UNIVERSIDAD CATÓLICA DE CUENCA

Maestría en Ciberseguridad

Informe de Investigación previo a la obtención del título de Magíster en Ciberseguridad

Tema: Propuesta de directrices de ciberseguridad para redes de comunicación de infraestructuras críticas en la distribución eléctrica del Ecuador.

Autor: Ing. Fabián Cristóbal Jaramillo Jaramillo, Mg.

Asesores: Ing. Miguel Santiago Andrade López, Mg.

Ing. Juan Carlos Ortega Castro, Mg.

Cuenca, 2024

Certificación de Asesores

Se certifica que:

El informe de investigación "Propuesta de directrices de ciberseguridad para redes de comunicación de infraestructuras críticas en la distribución eléctrica del Ecuador", de autoría del Señor Ingeniero Electrónico Fabián Cristóbal Jaramillo Jaramillo, CC: 0103203600, ecuatoriano, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Ciberseguridad, cumple con la caracterización y estructura (parte protocolaria y parte expositiva) y se sujeta a la normativa pertinente exigida por el Consejo de Educación Superior, CES y la Universidad Católica de Cuenca, en consecuencia se autoriza su presentación para los trámites pertinentes.

Santa Ana de los Ríos de Cuenca

Julio, 2024

_____	_____
Ing. Miguel Andrade López. Mg	Ing. Juan Carlos Ortega Castro. Mg
Asesor Científico	Asesor Metodológico

Certificación de Autoría

Certifico que:

“Propuesta de directrices de ciberseguridad para redes de comunicación de infraestructuras críticas en la distribución eléctrica del Ecuador”, es el tema del informe final de investigación de mi AUTORÍA, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Ciberseguridad, por lo que, asumo su originalidad y el uso de fuentes de terceros registrados según las normas APA vigentes.

Santa Ana de los Ríos de Cuenca

Julio, 2024

_____

Ing. Fabián Cristóbal Jaramillo Jaramillo. Mg

CC: 0103203600

Agradecimiento

A la Empresa Eléctrica Regional Centro Sur C.A., y en particular al Ing. Patricio Pérez Fajardo, quiero expresar mi profundo agradecimiento por su desinteresada y generosa colaboración durante el desarrollo de este trabajo.

A los Ingenieros Miguel Andrade y Juan Carlos Ortega, tutores de este proyecto de investigación, quienes con su cooperación han permitido alcanzar los objetivos del presente estudio.

Dedicatoria

A Dios, por guiarme y permitirme avanzar un paso más en mi vida académica y profesional.

A las mujeres de mi vida, Isabel y Elisa, quienes son la fuente de mi inspiración y dedicación.

Resumen

En Ecuador, las empresas de distribución eléctrica carecen de metodologías para enfrentar amenazas cibernéticas en sus redes de operación, que permiten el telecontrol y la operación del sistema eléctrico de potencia. Este estudio se enfoca en desarrollar directrices específicas para asegurar los sistemas de adquisición de datos y control en la distribución eléctrica tales como ADMS (Advanced Distribution Management System) y sus distintos módulos, abordando la necesidad de proporcionar enfoque y directrices de ciberseguridad en Tecnologías de Operación (TO). Centrado en la línea de Energía eléctrica y Tecnologías de la Operación, el estudio busca identificar y comprender vulnerabilidades cibernéticas, proponiendo "Directrices de ciberseguridad para el sistema eléctrico de potencia en empresas distribuidoras del Ecuador". Se plantea realizar un análisis holístico del entorno de la infraestructura de redes TO y proponer recomendaciones para fortalecer la resiliencia. Mediante la revisión de normativas, estudio de casos de ciberataques y propuestas de mejoras aplicando arquitecturas de ciberseguridad adecuadas, se busca establecer una metodología aplicable en el marco de las distribuidoras, considerando aspectos tecnológicos, operacionales y procedimentales. El estudio busca abordar la implantación de ciberseguridad en sistemas de comunicación de redes eléctricas, proponiendo medidas concretas para garantizar la continuidad y confiabilidad de los servicios eléctricos en Ecuador.

Palabras clave: vulnerabilidades, SCADA, ADMS, ciberseguridad, directrices

Abstract

In Ecuador, electrical distribution companies lack methodologies to address cyber threats in their operating networks, which allow for the remote control and operation of the electrical power system. This study focuses on developing specific guidelines to secure data acquisition and control systems in electrical distribution, such as the ADMS (Advanced Distribution Management System) and its various modules, addressing the need to provide focused guidelines for cybersecurity in Operational Technologies (OT). Focused on the realm of Electric Power and Operational Technologies, the study seeks to identify and understand cyber vulnerabilities and proposes "Cybersecurity Guidelines for the Electrical Power System in Distribution Companies in Ecuador." It aims to conduct a holistic analysis of the OT network infrastructure environment and recommend measures to strengthen resilience. Through the review of regulations, case studies of cyberattacks, and proposals for improvements using appropriate cybersecurity architectures, the study intends to establish a methodology applicable within the framework of distributors, considering technological, operational, and procedural aspects. The study addresses the implementation of cybersecurity in electrical telecommunications networks, proposing concrete measures to guarantee the continuity and reliability of electrical services in Ecuador.

Keywords: Vulnerabilities, SCADA, ADMS, cybersecurity, guidelines

Índice de contenidos

Contenido

Índice de figuras

Índice de tablas

Capítulo I. Introducción

1.1 Situación problemática

Las empresas de distribución eléctrica en Ecuador carecen de una cultura robusta y una metodología definida de actuación en el ámbito de ciberseguridad para redes de infraestructuras críticas. La falta de conciencia y prácticas efectivas de ciberseguridad plantea amenazas significativas para la integridad de los sistemas eléctricos críticos. Un aspecto preocupante es la concentración de esfuerzos de protección en las redes de Tecnologías de la Información (TI), relegando a un segundo plano las redes de Tecnologías de la Operación (TO) utilizadas en entornos industriales, como los Sistemas de Gestión de Distribución Avanzada (ADMS).

Según la empresa de evaluación e investigación de tecnologías Gartner Inc., la terminología **tecnologías de la operación** refiere a "*hardware y software que detecta o provoca un cambio, a través de la supervisión y/o el control directo de los equipos, activos, procesos y eventos industriales*". Un concepto similar maneja el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) que señala que las tecnologías de la operación (TO) "*refieren al hardware y software que se utiliza para detectar o causar cambios en procesos físicos a través del monitoreo o ejecución de dispositivos que forman parte de sistemas de control industrial".*

Mientras que las tecnologías de información se enfocan en la gestión de datos y procesos administrativos como aplicativos, utilitarios y sistemas orientados a clientes interno y externo, las de TO se centran en el control y monitoreo de procesos físicos. Las tecnologías de operación generalmente se encuentran en ambientes industriales donde la fiabilidad y la robustez son esenciales, mientras que IT opera en entornos corporativos y de oficina.

La falta de enfoque integral de ciberseguridad en las empresas aumenta la vulnerabilidad de la infraestructura crítica del sector eléctrico. La escasa conciencia sobre amenazas específicas a estos sistemas y la falta de capacitación especializada contribuyen a estas vulnerabilidades. Por ello, se requiere desarrollar una propuesta de directrices de ciberseguridad específicas que aborden las particularidades y riesgos de la infraestructura de telecontrol del sistema eléctrico de potencia en la fase de la distribución eléctrica, fomentando una cultura sólida que considere tanto las redes de TI como las de TO, permitiendo una mejora sustancial en la integridad y confiabilidad de la infraestructura eléctrica del país.

En este análisis, el problema radica en la carencia de directrices específicas o falta de conocimiento en su aplicabilidad que permitirían asegurar a los Sistemas de Control en tiempo real de la distribución eléctrica. La convivencia de las redes de tecnologías de la información corporativa (TI) y las de tecnologías de la operación (TO), expone a la infraestructura crítica a riesgos significativos de ciberataques. Por otra parte, la falta de orientaciones especializadas para abordar estas amenazas plantea un desafío crítico.

Se busca, a través del presente documento, atender el problema científico, el cual se centra en cómo desarrollar directrices de ciberseguridad específicas para los sistemas de infraestructura crítica en la distribución eléctrica, considerando sus características únicas y la dinámica y acelerada evolución de las amenazas cibernéticas. La carencia de metodologías, análisis técnicos y cultura de operación impide una protección robusta y adaptada a los desafíos actuales, comprometiendo la disponibilidad, integridad y confiabilidad de la infraestructura eléctrica. El estudio busca, por tanto, abordar esta brecha identificada para proponer soluciones concretas y prácticas a fin de mitigar los riesgos cibernéticos en estos sistemas críticos para mejorar la continuidad y disponibilidad del suministro eléctrico.

1.2 Línea de Investigación

Tipo de línea	Líneas de investigación institucionales	Sub Línea	
En desarrollo	Energía eléctrica y Tecnologías de la Información para la innovación y el desarrollo sostenible	Ciencia de los ordenadores, analítica de datos y algoritmos computacionales	☒
		Sistemas eléctricos de potencia, energía e iluminación	☐
		Modelado, automatización y control	☐

Fuente: Universidad Católica de Cuenca

Este estudio facilitará el análisis y la creación de una guía sobre la evolución de los ataques cibernéticos a sistemas de infraestructuras críticas y estrategias avanzadas de ciberseguridad, con referencia en las normas de operación NIST SP 800-82, IEC 61968, automatización y control de subestaciones IEC 61850 y ciberseguridad ISA/IEC 62443.

1.3 Objeto de estudio

Este trabajo de investigación se concentra en la identificación y comprensión de las vulnerabilidades cibernéticas intrínsecas en estos sistemas, en el análisis de arquitecturas de red y mejores prácticas, así como en la evaluación de aplicación de metodologías y directrices especializadas para su protección en el ámbito de la ciberseguridad. El análisis busca examinar las características particulares de los sistemas de infraestructura crítica del sector de distribución eléctrica del país; y las vulnerabilidades y amenazas que podrían comprometer su disponibilidad y confiabilidad.

Se propone generar un documento que contenga directrices de aplicación procedimental y práctica que coadyuve al resguardo de elementos de telecontrol del sistema eléctrico de potencia en la distribución de energía eléctrica, que guíe la operación, administración y gestión de este sistema de forma segura.

1.4 Campo de acción

El ámbito de acción se enfoca en el desarrollo de una " Propuesta de directrices de ciberseguridad para redes de comunicación de infraestructuras críticas en la distribución eléctrica del Ecuador ". Este proceso comprenderá varias etapas fundamentales para fortalecer la seguridad de los sistemas de infraestructura crítica:

1. Revisión de principios, fundamentos y generalidades de los sistemas de control y supervisión SCADA.
2. Análisis de arquitectura y componentes de sistemas de infraestructura crítica. Para este fin se evaluará el sistema de la Empresa Eléctrica Regional Centro Sur C.A.
3. Inventario de activos críticos del sistema, en los cuales podría suceder incidentes o ataques informáticos.
4. Revisión de casos de ciberataques globales a infraestructuras críticas, lo cual permitirá identificar patrones y vulnerabilidades, proponer medidas preventivas, y desarrollar estrategias de respuesta efectivas, fortaleciendo la respuesta ante futuras amenazas cibernéticas.
5. Encuesta a personal involucrado en la operación, supervisión y administración de las redes del sistema de subestaciones eléctricas de CENTROSUR.
6. Elaboración de directrices detalladas que aborden los aspectos críticos de la ciberseguridad en estos sistemas, considerando particularidades de estos entornos.

1.5 Objetivos

General

Desarrollar un marco integral de recomendaciones de ciberseguridad específicas para la protección de redes del sistema eléctrico de potencia de distribución eléctrica en el Ecuador, con el propósito de mitigar riesgos de ataques cibernéticos, garantizar la continuidad de los servicios eléctricos y fortalecer la evolución de la infraestructura tecnológica eléctrica del país.

Específicos

- Identificar las principales amenazas actuales que afectan a los sistemas y redes de infraestructura crítica en la distribución eléctrica del Ecuador, incluyendo sus patrones, orígenes y posibles impactos en la integridad y operatividad del sistema.
- Evaluar la arquitectura y componentes de estos sistemas y redes, con el fin de identificar vulnerabilidades específicas y proponer medidas preventivas y correctivas.
- Desarrollar un conjunto de recomendaciones prácticas de ciberseguridad, adaptadas a las particularidades de los sistemas de infraestructura crítica en el ámbito de la distribución eléctrica del Ecuador, que aborden vulnerabilidades específicas y promuevan la implementación de medidas preventivas y correctivas.
- Proponer estrategias para fomentar una cultura sólida de ciberseguridad que abarque a redes de TO en el contexto de la distribución eléctrica en Ecuador, con el fin de concientizar sobre la importancia de la ciberseguridad en el sector energético y promover la implementación de medidas preventivas y correctivas.

1.6 Problema científico - preguntas de investigación

Preguntas científicas

- ¿Cómo proteger redes del sistema eléctrico de potencia en empresas distribuidoras del Ecuador de manera efectiva, ante las amenazas cibernéticas actuales y futuras?
- ¿Cómo realizar una concienciación eficiente y generar una cultura adecuada de ciberseguridad para operadores, administradores y alta gerencia?
- ¿Cuáles son los principales vectores de ataque en redes adquisición de datos y telecontrol de distribución eléctrica?
- ¿Cómo medir la efectividad y aplicabilidad de la guía de recomendaciones propuesta?

1.7 Hipótesis

La propuesta de una guía de ciberseguridad para redes de comunicación de infraestructuras críticas en la distribución eléctrica podría servir como un estándar de aplicación en el sector de la distribución eléctrica del Ecuador

1.8 Variables

- **Variable independiente:**
  - Elaboración de un documento de directrices de ciberseguridad para protección de redes del sistema eléctrico de potencia en empresas distribuidoras del Ecuador.
- **Variables dependientes:**
  - Análisis de arquitectura de redes y componentes de sistemas de infraestructura crítica de distribución eléctrica.

- Evaluación de amenazas y vulnerabilidades presentes en redes del sistema eléctrico de potencia en empresas distribuidoras del Ecuador.
- Investigación de reportes de ciberataques de gran impacto en empresas distribuidoras de electricidad a nivel mundial.

Conceptualización	Unidad de medida	Instrumento
Variable independiente: Propuesta de directrices de ciberseguridad para redes de comunicación de infraestructuras críticas en la distribución eléctrica del Ecuador Desarrollo de un documento que establezca pautas y recomendaciones para la ciberseguridad de los sistemas y redes de infraestructuras críticas en la distribución eléctrica del Ecuador	Documento generado	Investigación documental y revisión de normativas
Variable dependiente: Análisis de arquitectura de redes y componentes de sistemas de infraestructura crítica de distribución eléctrica Evaluación de la estructura y componentes de los	Documento generado	Revisión de documentación técnica y entrevistas con expertos en el tema

sistemas de infraestructura crítica utilizados en la distribución eléctrica del Ecuador		
Variable dependiente: Evaluación de amenazas y vulnerabilidades presentes en redes del sistema eléctrico de potencia en empresas de distribuidoras del Ecuador.	Documento generado	Matriz de evaluación y análisis de datos
Identificación y evaluación de las amenazas y vulnerabilidades que afectan a las redes del sistema eléctrico de potencia utilizados en la distribución eléctrica del Ecuador.		
Valor independiente: Investigación de reportes de ciberataques de gran impacto en empresas de energía a nivel mundial		
Recopilación y análisis de ciberataques producidos a nivel mundial en empresas de distribución eléctrica.	Documento generado	Investigación documental

1.9 Justificación – contribuciones de la investigación

Justificación teórica

El estudio sobre "Propuesta de directrices de ciberseguridad para redes del sistema eléctrico de potencia en empresas distribuidoras del Ecuador" es imperativo en el actual panorama tecnológico. Con el aumento de la interconexión digital en la infraestructura eléctrica, la vulnerabilidad de los sistemas de infraestructura crítica se ha vuelto evidente, enfrentándose a riesgos de ataques cibernéticos que podrían comprometer la estabilidad y seguridad energética. Esta investigación se justifica al abordar la falta de directrices específicas para proteger estos sistemas críticos. Al proporcionar recomendaciones de ciberseguridad, se busca llenar este vacío y ofrecer un marco integral para fortalecer la disponibilidad e integridad de las redes del sistema eléctrico de potencia.

Las contribuciones a la investigación incluyen el desarrollo de estrategias prácticas y efectivas para mitigar amenazas cibernéticas en entornos de infraestructura crítica, considerando las peculiaridades de la infraestructura eléctrica. Además, se espera que este estudio inspire la implementación de medidas preventivas y correctivas, promoviendo la conciencia sobre la importancia de la ciberseguridad en el sector energético. En última instancia, esta investigación no solo proporciona orientación técnica valiosa, sino que también contribuye a la seguridad global de las infraestructuras críticas en un mundo cada vez más digitalizado.

