Cuadro de indicadores para el gerenciamiento de la ciberseguridad en las tecnologías de operación de una empresa del negocio distribución de energía

Edgar Alexis Fernández Cardona
Luis Carlos Herrera Velásquez

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

TRABAJO DE GRADO MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA

CUADRO DE INDICADORES PARA EL GERENCIAMIENTO DE LA CIBERSEGURIDAD EN LAS TECNOLOGÍAS DE OPERACIÓN DE UNA EMPRESA DEL NEGOCIO DISTRIBUCIÓN DE ENERGÍA

ESTUDIO DE CASO

EDGAR ALEXIS FERNÁNDEZ CARDONA

ESCUELA SUPERIOR DE GUERRA

Bogotá D.C. 2020

CUADRO DE INDICADORES PARA EL GERENCIAMIENTO DE LA CIBERSEGURIDAD EN LAS TECNOLOGÍAS DE OPERACIÓN DE UNA EMPRESA DEL NEGOCIO DISTRIBUCIÓN DE ENERGÍA

EDGAR ALEXIS FERNÁNDEZ CARDONA

Trabajo de grado para optar al título de Magíster en Ciberseguridad y Ciberdefensa

Asesor:

LUIS CARLOS HERRERA VELÁSQUEZ

Ingeniero de Sistemas

ESCUELA SUPERIOR DE GUERRA

EMPRESAS PÚBLICAS DE MEDELLÍN EPM E.S.P.

Bogotá D.C.

2020

Resumen

Esta investigación propende por aportar elementos al gerenciamiento de la seguridad cibernética relacionado con la prestación del servicio de energía eléctrica, específicamente en lo concerniente a las tecnologías que realizan funciones de adquisición de datos, supervisión, control y telecomunicaciones que permiten operar remotamente, la infraestructura eléctrica con que se presta el servicio de electricidad a las poblaciones, ciudades y en general al país.

Para ello, se recurrió a la técnica de planeación por escenarios para identificar desde la seguridad cibernética, los aspectos más relevantes que deben ser gerenciados en una empresa de distribución de energía eléctrica, con el fin de minimizar el impacto en la continuidad del servicio y las pérdidas económicas relacionadas, producto de la materialización de eventos e incidentes cibernéticos. Los análisis se focalizaron en la continuidad y buen funcionamiento de la cadena de control entre las subestaciones eléctricas, las telecomunicaciones y los propios centros de control, desde donde se opera centralizadamente la infraestructura de prestación del servicio.

Con base en técnicas que involucran criterios de expertos y herramientas de modelación como MICMAC, MACTOR, SMIC, entre otras; se identifican y analizan las variables y actores clave, se proponen y validan hipótesis que permiten construir los tipos de escenarios más probables y se identifican los asuntos clave que deben administrarse en términos de ciberseguridad.

A partir de los asuntos clave encontrados y la información disponible de evaluación general de riesgos cibernéticos en tecnologías de operación de la compañía, se filtran las causas que afectan los asuntos clave y construyen los escenarios de riesgos. A partir de los

indicadores de riesgo actual, se propone un nivel objetivo para evitar la materialización de eventos de alto impacto en tecnologías de operación. Teniendo en cuenta las causas que originan dichos escenarios, se proponen los indicadores clave de riesgo - KRI (Key Indicator Risk) que deben ser monitoreados y gerenciados por la organización bajo estudio.

Summary

This research is intended to contribute elements to the management of cybersecurity related to the provision of the electricity service, specifically with regard to technologies that perform data acquisition functions, monitoring, control and telecommunications that allow remote operation, the electrical infrastructure with which electricity service is provided to populations, cities and in general the country.

To do this, the scenario planning technique was used to identify from cybersecurity, the most relevant aspects that must be managed in an electric power distribution company, in order to minimize the impact on continuity related economic losses, the product of materializing cyber events and incidents. The analyses focused on the continuity and smooth functioning of the control chain between the electrical substations, telecommunications and the control centers themselves, from where the infrastructure for the provision of the Service.

Based on techniques involving expert criteria and modeling tools such as MICMAC, MACTOR, SMIC, among others, key variables and actors are identified and analyzed, hypotheses are proposed and validated to build the most likely types of scenarios, and the key issues to be managed in terms of cybersecurity are identified and validated.

Based on the key issues found and the available general cyber risk assessment information in the company's operating technologies, the causes that affect them are filtered and build risk scenarios. Based on current risk indicators, a target level is proposed to avoid the materialization of high-impact events in operating technologies. Taking into account the causes that cause such scenarios, the key risk indicators - KRI (Key Indicator Risk) are proposed that must be monitored and managed by the organization under study.

Tabla de contenido

Contenido

Índice de Gráficas

Tablas

Anexos

Introducción

El gran desarrollo que han experimentado las tecnologías de la información y telecomunicaciones en los últimos años ha permitido mejorar servicios y procesos, mediante la transformación y creación de nuevos modelos de negocio y desencadenado transformaciones de la industria basadas en la conectividad de personas, objetos, artefactos y aplicaciones.

Con la gran cantidad de dispositivos y aplicaciones intercomunicadas que generan e intercambian datos, hoy quizás nadie discute el valor de la información como un insumo importante para obtener eficiencias operacionales y como una fuente permanente de ventaja competitiva para las organizaciones, la base para la generación de nuevos productos, servicios y la misma comercialización de éstos alrededor del mundo.

Esta conectividad basada en lo que se conoce como interoperabilidad entre aplicaciones y dispositivos, entendida como la capacidad de intercambiar información útil, ha traído impactos positivos, también ha traído consigo riesgos, los cuales están asociados a la pérdida de confidencialidad, integridad, y la disponibilidad y continuidad de la producción y prestación de algunos servicios esenciales para la sociedad, entre los que se encuentran la energía eléctrica, el suministro de agua y las telecomunicaciones, en las cuales se basa el funcionamiento de los servicios que requiere la sociedad moderna.

Un ejemplo de la materialización de estos riesgos, son los ciberataques que han ocurrido en los sistemas de control industrial, en los que se basan servicios esenciales para la sociedad. Quizás uno de los casos de incidentes de ciberseguridad en sistemas de control más divulgado y estudiado, ha sido el ocurrido en Ucrania el 23 de diciembre del año 2015 al sistema de

distribución de energía eléctrica en tres de sus empresas del sector. Este evento ocasionó la suspensión total en el servicio de electricidad a más de 225.000 usuarios por más de 8 horas, y dejó claro que los riesgos cibernéticos no son exclusivos de las aplicaciones informáticas que manejan la información de un negocio.

Aunque existía como otro antecedente importante el caso del malware STUXNET, como un ataque avanzado persistente perpetrado sobre sistemas de control industrial, en ese caso se trató del saboteó un sistema de producción en una planta específica que desarrollaba el enriquecimiento de uranio, pero ahora se está hablando del ataque a infraestructura crítica de todo un país con la afectación de servicios esenciales, corroborando también como lo hizo Stuxnet, que el simple hecho de tener sistemas aislados de otras redes o de internet, no significa que estén protegidos o que sean más seguros que otros sistemas que están interconectados o en red.

La materialización de estos riesgos, no solo impactan el funcionamiento de las aplicaciones informáticas de una compañía, sino aspectos más trascendentales como la confidencialidad de su información competitiva y sus secretos industriales, por mencionar a algunos activos y actividades clave. Sumado a lo anterior, estos riesgos ahora se han trasladado al propio ámbito del proceso productivo de bienes y servicios, afectando la continuidad e integridad de la infraestructura que soporta los servicios esenciales que un país necesita para su funcionamiento, la seguridad y la salud de sus habitantes.

Algunos países han visto afectados sus servicios esenciales como la electricidad de la cual dependen muchos otros sectores y servicios también catalogados como críticos, como el transporte, la banca, el funcionamiento de los mercados, las telecomunicaciones, entre otros. El presente trabajo aborda específicamente la gestión de los riesgos cibernéticos que

impactan la continuidad de las tecnologías que permiten operar la infraestructura eléctrica de una compañía de distribución de electricidad.

Este trabajo se divide en ocho capítulos, en el primero se presenta la unidad de información y unidad de análisis, el segundo aborda la definición del problema, el capítulo tres presenta el objetivo general, los específicos y el capítulo cuarto aborda el marco teórico. En el capítulo cinco se define el diseño metodológico y en el capítulo seis se desarrollan los objetivos, terminando con el capítulo siete que contiene las conclusiones y recomendaciones, y culminando con la bibliografía empleada la cual se lista en el último de estas secciones enunciadas.

1. Definición del objeto del caso

La situación por analizar es la identificación de los aspectos prioritarios de la seguridad cibernética que deben ser gerenciados en las tecnologías de operación, en una empresa de distribución de energía eléctrica en Colombia. Esto se realizará mediante el estudio de los factores y actores más importantes que influencian la disponibilidad y la continuidad de las tecnologías que soportan la operación, para luego construir hipótesis y escenarios posibles que contribuyan al mejoramiento de la ciberseguridad.

La construcción se realiza con base en criterios de expertos de operación de los activos de distribución de energía, expertos en soporte de tecnologías de operación y en seguridad cibernética. Se propondrán hipótesis con base en las variables clave identificadas, los actores más dominantes, las acciones que deben emprenderse, para construir los escenarios más probables. Finalmente se relacionarán estos aspectos clave a gestionar con los análisis de riesgos disponibles con el fin de para construir los indicadores clave de riesgo que deberán ser gerenciados, permitiendo definir controles y acciones en ciberseguridad, contrastándolos con los elementos teóricos encontrados. Con base en lo anterior, se propone un cuadro de indicadores orientados al gerenciamiento de la seguridad cibernética en tecnologías de operación.

1.1 Unidad de análisis

La sociedad moderna es cada vez más dependiente de la energía. Los países desarrollados y en vía de desarrollo evolucionan hacia una mayor automatización de los procesos de muchos de los servicios que requiere la sociedad para su funcionamiento. Estos procesos basados en ordenadores, telecomunicaciones y en el valor extraído a la información, se ha

convertido en la base para generar conocimiento, crear ventajas competitivas, transformar los negocios actuales a través de la generación de nuevos productos y servicios, basados en la información.

La prestación del servicio público de electricidad que tradicionalmente ha sido un servicio esencial requerido por las sociedades en general hoy experimenta unos grandes niveles de automatización en respuesta a unas mayores exigencias desde las perspectivas de continuidad, calidad del servicio y el mismo costo. Cada vez las interrupciones del servicio son más impactantes para el usuario final, el estado, los negocios y el regulador del servicio de electricidad penaliza con mayor rigor este tipo de fallas.

El buen desempeño y continuidad de este servicio, está soportado operativamente en el buen funcionamiento de muchos activos e infraestructura del sector eléctrico de cada país. Específicamente para conducir la electricidad desde los grandes puntos de transmisión y generación hasta el usuario o cliente final, existe infraestructura compuesta por: las subestaciones eléctricas de 110 kV e infraestructura lineal con circuitos eléctricos de media tensión de 44kV, 34,5 kV y 13,2 kV y en baja tensión correspondiente a los voltajes menores a 1kV. La disponibilidad de estos activos y la calidad de los servicios prestados basados en un eficiente esquema de operación constituyen lo que se conoce como el negocio de distribución de energía eléctrica.

Para la operación de estos sistemas eléctricos, los activos cuentan con sistemas de control industrial que toman decisiones de supervisión, control y adquisición de datos a través de herramientas SCADA por sus siglas en inglés. Estos sistemas trabajan de manera automática en el proceso que controlan y habilitan la supervisión y operación remota de todo el sistema eléctrico mediante el monitoreo y la toma de decisiones operativas centralizadas en tiempo

real. Dichas acciones operacionales son ejecutadas por ingenieros de la operación, desde lo que se conoce como un centro de control.

Específicamente este negocio, tiene implícitas tres condiciones de importancia que deben considerarse:(1) La actividad se encuentra actualmente en una gran transformación, al incorporar múltiples tecnologías basadas en las Tecnologías de Información y Telecomunicaciones, entre otras, tales como: la automatización de la distribución, la modernización de los centros de control, implementación de aplicaciones más avanzadas para la operación, la implementación de la infraestructura de medición avanzada – AMI por sus siglas en inglés, la cual es obligatoria su implementación en el 75% del mercado al 2030, según disposiciones del Ministerio de Minas y Energía en su decreto MME 4- 0072 y 4-0483 de 2019; (2) la propia regulación del negocio es muy dinámica en la forma en que mide y exige los niveles de la calidad del servicio que se le prestan al cliente, en términos de continuidad de los activos y la propia disponibilidad del servicio, el cual es penalizado según el número de interrupciones que se presenten y su respectiva duración; y, (3) la remuneración de la actividad de distribución en los últimos años ha tenido una fuerte tendencia a volverse más exigente; actualmente existe una metodología de costos eficientes, la cual verifica las inversiones que requiere el sistema eléctrico y que puedan demostrar que fueron necesarias y eficientes, de lo contrario no serán reconocidas dentro del cálculo de los ingresos para el operador de la red, el cual es regulado por ser un monopolio natural.

La tendencia del sector eléctrico a nivel mundial, conducen a que el desarrollo tecnológico, tenga gran orientación hacia las redes inteligentes o lo que se ha denominado "smart grid" el cual consiste en la incorporación de Tecnologías de Información y Telecomunicaciones – TIC para mejorar el desempeño del servicio y disminuir los costos de prestación del mismo. Este

avance tecnológico en las tecnologías de control, sumado a la estrategia del Grupo EPM de consolidar sus operaciones y ganar sinergias entre sus empresas, han llevado al grupo a evolucionar hacia una sola plataforma SCADA centralizada para supervisar y controlar todas las subestaciones de todas sus empresas de distribución en Colombia, las cuales están ubicadas en diferentes puntos geográficos.

La estrategia empresarial, sumada al concepto "Smart Grid" y la incorporación de tecnologías de telecomunicaciones que emplean protocolos IP, traen consigo mayores vulnerabilidades y riesgos cibernéticos a los sistemas de control. Estas condiciones hacen totalmente pertinente y de valor para el negocio distribución de energía eléctrica, contar con un cuadro de indicadores gerenciales que le permitan gestionar la ciberseguridad en las tecnologías de operación, las cuales permiten la supervisión y control propias del proceso de operación centralizada de sus activos.

El estudio del caso se realiza sobre un proceso específico, la operación centralizada de una subestación típica de distribución desde un centro de control de una empresa del Grupo EPM en Colombia y no hay otras unidades de análisis. Para ello, es necesario considerar tres elementos dentro de lo que se conoce como la cadena de control desde el centro de control: (1) el Sistema de Adquisición de Datos y Supervisión y Control - SCADA central por sus siglas en inglés; (2) el respectivo sistema de telecomunicaciones que permite la conectividad entre el sistema SCADA central; y, (3) el elemento con el nivel más alto de control que existe en una subestación conocido como Remote Terminal Unit – RTU por sus siglas en inglés o concentrador de subestación, dependiendo de la tecnología empleada.

1.2 Unidad de información

Esta investigación será elaborada para el Grupo mpresarial EPM, con la modalidad Caso de Estudio como tesis de grado en la Maestría de Ciberseguridad y Ciberdefensa que cursa el Ingeniero Edgar Alexis Fernández Cardona en la Escuela Superior de Guerra, con el fin de obtener el título de Magíster.

La información relacionada con las prácticas de ciberseguridad en tecnologías de operación requerida para este fin será suministrada por expertos de EPM, pertenecientes al negocio distribución energía, otras empresas del sector eléctrico, la academia, otros sectores como el militar y consultoría en ciberseguridad, su carácter es confidencial sólo podrá utilizarse para definir el cuadro de indicadores de ciberseguridad que se proponga para el negocio distribución energía del Grupo Empresarial EPM.

1.3 Definición del problema

Los sistemas de control industrial permiten el correcto funcionamiento de procesos productivos industriales y la prestación de servicios esenciales o críticos que requiere la sociedad para su funcionamiento, como los servicios de energía eléctrica, agua, gas, entre otros; a través de infraestructuras que se han catalogado por algunos Estados como críticas. Estos sistemas de control tradicionalmente han sido conocidos en la literatura técnica especializada, como sistemas SCADA y realizan funciones de adquisición de datos, control y supervisión. Su función principal es permitir la operación remota de los activos eléctricos en el caso de la prestación de servicio de energía eléctrica, desde un centro de control.

En los últimos años, estos sistemas de control han incrementado los riesgos de tipo cibernético, en contraste con una baja prioridad frente al objetivo de seguridad cibernética por parte de los grupos de interés de las empresas que los utilizan, operan y soportan, como lo enuncian (Knowles, Prince, Hutchison, Disso, & Jones, 2015, pág. 52) en su trabajo. Esto se debe principalmente a que las empresas que emplean sistemas de control industrial, han utilizado tradicionalmente la técnica de mantener en secreto o en oscurantismo los sistemas de control, mediante el aislamiento de estas redes de telecomunicaciones con otros sistemas, estrategia que tuvo diferente éxito durante la primera y segunda generación de SCADA como lo plantean estos autores.

En las primeras dos generaciones de SCADA como lo plantea (Ujvarosi, 2016, pág. 64), estas tecnologías trabajaban como soluciones monolíticas aisladas y utilizaban componentes propietarios o de única marca, tecnologías propietarias o cerradas y con limitada conectividad. Sin embargo, la tercera y actual generación de control evolucionó a ser interconectada en red con otros dispositivos que no fueron necesariamente sistemas de control, permitiendo una apertura que ha aumentado la susceptibilidad a los ataques principalmente por el uso de estándares de industria en telecomunicaciones. Esto se vuelve aún más crítico si se tiene en cuenta que muchos sistemas de control, soportan el funcionamiento de infraestructuras críticas lo cual los hace más atractivos a ataques cibernéticos.

Los fabricantes de sistemas de control industrial o SCADA se concentraron en la especialización de su sistema y abandonaron la fabricación de hardware. Esto ocasionó la incorporación de componentes de hardware y software comerciales utilizados en otros sistemas, incluyendo sistemas operativos, que se han denominado COTS o Commercial Off-The-Shelf como lo presenta en su trabajo (DOE, 2012, pág. 2). Estos componentes, permiten

conectividad a otras redes, incluyendo redes corporativas y telecomunicaciones con protocolos IP, las cuales eran utilizadas en mayor proporción por las Tecnologías de Información - TI u ofimática.

Aunque el propósito inicial de la introducción de los COTs en los sistemas de control industrial era mejorar el negocio y sus procesos, estas componentes también han incrementado los riesgos al introducir sus propias vulnerabilidades a los sistemas de control, las cuales son ampliamente conocidas. La consecuencia de esto es una mayor exposición de los sistemas de control frente a los riesgos de ciberataques, específicamente en las automatizaciones de las subestaciones, sistemas de telecomunicaciones y sistemas SCADA, denominados Tecnologías de Operación – TO, como un término emergente para denominar en general el hardware y software para operar los sistemas de control industrial.

Al abordar este problema, aparecen varios asuntos relacionados con la viabilidad de la aplicación de controles cibernéticos en el dominio del control industrial y su impacto en la continuidad del proceso controlado. Al respecto existen varias posturas de autores como (Knowles, Prince, Hutchison, Disso, & Jones, 2015, pág. 53) , en relación con la eficacia y aplicabilidad de controles tradicionalmente empleados en el dominio de TI, ahora en el dominio de control,sostienen que si bien, en los sistemas de información el orden de priorización en la seguridad son la confidencialidad, integridad y disponibilidad, en los sistemas de control este orden se invierte, con la disponibilidad como principal meta a cumplir, sustentando como ejemplo que las empresas prestadoras de servicio de energía, priorizan la disponibilidad del servicio.

Autores como (Piggin & Boyes, 2015, pág. 2) plantean que los métodos y técnicas para el aseguramiento de la información, utilizando la triada estándar de: confidencialidad,

integridad, y disponibilidad de la información pueden ser suficiente para las tecnologías de información de oficina, pero para los sistemas de control son insatisfactorias, como también lo sustenta (Park & Lee, 2014, pág. 1). No obstante, se siguen recomendando este tipo de tecnologías y controles para la seguridad de los sistemas de control industrial.

Existen tópicos importantes que deben ser abordados a nivel empresarial, como el ciclo de mejoramiento continuo de seguridad, la medición del desempeño y eficacia de los controles de seguridad cibernética y la asertividad de los planes implementados. Para sacar adelante estos asuntos, el tema de las métricas en seguridad es un campo importante y totalmente necesario. Al respecto, si existen algunas propuestas, en general varios autores que coinciden en que hay mucho por desarrollar.

En la literatura científica existe un número de normas, recomendaciones y controles desarrollados en ciberseguridad para el sector eléctrico y catalogadas como buenos referentes, sumado a que hay otras normas de seguridad de la información para TI que podrían ser aplicables a TO previa validación. Aunque existen recursos académicos y lineamientos, implementar todas estas mejoras basadas en modelos de madurez, los cambios en procesos y la inversión en infraestructura que conlleva puede ser muy oneroso y poco eficiente, sino se mide su efectividad y se contrasta con la misma evolución de los riesgos.

Autores como (Knowles, Prince, Hutchison, Disso, & Jones, 2015, pág. 53), al realizar una revisión exhaustiva y extensa de las prácticas y normas en seguridad en sistemas de control para el sector eléctrico, concluyen que la principal barrera que ha impedido la implementación de metodologías de seguridad en estos sistemas de control es la escasez de métricas específicas en seguridad. Las agendas de futuras investigaciones deben incluir la construcción de este tipo de métricas, dado que la disponibilidad de un conjunto completo y

robusto de las métricas, son esenciales para que las organizaciones cumplan objetivos de negocio.

Es por ello, que los controles a implementar deben ser realizados dentro de un ciclo de mejora continua. Las diferentes decisiones relacionadas con estos aspectos deben estar orientados y soportados por indicadores que permitan identificar la calidad y efectividad de los controles y el retorno sobre la inversión realizada o Return of Investment - ROI (por sus siglas en inglés). Autores como (Zaratiegui, 1999, pág. 87) en su propuesta de gestión por procesos, introduce las métricas como un componente importante y constante en las diferentes fases del mejoramiento de procesos.

La gerencia del negocio debe contar con un conjunto de indicadores gerenciales relacionados con la ciberseguridad en TO, que complementen su cuadro de mando integral y le permitan monitorear el dinamismo de la evolución de los riesgos que afectan directamente la continuidad de negocio. Específicamente riesgos relacionados con la continuidad y disponibilidad de sus activos, la confiabilidad de su operación, el impacto de su continuidad como infraestructuras críticas dentro del sector eléctrico y la evaluación de la eficacia de las acciones y decisiones organizacionales que se están emprendiendo. Esto es necesario implementarlo para disminuir los riesgos cibernéticos, neutralizando las amenazas e incrementando la resiliencia en las operaciones del negocio, de manera eficiente y sostenible.

El problema se puede resumir al responder la siguiente pregunta:

¿Cómo diseñar un conjunto de indicadores en ciberseguridad para las Tecnologías de Operación (TO) que sirvan de apoyo para la toma de decisiones gerenciales y administrativas?

2. Objetivos

2.1. Objetivo general

Diseñar un conjunto de indicadores en ciberseguridad para TO que sirvan de apoyo para la toma de decisiones gerenciales y administrativas, de una empresa del negocio de Distribución de Energía. Caso de estudio: EPM - Colombia.

2.2. Objetivos específicos

- ✓ Analizar estándares y lineamientos del subsector distribución de energía eléctrica.
- ✓ Construir un escenario teórico de ciberataque en una cadena de control típica de una subestación eléctrica.
- ✓ Identificar los controles cibernéticos de alto nivel que deban ser implementados y monitoreados en la cadena de control industrial estudiada.
- ✓ Plantear los indicadores gerenciales de ciberseguridad alineados a los objetivos de negocio.

3. Marco teórico

3.1. Estudio de Caso

Un estudio de caso se define según (Yin, 2003, pág. 2) como una metodología de investigación empleada por las ciencias sociales que busca estudiar y comprender a profundidad un sujeto o situación específica. Los resultados de estos estudios pueden servir posteriormente para planear investigaciones más extensas, pero no sirven para formular generalidades; en este sentido, esta herramienta contribuye al conocimiento de fenómenos que pueden ser individuales, organizacionales, sociales y políticos.

Los estudios de caso son técnicas válidas cuando las preguntas "cómo " y "por qué " son formuladas, cuando el foco del estudio es un fenómeno contemporáneo dentro de un contexto de la vida real y el investigador tiene poca influencia o control sobre los eventos, preferidos frente a otros métodos que pueden incluir inspecciones, historias y análisis de información de archivo. Este autor relaciona los diferentes tipos comunes de estudios de caso, los cuales pueden ser complementados por otros estudios como el descriptivo y exploratorio:

Explicativos: busca establecer la relación causa – efecto.

Descriptivos: explican las características que definen el caso investigativo.

Exploratorios: se recurre a este tipo de estudios cuando hay pocos conocimientos científicos en relación con el tema estudiado y no se dispone de una teoría consolidada dónde apoyar la investigación.

Para propósitos investigativos, la técnica de estudio de casos puede ser utilizada como una estrategia de investigación aplicada en estudios organizaciones y de administración.

Al aplicar la técnica se realiza una pregunta empírica que investiga un fenómeno contemporáneo en a una situación en un contexto real. Para el caso de este trabajo se formularon tres preguntas fundamentales qué, para qué y cómo, las cuales permiten abordar el tema en estudio y darle el foco que requiere la organización, desde las siguientes consideraciones:

Qué: Un cuadro de indicadores gerenciales con alcance de una empresa del negocio distribución energía. En este caso el Qué, es de carácter exploratorio.

Para qué: Se requiere un cuadro de indicadores gerenciales que permita monitorear el desempeño de la seguridad cibernética en las tecnologías de operación, dar cuenta de los principales indicadores de gestión y desempeño de los controles implementados y su eficacia, con el fin de realizar un seguimiento a su evolución y calidad.

Cómo: con un estudio definiendo un evento típico de ataque cibernético, identificando las variables clave de ciberseguridad a gerenciar por parte del negocio y los valores que toman estas variables en condiciones normales y anormales, y la forma de gestionarlos dentro de la cadena de control centralizado de una subestación desde el centro de control.

En esta investigación, el tipo de estudio de caso se establece como "explicativo", debido a que se requiere formular conjunto de indicadores de ciberseguridad a ser incorporados dentro de un cuadro de mando integral para una empresa del negocio distribución energía, que permita incrementar la eficiencia, el seguimiento y control de las mejoras en las capacidades

de ciberseguridad de la organización, como un apoyo para para dar forma y lograr los objetivos estratégicos y operacionales.

En el desarrollo de este trabajo se presenta el procedimiento para establecer la definición de un estudio de caso sobre un problema identificado, delimitando el mismo, estableciendo su unidad de análisis, los elementos investigativos, las exploraciones de resultados, y finalmente realizando una propuesta, conclusiones y recomendaciones finales producto del análisis de información cruzada de todo lo recopilado, con los elementos teóricos encontrados.

3.2. Conceptos relacionados con tecnologías

Dentro de una organización existen diferentes tecnologías del tipo technoware, entendida esta como software, hardware, telecomunicaciones y redes de datos, de acuerdo con su función o uso. Algunas están concebidas para atender necesidades empresariales relacionadas con el manejo y procesamiento de la información que requiere el negocio, la atención de clientes, contabilización y gestión de costos, entre otros aspectos transaccionales, comúnmente llamadas **Tecnologías de Información - TI**. El estándar ISO 20016-1/2014 (ISO/IEC, 2014, pág. 22) define los Sistemas de Tecnologías de Información o Information Technology System (IT System) como:

"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".

Existen otras tecnologías específicas dentro de la organización que hacen parte del proceso productivo de los bienes y servicios que ejecuta la organización, con la función específica de

realizar la supervisión y control de proceso, conocidas como Sistemas de Control Industrial. Los sistemas de control Industrial o Industrial Control Systems – ICS en sus términos y siglas en inglés han sido definidas por el National Institute of Standard and Technology de EEUU en su NIST SP 800-53 Rev. 4 (NIST, 2013, pág. B9) 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".

Así mismo, el estándar NIST 800-82R2 (NIST, 2015, pág. B8) también los define complementariamente, como:

"Es un término general que abarca diferentes Sistemas de control incluidos SCADA (Sistemas de adquisición de datos supervisión y control), Sistemas de Control Distribuidos – DCS y PLC (Controladores Lógicos Programables), a menudo encontrados en sectores industriales e Infraestructuras Criticas".

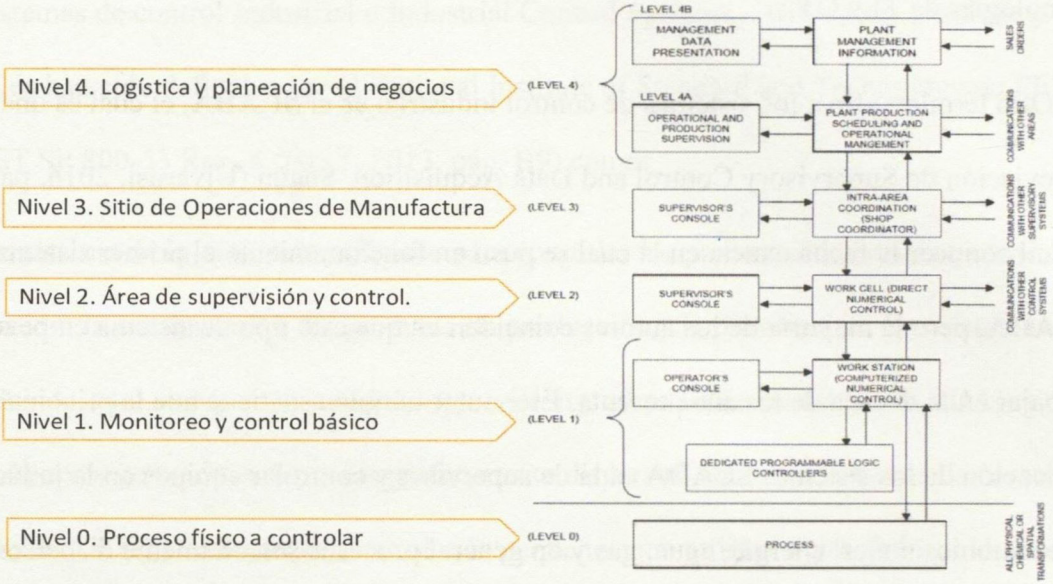
El departamento de energía de los Estados Unidos, en su documento Risk Management Process (DOE, 2012, pág. 2), plantea que el término **Tecnologías de Operación u Operation Technology (OT)** por sus siglas en inglés, es un término emergente dentro de la industria y es utilizado para describir los sistemas de hardware y software utilizados para operar dispositivos de control industrial o ICS, también conocido como OT. Así mismo (Sharma, 2017, pág. 362) sostiene que, un sistema de OT está compuesto de software y hardware para

monitorear y controlar un proceso o una planta y que existe una convergencia en las tecnologías de TI y OT.

Otro término afín a los sistemas de control industrial es el **SCADA**, el cual es una abreviación de Supervisory Control and Data Acquisition. Según (Ujvarosi, 2016, pág. 63) es difícil conocer la fecha exacta en la cual se puso en funcionamiento el primer sistema SCADA, pero la mayoría de los autores coinciden en que este tipo de sistema empezó a trabajar en la década de los años sesenta. Este autor también sostiene que la principal aplicación de los sistemas SCADA es la de supervisar y controlar equipos en la industria de telecomunicaciones, energía, agua, gas y en general procesos son altamente dispersos geográficamente.

Hay muchas similitudes entre los sistemas SCADA y los ICS, en general los dos términos son utilizados, pero normalmente en infraestructuras críticas, los Sistemas de Control Distribuido – DCS por sus siglas en inglés, trabajan en red a los sistemas SCADA. Los ICS son empleados para automatización industrial y procesos de producción industrial, pero en general la diferencia fundamental entre estos radica, en que el SCADA contiene una función específica de adquisición de datos el cual maneja bases de datos de tiempo real e histórico de las variables de supervisión y control. En su estándar IEC 62264-1 (IEC, 2003, pág. 192) Integración de Sistemas Empresariales y Sistemas de Control. Modelos y Terminología, define la jerarquía genérica que tienen los sistemas de control en una gran industria o en una planta de producción convencional. Entre los organismos encargados de normalizar técnicamente los sistemas de control se encuentran la Comisión Internacional de Electrotécnica - IEC por sus siglas en inglés, ISA 99, entre otros.

Gráfica 1. Jerarquía en sistemas de control industrial.



Basado en *(IEC, 2003, pág. 192)*

La norma IEC 62264 -1 describe la integración en los sistemas de control en una empresa. El objetivo de esta norma es la separación de los sistemas de producción de los sistemas empresariales. El estándar muestra la independencia de la información del proceso productivo y el proceso empresarial o de aplicaciones de negocio. En el cuadro se puede visualizar los diferentes niveles de control de un proceso que se ejecuta en una planta típica de producción.

3.3. Conceptos relacionados con seguridad cibernética en tecnologías de operación

En el 2015, el sector eléctrico mundial experimentó el derrumbe de un paradigma relacionado con la seguridad de los sistemas de control industrial y las infraestructuras críticas dedicadas a la prestación de servicios públicos de electricidad. Aunque existía como antecedente el caso de STUXNET, como un ataque avanzado persistente perpetrado sobre sistemas de control industrial con el objetivo de sabotear un proceso industrial local, ahora se estaba ante un ataque a la infraestructura crítica de todo un país con la afectación de servicios

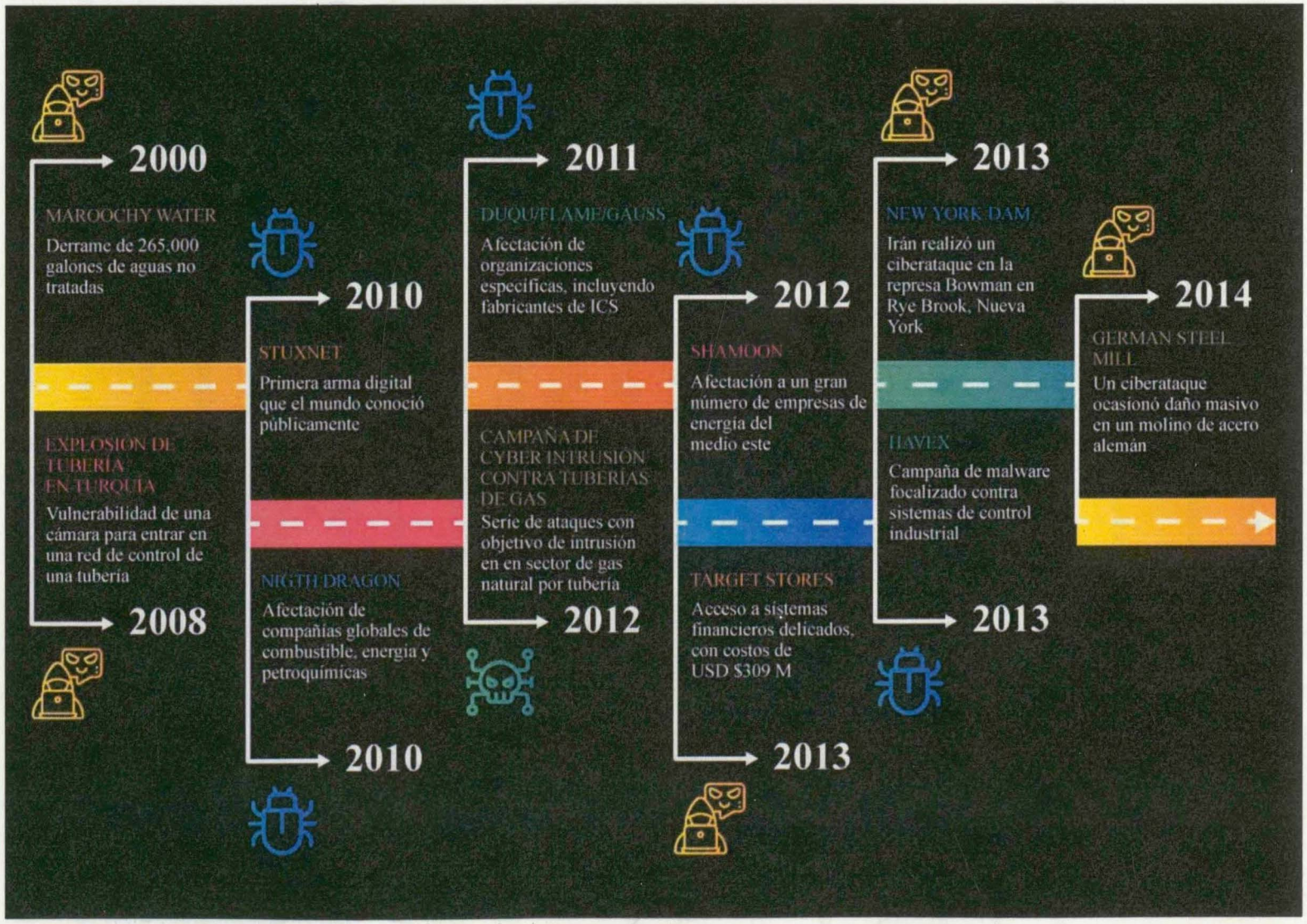
esenciales. Esto corroboró también como lo hizo Stuxnet en su momento, que el simple hecho de tener sistemas aislados de otras redes o de internet, no significa que sean seguros o estén protegidos o que sean más seguros que otros sistemas interconectados o en red.

Una nueva evidencia de ciberataques altamente planeados con el objetivo de indisponer la disponibilidad de una infraestructura crítica se materializó en el apagón del sistema eléctrico ucraniano. El mundo no había experimentado antes o al menos ninguna empresa de electricidad había aceptado públicamente, que habían tenido un apagón por causa de un ciberataque y mucho menos que había sido blanco de un plan organizado y altamente coordinado para dejar sin electricidad a todo un país por muchas horas.

El ciberataque realizado al sector eléctrico de Ucrania el 23 de diciembre del 2015, impactó específicamente a sus sistemas de distribución de energía, afectando 7 subestaciones eléctricas de 110 kV y 23 de 35 kV dejando sin servicio de electricidad a más de 225.000 usuarios por más de 8 horas, (SANS, 2016, pág. 4). Estos hechos son una evidencia de la materialización de los riesgos cibernéticos que enfrentan los sistemas de control industrial. Estos sistemas permiten la operación centralizada y las funciones de control sobre infraestructuras específicas, en las cuales se soportan servicios esenciales para los ciudadanos, los países y sus estados, las cuales por las razones antes enunciadas se han denominado por muchos gobiernos como infraestructuras críticas – IC.

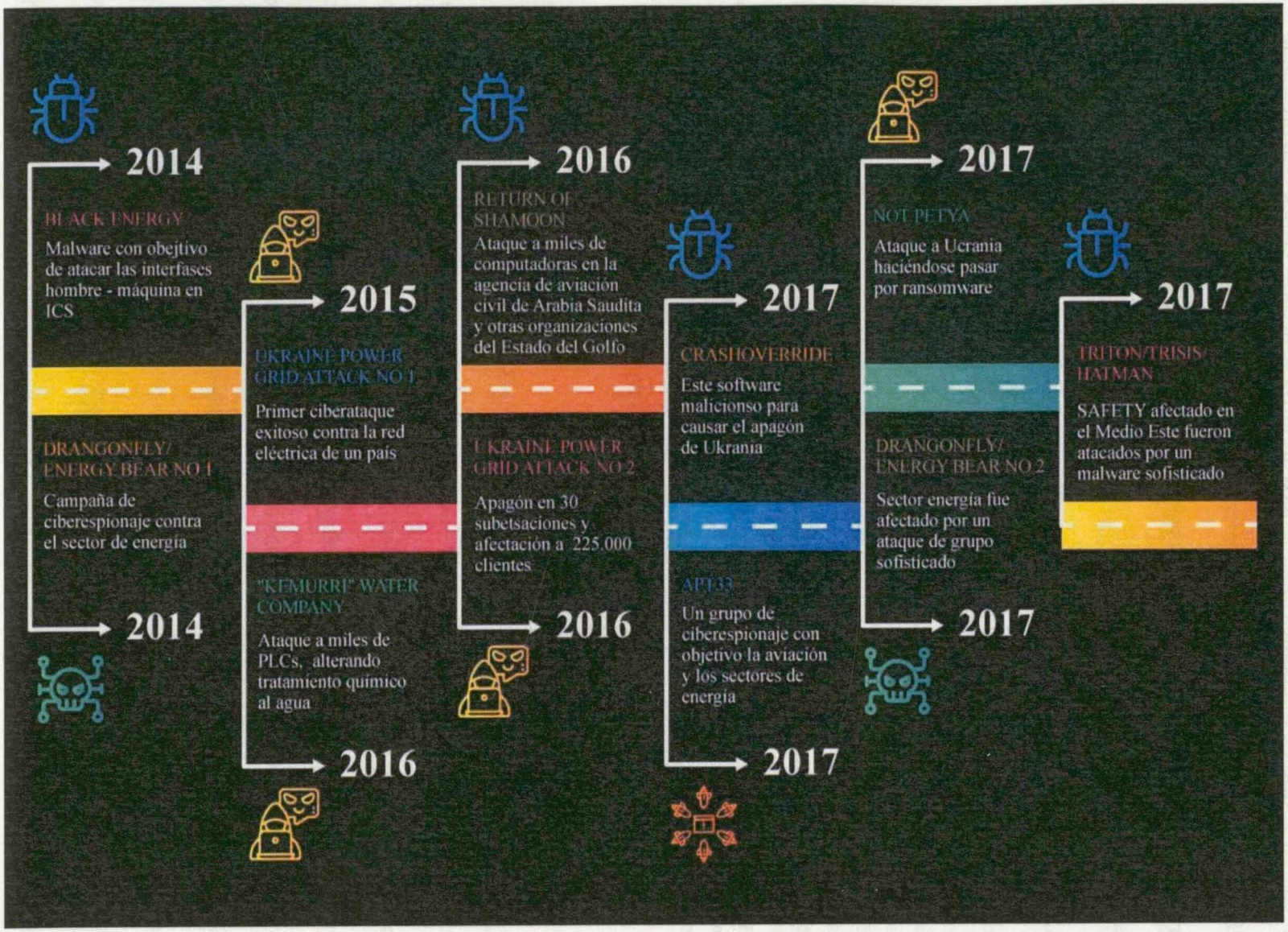
A continuación, se presenta la línea de tiempo de algunos de los ciberataques más relevantes o conocidos perpetrados en sistemas de control industrial.

Gráfica 2. Línea de tiempo ciberataques en ICS.



Elaborado con base en (Hemsley & Fisher, 2018, pág. 2)

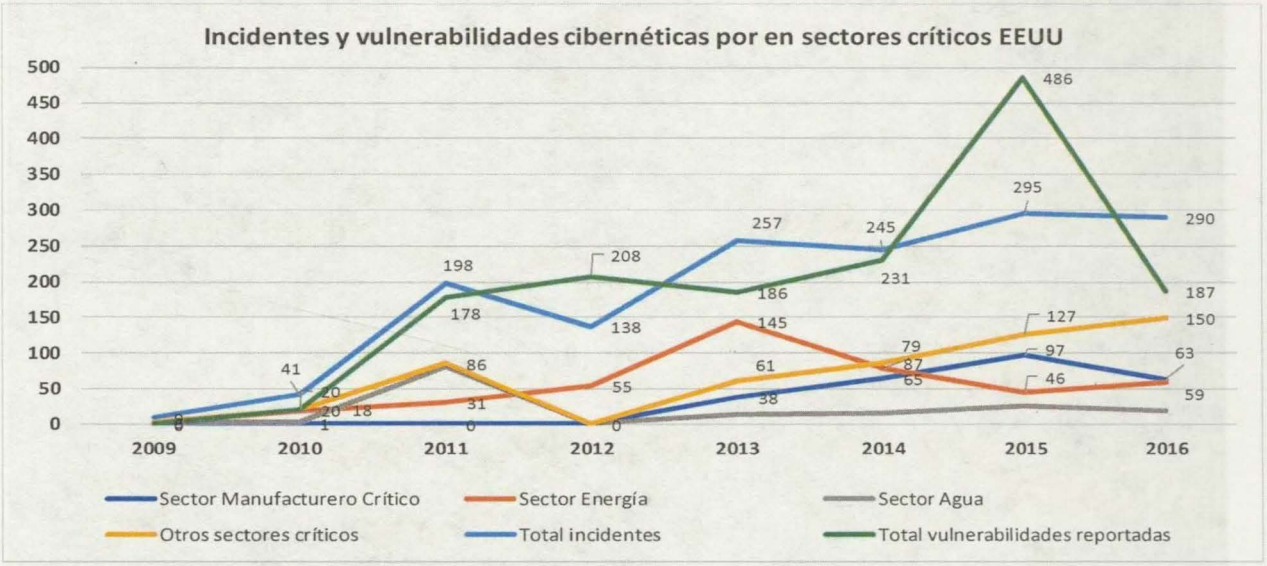
Gráfica 3. Línea de tiempo ciberataques en ICS.



Elaborado con base en (Hemsley & Fisher, 2018, pág. 3).

En cuanto al tipo de incidentes cibernéticos en infraestructuras críticas, se presentan las estadísticas relacionadas con la evolución en el número de incidentes por año según los informes del Equipo de Respuesta a Emergencias Cibernéticas en Sistemas de Control Industrial de los Estados Unidos.

