los grandes retos de la estrategia, se identifican, administran y gestionan los principales riesgos que pueden influir o presentar desviaciones sobre los recursos financieros y reputacionales en el largo plazo", uno de los factores es la seguridad (Isa Intercolombia, 2019, pág. 77).

En el Reporte Integrado de Gestión 2019 de ISA "La Gestión Integral de Riesgos en ISA y sus empresas busca preservar la integridad de los recursos empresariales y la continuidad y sostenibilidad de los negocios". Como se puede observar en la Ilustración 1, se identifica el riesgo de Tecnologías de Información y Comunicaciones (TIC).

Ilustración 1. Mapa de riesgos de ISA y sus empresas, tomado de: Reporte integrado de gestión 2019

En el Reporte de Integrado de Gestión 2019 de ISA la empresa tiene como relevante la Seguridad de las Infraestructuras, la Información y Ciberseguridad (ISA, 2019). La ciberseguridad es una dimensión de la mayor relevancia en la transformación digital de Grupo ISA, es por esto que se avanza en la implementación de la estrategia de ciberseguridad del grupo y su mapa de ruta, así como en la evaluación, control y medición del riesgo cibernético, el cual tiene seguimiento y está asociado con los niveles de responsabilidad en la estructura de la organización pasando por la capa de procesos para llegar a los niveles más altos de las compañías y es abordado en el mapa de riesgo emergentes del grupo como se presenta en el ítem 4 de la Ilustración 2.

Ilustración 2. Emergentes tomado de: Reporte Integrado de Gestión 2019 de ISA

Para la construcción de los lineamientos para ISA INTERCOLOMBIA, es importante el concurso de varias áreas de la organización, por lo tanto, para lograr los propósitos de este trabajo, se ha definido como lineamientos:

- La identificación de los marcos, guías, estándares y buenas prácticas que se pueden desplegar para la organización a la luz de su plan estratégico.

- El análisis conceptual y comparativo de los requerimientos surgidos del análisis del punto anterior para determinar las bases que den lugar a los lineamientos para ISA INTERCOLOMBIA.

5. Metodología

Se utilizará una metodología cualitativa, la cual es la recolección de información basada en la observación de comportamientos naturales, discursos, respuestas abiertas para la posterior interpretación de significados (Hernandez-Sampieri, Fernandez-Collado, & Baptista-Lucio, 2014). El método cualitativo analiza el conjunto del discurso entre los sujetos y la relación de significado para ellos, según contextos culturales, ideológicos y sociológicos (Rodriguez Gómez, Gil Flores, & García Jiménez, 1996), así mismo el tipo de modelo utilizado para el desarrollo del trabajo será una de tipo causal, la cual trata de explicar las causas por las cuales ocurren determinadas situaciones, hechos o fenómenos. En ese sentido, en este tipo de trabajo se encontrará la descripción de las variables de un fenómeno, así como el análisis de la relación que existe entre ellas y sus respectivas consecuencias en el modelo y los lineamientos.

6. Identificación de los marcos, guías, estándares nacionales e internacionales, buenas prácticas o herramientas aplicadas en el aseguramiento de los sistemas de control industrial.

En este apartado se presenta una aproximación a las normas, elementos que describen la importancia de la protección de las infraestructuras críticas en la sociedad mediante un enfoque de ciberseguridad en los Sistemas de Control Industrial, con el fin de visualizar la importancia de la protección de los principales componentes que permiten la operación de una red eléctrica, tales como: los SCADA y los DCS. También se relacionan los objetivos, metodología, unidad de estudio y alcance en este trabajo, con el fin de dar respuesta a la pregunta de investigación.

Igualmente, para la construcción de los lineamientos se identificarán y analizaran varios tipos de instrumentos los cuales deben emplearse como referencia y no como solución final, para nuestro diseño del modelo propuesto en el objetivo general, en el cual siempre se tendrá presente el enfoque de riesgos. Si bien cada instrumento puede tener controles, habrá que decidir cuáles son aplicables de acuerdo con las circunstancias y si es necesario efectuar ajustes o adaptaciones, un buen criterio no puede ser sustituido.

Para empezar, es importante que se identifiquen de manera clara las definiciones de marco, guía, estándar, mejores prácticas, herramientas y lineamientos, ya que esto permitirá hacer una mejor aproximación al modelo propuesto más adelante.

Marco: Es una guía voluntaria, basada en estándares, pautas y prácticas existentes para que las organizaciones administren y reduzcan mejor el riesgo de ciberseguridad, además de ayudar a las organizaciones a gestionar y reducir los riesgos, fue diseñado para fomentar las comunicaciones de gestión de riesgos y ciberseguridad entre las partes interesadas de la organización tanto internas como externas. (NIST, s.f.)

Guías: Es una definición procedimental que determina, por medio de actividades, los pasos que se deben ejecutar para producir un resultado con unas ciertas características o propiedades. En el contexto informático, se utilizan para expresar metodologías de trabajo que reflejan las mejores prácticas. (Mintic, s.f.)

Estándar: Definen las reglas o características que facilitan el manejo de temas específicos, entre ellos la gestión del servicio de IT, gobierno de IT y gestión de calidad en el sector público. Su objetivo es guiar a una entidad en cómo establecer una estrategia de adopción de una arquitectura empresarial enmarcada en su estrategia. En el contexto de IT, un estándar es un documento que contiene un conjunto de especificaciones técnicas de aplicación voluntaria, que ha sido construido a través de consenso y que refleja la experiencia y las mejores prácticas en un área en particular. (Mintic, s.f.)

Mejores prácticas: Es un conjunto de acciones que han sido implementadas con éxito en varias organizaciones, siguiendo principios y procedimientos adecuados Definen aspectos metodológicos y técnicos que facilitan la ejecución de elementos claves, que han dado resultados para implementar o gestionar características puntuales entre ellos gobierno de IT, gestión de los servicios de IT, modelo de madurez para la gestión del portafolio de proyectos

y marcos de referencia para la definición de la arquitectura empresarial. Su objetivo es mejorar las prácticas que son usadas por la industria de IT para apoyar la arquitectura y la gestión de IT (Ministerio de tecnologías de la información y las comunicaciones, 2014).

Herramientas: Son mecanismos que permiten a las instituciones realizar acciones específicas asociadas a las definiciones dadas por el marco de referencia, específicamente por un lineamiento o por una guía. Las herramientas son identificadas y referenciadas con base en las mejores prácticas de IT para apoyar la arquitectura de IT y la gestión de IT. Su objetivo es mejorar las prácticas que son usadas por la industria de IT para apoyar la arquitectura y la gestión de IT (Ministerio de tecnologías de la información y las comunicaciones, 2014).

Lineamiento: Documento en el cual se establecen directrices específicas o políticas internas asociadas a un tema, proceso o método en particular. (Departamento Administrativo de la Presidencia de la República, s.f.).

Para ISA INTERCOLOMBIA los lineamientos son documentos de gestión que definen el ámbito en que los procesos actúan en su día a día en la organización[1], los cuales se clasifican de acuerdo con su función, estos documentos son los marcos que contienen conceptos definidos para establecer el desarrollo seguro de los procesos y operaciones del negocio y permiten enfrentar entre otras, las situaciones de riesgo o crisis que amenacen la credibilidad, continuidad y sostenibilidad de la empresa.

[1] Definición ajustada con el área de estrategia de la organización

En resumen, los instrumentos analizados tienen similitudes a partir de que todos proporcionan un marco de referencia y son voluntarios para implementarse, contemplan un conjunto de pasos, órdenes y directrices que terminan en un documento que define unos principios los cuales se construyen de manera fácil y estructurados, además expresan un entendimiento preciso de una situación específica con el fin de ayudar a las organizaciones a establecer de manera ordenada la gestión de algún servicio. según las consideraciones anteriores, se entiende que con la ayuda de varios tipos de instrumentos se construirá a partir de pautas, pasos, procedimientos, metodologías, buenas prácticas, herramientas y técnicas entre otros, lineamientos de ciberseguridad que pueden regir en una entidad.

6.1 Antecedentes Nacionales

De acuerdo con la definición entregada por el doctor Jeimy J. Cano, Ph.D., miembro investigador del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho y Profesor de la misma Facultad de la Universidad de los Andes, Colombia y miembro del Subcomité de Publicaciones de ISACA, la seguridad informática es:

> La disciplina se encargaría de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que—articulados con prácticas de gobierno de tecnología de información—establecen la forma de actuar y

> asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo. (Cano, 2011)

Lo anterior, conlleva a la importancia de buscar diferentes medios como estrategia de protección ante las amenazas que se generan por la dependencia de la sociedad en el uso del ciberespacio.

A nivel nacional se tienen documentos tales como: políticas, lineamientos y planes que se han establecido con el objetivo de mitigar los riesgos en las Infraestructuras Criticas Cibernéticas, los cuales permiten la alineación, fortalecen la cooperación y coordinación de las diferentes instituciones, para el sector eléctrico colombiano, los documentos que rigen su relación y desarrollo son, entre otros encontramos:

- CONPES 3854 del 11 de abril de 2016. Política Nacional de Seguridad Digital:

El cual tiene como propósito soportar en temas de ciberseguridad al sector crítico del país y las economías que la integran en el entorno digital, con el fin de emitir políticas para la gestión de riesgos. Propende por "adoptar una estrategia para la protección y defensa de las infraestructuras criticas cibernéticas nacionales, siendo consciente de la necesidad de fortalecer las capacidades operativas, administrativas, humanas, científicas, tecnológicas y de infraestructura físicas de las instituciones." (DNP, CONPES 3854,2016 pág. 18). Lo anterior con el fin de contribuir al crecimiento de la economía digita nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país.

- CONPES 3995 del 01 de julio de 2020. Política Nacional de Confianza y Seguridad Digital:

Su propósito es de fortalecer y ampliar las capacidades de seguridad digital. Estableciendo medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital (CONPES 3995, 2020), este CONPES se cita por observación de los jurados evaluadores de este trabajo de grado, sin embargo, al momento de finalizar esta monografía, dicho documento no era público.

Igualmente propone como estrategia la gestión basada en los riesgos de tal forma que su enfoque sea flexible y ágil en la identificación de la incertidumbre digitales que se presenten.

- Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia:

Define de manera general los lineamientos que deben adoptar los dueños y operadores de las infraestructuras críticas cibernéticas en Colombia, este plan estable las medidas de protección de protección y resiliencia a corto, mediano y largo plazo. El cual permitirá articular esfuerzos de manera coordinada, sistemática y eficiente, con el fin de prevenir y reaccionar ante la presencia de ataques cibernéticos que pongan en riesgo la continuidad y

disponibilidad de los servicios críticos para el país, entre los diferentes actores del entorno que administran la infraestructura crítica cibernética del país.[2]

- El Plan Sectorial de Protección y Defensa para la Infraestructura Crítica Cibernética del Sector Electricidad Colombiano:

Define los lineamientos que deben adoptar los diversos agentes del Sector electricidad y operadores de las infraestructuras críticas con el propósito de coordinar acciones eficientes e integrales que permitan prevenir y/o mitigar potenciales amenazas cibernéticas que pongan en riesgo la disponibilidad y continuidad del servicio de energía eléctrica.

A la par se tienen unos documentos a nivel nacional provenientes del Consejo Nacional de Operación - CNO, en el que se han establecido (02) dos acuerdos orientados a disminuir los riesgos de ciberseguridad en el sector eléctrico: acuerdo No. 788 publicado el 3 de Septiembre de 2015, mediante el cual se adoptó la Guía de Ciberseguridad para el sector eléctrico en su primera versión y acuerdo 1241 publicado el 30 de septiembre de 2019, el cual permitió actualizar los acuerdos del 2015 y reconoció la necesidad de la implementación de una normativa de ciberseguridad que garantice la prestación eficiente del servicio de energía eléctrica en Colombia (Comite Nacional de Operación, 2019). Los aspectos generales de las guías emitidas por el CNO se exponen en la tabla 2.

[2] Comando Conjunto Cibernético. Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia. https://www.ccoc.mil.co/?idcategoria=281&download=Y

Tabla 2. Guías de ciberseguridad. Fuente: Elaboración Propia (2020)

Nombre	Descripción
Guía de Ciberseguridad, acuerdo No. 788 del 03 de septiembre de 2015. CNO.[3]	La guía está orientada a mitigar los riesgos de ciberseguridad en el sector eléctrico y establece como premisa; la adopción de requerimientos mínimos de seguridad en los activos críticos para la operación del Sistema Interconectado Nacional. Utilizó como referencia la Norma NERC CIP del 002 a la 009. Objetivos Principales: Identificación de Activos Críticos, Gestión de la Seguridad de Ciber Activos Críticos, Seguridad Física de los Ciber Activos Críticos y Plan de Recuperación (Comite Nacional de Operación , 2015).
Guía de Ciberseguridad, acuerdo No. 1241 del 30 de septiembre de 2019. CNO.[4]	Es la actualización de la Guía desarrollada en el 2015, extractando y adaptando aspectos de la Norma NERC CIP del 002 a la 014. Mediante la cual se recomienda "*la de los requerimientos mínimos de seguridad para la protección de los activos del Sistema Interconectado Nacional (SIN) que son considerados críticos para la operación confiable del sistema eléctrico, en este sentido es necesario identificar los activos críticos, los ciberactivos críticos, los perímetros de seguridad electrónica y seguridad física.*" (Comite Nacional de Operación, 2019). A diferencia de su predecesor, establece la necesidad de implementar un Plan de respuesta ante incidentes en ciberactivos críticos.

6.2 Sistemas de Control Industrial ICS

Los primeros ICS nacieron a través de una conectividad de red tipo punto a punto, la cual permite la comunicación entre un panel de monitoreo a un sensor (Caicedo-Eraso, 2015). Sin embargo, a medida que la sociedad evolucionó y las Tecnologías de la Información y Comunicaciones (TIC) se incorporaron en los diferentes ámbitos de la sociedad digital en un

[3] Consejo Nacional de Operación. Guía de Ciberseguridad del 2015. https://www.cno.org.co/content/acuerdo-788

[4] Consejo Nacional de Operación. Guía de Ciberseguridad del 2019 (actualización). https://www.cno.org.co/content/acuerdo-1241-por-el-cual-se-aprueba-la-actualizacion-de-la-guia-de-ciberseguridad

entorno globalizado, aparecen las amenazas cibernéticas que traen consigo nuevos riegos en las actividades sociales, económicas e industriales (Knowles, 2015). La evolución de las TIC ha generado una dependencia tecnológica en la sociedad, como son los servicios esenciales de los entes gubernamentales y privados que son ofrecidos a través de las infraestructuras críticas.

Los ICS han pasado por una transformación significativa, de sistemas privados y aislados, a topologías con tecnologías estándar interconectadas con otras redes de datos comerciales, convirtiéndolas en arquitecturas abiertas, por lo que frecuentemente utilizan software comercial. Lo que ha logrado una disminución en la inversión y costos en las OT, así como también el monitoreo remoto, y el control de su hardware y software de una manera más flexible (Sebastian Obermeier, 2012).

Es así como con la creciente interconexión de los ICS, con otros sistemas corporativos e incluso Internet, se abren cada vez más posibles vectores de ataque que deben ser abordados con el fin de garantizar un funcionamiento seguro de los ICS. Tradicionalmente hubo una separación completa entre la red de OT, la cual se encuentra representada por dispositivos y procesos de control y la red de IT, identificadas como las aplicaciones empresariales y de escritorio. Hoy en día las empresas están en proceso de apertura de los equipos de la red OT para obtener beneficios como la monitorización remota y facilidad para la administración, asumiendo mayores riesgos de seguridad cibernética (Pérez A, 2014). Los ICS, especialmente aquellos que afectan las infraestructuras críticas como las estaciones eléctricas, llevan años en el "*ojo del huracán*" (Albors, 2017) . Es importante mencionar que la ciberseguridad aplicada a los ICS ha venido tomando relevancia en los últimos años, al

punto que ciertos sectores e industrias en donde se utilizan estos sistemas son catalogados como infraestructuras críticas (García A, 217).

Por lo anterior, se hace necesaria la convergencia entre IT y OT, para aumentar la eficiencia de los procesos industriales, gestionando los riesgos y puntos de vulnerabilidad, sopesando los niveles de inseguridad de las organizaciones industriales. De hecho, en muchos casos, se observa una importante deficiencia en la forma en la que abordan la ciberseguridad de sus redes IT y de OT. Aunque en la mayoría de las ocasiones son conscientes de los posibles riesgos, no ponen en práctica medidas de seguridad para proteger sus redes operacionales (Ramírez, 2018).

En efecto, los operadores de infraestructuras críticas de las compañías eléctricas buscan la manera de asegurar sus sistemas y a menudo quieren prácticas de ciberseguridad más maduras. Sin embargo, el enfoque informático de la ciberseguridad no siempre es apropiado y tiene las limitaciones operacionales a las que se enfrentan las compañías eléctricas. Lo que significa que las soluciones en ciberseguridad del sector IT, son complementarias para aplicaciones de OT y viceversa. A medida que las compañías eléctricas experimentan una convergencia entre IT y OT, es cada vez más necesario desarrollar equipos interdisciplinares para abordar retos únicos de tecnología segura que abarquen ambos mundos. Las ciberamenazas actuales, requieren una mayor colaboración entre los responsables de IT y OT, que deben compartir sus conocimientos para identificar los posibles problemas y ataques que afectan a sus sistemas (Vinyes, 2017).

Los ICS se han convertido en sistemas complejos que admiten la comunicación en redes multipuntos, entre una unidad de control central y múltiples dispositivos y/o unidades remotas, logrando abarcar grandes distancias por medio de redes malladas. Los nodos en cada una de estas redes son dispositivos electrónicos integrados, tales como: las unidades terminales remotas (RTU), sensores, los controladores lógicos programables (PLC), entre otros. (Anabalón, 2018).

Si bien, los sistemas DCS y SCADA son considerados los componentes principales de los ICS, en el caso del SCADA, este tiene como característica principal que son sistemas altamente distribuidos que se utilizan para controlar activos desde cualquier ubicación geográfica. Así mismo, este sistema no pertenece exclusivamente a las redes de energía eléctrica, sino que también es utilizado en sistemas de distribución, tales como: sistemas de distribución de gas natural, agua, recolección de aguas residuales, petróleo y transporte ferroviario. Un centro de control SCADA de cualquier infraestructura crítica realiza monitoreo y control centralizado a través de redes de comunicaciones de larga distancia, incluyendo alarmas de procesamiento de datos de estado, a través de operaciones como abrir y cerrar válvulas, consultar el estado de los interruptores y recoge los datos de los sensores y los envía a un punto central para su procesamiento (Ardila, 2010).

Al igual que el sistema SCADA, los DCS se utilizan para controlar procesos industriales como la generación de energía eléctrica, las refinerías de petróleo y el tratamiento de aguas. Los DCS se integran como una arquitectura de control que supervisa múltiples subsistemas los cuales no están centralizados, sino que están distribuidos, y que son responsables de controlar los procesos que se ejecutan en las infraestructuras críticas. Para

lograr un producto deseado los DCS emplean un Controlador Lógico Programable (PLC por sus siglas en inglés Programmable Logic Controller), los cuales son configurados para proporcionar la tolerancia deseada del proceso (Ardila, 2010).

La infraestructura puede ser entendida como un sistema con diferentes instalaciones donde se llevan a cabo actividades, una interrupción puede impactar críticamente a uno o muchos países y con esto podría ocasionar una crisis socioeconómica

> ...los tres factores que pueden definir una infraestructura como crítica son: (1) La importancia simbólica de la infraestructura dentro del país (como por ejemplo: museos, monumentos, edificios, entre otros); (2) La dependencia directa de infraestructuras como las redes de energía y telecomunicaciones; y (3) La interconectividad entre infraestructuras que podrían causar efectos en cascada en caso de una interrupción. (Herrera, 2019, pág. 16)

A hora bien, el ciberespacio ha introducido una nueva dimensión en las sociedades favoreciendo el progreso, gracias a las nuevas tecnologías y al uso extensivo de internet. Los aspectos positivos de la utilización del ciberespacio son numerosos. La generación de nuevas capacidades en campos como las comunicaciones, la investigación científica, los procesos industriales o la gestión del conocimiento son evidentes. No obstante, esta situación presenta nuevos retos de los que no se sustraen los diferentes actores políticos, principalmente los Estados. Entre los desafíos a enfrentar se encuentran el ciberespionaje, las acciones de grupos terroristas y de corte yihadista, la ciberdelincuencia y la protección y recuperación de los sistemas de infraestructuras críticas, ante agresiones que utilizan el ciberespacio como

entorno y vehículo para interferir en las actividades de los ciudadanos y de las instituciones (Villalba, 2017).

Las infraestructuras críticas, en especial el sistema de energía eléctrica es vital para la supervivencia de una sociedad. Los ciberataques direccionados a estas infraestructuras no sólo afectan al país donde se generó el incidente, sino que también, otros sectores críticos nacionales y trasnacionales (Jarmakiewicz, 2017).

El escalamiento de privilegios no autorizados en los ciberactivos y alteración de información de los dispositivos de monitoreo en los servidores, son algunas de las amenazas que pueden explotar las vulnerabilidades de los centros de control y subestaciones eléctricas, un ejemplo de ello, fue el ciberataque contra las redes de energía eléctrica en Ucrania, como lo muestra Case Defense use (2016), donde 3 compañías de distribución de electricidad fueron infectadas con un software malicioso que ocasionó el apagón en gran parte del país. Este incidente inició a las 15:35 horas y finalizó a las 18:35 horas, afectando escalonadamente a 7 subestaciones de 110kV de Alta Tensión y a 23 Subestaciones de 35KV, y se estima que alrededor de 225.000 hogares y compañías fueron afectadas por la desconexión del servicio. Algunas de las vulnerabilidades explotadas durante el ciberataque en Ucrania, fueron la configuración de equipos por defecto de fábrica y que se identificaron VPNs sin una autenticación fuerte o doble autenticación.

Esto ha conllevado a que países como España, Hungría y Estonia han ido un poco más allá, y dentro de sus políticas nacionales han establecido medidas para mitigar los posibles ataques cibernéticos a estas infraestructuras que se encuentren dentro y fuera de sus fronteras

nacionales. En España, la responsabilidad recae en los operadores que deben identificar las dependencias transfronterizas (Kaska, 2015). En Hungría, la Estrategia Nacional de Seguridad Cibernética tiene como propósito mantener un ciberespacio seguro en el contexto nacional e internacional (Szadeczky, 2018). En Estonia, los proveedores y operadores de los servicios vitales son directamente responsables de garantizar la gestión de la información ubicada en países extranjeros, pero también de llevar a cabo periódicamente un análisis de riesgos en cada uno de ellos (Riigikogu, 2017).

Sin embargo, existen múltiples estrategias y enfoques para identificar los servicios vitales de las infraestructuras críticas. Por ejemplo Francia utilizó el enfoque "basado en operadores" para identificar un total de 12 sectores y subsectores críticos y 220 operadores vitales dentro de su territorio nacional, Suiza empleó un enfoque "orientado a servicios" para identificar 10 sectores críticos y 28 subsectores; y el Reino Unido utilizó una versión basada en activos que es un híbrido entre los enfoques "basados en servicios y los basados en operaciones" (Klaver, 2011).

Según Enisa (2014), el sector energía está compuesto por 3 subsectores: Electricidad, Petróleo y Gas Natural, donde el subsector Electricidad está compuesta por los siguientes servicios vitales: (1) Generación; (2) Transmisión-Distribución; y, (4) Comercialización de la electricidad, como se visualiza en la Tabla 3.

Tabla 3. Lista del sector crítico Energía y los servicios vitales, Fuente: ENISA (2014)

Sector crítico	Subsector crítico	Servicios Críticos
Energía	**Electricidad**	Generación (todas las formas)
		Transmisión/ distribución
		Mercado de electricidad
	Petróleo	Extracción
		Transporte/Distribución
		Almacenamiento
	Gas Natural	Extracción
		Transporte/Distribución
		Almacenamiento

Sumando a lo anteriormente presentado por ENISA, (2014) en la Tabla 3, el Comando Conjunto Cibernético de Colombia – CCOC en su documento "Sectores Estratégicos de la República de Colombia desde la óptica Cibernética", publicado en el 2016 nos muestra que los subsectores del sector Electricidad para el país son: Operación, Generación, Transmisión, Distribución y Comercialización, tal como se extracto del documento, el cual afirma qué:

> El Sistema Interconectado Nacional (SIN) está compuesto por plantas o centrales de generación, redes de transmisión y distribución y centros de consumo, los cuales están interconectados entre sí para realizar la prestación del servicio público de la energía eléctrica. Cada subsector está compuesto a su vez por diferentes compañías de carácter público, mixto y privado… (Comando General de las Fuerzas Militares, 2016, pág. 19).