1.10 Estado del arte o antecedentes

Tomando en cuenta la acelerada evolución tecnológica y la creciente interconexión de dispositivos y redes, los sistemas de control de infraestructura crítica que van desde estructuras básicas de SCADA (Supervisory Control and Data Acquisition) hasta ADMS (Advanced

Distribution. Management System), utilizados en la distribución eléctrica, han emergido como objetivos críticos para los ataques cibernéticos. (Rosas, Medina y Mesa, 2020).

Los ataques cibernéticos a redes de telecontrol en sistemas eléctricos de potencia han evolucionado desde hackers humanos hasta redes de *bots* y, más recientemente, la incorporación de inteligencia artificial (IA). Esta progresión complica la comprensión, detección y control de amenazas. La introducción de IA agrega una capa de complejidad, ya que los algoritmos de aprendizaje automático se adaptan en tiempo real. La seguridad en estos sistemas requiere medidas avanzadas y colaboración constante para enfrentar el panorama de amenazas en constante cambio.

En el marco de la contextualización de la ciberseguridad en sistemas de infraestructura crítica, se evidencia un aumento en las amenazas cibernéticas específicas que impactan la distribución eléctrica. Desde ataques de denegación de servicio (DoS) hasta programas malignos (malware) meticulosamente diseñado para infiltrarse en sistemas industriales, la gama de amenazas es amplia y sofisticada.

En respuesta a este panorama, se ha reconocido la necesidad crítica de establecer marcos regulatorios y normativas específicas para la ciberseguridad en redes e infraestructura de telecontrol del sistema eléctrico de potencia en la distribución del País. Diversas organizaciones gubernamentales y entidades reguladoras han buscado generar e implementar directrices que buscan impulsar la seguridad en el sector eléctrico, fomentando así un estándar de operación y una cultura de ciberseguridad. No obstante, hasta el momento los resultados no han sido favorables o adoptados como metodologías o culturas operativas de las empresas del sector eléctrico ecuatoriano.

Además, se observa un incremento en las investigaciones centradas en la ciberseguridad de infraestructuras críticas. Estudios previos han abordado cuestiones relacionadas con la protección de sistemas de controles críticos tomando como fundamento ataques de gran impacto ocurridos en el ámbito mundial.

El panorama actual también revela la diversidad de tecnologías y métodos utilizados para proteger la infraestructura de telecontrol de los sistemas eléctricos de potencia. Esto abarca desde cortafuegos (*firewalls*) industriales y sistemas de detección de intrusiones hasta la segmentación de redes y la implementación de mejores prácticas de seguridad cibernética.

A pesar de estos avances, persisten desafíos significativos en la implementación efectiva de medidas de ciberseguridad en sistemas de infraestructura crítica. Estos desafíos incluyen la resistencia al cambio en las operaciones industriales, la interoperabilidad de tecnologías, el desconocimiento del impacto en caso de un ataque y la falta de conciencia sobre la importancia de la ciberseguridad.

En cuanto a enfoques innovadores y tendencias de vanguardia, algunas investigaciones destacan la integración de inteligencia artificial y aprendizaje automático para detectar anomalías en estos sistemas.

Una observación relevante es la creciente colaboración entre las empresas y la academia en la búsqueda de soluciones efectivas. La investigación conjunta contribuye a una comprensión integral de las amenazas y a la identificación de soluciones prácticas y adaptativas.

La inclusión de casos de estudio en el estado actual proporciona lecciones valiosas sobre incidentes pasados, subrayando la importancia de aprender de la experiencia, tomar conciencia, crear planes de acción y mejorar continuamente las prácticas de ciberseguridad.

Finalmente, se identifican áreas clave para futuras investigaciones, tales como el desarrollo de tecnologías de ciberseguridad específicas para entornos de adquisición de datos y telecontrol de distribución eléctrica, la evaluación de la capacidad de respuesta frente a amenazas sofisticadas y la integración de medidas de seguridad en el diseño mismo de la infraestructura eléctrica. Este análisis holístico contribuye a la comprensión integral y al avance continuo de la ciberseguridad en sistemas críticos del sector eléctrico, permitiendo elaborar un documento que contenga las directrices necesarias y buenas prácticas para la aplicación al corto plazo en las empresas de distribución eléctrica del Ecuador.

1.11 Marco teórico referencial

El avance tecnológico ha permitido que la operación de las subestaciones eléctricas evolucione de sistemas de control electromecánicos y operación local, a sistemas de control con potentes microprocesadores, protocolos IP y operación centralizada (Castro y Salazar, 2019). En este contexto, las redes de control y adquisición de datos han emergido como una tecnología fundamental para supervisar y controlar los procesos críticos asociados con la generación, transmisión y distribución de energía eléctrica.

La aplicación de las redes de control y adquisición de datos en los sistemas eléctricos de potencia referentes a la distribución eléctrica ha transformado la forma en que se gestiona y operan las redes en subestaciones eléctricas. Estas redes permiten la monitorización en tiempo real, la automatización de procesos, el telemando y la toma de decisiones ágil en respuesta a eventos imprevistos. Además, facilitan la integración de fuentes de energía renovable, contribuyendo así a la transición hacia sistemas más sostenibles y resilientes.

La importancia de las redes de control y adquisición de datos se manifiesta en varios aspectos, pues, optimizan la gestión de recursos al proporcionar información detallada sobre el

rendimiento de los diferentes componentes de la red. Esto permite una asignación más eficiente de la carga y una reducción de las pérdidas en la distribución eléctrica. Además, las redes del segmento de TO facilitan la integración de tecnologías inteligentes tipo Internet de las Cosas (IoT), mejorando la calidad del suministro eléctrico y permitiendo la detección y acción temprana ante posibles anomalías.

A pesar de los beneficios, el auge y evolución de las redes de infraestructura crítica van acompañadas de desafíos considerables en cuanto a seguridad informática. La creciente interconexión de estos sistemas con redes de información estándar y el uso de tecnologías convencionales los hacen susceptibles a diversas amenazas cibernéticas. Las vulnerabilidades tecnológicas en cuanto a la seguridad informática de estos sistemas, obliga a realizar un profundo análisis en cuanto a metodologías de trabajo, mejores prácticas y controles.

Las amenazas a las que están expuestas estas redes, son diversas. Los ataques de tipo intrusión, malware, *ransomware, man-in-the-middle,* accesos no autorizados o denegación de servicio distribuido (DDoS) pueden impactar la disponibilidad de la red, lo que podría tener consecuencias significativas en la continuidad del suministro eléctrico. La manipulación de datos es otra preocupación seria, ya que podría comprometer la integridad de la información y conducir a decisiones erróneas en la operación del sistema.

Los ataques de acceso no autorizado o intrusión representan una amenaza potencial para la seguridad de estas redes, ya que podrían permitir a intrusos tomar control no autorizado de los dispositivos de telecontrol. Existen diferentes tipos de ataques que pueden ocurrir en cualquiera de las capas de operación de la organización, desde el nivel de supervisión hasta el nivel de los equipos de instrumentación, donde atacan al hardware, al software y a la conexión de red. (Torres Valero, 2020)

Estos riesgos no deben subestimarse, ya que las interrupciones en los sistemas de TO pueden tener impactos graves. Desde apagones que afectan a comunidades enteras, pérdidas económicas significativas para las empresas, así como multas y sanciones por parte de entidades reguladoras o inclusive pérdida de vidas humanas. La seguridad de las redes de los sistemas eléctricos de potencia se ha convertido en un componente crítico e indispensable de la infraestructura eléctrica moderna.

La ciberseguridad emerge como una necesidad imperante en este contexto. La implementación de medidas de seguridad informática robustas es esencial para proteger las redes de control y adquisición datos contra posibles amenazas. *Firewalls*, cifrado de datos, autenticación fuerte, sistemas de prevención de intrusos, redes de cero confianza (*zero trust networks*), conexiones en redes privadas virtuales (VPN) y otras prácticas de seguridad son herramientas clave en este esfuerzo. Otros aspectos fundamentales son la concienciación y formación en seguridad para el personal operativo para prevenir y responder eficazmente a las amenazas cibernéticas. Además, es indispensable conocer las vulnerabilidades de los componentes de estos sistemas, pues únicamente cuando se cuente con el conocimiento necesario sobre sus posibles debilidades, se podrá plantear planes de acción para prevenir eventos no deseados. Conocer el estado de cada dispositivo permite obtener información de su comportamiento. De esta forma se pueden deducir acciones y conformar estrategias diferentes que ayuden a reducir el riesgo cibernético (Quiroz Tascón et al., 2020)

Es crucial destacar que la seguridad no es un problema que pueda abordarse de manera aislada por cada empresa, ya que las empresas de distribución del país se conectan a un sistema ADMS nacional. La colaboración entre las distribuidoras y las entidades gubernamentales (Ministerio de Energía y Minas, CENACE, ARCERNNR, etc.), es esencial para desarrollar y

mantener estándares de seguridad efectivos. La creación de políticas y regulaciones que promuevan prácticas de ciberseguridad robustas es una responsabilidad compartida que garantizará la protección a largo plazo de las redes de control y adquisición de datos y, por ende, de la infraestructura eléctrica nacional en su conjunto.

La evolución de las redes y arquitecturas de infraestructura crítica representan un avance significativo en la gestión de sistemas de distribución eléctrica. Su capacidad para mejorar la eficiencia operativa, simplificar la gestión y la confiabilidad del suministro eléctrico es innegable. Sin embargo, la seguridad informática en este contexto es un desafío que debe abordarse de manera proactiva. La conciencia, el análisis oportuno, metodologías efectivas y la colaboración son varios de los aspectos clave para proteger estas redes críticas y garantizar que continúen contribuyendo positivamente a la operación de los sistemas eléctricos modernos. La inversión en ciberseguridad no solo es una medida preventiva, sino una salvaguarda para el futuro de los sistemas eléctricos del país. (Cornaglia, S., y Vercelli, A. (2017). La ciberdefensa y su regulación legal en Argentina. Urvio, Volumen 20, pp. 46-62.)

1.12 Procedimientos éticos

No aplica.

1.13 Fundamentación teórica

Contar con un conjunto de directrices y buenas prácticas de ciberseguridad en las redes de y sistemas de infraestructuras críticas, tales como los de distribución eléctrica, se vuelve imprescindible para garantizar la continuidad operativa y proteger contra ataques cibernéticos. Ejemplos como el ataque Stuxnet en 2010, que afectó instalaciones nucleares en Irán, y los ataques a la red eléctrica de Ucrania en 2015 y 2016, destacan la vulnerabilidad de estos sistemas y la necesidad de medidas de seguridad robustas. Los sistemas de telecontrol y adquisición de

datos son objetivos potenciales debido a su importancia estratégica, lo que resalta la urgencia de protegerlos contra amenazas cibernéticas y muchas veces son desestimados por priorizar las redes de TI.

Además de interrumpir el suministro eléctrico, los ataques pueden tener consecuencias económicas, sociales, regulatorias significativas. La implementación de medidas de seguridad, como *firewalls* industriales, sistemas de detección de intrusiones y autenticación de múltiple factor, segmentación de redes, es crucial para mitigar estos riesgos y proteger la infraestructura crítica. Además, las empresas eléctricas deben procurar implementar buenas prácticas a través de normativas, estándares de operación, control y ciberseguridad internacionales relacionados a estos ambientes, tales como NIST SP 800-82, IEC 61968, IEC 61850 e ISA/IEC 62443, para garantizar la integridad y disponibilidad de sus sistemas.

Capítulo II. Diagnóstico situacional

2.1 Metodología

Se han identificado 6 etapas para el desarrollo de este estudio, mismos que se detallan a continuación:

1. **Primera etapa**

Se recopiló información sobre principios, fundamentos y generalidades de los sistemas de infraestructura crítica. De igual manera, se realizó la selección y evaluación de fuentes bibliográficas fiables y necesarias para la elaboración del presente documento.

2. **Segunda etapa**

Se llevó a cabo un análisis técnico de las topologías y arquitectura de red de los sistemas de subestaciones eléctricas utilizadas por parte de la Empresa Eléctrica Regional Centro Sur C.A., con la finalidad de comprender la lógica de operación y seguridad implementada en la actualidad.

3. **Tercera etapa**

Una vez realizado el análisis técnico, se procedió a identificar los activos críticos y vulnerabilidades dentro de los sistemas de control y automatización industrial (IACS), los cuales se recomienda considerar para realizar un análisis de riesgos a los sistemas de las redes de tecnologías de la operación, conforme la normativa ISA/IEC-62443-3-2 la cual describe una metodología de evaluación de riesgos de seguridad específica para IACS.

4. **Cuarta etapa**

Se desarrolló un estudio de casos de ciberataques a sistemas industriales o de infraestructuras críticas a nivel mundial, con la finalidad de conocer métodos de ataque, impacto,

planes de recuperación y respuesta; y demás información relevante a ser considerada en el análisis.

5. **Quinta etapa**

Se realizó una recopilación de información a través de encuestas específicas en materia de seguridad de la información y ciberseguridad, al personal técnico y administrativo involucrado en la cadena de operación y gestión de los sistemas de infraestructura crítica.

6. **Sexta etapa**

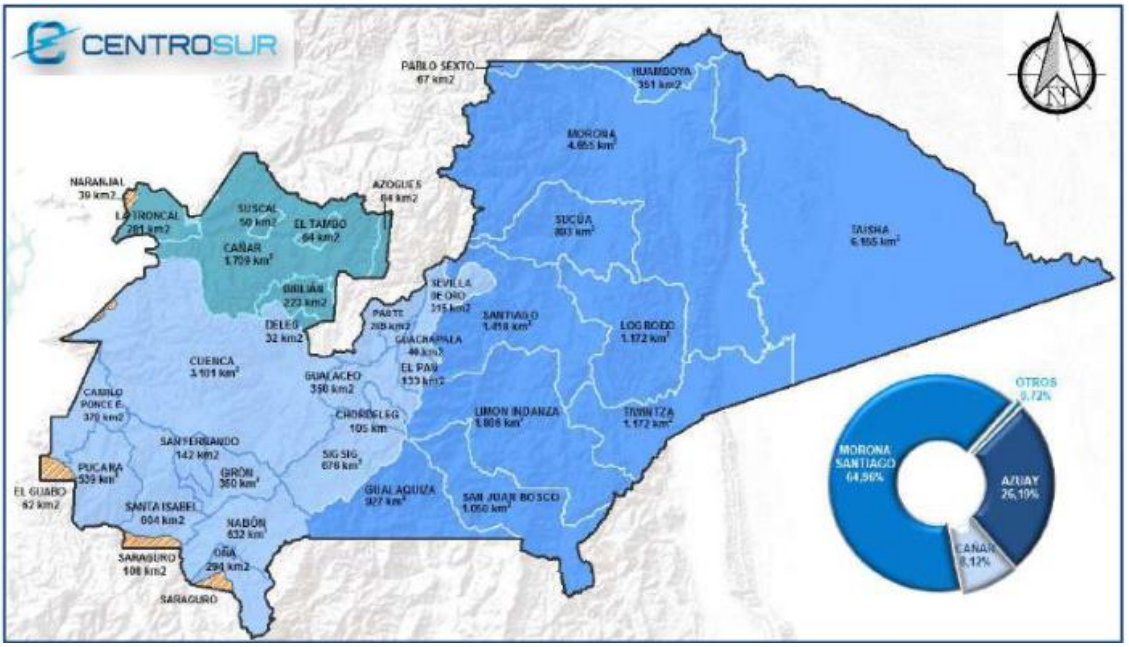
Finalmente, con todos los insumos de información descritos en las etapas anteriores, se pone a consideración una guía de propuesta de directrices de ciberseguridad para redes de comunicación de infraestructuras críticas en la distribución eléctrica del Ecuador.

2.2 Análisis situacional

Según su plan estratégico, la Empresa Eléctrica Regional Centro Sur C.A., se encarga de distribuir y comercializar energía eléctrica en las provincias de Azuay, Cañar y Morona Santiago, abarcando más de 30.000 km², lo que representa aproximadamente el 11.77% del territorio eléctrico nacional. La Empresa atiende alrededor de 430,000 clientes, lo que la sitúa en el tercer lugar entre las empresas distribuidoras, tanto por la cantidad de clientes como por la extensión de su área de concesión.

Figura 1

Área de concesión de la Empresa Eléctrica Regional Centro Sur C.A.



Nota: Zona geográfica de cobertura de servicio de CENTROSUR. Fuente: Plan Estratégico Empresa Eléctrica Regional Centro Sur 2022 – 2025

Al igual que las empresas de generación y de distribución eléctrica, CENTROSUR está considerada dentro de "áreas estratégicas" por el Estado Ecuatoriano. Por tal motivo, resulta imperativo realizar un estudio sobre los riesgos y vulnerabilidades a las que se encuentran expuestas sus redes de telecomunicaciones de tecnologías de operación, tales como redes LAN de subestaciones (Bus de procesos y Bus de estación), redes LAN de ADMS y redes LAN de equipos telegestionados de distribución (reconectadores, detectores de falla, reguladores de voltaje, etc.). Pues en específico, estos sistemas supervisan y controlan la distribución de energía eléctrica al usuario final a través de sus redes de media y baja tensión.