Gráfica 4. Incidentes y vulnerabilidades en Sistemas de control Industrial.



Elaborado a partir de (ICS CERT, 2016, pág. 24), (ICS CERT, 2015, pág. 17), (ICS CERT, 2014, pág. 19), (ICS CERT, 2013, pág. 16), (ICS CERT, 2012, pág. 12), (ICS-CERT, 2011).

En la gráfica se puede apreciar que tanto las vulnerabilidades a los sistemas de control industrial como los incidentes a los sistemas de control industrial de los sectores críticos pertenecientes a Estados Unidos presentan una tendencia creciente. En el período mostrado se identifica que el pico de incidentes en el sector de agua se presentó en el año 2013, mientras que en el sector energía se presentó en el año 2013.

Un estudio realizado por los autores (Schwab & Poujol, 2018, pág. 6) en nombre de la firma Kaspersky Labs basado en una encuesta CATI de 320 profesionales en todo el mundo, muestra que, el 77% de las compañías encuestadas que utilizan sistemas de control industrial,

manifestaron que su mayor prioridad de negocio es la ciberseguridad de OT en sistemas de control industrial.

Así mismo, estas empresas manifestaron que la mayor preocupación frente a un incidente de ciberseguridad en sus sistemas de control industrial es la consecuencia de los daños sobre la calidad de los productos o servicios, seguido del posible daño o muerte a sus empleados, pérdida de la confianza del cliente, seguida de la afectación a la marca o reputación, entre otros.

El mismo estudio plantea que la evolución de las redes inalámbricas y los SCADA en la nube son una realidad que está permeando los sistemas de control industrial debido a los beneficios que prometen, pero que no se debe dejar de lado los riesgos de interceptación de datos y e instrucciones de control.

3.3.1. Infraestructuras Críticas.

Los países desarrollados y tecnificados son más sensibles a las consecuencias de fallos en estas infraestructuras esenciales, porque dependen más de sistemas computacionales para su operación y funcionamiento. Países como los pertenecientes a la comunidad europea, han tomado la iniciativa de la identificación, designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, como lo determina la Directiva 2008/114/CE (Consejo de la Unión Europea, 2020, pág. 75), la cual establece a sus estados miembros y a los propietarios u operadores de las mismas, la responsabilidad de proteger sus infraestructuras críticas - IC y los insta a emprender iniciativas para su protección y establece los requerimientos mínimos que debe cumplir el plan de seguridad del operador de infraestructura crítica. En este sentido la Directiva en mención define las IC como: "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 y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones".

Los Estados Unidos a través de su gobierno federal, desde mediados de los años 90's cuenta con directivas, leyes, lineamientos y políticas para la protección de sus infraestructuras críticas, entendidas éstas como: "aquellas que son vitales para defensa nacional, económica, la seguridad y salud pública y el aseguramiento del funcionamiento de los servicios de la sociedad", como lo referencia (U.S. General Accounting Office, 2004, pág. 3) en su informe Evaluación de Tecnológica, Ciberseguridad para Infraestructuras Criticas.

El mismo autor referencia que EE. UU. definió 13 sectores de infraestructuras críticas dentro de los cuales se encuentran entre otros el sector Energía, entendida ésta como la provisión de potencia eléctrica a todas las infraestructuras del país, tanto a las críticas como a las no críticas. Dentro de otros sectores definidos como críticos se encuentran, la provisión de agua para el consumo y los sistemas de tratamiento, el sector gobierno, tecnologías de información y telecomunicaciones, cuidado y salud pública, sector químico, industria de producción militar.

En la misma línea el presidente Obama en el año 2013 en su orden presidencial (The White House, 2013, pág. 1) plantea que las ciber amenazas a las infraestructuras críticas es uno de los más serios cambios que deben enfrentar y que la seguridad nacional y la economía de los Estados Unidos dependen del confiable funcionamiento de sus infraestructuras críticas y enfocó la política de EEUU a mejorar la resiliencia y la seguridad de las mismas. Así mismo la

directiva presidencial President Issued Presidential Policy Directive PPD-21 (Obama Administration, 2013, pág. 2) expedida en febrero del mismo año, es un llamado a la actualización la protección de las infraestructuras de la nación a nivel de operadores y propietarios desde la seguridad y resiliencia, entendiendo la gestión integral del riesgo y basado en la criticidad de los activos, sistemas y redes y la interdependencia de las IC.

La misma orden plantea que la política establecida se puede lograr a partir de un trabajo mancomunado y colaborativo entre propietarios y operadores de infraestructura crítica para mejorar el intercambio de información sobre seguridad cibernética, desarrollando e implementando de manera colaborativa, estándares basados en el riesgo, a la vez que establece lineamientos para la coordinación entre entidades gubernamentales, públicas y privadas. Así mismo, (The White House, 2013, pág. 11) redefine las infraestructuras críticas como: "sistemas y activos, ya sean físicos o virtuales, tan importantes para Estados Unidos que la incapacidad o destrucción de dichos sistemas y activos tendrían un impacto debilitante en la seguridad, económica nacional, salud pública nacional o seguridad, o cualquier combinación de estos asuntos".

Este mandato también incluye la construcción de un marco de referencia en ciberseguridad para reducir los riesgos cibernéticos de las infraestructuras críticas, el cual fue encomendado al director del National Institute of Standards and Technology – NIST. Este marco de referencia incluye un conjunto de estándares, metodologías, procesos y procedimientos alineados a la política, negocios y enfoque tecnológico que direccionan los riesgos cibernéticos.

Un elemento importante a resaltar es que la política de EEUU (The White House, 2013, pág. 12) en este aspecto, está enfocada a incrementar la confiabilidad de sus IC basadas en dos

aspectos; la protección de sus infraestructuras críticas, entendida esta desde un aspecto físico, virtual e incrementando la resiliencia de estas infraestructuras, entendida esta como: "La capacidad de prepararse y adaptarse a las condiciones cambiantes y resistir y recuperarse rápidamente de las interrupciones ... incluye la capacidad de resistir y recuperarse de ataques deliberados, accidentes o amenazas o incidentes naturales".

Autores como (Labaka, Hernantes, & Sarriegi, 2015, pág. 410), en su revisión del estado del arte relacionado con la resiliencia, plantean que existen casi tantas definiciones de resiliencia como autores, pero que en general se pueden encontrar definiciones en dos tipos de perspectivas; la primera está relacionada con la capacidad de recuperarse a un estado normal después del impacto de un evento desencadenante, citando autores dentro de su estudio como (Mileti, 1999; McEntire, 2005); el segundo tipo de definición está relacionada con la capacidad para hacer frente a una crisis que ocurre y para evitar que ocurra un evento desencadenante, como lo plantean autores citados (Bruneau et al., 2003; Seville et al., 2008; Hollnagel et al., 2006).

Siguiendo la segunda perspectiva el mismo autor plantea la resiliencia como: La "capacidad de un sistema para prevenir una ocurrencia de crisis y, si un evento impacta el sistema, la capacidad del sistema para absorber el impacto y recuperarse rápidamente".

Los mismos autores afirman que existe un ciclo de vida de la resiliencia resumido en tres estados: prevención, absorción y recuperación, volviendo a la primera fase de prevención y que el seguir la segunda perspectiva como lo plantea (Bruneau et al., 2003), citado por (Labaka, Hernantes, & Sarriegi, 2015, pág. 410), traen consigo un modelo de capacidades que deben desarrollarse para alcanzar un nivel adecuado de resiliencia, como son la resiliencia técnica, la resiliencia organizacional, la resiliencia económica y la resiliencia social. Así

mismo plantea que es necesario crear políticas para cada uno de los cuatro aspectos antes mencionados y que debido al aumento significativo del número de actores que se involucran en una crisis, se requiere también de un manejo integrado y una alta coordinación con entidades externas, sumado a una alineación de las políticas a través de todos los involucrados.

Así mismo, (Rinaldi, Peerenboom, & Kelly, 2001, pág. 12), sustentan que las infraestructuras críticas son sistemas complejos, altamente interconectados, basados en sinergias y dependientes mucho más allá de lo físico, el intercambio de información o las telecomunicaciones. Plantean que la complejidad de dichas relaciones e interdependencias incluyen lo técnico, lo legal y regulatorio, económico, negocio, social/político, política pública, salud, seguridad, y que el modo como son conectadas y lo fuerte de sus conexiones, afectan e imponen retos para la misma operación de las mismas IC, frente a eventos de fallos comunes, fallos en cascada, entre otros.

Definen la dependencia como un vínculo o conexión entre dos infraestructuras a través del cual el estado de una infraestructura afecta o es correlacionada con el estado de la otra. Introducen también el término interdependencia cuando la dependencia es en ambos sentidos; normalmente estas se dan en sistemas de sistemas, como también lo menciona NIST 800-62r2 (NIST, 2015, págs. 3-7). Los autores plantean seis aspectos desde donde pueden ser entendidas.

Gráfica 5. Dimensiones para describir las interdependencias en infraestructura

Elaborado a partir de (Rinaldi, Peerenboom, & Kelly, 2001, pág. 12).

Estos autores también sostienen que las IC son colecciones complejas de componentes en continua interacción y cuyos cambios son a menudo el resultado de aprendizaje de procesos, por lo cual los llaman sistemas adaptivos complejos (CAS) por sus siglas en inglés, los cuales se basan en la experiencia pasada y han incorporado sistemas de computación para soportar funciones de tiempo real con el fin de incrementar su desempeño, por ejemplo, en el ajuste de generadores ante variaciones de potencia en la carga.

Específicamente los mismos autores plantean que el sector eléctrico tiene diferentes interdependencias con el sector de: telecomunicaciones, gas, suministro de combustible, transporte, agua, entre otros. Explican en (Rinaldi, Peerenboom, & Kelly, 2001, pág. 13) como la confiabilidad en el suministro de energía en el sector eléctrico, no se logra solamente por la

agregación de componentes como generadores, líneas de transmisión, redes de distribución, que simplemente se conectan y plantean que: "Solo la creación cuidadosa de un conjunto de servicios integrales se convertirá en un sistema que de manera confiable y continua suministra electricidad ".

3.3.2. Sistemas de Control Industrial y Sistemas de Información Corporativos.

El sector eléctrico basa su funcionamiento en las prestaciones de los sistemas de control industrial o Industrial Control Systems - ICS por sus siglas en inglés, los cuales realizan funciones de supervisión, control, protección de infraestructura de prestación de servicios, las cuales permiten realizar la operación local y centralizada de los sistemas de generación, transmisión y distribución de energía desde un centro de control.

Hay muchas similitudes entre los sistemas SCADA y los ICS, en general los dos términos son utilizados, pero normalmente en infraestructuras críticas, los Distribution Control System o DCS trabajan en red a los sistemas SCADA.

Según (NCS, 2004, pág. 10), la evolución de los sistemas SCADA ha estado íntimamente ligada a la evolución tecnológica de los sistemas de computación. Si se analiza su evolución desde el punto de vista de su arquitectura se pueden identificar tres generaciones. Como ya se mencionó en su primera generación los sistemas SCADA eran sistemas monolíticos, con un ordenador principal o mainframe, el cual no se conectaba con otras redes, dado que estas no existían. Así mismo las redes WAN (Wide Area Network) existían únicamente para conectar los sistemas SCADA a los dispositivos RTU o (Remote Terminal Unit), estos últimos son equipos de campo que habilitan la interacción con el proceso. Los protocolos para esta comunicación fueron generalmente protocolos propietarios desarrollados por vendedores de

RTU's, las cuales, si bien permitían una optimización de comunicaciones de tráfico de tiempo real, no permitían la comunicación con otras marcas u otros fabricantes.

Una segunda generación corresponde a los SCADA distribuidos, los cuales aprovecharon la miniaturización de componentes y el desarrollo tecnológico de las redes LAN (Local Área Network) para la distribución del proceso a través de múltiples sistemas. Varias estaciones de procesamiento se instalaron cada una con una función específica, las cuales fueron comunicadas por una red LAN, y servían para recibir las comunicaciones del proceso, como interfaz del operador. Autores como (Ujvarosi, 2016, pág. 66) resalta en su trabajo algunas ventajas de los sistemas distribuidos frente a los sistemas monolíticos de primera generación, entre los cuales está el aumento de capacidad de procesamiento e incremento en la disponibilidad, al contar con varias máquinas distribuidas y la flexibilidad de operar un sistema desde una Interfaz Hombre Máquina - HMI por sus siglas en inglés, bien sea desde una máquina principal o una máquina subordinada.

El crecimiento continuo de la industria, los procesos automatizados, el crecimiento de equipos industriales y la aparición de múltiples vendedores o fabricantes, ocasionaron la aparición de la siguiente generación de sistemas SCADA. Autores como (Ujvarosi, 2016, pág. 65) y (NCS, 2004, pág. 12) coinciden que la tercera generación de SCADA está íntimamente ligada a la segunda generación, excepto por la diferencia de integrar diferentes marcas. Podría decirse que la gran diferencia de la tercera generación fue la de utilizar una arquitectura abierta del sistema, utilizando protocolos de comunicación estándares y abiertos con el objetivo de utilizar las funciones de SCADA no solo en la LAN sino en la WAN, lo cual permitió desarrollar funciones en red adicionales en los SCADA y mejorar la disponibilidad del sistema frente a fallas generales.

Uno de los factores que permitió la masificación en el uso de los sistemas SCADA fue el empleo de protocolos IP y conexiones Ethernet, lo cual permitió una conexión entre una estación maestro y sus periféricos. Así mismo, (NCS, 2004, pág. 13), argumenta que la evolución hacia protocolos estándar, hizo que los fabricantes de SCADA, abandonaran la fabricación de hardware y empezaran a utilizar plataformas de computación básica como COMPAQ, Hewlett-Packard y Sun Microsystems y software de sistemas operativos, enfocándose en agregar valor en la componente SCADA en su software de estación maestra o central. Esta apertura hacia protocolos estándar, su conectividad en red, sumado a las vulnerabilidades de las mismas tecnologías, han incrementado su susceptibilidad a ataques cibernéticos.

La sociedad moderna ha experimentado en muy pocos años grandes avances tecnológicos, entre los cuales se encuentran la ampliación de las telecomunicaciones pasando de protocolos industriales propietarios al uso de redes IP en diferentes entornos industriales, comerciales y residenciales, a través de diferentes tecnologías que están orientadas a la interoperabilidad.

Esta evolución y el uso de protocolos estándar, que tradicionalmente han sido utilizados principalmente por las redes de telecomunicaciones y las tecnologías de información, han sido incorporadas por los fabricantes de artefactos de control industrial, en primera instancia al emplear hardware que permite la ejecución del sistema SCADA, las redes de telecomunicaciones WAN e incluso en los concentradores e interfaz hombre HMI de subestaciones, lo que está ocasionando lo que se ha denominado la convergencia de tecnologías de TI y TO, al utilizar el mismo hardware y sistemas operativos comerciales tradicionalmente utilizados en TI, para ahora ser utilizados como base del funcionamiento de aplicaciones de control industrial.

Esto mismo lo corrobora el documento Proceso de Gestión del Riesgo de Ciberseguridad en el subsector del Energía del Departamento de Energía (DOE,2012), el cual plantea que los ICS tradicionalmente fueron sistemas aislados y de tecnologías propietarias cerradas que en búsqueda de eficiencias en costos, han ido incrementando su dependencia de sistemas digitales y la incorporación de sistemas de libre comercio en hardware y software conocidos como COTS (Comercial of the Shelf), interconectando redes públicas y privadas y proporcionando gestión remota, sumado a la alta integración de información de sistemas de gestión de negocios que apoyan la toma de decisiones y los sistemas de control industrial bajo el concepto Smart Grid.

El uso de COTS utilizados ampliamente en hogares, por las empresas en ofimática, ahora empleados en los sistemas de control, han traído economías en reducción de costos y el desarrollo de aplicaciones de control y operación que funcionan bajo sistemas operativos comerciales como Windows, Linux, entre otros, estas prácticas han trasladado los riesgos y vulnerabilidades cibernéticas a este nuevo dominio de control industrial.

El National Institute of Standards and Technology - NIST en su guía de ciberseguridad para sistemas de control industrial 800-82R, muestra como las Tecnologías de Información tienen como premisas dentro de la protección de la seguridad, la confidencialidad, la integridad y la confiabilidad, mientras que los Sistemas de Control Industrial están enfocados a la disponibilidad como primera preocupación. Estos criterios tienen sentido si se tiene en cuenta que los sistemas de control industrial se diseñaron para controlar variables de procesos que soportan el funcionamiento de infraestructuras críticas y su prioridad es la continuidad de los servicios que se prestan.

Estos dos tipos de tecnologías si bien han ido evolucionando hacia el uso de artefactos comunes, tienen grandes diferencias desde lo misional y los dominios especializados que manejan. El siguiente cuadro muestra las diferencias en la especialización y el soporte de las diferentes tecnologías:

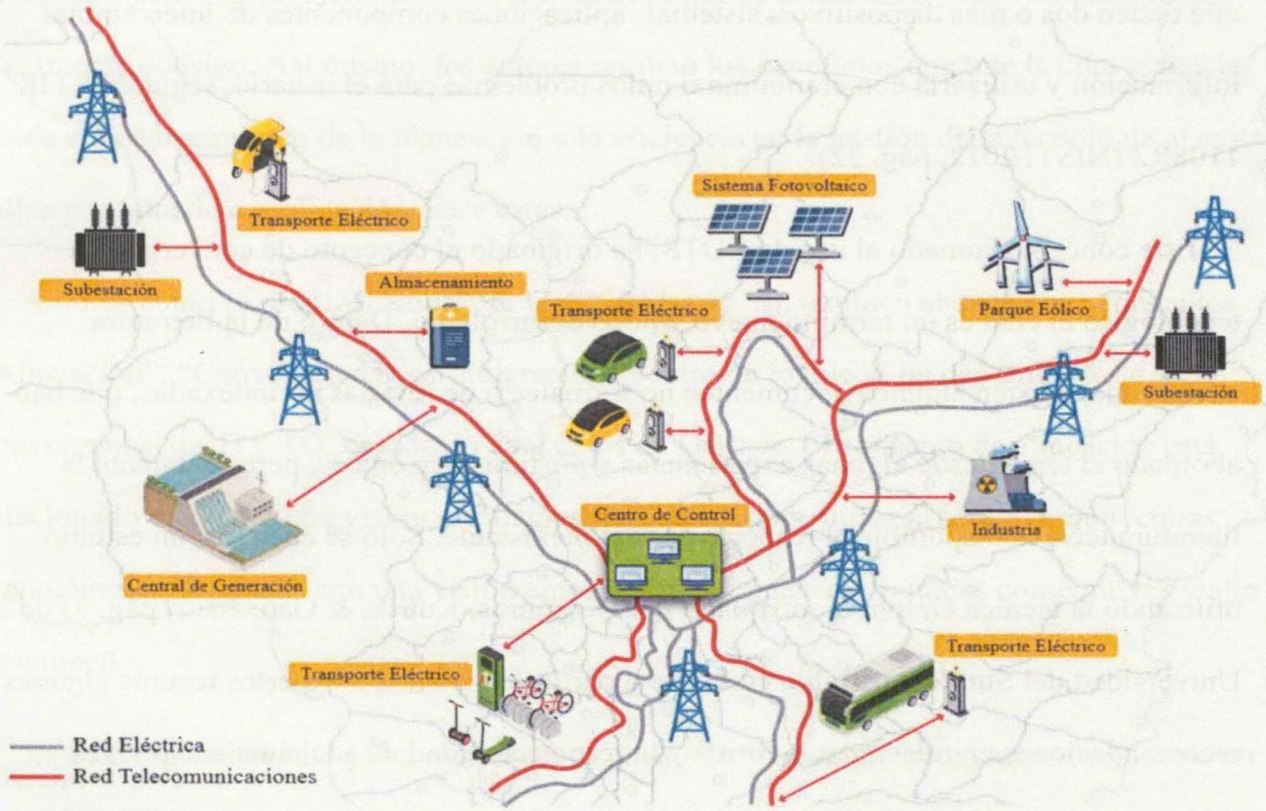
Tabla 1. Diferencias en el soporte de tecnologías de información y tecnologías de operación.

ITEM	TI	TO
CICLOS DE VIDA ACTIVOS	Menores a 5 años	Mayores a 10 años,
FORMACIÓN	Profesionales en sistemas: Ingeniería de sistemas, ingeniería de información, etc.	Profesionales en ingeniería: sistemas, control, protecciones, electrónicos, eléctricos, entre otros.
UBICACIÓN PERSONAL	Siempre en oficina, cerca a las áreas Administrativas.	En campo y en la oficina dentro de las sedes y áreas Operativas.
AMBIENTE OPERATIVO	Data Center y oficinas.	Centros de Control. Equipos dispersos sobre la infraestructura lineal de los negocios, en ambientes expuestos al polvo y la humedad. Procesos de planta y subestaciones.
INNOVACIÓN	Alta.	Baja
PRIORIDAD - SEGURIDAD	Confidencialidad de la información.	Confiabilidad del activo y el servicio.
HABILIDADES DEL PERSONAL	Constantemente actualizado. Maneja lo último en tecnología.	"Adoptante tardío". Altamente especializado y maneja tecnología legada y grandes retos en interoperabilidad.
PERFIL DE LAS PERSONAS	Jóvenes recién salidos de la Universidad conocimientos actualizados.	Personas mayores con mucha experiencia en campo, conocimiento del negocio e infraestructura.
TIPO CONTRATACIÓN	Tiende a tercerizar, muchas empresas prestan estos servicios que son estandarizados.	Personal propio por el conocimiento, cultura tecnologías legadas, complejidad del sistema, trabajo bajo presión.
PROPÓSITO	•Procesamiento de datos del negocio. •Análisis y aplicaciones transaccionales. •Soporte a las decisiones administrativas o comerciales de negocio.	•Proceso de adquisición de datos, análisis y control. •Seguridad del proceso.
ENTRADA DE DATOS	Manual, otros sistemas de TI.	•Datos de procesos de planta, estación o infraestructura lineal de prestación del servicio. •Operador desde la Interfaz hombre –máquina.
SALIDA DE DATOS	Reportes de resumen, análisis etc.	•Comandos de control hacia equipos de planta, estaciones. •Visualización en HMI (alarmas, errores, eventos, posiciones de elementos de control, tendencias, fluidos y servicios en tiempo real). •Información de monitoreo de variables controladas. •Desconexiones, fallos, paros de emergencia, interrupciones, alertas.
CULTURA	Personal de oficina, con ANS para atención en horario no hábil, poco conocimiento de la operación.	•Alta Conciencia Situacional y compromiso con la disponibilidad. El impacto por las afectaciones son costosas, incumplimiento regulatorio, ingresos, servicio, integridad de activos y vida humana. •Personal de campo, tiene la misma cultura del personal de control, protecciones y operación, disponibilidad 7x24.

Elaborado a partir de (Taylor, 2012, pág. 25).

Según la IEC 62351 – 10, (IEC, 2012, pág. 9) a medida que avanza la automatización de diferentes subestaciones, la operación manual con personas en cada subestación eléctrica desaparece y es remplazada por la operación centralizada o remota, por lo que la confiabilidad del sistema de potencia depende de la confiabilidad del sistema de información, responsable por integrar información de dispositivos de campo y aún más enviar comandos de telecontrol desde el centro de control hacia las subestaciones.

Gráfica 6. Sistemas Potencia y Sistemas de Información - Gestión de dos infraestructuras



Elaborado a partir de (IEC, 2012, pág. 9)

3.3.3. Smart Grid, IoT y Convergencia Tecnológica.

Este concepto contemporáneo desarrollado en el sector eléctrico a nivel mundial llamado Smart Grid o red inteligente, busca fundamentalmente incrementar la eficiencia y disponibilidad de los servicios de la red de distribución de energía, mediante la incorporación de tecnologías de información y telecomunicaciones para incrementar la inteligencia o capacidad de los dispositivos, tomar mejores decisiones basados en una mayor cantidad de información procesada y el concepto de interoperabilidad, entendida esta como la capacidad que tienen dos o más dispositivos, sistemas, aplicaciones componentes de intercambiar información y utilizarla con el mínimo o nulos problemas para el usuario, según NISTIR 1108R2 (NIST, 2012, pág. 22).

Este concepto sumado al uso de COTS, ha originado el concepto de convergencia tecnológica el cual es un término nuevo y poco desarrollado. Dentro de la literatura encontrada, existen algunos documentos no formales o de revistas no indexadas, que han abordado el tema desde algunas experiencias y posturas personales, pero realmente la literatura técnica disponible al respecto es casi inexistente. Solo se encontró un estudio utilizando la técnica Delphi desarrollado por (Koronios, Kuusk, & Gao, 2017, pág. 3) de la Universidad del Sur de Australia, en la que a partir de consulta a expertos resume algunas recomendaciones en relación a la forma y la responsabilidad de adelantar acciones de convergencia tecnológica en una compañía.

El mismo trabajo enfatiza que la convergencia tecnológica es un término y un fenómeno relativamente nuevo, por lo que no hay bibliografía formal, ni experiencias documentadas de los casos de éxito y no se conocen las implicaciones, riesgos y el camino para realizar esta convergencia tecnológica en las empresas de manera óptima y eficiente.

Autores como (Paes, Mazur, Venné, & Ostrzenski, 2017, pág. 89), plantean que dentro del tema de la convergencia tecnológica existe otra revolución que está sucediendo y relacionada con Internet de las Cosas - IoT por sus siglas en inglés, entendida esta como la capacidad de comunicar, intercambiar información y controlar dispositivos domésticos e industriales a través de redes IP. En relación a esto, dichos autores argumentan que la visión de seguridad debe darse a lo largo de toda la compañía, incluyendo todos estos nuevos artefactos tecnológicos. Las concepciones de seguridad deben incluir no solo las tecnologías legadas o heredadas, sino el gran incremento de dispositivos que se conectarán y las vulnerabilidades que traerán consigo. Así mismo, los autores resaltan los beneficios que trae la convergencia desde el fortalecimiento de la planeación y la eficiencia en la gestión de la tecnología al evitar fallos por falta de coordinación entre estas.

Autores como (Koronios, Kuusk, & Gao, 2017, pág. 3), también abordan tres conceptos "Alineación", "Convergencia" e "Integración" dentro de lo que se ha denominado la convergencia de TI y TO, basado en conceptos de Gartner. El concepto de alineación está relacionado con tener una visión estratégica de Tecnologías, infraestructura, arquitecturas tecnológicas, planeadas con una visión empresarial para generar ventajas competitivas y alto desempeño.

La convergencia como ya se mencionó es el uso de hardware común, antes propios de un solo dominio para convertirse en transversal. El documento plantea que "Las organizaciones deben planificar la convergencia cuando existan factores externos tales como una visión corporativa y estándares consolidados de la industria". En cuanto al concepto de integración datos e información, tecnologías y actividades de TI y TO, el documento plantea que el

direccionador para este es la productividad, cuando se presenten oportunidades de capturar ahorros en costos que sean crecientes.

Esta visión de convergencia e integración de tecnologías hacia las mismas aplicaciones y hardware que cita el documento basado en conceptos de Gartner, difiere de los principios de ciberseguridad establecidos por la IEC y NIST, en el sentido de tener dominios separados para entornos de sistemas de control industrial y los sistemas corporativos tanto a nivel físico de equipos como a nivel lógico a través de redes virtuales, como lo establece la IEC 62264-1 Anexo página A.2

3.3.4. Enfoque de la seguridad en sistema de información y sistemas de control.

- **Sistemas de Información Corporativa.**

Según la definición del término seguridad información, consiste en: "preservar la confidencialidad, integridad y disponibilidad de la información y puede incluir entre otras la autenticidad, no repudio, trazabilidad y confiabilidad". Fuente: ISO 27000 p.4.

Según la IEC 27002 (2005) citado por (Solms & Niekerk, 2013, pág. 98), esta definición incluye tanto la información impresa o escrita en papel, como la almacenada electrónicamente, transmitida por o a través de medios electrónicos. De acuerdo con los autores (Whitman and Mattord, 2009, pág. 8) citado por los mismos autores, asegurar la confidencialidad, integridad y disponibilidad de información, también ha sido conocido como el triángulo CIA por sus siglas en inglés y es considerado como un estándar de industria.

Plantean los autores (Solms & Niekerk, 2013, pág. 98), que la seguridad de la información tradicionalmente se ha visto solo como un asunto técnico a resolver, no siendo un producto,

una tecnología o algo que se pueda comprar, pero si es un proceso que debe gestionarse. En relación con las prácticas relacionadas con la seguridad de información o seguridad en tecnologías de información, existe una serie de normas ampliamente conocidas, relacionadas con la familia de la ISO 27000, cuyo alcance es la implementación de un Sistema de Gestión de Seguridad de la Información en cualquier organización. Este sistema se entiende, como el conjunto de políticas, procedimientos, guías, recursos y procedimientos, gestionados colectivamente para proteger sus activos de información (ISO/IEC, 2018).

Con base en estos estándares, las organizaciones pueden desarrollar e implementar un marco para administrar la seguridad de la información de sus activos cualquiera que sea su naturaleza o actividad, incluida la información financiera, la derivada de la propiedad intelectual y los empleados, o la información entregada por estos a terceras partes, como lo establece la misma (ISO/IEC, 2018).

Específicamente la ISO 27019/2017 (ISO, 2017, pág. 31), está enfocada en plantear los controles que debe tener una empresa prestadora de servicios de la industria energética. Para ello la norma cita los controles de la ISO 27002 (ISO/IEC, 2012), en cuanto a sistemas de información se refiere; en relación a los controles de seguridad para los sistemas de control industrial para estas empresas de servicios o utilities, establece que se deben seguir las normas, estándares, prácticas técnicas y recomendaciones de los organismos especializados y encargados en la normalización de los sistemas de control, en este caso la IEC, ISA, NERC-CIP, entre otras.

Como se puede observar, la seguridad de la información ha tenido un enfoque organizacional, de procesos, política y controles para proteger sistemas transaccionales o aplicaciones informáticas de negocio y en el campo de las medidas de seguridad en sistemas

de control las normas ISO delegan estas responsabilidades a los organismos especializados de estos dominios.

- **Sistemas de Control industrial**

Los sistemas de control industrial tienen la función específica de "controlar procesos industriales para la fabricación y distribución de productos y en sectores de infraestructuras críticas, que pueden estar geográficamente dispersos", como lo establece (NIST 2013) Apéndice B pág.9 en su documento NIST SP 800-53 Rev. 4.

El enfoque de los sistemas de control es realizar una función específica, lo cual obliga a que estos sistemas se conciban para cumplir requerimientos específicos desde su diseño, desempeño, su arquitectura, características técnicas específicas de sus componentes, para cumplir requerimientos específicos y condiciones específicas del proceso productivo, los cuales deben funcionar bajo el concepto safety o libre de riesgos no tolerable o aceptable, con altas restricciones a retardos en tiempo real de transmisión de datos, de 1 milisegundo como lo expone la norma ANSI/ISA–62443-1-1 (99.01.01)–2007 pág. 36.

Algunos autores como (Drias, Serhrouchni , & Vogier, 2015, pág. 4) plantean que los sistemas de control industrial son sistemas de información que difieren mucho del mundo de los sistemas tradicionales de TI, fundamentalmente porque tienen muchas características funcionales únicas, incluida la necesidad de respuesta en tiempo real y la extremada alta disponibilidad, predictibilidad, confiabilidad, así como una inteligencia distribuida. En su trabajo muestran componentes, arquitecturas, protocolos industriales, mostrando que la disponibilidad e integridad son atributos esenciales.

El estándar Integración de Sistemas Empresariales y Sistemas de Control. Modelos y Terminología IEC 62264-1, (IEC, 2013, pág. 17), define la jerarquía genérica que tienen los sistemas de control dentro de una organización, en una gran industria o en una planta de producción convencional. Este estándar muestra que en la organización existen fronteras claramente establecidas entre los sistemas de información y los sistemas de control, estos tienen especificaciones y restricciones diferentes y sus funcionalidades operan en dominios diferentes y que su relación está basada en intercambios de flujos de información de interés entre estos dominios.

En cuanto a la aplicación de controles en los sistemas de control industrial, autores como (Park & Lee, 2014, pág. 1) plantean que si bien, es apropiado aplicar un sistema de gestión de seguridad de la información en una organización, específicamente los sistemas de control tienen otros atributos más críticos a proteger como Safety o el aseguramiento. Este es el atributo más crítico en los sistemas de control, fundamentado en los requerimientos definidos por los estándares IEC 61508 para los fabricantes y suministradores de equipos industriales y en la IEC 61511 para los diseñadores, integradores y usuarios de sistemas de control.

Estos mismos autores plantean que los requerimientos y controles de ISO 27001 y la NIST 800-53 están basados en la confidencialidad, integridad y disponibilidad, y que estas normas abarcan solo una parte de aseguramiento o safety que es diferente al aseguramiento que establece la IEC 61511 para el aseguramiento de los sistemas de control. En su trabajo en su página 7, demuestran que solo cerca del 15% de los controles de seguridad ISO 27001 y el 16,49% de NIST 800-53, satisfacen los requerimientos de aseguramiento de la IEC 61511.

La siguiente tabla muestra un resumen de la comparación de servicios y requerimientos de seguridad cibernética entre redes de ofimática y ambientes de control, específicamente en el sector energía.

Tabla 2. Comparación de requerimientos de seguridad en sistemas de potencia y redes corporativas.

Requerimientos de seguridad	Sistemas de energía	Sistemas de información corporativos
Atributos a proteger	Disponibilidad e integridad de la información del estado del proceso controlado y los comandos de control enviados al proceso.	Confidencialidad, integridad y disponibilidad de la información de negocio o comercial.
Aplicación de antivirus	Difícilmente se pueden aplicar por riesgos de afectación del proceso.	Comúnmente aplicados.
Aplicación de parches de seguridad	Sólo en casos específicos, probados y aprobados por el fabricante del sistema.	Programados permanente.
Vida útil de los componentes tecnológicos	Entre 10 y 30 años.	Entre 3 y 5 años.
Requerimientos de tiempo real	Retardos no son aceptables porque ponen en riesgo el aseguramiento del proceso o SAFETY. Crítico funciones de teleprotecciones de líneas de Tx.	Retardos aceptados sin afectación del proceso.
Integración tecnológica y de servicios	No combinación de redes, equipos del dominio de control de tiempo real con redes u otros servicios corporativos.	Muchos servicios comparten la misma infraestructura.
Disponibilidad/confiabilidad del servicio	Criticidad muy alta. Servicio 7x24x365 días al año, regulado y penalizado con indicadores de calidad.	Criticidad media, retardos aceptados.

Elaboración basada en IEC62351-10 e IEC 1947/12

3.3.5. Diferencias entre el término Seguridad y Aseguramiento o Safety.

El concepto de Safety es ampliamente utilizado para el diseño y funcionamiento de los sistemas de control. El estándar IEC 61511-1 Functional safety – Safety instrumented systems for the process industry sector, aborda todas las funcionalidades relacionadas con el concepto Safety. Este se centra en garantizar una alta disponibilidad de los activos operados bajo un concepto de automatización, protegiendo la integridad de los mismos frente a fallos, las personas y el medio ambiente bajo lo que se conoce como modo de falla seguro.

Este modo de fallo seguro consiste en interrumpir de manera programada el proceso ante un evento que ponga en peligro la seguridad del proceso controlado, con el fin de garantizar que no se presenten afectaciones en las personas, medio ambiente e integridad de los activos operados. La función safety incluye características desde el diseño de los sistemas de control, como elementos redundantes, esquemas de alta disponibilidad y la parametrización de algunas funciones específicas de protecciones y control, para mantener el proceso dentro de rangos de variables que no sean peligrosas.

En otro planteamiento realizado por (Kriaa, Cambacedes, Bouissou, & Halgand, 2015, pág. 158) se argumenta que, si bien safety y security tienen muchas similitudes como el hecho de tener elementos comunes como tratar el tema de riesgos, medidas de protección y controles y su principal diferencia radica en el origen del riesgo que contrarrestan. Safety considera amenazas relacionadas con daños o la combinación de éstos que ocasionan un mal funcionamiento o daño accidental en el sistema, con efectos en el medio ambiente, mientras que la seguridad se enfoca en cómo las amenazas y potenciales ataques afectan los activos de sistemas y su operación derivado de vulnerabilidades.

Alineados con estos conceptos, autores como (Knowles, Prince, Hutchison, Disso, & Jones, 2015, pág. 70) introdujeron el concepto aseguramiento funcional, con el fin de satisfacer los requerimientos de safety y seguridad, como un enfoque de ciberseguridad para sistema de control. Aunque Safety es un término que no tiene traducción, significa libre de riesgo el cual no es tolerable o aceptable, según la IEC 61511. Así mismo, el concepto tradicional de seguridad está más orientada a los mecanismos, controles, para evitar una afectación por eventos no deseados, entre esta se encuentra el concepto de defensa en profundidad, o seguridad por capas o niveles.

Estos autores proponen que el **aseguramiento funcional** es un intento por alinear los conceptos de safety y seguridad, a través de un nivel mínimo de seguridad que permita operar un activo con niveles de confianza y protección, el cual debería entrar en modo de fallo seguro, basado en un nivel de riesgo conocido. Este es un enfoque de ciberseguridad totalmente diferente al concepto de defensa en profundidad ampliamente utilizado por los sistemas de información.

3.3.6. Métricas en seguridad cibernética.

- **Métricas en Seguridad de la Información**

El tema de métricas en seguridad es un problema complejo que no debe subestimarse según lo plantea (Bellovin, 2006, pág. 96) y que para abordarlo y poder hablar de esto en propiedad es necesario tener cuantificaciones para poder pasar de una simple idea que puede ser vaga o insatisfactoria. Esta temática de métricas fue incluida dentro de la lista de problemas retadores preparada por el Consejo de Investigación INFOSEC de EEUU.

Autores como (Naqvi & Riquidel, 2006, pág. 209), afirman que las métricas en seguridad deben seguir según el estándar NIST - Security Metrics Guide for Information Technology Systems, cuatro principios. Estos se constituyen según los autores, en un apoyo de muy alto nivel para la gestión de estas métricas, procedimientos y políticas de seguridad con la gestión de una autoridad competente que asegure su cumplimiento, el desempeño de métricas cuantificables y el análisis de métricas orientadas a resultados.

En el mismo trabajo proponen un modelo para implementar métricas, basado en la evaluación de entidades con las que exista alguna relación y con las que se debe garantizar la seguridad, otras que son relevantes y las que no. Posteriormente definen las medidas que se

deben realizar de manera directa, indirecta y las que no debe medirse por no representar un impacto en seguridad. Posteriormente establecen las dependencias entre equipos, servicios y flujos de información y finalmente proponen como establecer las métricas. Una de las conclusiones de estos autores en su trabajo es que aún la disciplina de métricas es inmadura, no hay lenguaje estandarizado, ni buenas prácticas a seguir.

Por parte de NIST se tiene el documento NISTIR 7564/2009 (NIST, 2009) Dirección de Métricas en Ciberseguridad, el cual plantea que en la literatura se propone un rango de definiciones variadas e interpretaciones de lo que son métricas en seguridad de TI. El documento desarrollado en 2009, enfatiza que hablar de métricas en sistemas de computación es algo que puede ser inapropiado porque este campo apenas estaba emergiendo como un área de desarrollo y no tiene la misma madurez que las métricas desarrolladas para las ciencias exactas como la física. Propone que las medidas a desarrollar deben referirse a aspectos evaluables de diferentes partes del sistema que contribuyan a la seguridad.

En el campo de la seguridad de la información se encuentra la norma técnica ISO 27004/2009 (ISO, 2009, pág. 20), la cual está enfocada en definir métricas relacionadas con la implementación de un sistema de Gestión de Seguridad de la información, principalmente en:

- Evaluar la efectividad de los controles o grupos de controles implementados.
- Evaluar la efectividad del SGSI implementado.
- Verificar en qué medida se han cumplido los requisitos de seguridad identificados.
- Proporcionar información para la revisión de la administración y la toma de decisiones relacionada con el SGSI, con el fin de justificar las mejoras necesarias del SGSI implementado.

En la misma línea, (Bayuk, 2011, pág. 943), argumenta que muchos de los programas de seguridad en las organizaciones se realizan enfocados al cumplimiento de normas y estándares con el fin de cumplir los requisitos de auditorías y con frecuencia, se les indican a los ingenieros de las organizaciones que organicen las métricas de seguridad, con las cuales se esperan sean auditados mostrando el cumplimiento del estándar.

La autora plantea que existen al menos 900 métricas diseñadas para seguridad, citando específicamente en el libro de Herrmann de 2007, diseñadas para tomadores de decisiones como auditores, ingenieros y administradores con un enfoque de entender el tema de seguridad, pero excluyendo las que requerían cálculos matemáticos o modelos para poder ser estimadas. Finalmente argumenta que es necesario cambiar el enfoque de las métricas convencionales y tratar de establecer métricas que midan por ejemplo que tan flexible es el sistema para cambiar la superficie de ataque, que tanta conciencia situacional se tiene, fuera de los aspectos convencionales.

También propone que las métricas en seguridad deben aportarle al rol de quien tiene las responsabilidades por el aseguramiento y que debe ser combinado con la medida de la seguridad como un atributo del sistema de seguridad. Finalmente recomienda que las métricas no tienen mucho sentido sino están ligadas a los objetivos de un programa de seguridad y propone un acercamiento a la construcción de métricas basado en un análisis de la misión o lo que se persigue en un contexto operacional, definir la seguridad requerida, la arquitectura de la seguridad, la arquitectura, las métricas y finalmente los métodos y herramientas para lograrlo.

Otros autores, (Kowalski, Barabanov, & Hoffman, 2011, pág. 22) plantean en su trabajo que a menos que algo sea medido, nuestro conocimiento es insuficiente, citando al Lord Kelvin. Específicamente plantean que nuestra capacidad de gestionar algo está directamente

relacionada con el conocimiento que se tiene sobre eso. Reconocen que existe un interés creciente por desarrollar métricas en seguridad de la información, motivado principalmente por temas regulatorios enfocados en una mayor transparencia y responsabilidad y por la necesidad de soportar decisiones de inversión en seguridad, mostrando alineación a los programas, objetivos de la compañía a través de una fina sintonización con la efectividad y eficiencia.

Otra perspectiva realizada de manera conceptual es la de (Purboyo, Rahardjo, & Kuspriyanto, 2011, pág. 1), los cuales desarrollan en su trabajo el tema de métricas en seguridad y afirman que una métrica implica un sistema de medición basada en medidas cuantificables. Así mismo sostienen que la seguridad de un sistema de información, enfoca las medidas a aquellos aspectos del sistema que contribuyen a su seguridad.

Plantean que el término "security metrics" se ha convertido en un estándar relacionado con un nivel, un desempeño, indicadores y la misma fortaleza en seguridad. En el ambiente de TI se utilizan términos como fortaleza en seguridad, indicadores de seguridad, o incluso medidas de seguridad, de manera indiferente con el término métricas de seguridad. Un resultado de la medición es una medida de un punto simple que tiene un valor y un contexto en el tiempo, mientras que métricas asegura el autor, es una descripción de múltiples medidas construidas como una herramienta para el tomador de decisiones.

Los autores (Jonsson & Pirzadeh , 2012, pág. 58), plantean que existe una gran cantidad de sugerencias sobre cómo medir la seguridad en un sistema en general y que muchas veces se busca llegar a una única métrica, aunque existe muchos limitantes y problemas para lograr este cometido. Argumentan también que el camino de construir métricas es complejo, dado que la seguridad es una propiedad compleja que está basada en una serie de atributos del sistema. En

su trabajo estos autores proponen un marco de referencia para establecer métricas en dos categorías. La primera está enfocada en la protección, la cual involucra fronteras de borde, externalidades, vulnerabilidades y la segunda está concentrada en el comportamiento, e involucra la confiabilidad, safety, disponibilidad y confidencialidad. La idea general de estos autores es que las métricas que se definan deben estar relacionadas a atributos que se quieren preservar.

Aunque durante los últimos años se ha incrementado el interés de cómo medir la seguridad por parte de académicos investigadores, organismos normalizadores, entre otros, no hay una definición unificada de lo que son las métricas, pero sí coinciden es que es un estándar de medida como lo sustentan (Vaarandi & Pihelga, 2014, pág. 294). Enfocan su propuesta de construcción de métricas de seguridad a través de la recolección de logs de IDS, IPS, Firewalls, worksation, y el uso de protocolos como Netflow desarrollado por Cysco, los cuales guardan estadísticas del tráfico de una red, a través del encabezado de cada paquete almacenado por este protocolo. Esta orientación para la construcción de métricas de seguridad, no debería ser un costo significativo para la compañía, partiendo del hecho que se cuentan con esta data en el almacenamiento de los equipos, como lo plantean los autores.

Por su parte, (Zeb, Yousaf, Afzal, & Mufti, 2017, pág. 126) sostienen que las métricas cuantitativas en seguridad son deseables para medir el desempeño de los controles de seguridad, apoyando la toma de decisiones funcionales y de negocios para mejorar el desempeño y el costo de los controles. Sin embargo, según los autores, definir un conjunto de métricas de seguridad a nivel empresarial, es uno de los problemas duros o difíciles listados en Infosec Research Council. La mayoría de los esfuerzos por definir métricas de seguridad absolutas a nivel empresarial no ha sido exitosa. También citan en su trabajo en la página 127

a Government Performance and Results Act GPRA y a Federal Information Security Management Act FISMA, como dos organismos que están presionando a nivel regulatorio para que se avance en el tema de métricas en seguridad.