Como se puede observar la taxonomía presentada por ENISA y por el CCOC son complementarias, toda vez que incluyen los mismos sectores, simplemente difieren en que

en Colombia para el sector energético se amplía un poco más, tal como se presenta en la Ilustración 3.

Sectores y Subsectores de Colombia

	Sector	Subsector (cada sector debe complementar la tabla)
1	ALIMENTACIÓN Y AGRICULTURA	Agricultura
		Acuario
		Pesquero
		Acuícola
2	AGUA	Acueducto
		Saneamiento Básico
		Red Matriz
3	COMERCIO, INDUSTRIA, TURISMO	Comercio
		Industria
		Turismo
4	DEFENSA	Unidad de Gestión General - MDN
		Ejército Nacional
		Armada Nacional
		Fuerza Aérea Colombiana
		Policía Nacional
5	EDUCACIÓN	Instituciones de Educación Preescolar, Básica, Media y Superior.
		Institutos para el Fomento de la Educación Superior.
		Entidades de Crédito Educativo.
		Entidades de Educación para personas con Discapacidad Auditiva y Visual.
6	ELECTRICIDAD	Operación
		Generación
		Transmisión
		Distribución
		Comercialización

Ilustración 3. Sectores y Subsectores de Colombia. Fuente: Comando Conjunto Cibernético de Colombia, 2016

Estos subsectores son supervisados y controlados por el Centro Nacional de Despacho (CND), adscrito a XM S.A E.S.P, el cual es el encargado de que la operación del SIN sea optima, confiable y se garantice la atención de la demanda a todos los usuarios del territorio nacional apoyados en centros control de generación (CCG) centros de supervisión y maniobra y centros locales de distribución administrados por múltiples empresas del sector, bajo las normas y regulaciones dictadas por los entes reguladores del sector (CCOC, 2016).

La generación, transporte y distribución de la energía eléctrica han iniciado un proceso de transformación hacia la automatización de sus procesos a través de la aparición de nuevas tecnologías. Estas OT dependen en gran medida de la manipulación segura de los ICS, los cuales son considerados críticos para el desarrollo socioeconómico de una nación. Es por esto que el diseño y la implementación de medidas *activas* tienen tiene un carácter proactivo, es decir, intenta prevenir que se produzcan incidentes de seguridad, tales como infecciones por malware, ataques de denegación de servicio, robo de información; las *pasivas,* tienen un carácter reactivo y se ejecutan una vez ha ocurrido el incidente (UNIR, 2020), estas medidas juegan un rol esencial para la protección cibernética de los sistemas de control de la red eléctrica (Knowles, 2015).

Los ICS han pasado de operar en un entorno relativamente confiable, donde se ejecutaban procesos aislados y no tenían ninguna interoperabilidad entre sus procesos, a la prevalencia actual de las redes públicas e Internet. Por ejemplo, en el año 2010, Stuxnet demostró lo vulnerables que son los sistemas de control, por lo que los ICS, la ciberseguridad y el gobierno se enfrentan a desafíos adicionales diferentes a las que amenazan las redes corporativas. El panorama de amenazas cibernéticas establece los lineamientos de ciberseguridad para mejorar la protección de los ICS a través de una comparación de estándares, políticas y estrategias nacionales e internacionales.

Las IC, son sectores necesitados de un modelo Ciberseguridad, los ICS están expuestos a amenazas de seguridad cibernética para los cuales nunca fueron diseñados. Repetidas intrusiones cibernéticas en organizaciones de todo tipo ponen de manifiesto la necesidad de mejorar la seguridad cibernética. Las amenazas cibernéticas siguen creciendo y representan

uno de los riesgos operativos más serios que enfrentan las organizaciones modernas. La seguridad de la sociedad y económica depende del funcionamiento confiable de la infraestructura crítica frente a esas amenazas. Se requiere de un modelo de ciberseguridad específico para los ICS que ayuden a las organizaciones de dicha categoría a evaluar y mejorar sus programas de seguridad cibernética (Said, 2016).

Sin embargo, si bien el Estado colombiano ha venido construyendo una serie de políticas frente a la protección de la infraestructura critica en el campo de la ciberseguridad, es importante tener en cuenta la existencia en el mercado de estándares internacionales en la materia, los cuales conforman un catálogo de buenas prácticas para establecer y desarrollar los lineamientos de ciberseguridad para mejorar la protección de los ICS aplicados ISA INTERCOLOMBIA, los cuales contemplen todos los niveles organizativos y operativos de una empresa y que pueden incorporar y adoptar varias de estas prácticas reconocidas.

En consecuencia, basados en estas prácticas, el desarrollo de las actividades de OT y IT presenta graves problemas en materia de engranaje y correlación, producto de la ausencia de lineamientos donde se vinculen los procesos, personas y tecnologías para incorporar el aprovechamiento de los recursos tecnológicos en la optimización de la operación. La estrategia para el desarrollo de los lineamientos tiene como objetivo, integrar prácticas existentes caracterizando y definiendo los elementos fundamentales que permitan la construcción de un macroproceso para gestionar la seguridad cibernética de forma integral, a través de un lenguaje común, unos fundamentos teóricos homogenizados y unos procedimientos en los que se describa el modo de actuar en materia de ciberseguridad.

Los Marcos, guías y estándares de ciberseguridad que veremos a continuación, permiten, a partir de la definición de lineamientos de ISA INTERCOLOMBIA, ser una herramienta cuyo propósito es alinear el comportamiento de todos los miembros de la organización hacia un horizonte y Visión compartida de la gestión del riesgo de ciberseguridad en los ICS.

La importancia de contar con estos elementos va más allá del tema netamente formal, y se constituyen más bien en instrumentos de gestión, para inspirar, motivar y comprometer a la organización en el logro de los propósitos contenidos en el Reporte Integrado de Gestión ISA 2019.

6.2.1 Marcos, guías y estándares para ciberseguridad en los ICS.

Para la gestión de seguridad de la información y asegurar la disponibilidad, integridad y confidencialidad de la empresa se considerara la a familia de las normas ISO/IEC Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC), forman parte de una serie de estándares que proveen un excelente marco de trabajo para todo tipo de industrias, las cuales se agrupan por temáticas y contienen mejores prácticas a ser aplicadas de acuerdo al entorno requerido, las normas más relevantes en materia de seguridad y que pueden considerasen para ser aplicados a los sistemas de control industrial, corresponden a la norma ISO/IEC 27002 y la familia de normas ISO 27000.

La norma ISO/IEC 27001 define los requisitos para un sistema de gestión de seguridad de la información (SGSI) y la ISO/IEC 27002 proporciona un catálogo detallado de los

controles de seguridad de la información que pueden gestionarse a través del SGSI. Si bien los controles se enfocan más en cuestiones de gestión y organización los cuales deben entenderse como mejores prácticas, estos pueden ser considerados con un primer acercamiento a nivel práctico para explorar las vulnerabilidades existentes de seguridad de los sistemas de OT, mediante un test de intrusión que permitan evaluar la seguridad física y lógica del sistema.

La norma ISO/IEC 27032 es un estándar de Ciberseguridad llamada: *Tecnologías de la información - Técnicas de seguridad Directrices para la Ciberseguridad,* garantiza directrices generales para fortalecer el estado de la ciberseguridad de una empresa, proporciona un marco seguro para el intercambio de información, el manejo de incidentes y la coordinación para hacer más seguros los procesos a nivel táctico y estratégico , integra todas la partes interesadas con el único fin de gestionar y minimizar los riesgo relacionados con:

- Seguridad de información
- Seguridad de la red
- Seguridad en internet
- Protección de la infraestructura de información crítica (CIIP).

La ciberseguridad se basa en la seguridad de la información, seguridad de las aplicaciones, seguridad de redes y seguridad de internet, por lo tanto, es una de las bases que se requieren para la protección de la infraestructura de información crítica, la norma mejora la seguridad de internet y esta garantiza un entorno seguro a través de algunas políticas de

seguridad para abordar el establecimiento de confiabilidad, colaboración, intercambio de información y orientación técnica para la integración del sistema entre las partes interesadas en el ciberespacio. Una falla de ciberseguridad de cualquier empresa puede tener un impacto negativo en la disponibilidad de sistemas de infraestructuras críticas de información suministrados por proveedores de infraestructuras críticas.

La norma ISO 27033: *Tecnología de la información - Técnicas de seguridad - Seguridad de la red.* Es una guía que contiene aspectos de seguridad, el funcionamiento y el uso de redes de sistemas de información y sus interconexiones. Brinda un enfoque general de como identificar y analizar los riesgos de seguridad en la red:

> Aplica a la seguridad de los dispositivos, la seguridad de las actividades de gestión relacionadas con los dispositivos, las aplicaciones / servicios y los usuarios finales, además de la seguridad de la información que se transfiere a través de los enlaces de comunicación". (iso.org, 2015)

La definición de los requisitos de seguridad de la red en función de ese análisis facilita una descripción general de los controles que respaldan las arquitecturas de seguridad técnica de la red y los controles técnicos relacionados, así como los controles no técnicos y los controles técnicos que son aplicables no solo a las redes. La seguridad de la red es desarrollada tanto por componentes de infraestructura tecnológicas como en tecnologías operacionales, según ISO, Consiste en 7 partes:

1. Gestión de seguridad de redes
2. Arquitectura de seguridad de redes

3. Marcos de redes de referencia
4. Aseguramiento de las comunicaciones entre redes mediante gateways
5. Acceso remoto
6. Salvaguardia de comunicaciones en redes mediante VPNs
7. Diseño e implementación de seguridad en redes.

ENISA (2011) considera que debería haber una única referencia mundial con respecto a políticas y lineamientos en ciberseguridad. Lo que facilitaría la estandarización y la aplicación de regulaciones para aquellos operadores de servicios críticos con presencia en varios países con centros de control y estructuras organizativas distribuidas y autónomas. Existen varios marcos internacionales de gobernanza y seguridad relacionados con los sistemas ICS, que se relacionan en la tabla 4.

Tabla 4. Marcos internacionales de gobernanza y seguridad relacionados con los sistemas ICS. Fuente: Elaboración Propia a partir de ENISA (2011)

Marco Internacional	Definición y objetivo
Guía para la Seguridad de los ICS, SP800-82, NIST[5]	El propósito de la guía es proporcionar orientación para asegurar los ICS, incluyendo los sistemas SCADA y DCS. El documento proporciona una visión general de ICS, revisa las topologías y arquitecturas típicas del sistema, identifica las amenazas y vulnerabilidades, y proporciona contramedidas de seguridad recomendadas para mitigar los riesgos asociados.
Controles de seguridad y privacidad para sistemas y organizaciones federales de información. NIST SP 800-53[6]	Tiene como objetivo facilitar un enfoque más consistente, comparable y repetible para seleccionar y especificar controles de seguridad para sistemas y organizaciones de información, igualmente proporcionar un catálogo de controles de seguridad para satisfacer las necesidades de protección de la información y las demandas de futuras necesidades de protección basadas en amenazas, requisitos y tecnologías.

[5] NIST SP800-82. (2015). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
[6] NIST SP800-53 (2015). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Marco Internacional	Definición y objetivo
Protección de los sistemas de control industrial: recomendaciones para Europa y los Estados miembros (ENISA, 2011).	El objetivo del estudio es identificar las amenazas, riesgos y desafíos en el área de protección de ICS, hace una relación de la creciente dependencia de los sistemas ICS con el Internet y la relación de los sistemas ICS con las áreas emergentes, como las redes inteligentes. Basado en el análisis, este documento propone buenas prácticas y recomendaciones para todas las partes interesadas que les ayudarán a mejorar la seguridad y la resistencia de los sistemas ICS europeos.
Guía de buenas prácticas para el control de procesos y seguridad SCADA - CPNI[7]	La guía proporciona una visión general de la necesidad de control de procesos y seguridad del sistema SCADA, destaca las diferencias entre el control de procesos y la seguridad del sistema SCADA y la seguridad de IT, e identifica 7 elementos para abordar la seguridad del sistema de control de procesos y para cada uno, presenta principios de buenas prácticas.
21 pasos para mejorar la seguridad cibernética de las redes SCADA - The U.S. Department of Energy[8]	Esta guía contiene 21 pasos para ayudar a cualquier organización a mejorar su seguridad para las redes ICS / SCADA y así evitar el acceso no autorizado a la información contra compromisos que podrían conducir a un mal funcionamiento o inestabilidad en el sistema.
Protección Infraestructura Crítica - NERC[9]	Este estándar contiene normas y medidas de seguridad para proteger los sistemas eléctricos de América del Norte y establece multas por incumplimiento de su aplicación. Reconoce los diferentes roles de cada entidad en la operación del sistema eléctrico, la criticidad y las vulnerabilidades de los activos que lo componen y los riesgos a los que están expuestos.
Automatización Industrial y Seguridad de Sistemas de Control– ISA99[10]	Engloba un conjunto de guías e informes técnicos, de los que finalmente sólo se publicaron las dos primeras guías y un informe técnico. La primera guía (ANSI/ISA-99.01.01-2007 publicada incluye los conceptos, términos y modelos que se han de usar en el resto de los componentes de la serie. La segunda guía (ANSI/ISA-99.02.01-2009) publicada describe los elementos necesarios para la implantación de un sistema de gestión de la ciberseguridad y cómo conocer los requerimientos de cada elemento. El informe técnico (SI/ISA-TR99.01.02-2007) publicado recoge una serie de herramientas de seguridad, al igual que su modo de implantación y despliegue dentro de los

[7] Centre for the Protection of National Infrastructure (CPNI). Good Practice Guide. https://bit.ly/2olfHYH
[8] United States. (2007) https://www.hsdl.org/?abstract&did=1826
[9] United States. Cyber Security — Information Protection. (2011). https://www.nerc.com/files/CIP-011-1.pdf
[10] ISA99. Industrial Automation and Control Systems Security. (2009). https://www.isa.org/isa99/

Marco Internacional	Definición y objetivo
	sistemas de control. Este informe fue actualizado para recoger nuevas herramientas.
Estándar ISA / IEC 62443 para la red industrial y seguridad del sistema[11]	Es la evolución de la norma ISA99, La norma se compone de un total de 13 documentos divididos en: (a) Cinco informes técnicos; (b) Una especificación técnica; y, (c) Siete guías agrupadas en cuatro bloques según su contenido, así: General, Políticas y procedimientos, Sistema, y Componentes.
Gestión de sistemas de energía e intercambio de información asociado - Seguridad de datos y comunicaciones. IEC 62351-4:2018[12]	El ámbito de actuación de la norma es la seguridad en las operaciones de control del sector energético. El objetivo es acometer el desarrollo de estándares de seguridad para los protocolos de comunicaciones definidos por el grupo IEC TC 57, específicamente IEC 60870-5 (IEC101, IEC104, entre otros), IEC 60870-6 (ICCP), IEC 61850 (MMS, GOOSE), IEC 61970 y IEC 61968. La norma IEC 62351 se divide en 11 documentos, siendo el primero la introducción a la norma, el segundo el glosario de términos y el resto el conjunto de medidas de seguridad aplicadas por familias de protocolos. Los últimos documentos unidos a la norma definen la implementación de medidas como el control de acceso basado en roles (RBAC – Role Based Access Control), la gestión de claves, la definición de una arquitectura de seguridad o las medidas de seguridad para utilizar con ficheros XML.
Estándar de capacidades de ciber seguridad para dispositivos electrónicos inteligentes. IEEE 1686-2007[13]	El estándar define las funciones y características que se proporcionarán en dispositivos electrónicos inteligentes (IED) de subestación para acomodar programas de protección de infraestructura crítica (CIP). El estándar aborda la seguridad con respecto al acceso, operación, configuración, revisión de firmware y recuperación de datos desde un IED.

A nivel mundial existen organizaciones y políticas de Estados que abordan la protección de los componentes de IT de las infraestructuras críticas. Sin embargo, no han sido los mismos esfuerzos para abordar el aseguramiento de los componentes de las ICS. La

[11] ISA. IEC 62443. https://www.isa.org/pdfs/autowest/phinneydone/
[12] ISA. IEC 62351. https://webstore.iec.ch/publication/30079
[13] IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities. https://ieeexplore.ieee.org/document/4453853

comunicación de la Comisión Europea al Consejo y al Parlamento Europeo del 20 de octubre 2010 "COM (2010)" reconoce que han surgido nuevas amenazas como lo fue "Stuxnet" para las OT. Sin embargo, estas no incluyen ningún listado de amenazas específicas para los ICS[14]. Por lo que, la Agencia Europea de Seguridad de Redes e Información (ENISA por sus siglas en inglés European Union Agency for Network and Information Security) declaró que: este tipo de amenazas deberán ser reconsideradas como un esfuerzo cohesivo entre el gobierno y la industria, para mejorar la postura de seguridad de los sistemas de control dentro de la infraestructura crítica de la nación.

Los ICS incluyen SCADA, los DCS y los PLC. Si bien, los sistemas SCADA son implementados para controlar de manera centralizada algunos componentes disgregados mediante la visualización y supervisión de datos, los DCS son desplegados para vigilar y controlar los sistemas de producción en una LAN[15]; los PLC son implementados para ejecutar aplicaciones específicas mediante el control regulatorio de cada una de ellas. Todos estos sistemas están altamente interconectados y entre ellos son mutuamente dependientes (Stouffer K. a., 2011).

Sin embargo, hay que tener en cuenta que los ICS tienen características particulares que difieren de los sistemas tradicionales de IT. Una de las principales diferencias es que su ejecución tiene un efecto directo en los servicios vitales que las infraestructuras críticas

---

[14] The European Commission. Critical infrastructure protection. (2010). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al33259

[15] Una red de área local o LAN es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio. La topología de red define la estructura de una red. Una parte de la definición topológica es la topología física, que es la disposición real de los cables o medios. (https://www.cisco.com/c/es_co/solutions/smb/networks/infographic-basic-concepts.html)

ofrecen a la sociedad, por ejemplo: comunicaciones y navegación aeronáutica, sistema eléctrico, tratamiento de aguas residuales, entre otros; que si llegaran a tener una interrupción no deseada afectaría directamente en la salud y la seguridad de las vidas humanas, pérdidas financieras, así como también daños graves al medio ambiente (Stouffer K. a., 2011).

Independientemente de la guía, política o estándar vistos en anteriormente, la mayoría de ellos expresan que los sistemas ICS de las OT suelen ser mucho más pequeños que las redes de IT, con configuraciones estáticas en lugar de dinámicas. Algunas de las recomendaciones son: (1) no usar el protocolo de control de host dinámico (DHCP); (2) deshabilitar las redes Wifi; (3) bloquear el acceso a Internet y al correo electrónico; (4) estar segregadas en subredes de las redes corporativas de IT, ya sea de forma independiente o mediante un sistema de seguridad de red que monitoree y controle el tráfico de red entrante y saliente basado en reglas de seguridad - firewall.

Los operadores de ICS constantemente están en búsqueda de normatividad y recomendaciones de acuerdo con sus necesidades y aplicación. Sin embargo, la naturaleza obligatoria de algunas regulaciones emitidas por el gobierno o sector específico no necesariamente los hace más efectivos para mejorar la ciberseguridad en este tipo de sistemas, tales como el SCADA o DCS, pero si proporciona unos requisitos mínimos necesarios para una seguridad mínima adecuada. Una encuesta realizada por Tripwire[16] en el año 2014 reveló que solo el 70% de las industrias dedicadas a la prestación de servicio eléctrico cree que tiene una comprensión clara de todos los requisitos actuales del standard

[16] Tripwire. Update NERC Survey Data. Portland, Oregon. https://www.darkreading.com/risk/tripwire-survey-nerc-cip-compliance-not-sufficient-to-ensure-bulk-electric-system-security/d/d-id/1140893

NERC CIP[17], del cual se hablará con más detalle adelante, y consideran que este es necesario para garantizar la seguridad, lo que permite observar que el 30% restante de los operadores de ICS no son conscientes de la implementación del estándar para la protección de sus sistemas.

Debido a que la gran mayoría de las publicaciones académicas, lineamientos y estándares están dirigidos a gestionar los riesgos de la seguridad de la información, IT, los operadores de infraestructura crítica consideran que la ausencia de investigaciones académicas de los procesos dentro de la protección de la información con un enfoque técnico en las OT son un riesgo para el aseguramiento de los entornos de sistemas de control industrial (Knowles, 2015).

Por ejemplo, las dimensiones de la tríada: Confidencialidad, Integridad y Disponibilidad (CIA por sus siglas en inglés Confiability, Integrity and Availability) en la seguridad de la información tienen la misma importancia en cada uno de sus 3 componentes, pero en la práctica, se podría considerar que de acuerdo con las características propias de la organización y por razones económicas, entre cada uno de los componentes, uno puede tener un mayor peso y relevancia que el otro. Sin bien, los ICS son responsables del monitoreo y control de las infraestructuras críticas de sociedad, como son la electricidad, el suministro de gas, las comunicaciones aeronáuticas, servicios de logística, bancos y hospitales, entre otros, en estos entornos industriales donde sus operadores dependen de los sistemas SCADA y DCS la prioridad la tiene el componente de Disponibilidad dando un giro a la triada, es decir, sí

[17] North American Electric Reliability Corporation. https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

para una compañía la triada está conformada en el orden CIA, para los operadores de infraestructura crítica, el orden puede cambiar a DIC (Knowles, 2015).

Sin embargo, unas de las principales falencias en la terminología y conceptualización de las palabras que describen la protección de las infraestructuras críticas se encuentran en la ambigüedad de estas. El concepto de aseguramiento se preocupa principalmente por garantizar parámetros operativos seguros, mientras que la seguridad se centraliza por evitar, prevenir y reducir los ataques cibernéticos exitosos en los ICS (Hemsley, 2018).

6.3 Análisis de Lineamientos, Estándares y Políticas Existentes.

Los lineamientos y guías son una herramienta para proporcionar niveles de ciberseguridad para la protección de cualquier sector de las infraestructuras críticas. El continuo crecimiento de la tecnología de la información permite que un mundo digital en el que el ciberespacio está surgiendo de manera significativa y donde el cibercrimen, el espionaje y las armas cibernéticas aumentan día a día, ponen en riesgo la operatividad de los servicios esenciales, haciendo que el sistema de control industrial sea vulnerable a estas amenazas de seguridad cibernética emergentes.

Para el presente trabajo y debido a que en la empresa ISA INTERCOLOMBIA aún no están definidos los lineamientos de ciberseguridad, por tal motivo tampoco están establecidos para los ICS, estos deben ser creados de manera interdisciplinar entre varias áreas, por tanto, entenderemos como lineamiento todo aquello que cumpla con los siguientes componentes:

- La identificación de los marcos, guías, estándares y buenas prácticas que se pueden desplegar para la organización a la luz de su plan estratégico.
- El análisis conceptual y comparativo de los requerimientos surgidos del análisis del punto anterior para determinar las bases que den lugar a los lineamientos para ISA INTERCOLOMBIA.

Una gran cantidad de recomendaciones y lineamientos abordan la seguridad del ICS para casos de uso y tecnologías particulares. Por ejemplo, El Departamento de Seguridad Nacional de los Estados Unidos ha emitido documentos que contienen: (1) estrategias para la protección de los ICS, denominado: "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies"; (2) prácticas y recomendaciones de administración de parches, llamado: "Recommended Practice for Patch Management of Control Systems"; y, (3) documentos relacionados con la configuración y administración de acceso remoto, como: "Configuring and Managing Remote Access for Industrial Control Systems", entre otros.

El Centro de Coordinación de Seguridad de Infraestructura Nacional del Reino Unido, también ha producido guías y buenas prácticas para desplegar sistemas de seguridad de red que monitorea y controla el tráfico basado en reglas de seguridad para entornos de sistemas de control industrial, entre ellos se encuentra: "Firewall Deployment for SCADA and Process Control Networks", donde se realiza una discusión de las ventajas y desventajas de la implementación de firewalls para segregar los ICS de una red empresarial (Byres, 2005).

El Instituto Nacional de Estándares y Tecnología (NIST), es una institución pública de los Estado Unidos que direcciona sus recursos (financieros y humanos) al desarrollo de investigación en el área de la seguridad de la información, uno de sus objetivos en la investigación es emitir documentos relacionadas con la protección de los ICS a través del Proyecto de Implementación de la Ley Federal de Gestión de Seguridad de la Información (FISMA por sus siglas en inglés Federal Information Security Management Act). Dentro de los múltiples estándares publicados por este Instituto, se encuentra la NIST-800-55, donde se proporciona información sobre el uso de métricas de rendimiento para evaluar una organización con respecto a los controles, políticas y procedimientos de seguridad ya establecidos, con el fin de decidir dónde invertir recursos de seguridad o evaluar controles ya obsoletos. Esta guía de medición del rendimiento para la seguridad de la información se describen tres grandes categorías de métricas para los controles de seguridad: (1) progreso de la implementación; (2) robustez (efectividad) y eficiencia; y (3) impacto de la seguridad (Barker, 2007).

Las organizaciones que emiten estándares de seguridad de la información han realizado un gran esfuerzo para expandir sus lineamientos a los requerimientos de los ICS, y esto ha generado fuertes discusiones entre aquellos que apoyan la idea de la segregación de las IT con las OT, y no comparten la implementación de estándares y lineamientos generados desde un principio para las IT, sin embargo, existen métricas exclusivas para los ICS, un ejemplo de ello es la taxonomía[18] I3P, la cual describe 11 áreas principales de controles de seguridad,

[18] Def. Taxonomía: ciencia que estudia los principios, métodos y fines de la clasificación. Este término se utiliza especialmente en biología para referirse a una clasificación ordenada y jerarquizada de los seres vivos

otro ejemplo, es la taxonomía de métricas de seguridad del sistema de control industrial emitido por Sandia National Laboratories, el cual es un laboratorio de investigación y desarrollo de seguridad nuclear en los Estados Unidos (Johnson, 2011).

En la Tabla 5, se describen aquellos documentos que contienen lineamientos y métricas para la protección y aseguramiento de los sistemas de control industrial del sector eléctrico:

Tabla 5. Publicaciones de Seguridad del Sistema de Control Industrial en el Sector Energía. Fuente: Elaboración propia a partir de la Guía IEEE para seguridad física y electrónica de subestación de energía eléctrica (2000),, Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP)from Terrorist Attacks Focusing on Threats Emanating from Cyberspace (2013), VGB PowerTech Annual Report (2013), U.S. DoE 21 Steps to Improve Cyber Security for SCADA Systems (2001), VGB PowerTech Annual Report (2018), Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities (2002); ELECTRICITY SUBSECTOR CYBERSECURITY RISK MANAGEMENT PROCESS (2012), NIST Special Publication 800-82 (2015).

#	**Publicación**	**Descripción**
1	IEEE 1402 Guide for Electric Power Substation Physical and Electronic Security	Esta guía describe las buenas prácticas y recomendadas para la seguridad física de las subestaciones de energía eléctrica. Aun cuando esta monografía está enfocada a establecer los lineamientos de ciberseguridad para mejorar la protección de los ICS se abordan temas de seguridad física como primer nivel de protección. Esta guía fue diseñada con base a amenazas físicas existentes, tales como: el acceso no autorizado a las instalaciones de la subestación, el robo de material y el terrorismo. Incluye recomendaciones para el control de acceso, el monitoreo de las instalaciones, entre otras herramientas para mitigar estas amenazas.
2	OSCE Good Practices Guide on Non-Nuclear	Esta guía ofrece recomendaciones de buenas prácticas para evitar ataques cibernéticos relacionados con los ataques terroristas

y en educación para ordenar y diseñar los objetivos del aprendizaje. (acción y efecto de clasificar). Fuente: RAE (2020)

#	Publicación	Descripción
	Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace	convencionales. En esta guía se describen las vulnerabilidades potenciales para los países consumidores de energía e identifica las amenazas a esa infraestructura. Resalta algunas recomendaciones para la mejorar la protección de los sistemas ICS. Por ejemplo: (1) Una de las maneras más efectivas para enfrentar las amenazas trasnacionales hacia las plantas de energía eléctrica no nucleares, los operadores y propietarios deben establecer mecanismos de cooperación y coordinación internacional; y, (2) El intercambio de información sensible entre las agencias de inteligencia y protección del Estado y los operadores de las infraestructuras de energía crítica no nuclear.
3	VGB Guideline R 175	Estos lineamientos tienen como objetivo principal ofrecer recomendaciones de cómo mejorar la seguridad en los sistemas IT y OT los operadores de plantas de energía. Hace una descripción de cada una de las áreas tecnológicas, separando los ICS que son las encargadas de controlar y supervisar los procesos operacionales de la industria y la cual no debería verse afectada por las amenazas en los sistemas IT.
4	NERC CIP 001-011	NERC CIP-011-1[19] Este lineamiento nace con el fin de evitar el acceso no autorizado a la información del sistema cibernético de un sistema eléctrico, donde se especifican los requisitos de protección de la información contra los compromisos que podrían conducir a una operación incorrecta o interrupción del sistema eléctrico.
5	U.S. DoE 21 Steps to Improve Cyber Security for SCADA Systems	▪ *Los 21 pasos para mejorar la seguridad cibernética de los sistemas SCADA20, emitidos por el Departamento de Energía de los Estado Unidos, los cuales están divididos en dos categorías. Los primeros 11 pasos tratan sobre la necesidad e implementación del ICS. Así:* ▪ *Identifique todas las conexiones a las redes SCADA.* ▪ *Desconecte las conexiones innecesarias a la red SCADA.* ▪ *Evalúe y fortalezca la seguridad de cualquier conexión restante a la red SCADA.* ▪ *Endurezca las redes SCADA eliminando o deshabilitando servicios innecesarios.* ▪ *No confíe en protocolos patentados para proteger su sistema.* ▪ *Implemente las características de seguridad proporcionadas por los proveedores de dispositivos y sistemas.* ▪ *Establezca un medio de control sólido que se utilice como puerta de entrada a la red SCADA.* ▪ *Implemente sistemas de detección de intrusos internos y externos y establezca monitoreo de incidentes las 24 horas del día.*

[19] United States. Cyber Security — Information Protection. https://www.nerc.com/files/CIP-011-1.pdf

[20] United States. Department of Energy. President's Critical Infrastructure Protection Board. 2002. https://www.hsdl.org/?view&did=1826

#	Publicación	Descripción
		▪ *Realizar auditorías técnicas de dispositivos y redes SCADA, y cualquier otra red conectada, para identificar problemas de seguridad.* ▪ *Realice encuestas de seguridad física y evalúe todos los sitios remotos conectados a la red SCADA para evaluar su seguridad.* ▪ *Establecer "Equipos rojos" SCADA para identificar y evaluar posibles escenarios de ataque.* Los siguientes 10 pasos abordan la gestión del sistema de control industrial (procesos, políticas, lineamientos, entre otros). Así: ▪ *Definir claramente los roles, responsabilidades y autoridades de seguridad cibernética para gerentes, administradores de sistemas y usuarios.* ▪ *Documente la arquitectura de red e identifique los sistemas que cumplen funciones críticas o contienen información confidencial que requiere niveles adicionales de protección.* ▪ *Establecer un proceso efectivo de gestión de riesgos.* ▪ *Establecer una estrategia basada en el principio de defensa en profundidad.* ▪ *Identifique claramente los requisitos de seguridad cibernética.* ▪ *Establecer métodos de gestión de la configuración.* ▪ *Realizar autoevaluaciones de rutina.* ▪ *Establecer copias de seguridad del sistema y planes de recuperación ante desastres.* ▪ *El liderazgo organizacional superior debe establecer expectativas para el desempeño de seguridad cibernética y responsabilizar a las personas por su desempeño.* ▪ *Establezca políticas y realice capacitaciones para minimizar la probabilidad de que el personal de la organización divulgue inadvertidamente información confidencial sobre el diseño del sistema SCADA, operaciones o controles de seguridad.*
6	U.S. DoE Electricity Subsector Cybersecurity Risk Management Process	El departamento de energía de los Estado Unidos[21] emitió un proceso de administración de riesgos en ciberseguridad. Estos lineamientos están divididos en 5 capítulos, los cuales están organizados de manera secuencial para proporcionar un proceso de gestión de gestión de riesgos escalable, específico para los riesgos de los ICS. El modelo de gestión de riesgos del departamento de energía desarrolla una estructura de tres niveles, así: ▪ Organizacional ▪ Procesos de negocios y misionales ▪ ICS
7	U.S. DoE Energy Infrastructure Risk	Listas de verificación de gestión de riesgos de infraestructura energética para instalaciones de energía pequeñas y medianas[22]. En

[21] electricity subsector cybersecurity risk management https://www.energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf

[22] U.S. Department of Energy Office of Energy Assurance (2012). https://www.hsdl.org/?view&did=446053

#	Publicación	Descripción
	Management Checklists for Small and Medium Sized Energy Facilities	este documento el nivel de riesgo de un activo es calificado mediante dos factores: ▪ El valor que el operador le asigna al activo debido a las consecuencias durante una interrupción. ▪ La probabilidad de que una vulnerabilidad específica del activo sea explotada por una amenaza. Esta lista de verificación incluye seis pasos: ▪ Paso 1. Identificar los activos críticos y los impactos de su pérdida. ▪ Paso 2. Identifique qué protege y respalda los activos críticos. ▪ Paso 3. Identificar y caracterizar la amenaza. ▪ Paso 4. Identificar y analizar vulnerabilidades. ▪ Paso 5. Evaluar el riesgo y determinar las prioridades para la protección de activos. ▪ Paso 6. Identifique las opciones de mitigación, los costos y las compensaciones.
8	NIST SP 800-82	La guía para la seguridad de los ICS, está enfocada principalmente a emitir recomendaciones para la gestión de herramientas de prueba de vulnerabilidad y penetración a los sistemas ICS. Igualmente proporciona medidas de cómo proteger los sistemas, incluidos los SCADA, DCS y otras configuraciones de sistemas de control, como son los PLC.

Ahora bien, algunos elementos comunes identificados en los marcos existentes de gobernanza y seguridad relacionados con los sistemas ICS y en Sector Energía, a nivel de normas, estándares, políticas, guías y mejores prácticas, entre otros, con el fin de asegurar los componentes de los sistemas de ICS, son descritos a continuación.

En la actualidad los ciberataques a infraestructuras críticas no pueden considerarse sólo teorías y tratarse a ese nivel, se deben definir planes de acción, hojas de ruta y sistemas de protección.

Las normas, estándares y guías son directrices de referencia voluntarias que pueden ser aplicadas de manera transversal (como se dijo anteriormente), tienen un lenguaje común y

orientado a la gestión del riesgo, ayudan a los responsables y operadores de infraestructuras críticas a identificar, inventariar y gestionar riesgos informáticos.

A la hora de aplicar medidas de seguridad a partir de los marcos de trabajo analizados parten de la importancia de tener una visión amplia del sistema completo e implantarlas a todos los niveles organizacionales. Comenzando desde los niveles técnicos más bajos, subiendo hasta las medidas organizativas, y de procesos que impliquen a todas las personas de la organización, desde los niveles de operario hasta la alta gerencia.

Cabe resaltar que los lineamientos a ser desarrollados no son pioneros en este campo, se tienen marcos para la gobernanza y aseguramiento de los ICS y con aplicabilidad al sector eléctrico, esto no quiere decir que el modelo de Ciberseguridad a desarrollarse excluya estos documentos, al contrario, se utilizaran para definir los lineamientos de cibeseguridad para mejorar la protección de los ICS.

7. Análisis de los estándares, políticas e información académica del sector eléctrico que permita identificar las ventajas y desventajas, junto con las mejores prácticas en la protección de los sistemas de control industrial.

Este capítulo presenta un análisis conceptual y comparativo de los estándares, normas, mejores prácticas, publicaciones gubernamentales y de la industria privada que están relacionadas con la seguridad y protección de los Sistemas de Control Industrial (ICS). Estas publicaciones son diseñadas para la evaluación de vulnerabilidades y auditorias de seguridad cibernética para proteger los sistemas SCADA y DCS.

7.1 Conceptos Relacionados con Tecnologías de la Información y de Operaciones

Dentro de una organización existen hardware como sistemas y dispositivos, al igual que software que interactúan entre sí para producir, transferir y almacenar información administrativa y operativa, la conexión entre estas redes de comunicaciones, datos, hardware y software es comúnmente llamada Tecnologías de Información (IT), esta afirmación se soporta en la definición que ISO 20016-1/2014 presenta:

> Conjunto de una o más computadoras, software asociado, periféricos, terminales, operaciones humanas, procesos físicos, medios de transferencia de información, que forman un todo autónomo, capaz de realizar procesamiento de información y / o transferencia de información. Pág. 46

Para abordar la jerarquización de los ICS es importante entender que estos constan de 4 niveles, como se muestra en la Ilustración 4, que luego será detallado para ISA INTERCOLOMBIA.

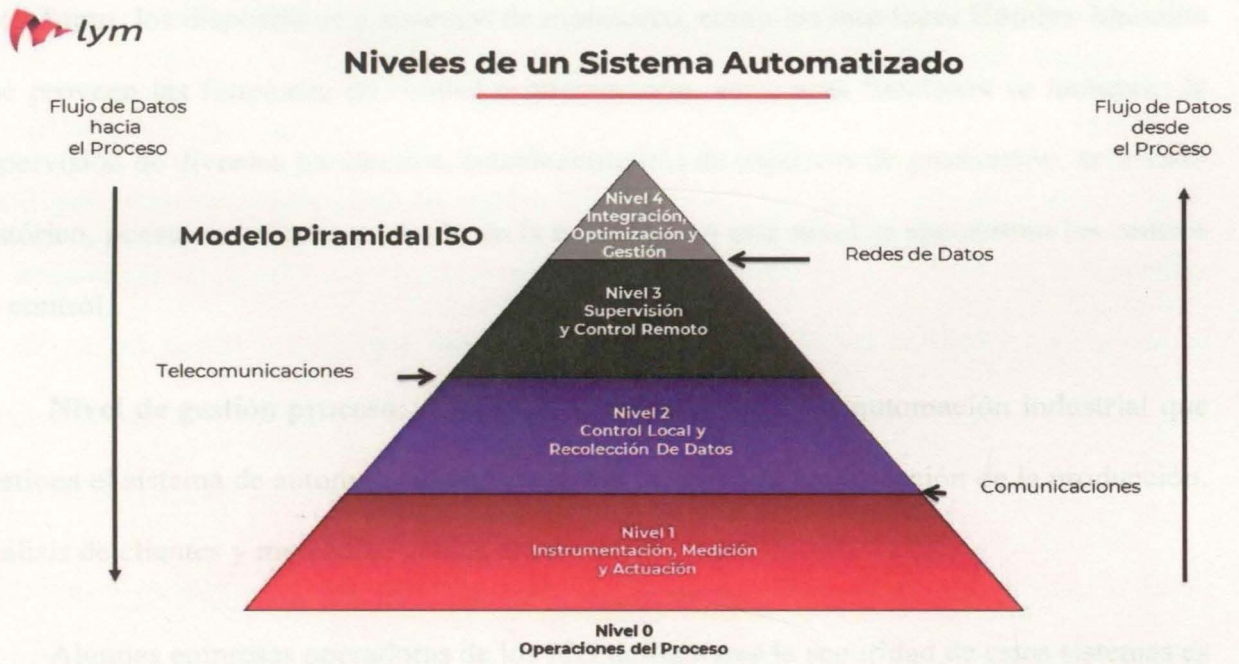

Ilustración 4. Niveles de un sistema de control industrial tomado de: https://www.lymcapacitacion.com/blog/14450/niveles

Nivel de instrumentación: Es el nivel más bajo, en el encontramos los dispositivos físicos como son los medidores, actuadores, relés, accionadores, sensores, estos son encargados de transferir los datos de procesos y maquinas al siguiente nivel de monitoreo y análisis.

Nivel de control: En este nivel un operador programa una función o estrategia de control para realizar ciertas operaciones automáticas durante el proceso, hacen parte de él los dispositivos controladores como son: los computadores, controladores, PLC, entre otros.

Nivel de supervisión : Corresponde a los sistemas de supervisión y control, allí se encuentran los dispositivos y sistemas de monitoreo, como las interfaces Hombre Maquina que proveen las funciones de control e intervención, entre esas funciones se incluyen: la supervisión de diversos parámetros, establecimientos de objetivos de producción, archivado histórico, puesta en marcha y parada de la máquina, en este nivel se encuentran los centros de control.

Nivel de gestión proceso: Este es el nivel superior de la automación industrial que gestiona el sistema de automatización, sus tareas incluyen la planificación de la producción, análisis de clientes y mercados, ventas etc.

Algunas empresas operadoras de los ICS definen que la seguridad de estos sistemas es paralela a las medidas tradicionales que se aplican a las IT, debido a algunas características, como son: sistemas aislados, arquitecturas de hardware y software comercial, entre otros. Sin embargo, al contar con implementaciones de dispositivos con protocolo de Internet (IP), traen consigo el incremento de riesgos, amenazas y vulnerabilidades de ciberseguridad, como se pudo leer en el capítulo anterior, pero al mismo tiempo, ha promovido la modernización y la conectividad remota a sus aplicaciones de supervisión y control, haciendo que los sistemas ICS de las OT comiencen a parecerse a los sistemas IT (Stouffer K. a., 2011).

Para el diseño y construcción de un sistema seguro en IT, la seguridad de la información es un factor clave y esencial, tal como se observó en los apartados anteriores, y esta se encuentra respaldada por la triada "CIA". La confidencialidad se refiere al acceso a información y que sólo las personas o sistemas autorizadas en el proceso pueden tener acceso, de lo contrario, cualquier que no tenga los privilegios y desea acceder es considerada una entidad no autorizada. Se considera vulnerada la confidencialidad cuando personas no autorizadas acceden intencionalmente o no a la información. La integridad se refiere a la fiabilidad de los datos que incluyen información completa, sin alteración y sin compromisos. La disponibilidad se refiere a la información o datos disponibles para usuarios autorizados en el tiempo, modo y lugar que sea necesario. La disponibilidad es vulnerada cuando el recurso no está disponible para los usuarios autorizados en el modo, tiempo y lugar que se requiere. (Whitman, 2011).

La disponibilidad del servicio público de electricidad es el eje principal de la distribución de energía eléctrica, el cual constituye un servicio crítico que requiere de la continuidad operativa de instalaciones, tales como: (1) subestaciones eléctricas de 110 kV; (2) una infraestructura lineal de circuitos eléctricos de media tensión de 13,2 kV, 34,5 kV y 44kV; (3) una infraestructura lineal de circuitos eléctricos en baja tensión. Los sistemas de distribución de energía eléctrica se encuentran entre las infraestructuras más críticas de una sociedad moderna, y sirven como la columna vertebral para el buen funcionamiento de otros servicios esenciales. Es por esta razón, que una de las prioridades de los países desarrollados es el aseguramiento de estos servicios contra los riesgos y amenazas cibernéticas (Dagoumas, 2019).

Existe otra clasificación de tecnología dentro de las empresas en general, que permite realizar la supervisión y control de los ICS, estos sistemas han sido definidos por el National Institute of Standard and Technology de EE. UU. en su NIST SP 800-53 Rev. 4, como:

> Un sistema de información utilizado para controlar los procesos industriales, como la fabricación, la manipulación del producto, la producción y la distribución. Los sistemas de control industrial incluyen sistemas de supervisión y adquisición de datos (SCADA) utilizados para controlar activos geográficamente dispersos, así como sistemas de control distribuido (DCS) y sistemas de control más pequeños que utilizan controladores lógicos programables para controlar procesos localizados. (National Institute of Standar and Technology, pág. 88).

Los sistemas SCADA están compuestas por tres elementos: (1) segmento de red corporativa, que en términos tecnológicos su operación es similar a la de una red corporativa de IT, la cual incluye actividades de administrativas y requiere de conexión a Internet. Por lo que la hace más vulnerable a los ataques tradiciones de las redes de IT, tales como: phishing, inyección SQL, entre otros; (2) segmento de red SCADA, integrado por servidores y estaciones conectados a los dispositivos de campo, lo cual permite el monitoreo y control de variables; y, (3) dispositivos de campo, compuesto por los Controladores Lógicos Programables (PLC por sus siglas en inglés), Unidades Terminales Remotas (RTU por sus siglas en inglés) y Dispositivos Electrónicos Inteligentes (IED por sus siglas en inglés). En este orden, los RTU monitorean los IED y trasmiten la información a los PLC, los cuales

están siendo monitoreados y controlados por la red SCADA (Byres, 2005). A continuación, se describen con mayor detalle los componentes mencionados:

- Unidad Terminal Remota (RTU) ubicadas en las subestaciones o en una parte remota de la planta. El objetivo de las RTU es monitorear los dispositivos de campo y transmitir los datos a una estación central que es monitoreada (Knapp, 2014).

- Unidad Terminal Maestra (MTU) es una unidad centralizada que recolecta datos del RTU y los transmite a una estación central (Knapp, 2014).

- Controladores Lógicos Programables (PLC) son máquinas especializadas, similares a una computadora, que se utilizan para automatizar funciones dentro de una red ICS/SCADA. Están especialmente configurados para entradas y salidas específicas, generalmente desde dispositivos de campo (Knapp, 2014).

- Interfaz Hombre-Máquina (HMI) es un panel de control físico que permite a los administradores de ICS monitorear, cambiar o configurar los ajustes del proceso subyacente (Stouffer K. A., 2011).

- Estaciones de trabajo de supervisión: estas estaciones de trabajo se ejecutan generalmente en sistemas operativos Windows y le brindan al usuario una descripción gráfica del entorno ICS/SCADA (Knapp, 2014).

- Historiadores de datos es un software especializado que almacena los valores y la información recopilados en una base de datos. Estos pueden contener desde frecuencias de motores, temperaturas, pesos o carga (Knapp, 2014).

Además, los protocolos de comunicación empleados por los ICS no se diseñaron teniendo en cuenta la seguridad informática, sino que fueron concebidos como protocolos seriales sin mecanismos integrados de autenticación o cifrado. Lo que expone a estos sistemas a una variedad de ataques cibernéticos, que incluyen el ciberespionaje, alteración de sus sistemas y la manipulación de sesiones. Como sucedió en Ucrania en diciembre de 2015, donde un ataque cibernético afectó directamente al sistema nacional de energía eléctrica, el cual tuvo una duración de aproximadamente 9 horas, en 30 subestaciones de 110 y 35 kV, donde se afectaron a más de 200 mil usuarios. Aun cuando, una infraestructura no se encuentra interconectada se podrían materializar actividades maliciosas. Como es el caso del programa "Stuxnet" que en el año 2010

demostró la posibilidad de una interrupción a un operador asilado de infraestructura crítica (Langner, 2011).

Existen una gran cantidad de regulaciones y recomendaciones publicadas por gobiernos, la academia y organizaciones dedicadas a la protección y aseguramientos de los ICS, los cuales pueden aplicarse directa o indirectamente a estos sistemas. Es importante resaltar que las normas y políticas son requisitos que deben ser cumplidas por las empresas que se encuentran dentro del Estado y que llevan a cabo este tipo de actividad. Los lineamientos y estándares son recomendaciones sobre lo que debe hacerse para mejorar la seguridad en los ICS, y las mejores prácticas son una guía que especifican lo que debe hacerse, de forma ideal, en situaciones particulares (Knowles, 2015).

La dependencia de los servicios vitales de la infraestructura crítica en la automatización de los ICS ha permitido centralizar los esfuerzos de organizaciones gubernamentales y privadas para hacer que el sistema sea lo suficientemente robusto y escalable para llevar a cabo sus operaciones diarias de forma remota y segura. Esta automatización se lleva a cabo no solo protegiendo los dispositivos que integran el sistema de control, sino que también, aquellos dispositivos de red y de ciberseguridad perimetral bajo redes IP integradas, controladores y sistemas SCADA.

En el año 2002, la Sociedad Internacional de Automatización (ISA) comenzó a trabajar en estándares de seguridad llamados Sistemas de Automatización y Control Industrial (IACS), donde incluyó los servicios SCADA que interactuaban con los sistemas de IT. En el 2006, el Departamento de Seguridad Nacional (DHS, por sus siglas en inglés United States Department of Homeland Security) publicó un informe para mitigar las vulnerabilidades encontradas en redes de Sistemas de Control (CS por sus siglas en ingles Control System) y en el 2008, el Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés National Institute of Standards and Technology) implementó el nombre que actualmente se utiliza como Sistemas de Control Industrial (ICS), a través de la NIST 800-82: Guía para la Seguridad del Sistema de Control Industrial (Knowles, 2015). Existen estándares de confiabilidad para identificar y proteger los sistemas eléctricos. Un ejemplo de ello es el conjunto de lineamientos establecidos en la NERC CIP-011-1[23] implementado en los Estados Unidos. Sin embargo, el estándar se ha considera limitado para la aplicación de redes distribuidas de otros países. Otro ejemplo para considerar, son los 21 pasos para mejorar la

[23] United States. Cyber Security — Information Protection. https://www.nerc.com/files/CIP-011-1.pdf

seguridad cibernética de los sistemas SCADA[24], emitidos por el Departamento de Energía de los Estado Unidos, los cuales están divididos en dos categorías. Los primeros 11 pasos tratan sobre la necesidad e implementación del ICS y los siguientes 10 pasos abordan la gestión del ICS (procesos, políticas, lineamientos, entre otros). A diferencia del NERC CIP-011-1, el "21 steps" puede ser aplicado en cualquier industria que utilice para su funcionamiento el sistema SCADA.

Otro estándar desarrollado para la gestión de riesgos de ciberseguridad del subsector eléctrico es el DOE/OE-0003[25] del Departamento de Energía de los Estados Unidos. El proceso comprende 3 niveles especializados: (1) organización y liderazgo; (2) misión y procesos comerciales; y (3) la gestión de sistemas. Las actividades de gestión de riesgos de ciberseguridad se llevan a cabo en todos los niveles y tiene como objetivo principal ejecutar con éxito la misión organizacional y las funciones comerciales a través de procesos de IT. Con el fin de conocer las mejores prácticas en la protección de los sistemas ICS, los cuales integran dispositivos tecnológicos que operan infraestructuras críticas como, por ejemplo: energía, agua, transporte, entre otros, estos componentes son exclusivos para la Tecnología de Operaciones (OT), que difiere de la Tecnología de Información corporativo (IT). Para entender mejor, la diferencia entre las OT y las IT, se contextualizarán a partir de la presentación de algunos de los ataques cibernéticos dirigidos a estos sistemas (OT), entre los que se encuentran los de software malicioso, campañas de intrusión e incidentes cibernéticos

---

[24] United States. Department of Energy. President's Critical Infrastructure Protection Board. 2002. https://www.hsdl.org/?view&did=1826

[25] U.S. Department of Energy. Electricity subsector cybersecurity risk management process. 2012. https://www.energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf

de las ICS más relevantes de los últimos años (Hemsley, 2018), como se puede ver en la tabla 6, a partir de ello encontraremos los elementos comunes que deben ser vigilados, protegidos y atendidos en las OT.

Tabla 6. Cronología de ciberataques a los ICS. Fuente: Elaboración propia a partir de Utility Hack led to security overhaul: Mysterious '08 Turkey Pipe blast Opened New Cyberwar: Closing the Case on the Reported 2008 Russian Cyber Attack on the BTC Pipeline: Homeland Security News Wire: Prepared Testimony and Statemen for the record of: Global Energy Cyberattacks: "Night Dragon".: ICS Advisory (ICSA-11-041-01A): RSA Conference Europe 2012- Duqu, Flame, Gauss: Followers of Stuxnet: Attackers Stole Certificate From Foxconn to hack Kaspersky Whit Duqu 2.0: ICS Joint Security Awareness Report (JSAR-11-312-01): Duque, Flame, Gauss: Followers of Stunxnet: Gauss: Abnormal Distribution: Gas Pipeline Cyber Intrusion Campaign: In cyberattack on Saudi Firm, U.S. Sees Iran Firing Back: ICS Joint Security Awareness Report (JSAR-12-241-01B): Qatari Gas Company Hit Whit Virus In Wave of Attacks on Energy Companies: ICS Alert (ICS-ALERT-14-281-01E): Everything We Know About Ukraine's Power Plant Hack: Analysis of the Cyber Attack on the Ukrainian Power Grid.

Año	Lugar	Descripción
2000	Australia – Servicio de agua	En marzo del 2000, la empresa de servicios de agua de Maroochy Shire en Queensland, Australia, identificó una falla en las comunicaciones enviadas por señales de radiofrecuencia a las estaciones de bombeo de aguas residuales. Estas estaciones estaban configuradas y parametrizadas para generar alarmas a los ingenieros responsables de sus operaciones en caso de que ocurriera una falla o interrupción. Durante las investigaciones se identificó al atacante[26], y el 23 de abril de 2001 la policía persiguió a Vitek Boden, de 49 años, y en su vehículo personal, encontró una computadora portátil y un equipo especializado de Control de

[26] M. Crawford. Utility hack led to security overhaul (2006). Computerworld. https://www.computerworld.com/article/2561484/utility-hack-led-to-security-overhaul.html

Año	Lugar	Descripción
		Supervisión y Adquisición de Datos (SCADA) que había utilizado en el mismo lapso en que ocurrió el incidente en el sistema de "Maroochy Water".
2008	Turquía – Servicio de Oleoducto	La explosión del oleoducto de Turquía en el año 2008 que fue atribuida a un ataque cibernético remoto[27], donde un segmento del oleoducto Baku-Tbilisi-Ceyhan explotó en la ciudad de Refahiye (Turquía). El 14 de diciembre de 2014, Bloomberg[28] publicó una investigación llamada: "La misteriosa explosión del oleoducto de Turquía en el 2008 abrió una nueva guerra cibernética" en donde se centró en cuatro afirmaciones que llevaban a pensar que era un ataque interno. Sin embargo, según las investigaciones posteriores se identificó que fue causada por un ataque físico y no un ataque cibernético como habían afirmado otros investigadores. En un análisis realizado por el equipo SANS ICS[29], divulgó que la explosión del oleoducto de Turquía no fue causada por medios cibernéticos. Según SANS existen una gran cantidad de fallas reportadas y no reportadas en los sistemas ICS y que sin los datos apropiados no se podría apuntar a un culpable, método o medio.
		Stuxnet fue uno de los softwares maliciosos más sofisticados conocidos en ese momento hasta el momento. Este programa maligno infectó las redes del sistema de control de una planta nuclear en Irán. Es por esto, que algunas compañías dedicadas a la seguridad de los sistemas de información de las infraestructuras críticas como el caso de Symantec[30], han hecho una alerta a los Comité de Seguridad Nacional del Senado de algunos Estados, que Stuxnet fue una alerta temprana al real aseguramiento de los

[27] Newswire, Turkish Oil Pipeline explosion may have been Stuxnet precursor (2008). Newswire. http://www.homelandsecuritynewswire.com/dr20141217-2008-turkish-oil-pipeline-explosion-may-have-been-stuxnet-precursor

[28] J. Riley, Mysterious 08 Turkey Pipeline blast opened new cyberwar, Bloomberg. https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar

[29] R. Lee. Closing the case on the reported 2008 Russian cyber-attack on the BTC Pipeline. SANS. https://www.sans.org/blog/closing-the-case-on-the-reported-2008-russian-cyber-attack-on-the-btc-pipeline/

[30] D. Turner, Prepared Testimony and Statement for the Record of Dean Turner (2010). United States Senate Committee on Homeland Security. https://www.hsgac.senate.gov/imo/media/doc/TestimonyTurner20101117REVISED2.pdf

Año	Lugar	Descripción
2010	Irán - Stuxnet	sistemas de infraestructura críticos en todo el mundo. Algunos factores hicieron que Stuxnet fuera un software muy peligroso (auto-replicaba) y que se extendiera a través de múltiples medios y sistemas a través de múltiples medios, tales como (Hemsley, 2018): ▪ *"Unidades extraíbles que aprovechan una vulnerabilidad que permite la ejecución automática"* ▪ *"Redes de área local (LAN) que explotan una vulnerabilidad en Windows Print Spooler".* ▪ *"Server Message Block (SMB) utilizado para proporcionar acceso compartido a archivos, impresoras y otros dispositivos mediante la explotación de una vulnerabilidad en el Servicio de Microsoft Windows Server".* ▪ *"Compartir archivos de red copiándose y ejecutándose a sí mismo".* ▪ *"Servidor de base de datos Siemens WinCC HMI copiándose y ejecutándose a sí mismo".* Stuxnet explotó un total de cuatro (04) vulnerabilidades de Microsoft tipo día cero, de los cuales, dos (02) que eran vulnerabilidades para la auto-replicación y dos (02) que proporcionaron una escalada de vulnerabilidades de privilegios (Hemsley, 2018).
2010	EE. UU. y Países Bajos. Night Dragon	La compañía de ciberseguridad, McAfee, ha llamado "Night Dragon" a los procedimientos especializados y técnicas de ciberataques encubiertos originados en el año 2009 y 2010 a las compañías petroleras, gas y de energía. McAfee[31] afirma que los atacantes en China utilizaron los servidores C2 "Night Dragon" ubicados en los Estados Unidos y los Países Bajos, para realizar estos ciberataques a los sistemas ICS. Este tipo de ataque integró técnicas como: la ingeniería social, spear phishing, explotación de las vulnerabilidades de los sistemas operativos Microsoft Windows y comprometió el directorio activo de Microsoft, así como también, el uso de troyanos de acceso remoto (RATs), con el fin de recopilar datos de los sistemas SCADA. El ICS-

[31] McAfee. Global energy cyberattacks: Night Dragon (2011). McAfee. https://www.heartland.org/_template-assets/documents/publications/29423.pdf

Año	Lugar	Descripción
		CERT[32] de los EE. UU. emitió una alerta en el mes de febrero de 2011 acerca de la amenaza de Night Dragon en las infraestructuras críticas. A través de este ataque se pudo demostrar que, aunque la técnica sea simple o básica, la habilidad de los atacantes puede ser un arma letal para interrumpir los servicios esenciales de las infraestructuras críticas y así comprometer los ICS.
2011	Duqu/ Flame/Gauss	En 2011, el laboratorio de ciberseguridad en Criptografía y Seguridad de Sistemas (CrySyS) ubicado en el Departamento de Telecomunicaciones de la Universidad de Tecnología y Economía de Budapest[33], descubrieron el un software malicioso denominado Duqu durante una investigación a unos registros obtenidos de unos incidentes. Este código fue diseñado para realizar la recopilación de información. Sin embargo, su diseño, estructura interna y mecanismos, detalles de implementación es muy similar al Stuxnet. Como, por ejemplo: falsificó un certificado digital robado de una empresa taiwanesa, tal como lo hizo Stuxnet (de una compañía ubicada en el parque empresarial en Taiwán)[34]. Estos certificados facilitaron la instalación del software malicioso en los sistemas de destino. Symantec y Kaspersky afirmaron que los ejecutables de Duqu es similar al código Stuxnet. Este permite el robo de información, disfrazando las transmisiones de datos como tráfico HTTP normal y agregando datos cifrados para que se filtraran en un archivo .jpg[35]. Sin embargo, este centro de investigación en Hungría (CrySyS) no solo identificó el software maligno Duqu, sino también el programa maligno Flame. Según los investigadores, este es un programa maligno extremadamente complejo

[32] ICS-CERT, Advisory (ICSA-11-041-01A): McAfee Night Dragon report, ICS-CERT. https://www.us-cert.gov/ics/advisories/ICSA-11-041-01A

[33] RSA Conference Europe 2012 – Duqu, Flame, Gauss: Followers of Stuxnet. https://kevinfielder.wordpress.com/2012/10/10/rsa-conference-europe-2012-duqu-flame-gauss-followers-of-stuxnet/

[34] K. Zetter. Attackers stole certificate from Foxconn to hack Kaspersky with Duqu 2.0 (2015). Wired. https://www.wired.com/2015/06/foxconn-hack-kaspersky-duqu-2/

[35] ICS-CERT. Joint Security Awareness Report (JSAR-11-312-01): W32. Duqu-malware. ICS-CERT. https://www.us-cert.gov/ics/jsar/JSAR-11-312-01

Año	Lugar	Descripción
		también diseñado[36] para robar información mediante el uso de: ▪ Micrófonos instalados en los sistemas. ▪ Cámaras web. ▪ Registro de pulsaciones de teclas. ▪ Extracción de datos de geolocalización de imágenes. El laboratorio Kaspersky[37] más tarde identificó otro software al que denominaron: Gauss, el cual está relacionado con Duqu y Flame, ya que todos los 3 usan el mismo marco. Se cree que Gauss obtuvo y recopiló la siguiente información de los sistemas que fueron comprometidos en países como, Líbano, Israel, Territorio Palestino y Estados Unidos: Contraseñas, cookies e historial del navegador al inyectar sus módulos en diferentes navegadores para interceptar las sesiones de los usuarios, detalles de BIOS y CMOS RAM, e información local, de red y de unidad extraíble.
2011	Campaña de ciber-intrusión en gasoductos	El ICS-CERT de los EE. UU., identificó una serie de actividades dirigido a empresas del sector de tuberías de gas natural. El análisis mostró que los intentos de phishing dirigidos a un grupo de personal seleccionadas. El ICS-CERT emitió una alerta (ICSA-12-136-01BP) con respecto a la amenaza, y difundió información relevante de como los ataques se estaban generando y direccionando a organizaciones y agencias del sector crítico, en especial a empresas del sector de gas[38]. Este tipo de intrusión y espionaje permitió que los operadores de infraestructura crítica trabajaran en equipo, compartiendo información clasificada de amenazas e irregularidades en sus operaciones diarias, con el fin de identificar potenciales riesgos dentro de su infraestructura.

[36] B. Boldizsár. Duqu, Flame, Gauss: Followers of Stuxnet (2012). https://el.newoutlook.it/download/book/stuxnet.pdf

[37] Kaspersky Lab. Gauss: Abnormal Distribution. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/20134940/kaspersky-lab-gauss.pdf

[38] ICS-CERT. Gas pipeline cyber intrusion campaign. ICS-CERT Monthly Monitor. https://www.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Apr2012.pdf

Año	Lugar	Descripción
2012	Shamoon – Saudi Aramco and RasGas	En agosto de 2012, la empresa de energía eléctrica más grande del mundo Saudi Aramco, fue atacada en sus sistemas informáticos por un programa maligno altamente destructivo. Este ataque coincidió con la preparación de una de las noches santa del año islam (Lailat al Qadr), lo que permito que los atacantes planearan cuidadosamente sus actividades[39]. Este programa robó y posterior sobrescribió los miles de datos e información de más de 30.000 dispositivos, el cual fue reemplazando con la bandera de los estados unidos. Este software al sobrescribir el registro de arranque (MBR) y las particiones primarias dejaba inutilizables estos dispositivos, las cuales no eran recuperables [40][41]. Sin embargo, el 27 de agosto de 2012, Shamoon afectó su segundo objetivo, una empresa de gas natural ubicada en Qatar llamada RasGas la cual es considerada la más grandes del mundo[42]. No obstante, no se encontraron evidencias contundentes de que este software malicioso haya sido direccionado a los ICS o SCADA de estas dos compañías, sino que al parecer fue un daño colateral.
2013	Represa en Nueva York	Según el Departamento de Justicia de los Estados Unidos, en el año 2013 una pequeña represa cerca de Rye Brook (Nueva York) fue accedida por piratas informáticos[43]. Los atacantes iraníes quienes asumieron la responsabilidad informan que era una prueba para ver a qué podían acceder, ya que no se emplearon técnicas complejas o avanzadas. Los operadores informan que el sistema SCADA estaba en mantenimiento en el momento del ataque, y no era posible controlarlo. Algunas de las hipótesis fue que la represa fue atacada debido a su conexión a Internet, que sin defensa en profundidad la dejo

[39] N. Perlroth. In cyberattack on Saudi firm. U.S. sees Iran firing back. The New York Times (2012). https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html

[40] Symantec. The Shamoon attacks (2011). Symantec. http://www.symantec.com/connect/blogs/shamoon-attacks

[41] ICS-CERT. JSAR-12-241-01B: Shamoon/DistTrack malware. ICS- CERT. https://www.us-cert.gov/ics/jsar/JSAR-12-241-01B

[42] K. Zetter. Qatari gas company hit with virus in wave of attacks on energy companies (2012). Wired. http://www.wired.com/2012/08/hack-attack-strikes-rasgas/

[43] S. Prokupecz, T. Kopan, and S. Moghe. Former official: Irani- ans hacked into New York dam (2015). CNN https://edition.cnn.com/2015/12/21/politics/iranian-hackers-new-york-dam/index.html

Año	Lugar	Descripción
		vulnerable, a esto se suma la falta de controles de seguridad. Debido a que la represa está dentro del grupo de infraestructura crítica, los detalles del ataque o intrusión no fue divulgada.
2014	Molino de acero	En diciembre de 2014, la Oficina Federal de Seguridad de la Información (BSI por sus siglas en alemán) publicó su informe anual de incidentes cibernéticos[44], en este reporte se describe la situación general de amenaza en el ciberespacio, específicamente hace referencia a un ataque contra una acería alemana a través de técnicas de spear phishing e ingeniería social, las cuales permitieron acceso en un inicio a la red administrativa y posterior a la red de producción. Los atacantes causaron múltiples fallas en los sistemas de control individuales, lo que eventualmente impidió que un alto horno pudiera apagarse de manera controlada, lo que resultó en "daños masivos a la planta". Las habilidades técnicas de los atacantes se describieron como "muy avanzadas". Los atacantes conocían no solo la seguridad informática avanzada, sino que también poseían un conocimiento detallado de los ICS y el proceso de producción de acero.
2014	Ucrania BlackEnergy	A finales del año 2014, "The Department of Homeland Security" de los Estados Unidos confirmó que una variante del programa maligno "BlackEnergy" había sido detectado en uno de los sistemas de energía de Ucrania, el cual ocasionó un corte de energía. Por lo que el ICS-CERT[45] lanzó alertas a los propietarios y operadores de infraestructura crítica del sector energía para buscar signos de compromiso dentro de los ICS.
2015	Ucrania Blackout	En diciembre de 2015, se conoció el primer ataque cibernético exitoso en una red eléctrica. Al sistema interconectado nacional de energía eléctrica, donde un ciber ataque deshabilitó por más de 9 horas el servicio eléctrico en 30 subestaciones de 110 y 35 kV, afectando a más de 225 mil usuarios. Aun

[44] BSI. Die Lage der IT-Sicherheit in Deutschland (2014). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

[45] ICS-CERT. Alert (ICS-ALERT-14-281-01E): Ongoing sophisticated malware campaign compromising ICS. ICS-CERT (2014). https://www.us-cert.gov/ics/alerts/ICS-ALERT-14-281-01B

Año	Lugar	Descripción
		cuando, una infraestructura no se encuentra interconectada se podrían materializar actividades maliciosas. El equipo SCADA quedó inactivo y las operaciones regresaron a la normalidad después de una restauración manual del sistema[46]. Según las investigaciones se encontró que se había utilizado el software maligno "BlackEnergy" para explotar algunas vulnerabilidades en los documentos de Microsoft Excel, el cual fue enviado a la red corporativa y ICS a través de correos electrónicos de phishing[47].
2016	Ucrania Blackout	Un año después del primer ataque a la red eléctrica de Ucrania, el 17 de diciembre de 2016 Ucrania sufrió un segundo ciberataque en su red eléctrica, con las mismas características del año anterior, esta vez, la capital quedó sin energía eléctrica durante 3 horas. Los interruptores se dispararon en 30 subestaciones, cortando la electricidad a más de 200,000 clientes. Sin embargo, una de las técnicas usadas para prolongar la interrupción del ICS, los atacantes lanzaron un ataque telefónico de denegación de servicio denominado TDoS contra el centro de atención telefónica de la empresa para evitar que los clientes informaran la interrupción. En esta ocasión los servicios se reestablecieron de manera manual[48].

Con los incidentes descritos anteriormente se puede concluir que algunos de los posibles efectos a los que se puede enfrentar un sistema ICS son:

- Interrupción en las operaciones de los ICS, debido a la afectación en el flujo de información a través de las redes corporativas que traslaparon a los sistemas SCADA y DCS.

---

[46] K. Zetter. Everything we know about Ukraines power plant hack. Wired (2016. https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/

[47] K. Zetter. Inside the cunning, unprecedented hack of Ukraine's power grid. Wired (2016). https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[48] R. Lee, M. Assante, and T. Conway, Analysis of the cyber-attack on the Ukrainian power grid, NERC (2016). https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

- Cambios no autorizados en las instrucciones o alteración en los sistemas de alarma, que ocasionan daño y deshabilitan los dispositivos que supervisan y controlan las operaciones vitales, generando consecuencias negativas para la salud y protección de la vida humana.

- Información errada enviada a los operadores de los SCADA y DCS, para ocasionar una mala toma de decisiones.

- Configuración alterada en los ICS a través de la inyección de software malicioso con el fin de generar efectos negativos.

7.2 Análisis de los estándares, políticas e información académica del sector eléctrico que permita identificar las ventajas y desventajas

Para asegurar el entendiendo de las características y elementos abordados en el análisis realizado en cada uno de los estándares, normas, mejores prácticas, guías y demás publicaciones de la industria privada que están relacionadas con la seguridad y protección de los ICS, es necesario definirlos y clasificarlos según la función y gestión que cumplen y que permita entender su funcionalidad dentro del contexto del análisis.

Características abordadas:

Dentro de este contexto se consideran tres factores o características que impulsan el cambio de las organizaciones y que permiten adaptasen a los nuevos tiempos que buscan una transformación digital, teniendo en cuenta la velocidad a la que los "disruptores" hacen evolucionar el mercado a través de la innovación:

Característica Procesos: Son documentos emitidos para asegurar la ejecución estandarizas y el control de las actividades de los procesos que se gestionan al interior de una organización. Es la representación de cómo deben hacerse las cosas en la organización, los procesos permiten asegurar de que se cumplan los objetivos del negocio y se logren los cambios que se quieren lograr.

Característica Personas: Deberían ser consideradas siempre en conjunto con los procesos, para lograr una solución "holística" son las personas las que harán realidad el cambio y usaran la solución. Las personas son en última instancia, las poseedoras del conocimiento.

Característica Tecnologías: Son los aspectos tecnológicos de la implementación de un proceso con tecnología adecuada.

Lograr el equilibrio de estos factores no es una tarea fácil, las personas, los procesos y las tecnologías son partes interdependientes de un todo, sin embargo, el cambio en unos de estos factores necesariamente causa un efecto sobre las demás, las acciones aisladas deben integrarse adecuadamente y tener un objetivo común, la suma de cada de estos genera una sinergia en la que la entrega final tiene más valor que la suma de cada entrega individualmente.

En este contexto, los procesos no vienen solos, estos generalmente están soportados por sistemas de información o de elementos tecnológicos y necesitan a las personas para que los ejecuten, por consiguiente, las personas tienen que conocer los procesos, tanto para

realizarlos de manera adecuada y ejecutarlos, como para poder mejorarlos de forma continua, del mismo modo, se debe elegir la tecnología adecuada.

Elementos Contenidos:

Los siguientes elementos en una organización hacen parte del sistema de planeación y gestión integrado y balanceado y son parte fundamental para enlazar las estrategias y objetivos lo cual es clave para el desempeño y resultados de una organización, los siguientes elementos son esenciales dentro de la planificación organización ya que determina donde la empresa quiere llegar y como lo hará para lograr el objetivo.

Elementos Estratégicos:

La participación de la alta dirección es relevante donde se evidencia el liderazgo, interés y compromiso, a través de este elemento se permite tener claridad de la planificación de una organización donde se definen y destinan los recursos que se usarán y las políticas a desarrollar para obtener y administrar los recursos. El liderazgo se refiere al compromiso que debe ejercer la dirección de la organización en el cualquier proceso de implementación. El compromiso de la dirección se verifica con la aportación de los recursos tanto humanos como materiales para la consecución de los objetivos.

"A mayor jerarquía mayor exigencia" que demuestre la incorporación de los valores éticos y de compromiso con la seguridad desde el más alto nivel (ISO27001). El elemento estratégico es fundamental, debido a que la alta gerencia tiene que asimilar fuertes y continuos cambios, no solo del entorno, sino también sociales, tecnológicos entre otros. Con

el fin de conseguir los objetivos establecidos en la misión organizacional, la vinculación del elemento estratégico y participación de la alta gerencia se convierten en una parte proactiva, jugando un rol relevante ya que permea de manera clara el liderazgo, compromiso y participación de manera transversal permitiendo el desarrollo e implementación de los lineamientos.

Ahora bien, desde el punto de vista costo beneficio, se puede observar que los elementos estratégicos ayudan a determinar los objetivos a largo plazo de abordaje de intervención de los ICS, así como la adopción de medidas y utilización de los recursos necesarios para lograr esos objetivos. El objetivo principal de la estrategia es asegurar la supervivencia y la prosperidad organizacional a partir de la garantía de continuidad, integridad y disponibilidad en la operación.

Elementos Tácticos:

Este elemento desarrolla detalladamente la planeación del funcionamiento de cada una de las áreas de la organización a partir del marco de referencia elaborado en el nivel estratégico, coordina la utilización de los recursos y su fin principal es la eficiencia, son las acciones para realizar, igualmente especifica las acciones declaradas y asignadas que hacen que los planes de la empresa sean documentadas y reales.

Elementos Operativos:

Es el elemento que describe la asignación de las tareas puntuales que debe realizar cada colaborador de la organización en cada una de las áreas de trabajo y ejecutan

las acciones. Es la guía operativa para la implementación de acciones y mecanismos para la incorporación, apropiación e implementación efectiva.

La alineación de estos elementos debe verse desde una visión holística del desempeño organizacional, el desarrollo de estos crean un verdadero impacto para el negocio, aportando a la eficiencia organizacional, desde la estrategia y la cultura, convirtiéndose en un proceso sistemático, independiente, documentado y conocido por todos, permitiendo mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos y asegurar beneficios económicos. Para ISA INTERCOLOMBIA permite la construcción de redes colaborativas en todas las áreas, a niveles estratégico, táctico y operativo.

7.3 Análisis de los incidentes identificados en los ataques a las ICS vs los estándares

Luego de realizar el estudio de los ataques y sus lecciones aprendidas, estos fueron cruzados con los estándares, ver la tabla 7, para verificar cuál de los estándares podría cubrir en mayor medida este tipo de ciberataques que se presentaron:

Tabla 7. Incidentes vs Estándares. Fuente: Elaboración Propia 2020

No	Estándar	**Interrupción en las operaciones de los ICS, debido a la afectación en el flujo de información a través de las redes corporativas que traslaparon a los sistemas SCADA y DCS.**	**Cambios no autorizados en las instrucciones o alteración en los sistemas de alarma, que ocasionan daño y deshabilitan los dispositivos que supervisan y controlan las operaciones vitales, generando consecuencias negativas para la salud y protección de la vida humana.**	**Información errada enviada a los operadores de los SCADA y DCS, para ocasionar una mala toma de decisiones.**	**Configuración alterada en los ICS a través de la inyección de software malicioso con el fin de generar efectos negativos.**
E1	Guía para la Seguridad de los ICS,SP800-82, NIST	*X*	*X*	*X*	*X*
E2	Controles de seguridad y privacidad para sistemas y organizaciones federales de información. NIST SP 800-53	*X*	*X*	*X*	*X*
E3	Protección de los sistemas de control industrial: recomendaciones para Europa y los Estados miembros (ENISA, 2011)	*X*	*X*	*X*	*X*
E4	Guía de buenas prácticas para el control de procesos y seguridad SCADA – CPNI	*X*	*X*	*X*	*X*
E5	21 pasos para mejorar la seguridad cibernética de las redes SCADA - The U.S. Department of Energy	*X*	*X*	*X*	*X*
E6	Protección Infraestructura Crítica - NERC CIP (001-011)	*X*	*X*	*X*	*X*
E7	Estándar ISA / IEC 62443 para la red industrial y seguridad del sistema	*X*	*X*	*X*	*X*
E8	Gestión de sistemas de energía e intercambio de información asociado - Seguridad de datos y comunicaciones. IEC 62351-4:2018 (Sector Eléctrico)	*X*	*X*	*X*	*X*
E9	Estándar de capacidades de ciber seguridad para dispositivos electrónicos inteligentes. IEEE 1686-2007	*X*	*X*	*X*	*X*
E10	IEEE 1402 Guide for Electric Power Substation Physical and Electronic Security	*X*	*X*	*X*	*X*
E11	OSCE Good Practices Guide on Non-Nuclear Critical Energy	*X*	*X*	*X*	*X*

No	Estándar	Interrupción en las operaciones de los ICS, debido a la afectación en el flujo de información a través de las redes corporativas que traslaparon a los sistemas SCADA y DCS.	Cambios no autorizados en las instrucciones o alteración en los sistemas de alarma, que ocasionan daño y deshabilitan los dispositivos que supervisan y controlan las operaciones vitales, generando consecuencias negativas para la salud y protección de la vida humana.	Información errada enviada a los operadores de los SCADA y DCS, para ocasionar una mala toma de decisiones.	Configuración alterada en los ICS a través de la inyección de software malicioso con el fin de generar efectos negativos.
	Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace				
E12	VGB Guideline R 175	X	X	X	X
E13	U.S. DoE Electricity Subsector Cybersecurity Risk Management Process	X	X	X	X
E14	U.S. DoE Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities	X	X	X	X
E15	ISO/IEC 27001 – Anexo	X	X	X	X
E16	ISO/IEC 27032	X	X	X	X
E17	ISO/IEC 27033	X	X	X	X

En el análisis realizado de los ataques cibernéticos, mostrados en la tabla 7, a los ICS se identificó que cada uno de los estándares tienen aplicabilidad en ellos, y tienen un enfoque basado en riesgo de ciberseguridad al cuál están expuestos los sistemas OT.

En un contexto global, los estándares analizados, se alinean para operar en función de las actividades y controles que se utilizan para protegerlos, permitiendo la aplicación de las mejores prácticas en los ICS, las cuales están basadas en un conjunto de acciones, metodologías, herramientas y técnicas, que han sido probadas con resultados favorables en materia de ciberseguridad.

Los estándares tienen distintos enfoques con un objetivo común que es el de proteger los ICS. Su protección requiere de un enfoque holístico, que considere distintas perspectivas: desde cuestiones tecnológicas, administrativas o físicas, hasta legales y contractuales.

Se puede observar cómo los estándares abordan diversos temas en las operaciones, cambios no autorizados en las instrucciones o alteración en los de los ICS, información errada enviada a los operadores que pueden ocasionar una mala toma de decisiones y por ultimo las configuraciones alterada a través de la inyección de software malicioso con el fin de generar efectos negativos en los ICS, las actividades que establecen los estándares consisten en la aplicación de la mejora continua que se da como resultado de la experiencia de expertos en temas de ciberseguridad, ya que se desarrollan a través de consensos de grupos conformados por representantes de la industria, entidades gubernamentales (ONGs), gobiernos y otras partes interesadas.

Por lo anterior, se puede evidenciar que cualquiera de los estándares aplicados debería cubrir las incidencias de un ciberataque, por lo tanto el criterio para decidir cuál estándar es el más completo a la hora de proteger una ICS no es por su amplitud de cobertura al suceso, en esto orden de ideas, se define en la tabla 8, las características y elementos para definir la completitud de abordaje del estándar con respecto a los ICS.

Según las consideraciones anteriores, las características se dividen en tres variables las cuáles son; personas, procesos y tecnología, estas permiten que una organización desarrolle de manera coordinada y eficiente un marco de trabajo para llevar acabo un conjunto de actividades interrelacionadas entre sí, por otro lado, las variables son el factor fundamental

en la transformación digital que enfrentan las organizaciones, las cuales se adaptan a las necesidades actuales y futuras en cuanto a la adopción de nuevas e innovadoras tecnologías, en la cual las personas juegan un papel fundamental para el desarrollo de una organización, las mismas se encargan de llevar a cabo los procesos que están soportados por las distintas tecnologías, esto determina una relación simbiótica que logra una solución holística.

Dentro de los elementos hay tres niveles de gestión: estratégico, táctico y operativo; los cuales cumplen una serie de tareas que se complementan para asegurar una buena gestión organizacional y tienen propósitos específicos.

Tabla 8. Evaluación de las características y elementos de los estándares. Fuente: Elaboración Propia,2020

No	Estándar	Características abordadas			Elementos contenidos			Total
		Procesos	Personas	Tecnología	Estratégico	Táctico	Operativo	
E1	Guía para la Seguridad de los ICS,SP800-82, NIST	1	1	1		1	1	5
E2	Controles deseguridad y privacidad para sistemas y organizaciones federales de información. NIST SP 800-53	1	1	1	1	1	1	6
E3	Protección de los sistemas de control industrial: recomendaciones para Europa y los Estados miembros (ENISA, 2011)	1	1	1		1	1	5
E4	Guía de buenas prácticas para el control de procesos y seguridad SCADA – CPNI	1	1	1		1	1	5
E5	21 pasos para mejorar la seguridad cibernética de las redes SCADA - The U.S. Department of Energy	1	1	1	1	1	1	6
E6	Protección Infraestructura Crítica - NERC CIP (001-011)	1	1	1		1	1	5
E7	Estándar ISA / IEC 62443 para la red industrial y seguridad del sistema	1	1	1		1	1	5
E8	Gestión de sistemas de energía e intercambio de información asociado -Seguridad de datos y comunicaciones. IEC 62351-4:2018 (Sector Eléctrico)			1		1	1	3
E9	Estándar de capacidades de ciber seguridad para dispositivos electrónicos inteligentes. IEEE 1686-2007			1		1	1	3
E10	IEEE 1402 Guide for Electric Power Substation Physical and Electronic Security			1		1	1	3
E11	OSCE Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from		1	1	1	1	1	5

No	Estándar	Características abordadas			Elementos contenidos			Total
		Procesos	Personas	Tecnología	Estratégico	Táctico	Operativo	
	Terrorist Attacks Focusing on Threats Emanating from Cyberspace							
E12	VGB Guideline R 175			1		1	1	3
E13	U.S. DoE Electricity Subsector Cybersecurity Risk Management Process			1		1	1	3
E14	U.S. DoE Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities	1	1	1		1	1	5
E15	ISO/IEC 27001 – Anexo	1	1	1	1	1	1	6
E16	ISO/IEC 27032	1	1	1		1	1	5
E17	ISO/IEC 27033	1	1	1		1	1	5
	TOTAL	11	12	17	4	17	17	

Encontramos que las características más importantes que se abordan en estos estándares y documentos analizados son las tecnologías, que como se puede observar en la tabla 8, obtiene el mayor número de vinculaciones a los estándares con un total de 17 coincidencias, lo cual tiene sentido, toda vez que son las que soportan, apalancan y permiten el funcionamiento de las ICS.

Como se dijo anteriormente, las tecnologías son las que permiten tener una la gestión de un sistema de control donde se monitorean un conjunto de dispositivos encargados de administrar, ordenar, dirigir o regular el comportamiento de otro sistema, con el fin de reducir las probabilidades de fallo y obtener los resultados deseados. Las tecnologías apalancan el buen funcionamiento de los procesos de los ICS con el objetivo de controlar equipos o máquinas, a través del su uso de la tecnología se logran importantes mejoras, pues automatizan los procesos operativos, suministran una plataforma de información necesaria para la toma de decisiones y, lo más importante, su implantación logra ventajas competitivas en hacer un buen uso de estas.

Al igual que la tecnología, los elementos más abordados y detallados en los estándares analizados es el "Operativo y Táctico", con igual número de coincidencias de 17, lo cual tiene sentido ya que cada uno de ellos tiene una relación donde el elemento operativo contiene una formulación y asignación de actividades a ser desarrolladas y deben ser ejecutadas de los planes enunciados en lo táctico.

En el análisis realizado en el elemento operativo se identificó que estos describen el conjunto de actividades que se llevarán a cabo y por quién para lograr un objetivo. En otras palabras, los elementos operacionales son altamente tácticos, debido a que estos últimos diseñan y describen lo que se debe hacer a través de un proceso documentado.

Componentes de los estándares

Si bien, en el apartado **Análisis de los incidentes identificados en los ataques a las ICS vs los estándares,** se identificaron diversas normas, metodologías y herramientas que tienen un espectro de cobertura amplio, se llegó a la conclusión, a partir de la

, que los estándares con mayor nivel de cobertura de características y elementos para ISA INTERCOLOMBIA son:

- ISO/IEC 27001 – Anexo.

- 21 pasos para mejorar la seguridad cibernética de las redes SCADA - The U.S. Department of Energy.

- Controles de seguridad y privacidad para sistemas y organizaciones federales de información. NIST SP 800-53.

Como se puede observar en la tabla 8, el autor realiza una evaluación de todas las normas que pueden ser parte del proceso de desarrollo para ISA INTERCOLOMBIA, la calificación partió del Informe Integrado de Gestión 2019, el cual en su página 86, identifica la importancia de vincular la NIST como parte de la seguridad cibernética, ver Ilustración 5, igualmente en 2019 se realizó una actualización las tendencias y riesgos emergentes relacionados con el negocio, de los cuales se determinaron los 6 elementos evaluados en la Tabla 8, (características y elementos que ya fueron explicados), por lo anterior, y luego de realizar una calificación con estos criterios, se puede observar que las normas seleccionadas previamente obtuvieron el mayor puntaje, 6 puntos sobre 6, con lo que se observa completitud de los elementos abordados para atender el direccionamiento que la organización entrega para tal fin.

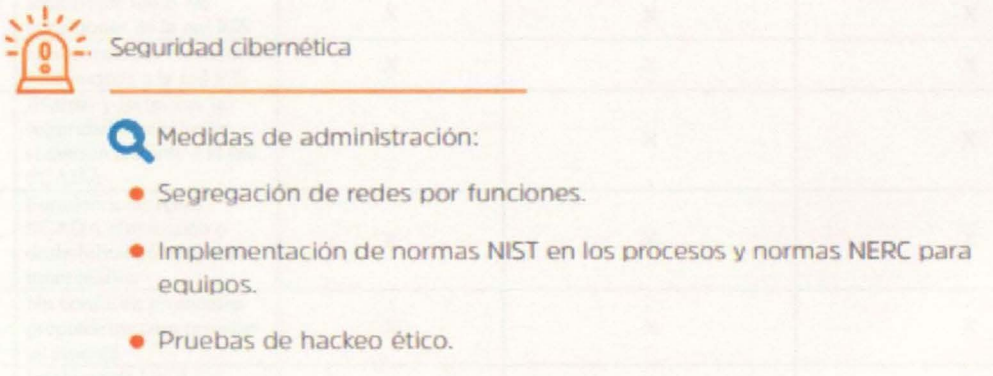

Ilustración 5. Seguridad cibernética, tomado de: Informe integrado de gestión ISA INTERCOLOMBIA

En la Tabla 9, se identificó el cumplimiento de los tres estándares con respecto a los 21 pasos que permiten mejorar la seguridad cibernética, la elección de este estándar como referente inicial se da toda vez que su forma de comprensión, aprehensión y entendimiento del personal técnico de ISA INTERCOLOMBIA SA es mayor con este sistema de verificación, sin embargo, cabe anotar que el autor, realizó un ajuste en dichos pasos para poder lograr dos cosas:

1. No personalizar el nombre de los sistemas a SCADA, toda vez que en un futuro podrían estos cambiar.

2. Ajustar el lenguaje a la operación desarrollada en la empresa.

Tabla 9. Medidas para mejorar la protección de las infraestructuras. Fuente: Elaboración propia adaptado de 21 pasos para mejorar la seguridad cibernética de las redes SCADA (2019)

	Actividades	**ISO/IEC 27001 -** Anexo	**21 pasos para mejorar la seguridad cibernética de las redes SCADA - The U.S. Department of Energy**	**Controles de seguridad y privacidad para sistemas y organizaciones federales de información. NIST SP 800-53**
1	Identifique todas las conexiones de la red ICS	X	X	X
2	Desconecte las conexiones innecesarias a la red ICS	X	X	X
3	Evaluar y fortalecer la seguridad de cualquier conexión restante a la red SCADA	X	X	X
4	Fortalezca las redes SCADA eliminando o deshabilitando servicios innecesarios	X	X	X
5	No confíe en protocolos propietarios para proteger su sistema	X	X	X
6	Implemente las características de seguridad proporcionadas por los proveedores de dispositivos y sistemas	X	X	X
7	Establezca controles sólidos sobre cualquier medio que se utilice como	X	X	X

Actividades		ISO/IEC 27001 - Anexo	21 pasos para mejorar la seguridad cibernética de las redes SCADA - The U.S. Department of Energy	Controles de seguridad y privacidad para sistemas y organizaciones federales de información. NIST SP 800-53
	puerta trasera en la red SCADA			
8	Implemente sistemas de detección de intrusos internos y externos y establezca monitoreo de incidentes las 24 horas del día	X	X	X
9	Realice auditorías técnicas de dispositivos y redes SCADA, y cualquier otra red conectada, para identificar problemas de seguridad.	X	X	X
10	Realice encuestas de seguridad física y evalúe todos los sitios remotos conectados a la red SCADA para evaluar su seguridad	X	X	X
11	Establecer "Equipos rojos" SCADA para identificar y evaluar posibles escenarios de ataque	X	X	X
12	Defina claramente roles, responsabilidades y autoridades de seguridad cibernética para gerentes, administradores de sistemas y usuarios	X	X	X
13	Documente la arquitectura de red e identifique los sistemas que cumplen funciones críticas o contienen información confidencial que requiere niveles adicionales de protección	X	X	X
14	Establecer un proceso riguroso y continuo de gestión de riesgos	X	X	X
15	Establecer una estrategia de protección de red basada en el principio de defensa en profundidad	X	X	X
16	Identifique claramente los requisitos de seguridad cibernética	X	X	X
17	Establecer procesos efectivos de gestión de la configuración	X	X	X
18	Realizar autoevaluaciones de rutina	X	X	X
19	Establecer copias de seguridad del sistema y planes de recuperación ante desastres	X	X	X
20	El liderazgo organizacional superior debe establecer expectativas para el desempeño de seguridad	X	X	X

Actividades		ISO/IEC 27001 - Anexo	21 pasos para mejorar la seguridad cibernética de las redes SCADA - The U.S. Department of Energy	Controles de seguridad y privacidad para sistemas y organizaciones federales de información. NIST SP 800-53
	cibernética y responsabilizar a las personas por su desempeño			
21	Establezca políticas y realice capacitaciones para minimizar la probabilidad de que el personal de la organización divulgue inadvertidamente información confidencial sobre el diseño del sistema SCADA, las operaciones o los controles de seguridad	X	X	X

Se puede identificar, a partir de la Tabla 9, que todos los estándares contienen y abordan de manera completa las características y elementos.

Por lo tanto, podemos definir que estos estándares permiten desarrollar una estrategia mucho más completa y holística para la gestión de los riesgos asociados a la protección de los activos de una organización, garantizando la gestión coordinada en la aplicabilidad de controles de seguridad de forma óptima, escalable e integrable.

Adicionalmente en el análisis se plantean unas características y elementos que componen estos estándares a partir de un enfoque común que podrían resumir en los siguientes puntos:

- Enuncian una la postura actual de ciberseguridad.
- Describen el estado objetivo de ciberseguridad.
- Identificar y priorizar oportunidades de mejora en el contexto de un proceso continuo y repetible.

- Evaluar el progreso hacia el estado objetivo.
- Comunicación entre las partes interesadas internas y externas sobre el riesgo de ciberseguridad.

Por lo tanto, estos estándares consideran condiciones y necesidades propias de cada organización, a través de una adecuada adopción e incorporación, facilitando la implementación de estos de manera racional y consciente, es de aclarar que la incorporación de estos en las organizaciones no puede ser considerados como la solución completa a los problemas que se tengan a nivel de ciberseguridad en los ICS.

La coincidencia mayor en los tres estándares identificados se basa en una metodología clara sobre cómo implementar la seguridad cibernética en una organización, en directrices y prácticas existentes para que las organizaciones de infraestructura crítica gestionen y reduzcan los riesgos de ciberseguridad.

Los estándares deben entenderse y pueden ser utilizados como punto de partida cuando se tiene alguna iniciativa relacionada con la protección de los ICS y recopilan la experiencia y conocimiento de otras personas que posiblemente se enfrentaron a resolver problemáticas similares cuando se plantearon como objetivo la protección de sus activos.

8. Proponer un análisis conceptual de los requerimientos mínimos para definir los lineamientos en el aseguramiento de los sistemas de control industrial caso de estudio: ISA INTERCOLOMBIA

Como se presentó en las limitaciones del presente trabajo, ISA INTERCOLOMBIA identifica el riesgo de ciberseguridad como un factor relevante para ser atendido, sin embargo, por razones de confidencialidad de la organización en el presente trabajo no se puede presentar la matriz de riesgos cibernéticos de la organización, toda vez que el contrato laboral del maestrante impide revelar este tipo de información. Sin embargo, el presente capitulo presenta cuales deberían ser esos requerimientos mínimos para el aseguramiento del ICS.

Como se observó, en los capítulos anteriores, la dependencia de los servicios vitales como son las comunicaciones y navegación aeronáutica, sistema eléctrico, tratamiento de aguas residuales, salud, entre otros, si llegaran a tener una interrupción no deseada afectaría directamente temas como la salud y la seguridad de las vidas humanas, pérdidas financieras, así como también daños graves al medio ambiente (Stouffer K. a., 2011) lo que ha conllevado a centralizar los esfuerzos de organizaciones gubernamentales y privadas para hacer que los sistemas que soportan las infraestructuras sean lo suficientemente robustos, se entiende por robusto aquellos sistemas los cuales tienen la capacidad de mantener sus condiciones esenciales de desempeño pese a recibir perturbaciones o ruidos; y escalable para llevar a cabo sus operaciones diarias de forma remota y segura. Esta automatización se lleva a cabo no solo protegiendo los dispositivos que integran el sistema de control, sino que también,

aquellos dispositivos de red y de ciberseguridad perimetral bajo redes IP integradas, controladores y sistemas SCADA.

La gestión de riesgos es un paso importante para asegurar los ICS y es un término que nace de la necesidad de monitorear y minimizar los riesgos de las principales actividades que se llevan a cabo en estos sistemas e instalaciones. El propósito de este capítulo es: identificar y analizar aquellas actividades de los ICS involucradas en el proceso de gestión que finalice en proponer un análisis conceptual de los requerimientos mínimos para definir los lineamientos en el aseguramiento de los sistemas de control industrial caso de estudio: ISA INTERCOLOMBIA.

En la actualidad, la gestión de los riesgos en las organizaciones ya no es sólo una cuestión de prevención de riesgos laborales o del departamento financiero, es una estrategia global que ayuda en la toma de decisiones estratégicas. La gestión de riesgos ayuda a los operadores a evaluar y mejorar sus prácticas en ciberseguridad, permitiendo conocer a que riegos están expuestos y así proteger cada activo que compone su infraestructura critica.

En términos amplios a partir de la revisión de la literatura analizada como fueron estándares y buenas prácticas entre otros, se tuvo en cuenta también algunos marcos en la gestión de riesgos, con el fin de identificar parámetros que permitan establecer lineamientos clave en la protección de los ICS. La gestión de riesgos es un punto de partida que permite identificar y analizar aquellas actividades involucradas en el proceso de gestión de riegos. Una de las mejores prácticas en la protección de los ICS, es el Modelo de Madurez de Capacidades (CMM por sus siglas en inglés), el cual se describe a continuación.

8.1 Marcos de Modelo de Madurez - Subsector Electricidad

Un modelo de madurez es un conjunto de controles, características, indicadores, y evaluaciones que visualizan la capacidad de una actividad en particular. (Stevens, 2014). El CMM (por su sigla en inglés Capability Maturity Model) puede usarse para describir la madurez de varios procesos de negocios, en otras palabras, para identificar las fortalezas, debilidades y riesgos en los procesos. Él CMM fue creado para el control de los niveles de procesos de software, desde los ad hoc, que consiste en una serie de actividades que no tienen un orden o un ejecutante definido, hasta procesos de software funcionales, sin embargo y debido a su efectividad este modelo ha expandido hacia otros procesos de operacionales, tales como los Sistemas de Control Industrial y SCADA. (Knowles, 2015).

El marco CMM diseña una ruta evolutiva dividida en fases de la madurez del proceso que se está evaluando en la organización. Estos niveles están fundamentados de manera hereditaria, con el fin de que la etapa siguiente obtenga de la etapa anterior las bases necesarias sobre cómo construir la siguiente mejora. Este modelo se encuentra divido en cinco (05) niveles, como se describen en la Tabla 10.

Tabla 10. Modelo de Madurez de Capacidades Elaboración propia a partir de modelo de madurez (CMM). (Paulk, 2002).

Nivel	Enfoque	Característica	Procesos Claves
Inicial	Gente competente y heroica	El éxito depende del esfuerzo individual y la heroicidad.	No aplica
Repetible	Procesos de gestión de proyectos	Se aplica la disciplina y experiencia de procesos anteriores con el fin de obtener	▪ Gestión de requisitos ▪ Planificación de proyectos de software

Nivel	Enfoque	Característica	Procesos Claves
		éxitos y proyectos con aplicaciones similares.	▪ Seguimiento y supervisión de proyectos de software ▪ Gestión de subcontratos de software ▪ Garantía de calidad de software ▪ Gestión de configuración de software
Definido	Procesos de ingeniería y soporte organizacional	Los proyectos deben estar documentados, estandarizados e integrados con el análisis de impacto de negocios a través de una versión aprobada y personalizada de los procesos de la organización.	▪ Enfoque del proceso de organización ▪ Definición del proceso de organización ▪ Programa de capacitación ▪ Gestión de software integrada ▪ Ingeniería de producto de software ▪ Coordinación intergrupal ▪ Revisiones por pares
Gestionado	Producto y calidad del proceso	El proceso de negocios como los productos se gestionan y controlan cuantitativamente.	▪ Gestión cuantitativa de procesos ▪ Gestión de calidad de software
Optimizado	Mejora continua de procesos	La mejora continua del proceso y el uso de tecnologías innovadoras.	▪ Prevención de defectos ▪ Gestión del cambio tecnológico ▪ Gestión del cambio del proceso

Posterior al CMM, el Departamentos de Energía y Defensa de EE. UU., emitió una nueva versión aplicable directamente a la seguridad del ICS denominado: Modelo de Madurez de Capacidad de Ciberseguridad del Subsector de Electricidad (ES-C2M2 por sus siglas en inglés). El cual tiene como propósito medir y mejorar las capacidades de seguridad del sector eléctrico (Stevens, 2014).

El modelo está estructurado en 10 dominios, cada uno de ellos contiene una agrupación de prácticas de ciberseguridad, y cada una de las prácticas se agrupan por objetivos, dentro de cada objetivo, las prácticas son ordenadas por MIL (Maturity Indicator Level, por sus siglas en inglés). Este nuevo modelo establece cuatro niveles de indicador de madurez, de MIL-0 a MIL-3, que se aplican de manera separada a cada dominio (Stevens, 2014). Cada uno de los diez dominios del modelo contiene un conjunto estructurado de prácticas de ciberseguridad y consecuentemente las prácticas están organizadas en objetivos. "*Por ejemplo, el dominio de Gestión de Riesgos puede estar compuesto por tres objetivos: (1) Establecer una estrategia de gestión de riesgos de ciberseguridad; (2) Administrar riesgos de ciberseguridad; y, (3) Prácticas de gestión*" (Stevens, 2014). A continuación, se definen los propósitos de cada uno de los 10 dominios (CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2), 2019).

1. Gestión de riesgos. "*Propósito: establecer, operar y mantener un programa de gestión de riesgos de ciberseguridad empresarial para identificar, analizar y mitigar el riesgo de ciberseguridad para la organización, incluidas sus unidades de negocios, subsidiarias, infraestructura interconectada relacionada y partes interesadas.". Pag.31.*

2. Gestión de activos, cambios y configuración. *"Propósito: Administrar los activos de IT y OT de la organización, incluidos el hardware y el software, y los activos de información proporcionales al riesgo para la infraestructura crítica y los objetivos de la organización". Pag.34.*

3. Gestión de identidad y acceso. *"Propósito: Crear y administrar identidades para entidades a las que se les puede otorgar acceso lógico o físico a los activos de la organización. Controle el acceso a los activos de la organización, de acuerdo con el riesgo para la infraestructura crítica y los objetivos de la organización.". Pag.37.*

4. Gestión de amenazas y vulnerabilidades. *"Propósito: Establecer y mantener planes, procedimientos y tecnologías para detectar, identificar, analizar, administrar y responder a amenazas y vulnerabilidades de ciberseguridad, proporcionales al riesgo para la infraestructura de la organización (por ejemplo, crítica, IT, operativa) y objetivos organizacionales.". Pag.40.*

5. Conciencia situacional. *"Propósito: Establecer y mantener actividades y tecnologías para recopilar, analizar, alarmar, presentar y usar información operativa y de seguridad cibernética, incluyendo información de estado y resumen de los otros dominios del modelo, para establecer conciencia situacional tanto del estado operativo de la organización como del estado de seguridad cibernética.". Pag.43.*

6. Respuesta a eventos e incidentes. *"Propósito: Establecer y mantener planes, procedimientos y tecnologías para detectar, analizar, mitigar, responder y recuperarse de eventos e incidentes de seguridad cibernética, proporcionales al riesgo para la infraestructura crítica y los objetivos organizacionales.". Pag.46.*

7. Gestión cadena de suministro y las dependencias externas. *"Propósito: Establecer y mantener controles para administrar los riesgos de ciberseguridad asociados con servicios y activos que dependen de entidades externas, proporcionales al riesgo para la infraestructura crítica y los objetivos organizacionales.". Pag.49.*

8. Gestión de la fuerza laboral. *"Propósito: Establecer y mantener planes, procedimientos, tecnologías y controles para crear una cultura de ciberseguridad y garantizar la idoneidad y competencia continua del personal, acorde con el riesgo para la infraestructura crítica y los objetivos organizacionales". Pag.52.*

9. Arquitectura de ciberseguridad. *"Propósito: Establecer y mantener la estructura y el comportamiento de los controles, procesos y otros elementos de seguridad cibernética de la organización, en proporción con el riesgo para la infraestructura crítica y los objetivos de la organización". Pag.56.*

10. Gestión del programa de ciberseguridad. *"Propósito: Establecer y mantener un programa de ciberseguridad empresarial que brinde gobernanza, planificación estratégica y patrocinio para las actividades de ciberseguridad de la organización de una manera que alinee los objetivos de ciberseguridad con los objetivos estratégicos de la organización y el riesgo para la infraestructura crítica.". Pag.60.*

Los aspectos más importantes de las MIL durante la aplicación del modelo son (Stevens, 2014):

- Cada dominio debe contener los niveles de madurez que van a ser aplicados, lo cual permite, que en una organización puede estar operando con diferentes MIL en diferentes dominios. Por ejemplo, una organización podría estar operando en MIL-1 en el dominio "Conciencia Situacional", MIL-2 en el dominio "Administración de Personal" y MIL-3 en el dominio "Gestión del Programa de Ciberseguridad".

- Se logra obtener un MIL completo en un dominio, siempre y cuando la organización realice todas las prácticas en ese nivel y en su nivel anterior. Por ejemplo, si la organización manifiesta estar en el MIL-2, se deben haber realizado todas las prácticas de dominio en MIL-0, MIL-1 y MIL-2 inclusive.

- Se recomienda establecer al menos un MIL objetivo para cada dominio, ya que esto permite gestionar una estrategia efectiva para la organización.

- Cada dominio debe basarse en la estrategia de ciberseguridad de la organización y el logro de cada uno de ellos depende directamente de su efectividad. Sin embargo, previo a la implementación de las prácticas y objetivos, la organización debe evaluar los costos-beneficios de implementar un MIL específico, en caso de no ser viable, se recomienda mantener hasta el MIL-1 o el anteriormente implementado.

A continuación, en la Tabla 11, se relacionan los niveles e indicadores de madurez

Tabla 11. Ejemplo de progresión del enfoque de "Gestión del programa ciberseguridad" (Stevens, 2014).

Nivel de Madurez	Descripción
MIL-0	▪ *La organización cuenta personal capacitado en desarrollo de programas de ciberseguridad.*
MIL-1	▪ *La organización cuenta con una estrategia de programa de ciberseguridad.* ▪ *La estrategia se encuentra aprobada por la alta gerencia.*
MIL-2	▪ *La estrategia establece los principales propósitos en las actividades de ciberseguridad.* ▪ *La estrategia define la estructura y organización del programa de ciberseguridad.*
MIL-3	▪ *La estrategia se actualiza para reflejar los cambios comerciales, los cambios en el entorno operativo y los cambios en el perfil de amenaza.*

Es importante entender que los estándares, normas y buenas prácticas analizadas en los capítulos anteriores están vinculados con los niveles de madurez, toda vez que nos permite entender y evaluar a la organización y su estado actual de la ciberseguridad, dando lugar a un amplio abanico de nuevas oportunidades de mejora en todos los procesos de una empresa, y a partir de un análisis y entrega de unos resultados iniciales, donde se describe un camino de mejoramiento evolutivo, los cuales se convierten en un punto de partida permitiendo tomar unas medidas para corregir las debilidades encontradas y llegar al nivel óptimo que se desea, a partir de los estándares analizados, los cuales presentan un esquema organizado, para el desarrollo de un programa completo de ciberseguridad.

A continuación, se describen aquellos estándares que fueron analizados en el objetivo 2 de este trabajo y que se deciden tomar como referencia para definir los lineamientos mínimos que permitan el aseguramiento de los sistemas de control industrial caso de estudio: ISA INTERCOLOMBIA.

Con base en los estándares y mejores prácticas analizados, como fueron los marcos internaciones de gobernanza y de seguridad relacionados con los sistemas de control industrial y de las publicaciones de seguridad del sistema de control industrial en el sector de energía, los cuales están basados en la gestión de riesgos lo cual permite asegurar que se está gestionando un programa de seguridad de una manera útil para las partes interesadas de toda la organización y ayudan a determinar cómo priorizar las actividades de seguridad, los estándares que se derivaron luego del análisis del capítulo 2 en este trabajo son: la familia de las normas ISO27000 entre las que se encuentra IOS27001 y su el Anexo A, los 21 pasos para mejorar la seguridad cibernética de las redes SCADA - The U.S. Department of Energy y la guías publicadas por el NIST de Controles de seguridad y privacidad para sistemas y organizaciones federales de información. NIST SP 800-53.

Con el fin de facilitar la comprensión de los estándares de ciberseguridad, estos se dividieron en dos categorías:

- Un marco de programa: Determina los procesos y pasos y controles a ser incorporados e implementados.
- Un marco de control: Comprende un conjunto de controles a implementar.

Cada uno de los marcos pueden complementarse entre ellos para lograr mejores resultados en el desarrollo de un programa seguridad, de una manera fácil, dentro de un entorno de mejora continua.

8.2 Marcos de Programas

En esta se encuentra la norma ISO 27001, Estándar internacional para Sistemas de Gestión de la Seguridad de la Información. Este estándar especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI), permitiendo el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002. En general la norma se utiliza de manera programática para hacer lo siguiente:

- Evaluar el estado del programa de seguridad general.
- Crear un programa de seguridad completo.
- Medir la madurez y realizar comparaciones de la industria.
- Simplificar las comunicaciones con los líderes de una organización.

La serie ISO 27000 es un referente de seguridad internacional y son las guías de buenas prácticas en seguridad en las que se apoya el estándar de Seguridad ISO27001, la cual involucra los requisitos del sistema de gestión de seguridad de la información y define las áreas de enfoque en la construcción de un programa de seguridad, incluyendo el contexto organizacional, el liderazgo, la planificación, el apoyo, la documentación, la operación, la evaluación del desempeño y la mejora.

8.3 Marcos de Control

En estos se encuentran:

1. La NIST de Controles de seguridad y privacidad para sistemas y organizaciones federales de información. NIST SP 800-53.

2. los 21 pasos para mejorar la seguridad cibernética de las redes SCADA - The U.S. Department of Energy.

Estos estándares y buenas prácticas determinan un conjunto de controles a implementar, y hacen lo siguiente:

- Identifican un conjunto de controles de referencia.
- Evalúan el estado de las capacidades técnicas.
- Priorizan a la implementación de controles.
- Desarrollan una hoja de ruta inicial para el equipo de seguridad.

1. La NIST de Controles de seguridad y privacidad para sistemas y organizaciones federales de información. NIST SP 800-53.

Los controles de seguridad descritos en la NIST SP 800-53, tiene una organización bien definida y estructurada, que facilitan la selección del control de seguridad y de las especificaciones de sus procesos, estos se organizan en 18 familias diferentes, cada familia contiene controles de seguridad relacionados con el tema general de seguridad de la familia y los controles a su vez pueden involucrar aspectos de política, supervisión, procesos,

manuales, acciones de individuos o mecanismos automatizados, implementados por información, sistemas, dispositivos, igualmente los controles se dividen en 3 clases según su impacto: bajo, moderado y alto. El estándar permite proteger la información y los sistemas de información de las organizaciones, proporcionando pautas que permiten seleccionar y especificar los controles de seguridad aplicable a las organizaciones y a cualquier sistema de información que apoyan las funciones misionales y comerciales de las empresas.

El estándar NIST SP 800-53r4 (2013) aborda áreas tales como: computación móvil y en la nube, seguridad de aplicaciones, confiabilidad, garantía y resistencia de los sistemas de información, amenaza interna, cadena de suministro seguridad, y la amenaza persistente avanzada, facilitando un enfoque más holístico de la seguridad de la información, basado en la gestión de riesgo proporcionando a las organizaciones la amplitud y profundidad de los controles de seguridad necesarias para fortalecer fundamentalmente sus sistemas de información y los entornos en los que esos sistemas funcionan, contribuyendo a sistemas que son más resistentes frente a los ataques cibernéticos y otras amenazas cambiantes.

En general, el conjunto de controles de seguridad puede ser adaptados a las necesidades específicas de acuerdo con la misión de la organización, el entorno operativo y las tecnologías utilizadas.

2. Los 21 pasos para mejorar la seguridad cibernética de las redes SCADA, emitidos por el Departamento de Energía de los Estado Unidos.

Los 21 pasos ayudan a cualquier organización a mejorar su seguridad para las redes ICS / SCADA y así evitar el acceso no autorizado a la información contra compromisos que

podrían conducir a un mal funcionamiento o inestabilidad en el sistema. Estos pasos están divididos en dos categorías. Los primeros 11 pasos tratan sobre las acciones específicas para mejorar la implementación del ICS y las siguientes 10 acciones abordan la gestión del sistema de control industrial (procesos, políticas, lineamientos, entre otros). Estos 21 pasos pueden ser aplicados en cualquier industria que utilice para su funcionamiento el sistema SCADA.

Los marcos de control y marcos de programas se pueden usar juntos y apoyarse mutuamente, estos se conectan y complementan entre sí, para ayudar a identificar, proteger, detectar, responder y recuperar, definen un lenguaje común para la gestión del riesgo, garantizando una gestión coordinada de los controles de seguridad de forma óptima, escalable e integrable, ayudando a las organizaciones a preguntarse, ¿Qué estamos haciendo hoy? ¿Cómo lo estamos haciendo? ¿Adónde queremos ir? ¿Cuándo queremos llegar allí?.

Tanto el estándar de la NIST, como los 21 pasos, están completamente alineados con la norma ISO. A medida que se madura un programa de seguridad, se puede elegir uno o más marcos de trabajo de cada categoría para trabajar de manera integrada y mejorar el estado de las actividades de seguridad en general de una organización. A medida que se actualice el programa de seguridad se debe aprovechar tanto el marco de programa como de control para socializar el plan con los líderes técnicos, de operaciones y directivo.

Cada uno de los estándares y marcos analizados parten de una visión muy general de los elementos que deben ser considerados para la implementación de un programa completo de seguridad en una organización, partiendo de elementos muy generales considerados tanto

en la norma ISO, en la guía de las buenas practica y el estándar NIST, hacia una visión más particular enfocada a fin de mejorar la seguridad en estos los sistemas de ICS.

El desarrollo de lineamientos adaptados a las necesidades de los sectores o empresas mejoraría significativamente la gestión de la ciberseguridad. La implementación de lineamientos, estándares o normas es una práctica que continúa teniendo validez para mitigar los riesgos asociados al uso de ciberespacio.

La evaluación de los lineamientos de Ciberseguridad en una empresa del sector eléctrico es un proceso que debe realizarse de manera cíclica y evaluarse a través de herramientas de medición, tales como: los Indicadores Clave de Rendimiento (KPI por sus siglas en inglés, Key Performance Indicators), modelos de madurez de capacidades, auditorias, pruebas de penetración o diagnóstico.

Para el cumplimiento del objetivo general del presente trabajo a través del desarrollo de lineamientos de ciberseguridad para la protección de ICS, los cuales incluyen las redes enrutadas de área amplia SCADA y de los DCS, con el fin de mitigar las amenazas y la creciente conectividad de estos sistemas a los protocolos de internet de las redes corporativas.

A partir de las consideraciones anteriores vamos a precisar la interrelación de los marcos y estándares de referencia junto con los modelos para el caso de ISA INTERCOLOMBIA.

8.4 Lineamientos de Ciberseguridad para la Protección de los ICS.

Empecemos diciendo que el Reporte Integrado de Gestión 2019 del Grupo ISA, del cual es filial ISA INTERCOLOMBIA, dice:

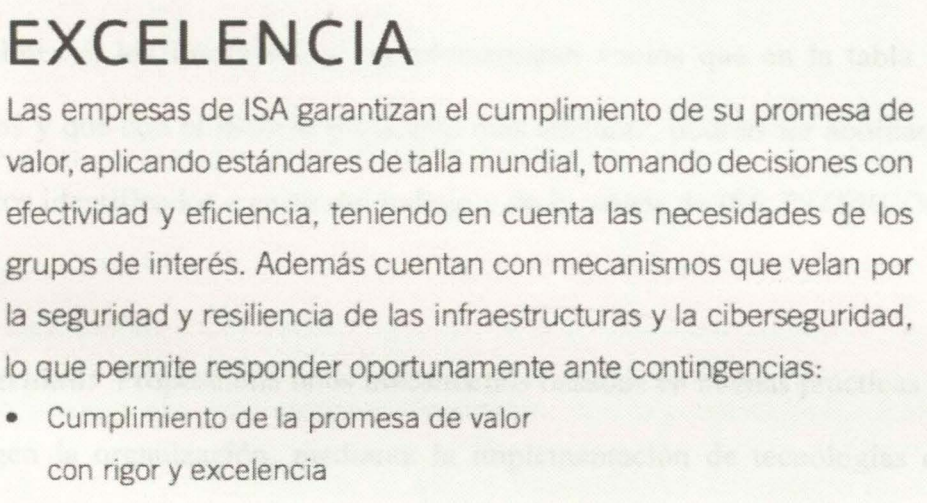

Ilustración 6. Excelencia en Isa, tomado de: Reporte integrado de gestión 2019

Como se puede observar en la Ilustración 6, la ciberseguridad hace parte de la vertical de excelencia, por lo tanto, la organización no solo busca el cumplimiento de las normas, políticas o criterios establecidos en el mercado, sino que debe ir más allá de las mismas.

Sumando a lo anterior se está buscando la recertificación en ISO 27.001 para algunos procesos críticos del negocio de energía eléctrica, la adopción de NIST CSF y la ampliación de la protección de los sistemas de TO (ISA, 2019) y en el mismo informe se pide profundizar, no solo la reconversión tecnológica, sino también el mejoramiento y la revisión de procesos, teniendo presente la realidad cultural, estructural y organizacional de la empresa.

Desde ese punto de vista los lineamientos seleccionados, permiten profundizar, articular, diferenciar y vincular estos elementos de ciberseguridad al entorno organizacional para los años siguientes, llevando las normas anteriormente citadas, un paso más allá del simple cumplimiento.

Finalmente, los lineamientos complementaran vacíos que en la tabla 8 y 9 fueron encontrados y que con el modelo propuesto más adelante, podrán ser abordados los cuatro lineamientos identificados a partir del trabajo y de la matriz de ISA INTERCOLOMBIA los cuales son:

Seguridad: Proporciona unos mecanismos basados en buenas prácticas y actividades que protegen la organización, mediante la implementación de tecnologías que permiten seleccionar medidas físicas y lógicas para la protección de los ICS, además, establecer e implementar políticas y planes de gestión de ciberseguridad.

Defensa: Establece y fortalece de una manera simple y efectiva mecanismos y herramientas para la gestión de identidad y acceso, mediante el entrenamiento y sensibilización de las mejores prácticas en ciberseguridad aplicables específicamente a los ICS, también la implementación y configuración de sistemas de detección de intrusos, antivirus, entre otros.

Aseguramiento: Esta enfocado en la continuidad del negocio permitiendo medir y mitigar los impactos en los ICS en caso de interrupción del servicio, asegurando los sistemas para que los componentes críticos estén en redes redundantes, con el fin de proteger sus activos e información como PLC, RTU, SCADA, considerando algunas técnicas de

mitigación como son el cifrado en las comunicaciones y hashes criptográficos en el almacenamiento de datos.

Monitoreo: Establecer los procesos necesarios para monitoreo y detección de incidente, con el fin de implementar medidas (tecnológicas y procedimentales), como también el monitorio de amenazas y vulnerabilidades.

8.4.1 Caso de Estudio ISA INTERCOLOMBIA

ISA INTERCOLOMBIA, es una empresa de ISA dedicada al transporte de energía eléctrica a alto voltaje en el país, es una empresa de servicios públicos mixta, constituida como sociedad anónima, encargada de administrar, operar y mantener los activos eléctricos propiedad de ISA en Colombia. Es el mayor transportador de energía en Colombia con cubrimiento nacional. Sus redes de transporte de energía se extienden a través de la diversa geografía nacional, aportando al desarrollo y a la competitividad de los colombianos.

Una de las estrategias para las empresas del grupo ISA está encaminada a la transformación digital[49] como se visualiza en la Ilustración 7, con el fin de mitigar los riesgos derivados de la implementación de tecnologías en los procesos industriales.

[49] ISA. Reporte integrado de gestión (2018). http://www.isa.co/es/sala-de-prensa/Documents/nuestra-compania/Reporte%20integrado%202018/última%20versión/Reporte%20Integrado%20ISA%202018.pdf

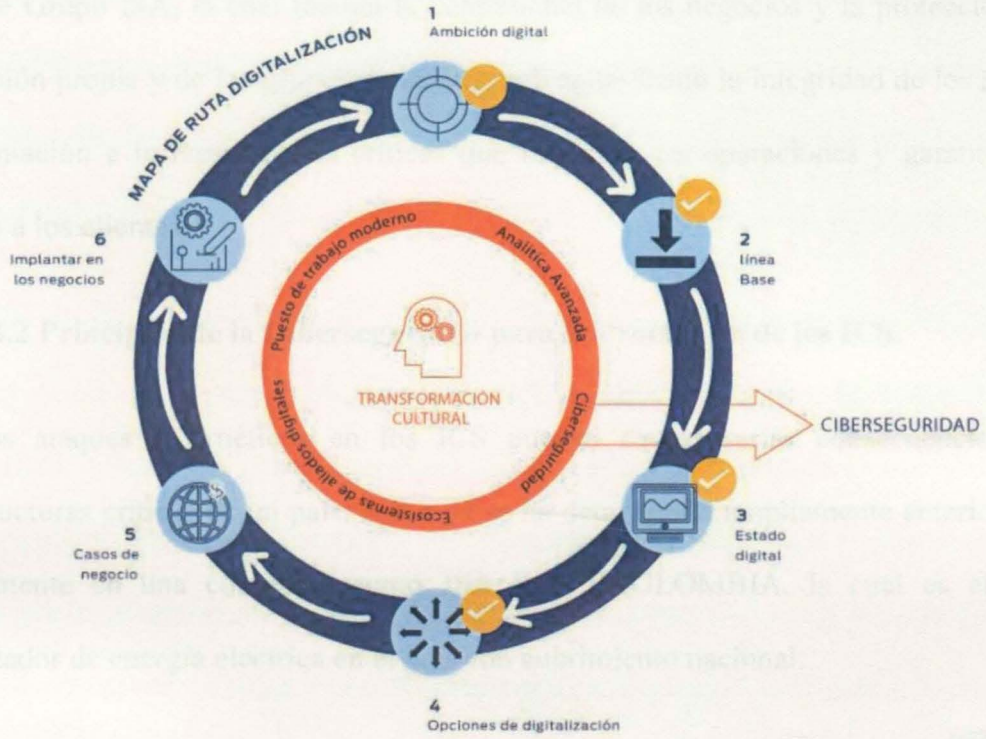

Ilustración 7. Mapa de Transformación Digital ISA INTERCOLOMBIA (2018), adaptado por el autor

ISA realiza una mirada complementaria de los eventos inciertos, generalmente, externos y complejos, que puedan afectar más que la estrategia vigente, los modelos de negocio a futuro. Desde la estrategia de la empresa se abordan algunos riesgos emergentes identificados y analizados, sus posibles impactos en las empresas de ISA INTERCOLOMBIA y las acciones emprendidas para gestionarlos, entre estos se encuentra la Seguridad cibernética. [50]

Es así como en el reporte Integrado de Gestión 2109, ISA INTERCOLOMBIA, reafirma que la ciberseguridad es una dimensión de mayor relevancia en la transformación

[50] ISA. Reporte integrado de gestión (2018). http://www.isa.co/es/sala-de-prensa/Documents/nuestra-compania/Reporte%20integrado%202018/última%20versión/Reporte%20Integrado%20ISA%202018.pdf

digital de Grupo ISA, la cual facilita la continuidad de los negocios y la protección de la información propia y de los grupos de interés; salvaguardando la integridad de los sistemas de información e infraestructuras críticas que impulsan las operaciones y garantizan los servicios a los clientes.[51]

8.4.2 Principios de la Ciberseguridad para la Protección de los ICS.

Los ataques cibernéticos en los ICS pueden causar serias consecuencias a las infraestructuras críticas de un país, como ya se ha demostrado ampliamente anteriormente, especialmente en una compañía como ISA INTERCOLOMBIA, la cual es el mayor transportador de energía eléctrica en el país con cubrimiento nacional.

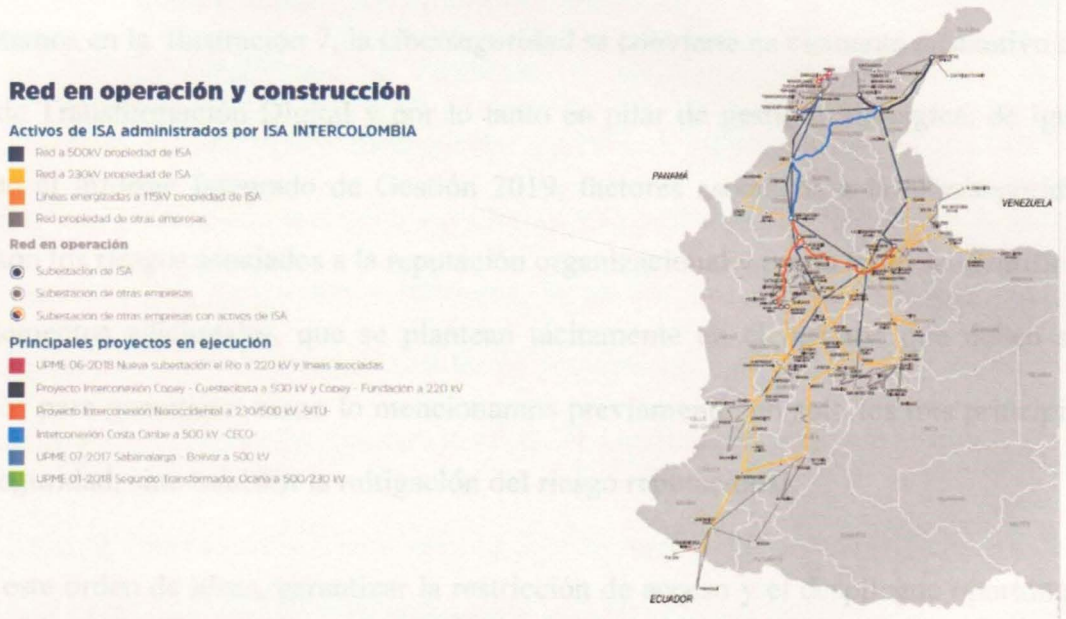

Ilustración 8. Red En Operación y construcción tomado de: Informe de gestión ISA INTERCOLOMBIA 2019

[51] http://www.isa.co/es/sala-de-prensa/Documents/nuestra-compania/informes-empresariales/ReporteIntegrado-ISA2019.pdf

Los efectos de un ataque cibernético se han convertido en una prioridad en la investigación que realizan los diferentes grupos de la empresa que velan por la seguridad de los servicios vitales de la sociedad colombiana, con el fin de mantener la tolerancia y la robustez del sistema de control y así evitar y mitigar las consecuencias de un posible ataque.

Los principales objetivos de ciberseguridad para la protección de los ICS deben responder de manera general a los principios de CONFIDENCIALIDAD, INTEGRIDAD y DISPONIBILIDAD, tal y como ya se ha discutido y presentado anteriormente, sin embargo para ISA INTERCOLOMBIA se deben presentar elementos adicionales a estos principios de modo tal que se garantice el servicio, toda vez que una vulnerabilidad al Sistema Energético Nacional puede poner en peligro las infraestructuras críticas en el país, debido a ello y como lo presentamos en la Ilustración 7, la ciberseguridad se convierte en elemento sustantivo del proceso de Transformación Digital y por lo tanto en pilar de gestión estratégica, de igual manera en el Informe Integrado de Gestión 2019, factores asociados a la ciberseguridad también son los riesgos asociados a la reputación organizacional y por lo tanto se identifican cuatro elementos adicionales, que se plantean tácitamente en el informe que deben ser observados para garantizar, como lo mencionamos previamente, no solo los tres principios de ciberseguridad, sino también la mitigación del riesgo reputacional.

En este orden de ideas, garantizar la restricción de acceso y el despliegue oportuno a partir de planes construidos revisten de especial importancia que debe ser atendida para la continuidad y la sostenibilidad del negocio, tal como lo anota el Informe Integrado de Gestión 2019 en su página 44, por lo anterior los cuatro elementos constitutivos que aportan a esta apuesta organizacional desde los ICS son:

- Restricción del acceso físico a los centros de los ICS: Mediante la implementación de tecnologías que permitan activar controles y sensores de acceso físicos (biométricos, sistemas de reconcomiendo facial, entre otros) es una de las medidas más efectivas de restricción de acceso no autorizado a los centros donde operan los sistemas ICS.

- Restricción de acceso lógico a la red ICS: a través de la implementación de una topología de red que establezca capas físicas y lógicas en los procesos más críticos, la cual podría incluir una zona desmilitarizada (DMZ) con sistemas de detección de intrusos y dispositivos de seguridad de red (Firewall) y así prevenir que el tráfico no inspeccionado de las redes corporativas llegue hasta los sistemas ICS.

- Protección contra la explotación de vulnerabilidades en los ICS: para evitar la explotación de vulnerabilidades ya existentes o día cero, los responsables de la ciberseguridad de las OT deben implementar parches de actualización en los sistemas operativos y sus aplicaciones, una vez que ya hayan sido probadas en condiciones de campo. La inactivación lógica de puertos y servicios, la realización periódica de auditorías de seguridad bajo un matriz de riesgos establecida previamente y así como de privilegios de acceso superior a los del usuario, limitará los tipos de ciberataques contra la red ICS.

- Planes de ciberseguridad: Esto implica diseñar unas políticas claras y contundentes de ciberseguridad para que los ICS funcionen de acuerdo con los diferentes escenarios probabilísticos establecidos, incluso en condiciones adversas. Este también deberá incluir políticas de resiliencia en áreas específicas externos a los centros de control, con el fin de evitar que una interrupción en una red corporativa genere interrupciones en las redes ICS,

como un evento en cascada. Sin embargo, una característica importante de una buena estrategia de ciberseguridad es la rapidez con la que se puede recuperar un sistema después de un incidente.

A partir de la recolección y análisis de la información de los estándares y mejores prácticas analizados en los capítulos anteriores, como los marcos internaciones de gobernanza y de seguridad relacionados con los sistemas de control industrial y de las publicaciones de seguridad del sistema de control industrial, los estándares que se tomaron con referencia para desarrollar los lineamientos fueron:

- La familia de las normas ISO27000 entre las que se encuentra IOS27001 y su Anexo A.
- Los los 21 pasos para mejorar la seguridad cibernética de las redes SCADA - The U.S. Department of Energy.
- Las guías publicadas por el NIST de Controles de seguridad y privacidad para sistemas y organizaciones federales de información. NIST SP 800-53.

A partir de los anteriores estándares y buenas prácticas se propone un modelo que contiene los requerimientos mínimos para definir los lineamientos en el aseguramiento de los sistemas de control industrial caso de estudio: ISA INTERCOLOMBIA.

Como se vio anteriormente los lineamientos son una tendencia, una dirección o un rasgo característico que busca desarrollar en la organización la posibilidad de profundizar los elementos necesarios para llevar a otra dimensión y profundidad el cumplimiento normativo,

por lo anterior dentro de la constante búsqueda de ISA INTERCOLOMBIA por encontrar herramientas para no solo evaluar su desempeño y estructurar su mejoramiento se encontró que los lineamientos entregan una oportunidad que permite elevar y mejorar el nivel de madurez organizacional, sobre todo en la dimensión de procesos que impacta transversalmente las evaluaciones y elementos propuestos en el nivel de madurez (entendido como el conjunto de buenas prácticas, herramientas de medición, criterios de análisis, entre otros), con lo cual se permitirá identificar las capacidades instaladas en dirección de proyectos en la organización, compararlas con estándares identificar fortalezas y debilidades.

Por lo anterior, los lineamientos presentados en este trabajo conectan y aportan al nivel de madurez de ISA INTERCOLOMBIA en la dirección que apoyan no solo la organización del trabajo interno en la empresa, sino que también ayudan a madurar la estrategia de ciberseguridad planteada por la empresa.

8.4.3 Modelo de Madurez de la capacidad de Ciberseguridad para la Protección de los ICS. Caso de estudio ISA INTERCOLOMBIA.

La protección de los ICS se puede obtener en el cumplimiento transversal de los lineamientos identificados en el apartado 8.4, para materializar estos lineamientos la organización definió su vinculación a partir de un modelo de madurez de la capacidad de protección, como se ilustra en la Tabla 12: (1) Seguridad; (2) Defensa; (3) Aseguramiento; y, (4) Monitoreo. Este modelo convierte los lineamientos en niveles contenidos en áreas de aplicación y las cuales están soportadas en unos factores de riesgo que son utilizados como indicador potencial para la confiabilidad y logro del nivel de protección en la organización.

El modelo de madurez de la capacidad de ciberseguridad para los ICS exige diseñar una ruta evolutiva según el nivel de madurez de cada capacidad dividida en los cuatros niveles de madurez de la capacidad de la organización mencionada en el párrafo anterior. Estos niveles no requieren del cumplimiento estricto de una etapa previa para construir la siguiente capacidad, es decir, todos los niveles pueden ser implementados de manera paralela y evolutiva en el tiempo. Por ejemplo, mientras se fortalece el nivel de protección de "Defensa", se puede ir trabajando en el nivel "Monitoreo".

Tabla 12. Modelo de Madurez de la Capacidad (Fuente: Elaboración propia, 2020).

Capacidades		**Niveles de indicador de madurez**			
		MIL-0	**MIL-1**	**MIL-2**	**MIL-3**
Seguridad	Seguridad Lógica	0	1	2	3
	Seguridad Física	0	1	2	3
	Planes de Ciberseguridad	0	1	2	3
Defensa	Gestión de Identidad y acceso	0	1	2	3
	Conciencia situacional	0	1	2	3
	Repuestas a incidentes	0	1	2	3
Aseguramiento	Aseguramiento en la continuidad del sector eléctrico	0	1	2	3
	Sistemas instrumentados de aseguramiento	0	1	2	3
Monitoreo	Monitoreo y detección de incidentes	0	1	2	3
	Monitoreo de amenazas y vulnerabilidades	0	1	2	3
Total Madurez		0	10	20	30

Para definir la estructura de valoración y peso de las diferentes capacidades, se definió el uso de una escala nominal donde cada estado, que para nuestro caso se denomina MIL,

toma cuatro valores que van desde cero (0) hasta (3), siendo cero el nivel más bajo de madurez de la capacidad y su factor y tres el mayor nivel de madurez del factor. Ahora bien, para la identificación de estos valores se presenta el desarrollo del concepto de escala de Likert, ya que la distancia sicológica que tenemos entre las diversas escalas es igual para el calificador, lo que está validado estadísticamente.

De esta forma, una organización puede obtener como puntaje mínimo cero, si todas las dimensiones tomaran el valor de cero y como valor máximo 30, si todas las variables tomaran el valor de tres tal como se puede observar en la Tabla 12.

El primer nivel de protección denominado "**Madurez de la Capacidad de Seguridad**", comprende tres grandes áreas: (1) seguridad lógica, la cual incluye la separación de las redes corporativas y operativas y la administración de parches de actualización y seguridad; (2) seguridad física, cual hace referencia a la protección perimetral de la organización y administración de control de acceso físico; y, (3) planes de ciberseguridad, que denota la capacidad de documentación en incidentes y políticas de ciberseguridad emitidas al interior de la organización. Como se ilustra en las ilustraciones 9, 10 y 11.

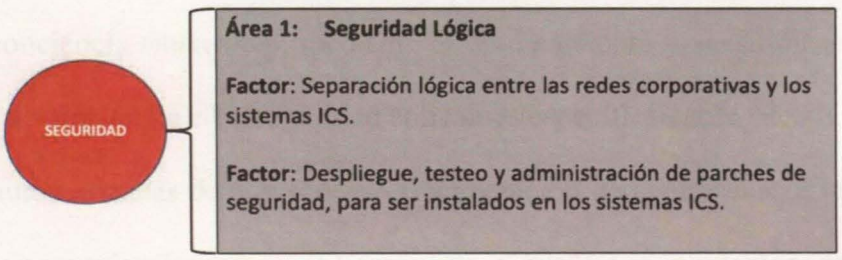

Ilustración 9. Madurez de la Capacidad de Seguridad, Área Seguridad Lógica.

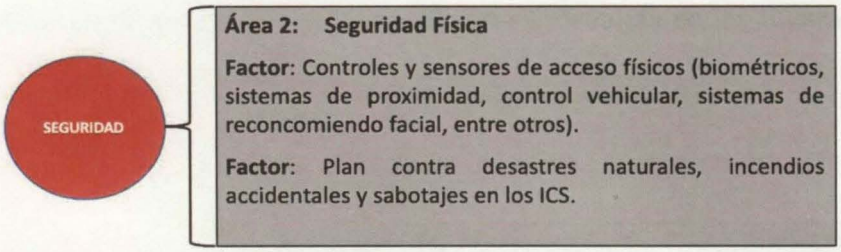

Ilustración 10. Madurez de la Capacidad de Seguridad, Área Seguridad Física

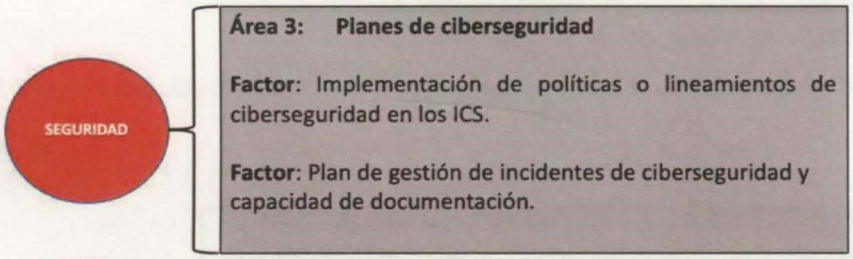

Ilustración 11. Madurez de la Capacidad de Seguridad, Área Planes de Ciberseguridad.

La siguiente capacidad denominada "**Madurez de la Capacidad de Defensa**", comprende tres áreas consecutivas al primer nivel: (4) gestión de identidad y acceso, la cual incluye gestión de usuarios, recursos y políticas bajo la coordinación de los departamentos de IT, OT y recursos humanos, con el fin de establecer el uso de mecanismos y credenciales de autenticación, autorización y acceso basado en roles de los usuarios a la red ICS y la red corporativa; (5) conciencia situacional, mediante el entrenamiento y sensibilización de las mejores prácticas de higiene de ciberseguridad aplicables específicamente a los ICS y el uso de herramientas automatizadas de autoservicio (recuperación de contraseñas e intercambio de información y comunicaciones); y, (6) respuesta a eventos e incidentes, mediante la implementación y configuración de sistemas de detección de intrusos, antivirus, software de verificación de integridad de archivos, entre otros, de acuerdo con el nivel de amenaza y

exposición del sistema ante riesgos cibernéticos. Como se visualiza en las ilustraciones 12, 13 y 14.

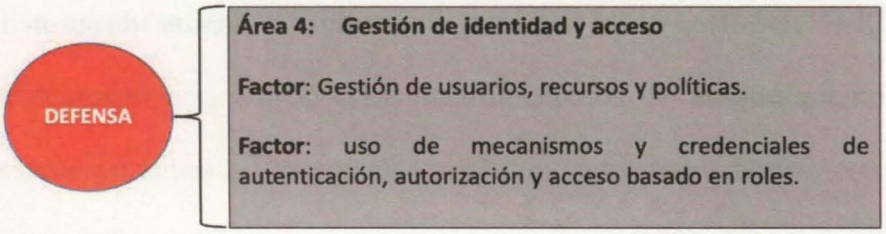

Ilustración 12. Madurez de la Capacidad de Defensa, Área Gestión de Identidad y Acceso

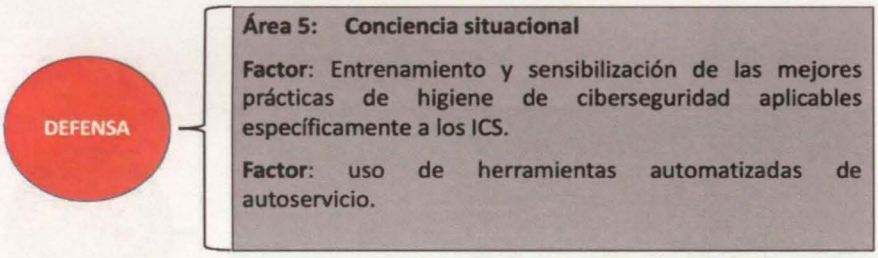

Ilustración 13. Madurez de la Capacidad de Defensa, Área Conciencia Situacional.

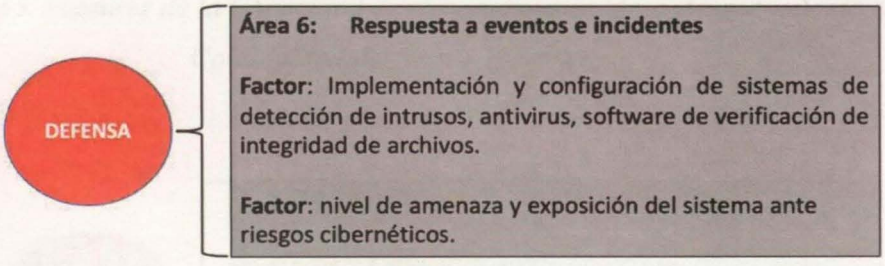

Ilustración 14. Madurez de la Capacidad de Defensa, Área Respuesta a Eventos e Incidentes.

La siguiente capacidad denominada "**Madurez de la Capacidad de Aseguramiento**", comprende dos áreas consecutivas al primer y segundo nivel: (7) aseguramiento en la

continuidad del sector eléctrico, el cual incluye características particulares de los ICS, que van desde el diseño, adquisición, instalación y mantenimiento de los sistemas de control, elementos redundantes y arquitecturas de alta disponibilidad de los activos utilizados en la automatización. Este aseguramiento permite medir y mitigar los impactos en los ICS en caso de interrupción del servicio; y, (8) sistemas instrumentados de aseguramiento, permite establecer que los componentes críticos sean y estén en redes redundantes, con el fin de proteger sus activos e información en los sistemas como PLC, RTU, SCADA, entre otros., algunas de las principales técnicas de mitigación son el cifrado en las comunicaciones y hashes criptográficos en el almacenamiento de datos. Como se ilustra en las ilustraciones 15 y 16.

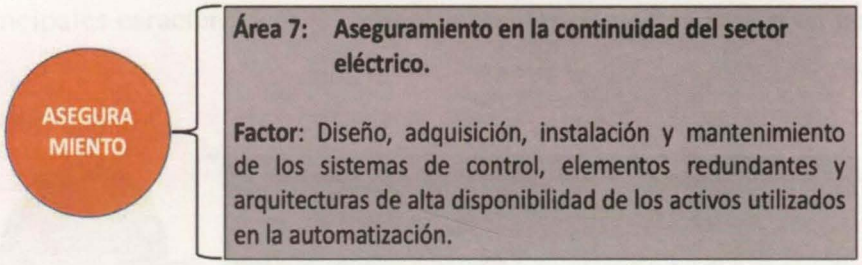

Ilustración 15. Madurez de la Capacidad de Aseguramiento, Área Aseguramiento en la Continuidad del Sector Eléctrico

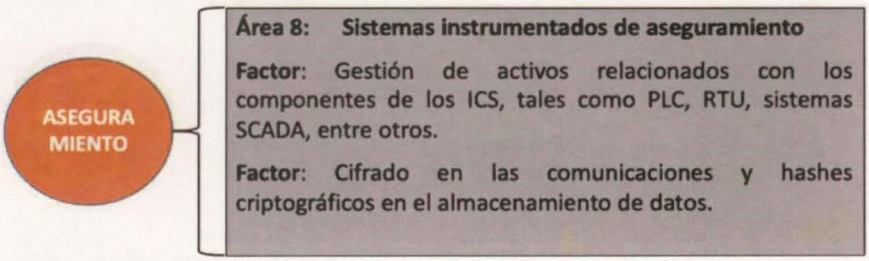

Ilustración 16. Madurez de la Capacidad de Aseguramiento, Área Sistemas Instrumentados de Aseguramiento

La última capacidad denominada "**Madurez de la Capacidad de Monitoreo**" indica que: aunque la organización en esta capacidad ya cuenta con todos los niveles de protección establecidos y una cultura sólida de disponibilidad de las operaciones en sus centros de control, cada sistema tiene sus propios riesgos dependiendo de su ubicación geográfica y regulaciones estatales, que deben analizarse de manera aislada, lo que ratifica que no existe un sistema 100% seguro. Este nivel contiene 2 áreas: (9) monitoreo y detección de incidente, con el fin de implementar medidas (tecnológicas y procedimentales) efectivas para limitar el impacto de un incidente de ciberseguridad en los ICS; y, (10) monitoreo de amenazas y vulnerabilidades, integrado por herramientas y procesos particulares durante los reportes de los sistemas de detección de intrusos y el análisis forense de incidentes cibernéticos para identificar las principales características y comportamientos. Como se ilustra en las gráficas 17 y 18.

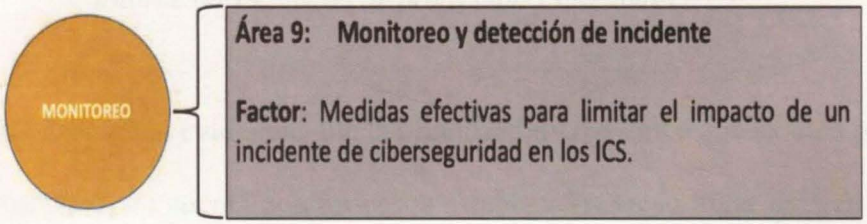

Ilustración 17. Madurez de la Capacidad de Monitoreo, Área Monitoreo y Detección de Incidentes

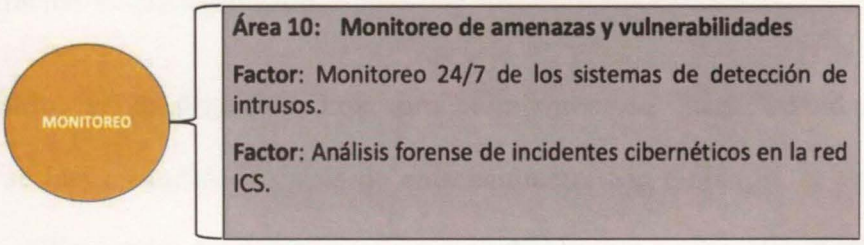

Ilustración 18. Madurez de la Capacidad de Monitoreo, Área Monitoreo de Amenazas y Vulnerabilidades

Una vez la organización le ha dado una valoración a cada factor se puede establecer el nivel de madurez para la protección de los ICS, los niveles de madurez se clasifican según la Ilustración 19.

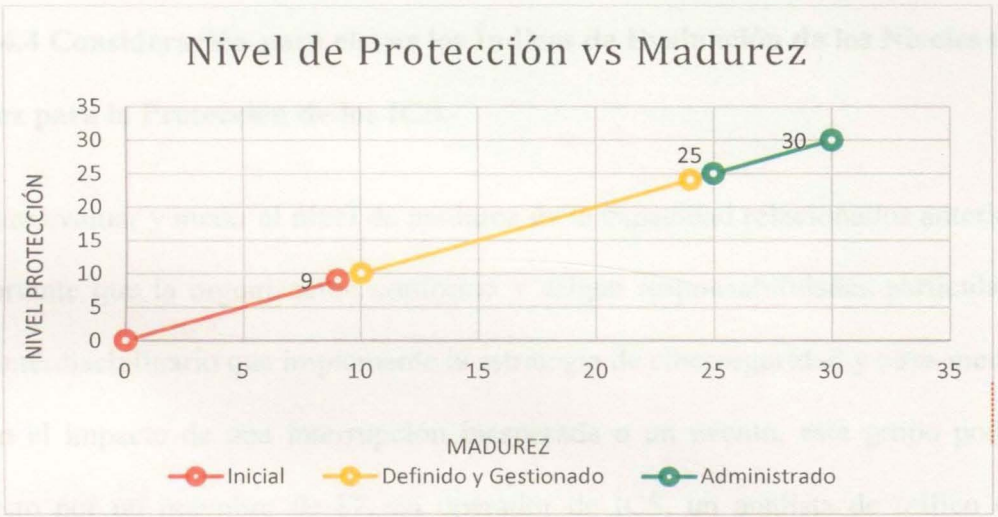

Ilustración 19. Nivel de protección Vs Madurez

- **Inicial:** Este nivel evidencia que la organización reconoce que existen problemas y requieren ser resueltos; no cuenta con procesos establecidos en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

- **Definido y gestionado:** Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados, pero formalizan las prácticas existentes.

- **Administrado:** Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

8.4.4 Consideración para elevar los Índices de Evaluación de los Niveles de Madurez para la Protección de los ICS.

Para evaluar y medir el nivel de madurez de la capacidad relacionados anteriormente, es importante que la organización conforme y asigne responsabilidades particulares a un equipo interdisciplinario que implemente la estrategia de ciberseguridad y otras medidas que mitiguen el impacto de una interrupción inesperada o un evento, este grupo podría estar compuesto por un miembro de IT, un operador de ICS, un analista de tráfico de red o integrador del sistema, el oficial de seguridad de la información (CISO), un representante de la alta gerencia y un miembro del departamento de seguridad física (Stouffer K. a., 2011). La gestión y despliegue debe estar enfocada a la protección de los ICS, a través de un proceso continuo de seis (06) pasos, los cuales fueron adaptados especialmente para este trabajo de los procesos establecidos por (ANSSI, 2014) (Klaver, 2011) (Knowles, 2015), como se ve en la Ilustración 20.

Ilustración 20. Pasos de los Índices de Evaluación de la Capacidad de los ICS (Autoría Propia)

- Paso 1. Conciencia de seguridad cibernética: Algunos de los incidentes descritos en el capítulo 2 están vinculados a la ausencia de conciencia de seguridad cibernética del usuario sobre los riesgos, amenazas y vulnerabilidades asociados con un sistema ICS. Promover la sensibilización y mejores prácticas de higiene de ciberseguridad ayudará a minimizar el riesgo y a cerrar algunas las brechas de oportunidad de ataques.

- Paso 2. Gestión de activos y análisis de riesgos: Para la implementación del modelo de madurez de capacidades uno de los prerrequisitos es el inventario de ciber activos de las plantas físicas, centros y sistemas de control y supervisión, el cual permitirá determinar un análisis de riesgos más preciso a la situación actual de la organización, a través de niveles de criticidad, mapeo de elementos, impactos en caso de interrupción del servicio, entre otros.

- Paso 3. Protección de la información: Consiste en proteger los datos que son almacenados, transmitidos y procesados en los sistemas ICS mediante una serie de barreras tecnológicas de forma sucesivas, con el fin de ofrecer una protección adicional contra aquellas vulnerabilidades que aún no se conocen y así reducir el perímetro del blanco donde puede dirigirse una amenaza en particular.

- Paso 4. Plan de recuperación ante desastres y planes de continuidad comercial: deben estar enfocados exclusivamente a los ICS, mediante la identificación de medios y procesos particulares de cada componente, con el fin de regresar a un estado normal de funcionamiento, incluyendo incidentes ocasionados por ciberataques, desastres naturales y sabotajes.

- Paso 5. Reporte de incidente: El reporte de incidentes en tiempo real permite a la organización el ahorro de esfuerzos adicionales (tiempo, presupuesto y recurso humano). Este debe ser transversal y transparente a los procesos operativos de los ICS, con el fin de no interrumpir su normal funcionamiento. Si el incidente es detectado en el primer lapso tolerable, la organización puede implementar medidas efectivas para limitar su impacto como, por ejemplo, aislar dispositivos y sistemas con procesos e información sensible.

- Paso 6. Auditoría de la idoneidad de los controles del sistema: Este paso incluye el cumplimiento de las políticas y estrategias de ciberseguridad en cada uno de los ciberactivos y procedimientos establecidos en la organización, con el fin de evitar y prevenir cualquier riesgo de seguridad como, por ejemplo: la fuga de información o que cualquier evento externo no autorizado tenga interacción con los ICS.

Se logra obtener un nivel de capacidad específico, siempre y cuando la organización cumpla con todos los seis pasos del índice de evaluación en ese nivel, de lo contrario su nivel de madurez de capacidad estará condicionado por el número del paso que alcanzó en ese nivel. Por ejemplo, si la compañía manifiesta tener un nivel de "Madurez de la Capacidad de Seguridad + **6**" y al mismo tiempo manifiesta que se encuentra en "Madurez de la Capacidad de Defensa **+2**". El modelo de madurez de esta compañía se interpreta como: ISA INTERCOLOMBIA se encuentra en un modelo de madurez de la capacidad de seguridad en un 100% (alcanzó los seis pasos del índice de evaluación +6) y en la capacidad de defensa en un 33.3% al cumplir únicamente con los 2 primeros pasos del índice de evaluación de la capacidad en este nivel.

Otro caso podría interpretarse como, la compañía aplicó el índice de evaluación únicamente al nivel de "Madurez de la Capacidad de Seguridad", el cual está integrado por tres áreas: (1) seguridad lógica; (2) seguridad física; y, (3) planes de ciberseguridad. En este caso, logró obtener en el área "Seguridad Lógica **+6**", "Seguridad Física **+4**" y "Planes de Ciberseguridad **+5**". El resultado de este nivel de madurez se interpreta como: ISA INTERCOLOMBIA cuenta con un nivel de "Madurez de la Capacidad de Seguridad **+4**" el cual representa el índice de evaluación más bajo alcanzado en sus tres áreas. Lo que obliga a las compañías a mantener una homogeneidad en cada una de las áreas asignadas al nivel de madurez de la capacidad. Sin embargo, los pasos de los índices de evaluación pueden ser adaptados, cambiados o reorganizados de acuerdo con las características propias de cada uno los operadores de la infraestructura crítica del sector, con base en su estrategia de ciberseguridad o políticas establecidas.

9. Conclusiones

Este trabajo dio cumplimiento a los objetivos propuestos, al ofrecer de manera estructural los lineamientos de ciberseguridad para mejorar la protección de los ICS, el cual ofrecen la oportunidad de incrementar la madurez de los siguientes cuatro lineamientos (1) Seguridad; (2) Defensa; (3) Aseguramiento; y, (4) Monitoreo. Y para de definir la valoración y peso de las diferentes capacidades, se presentó una escala nominal basada en Nivel indicador de madurez MIL, donde se toman cuatro valores que van desde cero (0) hasta (3), siendo cero el nivel más bajo de madurez de la capacidad y su factor y tres el mayor nivel de madurez del factor. Esta propuesta se desarrolló mediante un diseño de escala de Likert de esta forma, una organización puede obtener como puntaje mínimo cero, si todas las dimensiones tomaran el valor de cero y como valor máximo 30. Esta propuesta se desarrolló mediante un diseño pasivo para no ser intrusivo en las operaciones que se llevan a cabo en los sistemas.

El capítulo 6 da respuesta al objetivo No. 1 donde se identificaron los marcos, guías estándares, buenas prácticas y herramientas a nivel Nacional e Internacional, aplicadas en el aseguramiento de los sistemas de control industrial, además, se identificó que al momento de implementarse las medidas de seguridad a partir de los marcos de trabajo analizados deben ser utilizados como referencia y no como una solución final, también que todos parten de un enfoque basado en gestión de riegos, estableciendo requisitos y medidas de control para el resguardo de la seguridad cibernética, la adopción de estos parte de la importancia de tener

una visión amplia de un sistema de ciberseguridad completo para ser implantados a todos los niveles organizacionales.

En el análisis de los estándares, políticas e información aplicada al sector eléctrico se identificaron las ventajas y desventajas de las mejores prácticas en los sistemas de control industrial, el cual partió de una metodología que consiste en el análisis de los incidentes identificados en los ataques a los sistemas de control industrial y sus lecciones aprendidas, las cuales fueron cruzadas con los estándares identificados en el objetivo No. 1, desarrollado en capítulo 6 de este trabajo. Esta metodología de cómo implementar la seguridad cibernética en una organización, a partir de directrices y prácticas existentes para que las organizaciones de infraestructura crítica gestionen y reduzcan los riesgos de ciberseguridad, tuvo en cuenta unas características y elementos para luego realizar una calificación con estos criterios, los cuales fueron esenciales en el análisis, identificando los siguientes estándares con mayor nivel de cobertura según las características y elementos para ISA INTERCOLOMBIA:

ISO/IEC 27001 – Anexo.

21 pasos para mejorar la seguridad cibernética de las redes SCADA - The U.S. Department of Energy.

Controles de seguridad y privacidad para sistemas y organizaciones federales de información. NIST SP 800-53.

Adicional a la literatura analizadas como los estándares y buenas prácticas entre otros, se tuvieron en cuenta modelos de madurez que ayudan a identificar las fortalezas, debilidades

y riesgos en los procesos organizacionales, permitiendo entender y evaluar a la organización y su estado actual de la ciberseguridad. A partir de lo anterior se definió un modelo que contiene los requerimientos mínimos para construir los lineamientos que aseguren los sistemas de control industrial. El modelo parte de elementos muy generales considerados tanto en la norma ISO, como en la guía de las buenas prácticas y el estándar NIST, hacia una visión más particular enfocada a mejorar la seguridad de los sistemas de ICS. Los lineamientos propuestos a partir del trabajo y de la matriz de ISA INTERCOLOMBIA se enfocan en cuatro (4) capacidades denominadas: seguridad, defensa, aseguramiento y monitoreo, las cuales permiten elevar y mejorar el nivel de madurez organizacional de ISA INTERCOLOMBIA en la dirección que apoyan no solo la organización, sino que también ayudan a madurar la estrategia de ciberseguridad planteada por la empresa.

Como propuesta para la organización y en busca que estos lineamientos sean materializados en la gestión de la mitigación del riesgo de seguridad identificado en el informe de gestión 2019, se propuso modelarlos a través de un modelo de madurez que permite contemplar los diferentes estadios en los que la organización debería navegar para elevar y mejorar la mitigación del riesgo.

En este orden de ideas, convertir los lineamientos en un modelo de madurez garantizar, no solo su observancia, sino también su gestión, medición y control de parte de ISA INTERCOLOMBIA.

Se presentan unas consideraciones para elevar los Índices de Evaluación de los Niveles de Madurez para la Protección de los ICS, permitiendo evaluar y medir el nivel de madurez de la capacidad.

Para definir los marcos que permitieron la construcción de la propuesta de los lineamientos de ciberseguridad se abordaron y trataron desde la función y gestión que cada uno de estos cumplen, clasificándolos desde unas *características y elementos*, que permitieron analizar cómo cada estándar puede ser aplicado para gestionar gran parte de los ataques cibernéticos dirigidos a los sistemas OT que ayudarían a establecer un sistema formado por procesos, personas y tecnologías, que analice los riegos permitiendo definir y establecer las medidas y controles necesarios para minimizarlos a través de un ciclo de mejora continua.

La "tecnología" es una *característica* relevante en los estándares abordados y esto se debe a que es la que soporta y apalanca, además permite el funcionamiento de los procesos de los ICS con el objetivo de controlar equipos o máquinas. A través de las tecnologías se logran mejoras en los procesos operativos debido a que la automatización de estos permite la toma de decisiones de una manera oportuna para las organizaciones.

Igualmente, dentro de los *elementos* más relevantes identificados en los estándares están los "Operativo y Táctico", donde se pudo observar la correlación que tienen entre estos, debido a que el *elemento* "operativo" contiene una formulación y asignación de actividades y acciones a ser desarrolladas las cuales deben ser ejecutadas en los planes enunciados en lo "táctico". En definitiva, encontramos que, los elementos operacionales son altamente

tácticos, debido a que estos últimos diseñan y describen lo que se debe hacer a través de un proceso documentado.

Los tres estándares seleccionados presentan unas estrategias y metodologías muy completas y holísticas para la gestión de los riesgos asociados a la protección de los activos de una organización, a través de una gestión coordinada en la aplicabilidad de controles de seguridad de forma óptima, escalable e integrable. De manera general el conjunto de controles de seguridad puede ser adaptados a las necesidades específicas de acuerdo con la misión de cada organización.

Los estándares se pueden combinar y apoyarse mutuamente, estos se conectan y complementan entre sí, ayudando a identificar, proteger, detectar, responder y recuperarse frente algún evento cibernético, logrando mejores resultados en el desarrollo de un programa de seguridad, de una manera fácil, dentro de un entorno de mejora continua, porque definen un lenguaje común para la gestión del riesgo, garantizando la aplicación coordinada y organizada de los controles de seguridad de forma óptima, escalable e integrable.

Para nuestro caso en ISA INTERCOLOMBIA, los estándares deben emplearse como referencia y no como solución final, estos suministran información valiosa y útil en el diseño de los procesos de control y mitigación de riesgos de ciberseguridad. En ese orden de ideas, en el trabajo se identificó y decidió cuáles estándares son aplicables de acuerdo con las circunstancias, también se realizaron los ajustes expresados en el modelo propuesto. Se puede concluir que no existe una única alternativa para la adopción de los estándares que debe implementar una organización, lo más importante es comprender cual es la estrategia y hacia

dónde va la empresa para saber qué pasos se deben tomar y como mantener los lineamientos de ciberseguridad actualizados, por lo tanto, la ciberseguridad debe entenderse como un proceso de mejoramiento continuo que está alineado a la estrategia y a los objetivos de la organización.

Los lineamientos de ciberseguridad propuestos están alineados con la transformación digital del Grupo ISA, porque permiten facilitar la continuidad de los negocios, protegiendo la integridad de los sistemas de información e infraestructuras críticas que impulsan las operaciones y garantizando los servicios esenciales.

Los lineamientos de ciberseguridad juegan un papel fundamental, además, están alineados con la estrategia de ciberseguridad, describen los mecanismos de protección, son procesos que fomentan la cultura de ciberseguridad, planes de recuperación, permiten el monitoreo continuo de la evolución del riesgo, por tanto, es posible anticiparse a eventos futuros: prevención, detección, respuesta, predicción, adopción de mejores prácticas y tecnologías que se adapten a los desafíos de seguridad que trae consigo la transformación digital.

10. Recomendaciones

Se recomienda que este modelo en un futuro pueda ser evaluado para despliegue e implementación en otras empresas del sector energético, con el propósito de poder comparar los resultados obtenidos entre las diferentes empresas.

También, realizar una revisión sistemática de literatura para identificar la concordancia de trabajos similares en otros sectores de infraestructuras críticas y a partir de ello encontrar, no solo semejanzas, sino también complementariedades.

Además, tener en cuenta que este trabajo puede servir como base inicial para que cualquier sector pueda hacer uso del modelo, donde se permite evaluar sus prácticas y el estado de madurez actual de ciberseguridad.

Se propone de manera general las siguientes recomendaciones para darle continuidad al modelo presentado:

Identificar, catalogar y priorizar los sistemas (activos y ciberactivos) que necesitan ser protegidos.

Construir y separar grupos lógicamente de acuerdo con su funcionalidad, con el fin de evitar incidentes en toda la red corporativa e industrial.

Diseñar a la medida una estrategia de defensa en profundidad.

Monitorear y controlar los accesos físicos y lógicos a cada sistema.

Supervisar y controlar agentes externos, como contratistas, soporte, proveedores de servicio con acceso específicos a componentes o subsistemas de los ICS.

Supervisar las actividades de los empleados con altos roles y privilegios en la administración y configuración de los ICS.

Establecer un mecanismo de gestión de identidad y acceso, que permita la autenticación, autorización y acceso a los componentes críticos (servicios y aplicaciones) de los ICS.

Monitorear y supervisar los eventos que ocurren entre los grupos funcionales.

Establecer una matriz de riesgos y un plan de respuesta a eventos e incidentes.

El acuerdo 1241 fue reemplazado por el acuerdo 1347 del CNO el 16 de septiembre de 2020, sin embargo, durante el tiempo que duró el presente trabajo, dicho acuerdo no había entrado en vigencia, es por eso que no se realizó la incorporación del mismo en el documento y se deja para revisiones posteriores. Se vincula este párrafo, una vez que los jurados hacen una revisión del trabajo final y encontraron que dicho acuerdo debía ser anotado.

Bibliografía

Albors, J. (2017). ESTADO DE LA CIBERSEGURIDAD EN SISTEMAS DE CONTROL INDUSTRIAL. *Protegerse*.

Anabalón, J. D. (2018). Seguridad en Sistemas SCADA un Acercamiento Práctico a Través de EH e ISO 27001:2005. https://www.researchgate.net/publication/324918959_Seguridad_en_Sistemas_SCADA_un_Acercamiento_Practico_a_Traves_de_EH_e_ISO_270012005.

ANSSI. (2014). *Managing Cybersecurity for Industrial Control Systems*. Obtenido de https://www.ssi.gouv.fr/uploads/2014/01/Managing_Cybe_for_ICS_EN.pdf

Ardila, O. P. (2010). ESTADO ACTUAL Y FUTURO DE LA INGENIERÍA DE. *Universidad Pontificia Bolivariana, Seccional Bucaramanga*, http://dx.doi.org/10.18566/puente.v4n2.a01.

Arquitectura TI Colombia. (s.f.). *Herramientas estrategias TI*. Obtenido de https://www.mintic.gov.co/arquitecturati/630/w3-article-9275.html

Barker, C. (2007). *NIST Security Measurement NIST SP 800-55* . Retrieved January.

Byres, E. a. (2005). *Firewall deployment for scada and process control networks.* Centre for Protection of National Infrastructure, Government Digital Service.

Caicedo-Eraso, J. C. (2015). Redes industriales.

Cano, J. J. (06 de Octubre de 2011). *http://www.seguridadparatodos.es*. Obtenido de http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html

Case, Defense Use. (2016). Analysis of the cyber attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*.

Chaves, A. a. (2017). *Improving the cyber resilience of industrial control systems.* International Journal of Critical Infrastructure Protection.

Comando General de las Fuerzas Militares. (2016). *Sectores Estratégicos de la República de Colombia desde la óptica cibernética.* Bogotá.

Comite Nacional de Operación . (2015). *Guia de Ciberseguridad.* Bogotá.

Comite Nacional de Operación. (2019). *Guia de Ciberseguridad.* Bogotá.

CONPES 3995. (01 de julio de 2020). *DNP.GO.CO.* Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Cristina Alcaraza, S. (2014). Critical infrastructureprotection: Requirements and challengesforthe21stcentury. *Critical Infrastructure Protection.*

(2019). *CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2).*

Dagoumas, A. (2019). Assessing the Impact of Cybersecurity Attacks on Power Systems. *Energies.*

Departamento Administrativo de la Presidencia de la República. (s.f.). *Mintic*. Obtenido de https://dapre.presidencia.gov.co/dapre/procedimientos-y-lineamientos/lineamientos-dapre

Directiva Europea. (2008). *DIRECTIVA 2008/114/CE DEL CONSEJO de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.*

DNP. (07 de septiembre de 2020). *Documentos Conpes.* Obtenido de https://www.dnp.gov.co/CONPES/documentos-conpes/Paginas/documentos-conpes.aspx

ENISA. (2011). *Protecting Industrial Control Systems. Recommendations for Europe and Member States.* Obtenido de https://www.enisa.europa.eu/publications/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states

ENISA. (2014). Methodologies for the identification of Critical Information Infrastructure assets and services. *European Union Agency for Network and Information Security.*

Fundación In-Nova Castilla La Mancha. (2019). *Ciberseguridad y Ciberdefensa.*

García A, J. A. (217). Investigación de la Ciberseguridad aplicada a los Sistemas de Control Industrial con énfasis en el sector energético.

Hemsley, K. E. (2018). *History of industrial control system cyber incidents.* Idaho National Lab.(INL), Idaho Falls, ID (United States).

Herrera, L.-C. a. (2019). A Comprehensive Instrument for Identifying Critical Information Infrastructure Services. *International Journal of Critical Infrastructure Protection.*

Instituto de Auditores Internos de España. (Octubre de 2016). Buenas Prácticas en Gestión de Riesgos. *Ciberseguridad Una guía de supervisión*. Obtenido de https://auditoresinternos.es/uploads/media_items/guia-supervision-ciberseguridad-fabrica-pensamiento-iai.original.pdf

Instituto Español de Estudios Estratégicos; Instituto Universitario General Gutiérrez Mellado. (2011). *CIBERSEGURIDAD: RETOS Y AMENAZAS A LA SEGURIDAD NACIONAL EN EL CIBERESPACIO.* Dirección general de Relaciones Institucionales de la Defensa.

Instituto Español de Estudios Estratégicos; Instituto Universitario General Gutiérrez Mellado. (2011). *CIBERSEGURIDAD: RETOS Y AMENAZAS A LA SEGURIDAD NACIONAL EN EL CIBERESPACIO.*

ISA. (2019). *Reporte Integrado de Gestión.*

Isa. (29 de mayo de 2020). *Isa.* Obtenido de http://www.isa.co/es/nuestra-compania/Documents/Pol%C3%ADtica_Gesti%C3%B3n_Integral_Riesgos_firmado.pdf

ISA. (29 de mayo de 2020). *Isa.* Obtenido de http://www.isa.co/es/nuestra-compania/Documents/Pol%C3%ADtica_Gesti%C3%B3n_Integral_Riesgos_firmado.pdf

ISA. (29 de mayo de 2020). *isa.co.* Obtenido de http://www.isa.co/es/nuestra-compania/Documents/Pol%C3%ADtica_Informaci%C3%B3n_firmado.pdf

ISA INTERCOLOMBIA . (2019). *Isa Intercolombia.* Obtenido de http://www.isaintercolombia.com/Files/attachments?listname=InformesEmpresariales&id=16

Isa Intercolombia. (2019). *Isa Intercolombia.* Obtenido de http://www.isaintercolombia.com/Files/attachments?listname=InformesEmpresariales&id=16

Isa Intercolombia. (2019). *Isa Intercolombia.* Obtenido de http://www.isaintercolombia.com/Files/attachments?listname=InformesEmpresariales&id=16

iso.org. (2015). *iso.org.* Obtenido de iso.org: https://www.iso.org/fr/standard/63461.html

ISO27001. (s.f.). *NormaISO27001.* Obtenido de https://normaiso27001.es/liderazgo-en-iso-27001/

Jarmakiewicz. (2017). Cybersecurity protection for power grid control infrastructures.

Jarmakiewicz, J. a. (2017). *Cybersecurity protection for power grid control infrastructures.* International Journal of Critical Infrastructure Protection.

Johnson, J. a. (2011). *Photovoltaic DC arc fault detector testing at Sandia National Laboratories.* 2011 37th IEEE Photovoltaic Specialists Conference.

Kaska, K. a. (2015). Regulating Cross-Border Dependencies of Critical Information Infrastructure. *NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE): Tallinn, Estonia.*

Klaver, M. a. (2011). RECIPE: Good practices manual for CIP policies, for policy makers in Europe. *TNO Nederlandse Organisatie voor Toegepast-Natuurwetenschappelijk Onderzoek.*

Knapp, E. D. (2014). Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems. *Syngress.*

Knowles, W. a. (2015). *A survey of cyber security management in industrial control systems.* International journal of critical infrastructure protection.

Langher, R. (2011). *Stuxnet: Dissecting a cyberwarfare weapon.* IEEE Security & Privacy.

Li, Z. a. (2017). *Cybersecurity in distributed power systems.* Proceedings of the IEEE.

Li, Z. a. (2017). Cybersecurity in distributed power systems. *Proceedings of the IEEE.*

Liang, G. a. (2016). *The 2015 ukraine blackout: Implications for false data injection attacks.* IEEE Transactions on Power Systems.

Luiijf, E. (2006). Vital Infraestructure Threats and Assurance (VITA) project. *ECN.*

Martinez, M. (2018). *Ciberseguridad, un riesgo estratégico.* Obtenido de https://assets.kpmg/content/dam/kpmg/es/pdf/2018/04/folleto-ciberseguridad.pdf

Ministerio de tecnologías de la información y las comunicaciones. (27 de octubre de 2014). Obtenido de https://www.mintic.gov.co/arquitecturati/630/articles-9275_recurso_pdf.pdf

Mintic. (s.f.). Obtenido de https://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8061.html

Mintic. (s.f.). Obtenido de https://www.mintic.gov.co/arquitecturati/630/w3-article-9276.html

Mintic. (2011). Obtenido de Mintic: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

National Institute of Standar and Technology. (s.f.). *NIST SP 800-53 REV.4-*.

NIST. (s.f.). Obtenido de https://www.nist.gov/cyberframework/new-framework

Paulk, M. (2002). *Capability maturity model for software.* Encyclopedia of Software Engineering.

Pérez A, L. B. (2014). Tendencias de seguridad para sistemas ICS y Scada. *TechTarget*.

Perez San Jose, A. A. (2012). Estudio sobre la seguridad de los sistemas de monitorización y control de procesos e infraestructuras (SCADA). *INTECO : Instituto Nacional de Tecnologias de la Comunicación.*

Ramírez, A. (2018). Una buena estrategia de seguridad, clave para proteger los sistemas industriales. https://www.interempresas.net/Instaladores/Articulos/.

Riigikogu. (08 de 02 de 2017). *Emergency Act*. Obtenido de https://www.riigiteataja.ee/en/eli/513062017001/consolide

Said, C. G. (2016). Infraestructuras Críticas: Sectores Necesitados De Un Modelo De Ciberseguridad. *EUROPEAN SCIENTIFIC JOURNAL, ESJ*, https://eujournal.org/index.php/esj/article/download/7388/7116.

Sebastian Obermeier, S. S. (2012). Ciberseguridad : La protección de las infraestructuras. *Revista ABB - Dialnet*, http://docplayer.es/6360283-Ciberseguridad-la-proteccion-de-las-infraestructuras-criticas-en-un-mundo-cambiante.html.

Stevens, J. (2014). *Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)(Case Study).* CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

Stouffer, K. a. (2011). *Guide to industrial control systems (ICS) security.* NIST special publication.

Stouffer, K. A. (2011). Sp 800-82. guide to industrial control systems (ics) security: Supervisory control and data acquisition (scada) systems, distributed control systems (dcs), and other control system configurations such as programmable logic controllers (plc). *ational Institute of Standards & Technology*.

Szadeczky, T. (2018). Cybersecurity authorities and related policies in the EU and Hungary. *Facultas Verlags-und Buchhandels AG*.

Villalba, A. y. (2017). Análisis de las ciberamenazas. *Cuadernos de Estratregia (97 -138)*, https://dialnet.unirioja.es/servlet/articulo?codigo=6115622.

Vinyes, E. (2017). Entender los riesgos: ciberseguridad para la red eléctrica actual. *Energía de Hoy*, https://www.interempresas.net/Energia/Articulos/215021-Entender-los-riesgos-ciberseguridad-para-la-red-electrica-actual.html.

Whitman, M. E. (2011). *Principles of information security.* Cengage Learning.