Así también la calidad del servicio es normado y regulado por la Agencia de Regulación y Control de Energía y Recursos Naturales no Renovables (ARCERNNR), quienes establecen

parámetros de evaluación como frecuencias medias de interrupción (FMIK) y tiempos medios de interrupción (TTIK) de suministro eléctrico, lo que conlleva inclusive a multas y penalizaciones para las empresas distribuidoras en caso de no cumplir los indicadores regulados.

En la actualidad, CENTROSUR ha basado el aseguramiento de sus redes de infraestructura crítica en función de requerimientos puntuales y a la constante evolución de estos sistemas que han migrado de protocolos y conexiones de tipo serie a ethernet. Lo cual, si bien es una ventaja en cuanto a velocidades de transmisión, telegestión, convergencia, conectividad y otros aspectos relevantes, también se ve expuesta a vulnerabilidades propias de entornos de redes basadas en protocolo TCP/IP.

La Empresa tampoco cuenta con un plan de seguridad o directrices orientadas al aseguramiento de redes de tecnologías de operación (TO), el cual debería velar por garantizar la seguridad de la información de estos sistemas en sus 3 ejes principales: disponibilidad, integridad y confidencialidad del servicio eléctrico.

2.3 Análisis comparativo

Para este estudio, se ha escogido la norma IEC 62443 “Seguridad para sistemas de control y automatización industrial” debido a su enfoque integral y especializado en la seguridad de sistemas de automatización y control industrial (IACS). La IEC 62443 proporciona un marco detallado y estructurado para proteger estos sistemas críticos contra amenazas cibernéticas, abordando tanto aspectos técnicos como organizacionales. La norma abarca una amplia gama de prácticas y medidas de seguridad esenciales para la protección de sistemas de control industrial, desde el diseño seguro de sistemas hasta la gestión continua de riesgos y la respuesta a

incidentes. Este enfoque integral permite que las organizaciones adopten una estrategia holística para la seguridad de sus infraestructuras críticas.

Además, la norma IEC 62443 está diseñada específicamente para entornos de automatización y control industrial, fundamentales para la operación de infraestructuras críticas como las redes eléctricas. Al centrarse en las peculiaridades y desafíos específicos de estos sistemas, la norma proporciona directrices relevantes y aplicables. Su reconocimiento internacional y adopción por numerosas organizaciones en todo el mundo acreditan que la aplicación de las prácticas recomendadas por este estándar permite implementar controles y generar cultura de aseguramiento de infraestructura crítica.

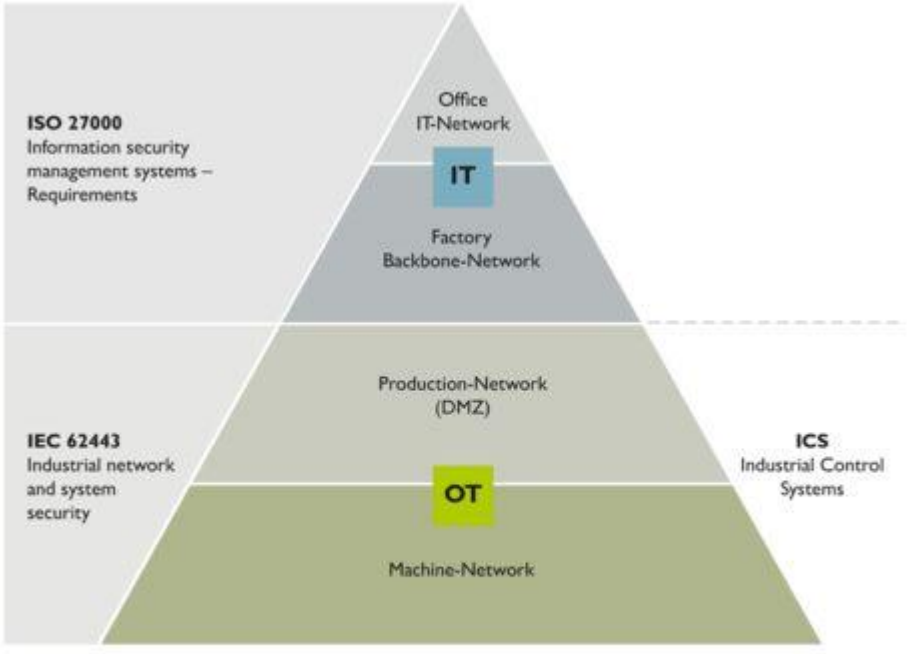
La aplicación de la norma IEC 62443 se puede complementar con otras normas de seguridad de la información, como las de la familia ISO/IEC 27000, que han sido consideradas relevantes para este estudio debido a su enfoque en la gestión de la seguridad de la información. Estas normas proporcionan un marco para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI). La ISO/IEC 27000 ofrece una metodología bien establecida para la gestión de riesgos de seguridad de la información, crucial para identificar y mitigar amenazas en sistemas de control industrial, y permite aprovechar las mejores prácticas globales en gestión de seguridad de la información, asegurando que las directrices desarrolladas sean completas y estén alineadas con estándares reconocidos internacionalmente.

La compatibilidad y sinergia entre IEC 62443 e ISO/IEC 27000 crean una postura de seguridad fortalecida, al integrar la seguridad de sistemas de control industrial con las prácticas generales de seguridad de la información, logrando una cobertura total de las necesidades de seguridad. En resumen, la elección de la norma IEC 62443 para este estudio se debe a su enfoque

detallado y específico para la protección de sistemas de automatización y control industrial, complementado por las normas ISO/IEC 27000, que aportan un marco robusto para la gestión general de la seguridad de la información, siendo un pilar fundamental para alcanzar conceptos en Industria 4.0.

Figura 2

Triángulo de seguridad ISO 27000 / IEC 62443



Nota: Esquema normativo de seguridad IT – TO. Fuente: https://www.phoenixcontact.com/es-mx/iec-62443-norma-ciberseguridad-industrial

Capítulo III. Propuesta

3.1 Principios, fundamentos y generalidades de redes SCADA

Los sistemas SCADA (Supervisory Control and Data Acquisition) son fundamentales para la supervisión y control de procesos industriales y de infraestructura crítica, como la distribución eléctrica, el tratamiento de agua, y la gestión del tráfico. Estos sistemas están diseñados para recopilar datos en tiempo real de los dispositivos y equipos distribuidos en el campo, procesar esta información, y permitir a los operadores monitorizar y controlar los procesos desde ubicaciones centralizadas. Los principios básicos de SCADA incluyen la adquisición de datos, el control en tiempo real, la supervisión remota, y la automatización de procesos.

Las primeras redes SCADA aparecieron en la década de 1960. Fueron desarrolladas para supervisar y controlar procesos industriales básicos, utilizando líneas telefónicas dedicadas y sistemas de radio para la transmisión de datos. Con el paso del tiempo, durante la década de 1970, el uso de estos sistemas comenzó a expandirse en diversas áreas, incluida la energía. Esto se debió a la creciente necesidad de mejorar la supervisión y el control en subestaciones de distribución eléctrica, lo que permitió una gestión más eficiente y segura de las infraestructuras críticas.

3.1.1 Componentes de las primeras redes SCADA

- **Unidades Terminales Remotas (RTU):** Dispositivos ubicados en sitios remotos que recopilan datos de sensores y otros dispositivos, y envían esta información a un sistema central. También podían recibir comandos del sistema central para controlar equipos locales.

- **Controladores Lógicos Programables (PLC):** En algunos sistemas, los PLCs se utilizan para realizar control local de procesos. A diferencia de las RTUs, los PLCs son más versátiles y tienen la capacidad de ser programados para realizar tareas complejas de control.
- **Sistema de Control Maestro (MCS):** Funciona como "el cerebro" del sistema SCADA, usualmente ubicado en un sitio de control centralizado. El MCS recibe datos de las RTUs y PLCs, los procesa, y presenta esta información a los operadores humanos a través de interfaces gráficas.
- **Interfaz Hombre-Máquina (HMI):** Las HMIs permiten a los operadores humanos interactuar con el sistema SCADA. Muestran datos en tiempo real y permiten a los operadores enviar comandos a los dispositivos remotos.
- **Red de Comunicaciones:** La red de comunicaciones conecta las RTUs y PLCs con el MCS. Al principio, esta red utilizaba líneas telefónicas dedicadas, radios, microondas y, en algunos casos, enlaces satelitales.

3.1.2 Puertos y Medios de Comunicación

Puertos Serie: Los primeros sistemas SCADA dependían en gran medida de la comunicación serie (RS-232, RS-485) para conectar RTUs y PLCs al MCS. Estos puertos eran adecuados para la comunicación a larga distancia con velocidades de transmisión limitadas.

Protocolos de comunicación y control: Al existir un entorno seguro basado únicamente en conexiones seriales, los protocolos de comunicación utilizados antiguamente en los sistemas de supervisión y control se consideraban completamente seguros, pues no había forma de vulnerarlos de manera externa. Los protocolos utilizados como MODBUS y DNP3 eran los más utilizados. Cabe indicar que los protocolos mencionados anteriormente evolucionaron de

conexiones seriales a protocolos TCP/IP, esto permitió no solo una mejora tecnológica sino inclusive provocó que se prescindiera de personal en sitio (subestaciones eléctricas) para operar, supervisar y controlar el sistema.

Líneas Telefónicas Dedicadas: En muchos casos, las RTUs y el MCS estaban conectados a través de líneas telefónicas dedicadas, que proporcionaban una conexión punto a punto confiable.

Radiofrecuencia (RF): Las redes de radiofrecuencia son utilizadas en áreas donde volvía complicada la instalación de cables. Estos sistemas permiten la transmisión de datos a través del aire entre largas distancias, aunque están limitados por la capacidad de ancho de banda y otros parámetros como interferencia y ruido.

Microondas y Satélites: Para conexiones de larga distancia y áreas remotas, se utilizan enlaces de microondas en bandas licenciadas y satélites. Estos métodos permiten cubrir grandes zonas geográficas.

3.1.3 Características y Limitaciones de los primeros modelos SCADA

Fiabilidad: Los primeros sistemas SCADA estaban diseñados para ser altamente fiables, ya que supervisaban infraestructuras críticas. Sin embargo, su dependencia de medios de comunicación físicos y dedicados limitaba su flexibilidad, escalabilidad y supervisión.

Seguridad: La seguridad no era una preocupación principal en los primeros sistemas SCADA, ya que operaban en redes cerradas, físicamente aisladas y con conexiones seriales entre un dispositivo y otro. Con el paso del tiempo y la incorporación de elementos digitales que incluyen conectividad a través de puertos ethernet y por consecuente utilizan protocolos TCP/IP, que por un lado permitió una evolución exponencial en cuando a flexibilidad, escalabilidad,

confiabilidad, interconectividad y mejoras en el control, también dio paso a la presencia de amenazas cibernéticas**.**

Capacidad de Procesamiento: Las capacidades de procesamiento y almacenamiento eran limitadas comparadas con los estándares modernos. Sin embargo, eran suficientes para las tareas de supervisión y control necesarias en ese momento. Hoy en día se requiere de redes estables, confiables, que ofrezcan mínima latencia y en los paquetes transmitidos y recibidos e inclusive con la implementación de subestaciones digitales, se requiere de anchos de banda cada vez mayores en los puertos de conexión de los dispositivos de red.

3.1.4 Evolución de los sistemas SCADA

Con el avance de la tecnología, los sistemas de control y automatización han evolucionado significativamente. La introducción de redes basadas en protocolo TCP/IP, protocolos de comunicación DNP3, IEC 60870-5-104 y estándar como IEC 61850, debido a mayores capacidades de procesamiento y almacenamiento han permitido sistemas más robustos, confiables y escalables.

Las primeras redes SCADA para la distribución eléctrica se basaban en una combinación de RTUs, PLCs, sistemas de control maestros, HMIs y diversas formas de comunicación a larga distancia, principalmente a través de puertos serie y líneas dedicadas. La evolución de estos sistemas basados en Ethernet ha traído muchas ventajas tecnológicas, pero también ha planteado desafíos significativos en cuanto a la ciberseguridad en entornos completamente digitales. Con el aumento de las amenazas cibernéticas, la ciberseguridad se ha convertido en una prioridad para los sistemas de infraestructura crítica. Para proteger los datos y garantizar la integridad de estos sistemas, se implementan equipos de seguridad como *firewalls*, sistemas de detección y prevención de intrusiones (IDS/IPS) y protocolos de comunicación seguros.

Los sistemas de infraestructura crítica modernos están diseñados para ser escalables, permitiendo la adición de nuevos dispositivos y la expansión del sistema sin interrupciones significativas. También permiten la integración con tecnologías de Internet de las Cosas (IoT) permite la recopilación de datos de una variedad de dispositivos conectados, mejorando la visibilidad y el control sobre los procesos. Además, la analítica de *Big Data* se utiliza para procesar grandes volúmenes de datos, aportando información valiosa de la operación y supervisión, facilitando la toma de decisiones.

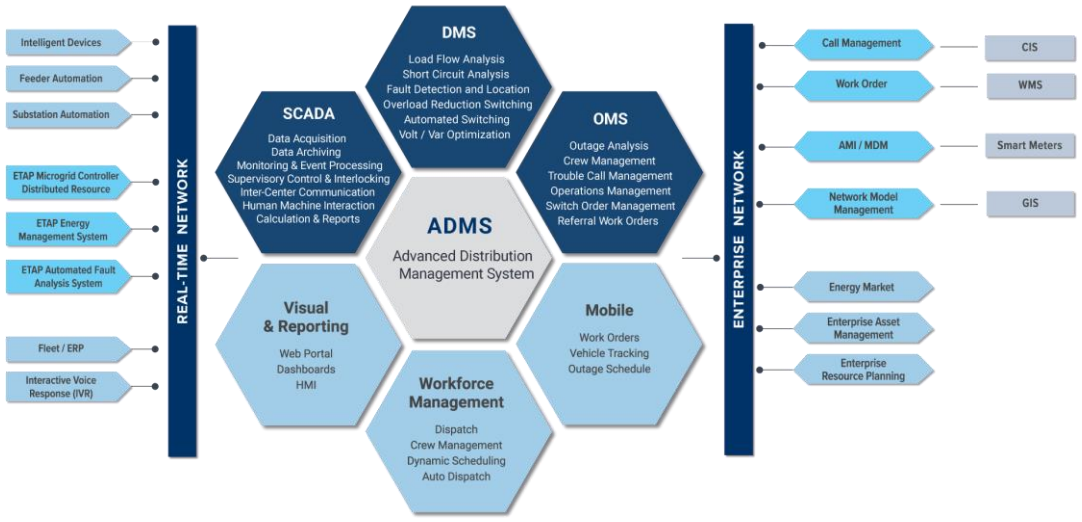
La evolución de estos sistemas ha permitido implementar arquitecturas redundantes en todos los niveles, desde los servidores hasta las comunicaciones y el almacenamiento de datos. Otra mejora son las interfaces de usuario cada vez más simples, intuitivas y ricas en funcionalidades. Utilizan gráficos de alta resolución, *dashboards* personalizables e inclusive soporte para dispositivos móviles, lo que permite a los operadores acceder y controlar el sistema desde cualquier lugar.

Los sistemas de TO se centran en la supervisión, automatización y el control en tiempo real de infraestructuras críticas, integrando dispositivos tales como RTU, dispositivos electrónicos inteligentes (IED) y empleando tecnologías de comunicación tradicionales como líneas dedicadas y radio. En contraste, los actuales sistemas ADMS (Advanced Distribution Management Systems), ofrecen capacidades avanzadas como la optimización de la red, la gestión de energía distribuida, y el análisis predictivo, integrando tecnologías modernas como IoT, inteligencia artificial y análisis de Big Data. Mientras que el sistema tradicional SCADA proporciona monitoreo básico y control, ADMS permite una gestión más eficiente y resiliente de la red eléctrica, facilitando la integración de energías renovables y una mejor respuesta a las fluctuaciones de demanda y eventos imprevistos. Actualmente el sistema ADMS Nacional con el

que cuenta CENTROSUR incluye los módulos de SCADA (Supervisory Control and Data Acquisition), OMS (Sistema de Gestión de Interrupciones); MWM (Gestión de la Fuerza de Trabajo Móvil) y DMD (Sistema de Gestión de la Distribución), según la norma IEC 61968.