El campo de la evaluación de seguridad mediante métricas cualitativas, afirman que es un campo en desarrollo e investigación y que el trabajo se ha realizado en métricas cualitativas, pero que es un método menos preciso porque se califican los controles con rangos, malo, regular, bueno y que el asunto cuantitativo solo ha sido desarrollado para cumplir con algunos requerimientos regulatorios.

Su trabajo se enfoca en proponer un modelo relativo de métricas en seguridad enfocado en tres métricas cuantitativas llamadas Medida de Resiliencia al ataque – ARM por sus siglas en inglés, Factor de Mejora del Desempeño – PIF por sus siglas en inglés y medida del costo/beneficio CBM - por sus siglas en inglés y lo valida mediante la implementación en laboratorios de máquinas virtuales.

- **Métricas en Sistemas de Control Industrial**

Aunque existe abundancia en estándares relacionados con sistemas de control industrial, existen pocos esfuerzos encaminados a proveer una guía para la evaluación de su cumplimiento, según (Knowles, Prince, Hutchison, Disso, & Jones, 2015, pág. 72).

Esto se corrobora, al encontrar en una de las normas técnicas más recientemente publicada, específicamente la IEC 62443-4-1:2018 (IEC, 2018, pág. 9), la cual plantea en su capítulo general que este organismo tiene planeada una norma que catalogará como IEC TS 62443-1-3 titulada Métricas de Cumplimiento de Seguridad del Sistema. Al realizar la búsqueda en otros organismos como ISA, NIST, IEC responsables por la normalización y prácticas de los

sistemas de control, tampoco se encontró información disponible enfocado a métricas en seguridad enfocados a sistemas de control. En este sentido la IEC fue el único organismo que anunció que el tema de métricas en sistema de control se desarrollará en una de sus normas, la cual se encuentra en la fase de planeación, como ya se expuso.

En cuanto a la literatura técnica o documentos de referencia, se encontró un artículo publicado por (Boyer & McQueen, 2008, pág. 2), en el cual los autores realizan una propuesta de métricas técnicas cuantificables para sistemas de control. En su trabajo argumentan que las métricas son datos que facilitan la visión y están orientadas a soportar la toma de decisiones, por lo que construir malas métricas conllevará a malas decisiones y viceversa. Mencionan que su punto de partida fue la revisión de más de 30 estándares y referencias incluida la NIST, pero que ninguna de ellas se ajusta a la definición de métricas en seguridad definidas en su trabajo, porque encontraron varias debilidades en estos estándares, como por ejemplo hablar de indicadores promedio de vulnerabilidades, trae consigo implicaciones de subvalorar los riesgos específicos en ciertos equipos o sistemas.

Proponen siete principios que se deben proteger o garantizar para los sistemas de control industrial y establecen el mismo número de métricas con base en estos así: (1) días de engaño por cambios (días sin que el equipo de seguridad conozca los últimos cambios en las plataformas o sistemas que protege), (2) el atacante no conoce nada del sistema (revisión de lo fuerte de las contraseñas y la exposición de información sin encriptar hacia fuera de la organización o sistemas), (3) Sistema es inaccesible a grupos de atacantes, (4) el sistema no tiene vulnerabilidades, (5) el sistema no puede ser dañado (pero caso de pérdidas), (6) el grupo de seguridad conoce cualquier compromiso inmediatamente, (7) el grupo de seguridad puede

reestablecer la integridad inmediatamente. Finalmente muestran un caso de estudio en el que estiman o calculan estos valores de métricas.

Definen la métrica técnica de ciberseguridad como un resultado de un modelo matemático. El trabajo está orientado a los tomadores de decisiones en sistemas de control y parten de que un conjunto de métricas no debe ser muy grande, menor a 20 para que sean manejables, ser de fácil entendimiento, ser medible y objetivo. En su propuesta, definen 7 principios a los que relacionan prácticas de seguridad y sobre estas basan su propuesta de métricas para los operadores de sistemas de control. Finalmente muestran como calcularlas mediante un caso de estudio.

(Department of Homeland Security, 2009, pág. 6), propone en el capítulo tres de su informe "Primer Control System Cybersecurity Framework and Technicals Metrics", diez métricas que deben ser desarrolladas en los Sistemas de control industrial.

Por su parte (Kisner, y otros, 2010, pág. 21), en su trabajo técnico sobre seguridad en sistemas de control plantean que normalmente la implementación de métricas proviene de varias fuentes o necesidades como:

"* Un medio para evaluar cómo se minimizan las consecuencias o impactos financieros de un incidente de seguridad.

* Indicar cual es el éxito con el que el sistema de control evita los problemas que ponen en peligro operación o comportamiento del sistema, es decir, para cuantificar la efectividad de l|as operaciones.

* Mostrar cual es el cumplimiento de los objetivos de calidad de la seguridad, es decir, cual es la eficacia para detectar las fallas.

* Un medio para documentar qué tan bien el sistema de control cumple con los requisitos de seguridad."

El enfoque de este trabajo es identificar las mediciones que conduzcan a determinar la confiabilidad, seguridad y resiliencia de un sistema de control.

Proponen, además, que las métricas en ciberseguridad deben ser de tres tipos:

✓ Métricas basadas en el diseño. Midiendo el diseño y la implementación del sistema más allá de su desempeño.

✓ Métricas basadas desempeño. Midiendo cuántos ataques ha sido capaz de neutralizar y cuantos de fueron exitosos, y midiendo tiempos antes de comprometer los servicios, entre otras características. Esta son las métricas más difíciles de implementar por lo ciertos de los tiempos.

✓ Métricas basadas en políticas. Son principios que se establecen y deben cumplir los sistemas.

Existe otra iniciativa de marco de referencia para la construcción de una propuesta de métricas en sistemas de control elaboradas por (McIntyre, Becker, & Halbgewachs, 2007, pág. 10), quienes plantean que, aunque se ha intentado aplicar controles y métricas de los sistemas de información a los sistemas de control industrial, esta técnica no ha sido exitosa. Plantean que establecer métricas en sistemas de control industrial trae beneficios como:

"* Mejorar la postura de seguridad, mejorando el conocimiento, conciencia y control de la arquitectura y el ambiente operacional.

* Proveer mayor información de la conciencia situacional permitiendo a los grupos de interés entender su estado actual de seguridad y cuales acciones son requeridas.

* Contar con la disponibilidad de información para apoyo a búsqueda de soluciones sobre qué activos y elementos de control necesitan ser protegidos.

* Invertir los recursos adecuadamente, basado en áreas críticas funciones y requerimientos.

* Permite definir y aplicar controles de seguridad entendiendo cual es la mejor protección en ambientes operacionales.

* Reducción del riesgo a través de soluciones ajustadas a los requerimientos."

Plantean que se deben desarrollar tres tipos de métricas: organizacionales, operacionales, técnicas y que, dentro de las organizaciones, las métricas deben seguir una estructura teniendo en cuenta los objetivos de negocio, los procesos y finalmente los controles. Así mismo mencionan que los estándares de industria en temas de seguridad son solo una guía de recomendaciones, buenas prácticas y controles que deberían implementarse y por su parte las métricas, permiten establecer qué tan buenos son los controles, y cuál es la posición real de la compañía frente a los riesgos.

Estos autores plantean que el uso de métricas en planeación, finanzas y sistemas de información es común. Sin embargo, argumentan que los entornos operativos tienen unos requisitos y objetivos totalmente diferentes a los de otras áreas de la organización y por ello el enfoque de la construcción de métricas debe ser específico para este dominio. Las infraestructuras críticas prestan servicios precisamente críticos.

Proponen también que, con base en la taxonomía de un sistema de automatización, se deben construir las métricas basadas en objetivos generales de la misión, funciones clave en cada dependencia, activos críticos en cada dependencia, integridad de los datos y procesos, participación humana en procesos clave y los controles de seguridad ya establecidos.

A partir de esto se define una serie de pasos para construir las métricas en el ambiente operacional. (Francia, 2016, pág. 8), propone que debido al incremento de los ataques cibernéticos y la gran preocupación que esto ha generado en la protección a las infraestructuras críticas, no solo es necesario implementar procedimientos de seguridad, estándares y políticas, sino que es necesario ejercitar una mejora continua. Para lograrlo, el autor plantea que es necesario desarrollar métricas. Argumenta que la experiencia en seguridad tradicional de sistemas de información no puede ser simplemente aplicada a sistemas de control industrial, debido principalmente a sus diferentes requerimientos y desarrollo.

Se necesita desarrollar un conjunto especial de métricas para sistemas de control industrial. Stoddard citado por (Francia, 2016, pág. 8), coincide con (McIntyre, Becker, & Halbgewachs, 2007) en describir que las métricas están organizadas en tres grupos organizacionales, operacionales y técnicas. Afirma también que los estándares NERC-CIP tienen en cada uno de los documentos, un capítulo relacionado con el nivel de severidad de violar o no cumplir cada estándar y que esta serie de indicadores debería convertirse en un conjunto de métricas de seguridad para los sistemas de control industrial. Adicionalmente plantea que herramientas de inteligencia de amenazas es eficiente desde el punto de vista de costo, al permitir cambiar la postura de seguridad ante amenazas y que el incluir indicadores de amenazas dentro de las métricas de sistemas de control industrial puede ser muy útil, recogiendo datos de herramientas de inteligencia.

3.4. Construcción de escenarios

Tradicionalmente las organizaciones se han visto enfrentadas a la pregunta ¿cómo prepararse para hacer frente a la incertidumbre del futuro? para lo cual han tratado de alguna

forma de anticiparse o recrear condiciones futuras que les permitan planear para hacer frente a las condiciones cada vez más cambiantes e inesperadas del devenir.

En su estudio (Godet, Monti, Meunier, & Roubelat, 2000, pág. 3), plantean que para que una organización pueda hacer frente a la incertidumbre, no es suficiente trabajar en términos de oportunidades y amenazas, sino que se requiere adoptar herramientas que le permitan identificar los retos futuros en una fase exploratoria o prospectiva y en una fase normativa definir las opciones estratégicas deseables, dentro de lo que plantean los autores serían fases preactividad y proactividad o preparatorias.

Así mismo dichos autores plantean en la página 14 de su trabajo, que las herramientas de prospectiva no buscan servir a las ciencias exactas como la física, sino que permiten apreciar de una mejor manera las múltiples realidades posibles. Frente al futuro posible, los autores plantean que el hombre tiene la posibilidad de tomar cuatro tipos de actitud; sufrir el cambio, actuar de manera reactiva frente a una situación, tomar una actitud preactiva o aseguradora en la cual hay una preparación para la situación y la actitud proactiva que consiste en conspirar para que la situación que el hombre desea se materialice.

Entre las herramientas de prospectiva que se han desarrollado durante los últimos años se encuentra la técnica de construcción de escenarios. Al respecto los autores plantean que, si bien existen varias definiciones relacionadas, la palabra escenario involucra palabras planeación, proyección, análisis, y conocimiento. Godet en su trabajo (Godet, Monti, Meunier, & Roubelat, 2000, pág. 17) plantean el término escenario como "un conjunto formado por la descripción de una situación futura y un camino de acontecimientos que permiten pasar de una situación original a otra futura".

Por su parte otros autores como (Vergara Schmalbach, Fontalvo Herrera, & Maza Ávila, 2010, pág. 23), citan en su trabajo una de las primeras definiciones encontradas por (Kahn & Wiener, 1967): "consecuencias hipotéticas de eventos construidos con el propósito de centrar la atención en los procesos causales y la toma de decisiones".

Otra definición citada por los mismos autores (Vergara Schmalbach, Fontalvo Herrera, & Maza Ávila, 2010, pág. 23), es la planteada por Paul Nicol en su trabajo Scenario Planning as an Organisational Change Agent, quien plantea: "los escenarios proveen unos marcos o restricciones para analizar el futuro, limitando el número posible de futuros a ser considerados."

Estos autores concluyen a partir de las diferentes definiciones estudiadas, que en general los escenarios no son empleados para predecir el futuro con certeza, pero si sirven para comprenderlo mejor.

La técnica de planeación por escenarios es una herramienta que si bien, como se dijo no predice el futuro, si ofrece a las organizaciones elementos para prepararse y enfrentar futuros probables o deseables, la cual ha venido en desarrollo durante los últimos años.

Según la revisión bibliográfica realizada en su trabajo por los mismos autores, existen fundamentalmente tres tipos de técnicas que han sido desarrolladas por diversas escuelas para la elaboración de escenarios orientados a la planeación, entre ellas están la lógica e intuitiva, la prospectiva y la tendencia probabilística.

Otros autores como (Godet & Roubelat, Creating the future: The use and misuse of scenarios, 2003, pág. 8) plantean que los escenarios se construyen con base en una serie de hipótesis las cuales deben cumplir tres requisitos o condiciones, deben ser relevantes,

coherentes y probables. De la misma manera estos autores argumentan que existen dos tipos de escenarios dependiendo de la visión con la cual hayan sido creados, los cuales pueden ser exploratorios los cuales siguen ciertas líneas de tendencias, los anticipatorios o regulatorios que parten de una visión o futuro deseado o temido.

Frente a la construcción de escenarios, (V & B, 1999, pág. 28) proponen una serie de pasos que constituyen una metodología para su materialización. Estos autores plantean que la metodología de escenarios persigue tres objetivos, los cuales deben ser desarrollados de manera adecuada y se enuncian a continuación:

"* Descubrir y vincular las variables claves que caracterizan al sistema en estudio mediante un análisis explicativo global.

* Determinar a partir de las variables clave, los actores fundamentales y los medios de que disponen para concretar sus proyectos.

* Describir, en forma de escenarios, la posible evolución del sistema en estudio a partir de la observación y análisis de las variables claves y de los comportamientos de los actores, respecto a un juego de hipótesis".

En el mismo sentido los mismos autores plantean que para el logro de estos objetivos, esta metodología se desarrolla basada en dos fases principales: la elaboración de la base analítica y la propia elaboración de los escenarios. El detalle del desarrollo de la metodología se resume de la siguiente manera:

- ✓ Delimitación del sistema: se identifican las variables clave que pueden influenciar o gobernar el modelo. Para ello se realizan entrevistas, lluvias de ideas con los expertos conocedores de la situación en estudio.

- ✓ Análisis de motricidad y dependencia. Se clasifican las variables de acuerdo a su influencia o motricidad y la dependencia que pueden tener con relación a las otras variables, teniendo en cuenta la definición de cada una de ellas para evitar confusiones. Se identifican cuáles son las variables clave del modelo. Para ello se utiliza la técnica MICMAC, la cual clasifica las variables, de acuerdo a su relación, directa, indirecta y potencial.

- ✓ Análisis de juego de actores. Se identifican los actores o grupos de interés que estarían impactados o tienen intereses o influencia sobre la situación en estudio mediante la matriz de actores y la herramienta MACTOR. Posteriormente se identifican los objetivos, las conductas, intereses de cada actor frente a las variables definidas. Seguidamente se construye la posición que tienen cada actor frente a los demás en relación a las variables clave identificadas. Esto se hace mediante la matriz, Matriz de Actores por Objetivos – MAO, determinando la posición, favorable, desfavorable o neutra que un actor toma sobre la posición de otro actor. Posteriormente se analizan las relaciones de poder entre actores, mediante la Matriz de Medios de Acción Directos - MAD y la Matriz de Medios de Acción Indirectos – MAI.

- ✓ Construcción de escenarios. La construcción de escenarios requiere la construcción de una serie de hipótesis basadas en las variables clave, que reflejan tendencias, rupturas o hechos de futuro que condicionan el comportamiento del sistema. Para lograr que las hipótesis estén acordes a las variables, es necesario que éstas estén dentro del contexto de unos objetivos estratégicos de lo que se persigue. Para la construcción de escenarios existen dos herramientas, el método de impactos cruzados - SMIC por sus siglas en inglés y el método Delphi. SMIC proporciona una combinación de variables, asignándoles una

probabilidad de ocurrencia de cuerdo a la probabilidad de ocurrencia de las hipótesis simples y condicionadas por la realización de otras hipótesis, basado en los criterios de los expertos.

Finalmente se elige aquel grupo de escenarios de mayor probabilidad. Si la probabilidad acumulada corresponde al 70%, este se considera que este es el grupo núcleo más probable. Probabilidades cercanas al 50% corresponden al núcleo tendencia y muestra claramente que esta es la tendencia de los expertos. Dentro de esto se debe seleccionar el escenario de más alta probabilidad.

Los escenarios de más alta probabilidad deben analizarse con base en el análisis estructural y los comportamientos de los actores, especificando cual es la forma de pasar de la situación actual a la cada uno de los escenarios más probables.

3.5. Prospectiva basada en juicios de expertos

Dentro de los estudios y técnicas de prospectiva, la construcción de diferentes visiones sobre lo que podría pasar a futuro implica la participación activa de personas que cuenten con un criterio, experiencia y conocimiento mínimo que les permita emitir juicios, opiniones o posiciones sobre los temas en estudio. En este sentido el autor (Armstrong, Long Range Forecasting: From Crystal Ball to Computer (2nd Edition)., 1986, pág. 81) plantea en su pág90 que, dentro del ejercicio de pronósticos basados en juicios, existen tres pasos básicos, el primero la selección de los expertos, el segundo plantear la pregunta problematizadora y el tercero realizar el proceso prospectivo.

Así mismo propone lo que llama "intención" como un comportamiento planeado y sobre las cosas que tiene control quien emite el juicio. Otro término que introduce el autor es la

opinión, la cual define como pronósticos sobre el cual la persona que emite el juicio tiene poco control. El mismo autor plantea que el problema de selección de los expertos dependerá de si lo que se quiere son datos de opinión o datos de intención.

Los casos de intención aplican cuando el juicio se trata de evaluar un evento que tiene importancia o compromete al encuestado, este tiene un plan o posición bien definida en relación con el evento, y que generalmente hace parte del corto plazo. En este tema el autor sostiene que una cuidadosa selección de expertos reduce el problema del muestreo ayudando a una mejor inferencia de la muestra a una población y que se debe apoyar en el muestreo probabilístico que está bien desarrollado por la literatura, evitando caer en el error del muestreo intuitivo.

Para los casos de la intención el autor sostiene que el valor de los expertos es indiscutible en ejercicios de pronóstico, pero que sus juicios tienen más valor para analizar situaciones actuales que en pronósticos, argumentado en su página 92 que existen cientos de estudios que plantean que después de cierto conocimiento mínimo, la precisión en el resultado de los pronósticos no aumenta con relación a una mayor experiencia.

En cuanto a las técnicas de encuestas, el autor plantea en sus páginas 116 y 117 que el método Delphi es una técnica de encuesta anónima por correo electrónico de las más utilizadas por las organizaciones, que implica que los encuestados sean expertos en el objeto de área de estudio, existe más de una interacción y que este método provee una retroalimentación controlada. Sin embargo, sostiene que estudios indican que incrementar rondas, aunque parece aumentar la precisión en el resultado del pronóstico, sus ganancias son modestas y no existe evidencia si fuese posibles obtener mejores resultados incrementando el número de expertos, en vez de realizar rondas.

El mismo autor en su página 121 plantea una serie de recomendaciones para el ejercicio de encuestas con expertos para temas prospectivos, resaltando el valor de realizar reuniones estructuradas y preparadas frente a la ejecución de simples reuniones grupales. Al respecto da una serie de recomendaciones para las reuniones estructuradas:

"* Utilizar un modelador que trabaje para el grupo en vez de un líder evitando que el grupo trabaje para él, llevando al grupo de manera sistemática en el sentido que este marque.

* Prepara las reuniones descomponiendo el problema y dándole participación a todos los miembros e inclusive a aquellos con ideas tímidas o minoritarias.

* Suspender la evaluación.

* El moderador evita introducir sus propias ideas al grupo",

El mismo autor en otro trabajo (Armstrong, Selecting Forecasting Methods, 2009, pág. 4) sostiene que el estructurar las entrevistas con expertos, contribuyen a la confiabilidad y validez de los resultados.

3.6. Ciclo de mejora continua

Como una herramienta de mejora en los procesos organizacionales, la Organización Internacional de Normalización - ISO por sus siglas en inglés, introdujo el ciclo de mejora continua Planear, Hacer, Verificar Actual PHVA en su estándar (ISO, 2008, pág. vii).

Planear: con base en los requisitos del cliente y las políticas de la organización, se establecen las metas y las adecuaciones a los procesos necesarios para lograr los resultados.

Hacer: consiste en implementar los procesos.

Verificar: realizar un seguimiento y validación del cumplimiento de los procesos y productos, con respecto a las políticas, los objetivos y requerimientos del producto.

Actuar: consiste en tomar decisiones de mejora continua sobre el desempeño del proceso.

3.7. Conclusiones del capítulo

A continuación, se presentan las principales conclusiones del marco teórico desarrollados en el capítulo 4:

- Existe una diferencia entre los términos Tecnologías de Información TI y Tecnologías de Operación TO, refiriéndose este último término a tecnologías de hardware y software que son utilizadas en sistema de control de procesos industriales y los cuales tienen diferentes prácticas de gestión, tienen diferentes objetivos y requerimientos desde el punto de vista de ciberseguridad, siendo la continuidad del proceso el atributo más importante a proteger.

- Las prácticas, procedimientos y tecnologías desarrolladas para el mundo de la seguridad de la información no son aplicables directamente a las tecnologías de operación, aun cuando se trate del mismo hardware y software, haciendo que sólo cerca del 16% de los controles de TI se puedan aplicar al mundo de TO.

- Los sistemas de control industrial pasaron de una seguridad aparente por oscurantismo o aislamiento de las redes de telecomunicaciones globales, a una realidad de ataques cibernéticos incluso sin necesidad de estar interconectados a otras redes, como el caso STUXNET, que el medio de infección fue una USB que se dejó premeditadamente en la planta de producción, empleando técnicas de ingeniería social.

- La tendencia de ataques cibernéticos a sistemas de control industrial es creciente en el período analizado entre los años 2009 y 2016.
- Debido a que los sistemas de control industrial están presentes en las infraestructuras críticas, denominadas de esta manera por prestar los servicios esenciales a la sociedad, los estados intervienen en la protección de dichas infraestructuras a través de planes, normas técnicas de obligatorio cumplimiento. Esto se ve reflejado en la normatividad en ciberseguridad del organismo de estándares y normas tecnológicas de Estados unidos - NIST para sistema de control, pero respetando la aplicación de las mismas a la IEC e ISA, quienes son los organismos técnicos de los sistemas de control industrial para el sector eléctrico y aguas.
- Dentro de los temas importantes a considerar en los análisis de ciberseguridad de las infraestructuras críticas se encuentran las interdependencias y la resiliencia, por los impactos que estos tienen sobre los servicios esenciales que se prestan.
- Se planteó el tema de aseguramiento funcional como un intento de alineación de los términos safety y seguridad, como un enfoque diferente al enfoque tradicional defensa en profundidad.
- Aunque se encontraron diferentes referencias bibliográficas del tema de métricas, algunos autores coinciden que las métricas en sistemas de información es un campo que aún falta por desarrollar.
- La mayoría de los documentos técnicos encontrados relacionados con ciberseguridad en sistemas de control, están enfocados a realizar recomendaciones técnicas de los controles a ser implementados, otros se enfocan a ser documentos de discusión técnica, otros son

estándares que no son de obligatorio cumplimiento. Algunos trabajos por el contrario muestran las diferencias y problemas de aplicar ciertas prácticas de las tecnologías de información de manera directa en los sistemas de control industrial, pero en general no se identifican documentos técnicos ni normas que aborden el tema de métricas de manera directa o específica en sistemas de control industrial.

- Existe un número de normas propuestas que indican el qué se debería implementar para mejorar los sistemas de control industrial, pero queda una gran incertidumbre, en el cómo implementar dichas recomendaciones de manera práctica y segura para el proceso.

4. Diseño metodológico

La problemática por resolver se abordará mediante la técnica estudio de caso, teniendo en cuenta que el estudio de caso no es como tal un método de investigación, sino una herramienta utilizada para resolver una problemática específica y que puede involucrar métodos cualitativos, cuantitativos y mixtos propios de las ciencias sociales, con enfoques deductivo o inductivo.

Fundamentalmente se emplearon análisis cualitativos complementados con métodos cuantitativos como entrevistas a expertos y profesionales del sector eléctrico con conocimiento en la continuidad y operación de activos de distribución del sector eléctrico, la ciberseguridad de tecnologías de operación, comparando la información levantada con la encontrada en la literatura.

Se parte de las variables teóricas encontradas en la literatura, guías, normas, buscando prácticas empresariales o controles cibernéticos relacionadas con dichas variables, y finalmente se realizan unos análisis, recomendaciones y un aporte para resolver la problemática planteada. Para abordar el trabajo, se propusieron la siguiente secuencia de fases.

1. Revisión de las prácticas, guías, normas y controles de ciberseguridad dispuestos para las tecnologías de operación del sector eléctrico, específicamente para activos como subestaciones, centros de control y subestaciones eléctricas.
2. Identificar la posición deseable u objetivo de negocio de la empresa de Distribución de Energía acorde a su perfil de riesgos, en términos de pérdidas económicas máximas admisibles y tiempos máximos de afectación de la continuidad del sistema eléctrico, ante la

materialización de incidentes cibernéticos. Este aspecto se abordó con la pregunta problematizadora, al plantear que las pérdidas fueran las mínimas posibles.

3. Plantear una situación de ciberataque hipotética que afecte los objetivos de negocio que involucre la cadena de control de una subestación eléctrica. Se planteó la peor condición que es la de generar un blackout o apagón generalizado del sistema de distribución.

4. Plantear la pregunta problematizadora que se quiere resolver en condiciones de ciberataque, para lograr la posición deseable de la empresa de distribución en términos de continuidad de la operación de la red eléctrica que es su principal activo operativo y que será resuelta con la metodología de planeación por escenarios.

5. Delimitar el alcance del análisis a realizar. Esta delimitación se realizó sobre la cadena de control objeto de estudio.

6. Utilizar la técnica de planeación por escenarios para construir escenarios posibles o probables en términos de seguridad cibernética que resuelven la pregunta problematizadora. Para ello se construye un modelo basado en variables, actores, sus objetivos, lo que finalmente culmina con la formulación de hipótesis que permitirán construir los escenarios.

   - Identificar y definir las variables relevantes que resuelven la pregunta problematizadora para el análisis básico de ciberseguridad de la cadena de control subestación, sistema de telecomunicaciones y sistema SCADA central.

   - Identificar y definir los actores que tienen relación o impacto con la pregunta problematizadora.

- Utilizar la técnica MICMAC para determinar las variables relevantes, dominantes, dominadas y su relación. Final se priorizan y filtran las variables que impactan el modelo o escenarios que se construirán.
- Utilizar la técnica MACTOR para determinar la relación e influencia de los actores, entendiendo éstos como aquellos grupos de interés, procesos, personas, actividades que pueden influenciar positiva o negativamente los escenarios. Con la matriz MACTOR se cruzan actores y objetivos y se determina cómo influencian los actores y sus objetivos cobre el modelo.
- Uilizar la herramienta SMIC, para relacionar y establecer, cual es la variable que se debe gobernar, qué actor la gobierna o influencia y a cuál objetivo está impactando y como se relacionan.
- Plantear hipótesis desde las variables clave, los actores relevantes y los objetivos, para finalmente dar forma a los posibles escenarios.

7. Seleccionar el más factible y que aporta más a resolver las pregunta problematizadora, con base en los escenarios planteados.
8. Validar la consistencia interna y plausibilidad de escenarios. Una vez formulado los escenarios iniciales, se revisa la congruencia de las narraciones que lo describen. Se revisan y ajustan los diferentes direccionadores de algunos escenarios de ser necesario.
9. Identifican y priorizan las variables clave que gobiernan el modelo.
10. Detallar los escenarios de incidentes cibernéticos en TO que pueden desencadenar en un blackout.

11. Identificar las variables clave priorizadas en el numeral 5.3.3.4, involucradas en los escenarios de riesgo planteados.

12. Filtrar los riesgos relacionados con las variables priorizadas, con base en los escenarios de riesgo del mapa de riesgos cibernéticos en tecnologías de operación de la empresa distribuidora en estudio.

13. Calcular el índice de riesgo actual para la cadena de control.

14. Asignar una calificación de probabilidad y consecuencia que debería tener cada uno de los riesgos consolidados de la cadena de control para migrar el riesgo hacia un valor deseable para la compañía, en este caso a la zona amarilla o tolerable, identificando las causas de los riesgos y los controles que deben implementarse para lograr disminuir el riesgo actual a tolerable.

15. Construir los indicadores clave de riesgo - KRI, con base en las causas de los riesgos identificados. Se elige la metodología de construcción de KRI y no KPI, dado que estos últimos miden el desempeño y no el riesgo. Este enfoque de riesgos basado en las causas del mismo permite una anticipación a la materialización de eventos y por lo tanto una mayor efectividad de los controles en la cadena de control analizada

16. Proponer los indicadores en el ámbito operación y el proceso

17. Proponer los indicadores para el safety, dado que fue identificado como la variable más determinante de la solución de la pregunta problematizadora.

4.1. Recolección de la información

Identificación de variables teóricas: parte de la identificación de las variables o aspectos clave que impactan la continuidad de la infraestructura de distribución y están relacionadas con los riesgos, controles e indicadores de ciberseguridad encontradas en la teoría o literatura en la cadena de control objeto de estudio y que guiarán la recolección de datos a ser suministrados por los diferentes expertos.

Diseño de recolección de datos: consiste en la definición de plantillas, formularios con preguntas dirigidas, la identificación de los entrevistados, la planeación y programación de entrevistas.

Recolección de datos: realización de entrevistas, identificación de documentos, diligenciamiento de plantillas definidas, orientadas para identificar las variables, controles o aspectos clave de ciberseguridad, encontradas en el grupo EPM actualmente relacionadas con el objeto de estudio.

Análisis de información: procesamiento de datos, análisis de información encontrada y documentada.

Resultados: principales hallazgos, conclusiones de la información, base para formular recomendaciones.

Recomendaciones: se realizan recomendaciones orientadas al cumplimiento de los objetivos del trabajo inicialmente propuestos, con base en los elementos teóricos enunciados y los hallazgos encontrados en la información procesada del objeto de estudio.

4.2. Conclusiones del capítulo

Del diseño metodológico se puede concluir:

- Se seleccionó la técnica caso de estudio para resolver una pregunta de investigación asociada a una situación en un contexto real combinado con otras técnicas como planeación por escenarios, para construir e identificar escenarios posibles que contribuyen a resolver la pregunta de investigación.

- Se emplean otras herramientas como el MICMAC, MACTOR, SMIC como técnicas válidas para procesar las diferentes respuestas de los expertos y encontrar relaciones de motricidad e influencia entre variables.

- Se propondrán indicares clave de riesgo KRI por sus siglas en inglés, en lugar de indicadores clave de gestión, debido a que los primeros permiten hacer gestión proactiva antes que sucedan los eventos, mientras que los segundos son indicadores del tipo resultado de la gestión.

5. Desarrollo de los objetivos

5.1. Analizar estándares y lineamientos del subsector distribución de energía eléctrica

5.1.1. Marco de referencia ciberseguridad en sistemas de control industrial.

El término ciberseguridad según la CNSSI-4009 citado por NISTIR 7298R2, es la habilidad de proteger o defender el uso del ciber espacio de ciber ataques.

Las directrices presidenciales de EE. UU. en el año 2011 en relación con las medidas de seguridad en infraestructuras críticas, incluyó la construcción un marco de referencia en normas y estándares de industria en temas de ciberseguridad, que contribuyeran a gestionar los riesgos cibernéticos de estas infraestructuras, tarea que fue encomendada al director del National Institute of Standards and Technology – NIST de EEUU. Este marco de referencia incluye un conjunto de estándares, metodologías, procesos y procedimientos alineados a la política, negocios de las organizaciones y un enfoque tecnológico que direccionan los riesgos cibernéticos, complementarios a los ya existentes en las industrias relacionadas con las infraestructuras críticas.

Al respecto existe múltiple documentación técnica para la protección de infraestructura críticas, enfocada en la ciberseguridad de sistemas de control industrial - ICS (por sus siglas en inglés) debido a que son estas tecnologías y sistemas las que permiten la operación y continuidad de las IC y están basadas en hardware, software y sistemas de telecomunicaciones que son vulnerables y blancos de los ataques cibernéticos, por lo que este conjunto de normas y documentos se vuelven un referente para la protección de las IC de muchos países.

A continuación, se lista la revisión de las principales normas, documentos técnicos, recomendaciones con su alcance, desarrolladas en general por la ISO para cualquier organización. Así mismo NIST por la orden presidencial ya mencionada, ha desarrollado toda una serie de documentación técnicas, normas y estándares en ciberseguridad orientados a la protección de infraestructuras críticas.

Específicamente para el sector eléctrico, los organismos técnicos y normalizadores en sistemas de control como IEC, ISA, han desarrollado documentación técnica, controles y prácticas recomendadas en ciberseguridad.

Tabla 3. Controles de ciberseguridad en ICS.

Título	Alcance del documento
ISO/IEC 62264-1	Estándar Internacional. Integración de Sistemas Empresariales y Sistemas de Control. Modelos y Terminología. * Muestra un modelo de jerarquia de funciones de supervisión y control en los sistemas de control industrial para procesos de producción. * El anexo A2. Establece que las redes de telecomunicaciones deben separadas entre el tiempo real o sistemas de control y los sistemas corporativos y que una práctica común es que quien gestiona las redes es reponsable por la cibersegruidad del dominio. * No presenta indicadores o métricas en el desempeño de la ciberseguridad en sistemas de control industrial. * Clausulas 5 y 6 muestra los modelos de jerarquia con las actividades tipicas en el dominio de control. * REferencia algunas normas IEC en el anexo C que deben ser aplicadas en los Sistemas de Control Industrial.
IEC 62351-13 TR (Technical Report). Preparado por el comité 57 de la IEC.	Conjunto de recomendaciones en seguridad para diferentes tópicos en Sistemas de Potencia. Es una lista de chequeo para implementar normas o utilizar en implementaciones y como guia para los desarrolladores de normatividad.
IEC 62351 (todas las partes), gestión de sistemas de potencia e intercambio de información asociada - Seguridad de datos y comunicaciones	IEC TS 62351-1, Parte 1: Seguridad de redes y sistemas de comunicación - Introducción a asuntos de seguridad IEC 62351-3, Parte 3: Seguridad de redes y sistemas de comunicación - Perfiles que incluyen TCP / IP IEC TS 62351-4, Parte 4: Seguridad de redes y sistemas de comunicación - Perfiles que incluyen MMS. especifica procedimientos, extensiones de protocolos y algoritmos para facilitar asegurando ISO 9506 - Especificación de mensaje de fabricación (MMS) IEC TS 62351-5, Parte 5: Seguridad de redes y sistemas de comunicación - Seguridad para IEC 60870-5 y derivados IEC TS 62351-6, Parte 6: Seguridad de redes y sistemas de comunicación - Seguridad para IEC 61850 Comunicaciones en Subestaciones eléctricas. IEC TS 62351-7, Parte 7: Seguridad de redes y sistemas de comunicación - Modelos de objetos de datos de gestión de redes y sistemas (NSM) IEC TS 62351-8, Parte 8: Seguridad de datos y comunicaciones - Control de acceso basado en roles IEC 62351-9, Parte 9: Seguridad de datos y comunicaciones - Gestión de claves de seguridad cibernética para equipos del sistema de potencia IEC TR 62351-10, Parte 10: Seguridad de datos y comunicaciones - Directrices de arquitectura de seguridad IEC 62351-11, Parte 11: Seguridad de datos y comunicaciones - Seguridad para archivos XML IEC TR 62351-12, Parte 12: Seguridad de datos y comunicaciones - Recomendaciones de resiliencia y seguridad para sistemas de energía con sistemas ciberfísicos de recursos de energía distribuida (DER). IEC 62351-13 TR (Technical Report). Preparado por el comité 57 de la IEC.
IEC TR 62351-10, Parte 10: Seguridad de datos y comunicaciones - Directrices de arquitectura de seguridad	Define la seguridad de datos y comunicaciones para la administración de sistemas de energía y el intercambio de información asociado. Comprende definiciones de seguridad para protocolos de comunicación, gestión de redes y sistemas, así como control de acceso basado en roles.
IEC TR 62351-12	Recomendaciones de Seguridad y Resiliencia en Fuentes de Energía Distribuidos
IEC 62443 (todas las partes), Redes de comunicación industrial - Seguridad de redes y sistemas	IEC 62443 (todas las partes), Redes de comunicación industrial - Seguridad de redes y sistemas IEC 62443-3-3, Redes de comunicación industrial - Seguridad de redes y sistemas - Parte 3-3: Requisitos de seguridad del sistema y niveles de seguridad IEC 62443-4-1, Seguridad para sistemas de control y automatización industrial. Parte 4-1: Requisito de ciclo de vida seguro para el desarrollo de productos
IEC 61511	GESTIÓN DE LA SEGURIDAD FUNCIONAL Se implementarán procedimientos para evaluar el desempeño del SIS frente a su requisitos de seguridad para: • Identificar y prevenir fallas sistemáticas que podrían poner en peligro la seguridad; • Monitorear y evaluar si los parámetros de confiabilidad del SIS están de acuerdo con aquellos asumido durante el diseño; • -definir la acción correctiva necesaria que debe tomarse si las tasas de falla son mayores que fue asumido durante el diseño; • Comparar la tasa de demanda en el SIF durante la operación real con las suposiciones hechas durante la evaluación de riesgos cuando se determinaron los requisitos SIL.

Elaboración basada en normas y documentos técnicos IEC, NERC, NIST, ANSI, ISA, ISO, IEEE.

Tabla 4. Controles de ciberseguridad en ICS.

Título	Alcance del documento
ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Overview and vocabulary
ISO/IEC 27001	Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos, especifica un conjunto de requisitos de gestión de la seguridad de la información diseñados para ser utilizados con fines de certificación en una organización.
ISO/IEC 27002	Tecnología de la información - Técnicas de seguridad - Código de práctica para la gestión de la seguridad de la información, establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información en una organización.
ISO/IEC TR 27019/2017:	* Tecnología de la información - Técnicas de seguridad - * Pautas de gestión de seguridad de la información basadas en ISO / IEC 27002 para sistemas de control de procesos específicos para la industria de energía.
IEC 62443 Basada en ISA 99. Redes de comunicación industrial - Seguridad de redes y sistemas	IEC 62443-1-1. Terminología y conceptos. IEC 62443-2-1. Establece un programa para los Sistemas de control industrial. IEC 62443 -3-2. Seguridad por diseño. configuraciones de red. IEC 62443 -3-3. Requisitos de seguridad del sistema y niveles de seguridad IEC 62443-4-1:2018. Requerimientos para el desarrollo del ciclo de vida de productos seguros.
ANSI/ISA-TR99.00.01	Tecnologías de Seguridad para Automatización Industrial y Sistemas de Control. IEC 62443 se basa en esta norma.
ANSI/ISA-TR99.00.02	Integración de Seguridad Electrónica dentro del ambiente de producción y sistemas de Control.
NIST 800-82 R2	Guia para seguridad de Sistemas de Control Industrial
NISTIR 7628	Guia de recomendaciones de Ciberseguridad en Smart Grid. Tres versiones que enuncian diferencias entre TI los sustemas de control industrial y el concepto Smart Grid.
NISTIR report 7920/2012	Discusiones sobre pruebas de software y referencias de pruebas de sotfware ISO/IEC/IEEE 29119.
NISTIR 7564/2009	Direccion de Métricas en Ciberseguridad
NIST Framework for improving Critical Infrastructure Cybersecurity, 2014	* Apartir de la orden presidencial 13636 Mejorar ciberseguridad de IC. Es voluntario y colaborativo entre sectores de IC y gobierno, adotar mejores prácticas sin necesidad de esstablecerlo de cumplimiento regulatorio o cumplimiento de negocios. Este framework reconoce los estándares y buenas prácticas de ciberseguridad a nivel global y puede ser utilizado fuera de US como un modelo para cooperación internacional para el fortalecimiento de la cibe en IC. * Interdependencias Tecnológicas entre IT, ICS y Telecomunicaciones incrementaron las amenazas internas y externas, expandiendo las vulnerabilidades potenciales y el riesgo para las operaciones. * Para manejar el riesgo en ciber se requiere un entendimiento claro de los drivers de negocio y conocimiento especifico del uso de IT e ICS. Porque en cada organización el riesgo es único, a lo largo de IT e ICS, por lo que la aplicación del marco de referencia puede cambiar.
NIST Special Publication 800-39/2011	Gerenciando el riesgo de Seguridad de la Información: Organización, Misión y una vista al sistema de información.
Energy Sector Cybersecurity Framework Implementation Guidance. US Department of Energy - DOE.	Energy Sector Cybersecurity Framework Implementation Guidance.
Electricity Subsector Cybersecurity Risk Management Process. DOE/OE-0003. US Department of Energy - DOE	Guia de Proceso de Gestión del Riesgo de Ciberseguridad en compañias de la industria del sector eléctrico, creada por NIST, NERC, DOE y expertos del S.E.
NERC CIP 2-9/2008: Critical Infrastructure Protection	CIP-002-5 — Cyber Security — BES Cyber Asset and BES Cyber System Categorization. CIP-003-5 — Cyber Security — Security Management Controls. CIP-004-5 — Cyber Security – Personnel & Training. CIP-005-5 — Cyber Security – Electronic Security Perimeter(s). CIP-006-5 — Cyber Security — Physical Security of BES Cyber Systems. CIP-007-5 — Cyber Security – Systems Security Management. CIP-008-5 — Cyber Security — Incident Reporting and Response Planning. CIP-009-5 — Cyber Security — Recovery Plans for BES Cyber Systems.
IEEE 1686.	Capacidades de ciberseguridad en dipositivos inteligentes electrónicos estándar.
ENISA (2011)	Protección de Sistemas de Control Industrial. Anexo V. Hallazgos Clave.
DHS. Catalogo de Seguridad para Sistemas de Control. 2011	Recomendaciones para desarrolladores de Estandares
CPNI. Cyber Security Assessments Of Industrial Control Systems. 2011	Evaluación de Ciberseguridad en Sistemas de Control Industrial
NIPP 2013	Plan de Ciberseguridad para Seguridad y Resiliencia en Infraestructura Crítica

Elaboración basada en normas y documentos técnicos IEC, NERC, NIST, ANSI, ISA, ISO, IEEE.

Como se ha mencionado la norma IEC 62264-1, realiza una jerarquía de los niveles de control y separa los dominios de control de los otros dominios corporativos buscando eficiencia y reducción de riesgos operacionales, a la vez que establece los límites y la forma de exportar información del proceso productivo hacia los procesos de negocio y sus sistemas de información, lo cual establece un orden funcional y jerárquico.

Específicamente esta norma en su anexo A2, realiza una recomendación o práctica de ciberseguridad importante:

"Parte del hecho que la seguridad a menudo es combinada con la gestión de las redes y en este sentido recomienda asegurar que las redes que son usadas en ambientes de operaciones de producción, especialmente en las que involucran el control físico de procesos estén o sean redes separadas de redes que no son tiempo real. Finaliza que esta separación puede ser física a través de diferentes redes o estándar de red o virtual a través de protocolos, firewalls, y enrutadores. Finaliza enunciando que el control de tiempo real requiere una red predecible, responsable y latente, la cual se logra a través de la separación de redes".

La norma IEC62351-10, realiza una comparación de los requerimientos de seguridad en redes de ofimática y sistemas de potencia, concluyendo que existen grandes diferencias en el orden de importancia de los atributos del servicio que se protegen. Mientras los sistemas de información de la gestión del negocio se enfocan en la confidencialidad, la integridad y por último la disponibilidad, en los sistemas de control industrial estas prioridades se invierten, primero la disponibilidad pro enfoque en los servicios críticos, en un segundo lugar la integridad de la información porque es fundamental para las decisiones técnicas y operativas y por último la confidencialidad, excepto si se hay información de innovación en los ambientes de producción o patentes que deben ser protegidas.

IEC 62351 en su numeral 4.2 plantea que la infraestructura de información para los sistemas eléctricos de potencia difiere de los ambientes de ofimática o de telecomunicaciones y remite al documento NISTIR 7628 en su volumen 3 el cual elabora un listado detallado de asuntos técnicos específicos. Así mismo la norma IEC 62351-5 aborda la definición de medidas apropiadas de seguridad en temas técnicos de los ambientes eléctricos.

Específicamente la IEC 62351-10 establece guías de arquitecturas de seguridad en sistemas de control industrial, también muestra problemas al aplicar técnicas ofimática o TIC´s a los ICS, que se suman los de NISTIR 7628:

"* Autenticación en subestaciones, en dispositivos de campo IED's, medidores, usuarios, Head end.

* Limitaciones y problemas para aplicar parches de seguridad.

* Equipos con 10 o 30 años de vida.

* Dispositivos instalados en campo y áreas desprotegidas como redes de distribución de energía.

* Interoperabilidad con los sistemas o equipos heredados, influye en el mantenimiento de los sistemas de potencia y hace que los sistemas sean más complejos.

* Dado que existen equipos de tecnologías heredadas de hace mucho tiempo, existen requisitos estrictos de interoperabilidad y migración que no es posible cumplir.

* Comunicaciones seriales de equipos de campo con SCADA que no tienen componentes que protejan la integridad y confidencialidad de la información, dado que se transmiten como textos claros.