Figura 3

Componentes de sistemas ADMS



Nota: Componentes y módulos adaptables a ADMS. Fuente: https://etap.com/es/solutions/advanced-distribution-management-system

3.1.4 Niveles de control en subestaciones

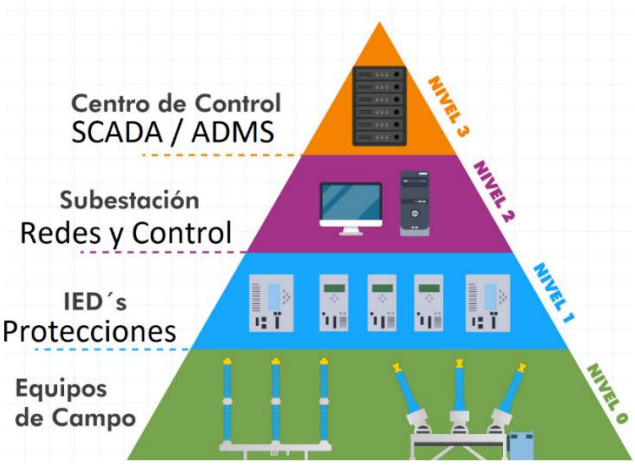
En la actualidad, la administración y responsabilidad del control de la operación del sistema eléctrico de CENTROSUR se dimensiona en 4 niveles según la norma IEC/61850, mismos que se detallan a continuación:

- **Nivel 0 (Patio):** Equipos de Campo (Transformadores, interruptores, seccionadores, sensores, actuadores, etc.)
- **Nivel 1 (Protecciones):** Dispositivo Electrónico Inteligente (IED)

- **Nivel 2 (Control):** Sistema de Automatización de Subestaciones (SAS), Sistema de Automatización de la Distribución (DAS), Unidad de terminal remota (RTU).
- **Nivel 3 (Centro de Control):** ADMS

Figura 4

Niveles de Control de las Subestaciones



Nota: Niveles de Control de las Subestaciones según norma IEC / 61850. Fuente: https://web.facebook.com/inelinc/photos/niveles-de-control-en-subestaciones-el%C3%A9ctricas%EF%B8%8F-desde-el-punto-de-vista-del-cont/704818106780285/?_rdc=1&_rdr

3.2 Análisis de arquitectura de los sistemas de comunicaciones de tecnologías de operación

Los diagramas de arquitectura de red presentados a continuación sintetizan la topología utilizada para la comunicación, control y operación del sistema eléctrico de potencia. En el primer diagrama se puede visualizar a manera muy general los elementos de telecomunicaciones utilizado para el control y automatización de la distribución eléctrica. El segundo diagrama detalla a través de bloques la interconectividad y lógica de comunicación de los dispositivos dentro de los niveles 0 hasta nivel 3.

Es importante señalar que, en el año 2017, por primera vez se incluyó un elemento de seguridad perimetral de TO por parte de CENTROSUR, con la finalidad de segmentar la red corporativa y servicios de tecnologías de la información de las de tecnologías de operación.

Como se había indicado anteriormente, todas las empresas de distribución del Ecuador se encuentran conectadas a un único servicio ADMS a través de una red nacional de telecomunicaciones del sector eléctrico (RENTSE). Los servidores del ADMS están físicamente ubicados de forma redundante en 2 centros de datos nacionales (Quito y Guayaquil), mismos que se encuentran protegidos por clúster de *firewalls* perimetrales que controlan tráfico de ingreso y salida hacia las distintas empresas distribuidoras, filtrando protocolos, puertos de conectividad, etc.

Adicional al sistema ADMS, las empresas distribuidoras cuentan con un módulo de supervivencia de SCADA-LOCAL denominado OASYS, mismo que funciona como contingencia en el caso de que la RENTSE o los sistemas nacionales sufran algún inconveniente o desperfecto, permitiendo a las empresas contar con la operación del sistema telegestionado ante eventos de fuerza mayor. Toda la información adquirida y recolectada es enviada tanto al sistema ADMS nacional como a los servidores CMX (concentrador de datos local).

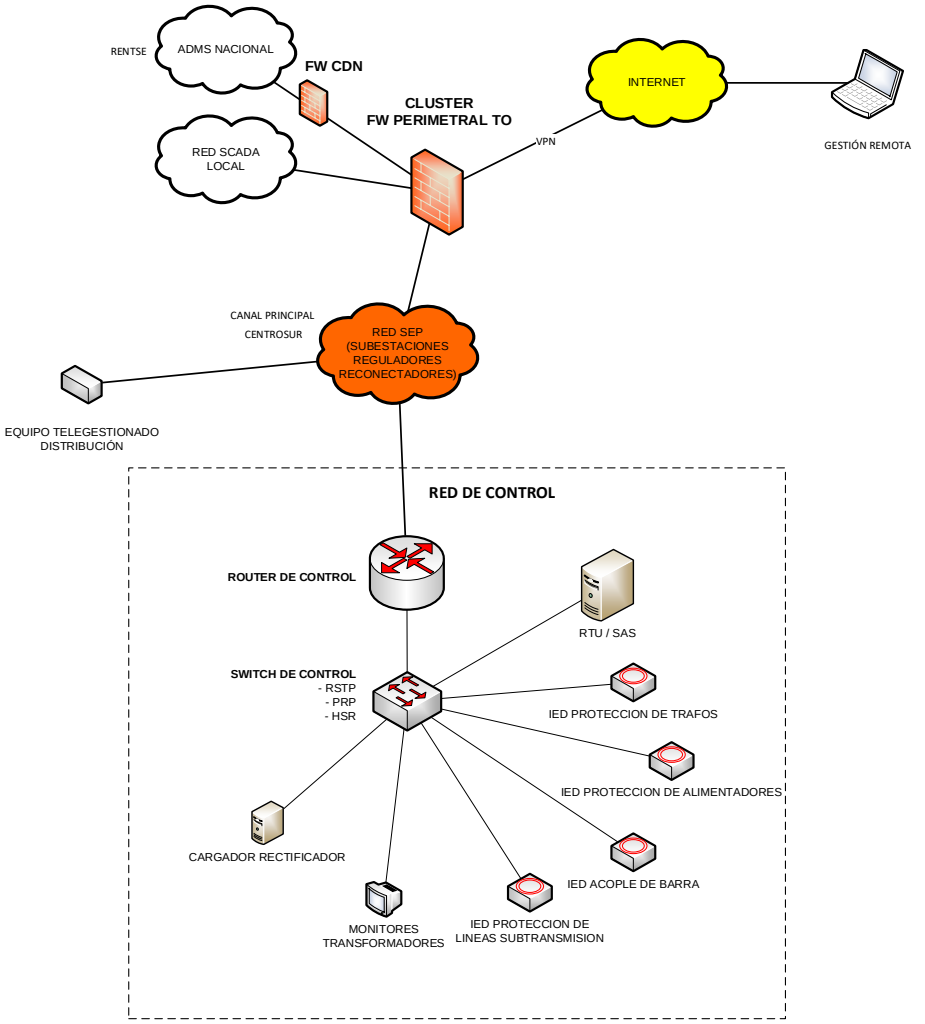
La Empresa Eléctrica Regional Centro Sur C.A., cuenta con 19 subestaciones de distribución eléctrica, mismas que están interconectadas a través de una red de tipo anillo IP/MPLS (Multiprotocol Label Switching).

A más de la infraestructura física de subestaciones descrita anteriormente, en CENTROSUR operan equipos de corte y maniobra de la distribución (reconectadores) que permiten supervisar y controlar la red eléctrica en tiempo real, con la intención de reducir los

parámetros de FMIK y TTIK; y buscan contribuir al incremento de la disponibilidad del suministro eléctrico y reducir el área de interrupción. Para este tipo de infraestructura generalmente se utilizan equipos de comunicación de última milla como enlaces en radio frecuencia en bandas no licenciadas o enlaces de fibra óptica.

Figura 5

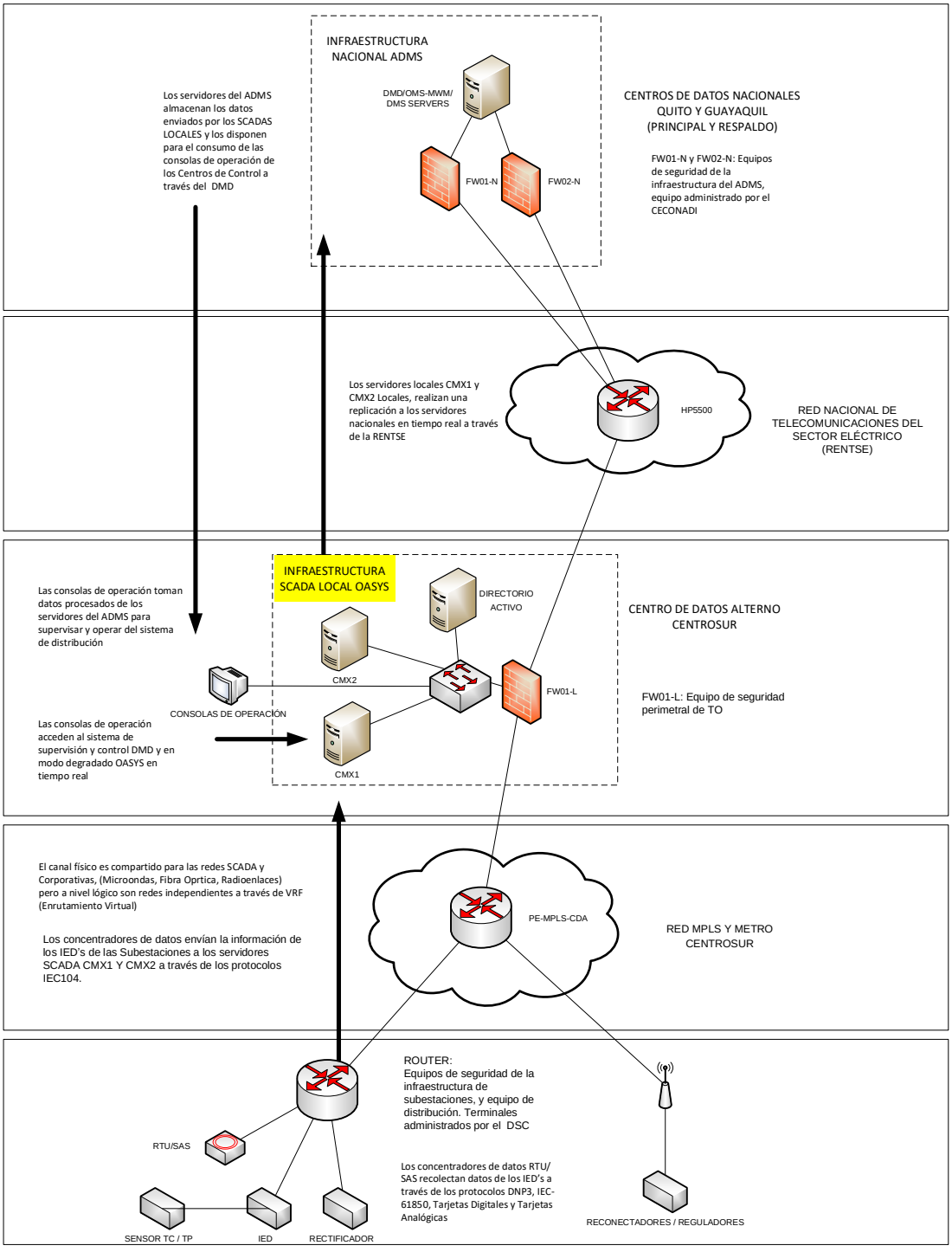
Topología actual de comunicación de sistema de TO de CENTROSUR



Nota: Diagrama de red de telecomunicaciones de sistema de TO. Fuente: Empresa Eléctrica Regional Centro Sur C.A.

Figura 6

Diagrama de comunicación de sistema de TO de CENTROSUR



Nota: Diagrama de bloques de telecomunicaciones y control N0 – N3. Fuente: Diagramas Empresa Eléctrica Regional Centro Sur C.A.

3.3 Inventario de activos

Tomando en cuenta que, para el propósito del estudio, se considerarán activos que cuenten con conectividad en puertos ethernet (que utilizan protocolo TCP/IP), debido a que son los únicos que podrían ser vulnerados o sufrir un ciberataque, se presenta el siguiente inventario de activos por niveles:

Tabla 1.

Levantamiento de activos de información de sistemas TO por niveles de control

Niveles de Control	Activo	Cantidad	Descripción / Observaciones
Nivel 0	N/A	N/A	N/A
Nivel 1	IED	700	Equipos distribuidos en subestaciones y en campo (reconectadores) – Cuentan con OS propietario
Nivel 2	Switch capa 2	76	Interconexión equipos de red LAN
	Switch capa 3 / Router	19	Equipo de borde de Subestación
	SAS	9	Control de automatización de subestación – Windows Server
	DAS	8	Control de automatización de distribución – Windows Server
	RTU	11	Concentrador de datos de subestación – OS propietario
Nivel 3	Servidor CMX	2	Concentradores de datos del sistema SCADA local – Windows Server
	Servidor AD	1	Autenticación de usuarios – Windows Server

	Consolas de operación	3	Acceso exclusivo a los sistemas de TO – Windows
	Consolas de simulación y configuración	2	Acceso exclusivo a los sistemas de TO – Windows – Bloqueo puertos USB – Direccionamiento estático
	Video Wall	1	Arreglo de monitores de 4 x 2
	Firewall Perimetral TO	1	Segmenta la red TI de TO y proporciona seguridad de perímetro
TOTAL ACTIVOS		**833**	

Nota: Inventario de activos de sistema de TO de CENTROSUR Fuente: Autor

3.4 Análisis de riesgos sobre activos

En función del levantamiento de activos realizado en el numeral anterior, se recomienda elaborar una categorización de activos críticos. Esta categorización permitirá identificar aquellos elementos que son esenciales para la operación continua y segura de la infraestructura de TO. Resulta indispensable la elaboración de planes de mitigación de riesgos, ya que contribuirá significativamente a la continuidad del negocio y de los sistemas de infraestructura crítica. Un análisis detallado permitirá detectar las amenazas y vulnerabilidades específicas que podrían afectar la disponibilidad, integridad y confidencialidad de estos activos críticos, evaluando el impacto potencial de diferentes escenarios de riesgo.

Los planes de tratamiento de riesgos deben incluir medidas de mitigación para reducir la probabilidad y el impacto de su ocurrencia, también proponer estrategias de transferencia de riesgo a terceros (como seguros o contratos), y mecanismos de aceptación cuando los riesgos se

consideren tolerables. En casos extremos, también puede ser necesario eliminar por completo ciertos riesgos mediante la reestructuración o actualización de activos.

De igual manera estos planes contribuirán a la mitigación de incidentes de seguridad, tales como ciberataques, fallos técnicos y errores humanos. Invertir en estos procesos no solo protege los activos críticos, sino que también fortalece la gestión de activos (inventario, estado, mantenimientos preventivos y correctivos, optimización de recursos, vida útil, etc.), capacidad de respuesta y recuperación ante incidentes, asegurando la estabilidad a corto, medio y largo plazo de los sistemas industriales y la infraestructura crítica.

3.5 Análisis de ataques a redes de infraestructura crítica documentados a nivel mundial

3.5.1 Caso Stuxnet (Irán-2010)

Stuxnet es un gusano informático descubierto en junio de 2010, famoso por su sofisticación y por ser uno de los primeros ejemplos de una ciberarma diseñada para causar daños físicos en el mundo real. Este malware fue diseñado específicamente para atacar los sistemas de control industrial SCADA utilizados por Siemens, que eran empleados en las instalaciones nucleares de Irán.

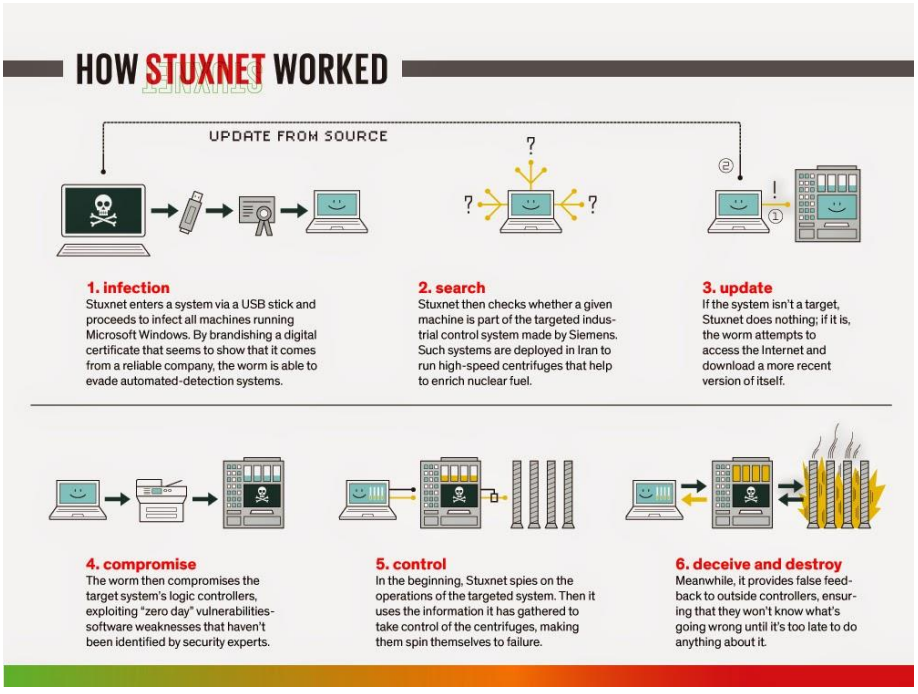
El principal objetivo de Stuxnet era la planta de enriquecimiento de uranio en Natanz, Irán. El gusano se propagaba a través de unidades USB infectadas y redes locales, buscando instalaciones de software específico de Siemens. Una vez que encontraba un sistema objetivo, Stuxnet alteraba la operación de las centrifugadoras utilizadas para enriquecer uranio, haciéndolas girar a velocidades peligrosamente altas y luego reduciéndolas drásticamente. Estas fluctuaciones dañaban las centrifugadoras mientras que el malware enviaba señales falsas a los sistemas de monitoreo, indicando que todo funcionaba correctamente, lo que dificultaba la detección del problema.

Se cree que Stuxnet fue desarrollado por Estados Unidos e Israel como parte de una campaña para retrasar el progreso del programa nuclear de Irán sin recurrir a ataques militares directos. La sofisticación de Stuxnet radica en su capacidad para explotar múltiples vulnerabilidades de día cero y en su conocimiento profundo de los sistemas industriales de Siemens, lo que sugiere un desarrollo con recursos significativos y conocimiento interno.

El descubrimiento de Stuxnet reveló una nueva dimensión de la guerra cibernética, demostrando que los ciberataques podían tener consecuencias físicas significativas. Además, puso de manifiesto la vulnerabilidad de las infraestructuras críticas a ataques cibernéticos sofisticados, subrayando la necesidad de fortalecer la ciberseguridad en instalaciones industriales y gubernamentales en todo el mundo.

Figura 7

Mecanismo de ataque de Stuxnet



Nota: Descripción de modo de infección de Stuxnet. Fuente*:* https://www.davidromerotrejo.com/2014/12/stuxnet-analizando-su-funcionamiento.html

3.5.2 Caso BlackEnergy (Ucrania-2016)

El caso de BlackEnergy en Ucrania es uno de los ciberataques más significativos contra infraestructuras críticas en la historia reciente. En diciembre de 2015, BlackEnergy, un malware originalmente desarrollado para llevar a cabo ataques de denegación de servicio distribuido (DDoS), fue empleado para atacar varias compañías eléctricas ucranianas, provocando cortes de energía que afectaron a aproximadamente 230,000 personas durante varias horas. Este ataque fue notable por su sofisticación y coordinación.

El ataque comenzó con correos electrónicos de *phishing* dirigidos a los empleados de las compañías eléctricas. Estos correos contenían documentos de Microsoft Office con macros maliciosas que, una vez habilitadas, descargaban y ejecutaban el malware BlackEnergy. Este malware permitió a los atacantes obtener acceso remoto a los sistemas de las compañías y moverse lateralmente dentro de las redes, identificando y comprometiendo los sistemas de control industrial (ICS).

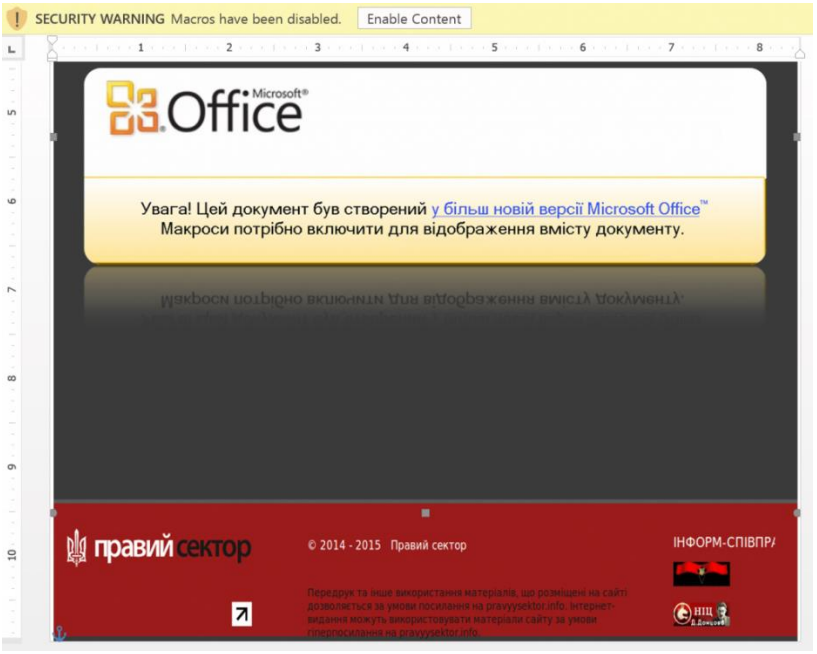
Una vez que los atacantes tuvieron el control de los sistemas ICS, utilizaron BlackEnergy para ejecutar comandos que causaron los apagones. Los atacantes también deshabilitaron los sistemas de respaldo, lo que complicó significativamente los esfuerzos de recuperación. Además, emplearon herramientas adicionales, como KillDisk, para borrar registros y archivos del sistema, lo que dificultó aún más la restauración del servicio y la investigación posterior.

El ataque no solo demostró la capacidad de los ciberatacantes para causar daños físicos a las infraestructuras críticas, sino que también subrayó las debilidades en la ciberseguridad del sector energético. La intrusión reveló la necesidad urgente de mejorar las defensas cibernéticas y el fortalecimiento de las infraestructuras críticas frente a amenazas sofisticadas.

El incidente de BlackEnergy en Ucrania es un recordatorio de las consecuencias potencialmente devastadoras de los ciberataques en la vida cotidiana y la economía. Destacó la importancia de implementar prácticas de seguridad robustas, incluyendo la formación en ciberseguridad para empleados, la segmentación de redes y el uso de sistemas de detección y respuesta ante intrusiones.

Figura 8

Mensaje malware BlackEnergy



Nota: Imagen de mensaje con macros maliciosas del malware BlackEnergy. Fuente: https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/

3.5.3 Caso LockBit (Italia-2021)

El ataque cibernético a ERG, uno de los principales operadores de energía en Italia, ocurrió en octubre de 2021. Este incidente fue parte de una ola de ciberataques dirigidos a infraestructuras críticas y empresas del sector energético. Los atacantes utilizaron un

ransomware, un tipo de malware que cifra los datos y sistemas de la víctima, exigiendo un rescate para su liberación.

El ransomware, identificado como "LockBit," logró infiltrarse en la red de ERG y afectar sus operaciones. Aunque la compañía no especificó la cantidad de datos comprometidos ni el monto del rescate exigido, el impacto fue significativo, ya que provocó interrupciones en sus actividades operativas. ERG tomó medidas inmediatas para contener el ataque, desconectando varios sistemas y trabajando con expertos en ciberseguridad para evaluar y mitigar el daño.

El ataque a ERG resaltó la vulnerabilidad de las infraestructuras críticas a ciberamenazas y la creciente sofisticación de los ataques de ransomware. Las interrupciones en la cadena de suministro de energía subrayaron la importancia de robustecer las defensas cibernéticas y de tener planes de respuesta ante incidentes bien definidos. También puso de manifiesto la necesidad de colaboración entre el sector público y privado para proteger los sistemas de infraestructura crítica.

Este incidente es parte de una tendencia más amplia de ataques cibernéticos dirigidos a empresas de energía y otras infraestructuras críticas en todo el mundo, subrayando la importancia de la ciberseguridad en un contexto de amenazas cada vez más sofisticadas y frecuentes.

Figura 9

Mensaje de ransomware LockBit

Nota: Imagen de notificación de infección por ransomware LockBit. Fuente: https://securityaffairs.com/120841/cyber-crime/erg-lockbit-2-0-ransomware.html

3.6 Encuestas a personal de CENTROSUR

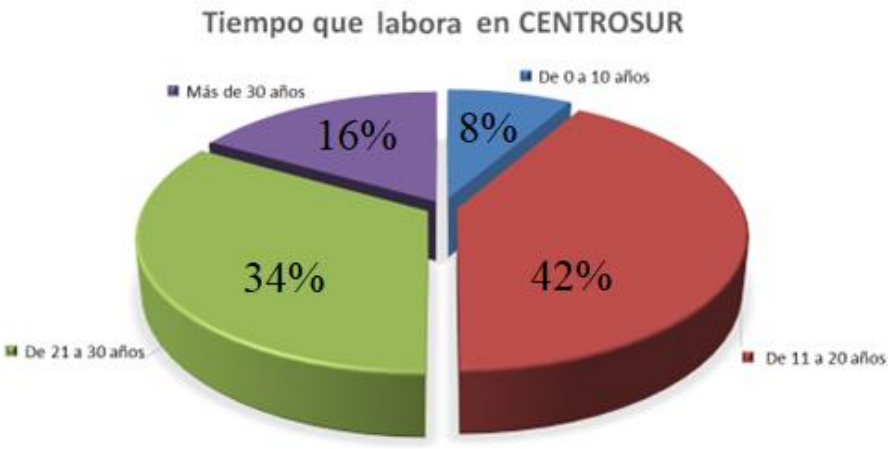
Se realizó una encuesta al personal involucrado en la operación, monitoreo y administración del sistema eléctrico de potencia, lo cual permitió obtener información valiosa sobre su nivel de conocimiento en aspectos básicos de ciberseguridad, el estado actual de la seguridad en las Tecnologías de Operación (TO) y la eficacia en la atención a incidentes de seguridad. Estas encuestas permiten evaluar la capacitación y concienciación del personal respecto a las mejores prácticas de seguridad, identificar posibles brechas en la formación y áreas que requieren mejoras.

Además, proporcionan una visión clara de cómo se perciben y manejan las medidas de seguridad existentes, así como la capacidad del equipo para responder adecuadamente a incidentes de seguridad. Esta información se utilizará para diseñar programas de capacitación más efectivos, mejorar las políticas y procedimientos de seguridad, y fortalecer la disponibilidad y confiabilidad del sistema eléctrico contra amenazas cibernéticas.

La encuesta se realizó a 12 funcionarios del Departamento de Supervisión y Control de la Dirección de Distribución, que incluyen operadores del Sistema Eléctrico de Potencia, Ingenieros Eléctricos y Electrónicos y Superintendentes. La encuesta consiste en un total de 8 preguntas, de las cuales 3 refieren a preguntas de información personal/laboral y 5 preguntas que refieren a conceptos básicos de ciberseguridad en redes TO. (Anexo 1), los resultados se presentan a continuación:

Figura 10

Pregunta N°2 de encuesta: Tiempo que labora en CENTROSUR



Nota: Gráfico que representa la cantidad de funcionarios encuestados por su tiempo de trabajo en la Empresa. Fuente: Autor

El análisis de los resultados a esta pregunta muestra que la totalidad de encuestados cuentan con un tiempo laboral importante dentro de la organización, por lo que la información provista será considerada de gran utilidad en función a su trayectoria y experiencia en el área de tecnologías de operación.

Figura 11

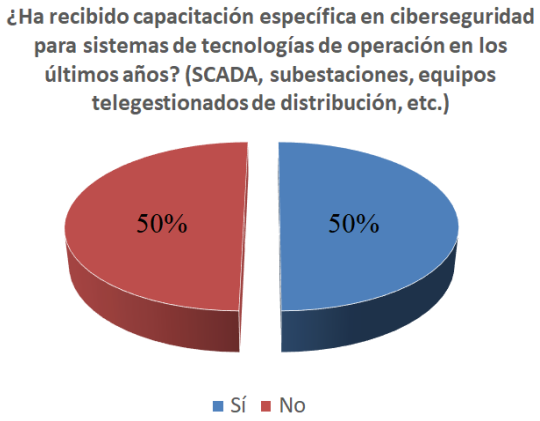
Pregunta N°3 de encuesta: Cargo que ocupa en CENTROSUR

Nota: Gráfico que representa la cantidad de funcionarios encuestados por su cargo en el Departamento de Supervisión y Control de CENTROSUR. Fuente: Autor

Como se puede observar, el 50% de personal encuestado cuenta con cargos administrativos y el 50% con cargos operativos, por lo que los criterios y perspectivas desde ambas aristas, permitirá contar con información equilibrada.

Figura 12

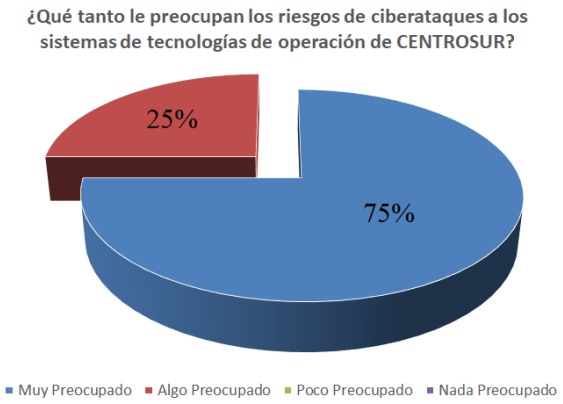
Pregunta N°4 de encuesta: Capacitación en ciberseguridad en sistemas de TO



Nota: Gráfico que representa la cantidad de funcionarios que han recibido capacitación específica en ciberseguridad para sistemas de tecnologías de operación. Fuente: Autor

Figura 13

Pregunta N°5 de encuesta: Preocupación por riesgos de ciberataques a sistemas de TO



Nota: Gráfico que representa la cantidad de funcionarios que han recibido capacitación específica en ciberseguridad para sistemas de tecnologías de operación. Fuente: Autor

Se aprecia que existe gran preocupación por los riesgos de ciberataques que podrían ocurrir en los sistemas de tecnologías de la operación, con un 75% que consideran que tienen gran preocupación por este particular, mientras que el restante 25% se considera “algo preocupado” por una posible ocurrencia de estos.

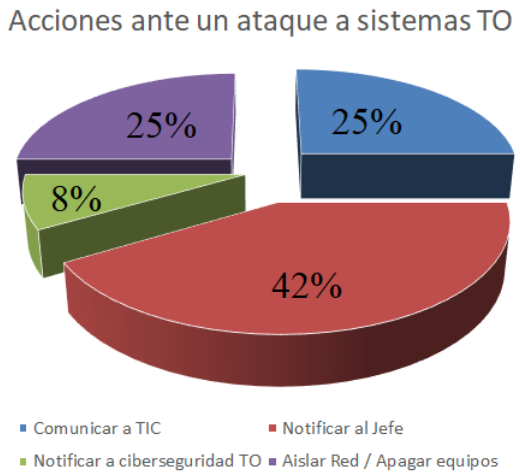
Figura 14

Pregunta N°6 de encuesta: Estrategias y medidas de ciberseguridad en TO

Nota: Gráfico que representa la opinión sobre la efectividad de estrategias y medidas actuales referentes a ciberseguridad en los sistemas de tecnologías de operación. Fuente: Autor

Figura 15

Pregunta N°7 de encuesta: Acciones ante un ciberataque a sistemas de comunicación TO

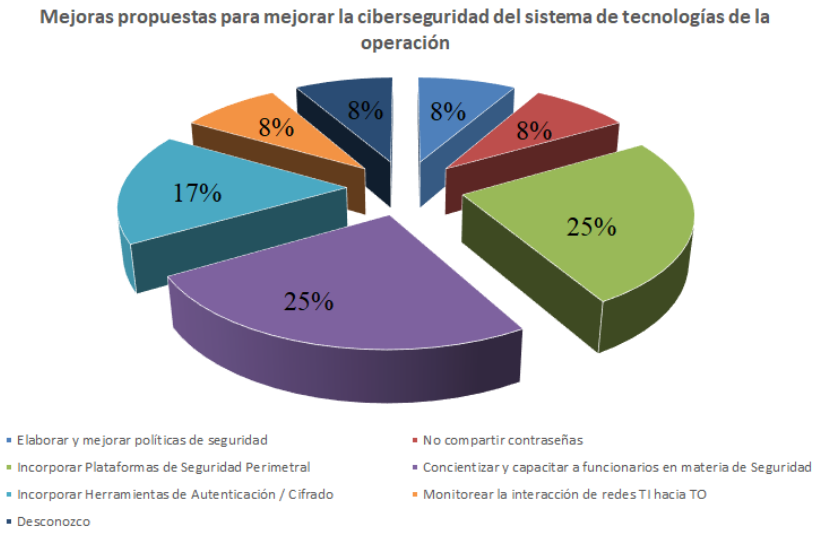


Nota: Gráfico que representa la acciones que realizarían los funcionarios encuestados ante un ciberataque registrado en sistemas de TO. Fuente: Autor

Las respuestas a esta pregunta denotan que no existe claridad en los procedimientos a seguir en caso de existir un ataque de ciberseguridad a los sistemas de TO, se aprecia que tampoco se han establecido directrices para que los funcionarios sepan cómo reaccionar ante un evento. Se puede concluir que esto se debe a que no existe un área ni un funcionario responsable que vele por la seguridad, quien pudiera dar coordinar la atención, tratamiento y respuesta a incidentes de seguridad en su segmento.