* Conexiones a subestaciones utilizando línea telefónica, por la cual se envían contraseñas, sin niveles de seguridad.

* No todos los IEDS´s crean logs de acceso, por limitaciones en ancho de banda de las comunicaciones".

Así mismo, el capítulo 7.3 del mismo documento técnico, menciona que es necesario acentuar en los diferentes estándares de sistemas de control, las diferencias que existen entre TI o sistemas de información empresariales, con el concepto Smart Grid por la complejidad, profundidad de estas temáticas y si bien la NIST 800 - 82 se puede utilizar de manera básica para estos fines, necesita ser más explícita en muchos temas de marcada diferencia.

El documento técnico NISTIR 7628/2010 revisado en 2014, en su capítulo 7.2. Reconoce qué si bien hay muchas recomendaciones en normas para sistemas de control, aún no es claro cómo llevarlas a cabo en su implementación, sumado a que algunos fabricantes no incluyen estas recomendaciones y controles dentro de sus soluciones para sistemas de control industrial.

Las normas, documentos técnicos, recomendaciones, estándares como NIST, IEC, IEEE, ISO buscan el desarrollo de prácticas de protección de seguridad del proceso, la salud de las personas y la protección del medio ambiente y el cumplimiento de la ley y la regulación, pero no aseguran el cumplimiento de estos requerimientos de seguridad. Esto se verifica en los avisos de notas importantes de algunos documentos, por ejemplo, como lo enuncia el estándar IEEE 1686 y en el hecho que muchos de ellos son solo referencias técnicas y no son de obligatorio cumplimiento en las empresas de la industria, por lo que queda a discreción de las empresas y fabricantes de software y hardware su implementación.

5.1.2. Modelos de madurez de capacidades en ciberseguridad.

Los modelos de madurez de capacidad miden madurez de varios procesos organizacionales.

Tabla 5. Modelos de madurez en ciberseguridad.

Modelo de Madurez en Ciberseguridad	Alcance
SSE-CMM. Systems Security Engineering. (ISO/IEC61827).	Ampliamente utilizado para evaluar los procesos de ingeniería. Tiene limitación para ser aplicado a ICS.
INFOSEC Assurance Capability Maturity Model. (IA-CMM).	Utilizado para medir capacidades organizacionales en el proceso de seguridad de la información.
Federal Aviation Administration Integrated Capability Maturity Model (FAA – iCMM).	No direccionan asuntos específicos de ciberseguridad.
CERT Resilience Maturity Model (CERT RMM)	Capacidades de resiliencia operacional. De relevancia para ICS en la disponibilidad.
Electricity Subsector Cybersecurity Capability Model (ES C2M2).	Desarrollado específicamente para el sector eléctrico, por el Departamento de Energía y Defensa Estadounidense y más de 40 principales expertos de la industria. Capacidades del subsector de energía.
Oil and Natural Gas Cybersecurity Capability Model (ONG-C2M2).	Modelo de madurez desarrollado para el sector de Gas Natural, basado en ES-C2M2

Elaboración basada en (Knowles, Prince, Hutchison, Disso, & Jones, 2015)

Específicamente el departamento de Seguridad Nacional de los Estados Unidos, desarrolló un modelo de madurez de capacidades para empresas del sector eléctrico como

empresas Generadoras, Transmisoras y Distribuidoras de Energía Eléctrica, llamado **Electricity Subsector Cybersecurity Capability Model ES - C2M2.**

El objetivo del C2M2 es la gestión de las prácticas de seguridad cibernética asociadas con la operación y el uso de la tecnología de la información, los activos de tecnología de operación y los entornos en los que operan, mediante el establecimiento de un modelo que les permita a las empresas medir sus capacidades en ciberseguridad y poder compararse contra un modelo de 5 niveles, compartir buenas prácticas, priorizar inversiones y priorizar acciones para mejorar la ciberseguridad a través de la adopción de las prácticas de ciberseguridad del marco de referencia de NIST.

El modelo aborda y está dividido en los siguientes diez (10) dominios:

- Gestión del Riesgo.
- Activos, cambios y gestión de la configuración.
- Gestión de Acceso e Identidad.
- Gestión de Amenazas y vulnerabilidades.
- Conciencia Situacional.
- Información compartida y telecomunicaciones.
- Respuesta a eventos, incidentes y continuidad de operaciones.
- Gestión de dependencias externas y cadena de suministro.
- Gestión de fuerza de trabajo.
- Gestión del programa de ciberseguridad.

5.1.3. Documentos de política y normatividad de ciberseguridad en Colombia

Tabla 6. Resumen de principales normas de ciberseguridad en Colombia.

Norma	Objeto
Constitución Política de Colombia, artículo 217.	Las Fuerzas Militares tendrán como finalidad primordial la defensa de la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional.
Ley 527 de 1999.	Trata conceptos para darle valor a la información en el medio electrónico bajo criterios de integridad y accesibilidad.
Ley 594 de 2000	Ley General de Archivos – Criterios de Seguridad.
Ley 962 de 2005	Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas.
Ley 1150 de 2007	Seguridad de la información electrónica en contratación en línea.
Ley 1266 de 2008	Habeas data financiera, y seguridad en datos personales.
Ley 1273 de 2008	Delitos Informáticos y protección del bien jurídico tutelado que es la información.
Ley 1341 de 2009	Tecnologías de la Información y aplicación de seguridad.
Ley 1273 del 2009	Sanciona las conductas penales contra la información.
Ley 1341 de 2009	Crea el concepto de la sociedad de la información y la organización de las TIC´S.
Ley 1453 de 2011	Medidas para garantizar la seguridad ciudadana. – Vigilancia electrónica. – Interceptación legal de comunicaciones.
Resoluciones CRC 3066 y 3067 de 2011	Régimen integral de protección de los derechos de los usuarios e indicadores de calidad para los servicios de telecomunicaciones.
Ley 1480 de 2011	Protección al consumidor por medios electrónicos. Seguridad en transacciones electrónicas.
Ley 1581 de 2012	Ley estatutaria de Protección de datos personales.
Decreto 1377 del 2013	Reglamenta la ley de datos personales.

Norma	Objeto
Decreto Ley 019 de 2012	Entidades de certificación digital y uso de medios electrónicos.
Ley 1712 de 2014	Transparencia en el acceso a la información pública.
Decreto 2573 de 2014	Gobierno en línea.
Acuerdo CNO 788/2015	Guía de ciberseguridad para el sector eléctrico del Consejo Nacional de operación -CNO. Esta normatividad tiene la misma fuerza de una resolución expedida por un ente de regulación. El documento contiene: Definición de sectores de infraestructuras críticas. • Inventario de activos y ciberactivos. • Evaluación de riegos. • Plan de gestión de riesgos. Controles mínimos cumpliendo las NERC CIP 005.
Acuerdo CNO 1241 de 2019	Consejo Nacional de operación -CNO. Esta normatividad tiene la misma fuerza de una resolución expedida por un ente de regulación. Actualiza la guía de ciberseguridad para el sector eléctrico definida en su versión CNO 788/2015.

Pese a que Colombia en general ha avanzado en legislación relacionada con la protección de datos personales, servicios informáticos, servicios de gobierno en línea y delitos informáticos y documentos CONPES que son de política pública, el país no ha avanzado en legislación relacionada con protección de infraestructuras críticas. Sólo se ha avanzado en la catalogación de los sectores de infraestructuras críticas del país y la elaboración de los planes de infraestructuras críticas. En este sentido se requiere el desarrollo de un marco jurídico robusto e integral, en el que se establezcan obligaciones para los prestadores de servicios esenciales e infraestructuras críticas, con planes de mejoras en las capacidades de ciberseguridad y fortalecimiento de las capacidades de ciberdefensa del país.

A continuación, se relacionan otros documentos de política pública y esfuerzos metodológicos por avanzar en el tema de ciberseguridad en el país:

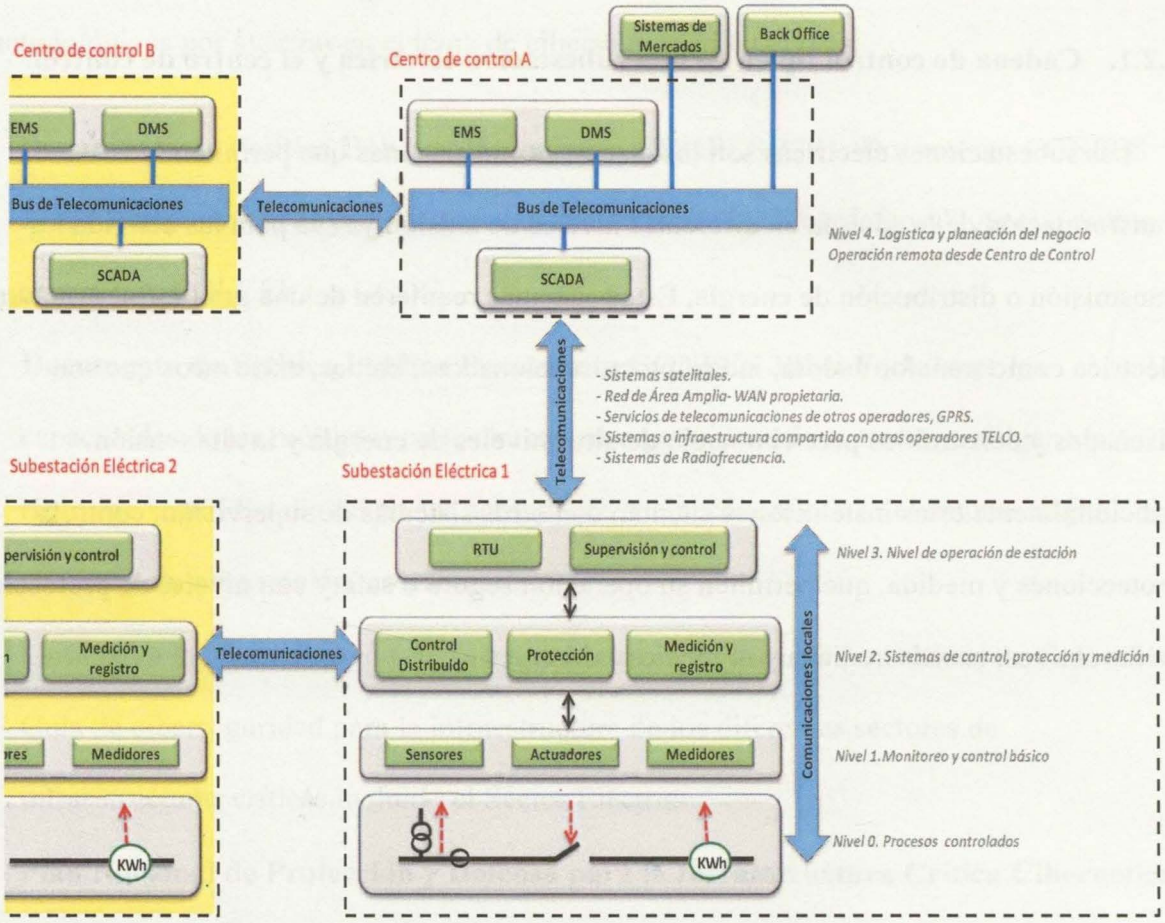
- **Documento de Política Pública. Documento CONPES 3701:** Documento CONPES 3701 "Lineamientos de política para la Ciberseguridad y Ciberdefensa". Apoyo mutuo entre CCP, COLCERT y CCOC.
- **Documento de Política Pública Documento CONPES 3854: Fortalecer** las capacidades de las múltiples partes interesadas para identificar, tratar y mitigar los riegos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración.
- **Guía para la Identificación de Infraestructuras Críticas Cibernéticas de Colombia:** Guía de ciberseguridad para la infraestructura de los diferentes sectores de infraestructuras críticas incluido el Sector Eléctrico.
- **Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia y el Plan Sectorial de Protección y Defensa de la ICC:** Plan del Comando Conjunto Cibernético para la protección de infraestructuras críticas del país.
- **Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas - Guía riesgos 2018:** El objetivo es orientar a todas las entidades del Gobierno nacional, territoriales y sector público en la implementación de la gestión de riesgos de seguridad digital basada en la definición metodológica del MGRSD para, incrementar la confianza de las múltiples partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información en cada entidad pública.

5.2. Identificar los tipos de incidentes cibernéticos en la cadena de control a estudiar

5.2.1. Cadena de control típica de una subestación eléctrica y el centro de control.

Las subestaciones eléctricas son instalaciones con sistemas que permiten la transformación de la energía en diferentes niveles de tensión ya sea para las actividades transmisión o distribución de energía. Estos sistemas requieren de una gran infraestructura eléctrica como transformadora, interruptora, seccionadora, bahías, entre otros que son diseñados y construidos para el manejo de altos niveles de energía y la alta tensión. Adicionalmente estas instalaciones cuentan con otros sistemas de supervisión, control, protecciones y medida, que permiten su operación segura o safety con niveles de protección de los activos, la vida humana y el medio ambiente.

Gráfica 7. Arquitectura básica de una subestación y un centro de control.



Elaboración propia basada en figura D.6 de la IEC TR 62357-1:2016 y la IEC 62264-1

El sistema SCADA por sus siglas en inglés permite la adquisición de datos de las diferentes subestaciones e intercambiar datos u órdenes en forma de comandos entre el centro de control y la subestación. A su vez intercambia datos entre otros centros de control de igual, mayor o menor jerarquía de control.

La siguiente tabla muestra las funciones de cada uno de los niveles de control.

Tabla 7. Impacto en recursos y tiempo debido a eventos que afectan la prestación del servicio.

Nivel de la jerarquía	Actividad
Nivel 0	En este nivel se encuentra la instrumentación del proceso, actuadores, sensores, transductores, medidores entre otros, los cuales permiten el muestreo y la conversión de variables físicas a variables eléctricas de instrumentación susceptibles de análisis discretos.
Nivel 1	Este nivel realiza el control del proceso y la protección de los activos productivos, como transformadores, interruptores, seccionadores, entre otros, a partir de la información suministrada del nivel 0.
Nivel 2	En este nivel integra y homologa los datos recolectados desde los niveles anteriores, permitiendo el uso y extracción otros provenientes de otros sistemas, como información necesaria para análisis, el registro histórico de lo que sucede en el proceso o para la operación local y remota.
Nivel 3	En este nivel se identifican todos los sistemas locales que habilitan de forma parcial o total la supervisión y operación de activos de una estación. SCADA Local.
Nivel 4	En este nivel contiene todos los sistemas remotos que permiten realizar parcial o totalmente la supervisión y la operación de activos de una o múltiples subestaciones. El SCADA central o remota y el intercambio de información que realizan con sistemas de información que apoyan los negocios.

Elaboración con base en IEC 62264-1

Aplicaciones como Energy Management System - EMS por sus siglas en inglés, permiten la gestión operativa y toma de decisiones en líneas de transmisión, plantas de generación y subestaciones eléctricas, mientras que el Distribution Management System – DMS, soporta

toda la información de análisis para la toma de decisiones de apertura, cierre, transferencia entre otras, en los circuitos de distribución.

5.2.2. Descripción de tipos de incidentes cibernéticos típicos en la cadena de control.

Se han identificado algunos tipos de incidentes que pueden presentarse en los centros de control y subestaciones, con base en la experiencia, el conocimiento y ejercicios previos de riesgos de ciberseguridad, realizados por algunos de los expertos invitados a participar de las encuestas.

Entre los tipos de incidentes cibernéticos factibles se encuentran:

- Ataque de hombre en el medio.
- Ingeniería social a los involucrados.
- Suplantación de Identidad.
- Escalamiento de privilegios no autorizados en los ciberactivos.
- Envío de comandos y solicitudes maliciosas a los ciberactivos.
- Desactivación de los controles de no repudio.
- Alteración de información de los dispositivos de monitoreo en los servidores del centro de control.
- Cambios no autorizados en las configuraciones de los ciberactivos.
- Inhabilitación de los sistemas auxiliares del centro de control y subestaciones: UPS, aire acondicionado, sistema ininterrumpido de potencia, sistemas antincendios.
- Afectación de parámetros de funcionamiento correcto de los dispositivos de control y protección de los activos críticos.

- Denegación de servicio al contact center de reporte de daños.
- Afectación de la disponibilidad de la infraestructura de voz operativa, trunking, radio, telefonía de misión crítica, grabadora órdenes de trabajo.
- Afectación del desempeño de procesamiento, almacenamiento y retardos en telecomunicaciones y plataformas de TO.
- Denegación de servicio en infraestructura de TO y telecomunicaciones.
- Afectación de la continuidad de las telecomunicaciones para el control.

Así mismo algunas de las causas que pueden atribuirse a estos incidentes son:

- Configuraciones por defecto o de fábrica en los ciberactivos.
- Falta o falla en los controles de acceso físico.
- Obsolescencia tecnológica y sistemas legados.
- Parches de seguridad incompletos en los sistemas operativos y aplicaciones.
- Puertos vulnerables habilitados en las reglas del FW.
- Falta de segmentación en las redes de TO.
- Obsolescencia Tecnológica.
- Falta de controles robustos en el Firewall, como doble factor de autenticación.
- Dispositivos sin línea base de seguridad.
- Ausencia de controles complementarios ante imposibilidad de aplicación de controles invasivos propios de TI en infraestructura de control y de TO.

- Divulgación de marcas, arquitecturas y dispositivos empleados en subestaciones y centros de control.
- Falta visualización y monitoreo de los ciberactivos en las redes de TO.
- Falta de visualización y control de cambios en la configuración de los ciberactivos de TO.
- Falta de control y administración de cuentas privilegiadas.
- Deficiencia en los diseños de los ciberactivos.

Algunos de estos tipos de incidentes y fallas en la ciberseguridad se puede corroborar en la cadena de eventos que originó el apagón de Ucrania, como lo muestra (SANS, 2016, pág. 6), los cuales hicieron parte de un plan altamente coordinado para lograr afectar el suministro de electricidad en todo un país.

Tres compañías de distribución de electricidad ucranianas fueron infectadas con un malware que provocó la desconexión de subestaciones eléctricas, afectando a cientos de miles de hogares. El incidente que inició a las 3:35 pm, afectó 7 subestaciones de 110kV de Alta Tensión, 23 Subestaciones de 35KV, las cuales fueron desconectadas por 3 horas hasta las 6:35 pm, afectando cerca de 225.000 clientes que recibían el servicio de energía eléctrica.

A través de un correo electrónico el cual contenía un archivo de office que se envió al personal de operación, se introdujo un código malicioso en una macro en Excel, el cual contenía un arma cibernética conocida como BlackEnergy 3, a través del cual se robaron credenciales para VPN, y escalaron privilegios en la red e instalaron una puerta trasera para poder acceder a la red de manera remota sin ser detectados.

Posteriormente procedieron con el reconocimiento de la red, estudiando los diferentes DMS que tenían en las empresas, extrayendo información de la red, utilizando killdisk para sobrescribir los archivos del disco duro con datos aleatorios para no ser detectados e instalaron firmware malicioso en SCADA y HMI.

Posteriormente generaron la apertura de los interruptores de subestaciones generando el apagón, cambiaron el firmware de los equipos de la red de telecomunicaciones para que fuera inutilizada, generaron un cambio en el firmware de la UPS del centro de control para que no funcionara y generaron una denegación de servicio al contact center para no saber de dónde vendrían las llamadas de los clientes reportando los daños. Como se nota se emplearon diferentes estrategias altamente coordinadas para generar un apagón general.

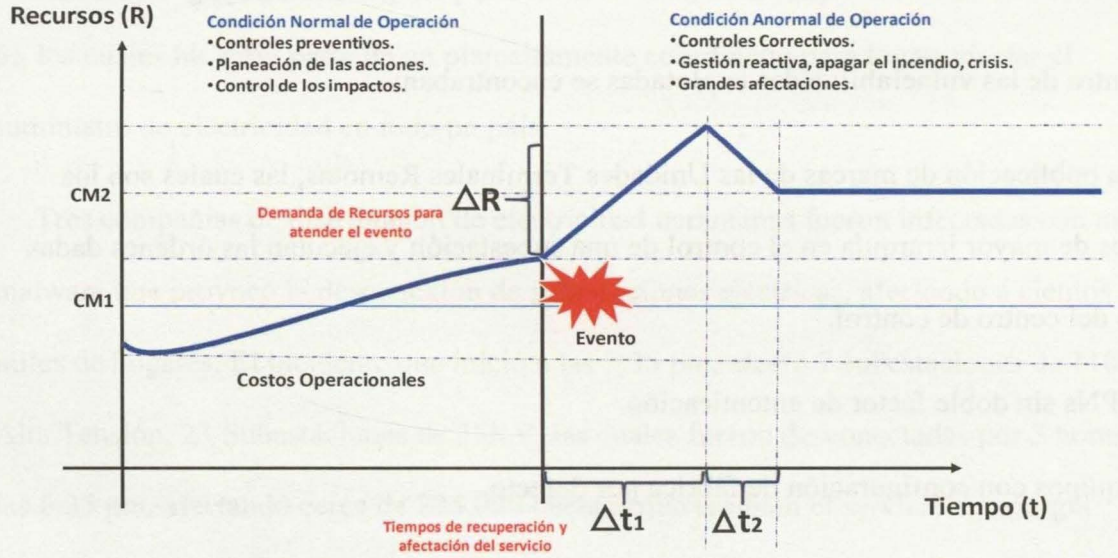
Dentro de las vulnerabilidades explotadas se encontraban:

- La publicación de marcas de las Unidades Terminales Remotas, las cuales son los equipos de mayor jerarquía en el control de una subestación y ejecutan las órdenes dadas dentro del centro de control.
- VPNs sin doble factor de autenticación.
- Equipos con configuración de fábrica por defecto.
- Mala administración de credenciales y privilegios.
- Los sistemas de operación no tenían visibilidad sobre cambios en sus configuraciones.
- Se evidenció falta de segmentación de los sistemas de control.

5.3. Identificar aspectos cibernéticos relevantes de la cadena de control estudiada.

Las empresas de distribución que manejan infraestructuras y servicios críticos, tienen dos condiciones operativas en las que se mueven. Por una parte, está la operación normal de los procesos operativos en los que se basa la prestación de los servicios, basados en prácticas de mantenimiento a la infraestructura para que los activos operen dentro de unas condiciones operativas normales y por otra está la condición en la cual se presentan eventos o fallas durante la operación, ya sea por deficiencias en el mantenimiento o por sabotaje o incidentes cibernéticos. La siguiente gráfica muestra las dos condiciones.

Gráfica 8. Impacto en recursos y tiempo debido a eventos que afectan la prestación del servicio.



Elaboración propia basada en metodología de gestión de riesgos de EPM.

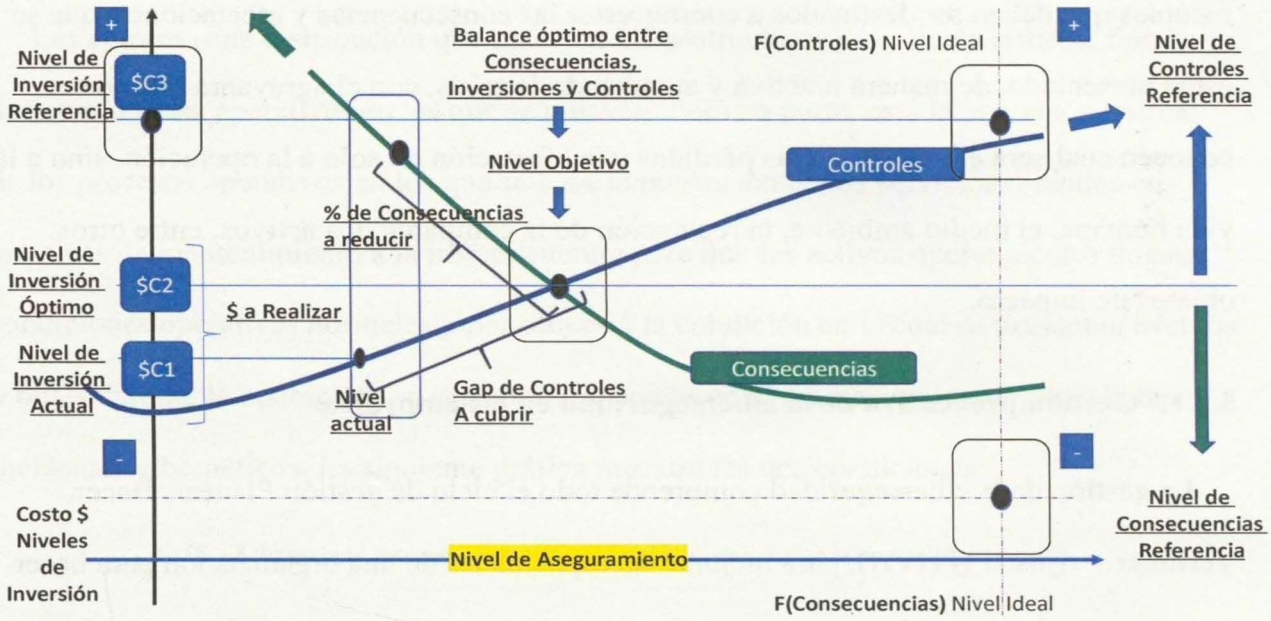
Durante la operación normal, existen recursos que se dedican a mejora continua de los controles, auditorías, planeación preventiva de las mejoras y gestión que se reflejan en costos operativos.

Frente a la presencia de un evento, existe una creciente y alta demanda o explosión de recursos que deben ser destinados a contrarrestar las consecuencias y afectaciones, que se están presentado, de manera reactiva y atendiendo la crisis, con el agravante que no se conocen cual será el tamaño de las pérdidas y la afectación no solo a la operación, sino a la vida humana, el medio ambiente, la reputación de la compañía, los activos, entre otros objetos de impacto.

5.3.1. Gestión preventiva de la ciberseguridad en las empresas.

La gestión de la ciberseguridad comprende todo el ciclo de gestión Planear, Hacer, Verificar y Ajustar (PHVA), para mejorar las capacidades de una organización para hacer frente las mejoras continuar y para contrarrestar una serie de posibles riesgos. Con esto se busca implementar controles, que involucran procesos, tecnologías, recursos humanos y financieros, para reducir las posibles consecuencias de la materialización de los mismos. En este sentido las compañías se enfrentan a decisiones de inversión, costo y riesgo, que deben administrar buscando un nivel óptimo para hacer una gestión eficiente.

Gráfica 9. Balance óptimo entre la gestión de la ciberseguridad y las consecuencias.

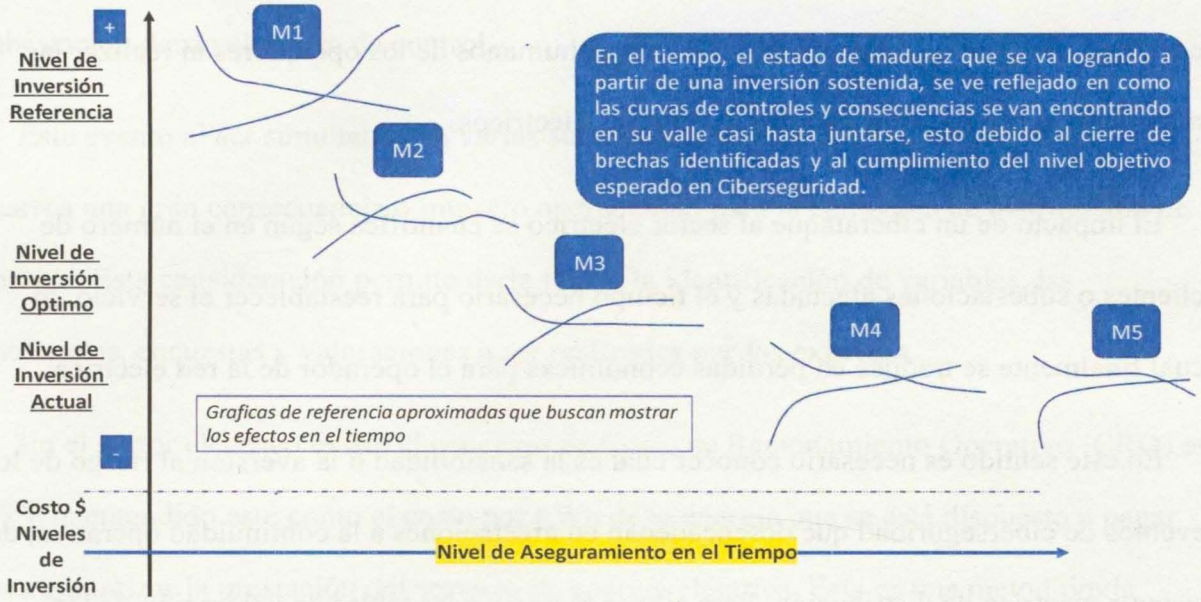


Basado en IEC 62443 capítulo Gestión de ciberseguridad e ISA 99.

Existe un nivel actual de inversiones en controles que busca reducir el nivel de consecuencias de los riesgos cibernéticos y a medida que las inversiones se incrementan las consecuencias se van reduciendo hasta alcanzar un punto óptimo, en el cual las inversiones en los controles son iguales a las consecuencias de lo que se están mitigando. A partir de este punto los controles comienzan a ser más costosos que las consecuencias, lo cual indicaría que los controles son más costosos que el riesgo que se quiere evitar o proteger. Este análisis parte de la premisa que los controles a implementar deben ser eficientes y eficaces.

A medida que la compañía va alcanzando mayores niveles de madurez, los controles mejoran su eficacia, las consecuencias se reducen y se va logrando una familia de curvas en la cuales se cruzan el costo de los controles y las consecuencias, que se van reduciendo a medida que aumenta el nivel de madurez, como se muestra a continuación.

Gráfica 10. Familia de curvas de costos de los controles y consecuencias en función del nivel de madurez de las compañías.



Elaboración basada en IEC 62443 e ISA 99.

5.3.2. Gestión correctiva de la ciberseguridad en las empresas.

Para identificar los asuntos más relevantes a gestionar en el ámbito de ciberseguridad en una empresa de distribución durante un evento, es necesario conocer el valor de lo que se quiere proteger o resguardar.

Como ya se ha mencionado, los sistemas eléctricos de un país o una región trabajan 7x24 365 días al año y todos los esfuerzos de la empresa distribuidora están encaminados a la continuidad del servicio prestado, lo cual está directamente relacionado con las decisiones operativas y la continuidad de las tecnologías que permiten operar remota y centralizadamente las subestaciones y los circuitos eléctricos desde un centro de control.

En este análisis solo se considerarán las afectaciones a las tecnologías de operación o al proceso de soporte de dichas tecnologías, producto de incidentes cibernéticos y no se considerarán eventos relacionados con errores humanos de los operadores al realizar las maniobras sobre las subestaciones y circuitos eléctricos.

El impacto de un ciberataque al sector eléctrico se cuantifica según en el número de clientes o subestaciones afectadas y el tiempo necesario para reestablecer el servicio, lo cual finalmente se traduce en pérdidas económicas para el operador de la red eléctrica.

En este sentido es necesario conocer cuál es la sensibilidad o la aversión al riesgo de los eventos de ciberseguridad que desencadenan en afectaciones a la continuidad operativa, del sistema eléctrico de distribución. Para ello se recurrió a las tablas de valoración de las afectaciones de continuidad de las operaciones de una empresa típica del sector, encontrando que la escala de criticidad en las pérdidas económicas en una empresa de distribución de un tamaño X que atiende un mercado Y, podría es la siguiente:

Pérdidas mínimas hasta $P millones de pesos al año

Pérdidas menores hasta $ Q millones de pesos.

Pérdidas moderadas hasta $R millones de pesos.

Pérdidas mayores hasta $Z millones de pesos.

Ahora bien, para ser conservadores en los análisis, es necesario partir del hecho que estas pérdidas se presentarán en el evento operacional de mayor impacto para la operación de la distribución, esto es en un blackout o apagón generalizado en todas las subestaciones operadas, lo cual implica que será el producto del peor evento de discontinuidad del

servicio que se presente. Esta condición permitirá acotar el presente estudio a uno o varios incidentes cibernéticos que puedan generar un apagón en la cadena de control de una subestación desde el centro de control.

Este evento al ser simultáneo en varias subestaciones críticas del sistema eléctrico acarrea una gran consecuencia o impacto operacional, para la compañía de distribución de energía. Esta consideración permite darle foco a la identificación de variables, las entrevistas, encuestas y valoraciones a ser realizadas por los expertos.

En el sector eléctrico existe el concepto de Costo de Racionamiento Operativo (CRO) en $/kWh, entendido este como el costo por kWh de la energía que se está dispuesto a pagar para garantizar la prestación del servicio de energía eléctrica. Esta es una metodología oficial de la Unidad de Planeación Minero-Energética - UPME1 y ampliamente utilizada para el cálculo del costo de racionamiento, establecida por el regulador de energía. La energía más costosa para los clientes es aquella que no se presta. Teniendo en cuenta el valor de Costo de Racionamiento Operativo - CRO para el año 2019 dado por la UPME, las tarifas de energía del OR2 y la curva típica de restablecimiento del servicio del último un apagón dado en el mes de junio del año 2007 de la empresa de distribución típica en estudio.

De la gráfica se puede concluir que existe un tiempo previo de preparación antes de iniciar las tareas operacionales para el restablecimiento, cerca de 30 minutos y un tiempo adicional propio de la ejecución de las maniobras técnicas de aumento de generación y la

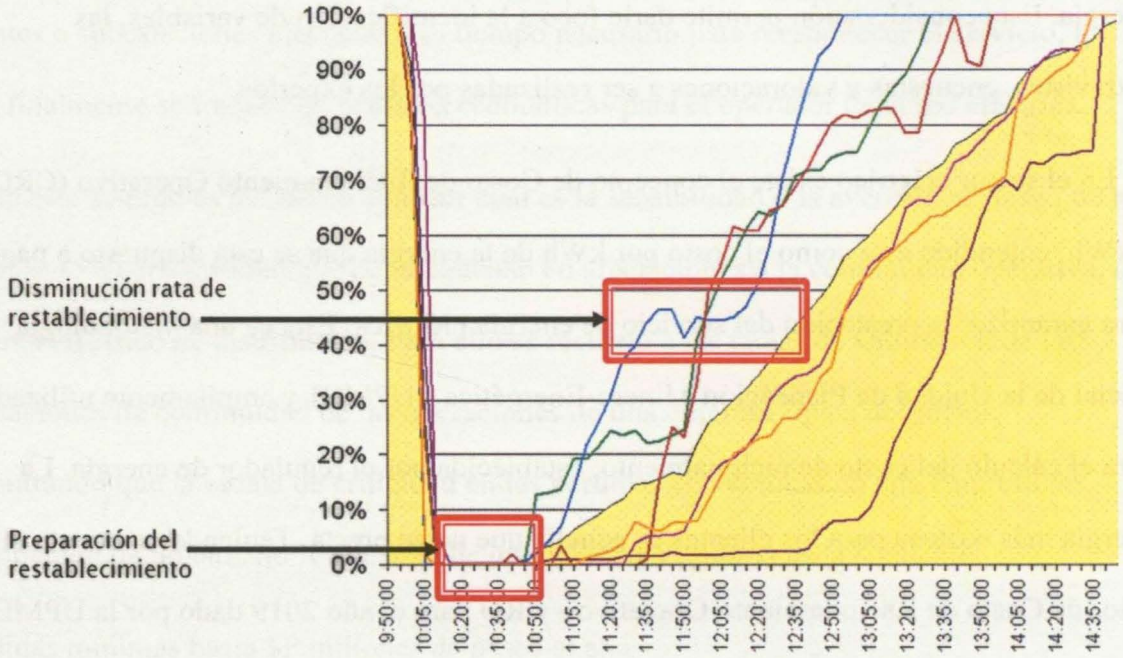
1 http://www.upme.gov.co/CostosEnergia.asp

2 https://www.epm.com.co/site/Portals/2/documentos/tarifas/Energia2019/Publicacion-Agosto-16-2019.pdf?ver=2019-08-20-073714-853

alimentación de los circuitos eléctricos que atienden la demanda o los clientes, cerca de 120 minutos.

Teniendo en cuenta la curva de restablecimiento del apagón del país en el año 2007 se tiene:

Gráfica 11. Curva de restablecimiento de algunas empresas del sector eléctrico colombiano después del blackout 2007.



Fuente Estudio de alternativas de restablecimiento EPM

Dado que estos datos son los reales del restablecimiento del año 2007, es necesario ajustarlos a la mejora en el desempeño de la compañía en estas tareas, debido a que actualmente se cuenta con algoritmos que permiten optimizar la curva de restablecimiento empleando el 70% del tiempo empleado inicialmente. SDL.

El restablecimiento de un apagón requiere cómo mínimo 2 horas teniendo en cuenta que todos los sistemas SCADA, telecomunicaciones y los sistemas SAS automatización de subestaciones están listos para efectuar las maniobras de restablecimiento. En este caso la

empresa estaría incurriendo en pérdidas equivalentes al costo de racionamiento operativo CRO por valor de **$11.356** millones de pesos, aclarando que realmente la penalidad estaría cobrada por el primer escalón de la demanda no atendida por el CRO lo que daría un valor de **$13.368.060** millones de pesos lo que se consideraría una pérdida moderada, según la escala de criticidad antes mencionada. Esta escala corresponde a la catalogación de las pérdidas según el tamaño de negocio, ingresos, la capacidad del negocio para asumir pérdidas económicas y la posición de sus dueños.

Sin embargo, si el apagón es producto de un ataque cibernético que impacta la continuidad de la operación, no solo se requerirán las dos horas de tiempo de restablecimiento teniendo en cuenta la curva, sino que habría que adicionar un tiempo en tareas previas de identificación, contención, erradicación del ciberataque, recuperación de las tecnologías de operación, según las actividades propuestas por el estándar NIST 800-53. Este tiempo es el requerido para la verificación de la idoneidad del funcionamiento de los sistemas SCADA, para poder iniciar la restauración del servicio.

Adicional a los costos de racionamiento, existen otros indicadores de calidad del servicio de energía que se denominan calidad media, los cuales se ven afectados tanto por las interrupciones en la prestación del servicio, como por la duración de estos, otra afectación a los ingresos lo que se conoce con energía no suministrada, la indisponibilidad de activos eléctricos y las multas por fallas en la prestación del servicio. Estos asuntos se desarrollan en más detalle en el numeral 5.4 de este estudio.

Con base en lo anterior se puede concluir que durante un incidente cibernético que genere un blackout, el tiempo más costoso del evento es el necesario para contener, erradicar el ataque y recuperar las tecnologías de operación, dado que la energía más

costosa para la empresa es aquella que no se presta, por las penalizaciones del servicio. Con base en lo anteriormente expuesto se requiere formular una pregunta para ser resuelta en los análisis y que guie la solución de la pregunta problematizadora.

¿Cuáles son las variables que se deben gerenciar desde la ciberseguridad en Tecnologías de Operación de una empresa del negocio distribución de energía eléctrica, para que las pérdidas del negocio sean las menores posibles bajo escenarios de riesgos de incidentes cibernéticos?

5.3.3. Identificar los factores clave del modelo.

- **Identificación de Variables Clave.**

Una empresa de distribución opera subestaciones eléctricas y circuitos eléctricos. El mayor impacto de las decisiones operativas se dan en la operación de las subestaciones eléctricas, por lo que el análisis se enfocará hacia la operación de los sistemas de distribución de energía teniendo en cuenta la cadena de supervisión y control de las subestaciones desde el centro de control. Estas funciones de operación centralizada, requieren del uso de tecnologías de SCADA y aplicaciones, telecomunicaciones y automatización de las subestaciones.

Para la identificación de las variables que resuelven la pregunta problematizadora se recurrió al criterio de expertos en:

- Operación de sistemas eléctricos de distribución
- Soporte de sistemas SCADA y aplicaciones de centros de control en distribución
- Telecomunicaciones que soportan las funciones SCADA, control y protección de los sistemas eléctricos.

- Automatización de susbestaciones eléctricas
- Ciberseguridad e infraestructuras críticas

A partir de reuniones con estos expertos se identificaron las siguientes variables que tienen relación directa con la pregunta problematizadora planteada. Con base en las variables identificadas, se logró consenso en las definiciones a cada uno de los términos llegando a las siguientes precisiones:

Tabla 8. Identificación y definición de variables para ejercicio prospectiva.

	Nombre de la variable	Descripción de la variable
V1	Posesión o control	Conservar el dominio y gobierno de las TO, impidiendo la ejecución de acciones no autorizadas de control, manipulación o interferencia de las TO que soportan funciones centralizadas desde el centro de control, por parte de funcionarios o terceros no autorizados, através del diseño, operación y mantenimiento de sistemas y los procesos asociados y controles asociados o la retoma del control perdido de las plataformas.
V2	Integridad y Autenticidad de la información proveniente y enviada al proceso o en el intercambio de información con fuentes externas	Que los datos del estado del proceso de campo que se transmiten y se procesan en el SCADA, Aplicaciones Operativas Centralizadas o fuentes externas, correspondan a la realidad del funcionamiento del proceso y que las órdenes y acciones operativas realizadas desde el centro de control hasta el proceso de campo (hasta los IED´s), lleguen consistente y oportunamente. Incluye asegurar que el dato o información proceda de la fuente quien dice ser o la autorizada.
V3	Seguridad física de Activos Críticos	Establecer y gestionar los controles de acceso físico para evitar el acceso no autorizado o el sabotaje al funcionamiento e integridad de la infraestructura, activos de producción y ciberactivos asociados, catalogados como críticos, por parte de funcionarios o terceros no autorizados.
V4	Configuración correcta de sistemas de TO	Mantener la consistencia, coherencia y la integridad de la configuración de parámetros eléctricos y de funcionamiento de los sistemas, SCADA, Telecomunicaciones, RTU-Concentradores, Control Local y Protecciones, previniendo un cambio no autorizado sobre ellos o configuraciones por defecto que otorguen una ventaja a ciberatacantes.
V5	Desempeño de las TO y sus servicios esenciales.	Que los sistemas SCADA, Telecomunicaciones, automatizaciones realicen correctamente todas las funciones para los cuales fueron diseñados con sus condiciones de disponibilidad, dentro de los parámetros adecuados de desempeño en el procesamiento de datos, capacidad de las plataformas, latencias y respuestas ante eventos y cambios en los tráficos de señales e información. Servicios esenciales (UPS, potencia eléctrica ininterrumpida, plantas de emergencia, aires acondicionados de precisión, sistemas antincendio, servicios de TI en el CC, ICCP entre CC-CND, entre otros).
V6	Vulnerabilidad a riesgos psicosociales en personal clave de TO u operación.	Cambios o trastornos al normal comportamiento del personal de TO o de operación, producto de factores psicológicos que introducen riesgos operacionales o por presiones que sirven a los intereses de un tercero y en contra de la disponibilidad del servicio, el buen funcionamiento de las TO o la integridad de los activos.
V7	Obsolescencia Tecnológica de los Activos.	Esta relacionada con la condición o estado de una tecnología, basado en su expectativa de vida útil remanente, funcionamiento acorde a las necesidades del proceso y cumplimiento normativo, factibilidad del soporte, existencia de repuestos en el mercado, los sobrecostos operacionales, tasa de fallas, factores que introducen riesgos en su funcionamiento, haciendo necesario su reemplazo.
V8	Dependencia Tecnológica	Es una condición que hace que el comprador de una tecnología esté sometido a condiciones de soporte, licenciamiento, actualización, cambio, reemplazo, por parte del fabricante de artefactos, software, hardware o el mercado de proveedores los cuales imponen condiciones comerciales o de obsolescencia tecnológica programada. ¿Qué tan moderno necesito estar o qué tanto nos conviene o necesito seguir los adelantos tecnológicos?.
V9	Incorporación de tecnologías apropiadas al proceso	Procesos, conocimiento y artefactos diseñados y construidos exclusivamente para TO, o adaptable a las necesidades de la industria del SE nacional y que están al margen de los cambios tecnológicos de obsolescencia programada de grandes multinacionales o del mundo de TI.
V10	Innovación en ciberseguridad de TO	Introducción de nuevos productos, servicios, modificación o mejora a los productos existentes de ciberseguridad, que sean adoptados por las Tecnologías de Operación TO, através de nuevas propuestas o formas de protección de las funcionalidades de TO, basados en la innovación en tecnologías y procesos.
V11	Retorno sobre la inversión en ciberseguridad.	Es la relación en valor monetario de las consecuencias evitadas por ciberataques, por implementar un conjunto de controles de ciberseguridad, en relación a las inversiones realizadas en dichos controles o en mejora de las capacidades organizacionales de ciberseguridad.
V12	Inclusión de la ciberseguridad en el ciclos de vida de los activos.	Incorporación de buenas prácticas, normas técnicas, legales y de proceso de ciberseguridad, en todo el ciclo de vida de los activos productivos, sus ciberactivos y de TO . Incluye actividades de ingeniería conceptual, de detalle, la solución técnica, arquirtecturas, diseños, adquisiciones de tecnología, transferencia de conocimiento, gestión de proveedores, montaje, puesta en operación, mantenimiento, reposición, desmantelamiento y dada de baja.
V13	Conciencia Situacional del personal de TO	Es una representación mental, comprensión de lo que ha sucedido, está sucediendo y pronosticar lo que puede suceder en un futuro próximo frente al entorno operacional y de funcionamiento de las TO.
V14	Idoneidad del personal de TO	Personal que tiene las habilidades y competencias de tomar decisiones asertivas en situaciones estables o críticas o complejas en el soporte y recuperación de las TO, conservando la conciencia situacional, con conocimiento del sistema soportado y operado, con una visión sistémica del impacto de sus decisiones y acciones sobre la vida útil, la salud del sistema y su continuidad.
V15	Confidencialidad de la información sensible (Operacional y de TO)	Garantizar la confidencialidad de la información y los datos del proceso, vulnerabilidades, marcas de equipos, arquitecturas, tecnologías, parámetros de configuración, secretos industriales y prácticas clave para la continuidad operacional y gestión de riesgos, durante el ciclo de vida de los activos y ciberactivos críticos.
V16	Control sobre el servicio de telecomunicaciones de terceros que soportan servicios IC.	Nivel de gestión sobre la calidad y oportunidad en la atención de daños en infraestructura de terceros u operadores de telecomunicaciones que soportan servicios de IC del operador de red.
V17	Afectación del SAFETY	Corresponde al no cumplimiento de al menos el 80% de las condiciones técnicas, funcionales y de protección que permiten operar un activo en condiciones "libre de riesgo aceptable".

Tabla 9. Identificación y definición de variables para ejercicio prospectiva.

	Nombre de la variable	Descripción de la variable
V18	Efectividad de las contramedidas	Establecer la calidad y eficacia de los controles de ciberseguridad implementados dentro del ciclo de vida de los mismos, producto de la implementación de líneas base de seguridad, planes de mejora, implementación de proyectos y auditorías.
V19	Resiliencia de los sistemas de TO	La capacidad del sistema, la información, datos y funcionalidades de TO a transformarse, renovarse y recuperarse en un tiempo de respuesta ante un evento desencadenante.
V20	Conocimiento de la situación	Actividades de recolección, procesamiento, análisis y presentación de información operativa y de ciberseguridad, incluida la información del estado y resumen de otros dominios, para formar una imagen operativa de lo que está sucediendo en los sistemas.
V21	Respuesta oportuna ante eventos de ciberseguridad	Responder a violaciones de seguridad a través de la notificación a la debida autoridad, reportando necesidad de preservación de evidencia por violaciones y automáticamente tomando acciones correctivas oportunas en situaciones de misión crítica o de afectación al SAFETY.
V22	Controles suplementarios	La implementación de controles alternos o compensatorios no intrusivos a TO, ante la imposibilidad de implementar controles intrusivos como parches, cambios y controles de vulnerabilidades que impacten el desempeño o pongan en riesgo la continuidad de las TO.
V23	Utilidad	Que el sistema y alguna información o datos permanezcan usables y útiles a lo largo del ciclo de vida del sistema y que de manera apropiada puedan ser transferida a un sistema sucesor.
V24	Cumplimiento normativo, legal y regulatorio de ciberseguridad	Cumplimiento de requerimientos de ciberseguridad de ley colombiana, acuerdos de sector CNO, CREG, normas técnicas, entre otros.
V25	Concienciación Directivas	Cumplimiento de compromisos educacionales frente a la estrategia de produccion, acompañada del safety y de la ciberseguridad.
V26	Concienciación Operación	Cumplimiento en el nivel de madurez de la operación en la implementación y uso de medidas de seguridad cibernética en los procesos internos y el comportamiento por fuera de la organización.
V27	Gestion y Retención del Talento Humano	Mecanismos de capacitación, entrenamiento y retención de personal experto en TO y ciberseguridad en Infraestructuras críticas.
V28	Ejercicios de Manejo de Eventos, de Recuperación de Servicio y de recuperación Control	Realización de ejercicios de restauración del servicio, recuperación del control de los procesos, funcionamiento de los sistemas operacionales, frente fallos y eventos de ciberseguridad.
V29	Administración de riesgos	Establecer, operar y mantener un programa empresarial de administración de riesgos de seguridad informática para identificar, analizar y mitigar los riesgos de seguridad informática para la organización, incluidas sus unidades de negocios, subsidiarias, infraestructura interconectada relacionada y partes interesadas.
V30	Gestión de amenazas y vulnerabilidades	Establecer y mantener planes, procedimientos y tecnologías para detectar, identificar, analizar, gestionar y responder a las amenazas y vulnerabilidades de seguridad cibernética, en consonancia con el riesgo para la infraestructura de la organización (por ejemplo, crítica, de TI, operacional) y los objetivos de la organización. .
V31	Nivel de madurez en ciberseguridad	Está relacionado con el nivel de cumplimiento de la organización frente al estándar de modelo de madurez del sector eléctrico SE-C2M2.
V32	Cadena de suministro	De acuerdo a las necesidades de la gestión de la operación, poder mantener (desde el punto de vista de la resilencia) la capacidad de tomar decisiones objetivas orientadas a sostener el poder de adquisición y el flujo de insumos (técnicos, económicos, humanos, seguros, confiables etc), con orientación estratégica seleccionados y estudiados como un grupo de proveedores que sean confiables (espionaje, países no amigos, proveedores originarios de países hostiles) , con capacidad de respuesta rápida.
V33	Interdependencia de los procesos/negocios	Disminuir los riesgos de afectación de la continuidad operativa o de TO, desde otra unidad organizacional, empresas filiales, contratistas que tienen alguna relación de confianza o cercanía con el proceso operativo y mantenimiento.
V34	Operación local en subestaciones con personal	Reestablecer y/o mantener la continuidad del servicio y la operación, mientras se llega a la disponibilidad y normal funcionamiento de las TO, a través del entrenamiento de una cantidad mínima de personal técnico, operativo a nivel local, sin la dependencia de personas exclusivas y garantizando un medio de comunicación de voz operativa.
V35	Esquemas flexibles y seguros para la atención no centralizada de eventos sobre las plataformas de TO	Estrategias técnicas y operativas para la atención de eventos y recuperación de la continuidad de las TO de manera distribuida, remota o acceso a la red en puntos satélites (o extendidos de la red en instalaciones seguras de la Empresa), bajo condiciones de acceso seguro a las plataformas, verificando la efectividad de la seguridad y probando el funcionamiento del esquema.

De acuerdo con las variables identificadas y claramente definidas por el consenso de expertos, se procedió a crear una matriz de valoración, en la cual se califica por cada uno de los expertos el nivel de influencia de una variable sobre las otras, teniendo en cuenta la siguiente escala de valoración:

0. Sin influencia
1. Influencia baja
2. Influencia media
3. Influencia alta

Con base en esta escala, la influencia de cada una de las variables sobre las otras es calificada por cada de uno de los expertos, a través de una encuesta basada en una matriz cuadrada de 35 por 35. Se obtuvieron 9 encuestas producto de la valoración de los diferentes expertos.

Para poder encontrar la tendencia de cada una de las 1.225 respuestas se empleó la moda para identificar cual es la respuesta que más se repite en la consolidación de respuestas de los diferentes expertos.

- **Identificación de las Fuerzas Motrices - Matriz de influencias directas – MDI**

Empleando la herramienta MICMAC, se identifican cuáles son las variables que tienen mayor motricidad e influencia sobre las otras y cuáles son las variables más dependientes. Para ello se utilizó el software MICMAC Desarrollado por LIPSOR - EPITA, versión 6.1.2 basado en las metodologías de prospectiva desarrolladas por GODET Y BOURSE en 1989.

Después de tabular las respuestas, consolidarlas y calcular la moda, se cargan los datos en el software, arrojando unos resultados estadísticos que son de valor para los análisis, encontrando cuáles variables son las realmente relevantes o dominantes en el modelo.

La influencia es la suma horizontal o filas y la suma vertical o columnas es la dependencia o las variables que más se dejan influir. Los valores más altos de la suma de las filas corresponden a las variables más influyentes y la variable con la suma más alta en la columna es la que más se deja influenciar.

Acciones sobre las variables que presentan valores más altos en la fila, influenciarán las otras, pero aún no es posible determinar si positiva o negativamente o si son las variables críticas del modelo, tomando como mínimo un puntaje de 70 sobre 100.

Tabla 10. Motricidad y dependencia de las variables

ıp workshop Window ?

N°	Variable	Total number of rows	Total number of columns
1	Posesión o control	64	70
2	Integridad y Autenticidad de la información proveniente y enviada al proceso o en el intercambio de información con fuentes exter...	62	62
3	Seguridad física de Activos Críticos	41	44
4	Configuración correcta de sistemas de TO	56	68
5	Desempeño de las TO y sus servicios esenciales.	53	53
6	Vulnerabilidad a riesgos psicosociales en personal clave de TO u operación.	23	29
7	Obsolescencia Tecnológica de los Activos.	26	24
8	Dependencia Tecnológica	22	34
9	Incorporación de tecnologías apropiadas al proceso	45	58
10	Innovación en ciberseguridad de TO	50	58
11	Retorno sobre la inversión en ciberseguridad.	69	51
12	Inclusión de la ciberseguridad en el ciclos de vida de los activos.	65	55
13	Conciencia Situacional del personal de TO	56	57
14	Idoneidad del personal de TO	52	89
15	Confidencialidad de la información sensible (Operacional y de TO)	66	47
16	Control sobre el servicio de telecomunicaciones de terceros que soportan servicios IC.	37	50
17	Afectación del SAFETY	79	61
18	Efectividad de las contramedidas	83	64
19	Resiliencia de los sistemas de TO	84	55
20	Conocimiento de la situación	58	68
21	Respuesta oportuna ante eventos de ciberseguridad	82	71
22	Controles suplementarios	70	47
23	Utilidad	44	26
24	Cumplimiento normativo, legal y regulatorio de ciberseguridad	91	88
25	Concienciación Directivas	49	83
26	Concienciación Operación	64	84
27	Gestion y Retención del Talento Humano	24	72
28	Ejercicios de Manejo de Eventos, de Recuperación de Servicio y de recuperación. Control	65	67
29	Administración de riesgos	88	87
30	Gestión de amenazas y vulnerabilidades	81	62
31	Nivel de madurez en ciberseguridad	89	99
32	Cadena de suministro	29	47
33	Interdependencia de los procesos/negocios	50	38
34	Operación local en subestaciones con personal	63	45
35	Esquemas flexibles y seguros para la atención no centralizada de eventos sobre las plataformas de TO	73	40
	Totals	2053	2053

Mientras que las variables con mayor peso en la columna o mayor dominadas son:

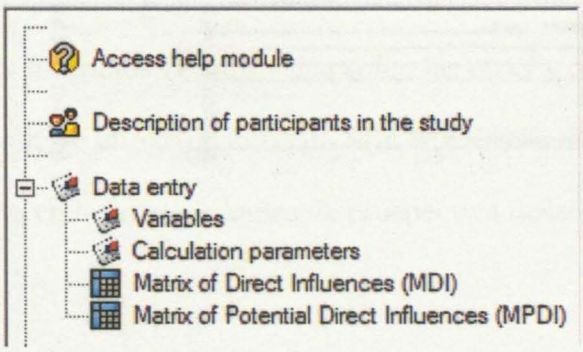
Tabla 11. Motricidad y dependencia de las variables

ıp workshop Window ?

N°	Variable	Total number of rows	Total number of columns
1	Posesión o control	64	70
2	Integridad y Autenticidad de la información proveniente y enviada al proceso o en el intercambio de información con fuentes exter...	62	62
3	Seguridad física de Activos Críticos	41	44
4	Configuración correcta de sistemas de TO	56	68
5	Desempeño de las TO y sus servicios esenciales.	53	53
6	Vulnerabilidad a riesgos psicosociales en personal clave de TO u operación.	23	29
7	Obsolescencia Tecnológica de los Activos.	26	24
8	Dependencia Tecnológica	22	34
9	Incorporación de tecnologías apropiadas al proceso	45	58
10	Innovación en ciberseguridad de TO	50	58
11	Retorno sobre la inversión en ciberseguridad.	69	51
12	Inclusión de la ciberseguridad en el ciclos de vida de los activos.	65	55
13	Conciencia Situacional del personal de TO	56	57
14	Idoneidad del personal de TO	52	89
15	Confidencialidad de la información sensible (Operacional y de TO)	66	47
16	Control sobre el servicio de telecomunicaciones de terceros que soportan servicios IC.	37	50
17	Afectación del SAFETY	79	61
18	Efectividad de las contramedidas	83	64
19	Resiliencia de los sistemas de TO	84	55
20	Conocimiento de la situación	58	68
21	Respuesta oportuna ante eventos de ciberseguridad	82	71
22	Controles suplementarios	70	47
23	Utilidad	44	26
24	Cumplimiento normativo, legal y regulatorio de ciberseguridad	91	88
25	Concienciación Directivas	49	83
26	Concienciación Operación	64	84
27	Gestion y Retención del Talento Humano	24	72
28	Ejercicios de Manejo de Eventos, de Recuperación de Servicio y de recuperación Control	65	67
29	Administración de riesgos	88	87
30	Gestión de amenazas y vulnerabilidades	81	62
31	Nivel de madurez en ciberseguridad	89	99
32	Cadena de suministro	29	47
33	Interdependencia de los procesos/negocios	50	38
34	Operación local en subestaciones con personal	63	45
35	Esquemas flexibles y seguros para la atención no centralizada de eventos sobre las plataformas de TO	73	40
	Totals	2053	2053

Así mismo, es posible concluir de manera temprana algunas características del modelo a partir de algunos parámetros:

Tabla 12. Características generales del modelo



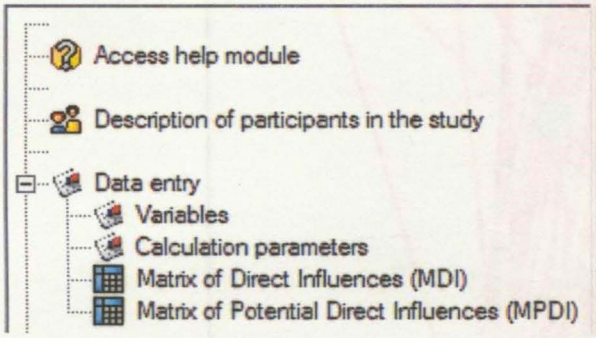
Matrix size	35
Number of iterations	4
Number of zeros	392
Number of ones	125
Number of twos	196
Number of threes	512
Number of P	0
Total	833
Fillrate	68%

Los resultados anteriores muestran que las variables presentan una fortaleza en la influencia de sus variables entre sí. De las 833 opciones de respuesta, hay 512 números elegidos como tres (3) que significa que existe una fuerte relación y 392 ceros o combinaciones donde no hay relación. El 68% de las variables tienen algún tipo de influencia de 1 a 3.

- **Estabilidad del modelo**

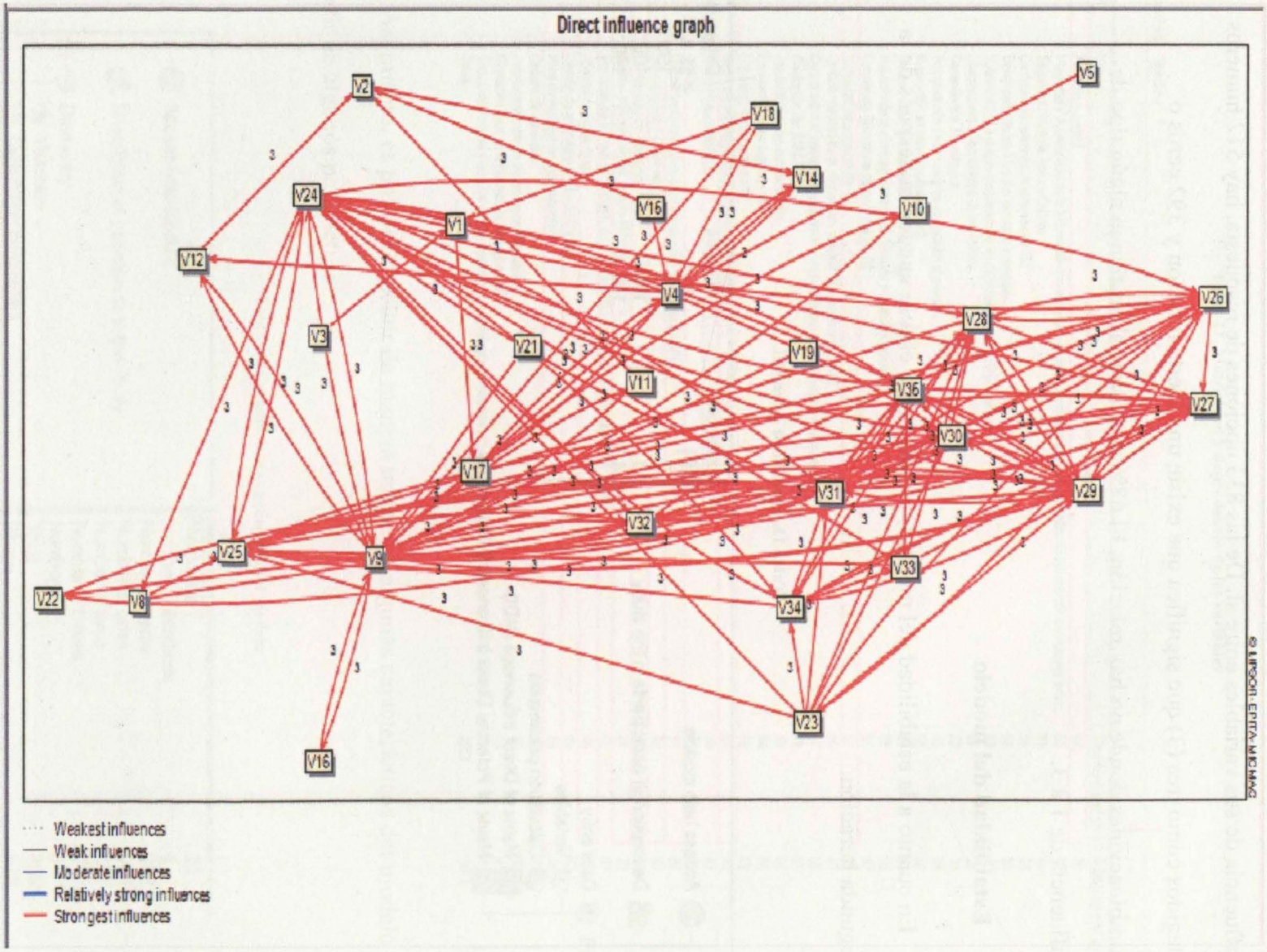
En cuanto a la estabilidad del modelo, se nota como esta se encuentra después de la segunda iteración.

Tabla 13. Estabilidad del modelo



Iteration	Influence	Dependence
1	101 %	98 %
2	100 %	100 %
3	100 %	100 %
4	100 %	100 %

Gráfica 12. Matriz de influencia directa

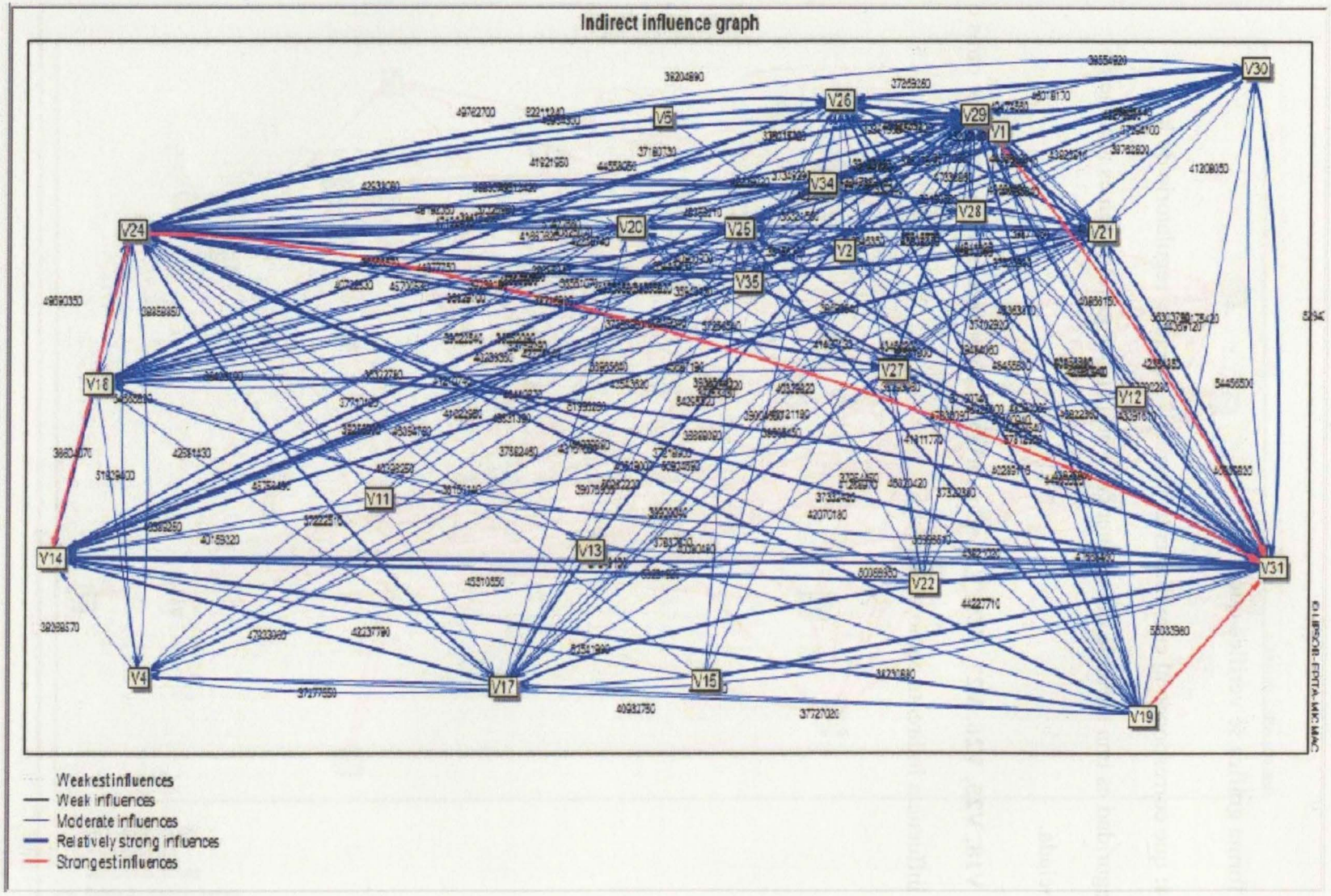


De forma gráfica se verifica que:

V24: que corresponde al cumplimiento normativo, legal y regulatorio de la ciberseguridad es una variable que influencia a otras pero que también es alta mente influenciada.

14, V18, V25, V26, V27, V29, V31 son variables altamente influenciadas por otras o tienen influencia indirecta como se muestra:

Gráfica 13. Matriz de influencia indirecta

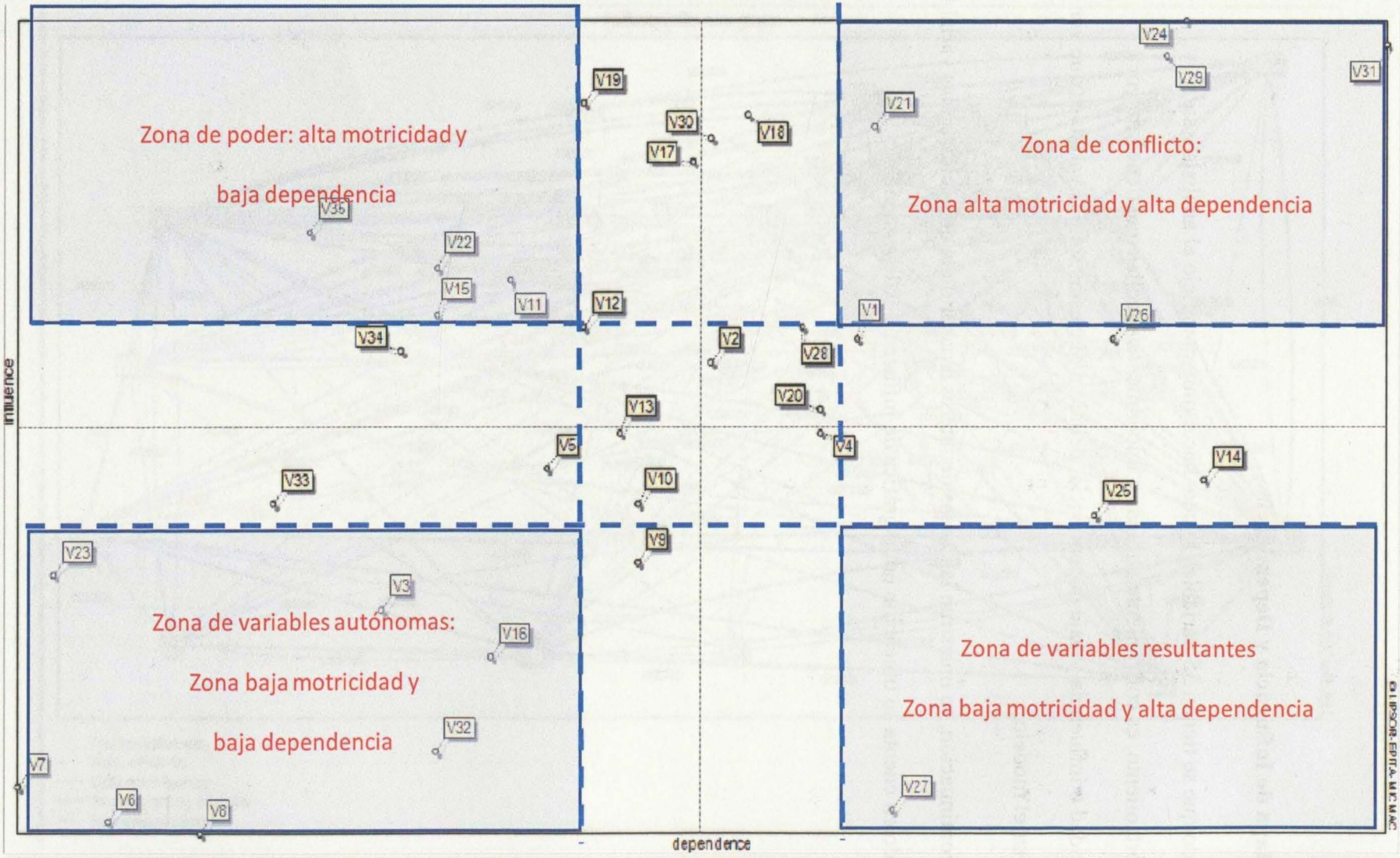


- **Mapa de Influencia y Dependencia**

Dado que se tienen 35 variables lo cual hacer muy complejo el análisis y su comportamiento, es conveniente enfocarse inicialmente aquellas que tienen mayor motricidad o influencia y baja dependencia, debido a que estas son las variables que van a gobernar el modelo.

A continuación, se muestran las zonas de interés a partir de la ubicación de las variables, teniendo en cuenta su ubicación en la gráfica de influencia y dependencia.

Gráfica 14. Mapa de influencia y dependencia directa



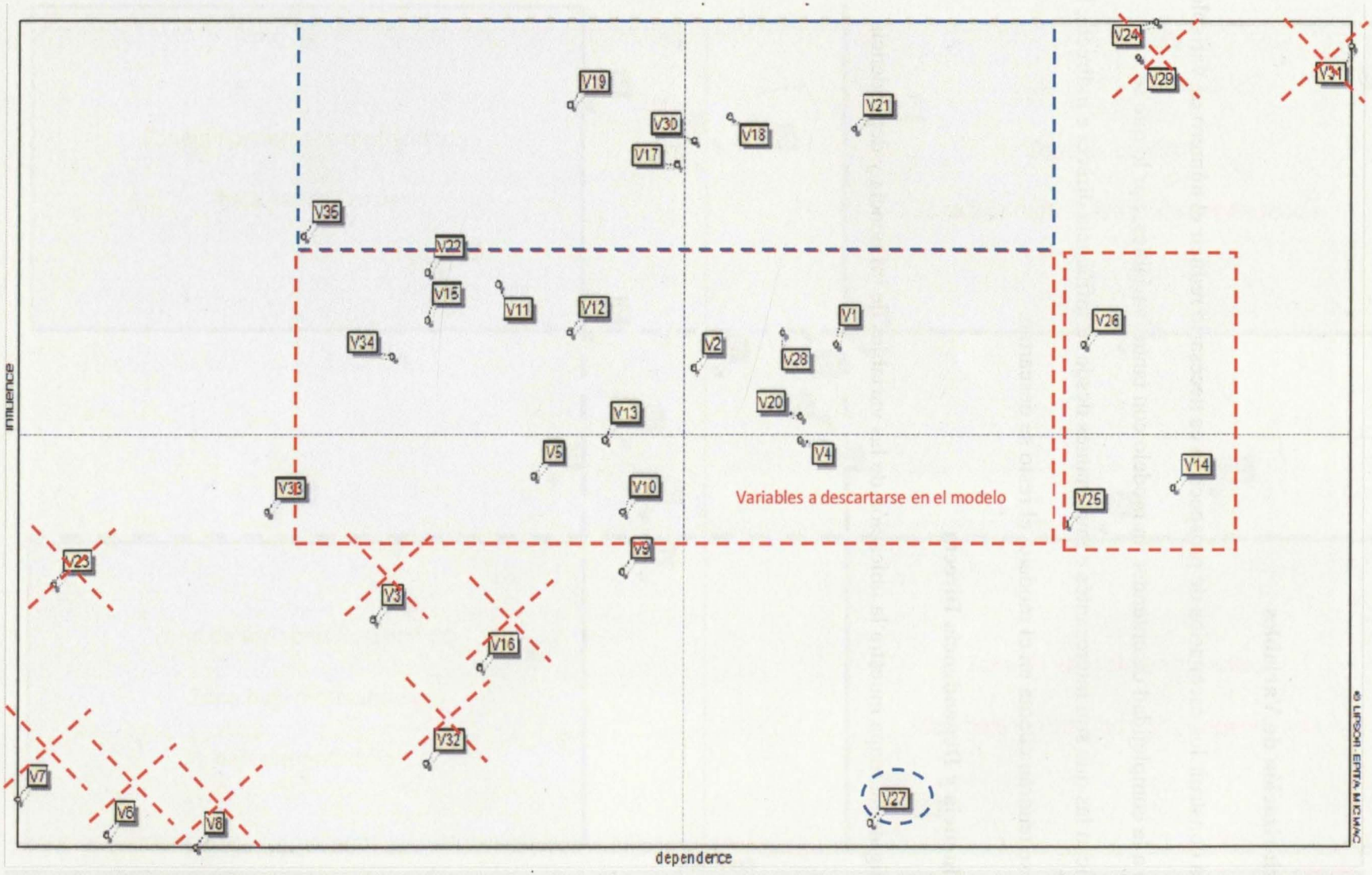
- **Priorización de Variables**

Para construir los escenarios de prospectiva es necesario reducir el número de variables, debido a la complejidad de entender un modelo con tantas variables, por lo que se identifican las que son interesantes e importantes desde su influencia directa e indirecta, las cuales se tendrán cuenta en el modelo, el resto se descartan.

- **Influencia y Dependencia Directa**

El siguiente mapa muestra la ubicación de las variables de influencia y dependencia directa.

Gráfica 15. Mapa de Influencia y Dependencia Directa



Se evidencia que en la zona de conflicto **V24, V29 y V31** son variables que si bien influyen directamente sobre otras variables en el modelo, a su vez también tienen una alta dependencia de otras, por lo que deben descartarse como variables motrices, debido a que su comportamiento también depende de otras.

V17, V18, V19, V21, V22, V30, V35, son variables de alta influencia y dependencia media o relativa por lo que son candidatas para incluir en el modelo.

V1, V2, V4, V5, V9, V10, V11, V12, V13, V15, V20, V28, V33, V34, se descartan porque están en una zona muy cercana al eje de influencia y baja dependencia relativa.

V3, V16, V32 deben ser descartadas debido a su baja influencia y dependencia medio baja.

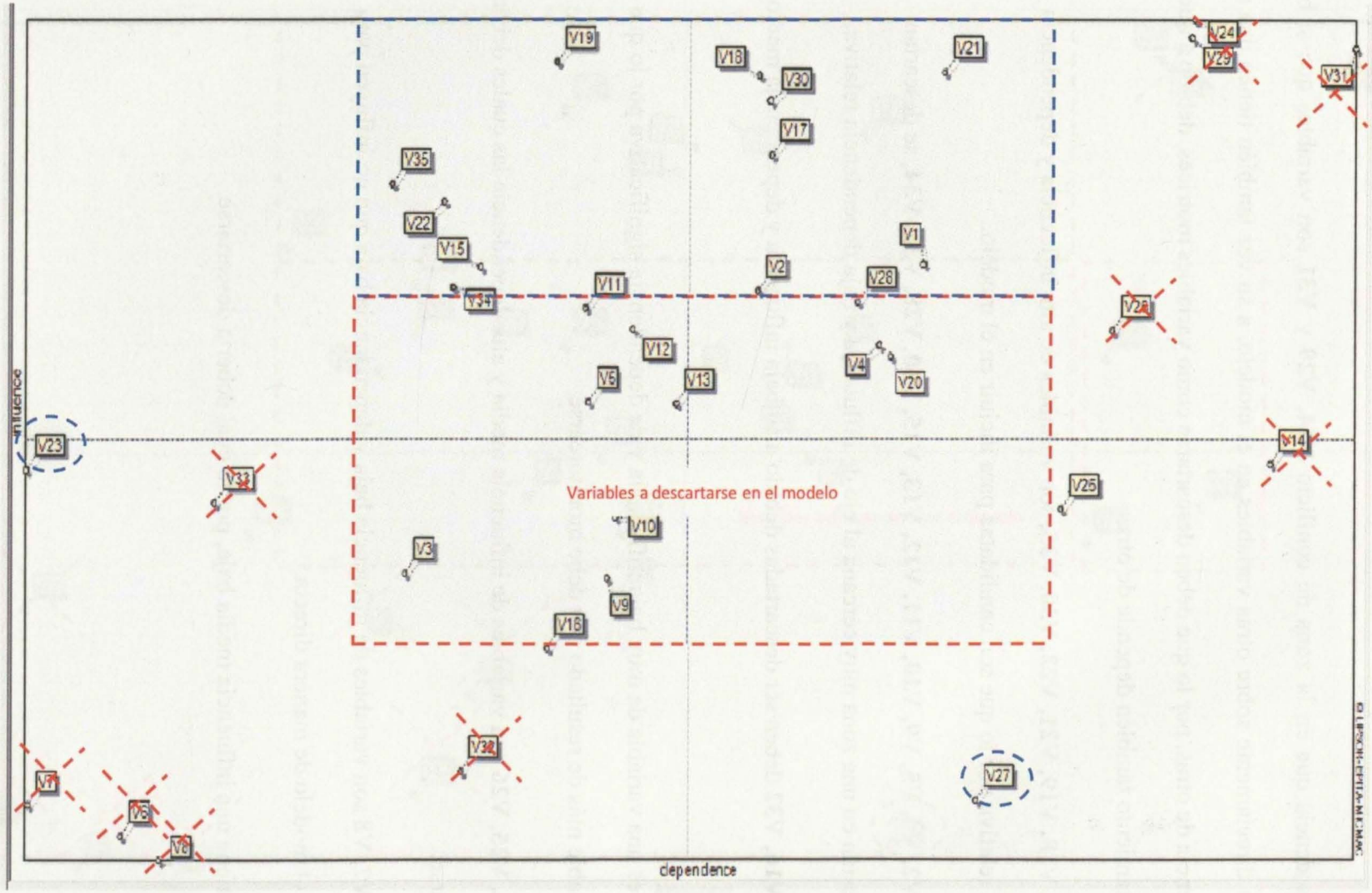
V27 es una variable de muy baja influencia y de dependencia significativa por lo que es una variable más de resultado que debe monitorearse.

V14, V25, V26 son variables de influencia media y alta dependencia las cuales deben descartarse.

V6, V7, V8 son variables de influencia baja y dependencia baja que no influyen para nada en el modelo de manera directa.

V23 tiene una influencia media baja, por lo cual debería descartarse.

Gráfica 16. Mapa de Influencia y Dependencia Indirecta



V24, V29 y V31 son variables de mayor influencia indirecta a través de otras variables en el modelo, pero al igual que en el análisis de influencia directa, también presentan una alta dependencia, por lo que debe descartarse, debido a que su comportamiento depende de otras.

V17, V18, V19, V21, V22, V30, V35, son variables que presentan comportamiento de alta influencia indirecta y coinciden con las identificadas en el gráfico de influencia directa para el mismo comportamiento. En este punto se incluyen **V1** y **V15** como variables adicionales. Son variables de alta influencia y dependencia indirecta media o relativa por lo que son candidatas para incluir en el modelo.

V1, V2, V4, V5, V10, V11, V12, V13, V15, V20, V28, V33, V34, se descartan porque están en una zona muy cercana al eje de influencia y baja dependencia relativa.

V3, V9, V16, V10 deben ser descartadas debido a su baja influencia y dependencias media.

V27 es una variable de muy baja influencia y de dependencia significativa por lo que es una variable de resultado que debe monitorearse.

V14, V25, V26 son variables de influencia media y alta dependencia las cuales deben descartarse.

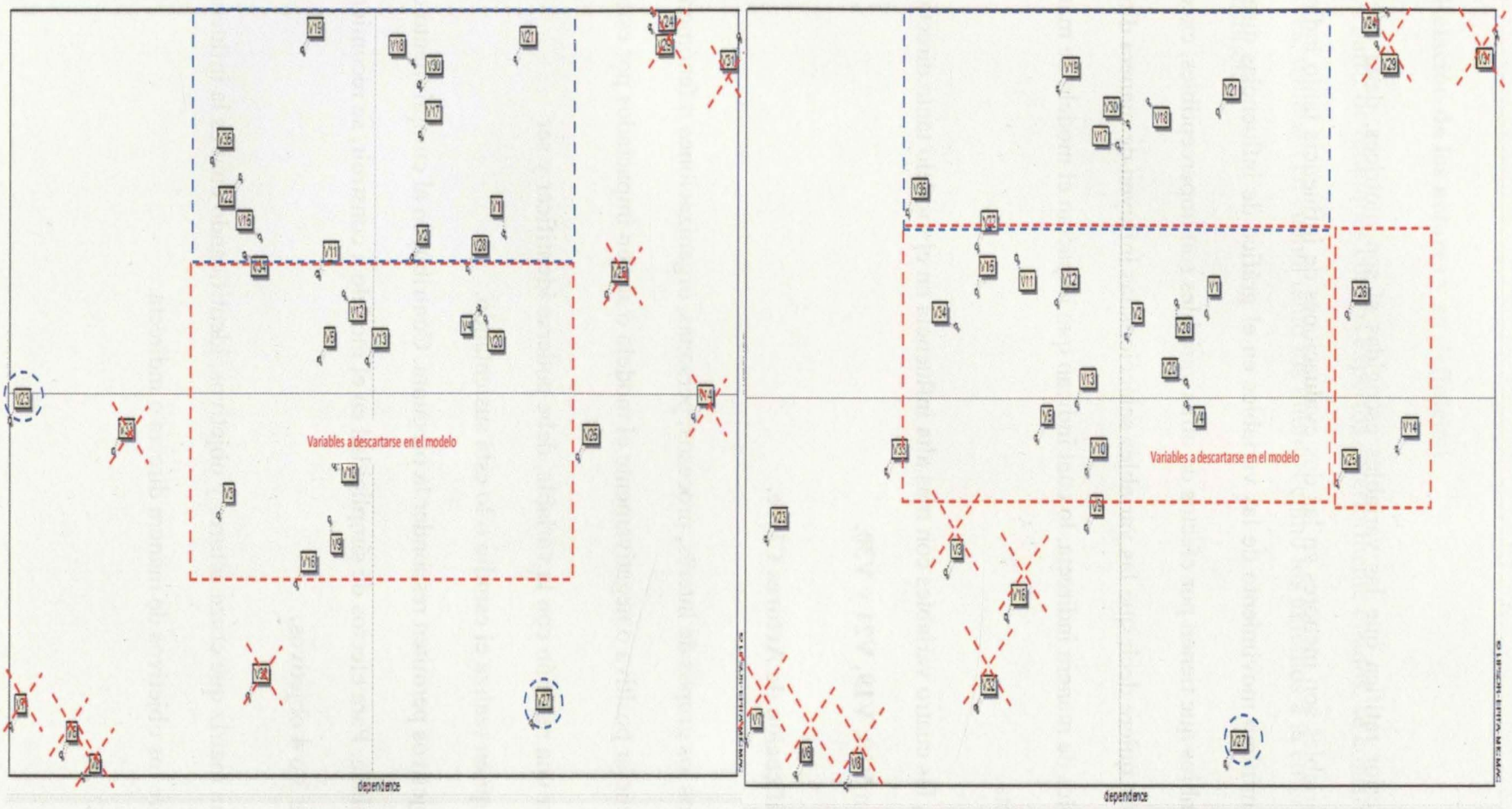
V3, V16, presentan una influencia y dependencia media baja.

V6, V7, V8 y **V32** son variables de influencia baja y dependencia baja que no influyen para nada en el modelo de manera directa.

V33 presenta una influencia indirecta medio baja y baja dependencia por lo que debe ser descartada.

Al comparar los dos mapas se tiene:

Gráfica 17. Comparación de los mapas de influencia y dependencias directas e indirectas



El gráfico anterior ratifica que las variables escogidas sí son motrices, dado que los cambios de las variables son menores en las dos evaluaciones de influencia tanto indirecta como directa. El mínimo movimiento de las variables en el gráfico de influencias directas indica que los cambios que tienen por efectos de otras variables son imperceptibles, excepto por **V15 y V1**. Esto quiere decir que las variables seleccionadas influyen de manera directa e impactan variables de manera indirecta, lo cual indican que impactan el modelo de manera indirecta e indirecta.

En conclusión, las cuatro variables con más alta influencia en el modelo tanto directa como indirecta son **V18, V19, V21** y **V30.**

5.3.3.1. Identificación de Actores Clave.

Actores: Son todos los grupos de interés, procesos, personas, organizaciones o fenómenos que pueden influenciar positiva o negativamente el modelo o se ven impactados por este.

El actor debe tener una relación con la variable, debe poderse identificar y ser independiente de quien realiza el estudio o lo está sustentando.

Objetivos: los objetivos permiten responder la pregunta. Contribuyen al cumplimiento de la pregunta formulada. Para efectos de simplicidad en el modelo a construir, se recomienda no trabajar más de 3 o 4 objetivos.

MACTOR: es una matriz que cruza actores y objetivos, identificando cual es la influencia de los actores sobre los objetivos de manera directa o indirecta.

- **Relación de los actores y su definición**

A partir de reuniones con los expertos anteriormente citados, se construyó la matriz de actores, teniendo en cuenta tanto los internos como los externos a la empresa de distribución.

Tabla 14. Relación de actores

	Nombre de la variable	Descripción de variables
AC1	**Atacante interno**	Cualquier miembro de la organización con capacidad para poder hacer daño o afectación a la operación empleando medios cibernéticos.
AC2	**Atacante externo**	Cualquier individuo, organización, estado, competidor, delicuente, u otro interesado en afectar, hacer daño, extorsionar a EPM, con capacidad de afectación a la operación empleando medios cibernéticos.
AC3	**Servicios corporativos prestados a la operación**	Servicios del tipo corporativos o de apoyo que se prestan como soporte al funcionamiento de las TO (Centros de Control, Telecomunicaciones, automatizaciones).
AC4	**Contratistas**	Empresas que pretan servicios a EPM con su personal propio, mediante una relación contractual. Ejemplo: Mantenimientos, correlación de eventos.
AC5	**Unidad Operación Integrada T&D Energía - UOI**	Unidad organizacional de EPM, encargada de operar remotamente desde el centro de control, la infraestructura eléctrica de subestaciones, líneas, redes de distribución a través de planes de operación y contingencia.
AC6	**Unidad Subestaciones y Líneas -USUL y Región Antioquia**	Unidad organizacional de EPM, encargada del mantenimiento de los equipos eléctricos de subestaciones y los equipos de control y protecciones de las mismas. Encargada de la coordinación de la operación local de las subestaciones a través de operadores en sitio, en situaciones contingencia.
AC7	**Unidad Soporte a Tecnologías de Operación T&D Energía**	Unidad organizacional de EPM, encargada de garantizar la continuidad de las tecnologías de operación, (infraestructura SCADA, Telecomunicaciones para el control, automatización de las subestaciones) y ciberseguridad de las TO.
AC8	**Operadores de telecomunicaciones (GPRS, FO...)**	Empresas de telecomunicaciones que prestan servicios de telecomunicaciones, que soportan funciones de operación, arrendamiento de FO oscura, enlaces de telecomunicaciones, GPRS, enlaces via radio, entre otros.
AC9	**CREG**	Comisión de Regulación de Energía y Gas.
AC10	**CNO (Acuerdos de Cibersguridad)**	Consejo Nacional de Operación - CNO.
AC11	**SSPPD**	Superintendencia de Servicios Públicos.
AC12	**Gerencia Control Interno (Auditorías)**	Gerencia de Control Interno
AC13	**Mindefensa (CCOCI, Policia, Ministerio de Defensa - Infraestructuras Críticas)**	Unidades organizacionales del Ministerio de defensa relacionadas con Infraestructuras Críticas. Comando Conjunto Cibernético CCOCI, Ministerio de Defensa.
AC14	**Operador Nacional - XM**	Operador Nacional
AC15	**Otros agentes**	Otros generadores, otros distribuidores, centros de control.

Se identifican las relaciones entre los actores y las variables que influencian.

Tabla 15. Relaciones entre los actores y las variables que influencian.

Actor	Variables con las que tiene relación
AC1: Atacante Interno	• V1: Posesión del control. • V2: Integridad y autenticidad de la información proveniente y enviada al proceso. • V3: Seguridad de activos físicos. • V4: Configuración correcta de TO. • V12: Inclusión de ciberseguridad en el ciclo de vida de los activos. • V15: Confidencialidad de la Información. • V17: Afectación del SAFETY. • V19: Resiliencia de los sistemas de TO. • V21: Respuesta oportuna ante incidente de ciberseguridad. • V23: Utilidad.
AC2: Atacante Externo	• V1: Posesión del control. • V2: Integridad y autenticidad de la información proveniente y enviada al proceso. • V5: Desempeño de las TO y sus servicios esenciales. • V15: Confidencialidad de la Información. • V16: Control sobre el servicio de telecomunicaciones de terceros. • V17: Afectación del SAFETY.
AC3: Servicios corporativos prestados a la operación	• V5: Desempeño de las TO y sus servicios esenciales. • V6: Vulnerabilidad a riesgos psicosociales en personal clave de TO u operación. • V15: Confidencialidad de la Información. • V16: Control sobre el servicio de telecomunicaciones de terceros. • V21: Respuesta oportuna ante eventos de ciberseguridad. • V33: Interdependencia de los procesos/Negocios.

AC4: Contratistas	• V5: Desempeño de las TO y sus servicios esenciales. • V15: Confidencialidad de la Información. • V16: Control sobre el servicio de telecomunicaciones de terceros. • V21: Respuesta oportuna ante eventos de ciberseguridad.
AC5: Unidad Operación Integrada T&D Energía – UOI	• V1: Posesión del control. • V6: Vulnerabilidad a riesgos psicosociales en personal clave de TO y operación. • V15. Confidencialidad de la información sensible (operacional y de TO). • V17: Afectación de SAFETY. • V20: Conocimiento de la situación. • V21: Respuesta oportuna ante eventos de ciberseguridad. • V26: Concienciación en operación. • V28: Ejercicios de manejo de eventos, de recuperación de servicio y de recuperación del control. • V30: Gestión de amenazas y vulnerabilidades. • V35: Esquemas flexibles y seguros para la atención no centralizada de eventos sobre las plataformas de TO.
AC6: Unidad Subestaciones y Líneas -USUL y Región Antioquia	• V17: Afectación del SAFETY. • V20: Conocimiento de la situación. • V21: Respuesta oportuna ante eventos de ciberseguridad. • V28: Ejercicios de manejo de eventos, de recuperación de servicio y recuperación de control. • V34: Atención local en subestaciones con personal.
AC7: Unidad Soporte a Tecnologías de	• V1: Posesión o control. • V2: Integridad y autenticidad de la información proveniente y enviada al proceso. • V4: Configuración correcta de los sistemas de TO.

Operación T&D Energía	• V5: Desempeño de los TO y sus servicios esenciales. • V6: Vulnerabilidad a riesgos psicosociales en personal clave de TO. • V7: obsolescencia tecnológica de los Activos. • V11: Retorno sobre la inversión en ciberseguridad. • V12: inclusión de la ciberseguridad en el ciclo de vida de los activos. • V13: Conciencia situacional del personal de TO. • V14: Idoneidad del personal de TO. • V15: confidencialidad de la información sensible (Operacional y de TO). • V17: Afectación de SAFETY. • V18: Efectividad de las contramedidas. • V19: Resiliencia de los sistemas de TO. • V20: Conocimiento de la situación. • V21: Respuesta oportuna ante eventos de ciberseguridad. • V22: Controles suplementarios. • V23: Utilidad. • V24: cumplimiento normativo. • V26: Concienciación en la operación. • V28: Ejercicios de manejo de eventos, recuperación del servicio, y de recuperación del control. • V29: Administración de riesgos. • V30: Gestión de amenazas y vulnerabilidades. • V31: Nivel de madurez en ciberseguridad. • V35: Esquemas flexibles y seguros par a la atención no centralizada de eventos sobre plataformas de TO.
AC8: Operadores de	• V5: Desempeño de las TO y sus servicios esenciales. • V16: control sobre el servicio de telecomunicaciones de terceros. • V19: Resiliencia de los sistemas de TO.

telecomunicaciones (GPRS, FO…)	• V21: Respuesta oportuna ante eventos de ciberseguridad. • V28: Ejercicio de manejo de eventos, recuperación de servicio y recuperación de control. • V29: Administración de riesgos. • V30: Gestión de amenazas y vulnerabilidades.
AC9: CREG	• V9: Incorporación de tecnologías apropiadas al proceso. • V11: Retorno sobre l inversión de ciberseguridad. • V12: Inclusión de la ciberseguridad en el ciclo de vida de los activos. • V18: Efectividad de las contramedidas. • V19: Resiliencia de los sistemas de TO. • V21: Respuesta oportuna ante eventos de ciberseguridad. • V20: Conocimiento de la situación. • V22: Controles suplementarios. • V24: Cumplimiento normativo y legal. • V31: Nivel de madurez en ciberseguridad.
AC10: CNO (Acuerdos de Ciberseguridad)	• V17: Afectación del SAFETY. • V18: Efectividad de las contramedidas. • V19: Resiliencia de los sistemas de TO. • V20: Conocimiento de la situación. • V21: Respuesta oportuna ante eventos de ciberseguridad. • V24: Cumplimiento normativo o legal. • V30: Gestión de amenazas y vulnerabilidades. • V31: Nivel de madurez de la ciberseguridad.
AC11: SSPPD	• V5: Desempeño de las TO y sus servicios esenciales. • V9: Incorporación de tecnologías apropiadas al proceso. • V18: Efectividad de las contramedidas. • V19: Resiliencia de los sistemas de TO.

	• V21: Respuesta oportuna ante eventos de ciberseguridad.
AC12: Gerencia Control Interno (Auditorías)	• V5: Desempeño de las TO y sus servicios esenciales. • V6: Vulnerabilidad a riesgos psicosociales. • V9: incorporación de tecnologías adecuadas al proceso. • V12: Incorporación de la ciberseguridad en el ciclo de vida de los activos. • V18: Efectividad de las contramedidas. • V21: Respuesta oportuna ante eventos de ciberseguridad. • V22: controles suplementarios. • V26: Concienciación operación. • V28: Eventos de manejo de eventos, recuperación del servicio, y recuperación del control. • V30: Gestión de amenazas y vulnerabilidades.
AC13: Mindefensa (CCOCI, Policía, Ministerio de Defensa - Infraestructuras Críticas)	• V1: Posesión o control. • V3: Seguridad física de activos críticos. • V19: Resiliencia de los sistemas de TO. • V21: Respuesta oportuna ante eventos de ciberseguridad. • V24: Cumplimiento normativo, legal y regulatorio en ciberseguridad. • V25: Concienciación de directivas. • V28: ejercicios de manejo de eventos, recuperación de servicio y recuperación de control
AC14: Operador Nacional – XM (CCIRT)	• V21: Respuesta oportuna ante eventos de ciberseguridad. • V24: Cumplimiento normativo, legal y regulatorio en ciberseguridad. • V28: Ejercicios de manejo de eventos, de recuperación de servicio y de recuperación de control.
AC15: Otros agentes	• V5: Desempeño de las TO y sus servicios esenciales.

5.3.3.2. Objetivos del ejercicio de modelación:

- **OB1: Mantener altos niveles de usabilidad de las TO.**

Mantener la integridad de la correcta configuración y parametrización de las plataformas tecnológicas principal y respaldos de SCADA, Aplicaciones Operativas, Telecomunicaciones y Automatizaciones, de manera que siempre estén operativas y reflejen información fiel de proceso de campo y disponibles para ejecutar acciones operativas.

- **OB2: Implementar y mantener altos niveles de continuidad de las TO**

Implementar, mantener operativos y funcionales los planes de contingencia e infraestructura redundante en infraestructuras críticas, de manera que el proceso operativo no se vea interrumpido o afectado, frente a fallas en infraestructura o eventos de ciberseguridad.

- **OB3: Recuperar la infraestructura TO en el mínimo tiempo, bajo escenarios de ciberataque**

Recuperar la infraestructura de TO en menos de 2 horas de haberse presentado un ciberataque.

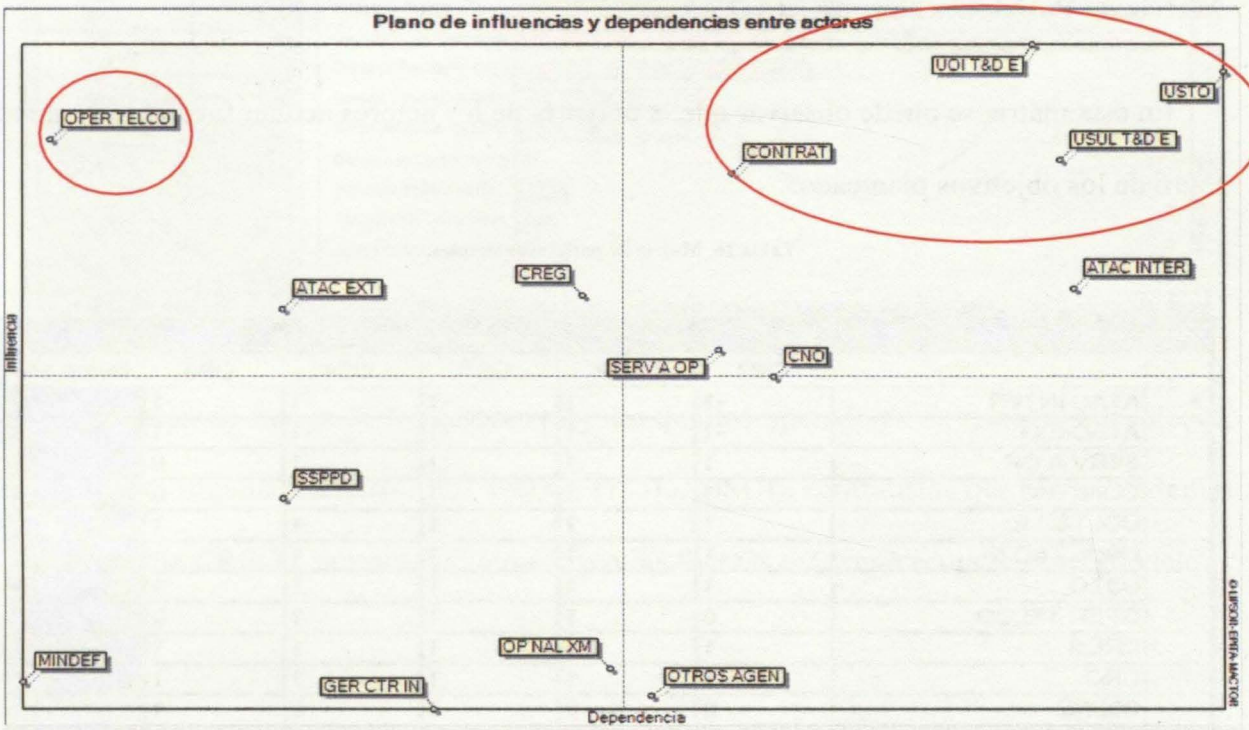
- **OB4: Mantener la posesión del control**

Mantener la posesión del control y la visibilidad de lo que ocurre en las plataformas del centro de control, la red de telecomunicaciones y automatizaciones en condiciones estables y bajo falla o ataque cibernético.

- **OB5: Gestionar técnica y financieramente la ciberseguridad**

Gestionar eficiente y sosteniblemente la ciberseguridad tanto desde lo técnico como lo financiero.

Gráfica 18. Plano de influencias y dependencias entre actores resultado de la metodología MACTOR.



Este plano muestra los actores más dominantes y los dependientes. Los más dominantes o con mayor influencia en círculo rojo.

Dado que algunos de los servicios emplean infraestructura de operadores de telecomunicaciones como FO, y redes, este actor es influyente en la continuidad de las telecomunicaciones que soportan la operación, por la calidad de los servicios que presta y los tiempos de respuesta ante eventos y fallos.

Así mismo el plano muestra que sobre la pregunta de investigación formulada, las tres unidades organizacionales Unidad Operación Integrada, Unidad Soporte a Tecnologías de Operación, Unidad Subestaciones y Líneas, y el personal contratista que apoya la operación y la ciberseguridad son altamente influyentes por las funciones y lo misional, pero a su vez dependen altamente de otros actores.

Matriz de Posiciones simples MAO

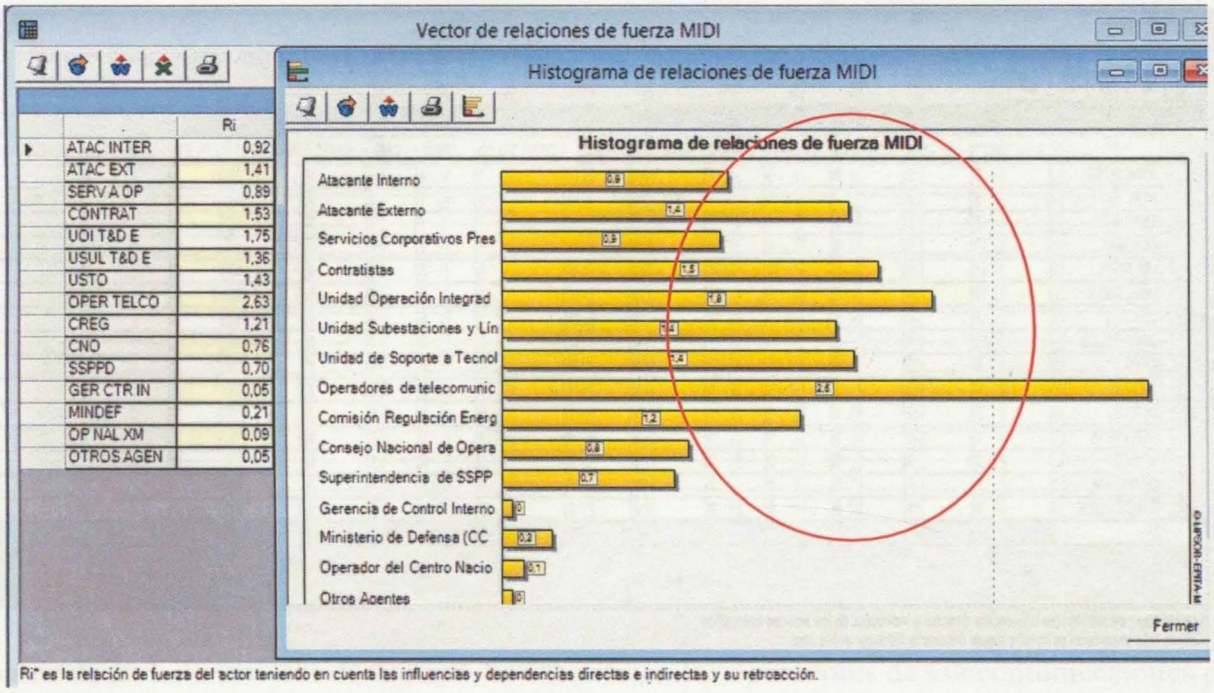
En esta matriz se puede observar que la mayoría de los actores actúan favorablemente al logro de los objetivos planteados.

Tabla 16. Matriz de posiciones simples.

	OB1	OB2	OB3	OB4	OB5	Suma abs
ATAC INTER	-1	-1	-1	-1	-1	5
ATAC EXT	-1	-1	-1	-1	-1	5
SERV A OP	1	1	1	1	0	4
CONTRAT	1	1	1	1	0	4
UOI T&D E	1	1	1	1	1	5
USUL T&D E	1	1	1	1	1	5
USTO	1	1	1	1	1	5
OPER TELCO	0	1	1	1	0	3
CREG	1	1	1	1	1	5
CNO	1	1	1	1	1	5
SSPPD	0	0	0	0	1	1
GER CTR IN	1	1	1	1	1	5
MINDEF	1	1	1	1	1	5
OP NAL XM	1	1	1	1	1	5
OTROS AGEN	1	1	1	1	1	5
Número de acuerdos	11	12	12	12	10	_
Número de desacuerdos	-2	-2	-2	-2	-2	_
Número de posicioones	13	14	14	14	12	_

-1 : actor desfavorable a la consecución del objetivo
0 : Posicion neutra
1 : actor favorable a la consecución del objetivo

Gráfica 19. Vector de relaciones de fuerza MIDI.



La relación de fuerza de los actores muestra que los operadores de telecomunicaciones, las unidades organizacionales UOI T&DE, USTO, USUL, contratistas que sirven en temas operativos, la CREG y atacantes externos, son las fuerzas más representativas del modelo.

Tabla 17. Matriz de influencias directas e indirectas MIDI.

Matriz de Influencias Directas e Indirectas (MIDI)

	ATAC INTER	ATAC EXT	SERV A OP	CONTRAT	UOI T&D	USUL T&D	USTO	OPER TELCO	CREG	CNO	SSPPD	GER CTR I	MINDEF	OP NAL XM	OTROS AGEN	Ii
ATAC INTER	9	2	8	9	7	10	11	1	4	4	3	6	1	3	2	71
ATAC EXT	9	6	7	6	7	10	12	5	1	2	2	4	0	1	2	68
SERV A OP	8	2	8	6	7	8	8	1	4	4	2	5	1	3	3	62
CONTRAT	14	5	9	9	10	11	11	4	4	6	2	5	1	3	3	88
UOI T&D E	13	4	9	10	13	11	13	4	8	9	4	5	2	7	8	107
USUL T&D E	10	4	7	7	10	10	13	1	6	8	4	5	2	6	7	90
USTO	13	6	8	8	12	15	19	1	6	8	4	5	2	7	8	103
OPER TELCO	12	5	9	11	11	9	11	2	5	4	3	4	1	4	4	80
CREG	6	2	4	5	7	6	7	0	6	10	4	3	2	7	7	70
CNO	4	2	3	3	7	6	6	0	7	9	3	2	1	7	7	58
SSPPD	2	2	1	1	4	4	4	0	4	6	2	1	1	5	5	40
GER CTR IN	1	0	1	1	1	1	1	0	1	1	0	1	0	1	0	9
MINDEF	0	0	0	0	2	0	2	0	2	2	1	0	0	2	2	13
OP NAL XM	0	0	0	0	2	0	2	0	2	4	1	0	1	2	3	15
OTROS AGEN	0	0	0	0	2	0	2	0	2	2	1	0	0	2	2	11
Di	92	34	66	67	89	91	103	17	56	70	34	45	15	58	61	898

Los valores representan las influencias directas e indirectas de los actores entre ellos :
Cuanto más importante es la cifra mayor influencia del actor sobre otro.

Esta matriz muestra la influencia directa e indirecta de un actor sobre otro. Los actores más influyentes son ciber atacantes, el agente interno y la SSPPD, mientras que el menos influyente es la operación local. De la misma forma, los actores más dependientes son la Unidad Soporte a Tecnologías de Operación, la Unidad Operación Integrada y el OR.

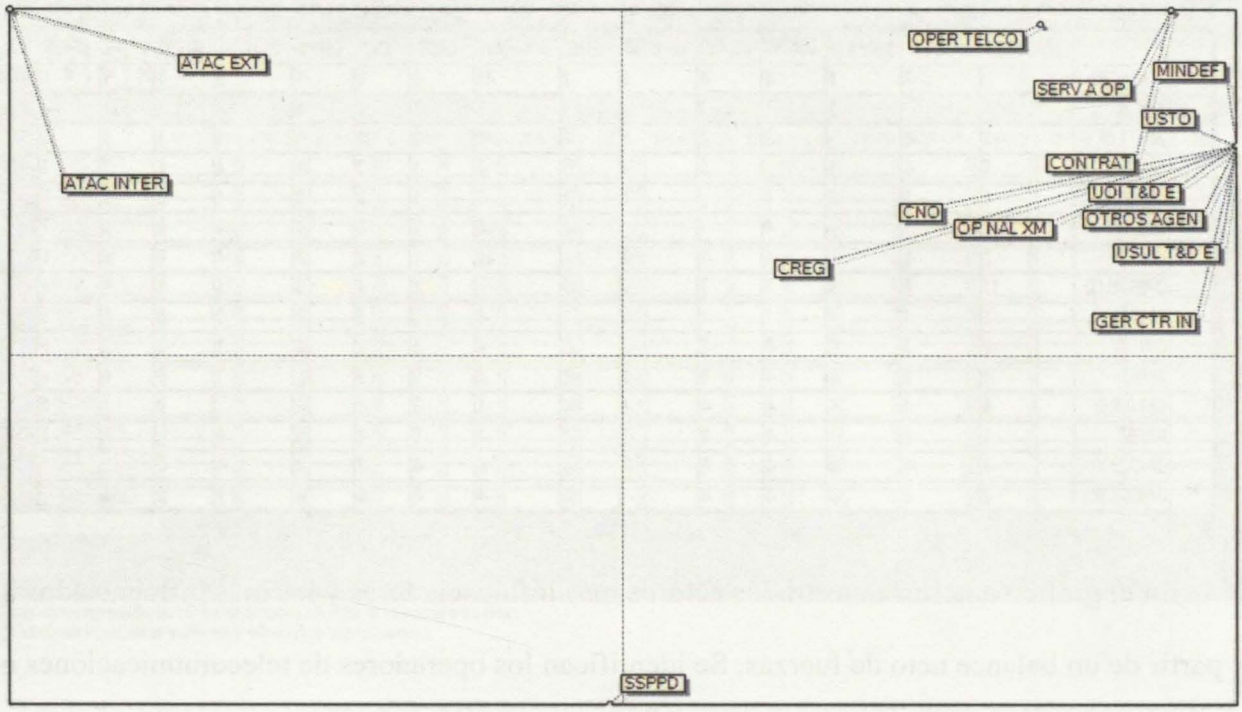
La siguiente matriz muestra el balance neto de las influencias.

Tabla 18. Balance neto de las influencias.

	ATAC INTER	ATAC EXT	SERV A OP	CONTRA	UOI T&D	USUL T&D	USTO	OPER TELC	CREG	CNO	SSPPD	GER CTR I	MINDEF	OP NAL	OTROS	Suma
ATAC INTER	_	-7	0	-5	-6	0	-2	-11	-2	0	1	5	1	3	2	-21
ATAC EXT	7	_	5	1	3	6	6	0	-1	0	0	4	0	1	2	34
SERV A OP	0	-5	_	-3	-2	1	0	-8	0	1	1	4	1	3	3	-4
CONTRAT	5	-1	3	_	0	4	3	-7	-1	3	1	4	1	3	3	21
UOI T&D E	6	-3	2	0	_	1	1	-7	1	2	0	4	0	5	6	18
USUL T&D E	0	-6	-1	-4	-1	_	-2	-8	0	2	0	4	2	6	7	-1
USTO	2	-6	0	-3	-1	2	_	-10	-1	2	0	4	0	5	6	0
OPER TELCO	11	0	8	7	7	8	10	_	5	4	3	4	1	4	4	76
CREG	2	1	0	1	-1	0	1	-5	_	3	0	2	0	5	5	14
CNO	0	0	-1	-3	-2	-2	-2	-4	-3	_	-3	1	-1	3	5	-12
SSPPD	-1	0	-1	-1	0	0	0	-3	0	3	_	1	0	4	4	6
GER CTR IN	-5	-4	-4	-4	-4	-4	-4	-4	-2	-1	-1	_	0	1	0	-36
MINDEF	-1	0	-1	-1	0	-2	0	-1	0	1	0	0	_	1	2	-2
OP NAL XM	-3	-1	-3	-3	-5	-6	-5	-4	-5	-3	-4	-1	-1	_	1	-43
OTROS AGEN	-2	-2	-3	-3	-6	-7	-6	-4	-5	-5	-4	0	-2	-1	_	-50

En el gráfico anterior muestra los actores más influenciadores y los más influenciados a partir de un balance neto de fuerzas. Se identifican los operadores de telecomunicaciones o quien haga sus veces al interior de la compañía, como quienes que ejercen una mayor influencia sobre los procesos o proyectos o la misión de los otros actores, seguidos de los atacantes externos, contratistas, y la unidad operación integrada. Los otros agentes y el operador nacional son los más influenciados por los valores y el signo negativo.

Gráfica 20. Matriz de convergencia entre actores.

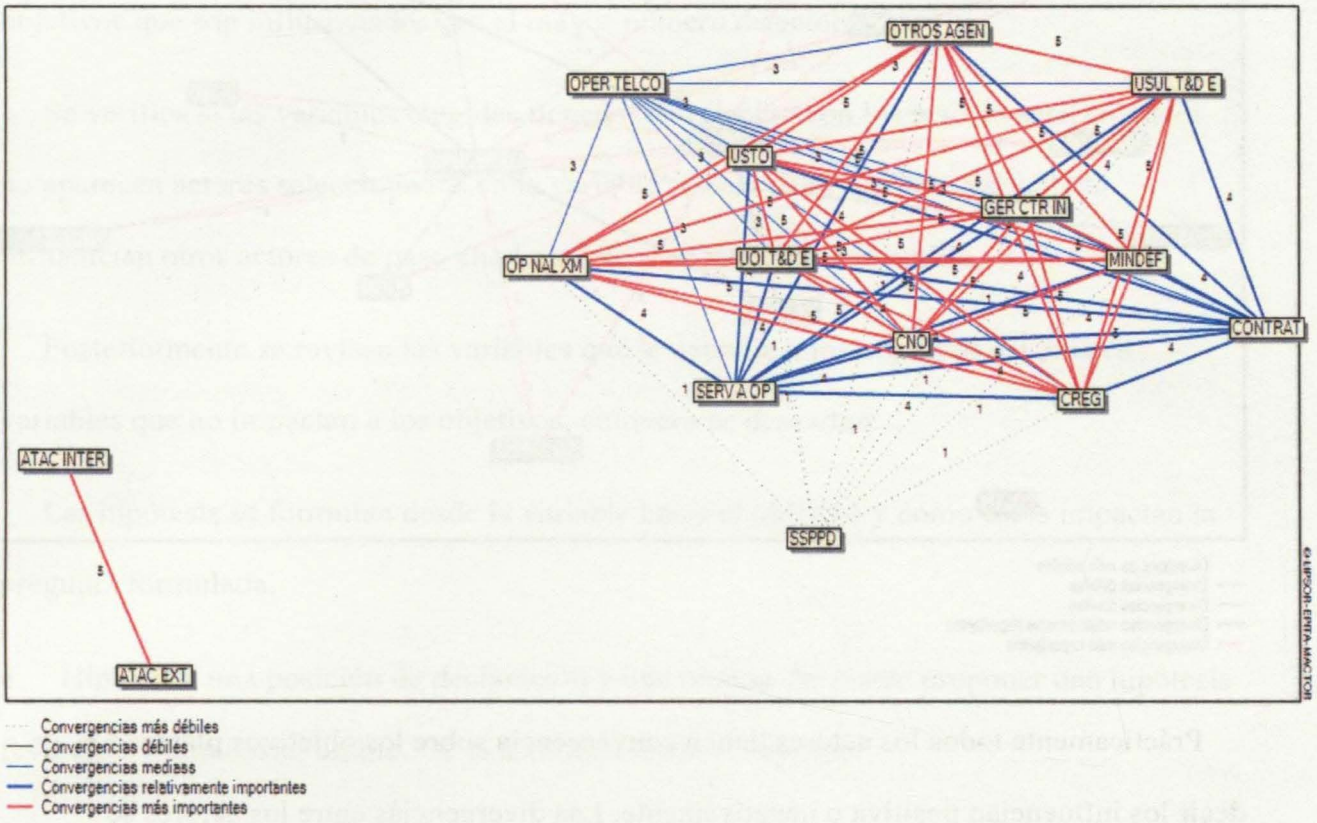


Este plano muestra la convergencia de actores sobre los objetivos. Básicamente existen dos grupos convergentes. El primer grupo corresponde a los atacantes externos e internos. El segundo grupo está compuesto por SERV A OP, CNO, USTO, CONTRATISTAS, UOI, USUL, GER CTR IN, MINDEF, OTROS AGENTES. Existen dos actores que no convergen son SSPPD y OPER TELCO. Esto último es de esperarse dado que la SSSPPD tiene como función sancionar incumplimientos y los OPER TELCO, prestan un servicio de Telecomunicaciones en general, pero no hacen parte del proceso de prestación del servicio de energía eléctrica.

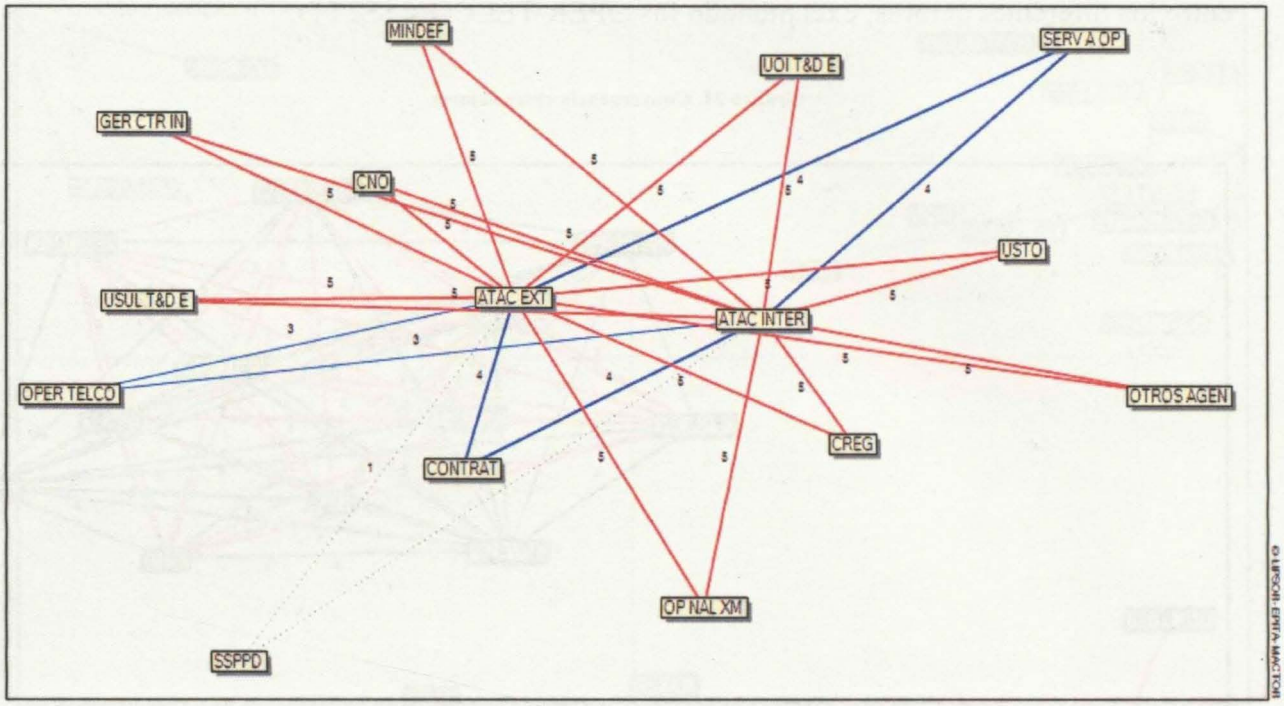
La no convergencia con los objetivos, indica que no existe una alineación directa entre los propósitos del actor con los objetivos del modelo.

El gráfico de convergencia muestra que hay una relación fuerte de convergencia de 3 y 4 entre los diferentes actores, exceptuando los OPER TELCO y SSPPD.

Gráfica 21. Convergencia entre actores.



Gráfica 22. Matriz de divergencia entre actores.



Prácticamente todos los actores tienen convergencia sobre los objetivos planteados, es decir los influencian positiva o negativamente. Las divergencias entre los actores se presentan entre cada uno de los atacantes internos y externos sobre el resto de los actores, con débil divergencia con CONTRAT, OPER TELCO y SERV OP. La divergencia más fuerte se presenta entre los Otros Agentes, los Atacantes Externos y el CNO.

5.3.3.3. Escenarios:

La prospectiva se enfoca en cuál va a ser el comportamiento de las variables y este comportamiento cómo impacta los objetivos. Los escenarios cargan las hipótesis con una probabilidad de ocurrencia que son valorados por los juicios de los expertos.

- Sucesos críticos: son eventos importantes que pueden tener un efecto en sobre las variables y los escenarios.

A partir de las variables priorizadas que son ocho y los actores dominantes, se filtran los objetivos que son influenciados por el mayor número de actores.

Se verifica si las variables elegidas tienen o no relación con los actores seleccionados. Si no aparecen actores seleccionados en la variable, quiere decir que esta variable la influencian otros actores de paso en el modelo y es razón para excluirla.

Posteriormente se revisan las variables que le apuntan a los objetivos. Si existen variables que no impactan a los objetivos, entonces se descartan.

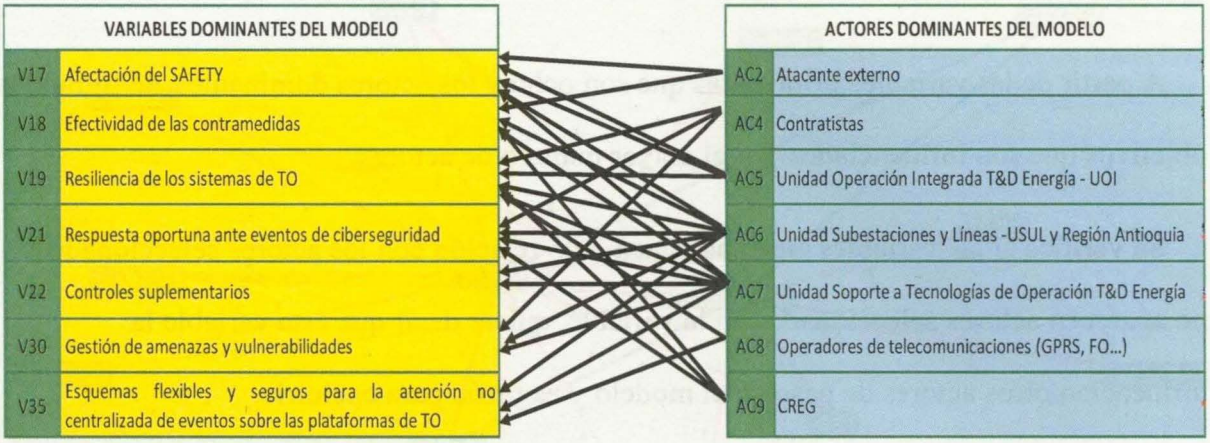
Las hipótesis se formulan desde la variable hacia el objetivo y cómo estos impactan la pregunta formulada.

- Hipótesis: una posición de declaración y una prueba. Se puede proponer una hipótesis favorable y otra desfavorable. De la actividad hacia el objetivo.

Como se tienen muchas variables que pueden crear muchas combinaciones de hipótesis. Para esto se recurre al MICMAC y se revisa la relación entre las variables y se seleccionan las más fuertes.

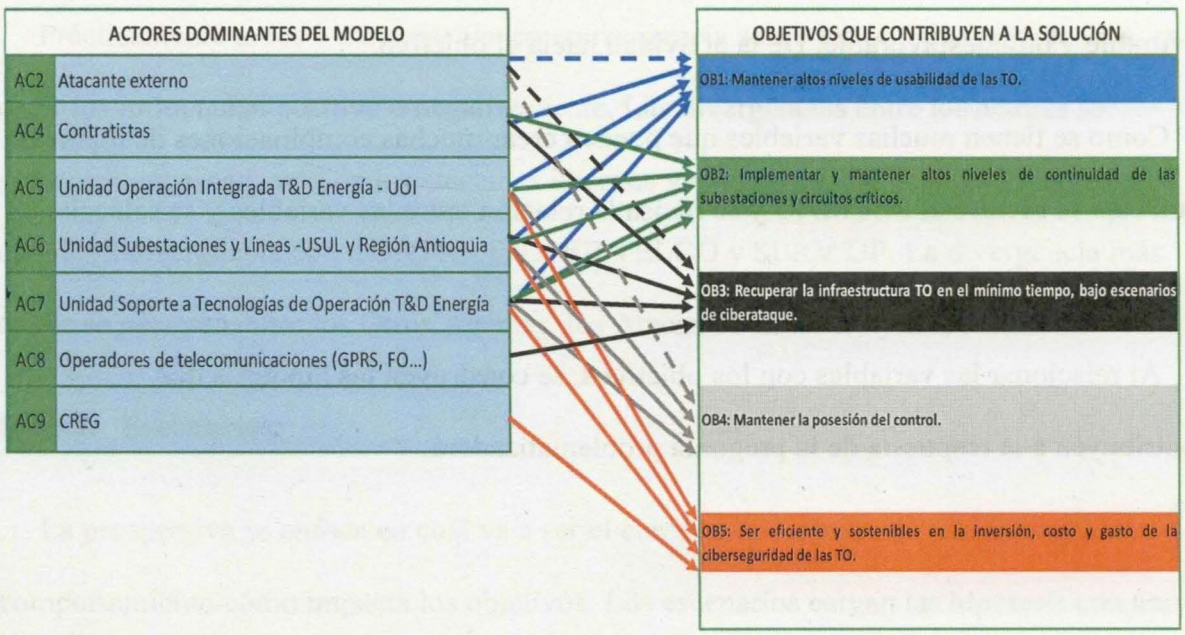
Al relacionar las variables con los objetivos, se construyen las hipótesis que contribuyen a la respuesta de la pregunta problematizadora.

Gráfica 23. Validación de los actores con las variables clave.

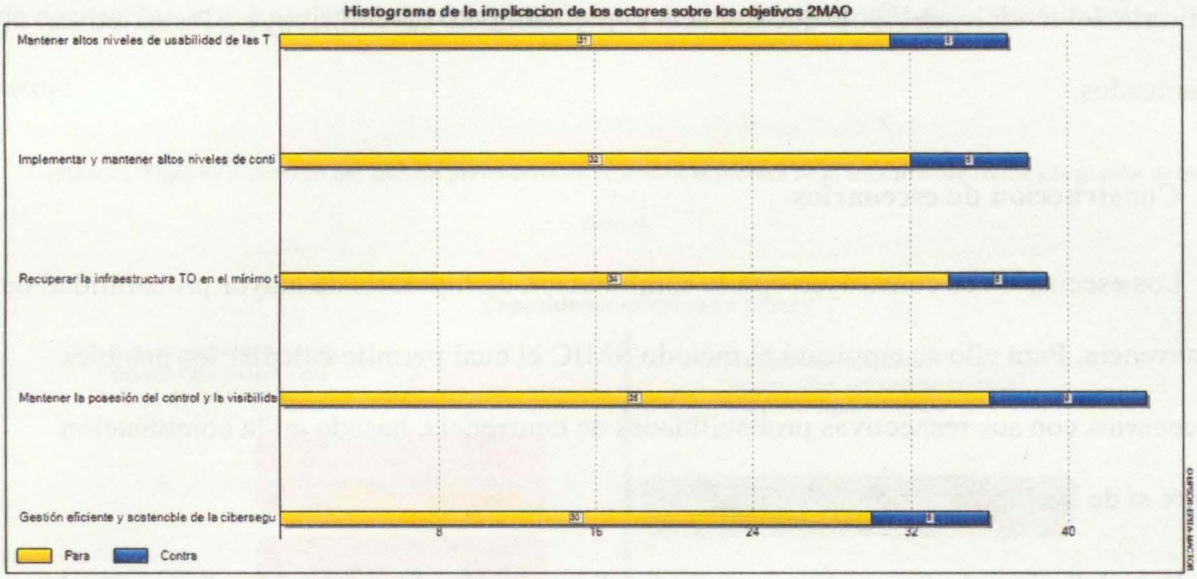


Debido a que todos los actores influencian todas las variables identificadas como clave, implican que no hay variables que deban ser eliminadas del modelo, por la razón de estar posiblemente influenciadas por actores de paso que no son los relevantes.

Gráfica 24. Relación de los actores con los objetivos.

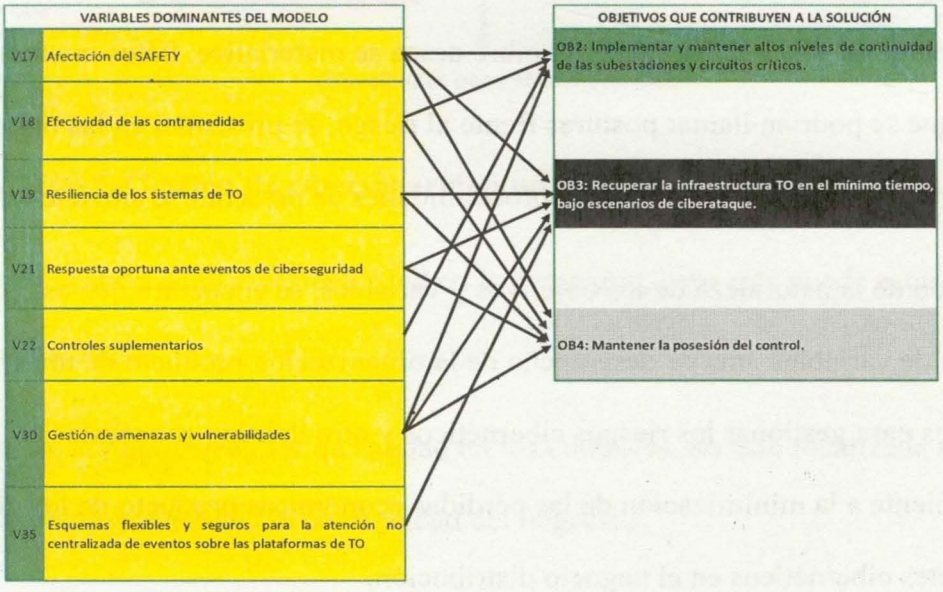


Gráfica 25. Implicaciones de los actores sobre los objetivos.



Se seleccionan los objetivos que son mayormente influenciados por los actores. En este caso serían OB2, OB3, OB4, a partir del MACTOR.

Gráfica 26. Contribución de las variables al logro de los objetivos.



Se verifica si existe alguna variable que no contribuya a ninguno de los objetivos, para retirarla del modelo, debido a que impacta el modelo, pero no contribuye a los objetivos planteados.

- **Construcción de escenarios**

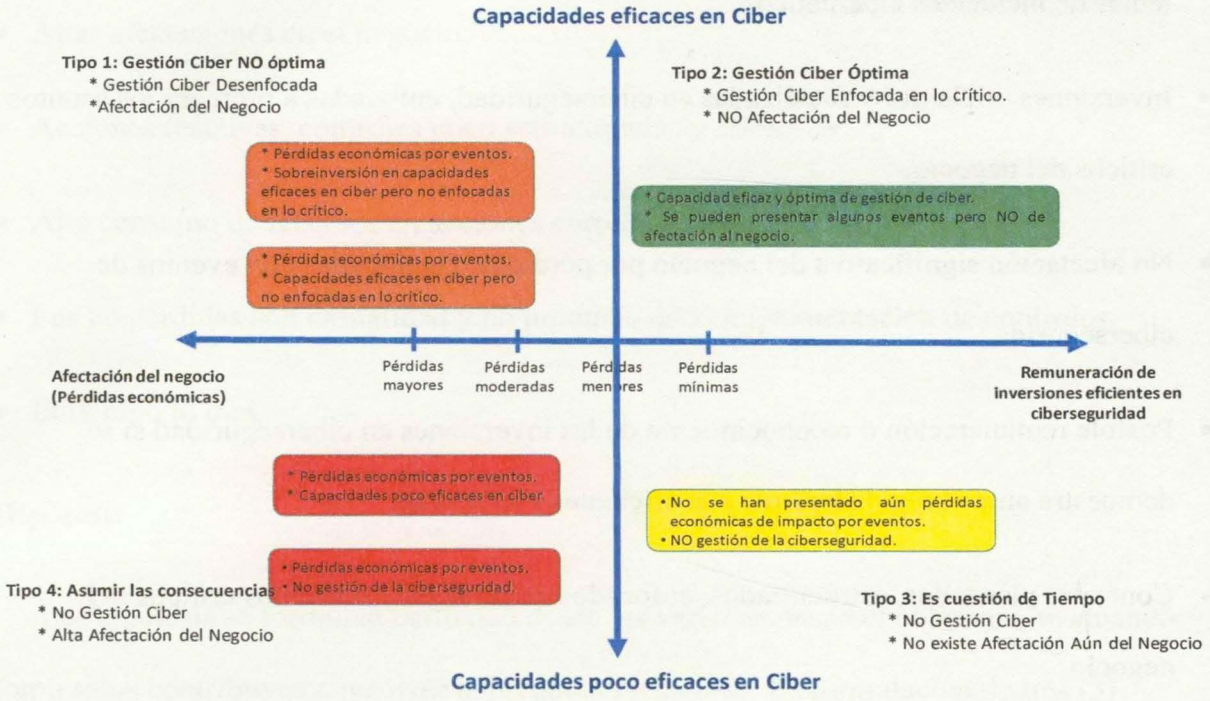
Los escenarios se construyen con la combinación de hipótesis de mayor probabilidad de ocurrencia. Para ello se empleará el método SMIC el cual permite calcular los posibles escenarios con sus respectivas probabilidades de ocurrencia, basado en la combinación entre sí de las hipótesis condicionadas.

Para delimitar el número de escenarios posibles o realizables, como lo plantea (Godet, Monti, Meunier, & Roubelat, 2000) en sus herramientas de Prospectiva, frente a situaciones que se le presenten, el ser humano puede tomar cuatro tipos de actitudes; sufrir el cambio, actuar de manera reactiva frente a una situación, tomar una actitud preactiva o aseguradora en la cual hay una preparación para la situación y la actitud proactiva que consiste en conspirar para que la situación que el hombre desea se materialice. Estos mismos tipos de actitudes que se podrían llamar posturas frente al riesgo, se presentan en las organizaciones desde la propia gestión de los riesgos o probabilidades de presentarse situaciones.

Partiendo de la naturaleza de los objetivos y variables, se encuentra que estos pertenecen a dos tipos de variables, una de desempeño de la organización producto de unas capacidades para gestionar los riesgos cibernéticos y otro del tipo económico, correspondiente a la minimización de las pérdidas económicas producto de los efectos de los incidentes cibernéticos en el negocio distribución.

Frente a la existencia de dos tipos de variables (n=2) se podrían presentar $2^n = 4$ tipos de escenarios, con base en el tipo de gestión que decida la compañía para encarar estos retos:

Gráfica 27. Tipos de escenarios que pueden presentarse de acuerdo a la postura de la organización frente a la gestión de los riesgos.



Escenarios Tipo 1. Gestión de ciberseguridad no óptima

- Se presenta gestión de la ciberseguridad en la compañía, pero esta puede estar sobredimensionada.
- Esta gestión, aunque pueda ser de calidad en los controles, no está focalizada en los asuntos críticos que afectan la continuidad del negocio.
- Se pueden presentar sobreinversiones en ciberseguridad, pero el negocio tiene pérdidas porque éstas no son eficaces.

- El sector público tiene organismos de control que auditan la correcta utilización de los recursos.

Escenarios Tipo 2. Gestión ciberseguridad óptima

- Gestión y capacidades necesarias para lograr minimizar las pérdidas del negocio por temas de incidentes cibernéticos.
- Inversiones eficientes y focalizadas en ciberseguridad, enfocadas a proteger los asuntos críticos del negocio.
- No afectación significativa del negocio por pérdidas relacionadas con eventos de ciberseguridad.
- Posible remuneración o reconocimiento de las inversiones en ciberseguridad si se demuestra ante el regulador, que son eficientes y efectivas.
- Controles planeados, estructurados, enfocados en proteger los asuntos críticos del negocio.

Escenarios Tipo 3. Es cuestión de tiempo

- No hay una gestión de la ciberseguridad.
- Pocas capacidades de ciberseguridad en la compañía.
- No existen afectaciones aún en el negocio, pero existen riesgos no gestionados que desencadenarán en eventos que crearán pérdidas en el negocio.
- Seguridad aparente basada en que en el pasado no ha sucedido nada.

Escenarios Tipo 4. Asumir las consecuencias

- No existe capacidad de gestión de la ciberseguridad.
- Altas pérdidas en el negocio.
- Se destruye valor en el negocio.
- Altas afectaciones en el negocio.
- Acciones reactivas, controles poco estructurados y eficientes.
- Alto consumo de recursos en acciones correctivas.
- Las no pérdidas son casualidad y no producto de la implementación de controles.
- El tiempo lo dirá.

Hipótesis

Las hipótesis se formulan partiendo desde las variables hacia el objetivo y evaluando como estos contribuyen a resolver la pregunta formulada. La formulación de tres (3) hipótesis que serán el punto de partida para la construcción de los diferentes escenarios. La evaluación condicionada de 3 hipótesis (n=3) llevará a una combinación de $2^n = 8$ escenarios posibles. A continuación, se presentan tres (3) hipótesis a evaluar por parte de los expertos:

H1 (Continuidad de TO): La no afectación del SAFETY, la efectividad de las contramedidas, los controles suplementarios, la respuesta oportuna de eventos de ciberseguridad y la gestión de amenazas y vulnerabilidades, permiten implementar y mantener altos niveles de continuidad de las TO.

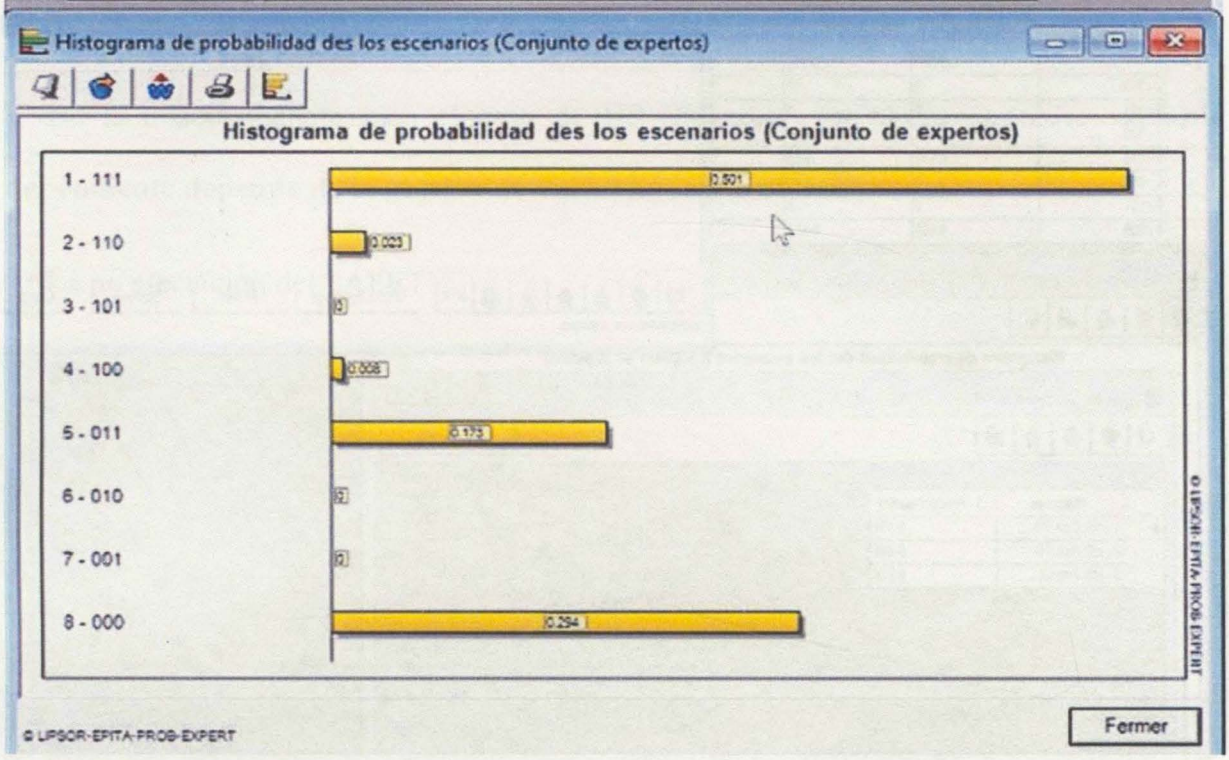
H2 (Recuperación de infraestructura de TO): La no afectación del SAFETY, los altos niveles de resiliencia en sistemas de TO, la respuesta oportuna ante eventos de ciberseguridad y la gestión de amenazas y vulnerabilidades, esquemas seguros y flexibles para la atención no centralizada de las TO, permiten recuperar la infraestructura de TO en el mínimo tiempo bajo escenarios de ciberataques.

H3 (Posesión del Control): Es necesario gestionar las amenazas y vulnerabilidades, realizar una respuesta oportuna ante eventos de ciberseguridad, tener resiliencia en los sistemas de TO, ser efectivos en las contramedidas y no afectar el SAFETY, para mantener la posesión del control.

Para esta evaluación se recurrió a la evaluación de los expertos, teniendo en cuenta la probabilidad de ocurrencia simple de cada hipótesis, la combinación de las diferentes hipótesis, en caso de que cada una se dé o no se dé.

Gráfica 28. Histograma de probabilidades de escenarios.

	Escenarios	1 - Experto Operació	2 - Experto en Ciber	3 - Experto en TO	4 - Ensemble des ex
▶	1 - 111	0.546	0.504	0.489	0.501
	2 - 110	0	0	0.034	0.023
	3 - 101	0	0	0	0
	4 - 100	0.01	0.01	0.007	0.008
	5 - 011	0.189	0.15	0.175	0.173
	6 - 010	0	0	0	0
	7 - 001	0	0	0	0
	8 - 000	0.255	0.336	0.293	0.294

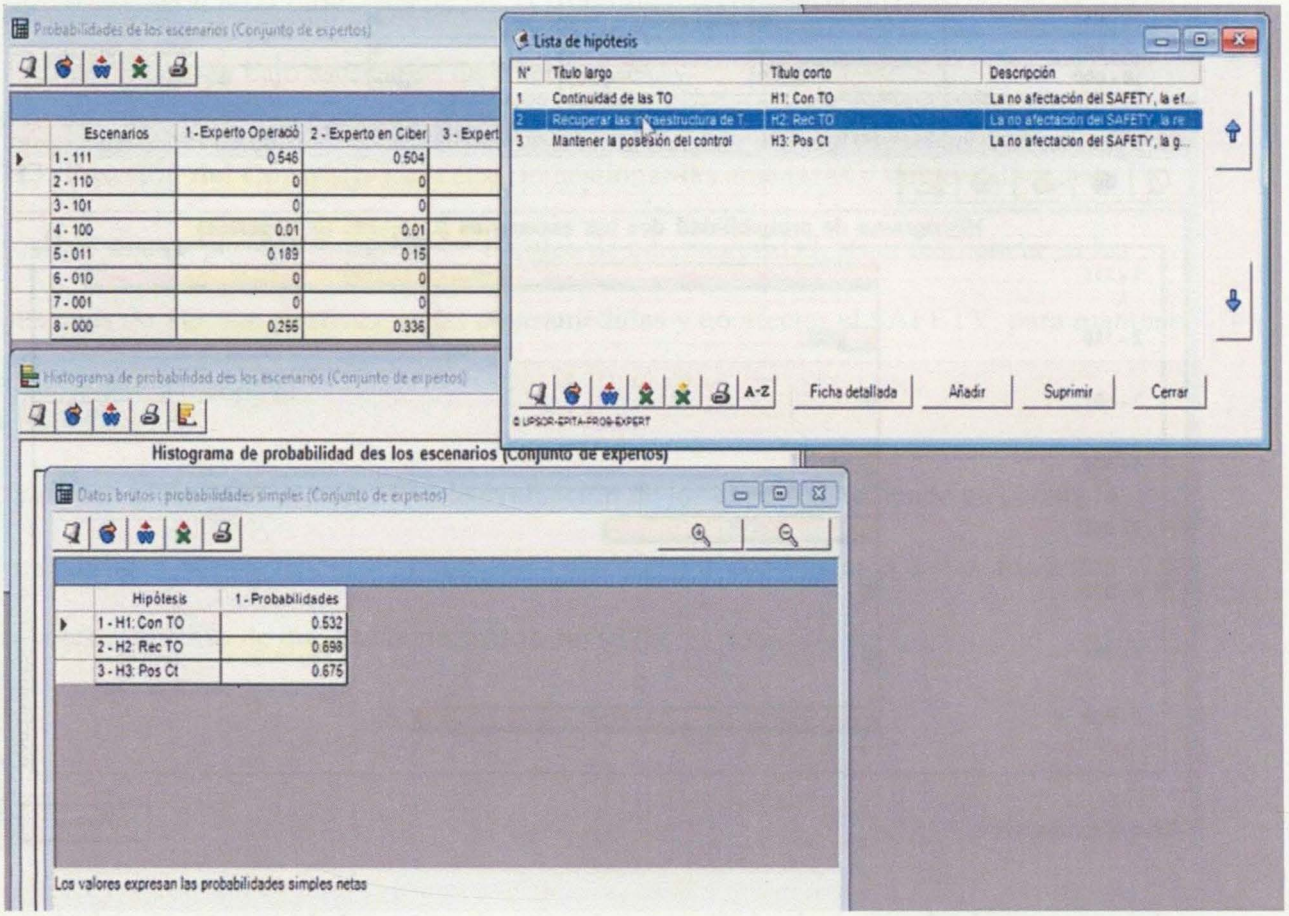


La construcción de escenarios indica que el escenario más probable es el escenario 1 con el 50% de probabilidad, en el que se dan las tres hipótesis. El siguiente escenario con una probabilidad del 29%, es que ninguno de las tres hipótesis se dé y por último, el escenario en el que no se cumpla la primera hipótesis pero se dé la segunda y la tercera es de 17%.

Revisando la asignación de probabilidades simples del conjunto de expertos a cada una de las hipótesis, se encuentra que los conjuntos de expertos aceptan la hipótesis 1 con un 50% de probabilidad, la hipótesis 2 con cerca de un 70% de probabilidad y la hipótesis 3

con un 67%. Estas probabilidades cerca del 70% muestran una aceptación muy fuerte por parte de los expertos, de que se cumplan las hipótesis 2 y 3.

Tabla 19. Histograma de probabilidades de escenarios.



El conjunto de expertos está ratificando que en el caso de **H2 (Recuperación de infraestructura de TO), la variable dependiente que es el tiempo de recuperación de TO, y depende de otras variables independientes,** como:

- La no afectación del SAFETY.
- Los altos niveles de resiliencia en sistemas de TO.
- La respuesta oportuna ante eventos de ciberseguridad.

- La gestión de amenazas y vulnerabilidades,
- Esquemas seguros y flexibles para la atención no centralizada de las TO.
- Es decir, si se gestionan adecuadamente estas variables independientes **se tendrá un resultado positivo sobre la recuperación de la infraestructura de TO bajo escenarios de ciberataque**.

De la misma manera para el caso de **H3 (Posesión del Control), como variable dependiente depende de la gestión de variables independientes como:**

- La no afectación del SAFETY.
- Los altos niveles de resiliencia en sistemas de TO.
- Respuesta oportuna ante eventos de ciberseguridad.
- La gestión de amenazas y vulnerabilidades.
- Efectividad de las contramedidas.

Las variables que son comunes son las de mayor impacto en todas las hipótesis. Debido a que las organizaciones cuentan con recursos económicos, humanos, logísticos limitados, el foco de atención o gestión deberían ser estas variables, dado que son las que gobiernan el modelo.

El caso de las probabilidades simples de **H1**, el nivel de 53% frente a casi 70% de H2 y H3 indica que H1 tiene variables que impactan el modelo, pero es posible que contenga otras variables que no están contenidas en la hipótesis. **H1 (Continuidad de TO)** tiene variables como:

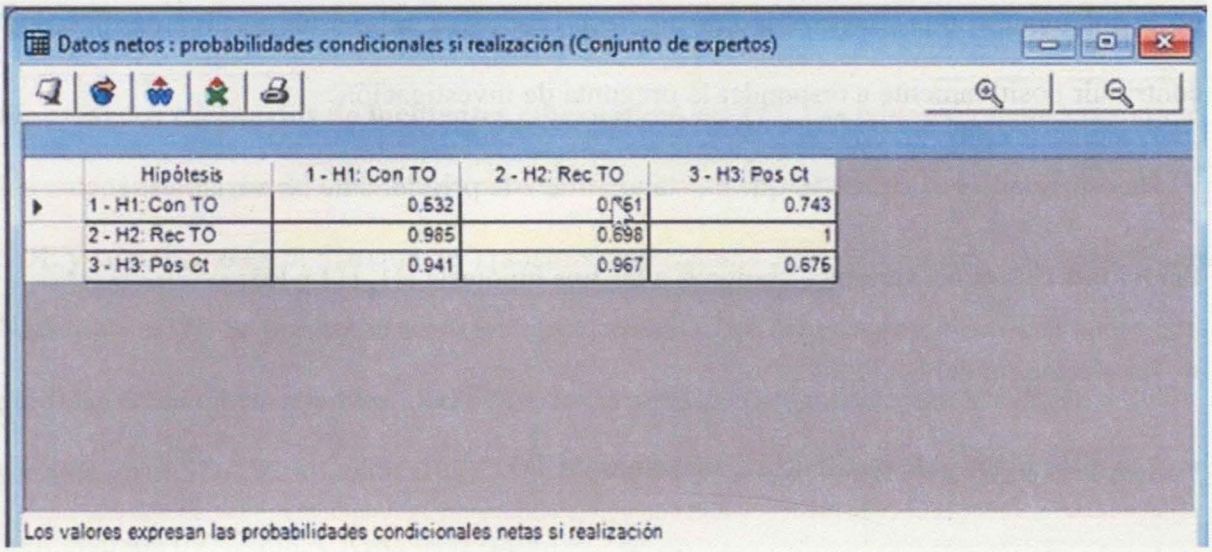
- La no afectación del SAFETY.
- La respuesta oportuna ante eventos de ciberseguridad.
- La gestión de amenazas y vulnerabilidades.
- La efectividad de las contramedidas.
- Los controles suplementarios.

Las variables comunes a las tres hipótesis que son reconocidas por los expertos son:

- La no afectación del SAFETY.
- Los altos niveles de resiliencia en sistemas de TO,
- La respuesta oportuna ante eventos de ciberseguridad.
- La gestión de amenazas y vulnerabilidades.

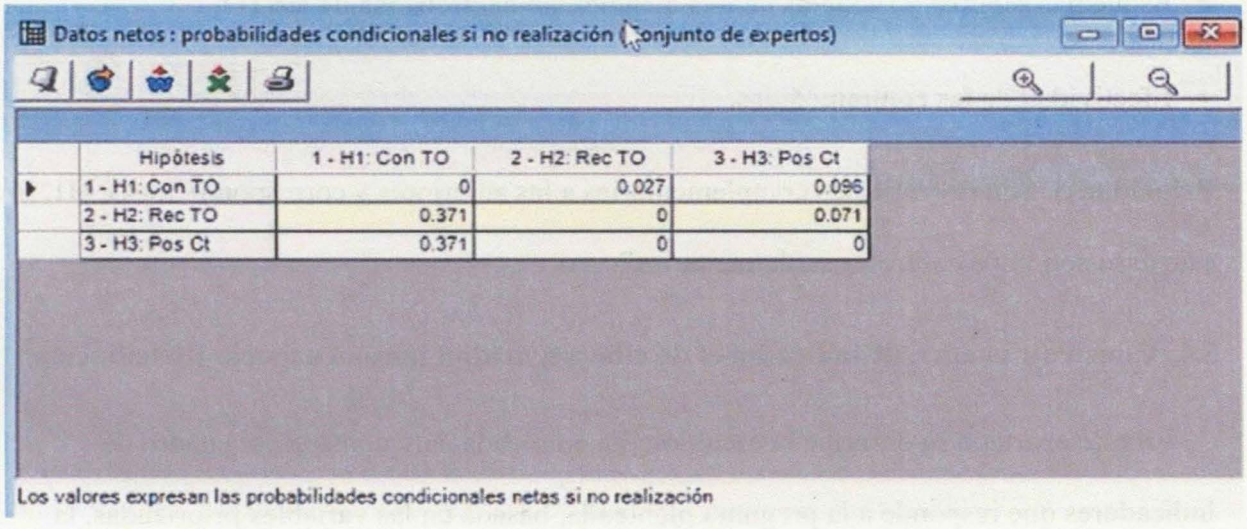
Al revisar las probabilidades condicionales de si realización, se evidencia que la probabilidad de que se dé H1 si se da H2 es del 98.5% y la probabilidad de que se dé H1 si se da H3 es del 94,1%, lo que ratifica que las hipótesis H2 y H3 tienen una mayor probabilidad de ocurrencia y que si se da H2 y H3 es muy probable que se garantice que se dé H1. No así el efecto de H1 sobre H2 y H3, dado que el impacto en este otro sentido no es tan grande o no se ve tan reflejado.

Tabla 20. Probabilidades condicionales de sí realización.



En cuanto a las probabilidades condicionadas de no realización mostrados en el siguiente gráfico, se tiene en cuenta que las probabilidades que se de H1 si no se da H2 o si no se da H3 son muy bajas, lo cual ratifica la alta dependencia de H1 de H2 y H3.

Tabla 21. Probabilidades condicionales de no realización.



Estos análisis ratifican el escenario 1 de mayor nivel probabilidad, el cual plante la ocurrencia de las tres hipótesis. Seguidamente el escenario 8 donde ninguna de las hipótesis

se da, es descartado debido a si bien es posible que se dé matemáticamente, este resultado no es coherente con la construcción de hipótesis, dado que todas están formuladas para contribuir positivamente a responder la pregunta de investigación.

De este análisis se concluye que existe un orden de prioridad de las variables.

Prioridad 1. Son las variables comunes a las tres hipótesis H1, H2 y H3:

- La afectación del SAFETY.
- Los altos niveles de resiliencia en sistemas de TO.
- La respuesta oportuna ante eventos de ciberseguridad.
- La gestión de amenazas y vulnerabilidades.

Prioridad 2. Son las variables complementarias a las anteriores y correspondientes a H2 y H3.

- Esquemas seguros y flexibles para la atención no centralizada de las TO.
- Efectividad de las contramedidas.

Prioridad 3. Son las variables complementarias a las anteriores y correspondientes a H1. En este caso son "Los controles suplementarios".

5.4. Construir cuadro de indicadores de ciberseguridad para el negocio Distribución

En este apartado se describe la metodología empleada para construir el cuadro de indicadores que responde a la pregunta planteada, basada en las variables priorizadas, la información disponible de evaluación de riesgos de la compañía y los criterios de expertos para evaluar la calidad de controles. La información detallada de los riesgos específicos, no

se presenta por temas de confidencialidad de la información, sin embargo, se presenta la metodología, los resultados y la evidencia de los análisis realizados.

- **Plantear los escenarios de incidentes cibernéticos en TO.** Las tablas siguientes resumen los escenarios de riesgo cibernético para el negocio en el Sistema de Distribución Local - SDL y su impacto en el Sistema de Transmisión Regional STR y el Sistema de Transmisión Nacional - STN. Se presentan tanto las afectaciones sobre los sistemas eléctricos como las pérdidas económicas posibles, derivados de las afectaciones al esquema de calidad del servicio en el SDL Resolución CREG 015/2019, las penalizaciones CREG por energía no suministrada 097/2008, CREG 011/2007

Gráfica 29. Escenarios de pérdidas o afectaciones económicas de una empresa de distribución de energía, frente a incidentes cibernéticos altamente especializados y dirigidos.

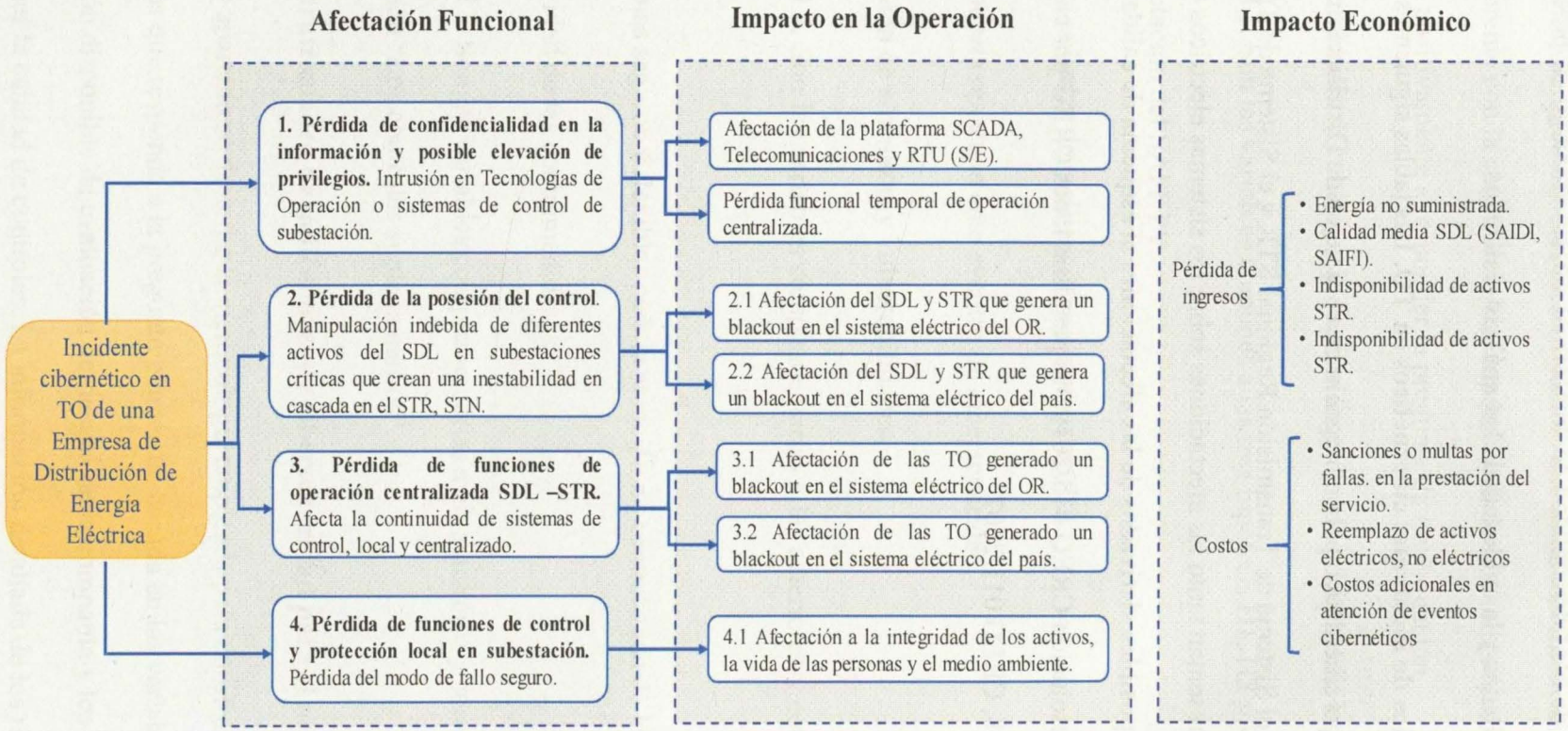


Tabla 22. Escenario de pérdida económica de una empresa de distribución de energía, frente a incidentes cibernéticos altamente especializados y coordinados. Cifras en millones de pesos de febrero de 2020.

Descripción del escenario de pérdida	Activos eléctricos afectados	Calidad media	Pérdidas por energía no suministrada	Indisponibilidad de activos STR-STR	Multas por fallas en la prestación del servicio	Otros costos derivados del incidente cibernético	Total
1. Intrusión en centro de control y sistemas de control	Ninguno	-	-	-	-	- 150	- 150
2.1. Pérdida de la posesión del control que genera un blackout en el SDL.	Sistema de Distribución Local SDL, STR, STN.	- 47.020	- 13.368	- 375	- 4.141	-	- 64.903
2.2. Pérdida de la posesión del control que genera un blackout que se escala desde el SDL al Sistema Interconectado Nacional.	Sistema Interconectado Nacional	- 47.020	- 89.120	- 375	- 8.281	-	- 144.796
3.1. Pérdida de las funciones de operación centralizada SDL –STR	Sistema de Distribución Local SDL, STR, STN	- 47.020	- 13.368	- 625	- 8.281	-	- 69.294
	Sistema Interconectado Nacional	- 47.020	- 89.120	- 917	- 9.937	-	- 146.994
3.2 Afectación del funcionamiento de subestaciones S/E	Sistema de Distribución Local SDL, STR, STN	- 47.020	- 13.368	- 625	- 8.281	-	- 69.294
	Sistema Interconectado Nacional	- 47.020	- 89.120	- 1.250	- 9.937	-	- 147.327
4. Afectación a la integridad física de dos o mas subestaciones S/E	Sistema de Distribución Local SDL, STR, STN	- 47.020	- 13.368	- 625	- 8.281	- 6.800	- 76.094
	Sistema Interconectado Nacional	- 47.020	- 89.120	- 1.250	- 9.937	- 6.800	- 154.127

Los escenarios de pérdidas contemplan las fallas en la prestación del servicio basados en un rango de horas duración del evento cibernético y horas de afectación del servicio para el sistema eléctrico que opera la empresa y el país, con base en las capacidades en ciberseguridad de la empresa en estudio.

Estos escenarios de pérdidas contribuyen a resolver la pregunta de cuáles son las variables a gestionar para que las pérdidas económicas del negocio bajo eventos de ciberseguridad sean las mínimas. Nótese como los escenarios por encima del primero, es decir E2, E3 y E4 conllevan a altas pérdidas económicas, lo cual indica que el escenario al que se debe apuntar es a mantener el riesgo que conlleve máximo al E1, de manera controlada y evitando que se materialicen los escenarios de pérdidas por encima de esto dado que son de alto impacto. Estos escenarios permitieron encontrar los riesgos y las componentes de estos que deben gestionarse, para restringir la ocurrencia de eventos que lleven a estos escenarios.

- **Identificar las variables priorizadas en el numeral 5.3.3.4, involucradas en los escenarios de riesgo planteados.**

A partir de las siete variables clave encontradas y priorizadas en el numeral 5.3.3.4 empleando la metodología de planeación por escenarios, se procedió a identificar y filtrar cuáles de los riesgos cibernéticos del mapa de riesgos de la organización en estudio, tenían relación con estas variables clave.

A continuación, se muestran las variables priorizadas que tienen relación con los escenarios de pérdida. Como se evidencia todas las variables priorizadas tienen relación

con el evento a partir del nivel 2 que es donde se presentan las pérdidas y es aquí donde se ve el valor del ejercicio de escenarios para priorizar las 35 variables inicialmente identificadas para llegar a estas 7. Para poder tener gestionar las casusas efectos y los controles preventivos y correctivos de mayor correlación para controlar el nivel de riesgo.

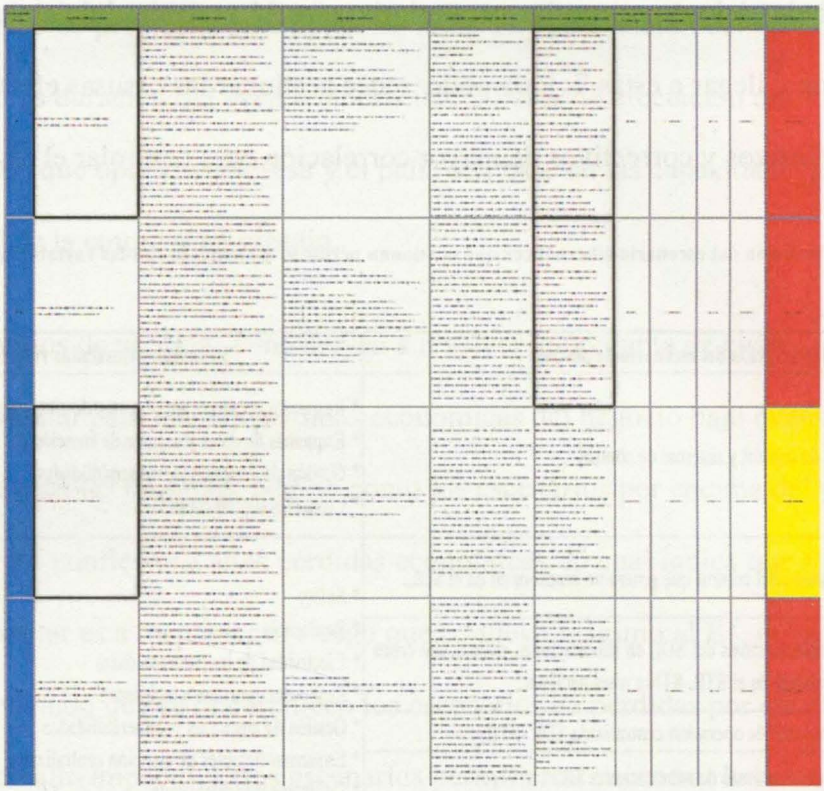
Tabla 23. Relación del escenario cibernéticos que ocasionan pérdidas económicas con las variables priorizadas.

Descripción del escenario de pérdida	Variables priorizadas relacionadas
1. Intrusión en centro de control y sistemas de control	* Respuesta oportuna ante eventos de ciberseguridad. * Esquemas flexibles y seguros de atención de TO. * Gestión de Amenazas y vulnerabilidades. * Controles suplementarios.
2.1. Pérdida de la posesión del control que genera un blackout en en el SDL.	* Safety * Resiliencia * Efectividad de las contramedidas * Respuesta oportuna a incidentes * Gestión de amenazas y vulnerabilidades * Esquemas flexibles de atención centralizada * Controles suplementarios.
2.2. . Pérdida de diferentes activos del SDL en subestaciones críticas que crean una inestabilidad en cascada en el STR, STN a nivel nacional.	
3.1. Pérdida de las funciones de operación centralizada SDL -STR	
3.2. Afectación del funcionamiento de subestaciones S/E	
4. Afectación a la integridad física de dos o mas subestaciones S/E	

- **Filtrar los riesgos relacionados con las variables priorizadas, con base en los escenarios de riesgo del mapa de riesgos cibernéticos en tecnologías de operación de la empresa distribuidora en estudio.**

Al filtrar los riesgos consolidados de la cadena de control, con base en las variables priorizadas, se están conectando las causas y el efecto de los mismos con el riesgo los escenarios de pérdida solamente evaluando la variable financiera focalizando el análisis en los riesgos que generan dichos escenarios. Por temas de confidencialidad de información no se presentan detalles de los riesgos evaluados.

Tabla 24. Identificación de los riesgos con las variables priorizadas.



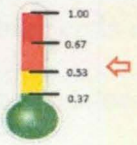
De los 54 riesgos encontrados en la cadena de control estudiada, correspondiente a los subestaciones, telecomunicaciones y centros de control, se filtraron 18 los cuales corresponden a los riesgos que se encuentran comunes a los tres sistemas, empleando un índice de correlación. El cálculo de probabilidad y consecuencia de los riesgos para la cadena de control, también se consolidó asignando la valoración de probabilidad y consecuencia más alta encontrada en los elementos de la cadena de control estudiada.

- **Calcular el índice de riesgo actual para la cadena de control.** subestación, telecomunicaciones y centro de control, con base en los riesgos filtrados que afectan las variables priorizadas y la asignación a la cadena de control estudiada, de la calificación más alta de probabilidad y consecuencia encontrada para subestación, telecomunicaciones y centro de control.

Una vez filtrados los riesgos y consolidando la valoración de los relacionados con la cadena de control, se llega a un valor de riesgo de 0,704 catalogado como extremo con un nivel de controles de 2.1 muy bajo, lo cual indica la probabilidad de ocurrencia de un evento del tipo E2, E3 o E4 con sus variantes. A continuación, se muestra a matriz de probabilidad versus consecuencia para la situación actual de los 18 riesgos.

Gráfica 30. Matriz de probabilidad versus consecuencia para la situación actual de los 18 riesgos.

		CONSECUENCIA				
PROBABILIDAD		Mínima	Menor	Moderada	Mayor	Máxima
		1	2	4	8	16
Muy alta	5					
Alta	4			R5,R9	R2,R4,R6,R8,R11,R14,R15,R16,R18	R1
Media	3			R3,R7	R10,R12,R13,R17	
Baja	2					
Muy baja	1					



Índice de Riesgo

0.704 Extremo

Cantidad de riesgos	
Extremo	10
Alto	6
Tolerable	2
Aceptable	0
Total riesgos	18

- **Asignar una calificación de probabilidad y consecuencia que debería tener cada uno de los riesgos consolidados de la cadena de control** para que el riesgo de la cadena sea tolerable. Esta calificación se realiza con base en criterios de experto sobre la viabilidad y eficacia de los controles propuestos para cada riesgo, de manera que se valide que efectivamente si se puede llegar a estos valores. De lo contrario se le asigna la valoración cualitativa de probabilidad y consecuencia que es posible alcanzar con ese control.

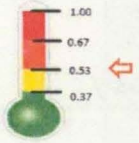
Tabla 25. Identificación de los riesgos con las variables priorizadas.

Código del riesgo	Nivel de Riesgo Actual	Nivel de Riesgo Objetivo
R1	Extremo	Tolerable
R2	Extremo	Aceptable
R3	Tolerable	Tolerable
R4	Extremo	Tolerable
R5	Alto	Tolerable
R6	Extremo	Aceptable
R7	Tolerable	Tolerable
R8	Extremo	Aceptable
R9	Alto	Tolerable
R10	Alto	Aceptable
R11	Extremo	Aceptable
R12	Alto	Tolerable
R13	Alto	Tolerable
R14	Extremo	Aceptable
R15	Extremo	Aceptable
R16	Extremo	Aceptable
R17	Alto	Tolerable
R18	Extremo	Tolerable

La tabla muestra la propuesta de nivel de riesgo objetivo de cada uno de los riesgos individuales, con el fin de llevarlo a un nivel de consecuencia tolerable o menor, para no estar en un escenario más severo o superior que E1, es decir E2, E3, o E4. La siguiente tabla muestra la matriz de riesgos y consecuencias para la situación deseada de riesgos.

Gráfica 31. Matriz de probabilidad versus consecuencia para la situación futura deseada de los 18 riesgos.

PROBABILIDAD		CONSECUENCIA				
		Mínima	Menor	Moderada	Mayor	Máxima
		1	2	4	8	16
Muy alta	5					
Alta	4					
Media	3			R1,R4,R7,R9,R12		
Baja	2		R2,R6,R10	R3,R5,R13,R17,R18		
Muy baja	1	R8		R15		



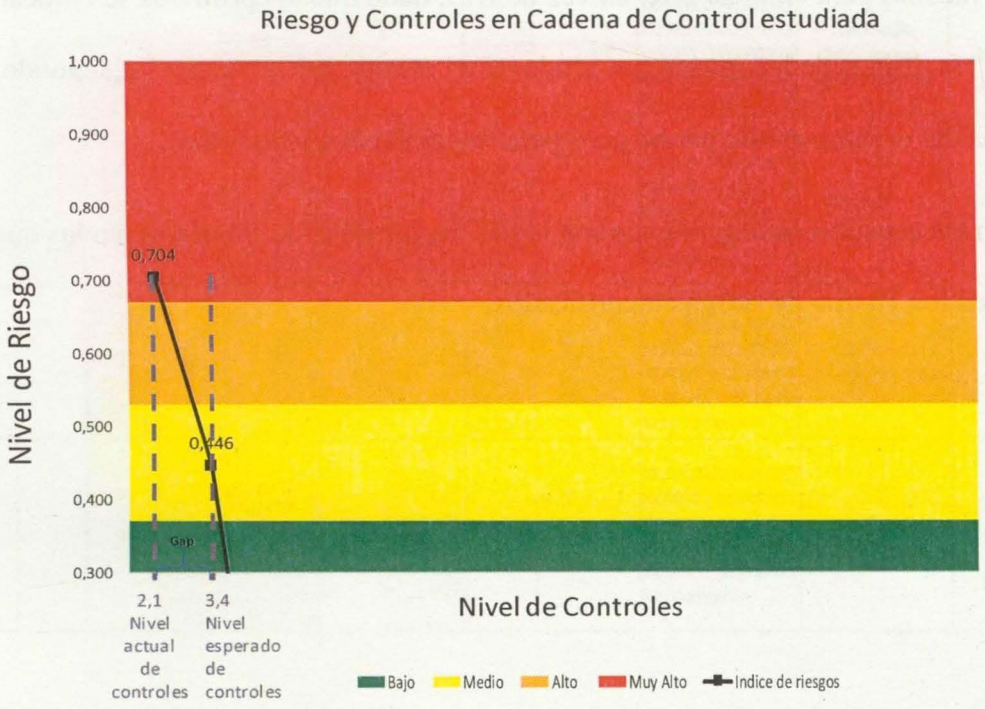
Índice de Riesgo

0,446
Tolerable

Cantidad de riesgos	
Extremo	0
Alto	0
Tolerable	10
Aceptable	8
Total riesgos	18

Con base en la nueva valoración de los riesgos individuales se calcula en nuevo valor de riesgos de la cadena de control, validando que el nivel de riesgos de es tolerable.

Gráfica 32. Nivel de riesgo actual y deseable basado en la implementación de controles



Para lograr el nivel de riesgo objetivo como "tolerable" para la cadena de control en estudio, es necesario implementar un gap de controles de nivel 2,1 a 3,4 de manera que los riesgos no materialicen los escenarios de pérdidas N2.1., N2.2, N3.1, N3.2 y N4.1 y N4.2.

- **Construir los indicadores clave de riesgo – KRI, con base en las causas de los riesgos identificados**

Existen diferentes momentos en los cuales realizar gestión sobre un evento, antes de que suceda, durante el desarrollo del evento y posterior al evento.

Como se presentó en la gráfica 8, las consecuencias del evento traen grandes costos y demanda de recursos de la organización para llevar la condición operativa durante y después del evento a rangos normales. Es por ello que la gestión de los riesgos se enfoca en prevenir la ocurrencia de los eventos a partir de las causas, porque esta técnica permite a las organizaciones planear los controles y hacer una racionalización en los recursos. Esta es una de las razones para emplear KRI en vez de KPI, dado que los primeros se enfocan en la gestión de los riesgos de las causas que producen el evento, mientras que los segundo es una medida del desempeño de lo que pasó para tomar decisiones a futuro.

Se ordenan las causas más importantes son las de mayor nivel de correlación o las que más se repiten en los 18 tipo de riesgos identificados.

Tabla 26. Relación entre causas de los riesgos y las variables priorizadas.

Código de Causa	1. Afectación del Safety	2. Efectividad de las contramedidas	3. Altos niveles de Resiliencia en los sistemas de TO	4. Respuesta oportuna ante eventos de ciberseguridad	5. Gestión de amenazas y vulnerabilidades	6. Esquemas flexibles y seguros para la atención no centralizada de eventos sobre las platformas de TO	7. Controles Suplementarios	Pregunta Inspección	Nombre de la Causas	Activos Vinculados	Cantidad de Riesgos Vinculados	% Correlación Riesgos
44	X	X	X		X	X	X	3, 5, 6, 8, 11, 14	XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXX.	CdeCEnergía, Subestaciones, Telecomunicaciones	47	87,0
1	X	X	X	X	X	X	X	4, 5, 12, 13	XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXX.	CdeCEnergía, Subestaciones, Telecomunicaciones	44	81,5
45	X	X	X			X	X	1, 2, 3, 5, 11, 14	XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXX.	CdeCEnergía, Subestaciones, Telecomunicaciones	42	77,8
28	X	X		X	X		X	1, 2, 8, 9	XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX	CdeCEnergía, Subestaciones, Telecomunicaciones	31	57,4
17	X			X	X	X	X	8	XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXX.	Subestaciones	3	5,6
30		X	X	X	X	X	X	3, 14	XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXX.	CdeCEnergía, Telecomunicaciones	3	5,6
40		X	X	X	X	X	X		XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXXXX XXXXXXXXXXXX.	CdeCEnergía, Subestaciones	2	3,7

- **Indicadores propuestos desde la operación y el proceso**

Tabla 27. Relación entre causas de los riesgos y las variables priorizadas.

Causa del riesgo	Objetivo/Indicador	KRI	Meta
XXXXXXX,XXXXXXXXXXX XXXXXXXXXXX.	OBJ: Reducir el comportamiento y usos no aceptables de activos y ciberactivos de TO.	**KRI 1 = # Usos inadecuados/ # Total de Acceso a ciberactivos propios y de terceros que se conectan a las redes.**	1. Medir el 100% del acceso a los ciberactivos. 2. Alcanzar una tasa menor al 5% de comportamientos anómalos, con respecto a política de uso de activos y ciberactivos.
XXXXXXX,XXXXXXXXXXX XXXXXXXXXXX.	OBJ: Incrementar las competencias de ciberseguridad básicas del personal de TO de acuerdo al perfil referencia definido.	**KRI 2: # de personas que no cumplen el perfil de competencias /# Total de funcionarios de TO.**	1. Alcanzar una nivel menor al 10% de personas con falta de al menos una competencia básicas en ciberseguridad en personal de TO. Menor al 5% de los funcionarios.
XXXXXXX,XXXXXXXXXXX XXXXXXXXXXX.	OBJ: Lograr una efectividad del 100% en la asignación correcta de privilegios.	**KRI 3 = #Permisos incorrectamente asignados / #Total de perfiles asignados.**	Alcanzar una cifra menor al 3% de los privilegios incorrectamente asignados reduciendo el 1% anual hasta llegar al 0% de errores en el proceso.
XXXXXXX,XXXXXXXXXXX XXXXXXXXXXX.	OBJ: Alcanzar el 100% de la efectividad o calidad del control o contramedidas.	**KRI 4 = # Contramedidas ineficaces/# controles totales**	Alcanzar una tasa del 90% de efectividad de las contramedidas en funcionamiento físico y lógico.
XXXXXXX,XXXXXXXXXXX XXXXXXXXXXX.	OBJ: Atender el 100% de las vulnerabilidades en TO cumpliendo los ANS establecidos.	**KRI 5 = # Vulnerabilidades no atendidas o que no cumplen ANS / # Vulnerabilidades encontradas, reportadas, publicadas.**	Cumplimiento de los ANS de atención de vulnerabilidades reportadas, identificadas y publicadas.
XXXXXXX,XXXXXXXXXXX XXXXXXXXXXX.	OBJ: Medir la efectividad del control perimetral (IDS, FW o IPS) sobre TO.	**KRI 6 = # Eventos de falsos positivos (incidentes) de intrusión en la red/ # Incidentes registrados.**	Alcanzar la mayor probabilidad de bloqueo (100%) de intrusiones de la red.
XXXXXXX,XXXXXXXXXXX XXXXXXXXXXX.	OBJ: Lograr un 100% de personal de TO con alta concientización y conocimiento de prácticas de ingeniería social.	**KRI 7 = # de incidentes positivos de ingeniería social en TO y Operación/ # funcionarios de TO y operación objeto de ejercicios de ingeniería social.**	Alcanzar la tasa menor a 1 % de incidentes de ingeniería social en la operación y el soporte a TO.

- **Indicadores propuestos para el safety**

En el ejercicio de escenarios, la variable **SAFETY** resultó como la más importante que arrojó el análisis construido por los expertos. Esto es un llamado de los expertos a concentrar la atención en el aseguramiento del proceso, lo cual implica un enfoque basado en la garantía funcional como una estrategia complementaria a la utilización de la técnica de seguridad basada en defensa en profundidad.

A continuación, se presentan los asuntos funcionales esenciales, en los cuales se basa en la operación segura de los activos eléctricos y lo cual se debe resguardar bajo el concepto de aseguramiento o safety, y no se debe afectar en condiciones de incidentes cibernéticos.

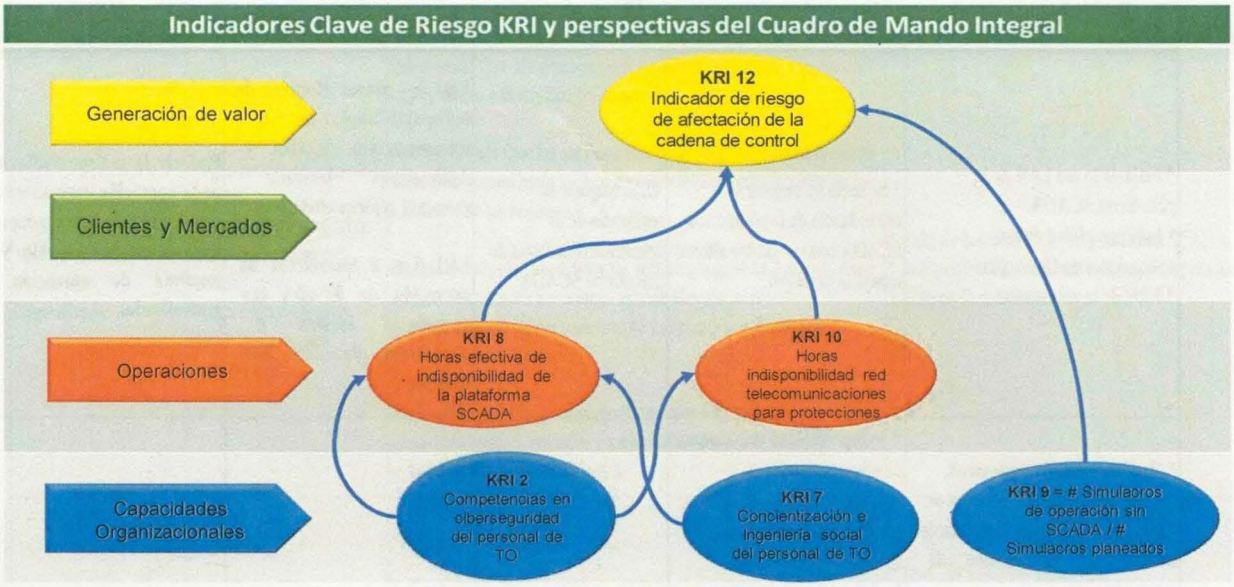
Tabla 28. Asuntos funcionales del Safety necesarios para la operación.

Ciberativos	Funcionalidad	Aseguramiento Funcional	Falla funcional
SCADA y Aplicaciones de Operación Centralizada	* Adquisición de Datos del proceso. * Supervisión y control de variables eléctricas del sistema. * Operación de activos eléctricos de manera centralizada.	**Integridad:** Que los datos del proceso que se transmiten y procesan corresponden a la realidad del mismo. **Confiabilidad:** Que las acciones operativas realizadas desde el centro de control lleguen hasta las borneras de salida del concentrador de las estaciones de los negocios. **Oportunidad:** Que los datos y las acciones operativas desde el centro de control se den en los tiempos establecidos por el proceso y acordados con el cliente para realizar la operación centralizada adecuadamente. **Disponibilidad:** que las funciones de supervisión, control y medición los sistemas estén habilitados para ser utilizados por el cliente y cumplan con los niveles pactados.	* Falla de la red LAN de la plataforma SCADA. * Indisponiblidad de las aplicaciones de Operación. * Falla de la aplicación.
Red de Transporte Telecomunicaciones	* Transporte señales SCADA Central. * Funcionamiento Teleprotecciones. * Voz Operativa. * Video vigilancia.	* **Confiabilidad:** No pérdida de paquetes, entre componentes de Teleprotección, para funciones SCADA Centrizado y voz operativa. 10-4 <= **BER<= 10-6** * **Disponibilidad:** Disponibilidad del sistema de telecomunicaciones superior a 99.95%, para teleprotecciones, SCADA y voz operativa. * **Redundancia:** Contar con la disponibilidad de otro sistema de telecomunicaciones alterno que cumpla los requerimientos de teleprotecciones, SCADA y voz operativa estos dos últimos en activos críticos. * **Desempeño:** No retardos superiores a 5 ms para transporte de datos entre componentes de teleprotección.	* **Red con retardos excesivos.** * **No confiabilidad Teleprot:** Comando ausente o con retardo excesivo en el extremo de recepción. * **Indisponibilidad Teleprot:** Tiempo en el que la línea no cuente con un sistema de protección activo. * **No Redundancia Teleprot:** Tiempo en el que el esquema de protección no cuenta con elementos duplicados para el funcionamiento incluidos los elementos de telecomunicaciones. * **No disponiblidad de funciones SCADA** Centralizado.
RTU / Concentrador + IHM	* SCADA Local, Sincronismo, bases de Datos, alarmas.	* **Integridad** de variables del proceso (alarmas, indicadores, variables) hacia el SCADA. * **Disponibilidad** de variables del proceso.	* No envío de variables del proceso. * Falta de integridad de variables del proceso. * No reponder ante comandos desde el Centro de Control.
Red LAN Subestación	* Conectividad componentes de Subestación.	* **Disponibilidad de la LAN:** Disponibilidad de los servicios de conectividad en el proceso. * **Acceso lógico:** control perimetral - Firewall local. * **Conectividad:** Infraestructura física cableado. * **Confiabilidad:** Sistema de Redundancia. * **Sincronización de tiempo:** sincronismo de tiempo para análisis de eventos eléctricos.	* Fallas en el control de acceso lógico. * Fallas de funcionamiento. * Pérdida de sincronismo.
Control y Protecciones	* Protección local -Modo de fallo seguro * Protecciones línea.	* **Confiabilidad:** Que los sistemas operen adecuadamente, aun cuando su tiempo entre operaciones sea muy alto. * **Disponiblidad:** Que los sistemas operen cuando se requiere. * **Selectividad y Desempeño:** Que los sistemas operen con la acciones y dentro de los parámetros esperados, basados en la correcta parametrización variables eléctricas.	* Funcionamiento inadecuado de los sistemas de control y protección.

Tabla 29. Indicadores Clave de Riesgo KRI del proceso basado en Safety fallas funcionales producto de un ciberataque.

Posible Falla funcional	Causa del posible riesgo	Objetivo/Indicador	KRI	Meta
* Falla de la red LAN de la plataforma SCADA. * Indisponiblidad de las aplicaciones de Operación. * Falla de la aplicación.	* Se requiere mejorar la redundancia de la plataforma SCADA con un centro alterno espejo al principal.	OBJ: Mejorar la resiliencia de la operación ante fallas de plataforma SCADA	**KRI 8 = Horas efectivas de indisponibilidad de la infraestructura SCADA y Aplicaciones teniendo encuenta centros alternos.** **KRI 9 = # Simulacros de operación sin SCADA con operadores locales/ # Simulacros planeados por trimestre.**	**Reducir la indisponibilidad de la operación centralizada a 1 hora, basado en centro de control de respaldo y esquema de operación centralizado.**
*** Red con retardos excesivos.** *** No confiabilidad Teleprot:** Comando ausente o con retardo excesivo en el extremo de recepción. *** Indisponibilidad Teleprot:** Tiempo en el que la línea no cuente con un sistema de protección activo. *** No Redundancia Teleprot:** Tiempo en el que el esquema de protección no cuenta con elementos duplicados para el funcionamiento incluidos los elementos de telecomunicaciones. *** No disponiblidad de funciones SCADA** Centralizado.	* Indisponiblidad del sistema de telcomunicaciones. * Errores en la transmisión, afecta telerotecciones, SCADA, voz operativa. * Retardos excesivos para servicios críticos, SCADA, Teleprotecciones. * Ausencia o falla en la redundancia de la red de telecomunicaciones que soporta funciones críticas como SCADA y teleprotecciones. * Falta de proceso que asegure la gestión del desempeño de la red IP, para buen funcionamiento de teleprotecciones.	OBJ: Garantizar las condiciones de alta disponibildiad y latencia de la red de Telecomunicaciones para las funciones SCADA y Teleprotecciones, voz operativa.	**KRI 10 = # horas de indisponibilidad de la red o con configuraciones de retardos excesivos o sin redundancia para los servicios de teleprotección/ 8760**	**Mantener la disponibilidad de los enlaces de teleprotecciones en 100% de disponibilidad y con las condiciones requeridas por los equipos de protección.**
* Funcionamiento inadecuado de los sistemas de control y protección.	* Obsolescencia tecnológica. *** Alteración de parámetros de estudios de protecciones en los sistemas de protección.** * Fallas en la red LAN. * Fallas en la red de Transporte. * Fallas en los equipos de protección.	OBJ: Monitorear y controlar la idoneidad de la parametrización eléctrica de los sistemas de protección.	**KRI 11 = # cambios de parámetros NO coincidentes con los parámetros de estudios de protección.**	**Garantizar la idoneidad de la parametrización de los equipos de protección del proceso.**
* Afectación de la cadena de control que soporta la operación centralizada del negocio.	18 Riesgos encontrados en la cadena de control.	OBJ: Orientar las inversiones y costos en ciberseguridad a proteger la cadena de control que soporta la operación centralizada	**KRI 12 = # Indice de Riesgo de la cadena de control, Centro de control, subestación, y Automatización**	**Mantener el indice de riesgo en niveles de riesgo tolerable**

Gráfica 33. Indicadores Clave de Riesgo KRI del proceso basado en Safety.



La gráfica muestra los principales indicadores clave de riesgo – KRI que deben ser gerenciados dentro de un Cuadro de Mando Integral – CMI por sus siglas en inglés, el cual se lee de abajo hacia arriba.

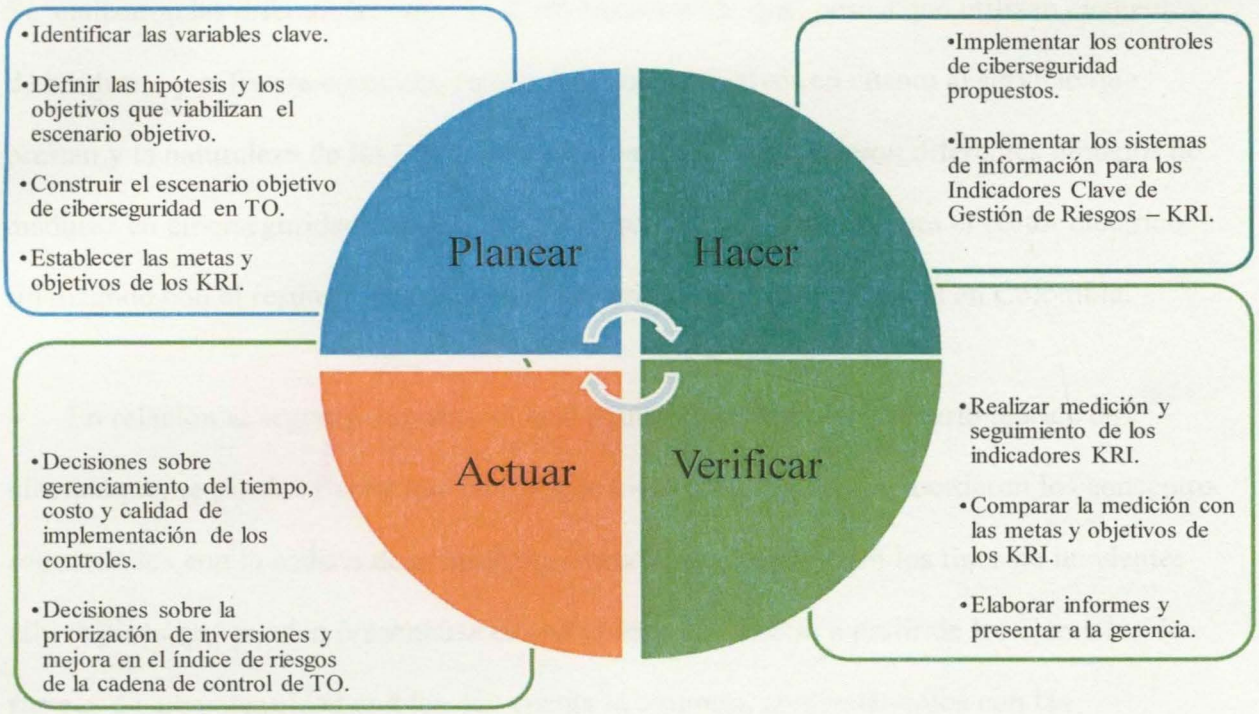
Desde la perspectiva "Capacidades Organizacionales", se establecieron tres (3) indicadores KRI 2, KRI 7 y KRI 9. El Desarrollo de las Competencias en Ciberseguridad del Personal de TO – KR2 y la Concientización e Ingeniería Social del Personal de TO - KR7, contribuye a mejorar el desempeño y la Disponibilidad de la Plataforma SCADA - KRI 8 y la Disponibilidad de las Telecomunicaciones para las teleprotecciones – KRI 10 las cuales pertenecen a la perspectiva "Operaciones" a partir de un enfoque de garantía funcional del safety. Esto a su vez permite mejorar la resiliencia en sinergia con el esquema de operación local. Estas mejoras en los dos últimos indicadores contribuyen a disminuir el Índice de Riesgo de Afectación a la Cadena de Control KRI 12, el cual está ubicado en la perspectiva "Generación de Valor". De este modo se minimizan los riesgos y las pérdidas en la

operación derivados de incidentes cibernéticos, desde una perspectiva gerencia, táctica y operacional.

- **Enfoque en mejora continua**

El cuadro de Indicadores Clave de Riesgo KRIs permite tener un enfoque en los asuntos clave del negocio. Dicho cuadro de indicadores es el producto de un proceso el cual es necesario insertarlo dentro de la organización mediante un enfoque de mejora continua el cual se presenta en la gráfica 34.

Gráfica 34. Ciclo de mejora continua con base en los KRI definidos



A partir de la implementación de este ciclo, la gerencia del negocio podrá en la etapa PLANEAR establecer los objetivos de la ciberseguridad en TO que gestionan los riesgos cibernéticos de los asuntos críticos del negocio. Mediante el HACER la organización debe implementar los procesos y los sistemas de información que le permitirán poner en

funcionamiento los controles y la forma de calcular los indicadores KRI. En la etapa VERIFICAR el proceso deberá realizar la medición y seguimiento a los indicadores, calculando las brechas de mejora, entre los resultados de la efectividad de los controles frente a las metas inicialmente establecidas. Finalmente, en la etapa AJUSTAR la gerencia del negocio deberá tomar las decisiones en la gestión, efectividad que le permitan un impacto sobre el indicador de riesgos de la cadena de TO, objeto de estudio de este trabajo.

6. Conclusiones

- En general se cumplieron todos los objetivos planteados en el presente trabajo. En relación con el primer objetivo trazado, en el numeral 5.1 se analizaron los estándares y lineamientos desarrollados para los sistemas de control industrial en el sector de energía eléctrica, los cuales se resumieron en las tablas 3 y 4 con base en normas, documentos técnicos construidos por organismos normalizadores del sector eléctrico como IEC, ANSI y otras entidades como IEEE, NIST este último para infraestructuras críticas norteamericanas y otros sectores de control industrial como ISA.

Se analizaron las diferencias entre TI y TO encontrando que, pese a que utilizan elementos de hardware y software comunes, tienen diferentes objetivos en cuanto al servicio que prestan y la naturaleza de las funciones que soportan. Se resumieron diferentes modelos de madurez en ciberseguridad incluido el C2M2 que fue desarrollado para el sector eléctrico, finalizando con el resumen de las principales normas de ciberseguridad en Colombia.

- En relación al segundo objetivo el cual planteó construir un escenario teórico de ciberataque, se puede afirmar que también se logró toda vez que se abordaron los conceptos relacionados con la cadena de control bajo estudio, se describieron los tipos de incidentes cibernéticos que pueden presentarse en esa cadena de control, a partir de los ejercicios de riesgos de ciberseguridad con los que cuenta la empresa, contrastándolos con las vulnerabilidades encontradas en el análisis de caso del blackout de Ucrania en el 2015 y encontrando que comparten vulnerabilidades comunes que fueron explotadas en este incidente.

Posteriormente se calcularon las pérdidas económicas que generaría un ciberataque que ocasione un blackout o apagón generalizado. Posteriormente se realizó un ejercicio de planeación por escenarios cuya pregunta problematizadora estaba relacionada con las variables clave de ciberseguridad que debería gestionar una empresa de distribución, para que las pérdidas económicas sean las menores posibles. Este ejercicio se basó en criterio de expertos, buscando construir el escenario en el que debería moverse la organización en estudio, realizando un enfoque diferente al tradicional de defensa en profundidad y focalizando el análisis en lo que se ha llamado aseguramiento funcional, encontrado en la literatura como un enfoque complementario.

- Con base en la técnica planeación por escenarios se definieron 35 variables que fueron estudiadas por diez expertos en ciberseguridad, centros de control, SCADA, telecomunicaciones y automatizaciones. Se llegó a la priorización de 7variables clave a gestionar, con base en la cuales se filtraron los riesgos que tenían relación con estas variables y podrían generar el blackout. A partir de este filtro de 18 riesgos, se calculó el indicador de riesgo de la cadena de control de encontrando un valor de 0,704, se evaluaron los controles que podrían disminuir cada riesgo desde una consecuencia alta o extrema hacia valores considerados como tolerables, encontrando un gap de controles a implementar y una disminución del riesgo total, con lo cual se considera alcanzado el tercer objetivo planteado.

- En cuanto al último objetivo se construyó un cuadro de indicadores KRI de 12 indicadores del tipo gerencial, táctico y operacional, describiendo cada indicador, la forma de calcularlo, y el objetivo que debe perseguir, basado en la causa que generó el riesgo que

se quiere abordar o gestionar. Finalmente se propone el cuadro de indicadores en las tablas 29, 31 y se presenta la ubicación de cinco de estos indicadores en un cuadro de mando integral genérico con sus perspectivas, con lo cual se cumple el objetivo general planteado, resumido en la gráfica 33.

- Este trabajo mostró la aplicación de otros enfoques válidos para el análisis de la ciberseguridad, empleando otras herramientas como la planeación por escenarios, y la utilización de indicadores clave de riesgo KRI con un enfoque en las causas de los riesgos que se quieren gestionar y analizando conceptos clave como el safety o aseguramiento en la continuidad del sector eléctrico. El safety, aunque es un concepto amplio, se logró focalizar y profundizar en los asuntos clave que pueden ser objeto de un incidente cibernético y que contribuyen a la confiabilidad del servicio y la seguridad en la operación.

- Los KRI propuestos llevan implícitos retos en el monitoreo de dispositivos y variables, para poder anticiparse a eventos y materialización de riesgos. Pero no es suficiente con sólo tener registros de manera continua, se debe fortalecer el proceso de análisis de la información con el fin auditar los comportamientos anómalos, detectando lo que está ocurriendo, generando las alertas, las acciones correctivas respectivas y alertando tanto el proceso productivo como la gestión de incidentes.

- El cálculo de los indicadores KRI basados en el safety y el aseguramiento funcional no solo compromete el equipo de respuesta a incidentes, sino que invita a trabajar de manera colaborativa con el proceso, debido a que cualquier anomalía que se detecte debe activar los dos procesos, tanto de gestión de respuesta a incidentes cibernéticos, como el personal

de mantenimiento de las TO para retornar el proceso al rango normal de las variables clave, basados en la resiliencia y las herramientas de continuidad del negocio.

7. Referencias bibliográficas

Armstrong, J. (1986). Long Range Forecasting: From Crystal Ball to Computer (2nd Edition). *The Journal of the Operational Research Society Vol 37*, 79-149.

Armstrong, J. (2009). Selecting Forecasting Methods. *Electronic Journal*, 1-19. Obtenido de http://ssrn.com/abstract=1941247

Bayuk, J. L. (2011). Alternative Security Metrics. *IEEE COmputer Society*, 943-946.

Bellovin, S. (2006). On the Brittleness of Software and the Infeasibility of Security Metrics. *IEEE Security and Privacy*.

Boyer, W., & McQueen, M. (2008). Ideal Based Cyber Security Technicals Metrics for Control Systems. *LNCS CRitical Information Infrastructures Security (CRITIS)*.

Consejo de la Unión Europea. (03 de 02 de 2020). *Diario Oficial de la Unión Europea.* Obtenido de Oficina de Publicaciones de la Unión Europea: https://op.europa.eu/es/publication-detail/-/publication/ba51b03f-66f4-4807-bf7d-c66244414b10/

Department of Homeland Security. (2009). *Primer Control System Cybersecurity Framework and Technicals Metrics* . DHS.

DOE. (2012). *Electricity Subsector Cybersecurity. Risk Management Process.* U.S. Departament of Energy - DOE.

Drias, Z., Serhrouchni , A., & Vogier, O. (2015). Analysis of Cyber Security for Industrial Control Systems. *IEEE*.

Francia, G. A. (2016). Baseline Operational Security Metrics for Industrial Control Systems. *Security and Management SAM16.* SAM.

Godet, M., & Roubelat, F. (2003). Creating the future: The use and misuse of scenarios. *Long Range Planning*, 164-171.

Godet, M., Monti, R., Meunier, F., & Roubelat, F. (2000). *La Caja de Herramientas de la Prospectiva.* París: Gerpa.

Hemsley, K. E., & Fisher, R. E. (2018). *History of Industrial Control System Cyber Incidents.* Idaho: Idaho National Laboratory.

ICS CERT. (2012). *ICS CERT Year in Review 2012.* U.S. Departament of Homeland Security.

ICS CERT. (2013). *ICS CERT Year in Review 2013.* U.S. Departament of Homeland Security.

ICS CERT. (2014). *ICS CERT Year in Review 2014.* U.S. Departament of Homeland Security.

ICS CERT. (2015). *ICS CERT Year in Review 2015.* U.S. Departament of Homeland Security.

ICS CERT. (2016). *ICS CERT Year in Review 2016.* U.S. Departament of Homeland Security.

ICS-CERT. (2011). *ICS-CERT Incident Response Summary Report 2009-2011.* U.S. Departament of Homeland Security.

IEC. (2003). *IEC 62264-1 Ed 1.0.* Suiza: IEC.

IEC. (2012). *IEC 62351-10 Guia de Arquitecturas de Seguridad Ed. 1.0.* Switzerland: IEC.

IEC. (2013). *Integración de Sistemas Empresariales y Sistemas de Control.* Suiza: IEC.

IEC. (2018). *IEC 62443-4-1. Security for industrial automation and control systems.* Switzerland: IEC.

ISO. (2008). *ISO 9001: 2008. Sistemas de gestión de la calidad - Requisitos.* Ginebra: Secretaría Central de ISO.

ISO. (2009). *ISO/IEC 27004. Information technology — Security.* Switzerland: ISO/IEC.

ISO. (2017). *Information technology — Security techniques — Information security controls for the energy utility industry .* Switzerland: ISO.

ISO/IEC. (2012). *Information technology — Security techniques — Code of practice for information security controls .* Switzelard.

ISO/IEC. (2014). *ISO/IEC 20016-1:2014.* Switzerland: ISO.

ISO/IEC. (2018). *Information technology — Security techniques — Information security management systems — Overview and vocabular.* Switzerland.

Jonsson, E., & Pirzadeh , L. (2012). A Framework for Security Metrics Based on Operational System Attributes. *IEEE COmputer Society*, 58-61.

Kahn, H., & Wiener, K. (1967). *The year 2000 a framework for speculation on the next thirty-tree years.* Washinton: The Huston Institute.

Kisner, R., Manges, W., MacIntyre, L., Nutaro, J., Munro, J., Ewing, P., . . . Olama, M. (2010). *Cybersecurity through Real-Time Distribuited Control Systems.* Springfield: Oak Ridge National Laboratory, Technical Report ORNL/TM-2010/30.

Knowles, W., Prince, D., Hutchison, D., Disso, J., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, 52-80.

Koronios, A., Kuusk, G., & Gao, J. (2017). *Convergence, alignment and integration of Operational and Information Technologies in organisations with Engineering Asset Management functions.* University of South Australia, CIEAM.

Kowalski, S., Barabanov, R., & Hoffman, R. (2011). Ciber Security Alert Warning System: A socio-technical coordinate system proposal. *IEEE Computer Society*, 21-24.

Kriaa, S., Cambacedes, L. P., Bouissou, M., & Halgand, Y. (2015). A survey of approaches combining safety and security for industrial control systems. *Reliabitity Engineering System Safety*, 157-175.

Labaka, L., Hernantes, J., & Sarriegi, J. M. (2015). A framework to improve the resilience of critical infrastructures. *International Journal of Disaster Resilience in the Built Environment; Bingley*, Tomo 6, Número 4, Páginas 409-423.

McIntyre, A., Becker, B., & Halbgewachs, R. (2007). *Security Metrics for Process Control System.* California: SANDIA National Laboratories.

Naqvi, S., & Riquidel, M. (2006). *Quantifiable Security Metrics for Large Scale Heterogeneous System.* Eureka - Celtic Project BUGYO.

NCS. (Octubre de 2004). *TECHNICAL INFORMATION BULLETIN 04-1 SCADA.* Arlington: OFFICE OF THE MANAGER NCS. Obtenido de http://docplayer.net/16998386-Supervisory-control-and-data-acquisition-scada-systems.html

NIST. (2009). *Directions in Security Metrics Research.* Gaithersburg,: U.S Deparment of Commerce.

NIST. (2012). *NIST SP 1108 R2 Framework and Roadmap for Smart Grid Interoperability Standars.* U.S Department of Commerce.

NIST. (2013). *NIST 800-53 R4 Security and Privacy Controls for Federal Information Systems.* Gaithersburg: U.S. Department of Commerce.

NIST. (2015). *NIST 800-82R2 Guide to Industrial Control Systems (ICS) Security.* Gaithersburg: U.S. Department of Commerce.

Obama Administration. (2013). *Presidential Policy Directive/PPD–21.* Washington: Administration of Barack Obama.

Paes, R., Mazur, D., Venné, B. K., & Ostrzenski, J. (2017). A Guide TO Securing Industrial Control Networks (IT/OT) Convergence. *Paper No PCIC-2017-10*, 89-96.

Park, S., & Lee, K. (2014). Advanced Approach to Information Security Management System Model for Industrial Control System. *The Scientific World Journal.*

Piggin, R., & Boyes, H. (2015). *Safety and security - a story of interdependence.* Walwich: Cyber security Centre, University of Warwich U.K.

Purboyo, T. W., Rahardjo, B., & Kuspriyanto. (2011). Security Metrics: A Brief Survey. *Information Technology and Biomedical Engineering.*

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (Diciembre de 2001). Identifying, Understanding, and Analyzing Critical Infrestructure Dependencies. *IEEE Control Systems Magazine*, 11-25. Obtenido de IEEE: https://ieeexplore.ieee.org/document/969131/

SANS. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid.* Washington: E- ISAC.

Schwab, W., & Poujol, M. (2018). *The State of Industrial Control System 2018.* Munich: CXP Group.

Sharma, K. (2017). *Overview of Industrial Process Automation.* Bengaluru, India: Elsevier.

Solms, R. v., & Niekerk, J. v. (2013). Fro Information Sucurity to cyber security. *Computers & Security*, 97-102.

Solms, R. V., & Niekerk, J. V. (2013). From Information Security to Cyber security. *Computers & Security 38*, 97-102.

Taylor, T. (2012). Convergencia TI/ TO. *Revista ABB*, 22-27.

Thafasal, L., Babu, B., Munner, P., & Varghese, J. (2017). Security Issues in SCADA based Industrial Control System. *IEEE*.

The White House. (12 de 02 de 2013). *Executive Order 13636—Improving Critical Infrastructure Cybersecurity* . Wasington: Obama Administration. Obtenido de https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

U.S. General Accounting Office. (04 de 2004). *Goberment Publishing Office.* Obtenido de https://www.gpo.gov/fdsys/pkg/GAOREPORTS-GAO-04-321/pdf/GAOREPORTS-GAO-04-321.pdf

Ujvarosi, A. (2016). Evolution of Scada Systems. *Bulletin of Transilvania University of Brasov*, 63-68. Obtenido de http://webbut.unitbv.ro/BU2015/Series%20I/2016/BULETIN%20I%20PDF/Ujvarosi_Al.pdf

V, A., & B, C. (1999). Metodología de los Escenarios para Estudios Prospectivos. *Revista Ingeniería e Investigación No. 44*, 26-35.

Vaarandi, R., & Pihelga, M. (2014). Using Security Logs for Collecting And Reporting Technical Security Metrics. *IEEE Computer Society*, 294-299.

Vergara Schmalbach, J. C., Fontalvo Herrera, T. J., & Maza Ávila, F. (2010). La planeación por escenarios: Revisión de conceptos y propuestas metodológicas. *Prospect*, 21-29.

Yin, R. K. (2003). Investigación sobre Estudio de Casos. *Applied Social Research Methods Series*, 35.

Zaratiegui, J. R. (1999). La gestón por procesos: Su papel e importancia en la Empresa. *Economía industrial*, 81-88.

Zeb, T., Yousaf, M., Afzal, H., & Mufti, M. R. (2017). A Quantitative Security Metric Model for Security Controls: Security Virtual Machine Migration Protocol as Target of Assessment. *Security & Management*, 126 - 140.

Zhou, C., Li, X., Zhang, Q., & Yang, S. (2014). *Risk-Based Task Scheduling Approach For Integrated Control Of System Safety And Cybersecurity In Industrial Control System.* Huazhong: University of Science And Technology, China.

8. Anexos

Anexo 1. Información Expertos Encuestados - Telecomunicaciones.

Nombre del experto	Profesión	Estudios	Especialidades/Disciplinas	Actividades generales
Andrés Felipe Vargas Ocampo	Ingeniero Electrónico	**Posgrado** • Especialización en Telecomunicaciones (UPB). • Especialización en Gerencia de Proyectos (UPB). • Maestría en TIC (UPB) (Pendiente Tesis). **Certificaciones** • Cisco CCNP desde 2006. • Administración y gestión de plataformas IP y Seguridad de Routers, Suiches y Firewall de los sistemas Cisco, Alcatel, Juniper, Nortel, Huawei, Sandvine, Fortinet, F5.	**Sistemas de control, instrumentación y comunicaciones en procesos de producción:** Sistema de control industrial, sistema SCADA para control del proceso de laminado y galvanizado, automatización de control por sistemas PLC, 5 años. **Telecomunicaciones** • Telecomunicaciones LMDS, ATM, Frame Relay, TCP/IP. 1 año. • Telecomunicaciones y seguridad cibernética, 13 años. • Ingeniería de red en sistemas basados en IP para banda ancha ISP, IAP, LAN e IDC, 13 años. • Coordinador del grupo de IP y LAN IDC que incluye todo el tema de Internet y servicios basados en IP y la parte de seguridad de estos sistemas, 13 años. • Despliegue de la red MPLS, administración de una red de radios basada en IP con sistema de radio en frecuencia no licenciada de 5.8 GHz, 5 años. • Migración de sistemas de subestaciones a capa 3 con enrutamiento y con componente de seguridad basado en túneles IPSec, 3 años.	• Soporte de red de telecomunicaciones para los procesos de energía, agua y gas. • Análisis de Riesgos cibernéticos Sistemas SCADA y telecomunicaciones de centros de control e implementación de controles de ciberseguridad. • Administración de infraestructura tecnológica de telecomunicaciones.

Nombre del experto	Profesión	Estudios	Especialidades/Disciplinas	Actividades generales
Walter Emilio Rodríguez	Ingeniero Electrónico	**Posgrado** • Especialización en Redes de Datos • Especialización en Gerencia de proyectos. • Maestría en Automatización.	**Telecomunicaciones** Mantenimiento, diseño y evaluación de redes de telecomunicaciones para redes de SCADA y de sistemas de protección de sistemas de potencia, 23 años.	• Soporte de red de telecomunicaciones para los procesos de energía, agua y gas. • Análisis de Riesgos cibernéticos Sistemas SCADA y telecomunicaciones de centros de control e implementación de controles de ciberseguridad. • Administración de infraestructura tecnológica de telecomunicaciones para centros de control y automatizaciones.

Anexo 2. Información Expertos Encuestados – SCADA.

Nombre del experto	Profesión	Estudios	Especialidades/Disciplinas	Actividades generales
David Esteban Sierra Tobón	Ingeniero de Sistemas	**Posgrado:** • Especialización en Seguridad Informática (2012). • Especialización en Gerencia de Proyectos (2015).	• Informática, 15 años. • Bases de Datos, 15 años. • Sistemas Operativos, 15 años. • Almacenamiento, 15 años. • Ciberseguridad, 8 años. • Sistemas SCADA, 15 años. • Automatización y Comunicaciones, 15 años.	• Administración de infraestructuras Críticas, Sistemas SCADA, Comunicaciones. • Protección y aseguramiento en sistemas de tiempo real. • Planeación y ejecución de proyectos de ciberseguridad, infraestructura en Centros de control y automatización de estaciones.

Nombre del experto	Profesión	Estudios	Especialidades/Disciplinas	Actividades generales
Rafael Ignacio Aristizábal Gómez	Ingeniero Electrónico	NERC-CIP para infraestructuras críticas.	**Centros de Control del Sector Eléctrico, 26 años de experiencia.** • Instalación, puesta en servicio de centros de control SCADA del sector eléctrico. • Administración tecnológica de infraestructura de centros de control. • Análisis de riesgos en tecnologías de operación. • Atención de auditorías en ciberseguridad para sistemas SCADA de centros de control. • Puesta FAT del SCADA/AGC/NA del centro del control del CND (Centro Nacional de Despacho). Pruebas y sintonía de Unidades de generación en sistema AGC. • Pruebas y sintonía de unidades de generación en sistema AGC.	• Instalación, implementación y puesta en servicio de RTUs y centros de control de energía eléctrica. • Análisis de Riesgos en Sistemas SCADA y Telecomunicaciones de centros de control. • Administración de infraestructura tecnológica de centros de control. • Soporte y mantenimiento de infraestructura de centro de control.

Anexo 3. Información Expertos Encuestados – Ciberseguridad.

Nombre del experto	Profesión	Estudios	Especialidades/Disciplinas	Actividades generales
Luis Carlos Herrera Velásquez	**Pregrado** Ingeniero de Sistemas **Profesión** Militar Fuerza Aérea – Fuerzas Militares Colombia	**Posgrado:** Maestría en Ciberseguridad y Gerencia Educativa.	**Infraestructuras Críticas** Protección cibernética de infraestructuras críticas, 10 años.	Identificación, protección, de infraestructuras críticas aeronáuticas.

Nombre del experto	Profesión	Estudios	Especialidades/Disciplinas	Actividades generales
Diego Zuluaga	**Pregrado** Ingeniero de Sistemas	**Posgrado:** • Especialista en Gerencia, CEIPA, 2003 • Maestría. Executive M.B.A. Máster en Dirección de Empresas, Escuela de Administración de Empresas de Barcelona, España, 2003. **Certificaciones** Gestión y riesgos de TIC, seguridad en información y de sistemas de control industrial (CISM, CRISC, CGEIT, GICSP, ISO 27001 L.A.).	**Ciberseguridad de Infraestructuras Críticas** • Líder del Sector eléctrico en la Mesa Nacional de Infraestructura Crítica, Riesgo Operacional y Ciberdefensa que lidera el Ministerio de defensa. • Lineamientos de ciberseguridad CNO (representante ISAGEN). • Implantación de normas NERC CIP. • Coordinador Nacional en Colombia del Centro de Ciberseguridad Industrial desde 2016. • Experto nacional seleccionado para asesorar a Colombia en ciberseguridad como contribución a la misión de asistencia técnica de la Organización de los Estados Americanos en la materia. • Líder de la comisión de ciberseguridad y del tema en el Comité que definió las guías en la materia para el sector eléctrico colombiano "Acuerdo C N O 788". **Seguridad de la información** Implantación del modelo integral de seguridad de la información, empleando como base las normas ISO 27000 y desde el 2010	Experto en temas de seguridad y ciberseguridad de infraestructuras críticas. Responsable de ciberseguridad en ISAGEN.

Anexo 4 Información Expertos Encuestados – Ciberseguridad, continuación…

Nombre del experto	Profesión	Estudios	Especialidades/Disciplinas	Actividades generales
Exell Enrique Franklin Jiménez	**Pregrado** Ingeniero Electrónico	**Certificaciones** • Security+ Certified • Enterprise Security Architecture Certified • ISA/IEC 62443 Cybersecurity Fundamentals Specialist • ISA/IEC 62443 Cybersecurity Risk Assessment Specialist. • ISA/IEC 62443 Cybersecurity Design Specialist. • Curso certificado del riesgo y resilencia en sistemas de aguas (awwa, norma G430, J100) • Curso NERC CIP SANS.	**Ciberseguridad de Infraestructuras Críticas** • Ingeniero de proyectos. Experiencia en 32 proyectos de automatización, 8 años. • Senior Member/IEEE.	Experto en temas de seguridad y ciberseguridad de infraestructuras críticas. Desarrollo de Actividades de consultoría en UNISYS.

Nombre del experto	Profesión	Estudios	Especialidades/Disciplinas	Actividades generales
Manuel Santander	**Pregrado** Ingeniero de Sistemas	**Posgrado:** • Maestría en Administración. • Maestría en Science in Information Security Engineering. • Estudiante de Doctorate of Science in Information Security. **Certificaciones** Certificaciones vigentes en seguridad desde el año 2005 (GSE, GCFA, GCIA, GCIH, GSEC, GPPA, GICSP, GNET, S.T.A.R. -IP Paquet Analysis.)	**Ciberseguridad de Infraestructuras Críticas** • Gestión del riesgo cibernético en sistemas de control industrial y SCADA., 10 años. • Diseño e implementación de arquitecturas de ciberseguridad, 6 años. • Gestión del riesgo de seguridad en sistemas de tecnologías de información, 24 años. • Respuesta a incidentes en ciberseguridad en sistemas de tecnologías de información y tecnologías de operación, 6 años. • Análisis forense en sistemas de tecnologías de información y tecnologías de operación.	Experto en temas de seguridad y ciberseguridad de infraestructuras críticas. Responsable de ciberseguridad en PUNTOS COLOMBIA.

Anexo 5. Información Expertos Encuestados – Automatización de Subestaciones.

Nombre del experto	Profesión	Estudios	Especialidades/Disciplinas	Actividades generales
Rodrigo Oswaldo Sánchez Forero	Ingeniero Electrónico	**Posgrado:** • Especialización en técnicas computarizadas para control de procesos. EAFIT • Especialización en Teleinformática. Universidad EAFIT	**Sistemas SCADA y de control distribuido:** • Planta de generación Tasajera, 9 años. • Planta de tratamiento San Fernando, 15 años. **Sistemas de control, instrumentación y comunicaciones en procesos de producción:** • Soporte y mantenimiento de sistemas de control en empresa privada, 9 años. • Soporte y mantenimiento de sistemas de control en empresa Planta Tasajera, 15 años. • Soporte y mantenimiento de sistemas de control en empresa Planta tratamiento San Fernando, 15 años. **Programación, configuración, montaje y puesta en servicio de sistemas de supervisión remota:** • Primer sistema SCADA de EPM en Subestación Central, 2 años. • Sistema SCADA de Aguas de Urabá, 1 año. **Diseño, especificaciones técnicas y contratación de sistemas de control:** • Central Tasajera • Planta San Fernando.	• Diseño • Programación • Configuración • Montaje. • Planeación • Acondicionamiento de señales. • Soporte y mantenimiento.

Nombre del experto	Profesión	Estudios	Especialidades/Disciplinas	Actividades generales
Paula María Roldán Zapata	Ingeniera Electrónica	**Posgrado:** • Especialización en Finanzas, Preparación y Evaluación de Proyectos. • Especialización en Mercados Energéticos. • Maestría en Ingeniería con Énfasis en Sistemas Energéticos	**Sistemas de control, instrumentación y comunicaciones en procesos de producción:** • Sistemas de Automatización de Subestaciones (SAS), 10 años. • Integración de cada uno de los procesos de automatización al centro de control, 10 años.	• Pruebas de integración de diferentes tipos de SAS con el Centro de Control • Pruebas de los nuevos protocolos para la automatización de subestaciones • Revisión de equipos e integración de nuevas tecnologías • Mantenimiento de los SAS de subestaciones • Implementación de acciones de mejora de acuerdo a la evolución de las tecnologías para SAS de subestaciones.

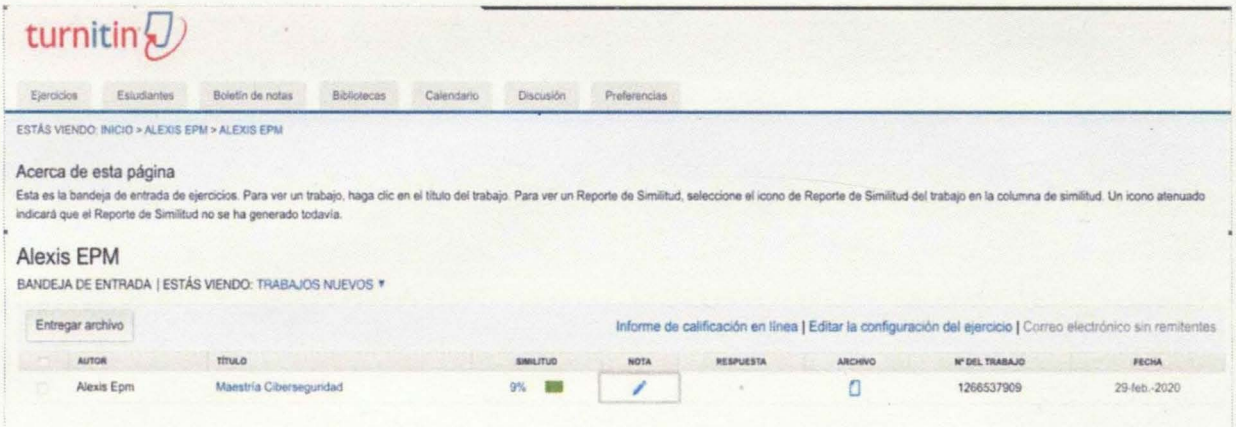
Anexo 6. Información Expertos Encuestados – Operación del Sistema Eléctrico.

Nombre del experto	Profesión	Estudios	Especialidades/Disciplinas	Actividades generales
Juan Carlos Villa Lopez	Ingeniero Electricista	**Posgrado:** • Especialización en Automática • Especialización en Gerencia de Proyectos • Especialización en Gerencia Financiera	**Planeación y Operación de Sistemas Eléctricos** • Estudios eléctricos, 7 años. • -Operación de Sistemas de potencia, 7 años. • Mantenimiento centros de control (SCADA y aplicaciones de tiempo real), 19 años.	Soporte y mantenimiento bases de datos para sistemas SCADA y Aplicaciones de tiempo real para análisis de sistemas de potencia eléctrica.

Anexo 7. Información de validación de la originalidad de la monografía.

Se adjunta reporte de similitud u originalidad del trabajo a partir de la herramienta **turnitin,** la cual arrojó un porcentaje de similitud de la monografía del 9% con otras fuentes, es decir una originalidad del 91%.

Fecha de entrega: 29-feb-2020 05:24p.m. (UTC+0100)
Identificador de la entrega: 1266537909
Nombre del archivo: MONOGRAFIA_ALEXIS_VERSIO_N_COMPLETA_APA.docx (8.7M)
Total de palabras: 32488
Total de caracteres: 181238



Maestría Ciberseguridad

INFORME DE ORIGINALIDAD

9%	5%	1%	6%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Universidad Militar Nueva Granada Trabajo del estudiante	1%
2	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	1%
3	Submitted to UNILIBRE Trabajo del estudiante	<1%
4	Submitted to Universidad Nacional de Colombia Trabajo del estudiante	<1%
5	Submitted to Universidad Pontificia Bolivariana Trabajo del estudiante	<1%
6	www.bdigital.unal.edu.co Fuente de Internet	<1%
7	Submitted to Western Governors University Trabajo del estudiante	<1%
8	www.essa.com.co Fuente de Internet	<1%

Fe de erratas

Se omite el punto seguido después de los niveles tres y cuatro.

Según las normas APA para identificar una página no se escribe pág sino la letra p. Debido a que la citación se realizó empleando funciones automáticas de office, las cuales tienen por defecto pág, esta función no es posible cambiarla en el editor de texto.