Figura 16

Pregunta N°8 de encuesta: Propuesta de mejoras para ciberseguridad para sistemas de TO



Nota: Gráfico que representa la acciones que realizarían los funcionarios encuestados ante un ciberataque registrado en sistemas de TO. Fuente: Autor

Existen varias propuestas de mejora, algunas de carácter técnico a través de la implementación de plataformas de seguridad, ya sea para aseguramiento y control del perímetro u otras que permitan mejorar la autenticación y cifrado de datos. Por otra parte, existen respuestas que orientan a la necesidad de contar con capacitación y concientización a los funcionarios en materia de seguridad y otras de tipo procedimental que sugiere la elaboración de documentación normativa.

3.7 Identificación de las principales motivaciones, vulnerabilidades y amenazas

Una vez que se cuenta con los insumos de información, tanto de los análisis de topologías de red de comunicaciones de TO, niveles de control, encuestas a los funcionarios encargados de la operación y administración del sistema eléctrico y revisados los casos de ciberataques documentados a nivel mundial, se puede concluir que las principales vulnerabilidades y amenazas son las siguientes:

- **No contar con una segmentación de redes basado en el modelo Purdue:** lo que impediría la comunicación entre el tráfico de la red del segmento corporativo (TI) y las redes de TO.
- **Insuficiente infraestructura de ciberseguridad en los segmentos de red de infraestructura crítica**: La incorporación de elementos como *firewalls* de nueva generación, sistema de prevención de intrusos (IPS), microsegmentación de servicios, sistemas Zero Trust, sistemas antimalware, sistemas robustos de autenticación, dificultaría de forma significativa a un atacante ingresar a un sistema, avanzar en su zona de ataque o escalar privilegios.
- **Falta de políticas y gobierno de seguridad:** El contar con procedimientos claros no solo en procesos de ciberseguridad de TO sino en prevención y acciones tempranas ante un evento de ciberseguridad, es vital para cualquier organización.
- **Priorización en la seguridad de TI:** La errónea percepción de que las redes de Tecnología Operacional (TO) no son objetivos atractivos para los ciberatacantes o que estos incidentes de ciberseguridad sólo ocurren en otros países, constituye uno de los errores más graves y peligrosos en el sector. Este pensamiento reduce la urgencia y la prioridad que debería darse a la implementación de medidas de seguridad robustas. Las infraestructuras críticas, como las redes de distribución eléctrica, son objetivos valiosos para actores malintencionados debido a su importancia en la seguridad nacional y su impacto económico y social. Los ciberatacantes buscan constantemente vulnerabilidades en estos sistemas para causar interrupciones operativas, sabotajes, para obtener ganancias financieras o ganar reputación a través del secuestro de información o la paralización de servicios.

- **Desactualización:** En el entorno de tecnologías de operación, prevalece la filosofía de que “lo que funciona no se toca”. Bajo esta premisa, los sistemas operativos y software utilizados se vuelven obsoletos con el paso de los años. Estos sistemas no son parchados ni revisados de manera continua, tampoco se realiza un análisis de vulnerabilidad en los activos, lo que crea un ambiente potencialmente inseguro. La falta de actualizaciones permite que las amenazas y *exploits* permanezcan sin mitigación, exponiendo los sistemas a riesgos de ciberataques, fallos operativos y brechas de seguridad. Esta práctica de mantener sistemas desactualizados versus el avance de métodos y técnicas de ciberataques avanzadas resulta en un escenario donde debe equilibrarse la operación y la seguridad de los sistemas.
- **Desconocimiento y falta de capacitación:** Una de las mayores vulnerabilidades en el entorno de Tecnología Operacional (TO) es el desconocimiento y la falta de capacitación adecuada del personal. Muchos empleados no están plenamente conscientes de las amenazas cibernéticas específicas que enfrentan las infraestructuras críticas ni de las mejores prácticas para mitigarlas. Este déficit de conocimiento puede resultar en la implementación inadecuada de medidas de seguridad, manejo incorrecto de incidentes y una respuesta tardía a las amenazas. La falta de capacitación especializada también significa que el personal no está preparado para utilizar las herramientas de seguridad avanzadas ni para seguir los protocolos de ciberseguridad de manera eficaz. Para abordar esta vulnerabilidad, es imperativo que las organizaciones desarrollen y mantengan planes de capacitación continuos y especializados para el personal, no solo operativo sino también administrativo y de alta gerencia. Estos planes deben incluir formación regular en

ciberseguridad, simulaciones de ataques, y actualizaciones sobre las últimas amenazas y técnicas de defensa. Al invertir en la educación y el entrenamiento del personal, las organizaciones pueden fortalecer significativamente su postura de seguridad, asegurando que todos los empleados estén preparados y cuenten con conocimiento para proteger los sistemas TO contra posibles ciberataques y contribuir a la continuidad operativa de las infraestructuras críticas.

- **Planes de contingencia / Continuidad del negocio**

  Las empresas de distribución, si bien cuentan con un sistema ADMS en alta disponibilidad y un módulo de supervivencia local, no cuentan con redes de comunicación redundantes o de respaldo, alta disponibilidad, copias en tiempo real a través de sistemas de inmutabilidad de datos, lo que podría lograr un menor impacto en la afección de su servicio en caso de un ataque. Tampoco disponen de planes de contingencia o continuidad del negocio para este tipo de eventos.

3.8 Propuestas de ciberseguridad para redes de comunicación de infraestructuras críticas en la distribución eléctrica del Ecuador

3.8.1 Segmentación de la Red

La segmentación de las redes de TI y TO es esencial según las normas ISA99 (actual IEC 62443) debido a varios factores clave que mejoran la seguridad y resiliencia de las infraestructuras críticas. El modelo Purdue, un marco de referencia ampliamente utilizado en la arquitectura de redes industriales, ilustra la importancia de segmentar las redes en niveles jerárquicos separados.

Esta segmentación no solo que separa los activos utilizados en la empresa por los funcionarios administrativos con sus distintas redes cableadas, inalámbricas, uso de aplicativos,

impresoras, teléfonos y demás, sino que también reduce la superficie de ataque al limitar los puntos de acceso que los atacantes pueden explotar, y ayuda a contener la propagación de vulnerabilidades, evitando que una brecha en una parte de la red corporativa se traslade a áreas críticas. Además, permite aplicar políticas de seguridad específicas para las diferentes funciones de las redes de TI y TO, que tienen distintos requisitos y prioridades de seguridad.

Cumplir con los estándares y regulaciones de seguridad cibernética como IEC 62443, no busca mejorar la postura de ciberseguridad general. La segmentación también protege contra amenazas internas, restringiendo el acceso a partes sensibles de la red solo a personal autorizado, y facilita una mejor gestión y control del tráfico de red, asegurando que el tráfico entre segmentos se supervise y controle adecuadamente.

Generalmente la segmentación de redes requiere de la implementación de un *firewall* de perímetro para el segmento de tecnologías de operación, tal como se había comentado anteriormente lo había realizado CENTROSUR en el año 2017. En caso de requerirse conexiones desde redes corporativas a redes TO, se podrá realizar a través de una conexión de tipo Red Virtual Privada (VPN) otorgada por el mismo *firewall* de TO. Cabe indicar que el sistema de VPN que se utiliza por CENTROSUR, está integrado a un directorio activo propio el cual autentica a los usuarios y autoriza el acceso únicamente a quienes formen parte de él. Por otra parte, los funcionarios de cada nivel (N0-N3) tienen acceso VPN únicamente al segmento de red que contempla su ámbito de trabajo, es decir se garantiza que ningún funcionario ajeno al área pueda ingresar a otros segmentos que no le corresponde.

Además de la segmentación de redes, la IEC 62443 sugiere creación de zonas de seguridad. Para redes críticas, se sugiere utilizar infraestructuras de seguridad dedicadas para minimizar el riesgo de propagación de amenazas desde redes menos seguras. Esto incluye no

solo la utilización de un sistema de directorio activo propio que cuenten con políticas de contraseñas robustas, control de periféricos, sino también soluciones de antivirus y antimalware específicas para los componentes del sistema, distinto al antivirus utilizado para redes corporativas.

En CENTROSUR existe la buena práctica de que en las distintas redes LAN de TO, manejan direccionamiento IPv4 estático y, además, ningún puerto de equipo de comunicación (switch) se encuentra activo si no existe una conexión autorizada y configurada para su operación, lo que reduce notablemente la probabilidad de que un equipo ajeno al ámbito empresarial pueda contar con acceso a la red.

3.8.2 Gestión de Acceso y Autenticación

Implementar controles estrictos de acceso basado en roles (RBAC) se refiere a una práctica de seguridad en la que los permisos de acceso a los recursos y datos dentro de una organización se asignan según los roles específicos que los empleados ocupan en la empresa.

Los roles se definen según las funciones, roles y responsabilidades de los empleados, por ejemplo, un administrador de red, un ingeniero de sistemas y un operador de planta tendrán diferentes roles. A cada rol se le asignan permisos específicos que determinan qué recursos y datos puede ver o modificar un usuario con ese rol, asegurando que los empleados solo tengan acceso a la información y a los sistemas necesarios para realizar sus tareas laborales.

Esta práctica ayuda a aplicar el principio del menor privilegio, garantizando que los usuarios no tengan más permisos de los necesarios, lo que reduce el riesgo de acceso no autorizado o de daños accidentales. Administrar permisos de acceso mediante roles también simplifica la gestión, especialmente en organizaciones grandes, ya que los cambios en las

responsabilidades de un empleado pueden manejarse cambiando su rol en lugar de modificar múltiples permisos individuales.

Implementar RBAC también facilita la auditoría y el cumplimiento normativo, proporcionando un marco claro y documentado de cómo se gestionan los accesos y quién tiene acceso a qué recursos, lo cual es esencial para cumplir con las regulaciones de seguridad y privacidad.

Por otra parte, implementar la autenticación de múltiple factor (MFA) para el acceso a sistemas críticos es crucial porque añade una capa adicional de seguridad, requiriendo al menos dos formas de verificación antes de conceder acceso. Esto mejora significativamente la seguridad al reducir el riesgo de acceso no autorizado, incluso si una contraseña es comprometida. Además, MFA protege contra ataques de *phishing* y robo de credenciales, ya que los atacantes necesitarían obtener la segunda forma de autenticación, lo cual es mucho más difícil. También mitiga los riesgos asociados con contraseñas débiles o reutilizadas, ya que una contraseña comprometida no es suficiente para acceder sin el segundo factor.

3.8.3 Gestión de Vulnerabilidades

Establecer procesos regulares para identificar, evaluar y mitigar vulnerabilidades es fundamental para asegurar la protección continua de los sistemas críticos en una organización. Este enfoque proactivo implica la implementación de un ciclo continuo de escaneo y monitoreo de vulnerabilidades para detectar posibles debilidades en el software, hardware y configuraciones de red. Además, es esencial realizar análisis de penetración en redes y sistemas de Tecnologías de Operación (TO).

Estos análisis simulan ataques reales para identificar vulnerabilidades que podrían ser explotadas por atacantes malintencionados. Una vez identificadas, estas vulnerabilidades deben ser evaluadas en términos de su gravedad y el impacto potencial en las operaciones, priorizando aquellas que representan mayores riesgos. La mitigación de vulnerabilidades puede incluir la aplicación de parches y actualizaciones, la reconfiguración de sistemas y la implementación de controles adicionales de seguridad. Este proceso debe ser documentado y revisado regularmente para adaptarse a la evolución de las amenazas y asegurar que se mantengan las mejores prácticas de seguridad.

Al establecer estos procesos regulares y periódicos, incluyendo el *ethical hacking*, las organizaciones pueden reducir significativamente el riesgo de ciberataques, contar con oportunidades de mejora y dar continuidad de sus operaciones críticas. También generar planes de acción para mitigar las amenazas a corto, mediano y largo plazo, en función de su criticidad. Es también recomendable mantener el software y *firmware* actualizado con los últimos parches de seguridad.

3.8.4 Seguridad en el Ciclo de Vida del Sistema

Integrar la ciberseguridad en todas las fases del ciclo de vida del sistema implica considerar la seguridad desde el diseño hasta la operación y el mantenimiento. En la fase de diseño y planificación, se realiza un análisis de riesgos para identificar amenazas y vulnerabilidades, y se desarrolla una arquitectura de seguridad sólida que define zonas y conductos seguros.

Durante la implementación, se aplican controles de seguridad según las mejores prácticas y estándares, y se realizan pruebas para validar la efectividad de las medidas de seguridad. En la fase de operación y mantenimiento, se monitorean activamente los sistemas en busca de posibles

anomalías y se implementan actualizaciones y parches de seguridad de forma regular para hacer frente a las nuevas amenazas emergentes. Este enfoque garantiza que la seguridad sea una prioridad en todas las etapas del ciclo de vida del sistema, proporcionando una protección integral contra las amenazas cibernéticas.

3.8.5 Protección y Respuesta a Incidentes:

Implementar sistemas de detección y respuesta ante intrusiones (IDS/IPS) junto con *firewalls* de nueva generación es esencial para fortalecer la postura de seguridad de una organización contra amenazas cibernéticas. Los *firewalls* actúan como la primera línea de defensa al monitorear y controlar el tráfico de red entrante y saliente, permitiendo o bloqueando el acceso según reglas predefinidas. Combinados con IDS/IPS, que monitorean continuamente el tráfico en busca de actividades sospechosas, se crea una defensa en profundidad que mejora significativamente la capacidad de la organización para detectar y responder a amenazas.

Los IDS identifican y alertan sobre posibles intrusiones, mientras que los IPS pueden tomar medidas proactivas para bloquear o mitigar las amenazas en tiempo real. Al implementar esta combinación de tecnologías, las organizaciones pueden detectar y responder rápidamente a los ataques, minimizando el impacto de las brechas de seguridad y protegiendo la integridad y confidencialidad de sus datos críticos.

Así también, desarrollar y mantener planes de respuesta y recuperación ante incidentes de ciberseguridad resulta crucial para mitigar los impactos negativos de posibles ataques y garantizar la continuidad de las operaciones. Estos planes establecen procedimientos claros y detallados para identificar, contener, erradicar y recuperarse de incidentes cibernéticos, con roles y responsabilidades definidos para el personal involucrado. Además, se incluyen pasos para notificar a las partes interesadas relevantes, coordinar con equipos internos y externos, preservar

la evidencia digital y restaurar los sistemas afectados de manera rápida y segura. Al mantener estos planes actualizados y realizar simulacros periódicos de respuesta a incidentes, las organizaciones pueden mejorar su capacidad para detectar y responder eficazmente a las amenazas cibernéticas, minimizando el tiempo de inactividad y reduciendo el impacto económico y reputacional de los ataques.

3.8.6 Control de Seguridad Física

Es muy importante asegurar que las instalaciones físicas que albergan sistemas críticos estén protegidas contra accesos no autorizados, para garantizar la integridad y la seguridad de los activos y evitar manipulaciones o accesos no autorizados.

Las instalaciones que alojan sistemas críticos, como subestaciones, tableros de control, centros de datos, centros de control, son objetivos principales para los ataques cibernéticos y físicos. Por lo tanto, es necesario implementar medidas de seguridad física o controles a través de autorizaciones para prevenir intrusiones.

En ciertos casos, implica la implementación de sistemas de control de acceso físico, como cerraduras biométricas, tarjetas de acceso a bastidores y sistemas de vigilancia por video, para garantizar que solo el personal autorizado tenga acceso a áreas sensibles y acceda únicamente al área donde necesita realizar su trabajo. Además, se deben establecer procedimientos de verificación de identidad y autorización estrictos para garantizar que solo aquellos con la autorización adecuada puedan ingresar a las instalaciones críticas. En el caso de CENTROSUR, se encuentra vigente el formulario de “Permiso de Ingreso a Subestaciones” (Anexo 2), con el cual se procura guardar un control de los accesos, personal y actividades realizadas en dichas localidades.

Considerando que el Centro de Datos de CENTROSUR, alberga el sistema de SCADA local, también se encuentra vigente el formulario de registro “Solicitud de ingreso Centro de Datos” (Anexo 3), ya que se procura registrar toda actividad realizada en el Data Center.

La seguridad perimetral también juega un papel crucial, con la instalación de cercas, presencia de guardias, personal técnico, barreras físicas y sistemas de detección de intrusos para proteger el perímetro de las instalaciones. La capacitación del personal en conciencia de seguridad física es igualmente importante para garantizar que se sigan los procedimientos de seguridad establecidos y se reporten cualquier actividad sospechosa.

3.8.7 Defensa en Profundidad (Seguridad en Capas)

La defensa en profundidad es una estrategia de ciberseguridad que implementa múltiples capas de defensa a lo largo del sistema para proteger infraestructuras críticas contra una amplia variedad de amenazas. Esta estrategia se basa en la idea de que no existe una única solución que pueda proporcionar una protección completa, por lo que se utilizan diversas medidas de seguridad superpuestas para mitigar los riesgos

Se compone de varias capas, las cuales tienen un segmento específico de defensa y control:

- **Capa de Seguridad de Datos:** Asegura la integridad, confidencialidad y disponibilidad de los datos. Incluye sistemas de respaldo y recuperación de información.

  Medidas: Cifrado de datos en tránsito y en reposo, políticas de respaldo y recuperación de datos, gestión de derechos de acceso, y herramientas de prevención de pérdida de datos (DLP).

- **Capa de Seguridad de las Aplicaciones:** Protege las aplicaciones y software utilizados dentro de la infraestructura.

  Medidas: *Firewalls* de aplicaciones, escaneo de vulnerabilidades, prácticas de desarrollo seguro, pruebas de penetración, políticas de gestión de acceso y autenticación de múltiple factor.

- **Capa de Seguridad de los Equipos:** Asegura los dispositivos y equipos que forman parte de la red.

  Medidas: Antivirus y antimalware, gestión de parches y actualizaciones, configuraciones seguras, control de acceso a dispositivos, y cifrado de discos duros. Inclusive se puede considerar la incorporación de un sistema de IAM (Identity Access managemente) o PAM (privileged access management) para la autenticación y supervisión centralizada de los accesos a los equipos que forman parte del sistema de infraestructura crítica y grabar en archivos de video las sesiones de los ingresos y modificaciones en dichos equipos.

- **Capa de Seguridad de Red:** Protege la infraestructura interna de la red, segmentando y controlando el tráfico dentro de la red.

  Medidas: Segmentación de red y VLANs, routers y switches debidamente asegurados y controles de acceso, uso de VPNs para comunicaciones remotas, monitoreo de tráfico de red, y protocolos seguros de comunicación (como SSL/TLS). Se sugiere también que en los dispositivos con sistema operativo Windows (tales como concentradores CMX, SAS, DAS, directorio activo, consolas, estaciones de trabajo de operadores, etc.), se deshabilite el protocolo SMB (*Server Message Block*) en sus versiones 1 y 2 debido a que estas versiones han sido muy utilizadas para la propagación de *ransomware* dentro

de los equipos interconectados en el segmento de red. Si bien SMB v3 cuenta con algunas vulnerabilidades conocidas como CVE-2020-0796 (SMBleed/SMBGhost), CVE-2022-32230, CVE-2020-1206 aún se considera la versión más segura y siendo la versión más actual de este protocolo, se recomienda que en estos entornos se utilice únicamente SMB v3.

- **Capa Seguridad Perimetral:** Esta capa es la primera línea de defensa contra amenazas externas.

  Medidas: *Firewall*s perimetrales, sistemas de detección y prevención de intrusiones (IDS/IPS), gateways de seguridad y filtrado de tráfico.

- **Capa de Seguridad Física:** Protege el acceso físico a las instalaciones y equipos.

  Medidas: Control de acceso mediante tarjetas de identificación, vigilancia con cámaras de seguridad, guardias de seguridad, cerraduras biométricas y alarmas contra intrusiones.

- **Capa de Normas y Procedimientos:** Incluye las políticas, normas y procedimientos que guían el comportamiento y las acciones del personal en relación con la seguridad.

  Medidas: Desarrollo y mantenimiento de políticas de seguridad, capacitación y concienciación de empleados, procedimientos de respuesta a incidentes, auditorías y revisiones regulares de seguridad, cumplimiento de normativas y estándares de la industria.

Figura 17

Defensa en profundidad

Nota: Descripción de capas de defensa en profundidad. Fuente: https://www.stormshield.com/es/ressourcescenter/iec-62443-el-concepto-de-defensa-en-profundidad/

3.8.8 Mejoras en Comunicaciones y Seguridad

La modernización de las infraestructuras de comunicaciones y seguridad en las subestaciones eléctricas es una prioridad para las empresas del sector, especialmente en entornos cada vez más digitales e interconectados. La inclusión de enlaces redundantes en la red de comunicaciones garantiza la disponibilidad continua de los servicios, minimizando los tiempos de inactividad y aumentando la confiabilidad operativa.

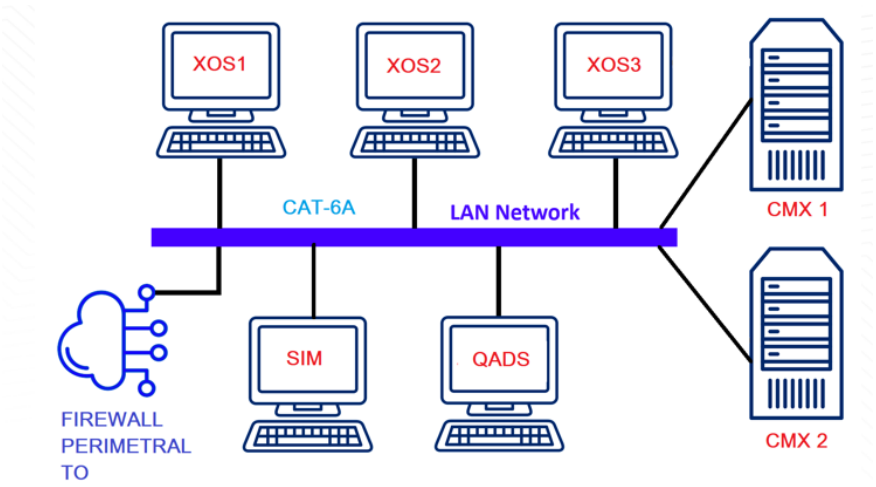
Considerar la implementación de *firewalls* de nueva generación en cada una de las subestaciones, lo cual proporcionaría una defensa robusta contra amenazas cibernéticas en cada localidad, protegiendo los sistemas críticos de ataques malintencionados, garantizando un aseguramiento en el tráfico de red perimetral.

La adopción de tecnologías como SD-WAN en las subestaciones introduce una capa adicional de conexión y seguridad al permitir la diversificación de los proveedores de servicios, lo que garantiza una conectividad confiable incluso en caso de falla de un proveedor. Estas medidas combinadas no solo fortalecen la infraestructura de comunicaciones y seguridad, sino que también mejoran notablemente la confiabilidad y disponibilidad del suministro eléctrico.

Considerando que la disponibilidad es un pilar fundamental de la seguridad, se propone que las redes LAN de SCADA local cuenten con alta disponibilidad (clúster) de *next generation firewall* perimetral de TO, redundancia de tipo activo-activo para red LAN lo cual permitirá incrementar notablemente la disponibilidad y confiabilidad del sistema.

Figura 18

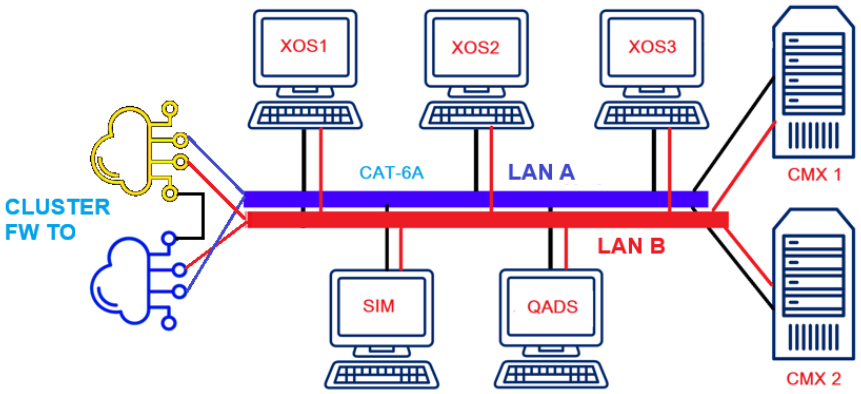
Red LAN SCADA local actual CENTROSUR



Nota: Diagrama de red LAN SCADA local CENTROSUR. Fuente: Empresa Eléctrica Regional Centro Sur C.A.

Figura 19

Red LAN SCADA local propuesta para CENTROSUR

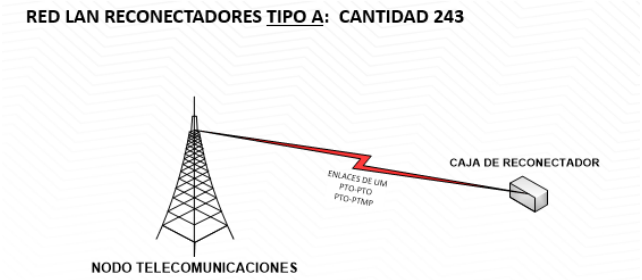


Nota: Diagrama de red LAN SCADA local propuesto. Fuente: Empresa Eléctrica Regional Centro Sur C.A. y Autor

CENTROSUR ha clasificado las redes LAN de reconectadores en “Tipo A” los cuales cuentan con un enlace de última milla desde el repetidor hacia la caja de reconectador, de los cuales existen instalados 243 y los “Tipo B” que cuentan con redundancia de enlaces, los cuales convergen en una caja de equipos de telecomunicación, para posteriormente conectarse a la caja del reconectador a través de puerto Ethernet, de este tipo existen instalados 67.

Figura 20

Enlaces a Reconectadores Tipo A



Nota: Red LAN reconectadores Tipo A. Fuente: Empresa Eléctrica Regional Centro Sur C.A.

Figura 21

Enlaces a Reconectadores Tipo B

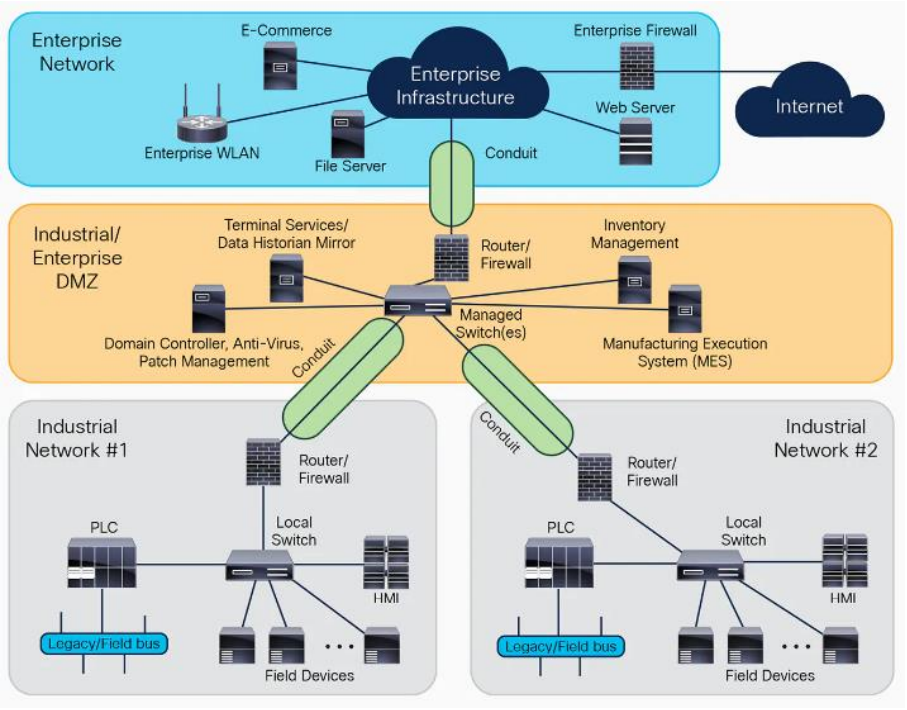
Nota: Red LAN reconectadores Tipo B. Fuente: GEmpresa Eléctrica Regional Centro Sur C.A.

Considerando el modelo propuesto por Cisco® en referencia a la norma IEC 62443, mismo que detalla a continuación cómo debe coexistir y a la vez proteger los segmentos de redes corporativos y de tecnologías de operación, el cual indica “Según el estándar, una zona es un conjunto de activos unidos física y/o funcionalmente que tienen requisitos de seguridad comunes. Estas zonas se definen en base a los modelos físicos y funcionales de la arquitectura de control del sistema industrial. Todos los activos en un IACS deben estar ubicados en una zona.

Los conductos apoyan la comunicación entre zonas. Un conducto es una agrupación lógica de canales de comunicación entre dos o más zonas.”

Figura 22

Redes TI - TO según norma IEC 62443



Nota: Descripción de coexistencia de redes TI y TO según norma IEC 62443. Fuente: https://www.cisco.com/c/dam/en/us/products/collateral/security/isaiec-62443-3-3-wp.docx/_jcr_content/renditions/isaiec-62443-3-3-wp_1.png

Se recomienda que todos los equipos de conectividad de red como routers y switches, cuenten con la configuración de Port-Security el cual permite garantizar que la dirección MAC de cada dispositivo sea la única que puede conectarse a dicho puerto. Así también, mantener deshabilitados los puertos que no se encuentran en uso y sean activados solo bajo demanda según los requerimientos o necesidades de las áreas correspondientes.

3.8.9 Topología de seguridad y telecomunicaciones propuesta

En este contexto, se propone la siguiente topología para las redes de telecomunicaciones del sistema eléctrico de CENTROSUR, en el cual se puede observar la configuración en clúster

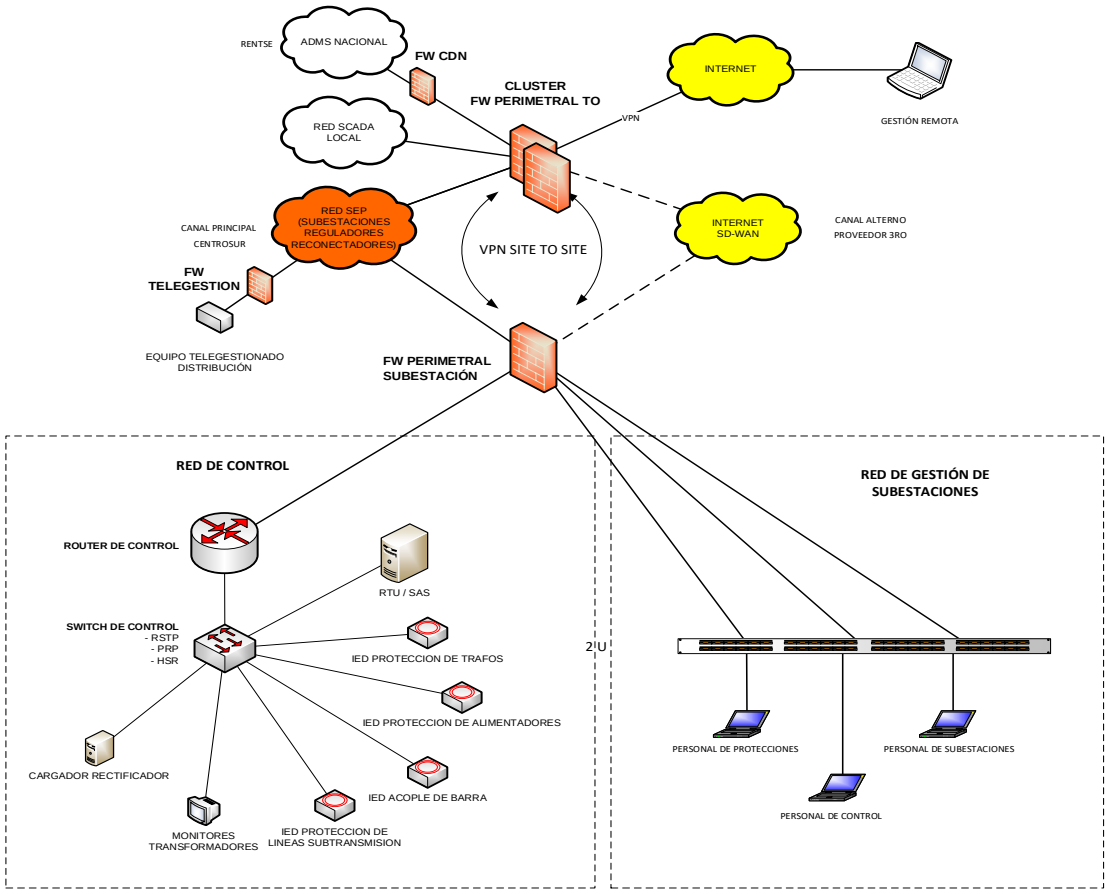
del *firewall* perimetral de TO, el cual cuenta con características para conexiones remotas a través de VPN, este clúster protegerá de forma perimetral a las redes de TO de subestaciones, a los sistemas de comunicación de reconectadores y segmento ADMS. Se contará también con un equipo *firewall* de nueva generación por cada subestación el cual incluirá al menos módulos de IPS, antimalware y capacidad SD-WAN para contar con conectividad a través del canal del anillo IP/MLPS de CENTROSUR y servicio de un tercero. Tanto el clúster de *firewalls* de TO como el *firewall* de subestación estarán conectados a través de una VPN sitio-a-sitio, de manera de asegurar tráfico encriptado entre los 2 segmentos.

El segmento del Sistema Eléctrico de Potencia (SEP), contempla las redes de subestaciones y reconectadores. Se debe tomar en cuenta que todos estos dispositivos están interconectados a través de una red tipo *MESH* a través de enrutamiento VRF (Virtual Routing and Forwarding) específica para este fin, que permite la comunicación entre todos estos segmentos. Por lo tanto, se propone que cada subestación cuente con un *firewall* de perímetro y del mismo modo cada reconectador, de manera que el tráfico pueda tener un elemento de control y protección.

Al momento existe un solo switch LAN en cada subestación, el cual mantiene la interconexión entre los dispositivos y permite la operación de los sistemas de TO. Sin embargo, se sugiere que se incorpore un switch de gestión de manera que ante un requerimiento de configuración o modificación en cualquier equipo de comunicación y control de subestación (IED, RTU, SAS, DAS), no tenga conexión directa con un computador sino a través de un switch, esto con la finalidad de evitar infección o propagación de malware en caso de sistemas operativos Windows (SAS y DAS especialmente).

Figura 23

Propuesta de arquitectura de red basada en IEC 62443 y mejoras en disponibilidad



Nota: Propuesta de arquitectura de red de TO basada en estándar IEC 62443. Fuente: Autor

Bajo este criterio, se propone incrementar la cantidad de equipos de seguridad perimetral de TO, incluir equipamiento de seguridad perimetral en subestaciones y equipos telegestionados de distribución (reconectadores).

Tabla 2

Inventario de activos actuales y proyectados

Tipo de Red	Firewall	Router	Switch	Caja Telecom
Red LAN SCADA	1 existente + 1 proyectado	0	2 existentes	0
Red LAN Subestaciones	19 proyectados	19 existentes	76 existentes	0
Red LAN Reconectadores	310 proyectados	0	67 existentes	67 existentes

Nota: Inventario de activos de red y seguridad actuales y proyectados. Fuente: Autor

3.8.10 Formación y Concienciación

La capacitación del personal es una de las estrategias más efectivas para mejorar la ciberseguridad en redes de infraestructura crítica, por lo que resulta esencial que todos los empleados, desde el personal operativo hasta la alta gerencia se encuentren bien informados sobre las prácticas de ciberseguridad. Esto incluye proporcionar formación regular y actualizada sobre cómo identificar y responder a posibles amenazas cibernéticas.

Los programas de capacitación deben cubrir una variedad de temas, como el reconocimiento de correos electrónicos de *phishing*, el uso de contraseñas seguras, la importancia de mantener el software actualizado, la autenticación y las mejores prácticas para la gestión de accesos y permisos. Además, el personal debe ser entrenado para detectar comportamientos y reportar actividades inusuales en la red que podrían indicar una brecha de

seguridad, como accesos no autorizados o actividad anómala en los sistemas. Simulaciones de ataques y ejercicios de respuesta a incidentes pueden ser herramientas útiles para preparar al personal a actuar de manera efectiva en caso de un ataque real.

La creación de una cultura de seguridad dentro de la organización, donde cada empleado comprende su papel en la protección de los sistemas de infraestructuras críticas, es fundamental para minimizar los riesgos y contar con procedimientos y acciones frente a posibles ciberataques. Fomentar una cultura de seguridad dentro de la organización.

3.8.11 Políticas y Procedimientos

Desarrollar y mantener políticas y procedimientos claros de ciberseguridad es esencial para proteger las redes corporativas de amenazas cibernéticas. Estas políticas deben definir las directrices y prácticas que todos los empleados deben seguir para asegurar la integridad, disponibilidad y confidencialidad de los sistemas. Es crucial que estas políticas sean revisadas y actualizadas regularmente para reflejar las mejores prácticas y adaptarse a los cambios en el entorno de amenazas. La revisión periódica permite incorporar nuevas técnicas de defensa, abordar vulnerabilidades emergentes y asegurar el cumplimiento con las normativas vigentes.

Las empresas de distribución eléctrica, al igual que todas las entidades que presten servicios públicos, según el Acuerdo Ministerial No. -0003-2024 inscrito en el registro oficial el 1 de marzo de 2024, deben cumplir con la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) en su tercera versión. Además, las normas de control interno de la Contraloría General del Estado emitidas en febrero de 2023, a través del numeral 410 disponen la creación de los roles de Oficial de Seguridad de la Información (CISO, por sus siglas en inglés) y del Comité de Seguridad de la Información, lo cual es fundamental para una gestión efectiva de la ciberseguridad.

El CISO tiene la responsabilidad de generar, regular y controlar la implementación de políticas de ciberseguridad que abarquen tanto la tecnología de la información (TI) como la tecnología operativa (TO), así como la seguridad de la información empresarial en su totalidad. Este rol centralizado permite una visión unificada de las amenazas y la seguridad, asegurando que todas las áreas de la organización sigan un enfoque coherente y coordinado. El CISO también juega un papel crucial en la formación y concienciación del personal, promoviendo una cultura de seguridad que es vital para la protección de las infraestructuras críticas.

La existencia de un CISO dedicado facilita la respuesta rápida y eficiente a incidentes de seguridad, la gestión de riesgos y la implementación de estrategias de recuperación ante desastres, garantizando que la organización esté siempre preparada para enfrentar los desafíos de la ciberseguridad en el entorno dinámico de las redes de infraestructura crítica.

Otro aspecto clave de éxito para las instituciones es determinar el alcance y delimitar de forma clara las competencias de ciberseguridad de TI y de TO, si bien pueden ser equipos de apoyo, la responsabilidad sobre el tratamiento de incidentes y eventos deben ser asumidos por el área correspondiente.

El plan estratégico 2022-2025 de CENTROSUR indica: "..*En la Gestión Tecnológica, se ha trabajado en la implementación de la norma ISO 27001 de Seguridad de la Información, para lo cual en el año 2021 se llevó a cabo la contratación de servicios para la revisión y actualización del Sistema de Gestión de la Información, basado en dicha norma, lo cual permitió contar con un plan de acción detallado para mejorar y fortalecer este sistema, encaminado a obtener la certificación correspondiente*..", es decir actualmente la Empresa ha considerado incorporar estándares de seguridad de la información a la organización, de manera que a través de la adopción de normativas y un marco de gobernanza en

seguridad de la información, en primera instancia ISO 27001 y la posterior la incorporación de un estándar IEC 62443 con lo propuesto a través del presente análisis, se cuente con una cultura de seguridad de la información y ciberseguridad corporativa holística.

3.8.12 Monitorización y registro de lecciones aprendidas

La monitorización y el registro de lecciones aprendidas son componentes necesarios en la estrategia de ciberseguridad de cualquier red de infraestructuras críticas. La monitorización continua de los sistemas permite la detección temprana de actividades inusuales o potencialmente maliciosas, lo que facilita una respuesta rápida y eficaz ante incidentes de seguridad. Implementar sistemas avanzados de detección de intrusiones y herramientas de análisis de tráfico de red es esencial para identificar patrones y comportamientos que puedan indicar una brecha de seguridad.

Además, el registro detallado de todos los eventos y respuestas ante incidentes proporciona una valiosa base de datos de información que puede ser analizada para extraer lecciones aprendidas. Este análisis retrospectivo permite identificar debilidades en los sistemas y procedimientos, así como mejorar las estrategias de defensa y respuesta. Documentar estas lecciones y actualizarlas continuamente asegura que la organización evolucione y fortalezca sus defensas contra amenazas futuras. Al compartir estas lecciones aprendidas con todo el personal, se fomenta una cultura de mejora continua y se incrementa la capacidad colectiva de enfrentar y mitigar riesgos de ciberseguridad en las redes de infraestructuras críticas.

Se recomienda contar con un servicio de SOC (Security Operations Center) o CSIRT (Computer Security Incident Response Team) especializado en redes TO, para el monitoreo y la respuesta de incidentes de seguridad en redes de infraestructuras críticas, ya que ofrecen monitoreo continuo 24/7, detección avanzada de amenazas mediante inteligencia artificial,

respuesta rápida y efectiva a incidentes, análisis forense detallado, y consultoría experta, todo ello enfocado en asegurar la protección de los sistemas de TO, adaptándose a las necesidades específicas y mejoras de las empresas.

Conclusiones

- Una vez analizada la topología y arquitectura de red de tecnologías de la operación de CENTROSUR, las encuestas a sus funcionarios y análisis de ciberataques documentados a nivel mundial se han identificado los activos de TO que deben ser sujetos a un análisis de riesgos para su categorización y tratamiento.
- Se ha propuesto un plan integral técnico – operativo – administrativo, basado en normas internacionales de seguridad de la información y ciberseguridad de ambientes industriales, mismas que son puestas a consideración para su aplicación en empresas de distribución eléctrica de Ecuador.
- Para asegurar la protección de las redes de Tecnología Operacional (TO) en el contexto de la distribución eléctrica en Ecuador, es fundamental proponer estrategias que fomenten una cultura sólida de ciberseguridad.
- Las empresas de distribución eléctrica del Ecuador carecen de madurez en aspectos de ciberseguridad de TO, pues no aplican normativas, estándares, y tampoco cuentan con planes de capacitación y personal calificado para la atención de vulnerabilidades de estos sistemas.
- El presente trabajo es aplicable para cualquier empresa eléctrica del país, ya que comparten arquitecturas similares y se conectan a un único servicio nacional ADMS.

Recomendaciones

- Aunque el presente estudio abarca aspectos de inversión tecnológica, se sugiere a las empresas eléctricas de distribución analizar la factibilidad de la aplicación de la guía propuesta, de modo que se puedan reducir las brechas de seguridad conforme a sus presupuestos y necesidades.
- Las empresas de distribución del Ecuador, en estricto cumplimiento normativo deben incorporar a un oficial de seguridad, mismo que está contemplado en el numeral 410-01 del ACUERDO No. 004-CG-2023 “Normas de control interno (NCI)” de la Contraloría General del Estado y en el acuerdo ministerial N°MINTEL-MINTEL-0003-2024 (EGSI v3), lo cual permitirá contar con un área de gobierno de seguridad de la información empresarial, quienes normen y regulen a nivel corporativo el cumplimiento íntegro de las áreas de ciberseguridad TI / TO y seguridad de la información.
- Al igual que en tecnologías de la información, resulta indispensable contar con un área dedicada a la ciberseguridad de TO, la misma que incluya personal con experiencia y conocimiento tanto en seguridad informática como en sistemas de comunicación de infraestructuras críticas.
- La incorporación de un gran número de elementos de red y seguridad, deberán no solo ser evaluados en aspectos económicos sino operativos, pues la instalación, configuración, puesta en marcha, actualización de inventarios, operación y mantenimiento, deberán estar correctamente dimensionados a nivel de recursos. Por otra parte, puede considerarse alternativas de servicios gestionados a través de acuerdos de nivel de servicio (SLA) con terceros.

- Resulta indispensable desarrollar planes de capacitación continuos y especializados que incluyan formación regular en ciberseguridad, simulaciones de ataques y actualizaciones sobre las amenazas y técnicas de defensa.

Bibliografía

Alcaraz, C., Fernández, G., Román, R., Balastegui, Á., & López, J. (2008). *Gestión Segura de Redes SCADA*. https://www.nics.uma.es/publications

Anabalón, J. *, & Donders, E. (2014). *Seguridad en Sistemas SCADA un Acercamiento Práctico a Través de EH e ISO 27001:2005*.

Abreu Cañamares, D. (2018). *Universidad Autónoma De Madrid Trabajo Fin De Grado*.

Bello, R., Andrés, W., Medina Becerra, Andrés, F., Lara, M., & Alonso, J. (2020). Metodologías de evaluación del riesgo en ciberseguridad aplicadas a sistemas SCADA para compañías eléctricas Methodologies for cyber security risk assessment applied to SCADA systems for power companies Contenido. In *ISSN* (Vol. 41).

Pascual, C. (2020). *Desarrollo de un sistema eficiente de análisis de tráfico Modbus TCP para la detección de anomalías en redes SCADA*

CISCO. (2022). ISA/IEC-62443-3-3: *What is it and how to comply?*. https://www.cisco.com/c/en/us/products/collateral/security/isaiec-62443-3-3-wp.html

Inprotech. (2023) GUÍA DE SEGURIDAD OT NIST SP 800-82: INTRODUCCIÓN Y TERCERA REVISIÓN. https://inprotech.es/guia-de-seguridad-ot-nist-sp-800-82/

Franceschett, A. L., de Souza, P. R., de Barros, F. L. P., & de Carvalho, V. R. (2019, September). *A holistic approach-How to achieve the state-of-art in cybersecurity for a secondary distribution automation energy system applying the IEC 62443 standard*. In 2019 IEEE PES Innovative Smart Grid Technologies Conference-Latin America (ISGT Latin America) (pp. 1-5). IEEE.

Rintala, J., Loukkalahti, M., Musunuri, S., Haapaniemi, J., & Hampel, C. (2023, June). *Is the cybersecurity standard IEC 62443 applicable to distribution substations?*. In 27th International Conference on Electricity Distribution (CIRED 2023) (Vol. 2023, pp. 1554-1558). IET.

Kanabar, P. M., Kanabar, M. G., El-Khattam, W., Sidhu, T. S., & Shami, A. (2009, July). *Evaluation of communication technologies for IEC 61850 based distribution automation system with distributed energy resources*. 2009 IEEE Power & Energy Society General Meeting (pp. 1-8). IEEE.

E-Virtus. (2021). Modelo de Purdue y los Principios de Ciberseguridad Industrial. https://blog.e-virtus.com/posts/modulo_de_purdue_y_los_principios_de_seguridad_industrial/

ANEXOS

Anexo 1 – Formato de Encuesta

Ciberseguridad en redes de Tecnologías de Operación

Esta encuesta busca recopilar información de la percepción y conocimiento de ciberseguridad en ambientes de Tecnologías de Operación (TO). El objetivo de este análisis servirá como insumo para un trabajo de tesis de posgrado, la cual busca proponer directrices de ciberseguridad para redes de infraestructuras críticas de las empresas distribuidoras del País.
Gracias por su gran aporte!

* Indica que la pregunta es obligatoria

1. **1. Nombres Completos** *

_____

2. **2. Cargo** *

_____

3. **3. Tiempo que labora en CENTROSUR** *

_____

4. **4. ¿Ha recibido capacitación específica en ciberseguridad para sistemas de tecnologías de operación en los últimos años? (SCADA, subestaciones, equipos telegestionados de distribución, etc.)** *

Marca solo un óvalo.

- ◯ Sí
- ◯ No

5. **5. ¿Qué tanto le preocupan los riesgos de ciberataques a los sistemas de tecnologías de operación de CENTROSUR?** *

Marca solo un óvalo.

- ◯ Muy Preocupado
- ◯ Algo Preocupado
- ◯ Poco Preocupado
- ◯ Nada Preocupado

6. **6. ¿Considera que las estrategias y medidas de ciberseguridad implementadas en los sistemas de tecnologías de operación, son adecuados para proteger contra ciberataques?** *

Marca solo un óvalo.

- ◯ Sí, son completamente adecuados
- ◯ Son adecuados, pero podrían mejorarse
- ◯ No son adecuados
- ◯ Desconozco

7. **7. En caso de experimentar o evidenciar un ciberataque a redes o sistemas de tecnologías de operación, ¿cuál sería su primera acción? (Respuesta abierta)** *

_____

_____

_____

_____

_____

Anexo 2 – Formato de Acceso a Subestaciones

PERMISO INGRESO SUBESTACIONES				
Fecha de Solicitud:			**Período**	
Solicitante:			**Desde:**	**Hora:**
Subestación N°			**Hasta:**	
Subestación N°				
Subestación N°				

Descripción de Actividad	

Área de acceso:							
Patio de maniobras		**Cuarto de control**		**Comunicaciones**		**Instalaciones generales**	

Personas:				**Vehículos:**	
Nombre		**Cédula**		**Tipo**	**Placa**

Firmas:			
Solicitante:		**Autorizador:**	

Anexo 3 – Formato solicitud ingreso centro de datos

CENTROSUR	SOLICITUD DE INGRESO CENTRO DE DATOS	R-DITIC-558

		Fecha elaboración solicitud: (dd/mm/aaaa)	
Fecha para Ingreso: (dd/mm/aaaa)		Hora para ingreso: (hh:mm)	
Tiempo Aproximado de Actividad: (En Horas)		Nro. De Consignación relacionada:	
Nombre y Apellido del Responsable:		Área Solicitante:	

Personas Adicionales que acompañan:

Nombre y Apellido	Área / Empresa	Relación	Firma

Detalle de actividades a realizar

_____ _____

Funcionario Responsable **Jefe Inmediato**

Nombre y Apellido: Nombre y Apellido:

_____

Funcionario Centro de Datos que Autoriza

Nombre y Apellido: