UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

INFORME FINAL DEL TRABAJO DE INTEGRACIÓN CURRICULAR,

MODALIDAD PROYECTO DE INVESTIGACIÓN

TEMA:

"PLAN DE SEPARACIÓN DE LOS SERVICIOS DE RED IT Y OT ENFOCADOS A LA CIBERSEGURIDAD Y EFICIENCIA OPERATIVA EN LA EMPRESA ELÉCTRICA REGIONAL NORTE S.A. EMELNORTE"

Trabajo de Titulación previo a la obtención del Título de Magíster en Computación con Mención en Seguridad Informática

Línea de investigación: Ciberseguridad (seguridad cibernética)

AUTOR:

ING. OREJUELA PÉREZ ANA CRISTINA

DIRECTOR:

MSC. GUEVARA VEGA VICENTE ALEXANDER

IBARRA – ECUADOR

2025

CERTIFICACIÓN DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Ibarra, 24 de julio de 2025

MSc. Vicente Alexander Guevara Vega

DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICA:

Haber revisado el presente informe final del trabajo de Integración Curricular, mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en constancia, autorizo su presentación para los fines legales pertinentes.

.....

MSc. Vicente Alexander Guevara Vega

C.C.: 1002334827

UNIVERSIDAD TÉCNICA DEL NORTE

Acreditada Resolución Nro. 173-SE-33-CACES-2020

DIRECCIÓN DE BIBLIOTECA

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD	100256476-1		
APELLIDOS Y NOMBRES	OREJUELA PÉREZ ANA CRISTINA		
DIRECCIÓN	RÍO CHIMBO Y ESPINOZA DE LOS MONTEROS		
EMAIL	acorejuelap@utn.edu.ec		
TELÉFONO FIJO	N/A	**TELÉFONO MÓVIL:**	0999027678

DATOS DE LA OBRA	
TÍTULO:	PLAN DE SEPARACIÓN DE LOS SERVICIOS DE RED IT Y OT ENFOCADOS A LA CIBERSEGURIDAD Y EFICIENCIA OPERATIVA EN LA EMPRESA ELÉCTRICA REGIONAL NORTE S.A. EMELNORTE
AUTOR (ES):	OREJUELA PÉREZ ANA CRISTINA
FECHA: DD/MM/AAAA	24/07/2025
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA DE POSGRADO	☐ **GRADO** ☒ **POSGRADO**
TITULO POR EL QUE OPTA	MAGISTER EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA
TUTOR	MSC. GUEVARA VEGA VICENTE ALEXANDER

2. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 24 días del mes de julio del 2025

EL AUTOR:

.....

Ana Cristina Orejuela Pérez

Dedicatoria

Dedico esta tesis a mi familia, por ser el refugio en mis momentos de incertidumbre y la fortaleza en cada desafío. En especial a mi madre, cuyo amor incondicional, sacrificio y apoyo inquebrantable me han acompañado en cada paso de este camino. Su dedicación y confianza en mí han sido la base sobre la que he construido este logro, y por ello le estaré eternamente agradecida. Sin su amor y respaldo, este camino habría sido mucho más difícil.

A mi hija, mi mayor inspiración y motivo de lucha. Su existencia da sentido a cada esfuerzo y me recuerda que los sueños se alcanzan con dedicación y perseverancia. Este logro es para ella, con la esperanza de que siempre persiga sus metas con valentía y determinación.

A los docentes de la Universidad Técnica del Norte, cuya dedicación y compromiso con la enseñanza han sido fundamentales en mi formación. Su guía ha dejado una huella imborrable en mi desarrollo académico y profesional, por lo que les expreso mi más sincero agradecimiento.

Con amor y gratitud eterna, este trabajo es para ustedes.

Índice de Contenido

Índice General

Índice de Tablas

Índice de Figuras

Resumen

El diseño actual de las redes de Tecnología de la Información (IT) y Tecnología Operacional (OT) en la Empresa Eléctrica Regional Norte S.A. EMELNORTE se enfocó en mejorar la eficiencia y la interoperabilidad de los sistemas, sin embargo, esta integración ha incrementado el riesgo de ciberataques, ya que una vulnerabilidad en la red IT podría comprometer la seguridad de la red OT, afectando la infraestructura crítica de la empresa. Para mitigar estos riesgos, se propone un plan de separación de los servicios de red IT y OT enfocados en la ciberseguridad y eficiencia operativa en la empresa EMELNORTE, estableciendo un modelo de segmentación de red que minimice la exposición a amenazas externas y reduzca la superficie de ataque sin afectar la operatividad de los sistemas, para lo cual se aplicará el modelo Purdue, mismo que es recomendado como estándar de mejores prácticas en el sector eléctrico y es referente en su adopción en la segmentación de redes industriales. La presente investigación se realizó con un enfoque cuantitativo, utilizando encuestas a 7 participantes de EMELNORTE. La selección de participantes fue por muestreo intencional, buscando una diversidad técnica. El análisis de datos se llevó a cabo de forma cuantitativa, identificando riesgo de ataque y patrones en las recomendaciones de los participantes, se han considerado las recomendaciones de entes de control en materia de ciberseguridad industrial y protección de infraestructuras críticas. La separación de redes mediante estrategias como zonas de seguridad y segmentación basada en firewalls por capas lo que reduce significativamente los riesgos de ciberseguridad y además evidencia que una segmentación adecuada no solo mejora la seguridad, sino que también optimiza el desempeño operativo, facilitando la gestión y monitoreo de los sistemas IT y OT de manera independiente, lo que permitirá fortalecer la resiliencia de EMELNORTE ante posibles ciberataques y asegurar la continuidad de los servicios eléctricos y la estabilidad de su infraestructura crítica.

Palabras clave: Ciberseguridad, segmentación de redes, modelo Purdue, IT y OT, infraestructuras críticas.

Abstract

The current design of the Information Technology (IT) and Operational Technology (OT) networks at Empresa Eléctrica Regional Norte S.A. (EMELNORTE) was aimed at enhancing system efficiency and interoperability. However, this integration has increased the risk of cyberattacks, as a vulnerability in the IT network could compromise the OT network's security, potentially affecting the company's critical infrastructure. To mitigate these risks, a network separation plan for IT and OT services is proposed, focusing on cybersecurity and operational efficiency at EMELNORTE. This plan involves the implementation of a network segmentation model that minimizes exposure to external threats and reduces the attack surface without impacting system operability. The Purdue Model will be applied, as it is recommended as a best-practice standard in the electric sector and serves as a key reference for industrial network segmentation. This research was conducted using a quantitative approach, employing surveys with seven EMELNORTE participants. Participants were selected through purposive sampling to ensure technical diversity. Data analysis was carried out quantitatively, identifying attack risks and common patterns in the participants' recommendations. Additionally, guidelines from regulatory bodies in the field of industrial cybersecurity and critical infrastructure protection were considered. Network separation through strategies such as security zones and multi-layered firewall-based segmentation significantly reduces cybersecurity risks. Furthermore, proper segmentation not only improves security but also enhances operational performance by enabling independent management and monitoring of IT and OT systems. This approach will strengthen EMELNORTE's resilience against potential cyberattacks and ensure continuity of electric services and the stability of its critical infrastructure.

Keywords: Cybersecurity, network segmentation, Purdue model, IT and OT, critical infrastructures.

CAPITULO I

1. EL PROBLEMA

1.1. PROBLEMA DE INVESTIGACIÓN

En el año 2018 EMELNORTE realizó la adquisición de la solución de seguridad basada en Checkpoint con un soporte sobre el licenciamiento por un período de 3 años, según el Contrato N° 362, correspondiente al proceso de Subasta Inversa Electrónica N° SIE-EENORTE-216-2017.

En el año 2021 se realizó la renovación del soporte por 2 años adicionales según el Contrato Nro. 200, correspondiente al proceso de Subasta Inversa Electrónica N° SIE-EENORTE-117-2021.

Dentro de las principales funciones que realiza el firewall de siguiente generación, se listan las siguientes:

- Funciones de Firewall: Control de Puertos TCP/UDP y ruteo avanzado.
- Accesos VPN Site to Site y Clientes Remotos.
- IPS
- Filtrado URL y Control de Aplicaciones
- Anti-virus, Anti-bot, Anti-Spam.
- Accesos seguros hacia la red de EMELNORTE, direccionamiento IP, separación de redes, control del tráfico de red.
- Bloqueo de Páginas de Redes Sociales y de Streaming (Facebook. YouTube, etc.)
- Apertura de puertos a Páginas del Gobierno.

- Apertura de puertos de Páginas de Instituciones Privadas que tienen relación con EMELNORTE.
- Apertura de puertos para salida de correos desde el Sistema de Facturación Electrónica.
- Habilitación de IP's para que Presidente Ejecutivo y directores puedan navegar sin ninguna restricción.
- Funcionarios con autorización de Presidente Ejecutivo y directores para la habilitación de filtrado de aplicación y URL's con menor restricción para su navegación en Internet.
- Protección de todos los sistemas y Aplicativos de EMELNORTE.
- Funciones de administración, administración de reglas y registros de tráfico (logs).

Mediante la administración y configuración de los componentes de la plataforma de seguridad perimetral, se garantiza la disponibilidad de los servicios informáticos institucionales. Estos servicios son considerados de misión crítica para empresas del sector estratégico. Cualquier mal funcionamiento podría afectar significativamente la operatividad general.

Los servicios informáticos institucionales dependen de la infraestructura tecnológica. Es crucial renovar las licencias de la plataforma de seguridad antes de que caduquen, asegurando así la operación integral con prestaciones actualizadas y modernas. Esto es fundamental para soportar el crecimiento de la infraestructura de red. Además, es necesario contar con herramientas que permitan controlar los sistemas y servicios informáticos, cumpliendo con las mejores prácticas y separando las redes IT y OT según las necesidades de EMELNORTE.

La vigencia tecnológica, el soporte técnico, las actualizaciones que proporciona el fabricante hasta el distribuidor sobre los equipos de protección perimetral son fundamentales. Estos aspectos son cruciales debido a la constante evolución de los requerimientos y las nuevas versiones de software que surgen. Garantizar estas actualizaciones no solo permite mantener la operatividad y seguridad de nuestra infraestructura, sino también facilita la escalabilidad necesaria para estar a la vanguardia en competencias institucionales y satisfacer los crecientes requisitos laborales.

Según el informe emitido por la Sección de Bienes, mediante Memorando EMELNORTE-DF-2024-0156-MM con fecha 06 de febrero de 2024, los equipos actualmente se encuentran en un estado obsoleto, lo cual representa una amenaza para el buen funcionamiento de los servicios que alojan y para el desenvolvimiento normal de los procesos institucionales. Es crucial proceder con su reemplazo urgente para asegurar la continuidad operativa, mejorar la eficiencia de los servicios y garantizar que la institución esté equipada con tecnología moderna y segura. Esto no solo fortalecerá la capacidad para cumplir con los objetivos institucionales, sino que también permitirá adaptarse de manera más efectiva a los desafíos tecnológicos actuales y futuros.

Ilustración 1. Equipos obsoletos

Código	Descripción	Marca	Serie	Fecha de Adquisición	Vida Útil	Estado
2601040060001	SERVIDOR DE SEGURIDAD HP DL380 S# MXQ7280DML	HP	MXQ7280DML	31/03/2018	5 años	Obsoleto
2601040060002	SERVIDOR DE SEGURIDAD HP DL380 S# MXQ7280DMJ	HP	MXQ7280DMJ	31/03/2018	5 años	Obsoleto

La convergencia de tecnologías de información por sus siglas en ingles IT y OT en el sector energético gubernamental como es el caso de empresas eléctricas como EMELNORTE ha generado un entorno complejo donde la ciberseguridad y la eficiencia operativa son temas críticos. La interconexión de sistemas informáticos con

equipos y dispositivos operativos presenta desafíos significativos en términos de protección de datos, seguridad de infraestructura y operatividad continua.

La falta de una clara separación entre las redes IT y OT en EMELNORTE puede exponer la infraestructura eléctrica a riesgos de ciberseguridad, incluyendo accesos no autorizados, ataques de malware y potenciales interrupciones en el suministro eléctrico. Además, esta integración dificulta la optimización de los procesos operativos, ya que las demandas y requerimientos de cada tipo de red son distintos y a menudo contradictorios.

Cuando las redes de IT y OT no están separadas adecuadamente, se pueden presentar varias vulnerabilidades que pueden comprometer la seguridad y la integridad de los sistemas. Algunas de las principales vulnerabilidades que pueden ser:

Ilustración 2. Vulnerabilidades

Riesgos de seguridad cibernética: La falta de separación entre las IT y tecnologías operativas OT puede permitir que los ciber atacantes accedan a los sistemas de control industrial desde la red corporativa, o viceversa. Esto podría resultar

en la manipulación de procesos industriales críticos o en la exfiltración de datos confidenciales. (Langner, 2011)

Interferencia operativa: Las actividades de la red IT pueden interferir con los sistemas de control industrial, lo que podría afectar la operación segura y eficiente de los procesos industriales. Por ejemplo, las actualizaciones automáticas de software en la red IT podrían afectar inadvertidamente los sistemas de control industrial, causando interrupciones no deseadas. (Haimes, 2013)

Vulnerabilidades de software y sistemas obsoletos: Los sistemas de control industrial a menudo utilizan software y hardware específicos, algunos de los cuales pueden estar desactualizados y no recibir parches de seguridad regulares. Si estos sistemas están conectados directamente a la red IT, pueden representar puntos de vulnerabilidad que podrían ser explotados por los atacantes. (McQueen, 2015)

Exposición a malware: La exposición a malware diseñado para atacar sistemas IT podría propagarse fácilmente a través de la red OT si no hay una segmentación adecuada. Esto podría resultar en la infección de dispositivos de control industrial y la interrupción de las operaciones. (Research, 2018)

Ataques de ingeniería social: La falta de separación entre las redes IT y OT incrementa el riesgo de ataques de ingeniería social. En estos ataques, los atacantes intentan manipular a los empleados para que divulguen información confidencial o realicen acciones que comprometan la seguridad de los sistemas. (Hadžiosmanović D. e., 2018)

La OWASP (Open Web Application Security Protect) enfatiza la importancia de la ingeniería social como un vector de ataque que afecta directamente la seguridad de las aplicaciones y los sistemas. (OWASPFoundation, 2021)

Estas vulnerabilidades destacan la importancia de implementar medidas de seguridad adecuadas, como la segmentación de redes, firewalls industriales, autenticación de usuarios y capacitación del personal en conciencia de seguridad cibernética.

1.2. INTERROGANTES DE LA INVESTIGACIÓN

¿Cuáles son los principales desafíos de seguridad informática que enfrenta EMELNORTE en la convergencia de los servicios de red IT y OT?

¿Cuál es el estado actual de la infraestructura de red de EMELNORTE en términos de integración entre los servicios de IT y OT?

¿Cuáles son las mejores prácticas y estándares de separación de servicios de red IT y OT para garantizar la ciberseguridad en el sector eléctrico?

¿Cómo afecta la integración de servicios de red IT y OT la eficiencia operativa de EMELNORTE?

¿Qué estrategias de separación de servicios de red IT y OT pueden implementarse para mitigar los riesgos de ciberseguridad y mejorar la eficiencia operativa en EMELNORTE?

1.2.1. OBJETIVOS DE LA INVESTIGACIÓN

1.2.2. OBJETIVO GENERAL

Elaborar un plan de separación de los servicios de red de Tecnologías de la Información y Tecnologías Operativas, que garanticen la ciberseguridad y mejore la eficiencia operativa en la Empresa Eléctrica Regional Norte S.A. EMELNORTE.

1.2.3. OBJETIVOS ESPECÍFICOS

- Evaluar la arquitectura actual de la red de EMELNORTE, para comprender la interacción entre los servicios de IT y OT, identificando puntos de

conexión y posibles vulnerabilidades que podrían comprometer la seguridad y la eficiencia operativa.

- Diseñar un modelo de arquitectura de redes que permita la separación efectiva de los servicios de IT y OT en EMELNORTE, considerando las necesidades específicas de la empresa, los requisitos de seguridad y las mejores prácticas en ciberseguridad.
- Definir las medidas de seguridad cibernética tanto en las redes de IT, OT de EMELNORTE y el equipamiento adecuado, con el fin de proteger la integridad, confidencialidad y disponibilidad de la información.
- Evaluar el impacto del plan de separación de redes en la eficiencia operativa y la ciberseguridad de EMELNORTE, mediante la realización de pruebas de concepto tendientes a verificar la efectividad de las medidas implementadas y proponer ajustes necesarios para mejorar la protección de los sistemas y datos críticos.

1.3. HIPOTESIS DEL TRABAJO

Elaborar un plan de separación de los servicios de red de Tecnologías de la Información y Tecnologías Operativas, garantizará la ciberseguridad y mejore la eficiencia operativa en la Empresa Eléctrica Regional Norte S.A. EMELNORTE.

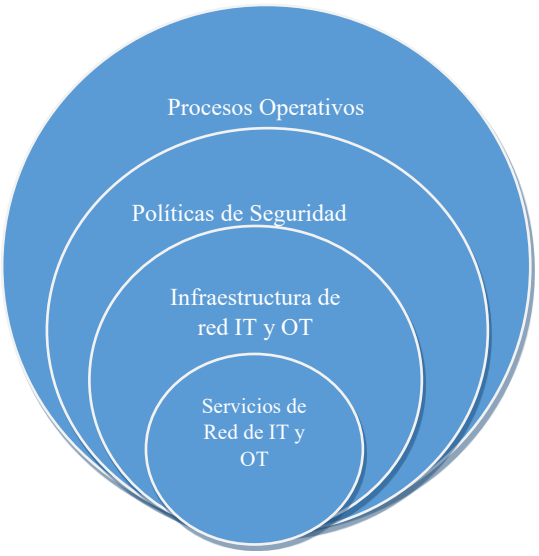
1.4. HIPOTESIS ALTERNATIVA

Elaborar un plan de separación de los servicios de red de Tecnologías de la Información y Tecnologías Operativas, no garantizará la ciberseguridad y mejore la eficiencia operativa en la Empresa Eléctrica Regional Norte S.A. EMELNORTE.

1.5. CATEGORIZACIÓN DE VARIABLES

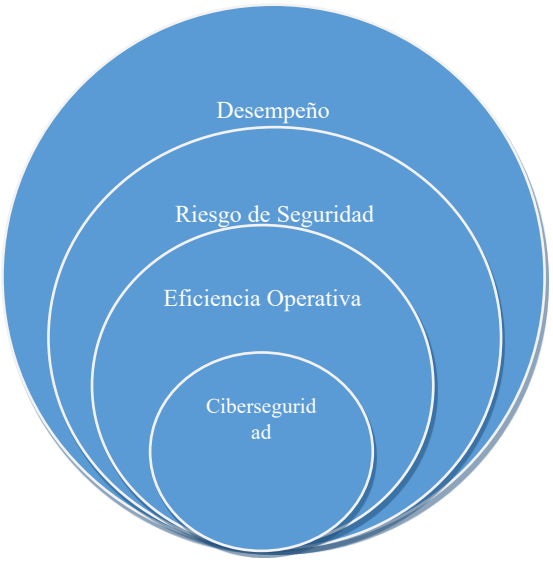
Variable independiente. Plan de separación de los servicios de red de Tecnologías de la Información y Tecnologías Operativas.

Ilustración 3. Variables Independientes



Variable dependiente. Ciberseguridad y eficiencia operativa en la Empresa Eléctrica Regional Norte S.A. EMELNORTE.

Ilustración 4. Variables Dependientes



1.6. JUSTIFICACIÓN

Realizar un plan para la separación de redes IT y OT en la empresa Eléctrica Regional Norte S.A. EMELNORTE es crucial por varias razones, especialmente en términos de ciberseguridad y eficiencia operativa:

La integración de las redes IT y OT puede crear vulnerabilidades significativas. Las redes OT están diseñadas para controlar procesos físicos, como la generación y distribución de energía, y son críticas para la seguridad y la operatividad de la infraestructura eléctrica. La separación de estas redes reduce la superficie de ataque y ayuda a mitigar el riesgo de ciberataques dirigidos a la infraestructura crítica.

La separación de las redes de Tecnología de la Información (IT) y Tecnología Operacional (OT) constituye una medida estratégica esencial para mejorar la postura de ciberseguridad en infraestructuras críticas, como las empresas del sector eléctrico. Esta segmentación reduce significativamente el riesgo de que un incidente en la red IT afecte a los sistemas críticos de OT, lo cual garantiza una mayor resiliencia operativa y continuidad del servicio, minimizando interrupciones en la generación, transmisión y distribución de energía eléctrica (Stouffer K. P., Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity. , 2022).

Diversos marcos normativos y estándares internacionales en materia de ciberseguridad establecen como requisito fundamental la separación lógica o física de las redes IT y OT en industrias críticas. El cumplimiento de estos estándares no solo permite elevar el nivel de protección, sino que también previene sanciones regulatorias y preserva la reputación institucional.

Desde una perspectiva operativa, la separación de redes favorece una mejor asignación de recursos y una optimización de la infraestructura tecnológica, lo cual permite una gestión más eficiente de los sistemas, mejora la capacidad de respuesta ante incidentes y aumenta la flexibilidad para adaptarse a los cambios del mercado eléctrico (Kandasamy, 2020).

Asimismo, esta separación posibilita la implementación de herramientas especializadas de monitoreo y gestión, específicas para cada entorno, lo que incrementa la visibilidad sobre el estado, rendimiento y seguridad de los sistemas críticos. Este enfoque fortalece las capacidades de detección temprana y respuesta a incidentes cibernéticos en tiempo real (Zhang, 2021).

En términos de seguridad, la segmentación entre IT y OT contribuye directamente a reducir la superficie de ataque y a contener la propagación de amenazas, lo cual es fundamental dentro de un enfoque de defensa en profundidad. Esta estrategia se vuelve particularmente relevante frente al creciente número de ataques dirigidos a infraestructuras críticas, como ha sido evidenciado en diversos estudios y casos recientes (Dragos., 2023).

Por lo tanto, la implementación de un plan de separación de redes IT y OT se justifica tanto desde el punto de vista normativo como operativo y estratégico, al contribuir directamente con la ciberseguridad, la eficiencia operativa y el cumplimiento regulatorio en el sector eléctrico.

La integración de sistemas IT y OT puede afectar la eficiencia operativa de una empresa eléctrica. La separación de estas redes puede mejorar la disponibilidad, confiabilidad y rendimiento de los sistemas de control industrial, lo que a su vez puede mejorar la eficiencia operativa y reducir el riesgo de interrupciones en el suministro eléctrico.

El plan propuesto puede tener implicaciones significativas en la industria eléctrica en general. Los resultados podrían servir como referencia para otras empresas del sector que enfrentan desafíos similares en términos de seguridad cibernética y eficiencia operativa.

La investigación propuesta contribuirá al conocimiento académico en el campo de la ciberseguridad y las tecnologías de la información en el sector eléctrico. Además, proporcionará a EMELNORTE y a otras empresas del sector información valiosa para la toma de decisiones estratégicas en cuanto a la gestión de riesgos y la mejora de la eficiencia operativa.

Realizar un plan para la separación de redes IT y OT en EMELNORTE no solo es importante para garantizar la seguridad cibernética y la eficiencia operativa, sino también para cumplir con regulaciones, optimizar recursos y mejorar la resiliencia de la infraestructura eléctrica ante posibles amenazas y desafíos del entorno operativo.

Se toma como referencia el Objetivo 7. “Plan de Creación de Oportunidades”. Potenciar las capacidades de la ciudadanía y promover una educación innovadora, inclusiva y de calidad en todos los niveles, presentando mi investigación a las nuevas generaciones para los desafíos intelectuales, profesionales y personales. (SEMPLADES, 2021)

El objetivo 9. “Plan de Creación de Oportunidades”. Garantizar la seguridad ciudadana, orden público y gestión de riesgo. (SEMPLADES, 2021) es un objetivo estratégico de la ciber seguridad que nos permite minimizar el riesgo que puede tener al no contar con respaldos de los sistemas de información.

Por último, este proyecto se relaciona con la línea No. 10 de investigación científica aprobada por el Honorable Consejo Universitario de la UTN concerniente al Desarrollo, aplicación de software y cybersecurity (seguridad cibernética) (UTN, 2023).

CAPITULO II

2. MARCO REFERENCIAL

2.1. ANTECEDENTES

En el contexto de las redes IT y OT, que son dos entornos distintos pero cada vez más interconectados en la era de la transformación digital e Industrial, hay varias normativas relevantes para la ciberseguridad. Las principales normativas y estándares son:

ISO/IEC 27001: Aunque no está específicamente diseñada para redes IT o OT, es la norma principal para la gestión de la seguridad de la información, que puede aplicarse a cualquier entorno tecnológico, incluidas las redes IT y OT (Standardization, 2022).

ISO/IEC 62443: Esta serie de normas se centra específicamente en la seguridad cibernética para sistemas de control industrial (ICS) y sistemas de automatización (como los utilizados en entornos OT). Se compone de varias partes, incluidas las siguientes:

ISO/IEC 62443-1: Terminología, conceptos y modelos de seguridad.

ISO/IEC 62443-2-x: Directrices para la implementación de medidas de seguridad específicas.

ISO/IEC 62443-3-x: Directrices para el sistema de gestión de la seguridad (Commission I. E., ISA/IEC 62443-3-3: Security for industrial automation and control systems — System security requirements and security levels., 2018).

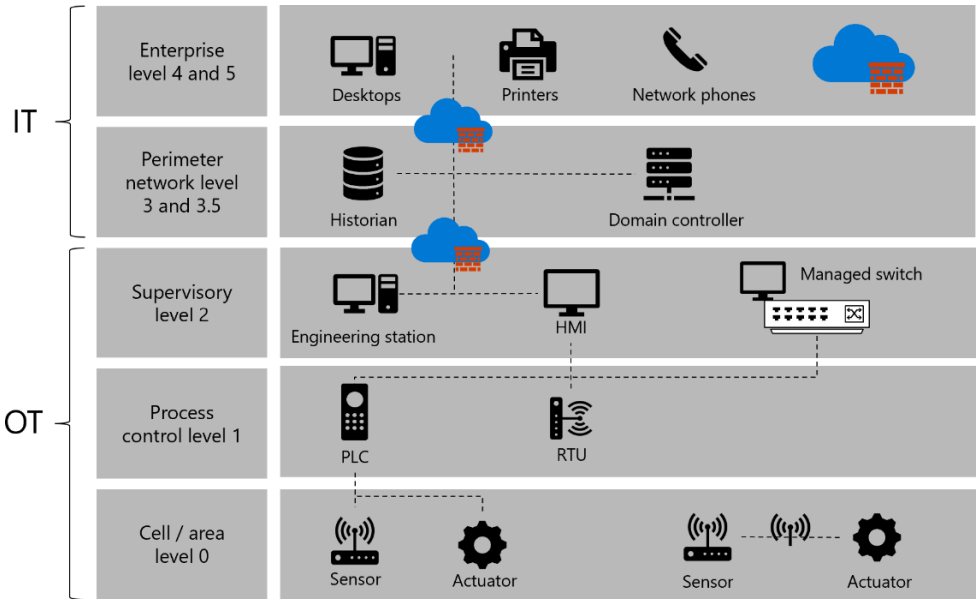
ISO/IEC 27019: Esta norma proporciona directrices específicas para la seguridad de la información en los sectores de energía y servicios públicos, que a

menudo abarcan tanto entornos IT como OT. Se basa en la norma ISO/IEC 27002 pero se enfoca en los riesgos y desafíos particulares de estos sectores.

NIST SP 800-82: Aunque no es una norma ISO/IEC, el Instituto Nacional de Normas y Tecnología (NIST) de Estados Unidos desarrolló este documento que proporciona pautas específicas para la seguridad de los sistemas de control y automatización en entornos industriales. Es especialmente relevante para la ciberseguridad en entornos OT.

Además, existe el Modelo Purdue para redes de comunicación, que es un marco conceptual utilizado en el diseño y la gestión de redes de computadoras. El modelo organiza las funciones de red en capas para facilitar la comprensión y el diseño de sistemas de comunicación. (Stallings, 2013) Es un modelo para la segmentación de redes del Sistema de control industrial (ICS) que define seis capas dentro de estas redes, los componentes que se encuentran en las capas y los controles lógicos de límites de red para proteger estas redes.

Ilustración 5. Modelo Purdue



El artículo "Security Challenges in Operational Technology Networks: A Review", ofrece una revisión detallada de los desafíos de seguridad presentes en las redes de tecnología operativa. Se examinan las vulnerabilidades comunes, las amenazas emergentes y las brechas en las prácticas de seguridad existentes en las infraestructuras OT. Además, se discuten estrategias y soluciones potenciales para abordar estas amenazas y fortalecer la ciberseguridad en las redes OT. (Smith & Johnson, 2020)

En el libro Advances in Industrial Network Security se proporciona una visión detallada de las amenazas de ciberseguridad que enfrentan las tecnologías operativas (OT) y presenta un análisis exhaustivo de las contramedidas disponibles. Se discuten diversos tipos de ataques, desde intrusiones maliciosas hasta fallos de sistemas, y se exploran las mejores prácticas y soluciones para mitigar estos riesgos en entornos OT. (Garcia & Martinez, 2019)

En la conferencia Proceedings of the IEEE International Conference on Industrial Cybersecurity, presenta las mejores prácticas para asegurar las redes de tecnología operativa (OT), ilustradas con casos de estudio relevantes. Se analizan enfoques proactivos y reactivos para proteger las infraestructuras críticas de ataques cibernéticos, junto con ejemplos concretos de implementación y resultados obtenidos en diversas organizaciones industriales. (Lee & Kim, 2021)

En el artículo Cybersecurity Framework for Critical Infrastructure Protection in Operational Technology Environments, se propone un marco de ciberseguridad específicamente diseñado para proteger la infraestructura crítica en entornos de tecnología operativa (OT). Se describen los componentes clave del marco, que incluyen evaluación de riesgos, medidas de seguridad preventivas y planes de

respuesta a incidentes, con el objetivo de fortalecer la resiliencia ante amenazas cibernéticas. (Wang & Chen, 2019)

En el libro Cybersecurity in Industrial Control Systems, se presenta un enfoque integrado para abordar la ciberseguridad en sistemas de tecnología operativa (OT), que combina medidas técnicas, organizativas y humanas. Se discuten estrategias para la detección temprana de amenazas, la respuesta eficaz a incidentes y la promoción de una cultura de seguridad cibernética dentro de las organizaciones industriales. (Lopez, 2018)

2.2. MARCO TEORICO

La revisión sistémica de literatura SLR realizada permite analizar estudios recientes para identificar enfoques, riesgos, modelos de separación y estándares de seguridad aplicables a EMELNORTE. Esta metodología es ampliamente recomendada en investigaciones académicas para obtener una visión estructurada, objetiva y reproducible del estado del conocimiento en un área específica (Kitchenham, 2007), lo que la convierte en una herramienta clave para sustentar decisiones técnicas en contextos críticos como la separación de redes IT y OT.

Tabla 1.Cantidad de estudios revisados

Tipo de Fuente	Cantidad de Estudios Revisados	Estudios Aplicables
IEEE Xplore	50	20
ScienceDirect	30	10
Scorpus	25	8
Otras fuentes	15	5
TOTAL	**120**	**43**

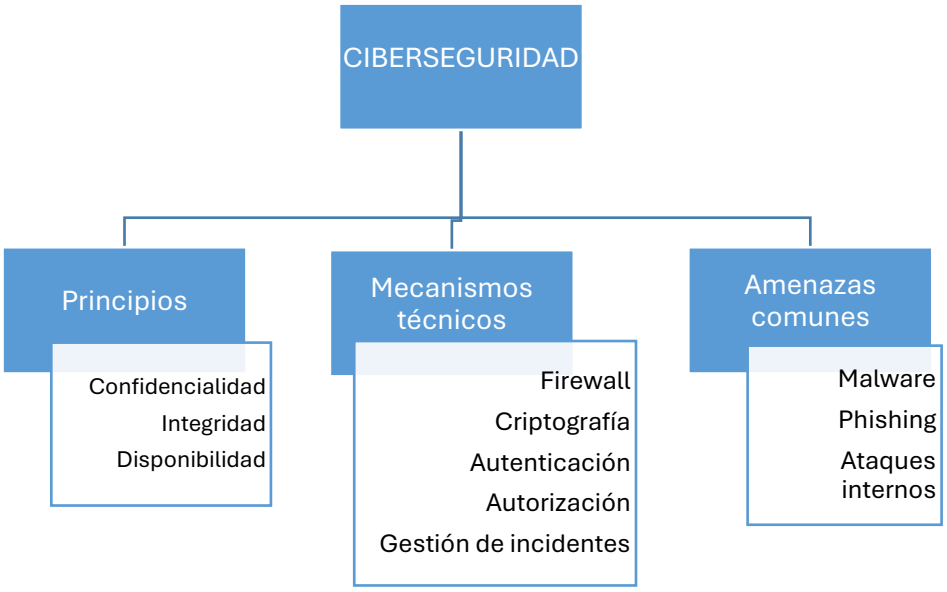
Tabla 2.Tabla comparativa de estudios

Autor(es)	Año	Título	Fuente	Principales hallazgos	Relevancia para la tesis
Smith et al.	2020	*Cybersecurity Strategies for IT/OT Segmentation*	IEEE Xplore	Propone un modelo basado en IA para segmentación de redes industriales	Aplicable a la mejora de seguridad en EMELNORTE
Zhang & Li	2021	*Risk Assessment in IT-OT Converged Networks*	ScienceDirect	Identifica amenazas específicas en sistemas SCADA	Relevante para la evaluación de riesgos en la separación
Johnson et al.	2022	*IEC 62443 Implementation in Power Grids*	IEEE Xplore	Discute implementación de IEC 62443 para seguridad de redes OT	Fundamental para la regulación en EMELNORTE
Brown et al.	2023	*The Role of the Purdue Model in ICS Security*	Scopus	Analiza la implementación del modelo Purdue en redes industriales	Clave para estructurar la separación de IT y OT

2.2.1. Introducción a la Seguridad Informática y OT:

La seguridad informática es un campo dedicado a proteger la integridad, confidencialidad y disponibilidad de la información y los sistemas de cómputo. Implica la implementación de medidas técnicas, procedimentales y organizativas diseñadas para prevenir, detectar, responder y recuperarse de eventos que puedan comprometer la seguridad de la información y los activos tecnológicos.

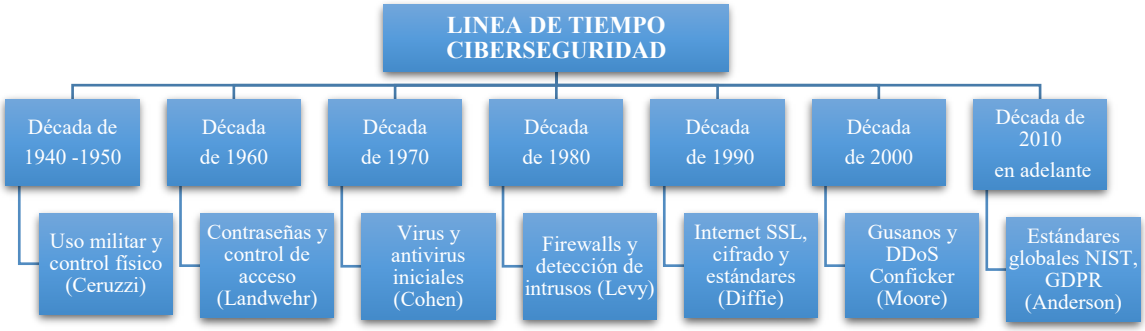
Ilustración 6. Seguridad Informática



La **seguridad en sistemas de control industrial** OT, por sus siglas en inglés, Operational Technology se refiere a la protección de los sistemas y dispositivos utilizados en entornos industriales y de producción, como plantas de fabricación, infraestructuras críticas y sistemas de energía, agua y transporte. A diferencia de la seguridad informática tradicional, que se centra en sistemas de tecnología de la información IT, la seguridad en OT se enfoca en proteger los sistemas de control y automatización que supervisan y controlan procesos físicos.

Seguridad Informática: La historia y evolución de la seguridad informática y su aplicación en entornos industriales se remonta a los primeros días de la computación. Los hitos más importantes son los siguientes:

Ilustración 7. Línea de Tiempo Ciberseguridad



En cuanto a su aplicación en entornos industriales, la seguridad informática evolucionó para abordar las necesidades específicas de sistemas de control industrial (OT). Esto incluye la protección de dispositivos y redes utilizados en infraestructuras críticas como plantas de energía, refinerías, plantas químicas, sistemas de transporte y otros entornos industriales. La seguridad en entornos industriales implica no solo proteger los sistemas de control contra amenazas cibernéticas, sino también considerar los riesgos asociados con el funcionamiento de equipos físicos, la seguridad de los procesos y la continuidad del negocio. Se han desarrollado estándares y mejores prácticas específicos para la seguridad en OT, y se ha prestado especial atención a la protección de sistemas de control contra amenazas cibernéticas, como ataques de malware, intrusiones y sabotaje industrial.

2.2.2. Importancia de la Seguridad Informática

La importancia de la seguridad informática en empresas eléctricas y otros sectores críticos radica en varios factores clave:

Protección de infraestructuras críticas: Las empresas eléctricas y otros sectores críticos, como la infraestructura de agua, transporte, salud y servicios financieros, son esenciales para el funcionamiento de la sociedad. La seguridad informática es fundamental para proteger estas infraestructuras vitales contra

amenazas cibernéticas que podrían causar interrupciones en los servicios, afectando la vida de las personas y la economía en general. (Stouffer K. F., 2011)

Prevención de ciberataques: Las empresas eléctricas y otros sectores críticos son blancos atractivos para los ciberatacantes debido a su importancia estratégica. Un ataque exitoso podría causar apagones masivos, interrupciones en servicios esenciales o incluso poner en peligro la seguridad pública. La seguridad informática es esencial para prevenir y mitigar estos ataques, protegiendo los sistemas de control y la infraestructura crítica contra intrusiones maliciosas. (Brenner, 2016)

Protección de datos sensibles: Las empresas eléctricas y otros sectores críticos almacenan y procesan grandes cantidades de datos sensibles, incluidos datos de clientes, información financiera y datos operativos. La seguridad informática es fundamental para proteger esta información confidencial contra accesos no autorizados, robos de datos y otras amenazas cibernéticas que podrían comprometer la privacidad y la confidencialidad de los datos.

Cumplimiento normativo: Los sectores críticos están sujetos a regulaciones y estándares específicos en materia de seguridad cibernética, diseñados para proteger la infraestructura crítica y garantizar la continuidad del negocio. Las empresas eléctricas y otros sectores críticos deben cumplir con estas regulaciones, lo que requiere implementar medidas de seguridad informática adecuadas y mantenerse al tanto de las mejores prácticas en el campo de la ciberseguridad.

Gestión de riesgos: La seguridad informática es esencial para identificar, evaluar y mitigar los riesgos asociados con el funcionamiento de empresas eléctricas y otros sectores críticos. Esto incluye evaluar las vulnerabilidades en los sistemas de

control y la infraestructura crítica, y tomar medidas para reducir la exposición a posibles amenazas cibernéticas. (Pfleeger & Pfleeger, 2015)

2.2.3. Amenazas cibernéticas en el sector eléctrico

En el sector eléctrico, la convergencia entre redes IT y OT ha incrementado la exposición a amenazas cibernéticas como malware en sistemas SCADA, ataques DDoS, ransomware y accesos no autorizados. Estas amenazas pueden afectar la continuidad del servicio y comprometer la seguridad operativa. Por ello, se requiere una estrategia de ciberseguridad basada en segmentación de redes, monitoreo continuo y cumplimiento de estándares.

Ataques de denegación de servicio (DDoS): Estos ataques buscan sobrecargar los sistemas de control y las redes eléctricas con tráfico malicioso, lo que puede resultar en interrupciones del servicio y daños a la infraestructura crítica. (Ackerman, 2018)

Malware dirigido: El malware diseñado específicamente para infiltrarse en los sistemas de control industrial puede causar interrupciones operativas, manipulación de datos y daños físicos a los equipos. (Rid & Buchanan, 2015)

Phishing y spear phishing: Los correos electrónicos fraudulentos pueden utilizarse para engañar a los empleados y obtener acceso no autorizado a los sistemas críticos, lo que facilita el robo de información confidencial o la manipulación de procesos. (Schneier, 2015)

Ingeniería social: Los atacantes pueden aprovechar la confianza de los empleados para obtener acceso a sistemas sensibles o información privilegiada, mediante técnicas como el engaño, la manipulación psicológica o la suplantación de identidad. (Hadžiosmanović D. B., 2017)

Vulnerabilidades en el software y hardware: Las debilidades en los sistemas de control y las infraestructuras críticas pueden ser explotadas por actores malintencionados para acceder, manipular o interrumpir las operaciones eléctricas.

2.2.4. Consecuencias de los ataques cibernéticos en el sector eléctrico:

Interrupciones del servicio: Los ciberataques dirigidos a sistemas eléctricos pueden provocar cortes de energía a gran escala, afectando a usuarios residenciales, industriales y servicios críticos. Estas interrupciones generan impactos sociales y económicos significativos, desde pérdidas productivas hasta la paralización de infraestructuras esenciales.

Daños a la infraestructura: La manipulación maliciosa de sistemas de control industrial puede causar daños físicos en equipos como transformadores, generadores y redes de distribución. Estos incidentes implican elevados costos de reparación, tiempos de inactividad prolongados y riesgos operativos para el personal técnico.

Pérdida de datos y confidencialidad: La filtración o exfiltración de datos sensibles, como diagramas de red, configuraciones de sistemas SCADA o información de usuarios, compromete la seguridad de las operaciones, la privacidad y la competitividad, especialmente en un entorno donde la inteligencia de amenazas es crítica.

Reputación y confianza: Un incidente de seguridad puede deteriorar la percepción pública sobre la confiabilidad de la empresa eléctrica y del sistema nacional de energía. La pérdida de confianza puede traducirse en presión regulatoria, afectación de relaciones con clientes e inversores y debilitamiento institucional.

2.2.5. Estrategias de mitigación:

Seguridad de la información: Implementar medidas robustas de seguridad de la información, como firewalls, sistemas de detección de intrusiones y encriptación de datos, para proteger los sistemas críticos contra amenazas cibernéticas. (Hadžiosmanović D. B., 2017)

Concienciación y capacitación: Educar a los empleados sobre las mejores prácticas de seguridad cibernética y fomentar una cultura de seguridad en toda la organización para reducir el riesgo de ingeniería social y phishing. (Slay, 2017)

Actualizaciones y parches: Mantener actualizados los sistemas de control y los equipos de infraestructura crítica mediante la aplicación regular de parches de seguridad y la gestión proactiva de vulnerabilidades. (Goodchild, 2020)

Colaboración y coordinación: Fomentar la colaboración entre los sectores público y privado para compartir información sobre amenazas, buenas prácticas y lecciones aprendidas en la protección de infraestructuras críticas contra ataques cibernéticos. (Rid T. &., 2015)

2.2.6. Separación de Redes IT y OT

La separación efectiva entre los entornos de Tecnologías de la Información (IT) y Tecnologías Operativas (OT) es fundamental para garantizar la seguridad y la integridad de los sistemas de control industrial. Las estrategias para su implementación son las siguientes:

Riesgos de convergencia IT-OT: La convergencia entre IT y OT ha creado nuevos desafíos de seguridad cibernética debido a la interconexión de sistemas tradicionalmente aislados. En su investigación, (Shenoy & K., 2019) analizan los

riesgos asociados con esta convergencia y proponen enfoques para mitigarlos, incluyendo la implementación de mecanismos de separación.

Arquitecturas de separación: La implementación de arquitecturas de separación física y lógica entre los entornos de IT y tecnologías operativas OT es crucial para minimizar el riesgo de intrusiones y ataques cibernéticos. En su artículo, (Gritzalis, 2018) proponen un marco arquitectónico para la segregación de sistemas de control industrial, destacando la importancia de una implementación adecuada y efectiva.

Políticas de seguridad: El establecimiento de políticas de seguridad claras y exhaustivas es fundamental para garantizar la efectividad de los mecanismos de separación entre IT y OT. En su libro, (Vacca, 2020) aborda la importancia de desarrollar políticas de seguridad cibernética específicas para entornos de control industrial, incluyendo directrices para la implementación de medidas de separación.

Tecnologías de seguridad: La adopción de tecnologías de seguridad específicas, como firewalls industriales y sistemas de detección de intrusiones, puede mejorar la protección de los entornos de IT y OT contra amenazas cibernéticas. En su investigación, (Xin, 2017) evalúan la eficacia de diferentes tecnologías de seguridad en la segregación de sistemas de control industrial.

2.3. MARCO LEGAL

Las principales normativas y estándares son:

Normas de control interno de la Contraloría General del Estado

410-07 Administración de proyectos tecnológicos

"La unidad de tecnologías de la información y comunicaciones definirá una metodología que facilite la administración de todos los proyectos relacionados con las tecnologías de la información y comunicaciones que ejecuten las diferentes áreas que conformen dicha unidad, así como de las otras unidades administrativas de la organización.

Los aspectos a considerar como mínimo son:

1. Documentación y aprobación de la justificación que da origen al proyecto, así como, descripción de la naturaleza, estudio de factibilidad pertinente, objetivos y alcance del proyecto, su relación con otros proyectos institucionales sobre la base del compromiso, participación y aceptación de los usuarios interesados.

2. Cronograma de actividades que facilite la ejecución y monitoreo del proyecto que incluirá el talento humano (responsables), tecnológicos y financieros, además de los planes de pruebas y de capacitación correspondientes.

3. La formulación de los proyectos considerará el Costo Total de Propiedad CTP; que incluya no sólo el costo de la compra, sino los costos directos e indirectos, los beneficios relacionados con la compra de equipos o programas informáticos, aspectos del uso y mantenimiento, formación para el personal de soporte y usuarios, así como el costo de operación y de los equipos o trabajos de consultoría necesarios.

4. Para asegurar la ejecución del proyecto se definirá una estructura en la que se nombre un servidor responsable con capacidad de decisión y autoridad y administradores o líderes funcionales y tecnológicos con la descripción de sus funciones y responsabilidades.

5. Se cubrirá, como mínimo las etapas de: inicio, planeación, ejecución, control, monitoreo y cierre de proyectos, así como los entregables, aprobaciones y

compromisos formales mediante el uso de actas o documentos electrónicos legalizados.

6. El inicio de las etapas importantes del proyecto será aprobado de manera formal y comunicado a todos los interesados.

7. Se incorporará el análisis de riesgos. Los riesgos identificados serán permanentemente evaluados para retroalimentar el desarrollo del proyecto, además de ser registrados y considerados para la planificación de proyectos futuros.

8. Se deberá monitorear y ejercer el control permanente de los avances del proyecto mediante un informe técnico económico que refleje la ejecución del proyecto.

9. Se establecerá un plan de control de cambios y un plan de aseguramiento de calidad que será aprobado por las partes interesadas.

10. El proceso de cierre incluirá la aceptación formal y pruebas que certifiquen la calidad y el cumplimiento de los objetivos planteados junto con los beneficios obtenidos."

410-09 Adquisiciones de infraestructura tecnológica

"La unidad de tecnologías de la información y comunicaciones definirá, justificará, implantará y actualizará la infraestructura tecnológica de la organización para lo cual se considerarán los siguientes aspectos:

1. Las adquisiciones tecnológicas deben basarse en los estándares vigentes para el sector público, y estarán alineadas a los objetivos de la organización, a los principios de calidad de servicio, y constarán en el plan estratégico de tecnologías de la información y comunicación y en el plan anual de contrataciones aprobado de la

institución. Las excepciones serán autorizadas por la máxima autoridad previa justificación técnica documentada.

2. Las adquisiciones tecnológicas, incluidas las de consultoría y de servicios de procesamiento, soporte y/o almacenamiento prestados por terceros, deben estar debidamente justificadas, documentadas y respaldadas por la planificación de su capacidad, el análisis de costo/beneficio, la previsión de su vida útil y la evaluación de riesgos pertinentes.

3. En la adquisición de hardware, los contratos respectivos, tendrán el detalle suficiente que permita establecer las características técnicas de los principales componentes tales como: marca, modelo, número de serie, capacidades, interfaces, software instalado, entre otros, a fin de determinar la correspondencia entre los equipos adquiridos y las especificaciones técnicas y requerimientos establecidos en las fases precontractual y contractual, lo que será confirmado en las respectivas actas de entrega/recepción. Los contratos deberán incluir cláusulas de garantías y multas.

4. Los contratos con proveedores de servicios incluirán las especificaciones formales sobre acuerdos de nivel de servicio y puntualizarán explícitamente los aspectos relacionados con la seguridad y confidencialidad de la información. Deberán incluir cláusulas de garantías y multas, además de los requisitos legales que sean aplicables.

Se aclarará expresamente que la propiedad de los datos corresponde a la organización contratante. La dirección de la organización debe monitorear el servicio contratado para asegurar el cumplimiento de las obligaciones comprometidas.

5. En caso de contrataciones de servicios externos en los que el proveedor realice el procesamiento de la información de la organización mediante sistemas que

pertenecen a terceros, careciendo la organización de los programas fuente, deben tomarse las previsiones necesarias para asegurar la disponibilidad de los mismos por parte de la organización en caso de alguna contingencia o salida del mercado del proveedor, o bien estableciendo otro mecanismo de contingencia para la continuidad operativa. En caso de tratarse de algún tipo de procesamiento o almacenamiento en la "nube" debe realizarse el análisis pertinente de riesgos y costo/beneficio, que deberá ser aprobado por la máxima autoridad. La información objeto de estos contratos debe estar formalmente clasificada, en base a los criterios definidos previamente por la entidad contratante, y se sujetará a lo establecido en el número 4 de esta norma.

6. Las bajas de equipamiento y/o residuos de aparatos tecnológicos, así como la finalización de contratos de servicios externos de procesamiento y/o almacenamiento de la información deben considerar el respaldo previo al borrado seguro de la información almacenada, así como la normativa ambiental de gestión de residuos aplicable."

410-11 Seguridad de tecnología de información

"La unidad de tecnologías de la información y comunicaciones debe garantizar el cumplimiento de la normativa de protección de datos personales, propiedad intelectual del software, seguridad de la información, utilización de estándares, sistemas o plataformas establecidas para el sector público, y estarán alineadas a los objetivos de la organización, a los principios de calidad de servicio, y constarán en el plan informático y en el plan anual de contrataciones aprobado de la institución. Las excepciones serán al acceso a la información pública, así como de las demás normas que resulten aplicables. Las entidades de la administración pública

implementarán una política de seguridad de la información sobre la base de las disposiciones legales y reglamentarias vigentes."

Oficio del Ministerio de Telecomunicaciones

El Ministerio de Telecomunicaciones y de la Sociedad de la Información mediante Oficio Nro. MINTEL-MINTEL-2021-0312-O, de 23 de julio de 2021, con Asunto: Recomendaciones Preventivas y correctivas de Ciberseguridad, menciona lo siguiente:

"...El constante crecimiento de ciberataques, demanda de una mayor concienciación sobre la necesidad de proteger los activos de información y así minimizar o evitar el daño económico e imagen institucional de la Administración Pública. La información que custodian las instituciones públicas constituye uno de los activos más valiosos y exige ser protegida, así como clasificada y valorada según su criticidad.

Bajo el contexto del ataque cibernético, de público conocimiento, en contra de la Corporación Nacional de Telecomunicaciones CNT EP., y a efectos de evitar eventuales afectaciones o posibles ataques similares en otras entidades gubernamentales, de lo cual no hay evidencia hasta el momento, se recomienda tomar al menos las siguientes medidas como necesarias:

1. Medidas Preventivas:

Reforzar al máximo posible (hardenización) la Infraestructura Tecnológica

Revisión de la seguridad perimetral como: políticas de firewall, antispam, IPS, SandBox, IDS, filtrado de contenidos, WAF, etc. ..."

Acuerdo Ministerial MINTEL-MINTEL-2024-0003 – EGSI V3.0

En el Acuerdo Nro. MINTEL-MINTEL-2024-0003, de fecha 08 de febrero de 2024, se anexa el Esquema Gubernamental de Seguridad de la Información (EGSI) Versión 3.0 "Sistema de Gestión de Seguridad de la Información para las Instituciones del Sector Público", en el que se indica:

"4.20. Seguridad de redes

Control

Proteger, administrar y controlar las redes y los dispositivos de red, para proteger la información en los sistemas y aplicaciones institucionales.

Recomendaciones para la implementación:

Se deben implementar controles para asegurar la seguridad de la información en las redes y para proteger los servicios conectados del acceso no autorizado, …"

"4.21. Seguridad de los servicios de red

Control

Los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red se deben identificar, implementar y monitorear, independientemente de si estos servicios se entregan de manera interna o están externalizados. (SLA´s).

Recomendaciones para la implementación:

Las medidas de seguridad necesarias para servicios particulares, tales como características de seguridad, niveles de servicio y requisitos de servicio, deben ser identificadas e implementadas por proveedores de servicios de red internos o externos.

La institución debe asegurarse de que los proveedores de servicios de red implementen estas medidas. …"

"4.22. Separación en las redes

Control

Separar las redes en función de los grupos de servicios, usuarios y sistemas de información.

Recomendaciones para la implementación:

Se deben considerar las siguientes recomendaciones para la implementación:

a) La institución debe considerar la gestión de la seguridad de las grandes redes dividiéndolas en dominios de red separados y separándolas de la red pública (es decir, Internet), documentar la división de red identificando las direcciones IP que se encuentran en cada segmento de red;

b) Los dominios se pueden elegir en función de los niveles de confianza, criticidad y

sensibilidad, por ejemplo, dominio de acceso público, dominio de escritorio, dominio de servidor, sistemas de alto y bajo riesgo, junto con unidades organizativas, por ejemplo, recursos humanos, finanzas o alguna combinación, por ejemplo, dominio de servidor que se conecta a varias unidades organizativas;

c) La separación se puede realizar usando redes físicamente diferentes o usando diferentes redes lógicas (VLAN); …"

ISO/IEC 27001: Aunque no está específicamente diseñada para redes IT o OT, ISO/IEC 27001 es la norma principal para la gestión de la seguridad de la

información y establece un marco sistemático para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Esta norma se utiliza como buena práctica porque ayuda a las organizaciones a identificar riesgos, gestionar controles y asegurar la confidencialidad, integridad y disponibilidad de la información en cualquier entorno tecnológico, incluyendo tanto redes IT como OT. Al aplicar ISO/IEC 27001, las organizaciones pueden proteger sus activos de información frente a amenazas internas y externas, cumplir con requisitos regulatorios y generar confianza en clientes y socios. Su enfoque basado en el riesgo facilita la adaptación de controles específicos a las necesidades de cada red o sistema, garantizando así una gestión de seguridad eficaz y alineada con los objetivos del negocio (Commission I. E., https://www.iec.ch/standards, 2024).

ISO/IEC 62443: Esta serie de normas está centrada específicamente en la seguridad cibernética para sistemas de control industrial (ICS) y sistemas de automatización, que son la base de los entornos OT. Se considera una buena práctica clave porque aborda las particularidades y vulnerabilidades propias de estos sistemas, que a menudo tienen requisitos operativos y restricciones técnicas diferentes a los entornos IT tradicionales. Las diferentes partes de la norma permiten una implementación integral y modular de la seguridad:

ISO/IEC 62443-1: Establece la terminología y conceptos fundamentales, proporcionando un lenguaje común y un marco conceptual que facilita la comunicación entre los equipos técnicos y de gestión.

ISO/IEC 62443-2-x: Ofrece directrices prácticas para la implementación de medidas de seguridad específicas, permitiendo a las organizaciones proteger componentes individuales, como dispositivos, redes o aplicaciones dentro del entorno industrial.

ISO/IEC 62443-3-x: Proporciona orientación para establecer un sistema de gestión de la seguridad que integra políticas, procedimientos y controles, asegurando que la seguridad sea gestionada de manera continua y alineada con las operaciones industriales.

El uso de ISO/IEC 62443 ayuda a reducir riesgos de ciberataques que podrían comprometer la continuidad operativa, la seguridad física y la integridad de los procesos industriales.

ISO/IEC 27019: Esta norma proporciona directrices específicas para la seguridad de la información en los sectores de energía y servicios públicos, ámbitos en los que convergen redes IT y OT y donde los riesgos y amenazas presentan características particulares. Se basa en la ISO/IEC 27002, adaptando sus controles para enfrentar desafíos propios como la gestión segura de infraestructuras críticas, la protección contra interrupciones del suministro eléctrico y el manejo seguro de sistemas SCADA y otros sistemas de control industrial. Es una buena práctica porque ayuda a las organizaciones a establecer un marco de seguridad adaptado a los riesgos inherentes al sector energético, mejorando la resiliencia ante incidentes y ataques cibernéticos que podrían afectar la seguridad nacional, la economía y la sociedad. Además, facilita el cumplimiento de regulaciones sectoriales y mejora la interoperabilidad entre sistemas IT y OT, promoviendo una gestión integrada de la ciberseguridad (Commission I. O., 2024).

NIST SP 800-82: Aunque no es una norma ISO/IEC, el documento NIST Special Publication 800-82 es una guía muy valorada que proporciona pautas específicas para la seguridad de sistemas de control y automatización industrial. Esta guía es especialmente relevante para entornos OT porque reconoce las diferencias críticas entre sistemas industriales y redes IT convencionales, incluyendo la necesidad

de asegurar la disponibilidad y seguridad física de procesos críticos. NIST SP 800-82 ofrece recomendaciones prácticas para evaluar riesgos, seleccionar controles de seguridad y diseñar arquitecturas seguras en sistemas industriales. Su enfoque ayuda a las organizaciones a implementar defensas efectivas que mitigan amenazas cibernéticas sin afectar la operación continua de los sistemas. Adoptar esta guía permite a las empresas mejorar su postura de ciberseguridad de manera consistente, basándose en un marco reconocido internacionalmente y apoyado en experiencia técnica detallada (Technology, 2023).

CAPITULO III

3.1. Descripción del área de estudio / Descripción del grupo de estudio

EMELNORTE es una empresa del sector estratégico ecuatoriano que tiene como misión brindar el servicio público de energía eléctrica y servicio de alumbrado público general, con calidad, calidez, responsabilidad social y ambiental a la población del área de cobertura.

EMELNORTE dispone de una gran cantidad de servicios informáticos que son utilizados por los funcionarios de la Empresa desde toda el área de concesión. Entre estos servicios se dispone de sistemas de atención al cliente, sistema financiero, sistema de gestión de nómina, etc.

EMELNORTE dentro de su arquitectura de red que tiene como punto principal el Centro de Datos del edificio matriz, ubicado en la calle Juan Manuel Grijalva 6-54 entre Bolívar y Olmedo y se extiende hacia 3 edificios en la ciudad de Ibarra, 14 agencias, 18 subestaciones y 4 centrales de generación, expandidas a lo largo de las provincias de Imbabura, Carchi y norte de Pichincha.

Ilustración 8. Edificio Matriz EMELNORTE

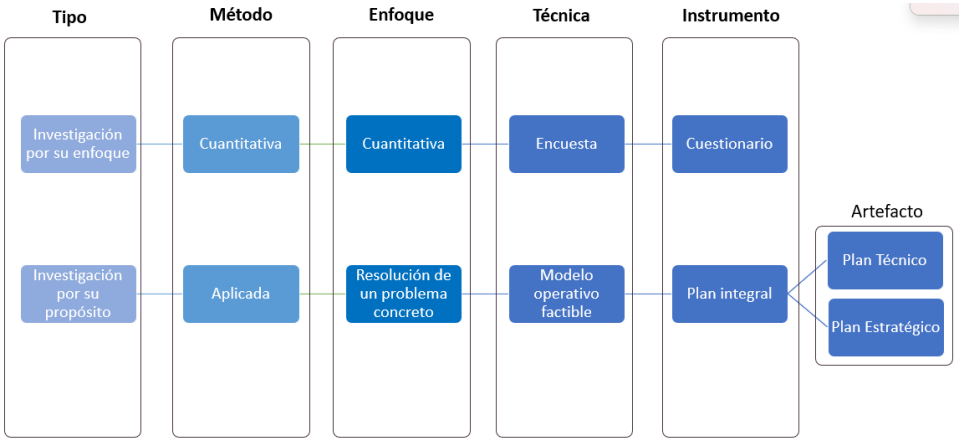
3.2. Enfoque y tipo de investigación

Se elaboró el plan, dado el alcance y la naturaleza multidimensional del tema de investigación, un enfoque cualitativo para una evaluación más completa de la viabilidad de la separación de redes IT y OT en EMELNORTE, considerando las implicaciones en ciberseguridad y eficiencia operativa.

La separación de redes IT y OT es un problema multidimensional que involucra aspectos tecnológicos, de seguridad, regulatorios y organizativos. Un enfoque cualitativo permitirá abordar esta complejidad desde diferentes ángulos, utilizando métodos para comprender los contextos.

Al estudiar la separación de redes IT y OT, es importante considerar las perspectivas de diversos stakeholders, como empleados, directivos, reguladores y posiblemente incluso clientes.

Ilustración 9. Metodología



Las preguntas realizadas en la encuesta se aplicaron al personal de EMELNORTE, que tiene conocimientos en redes y comunicaciones y que interactúan con las redes de la Institución.

Se realizaron las siguientes preguntas:

Ilustración 10. Encuesta Página 1

EmelNorte

Encuesta sobre la Separación de Redes IT y OT

Objetivo: Conocer el nivel de conocimiento, percepción de riesgos y prácticas en la segmentación de redes IT y OT en servicios críticos.

1. ¿Qué nivel de conocimiento tiene sobre la separación de redes IT y OT?

   ☐ Básico

   ☐ Intermedio

   ☐ Avanzado

2. ¿Cuáles considera que son los principales riesgos de no separar las redes IT y OT? (Seleccione hasta 3 opciones)

   ☐ Ciberataques

   ☐ Pérdida de datos

   ☐ Interrupción operativa

   ☐ Acceso no autorizado

   ☐ Otros (especificar) _____

3. ¿Su empresa ha implementado una estrategia de segmentación de redes IT y OT?

   ☐ Sí

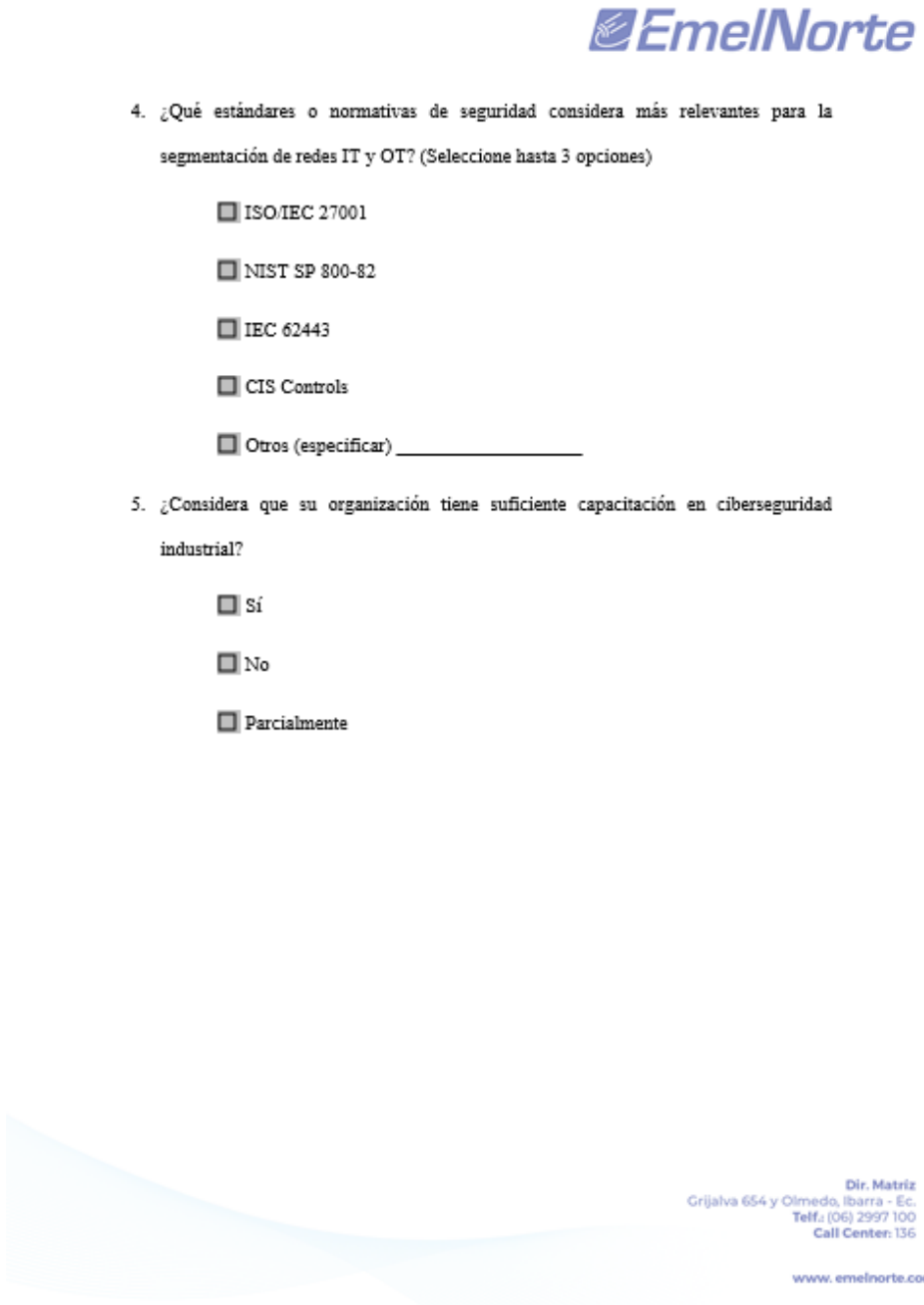
   ☐ No

   ☐ En proceso

Dir. Matriz
Grijalva 654 y Olmedo, Ibarra - Ec.
Telf.: (06) 2997 100
Call Center: 136

www.emelnorte.com

Ilustración 11. Encuesta Página 2



EmelNorte

4. ¿Qué estándares o normativas de seguridad considera más relevantes para la segmentación de redes IT y OT? (Seleccione hasta 3 opciones)

- ☐ ISO/IEC 27001
- ☐ NIST SP 800-82
- ☐ IEC 62443
- ☐ CIS Controls
- ☐ Otros (especificar) _____

5. ¿Considera que su organización tiene suficiente capacitación en ciberseguridad industrial?

- ☐ Sí
- ☐ No
- ☐ Parcialmente

Dir. Matriz
Grijalva 654 y Olmedo, Ibarra - Ec.
Telf.: (06) 2997 100
Call Center: 136

www. emelnorte.com

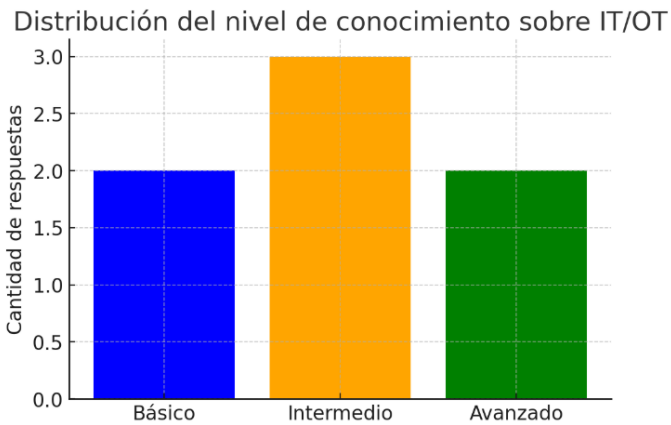
La encuesta fue dirigida a 7 funcionarios, cuyas funciones se desarrollan principalmente en el área de redes y comunicaciones, así como a los directores de las áreas involucradas en la operación y seguridad de los sistemas IT y OT de la organización. La selección de los participantes se realizó en función de su

responsabilidad directa o indirecta en la gestión de la infraestructura tecnológica y su relación con los procesos de ciberseguridad industrial. Los resultados que se obtuvo son los siguientes:

Tabla 3. Respuesta encuestas

Pregunta \ Participante	**P1**	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**
Nivel de conocimiento	Básico	Intermedio	Avanzado	Intermedio	Básico	Avanzado	Intermedio
Principales riesgos	Ciberataques, Pérdida de datos	Interrupción operativa, Ciberataques	Acceso no autorizado, Ciberataques, Pérdida de datos	Pérdida de datos, Interrupción operativa	Ciberataques, Interrupción operativa	Acceso no autorizado, Ciberataques	Ciberataques, Pérdida de datos
Estrategia implementada	Sí	No	En proceso	Sí	No	Sí	En proceso
Normativas relevantes	ISO/IEC 27001, IEC 62443	NIST SP 800-82, CIS Controls	IEC 62443, NIST SP 800-82	ISO/IEC 27001, CIS Controls	IEC 62443, ISO/IEC 27001	NIST SP 800-82, IEC 62443	CIS Controls, NIST SP 800-82
Capacitación en ciberseguridad	Sí	No	Parcialmente	Sí	No	Parcialmente	No

Ilustración 12. Nivel de Conocimientos



Como se muestra en el gráfico, la mayoría de los encuestados (3 de 7) se ubicó en un nivel intermedio, lo que sugiere que poseen una comprensión funcional del tema,

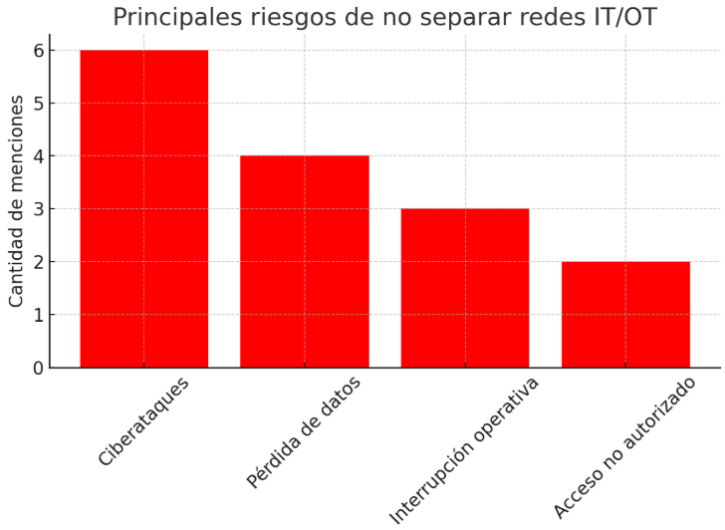
probablemente derivada de experiencias previas o formación parcial en ciberseguridad industrial.

Por otro lado, dos funcionarios manifestaron tener un nivel básico, lo que evidencia la necesidad de fortalecer sus conocimientos para que puedan entender e implementar buenas prácticas de segmentación. Estos perfiles posiblemente requieren mayor capacitación en normativas, riesgos y estrategias específicas de separación IT/OT.

Finalmente, dos encuestados indicaron un nivel avanzado, lo cual representa una fortaleza para la organización, ya que estos profesionales pueden actuar como líderes técnicos o mentores dentro del proceso de implementación de medidas de ciberseguridad y segmentación de redes. Su conocimiento profundo resulta clave para guiar la implementación del proyecto.

Este panorama mixto evidencia que, aunque existen bases sólidas en algunos perfiles, se requiere una estrategia continua de capacitación técnica y sensibilización para garantizar un entendimiento homogéneo en todo el equipo, condición indispensable para la correcta separación y protección de redes IT y OT.

Ilustración 13. Riesgos Identificados



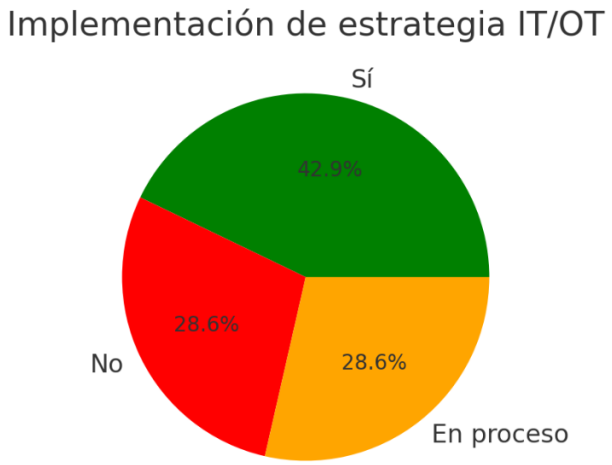
Se muestran una clara preocupación de los encuestados por las consecuencias de no implementar una separación adecuada entre las redes IT y OT dentro de la organización. El riesgo más mencionado fue el de ciberataques, con 6 menciones, lo cual destaca el alto grado de sensibilidad que existe en torno a la posibilidad de intrusiones externas que puedan comprometer la operación o la infraestructura crítica.

En segundo lugar, con 4 menciones, se identificó la pérdida de datos, un riesgo que puede derivar de accesos no controlados, vulnerabilidades compartidas entre redes o falta de controles adecuados en la frontera entre entornos IT y OT. Este tipo de impacto podría no solo comprometer la continuidad operativa, sino también afectar el cumplimiento normativo y la confianza de los usuarios.

La interrupción operativa, con 3 menciones, también fue considerada una consecuencia importante, ya que una falla o ataque en la red IT podría propagarse al entorno OT, deteniendo procesos productivos o servicios esenciales. Finalmente, el acceso no autorizado, con 2 menciones, cierra el conjunto de riesgos identificados, señalando que, aunque se percibe como menos probable, sigue siendo una amenaza latente cuando no existen barreras o segmentaciones claras entre los dominios tecnológicos.

Estos resultados respaldan la necesidad urgente de fortalecer la arquitectura de red mediante la segmentación y aplicación de controles específicos, así como adoptar estándares como IEC 62443 y NIST SP 800-82, que abordan específicamente estos riesgos. La percepción de los encuestados también valida que la separación IT/OT no es solo una recomendación técnica, sino una estrategia clave para proteger la infraestructura crítica de la organización.

Ilustración 14. Implementación de Estrategias



El gráfico de distribución porcentual revela que el 42.9 % de los encuestados indicó que ya ha implementado una estrategia de segmentación entre redes IT y OT, lo cual representa un avance significativo hacia la mejora de la ciberseguridad industrial. Este grupo posiblemente cuenta con lineamientos, controles y políticas activas que delimitan claramente los entornos tecnológicos, reduciendo la superficie de ataque y mejorando la resiliencia operativa.

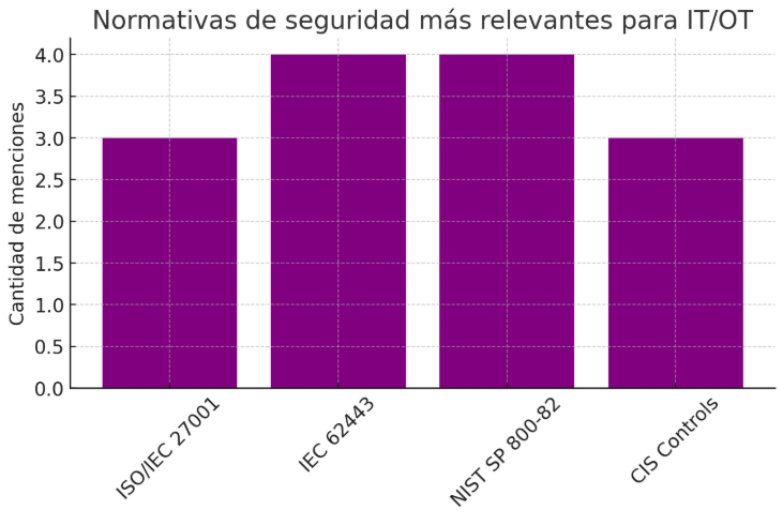
Por otro lado, un 28.6 % manifestó que aún no se ha implementado ninguna estrategia formal, lo que puede indicar brechas organizacionales, desconocimiento del riesgo o falta de prioridad institucional sobre el tema. Este segmento representa una zona crítica que debe ser atendida mediante procesos de concienciación, evaluación de riesgos y apoyo de la alta dirección.

El restante 28.6 % señaló que su organización está actualmente en proceso de implementación, lo que denota una transición positiva hacia la adopción de prácticas más seguras.

En conjunto, los resultados muestran que, aunque una parte importante de las organizaciones ha tomado acciones concretas, aún existe un porcentaje significativo que requiere soporte estratégico, técnico y normativo para lograr una implementación

completa y efectiva de la segmentación IT/OT. Esto refuerza la importancia de impulsar políticas institucionales y programas de fortalecimiento de capacidades en el ámbito de la ciberseguridad industrial.

Ilustración 15. Normativas



Los resultados obtenidos muestran una clara preferencia por normativas especializadas en entornos industriales y de control, particularmente aquellas que abordan explícitamente los desafíos de ciberseguridad en la convergencia entre IT y OT.

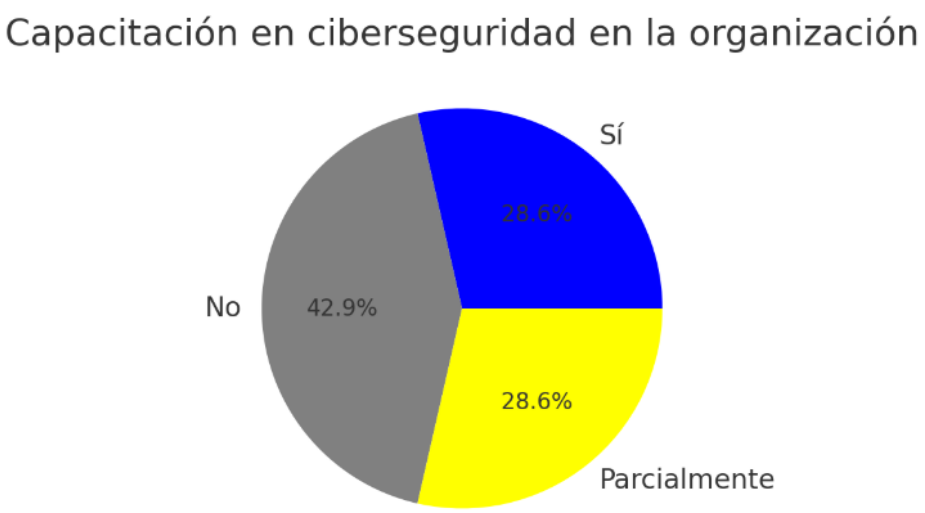
Las normas IEC 62443 y NIST SP 800-82 fueron las más mencionadas, con 4 votos cada una, lo que refleja el reconocimiento de los encuestados hacia marcos normativos diseñados específicamente para proteger sistemas de automatización y control industrial. Esto indica una comprensión adecuada sobre la necesidad de adoptar enfoques de seguridad que consideren la criticidad de los procesos OT y la interoperabilidad con entornos IT.

Por su parte, ISO/IEC 27001 y los CIS Controls recibieron 3 menciones cada uno. Aunque estos marcos no están enfocados exclusivamente en entornos OT, siguen siendo percibidos como fundamentales para establecer políticas de gestión de la

seguridad de la información, controles técnicos básicos y prácticas organizacionales sólidas. Su inclusión sugiere que los participantes valoran un enfoque integrado y complementario entre normas generales de ciberseguridad y marcos especializados.

Este resultado resalta la importancia de aplicar una combinación de normativas para abordar de manera integral los riesgos tecnológicos. La adopción de normas como IEC 62443 y NIST SP 800-82 permite asegurar entornos OT frente a amenazas operativas, mientras que marcos como ISO/IEC 27001 y CIS Controls fortalecen la gobernanza de seguridad en todo el ecosistema digital de la organización.

Ilustración 16. Capacitación



Se refleja una situación preocupante en cuanto a la preparación del personal frente a amenazas cibernéticas, especialmente en entornos industriales donde convergen redes IT y OT. El 42.9 % de los encuestados indicó que su organización no cuenta con programas de capacitación en ciberseguridad, lo cual evidencia una brecha crítica en la formación del talento humano frente a riesgos crecientes y sofisticados en la infraestructura tecnológica.

Por otro lado, un 28.6 % señaló que existe capacitación parcial, lo que sugiere la presencia de esfuerzos aislados o no sistemáticos, posiblemente limitados a ciertos roles o departamentos. Este grupo puede beneficiarse de programas estructurados que incluyan normativas específicas como ISO/IEC 27001, IEC 62443 o guías NIST para fortalecer la comprensión y las competencias técnicas.

Finalmente, solo un 28.6 % manifestó que su organización sí cuenta con una capacitación adecuada, lo que representa una oportunidad para que este grupo actúe como referente interno, compartiendo buenas prácticas y apoyando la creación de una cultura organizacional de ciberseguridad.

En conjunto, este resultado pone en evidencia la necesidad de desarrollar un plan integral de formación continua en ciberseguridad industrial, orientado a todos los niveles de la organización. Esta es una condición esencial para fortalecer la resiliencia, minimizar errores humanos y garantizar una correcta implementación de estrategias de segmentación y protección en entornos IT/OT.

3.3. Procedimiento de investigación

Fase 1: Evaluación de arquitectura de red de EMELNORTE

Se evaluó la infraestructura de red existente en EMELNORTE, incluyendo la topología, equipos de red y protocolos utilizados.

Se realizó encuestas al personal técnico de EMELNORTE que está familiarizado con la arquitectura de red actual. Esto proporcionó información detallada sobre cómo se diseñó, implementó y opera la red actualmente.

Se realizó un análisis de los riesgos de ciberseguridad asociados con la red actual, considerando tanto los servicios de red IT como los OT. Identificando posibles

vulnerabilidades y amenazas que podrían afectar la seguridad de la red y los sistemas de control.

Se comparó la arquitectura de red actual de EMELNORTE con las mejores prácticas y estándares de la industria en términos de ciberseguridad y eficiencia operativa, como lo es el modelo Purdue.

Fase 2: Diseño de modelo de arquitectura de redes que permitan la separación efectiva de los servicios de IT (Information Technology) (IT) y tecnologías operativas OT (Operational Technology) (OT)

Se identificó y documentó los requisitos específicos para la separación efectiva de los servicios de IT y OT en EMELNORTE. Esto incluyó los requisitos de seguridad, de rendimiento y de disponibilidad.

Se realizó un análisis de los riesgos asociados con la interconexión de los servicios de IT y OT en la red actual de EMELNORTE. Se identificó posibles vulnerabilidades y amenazas que podrían afectar la seguridad y la operatividad de los sistemas.

Se investigó las mejores prácticas y estándares de la industria en términos de arquitectura de redes para la separación efectiva de servicios de IT y OT. Se incluyó estándares como el IEC 62443, NIST SP 800-82, y modelo Purdue.

Se diseñó una arquitectura de red que permite la separación efectiva de los servicios de IT y OT en EMELNORTE. Se incluyó la segmentación de la red, la implementación de firewalls y otros dispositivos de seguridad y la definición de políticas de acceso.

Se tomó en cuenta la infraestructura de red existente en EMELNORTE al diseñar la nueva arquitectura. Se determinó qué aspectos de la infraestructura actual pueden reutilizarse y qué aspectos necesitan ser actualizados o reemplazados.

Fase 3: Definición de medidas de seguridad cibernética en redes IT y OT

Se realizó un inventario de los activos críticos de información y de infraestructura en las redes IT y OT de EMELNORTE. Esto incluye equipos de red, sistemas de control industrial, bases de datos y aplicaciones.

Basándose en los resultados del análisis de riesgos, se definen controles de seguridad adecuados para mitigar los riesgos identificados. Esto incluyó controles técnicos, como firewalls, sistemas de detección de intrusos, sistemas de prevención de intrusiones, cifrado de datos, y controles de acceso físico, así como controles organizativos y de procedimiento.

Se consideró sistemas de monitorización de seguridad en tiempo real y sistemas de detección de intrusiones para identificar y responder rápidamente a posibles amenazas cibernéticas en las redes IT y OT.

Fase 4: Evaluación del impacto del plan de separación de redes en eficiencia operativa y la ciberseguridad de EMELNORTE

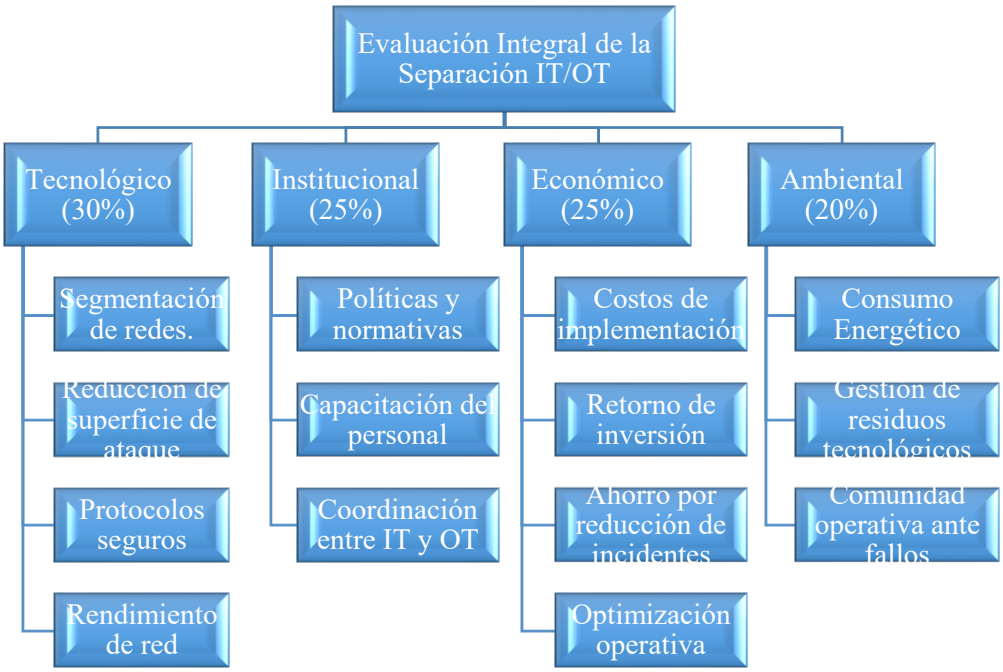
Se validó el diseño de la nueva arquitectura de red mediante pruebas y simulaciones en un entorno controlado. Verificando que el diseño cumple con los requisitos identificados y es capaz de mitigar los riesgos de seguridad identificados.

Se presentó el diseño de la nueva arquitectura de red a los responsables de EMELNORTE, incluyendo a los responsables de seguridad de la información,

operaciones de red, y departamento SCADA. Se obtiene la aprobación antes de proceder con la implementación.

Se documentó el diseño de la nueva arquitectura de red en detalle, incluyendo diagramas de red, especificaciones técnicas, políticas y procedimientos. Esto para facilitar la implementación y la gestión continua.

Ilustración 17. Evaluación del Impacto



3.4. Consideraciones Bioéticas

Las consideraciones bioéticas para el presente plan no fueron el enfoque principal del estudio, ya que el tema está más relacionado con aspectos técnicos y de seguridad informática en el ámbito empresarial. Sin embargo, se pudo identificar algunas consideraciones bioéticas relevantes, especialmente en relación con la privacidad, la seguridad de los datos y el impacto en los empleados y la comunidad en general.

Privacidad y Protección de Datos: La separación de redes IT y tecnologías operativas OT implicó el manejo de información confidencial y sensible. Fue importante garantizar que se respeten las normativas de privacidad de datos y que se implementen medidas adecuadas para proteger la información personal de los empleados y clientes.

Transparencia y Consentimiento Informado: Fue crucial informar a todas las partes interesadas sobre los cambios propuestos en la infraestructura de red y obtener su consentimiento informado. Esto incluye a los empleados que puedan verse afectados por la separación de redes.

Equidad y Acceso: Se consideró que la separación de redes IT y tecnologías operativas OT tubo impacto en la equidad de acceso a los servicios eléctricos, especialmente en comunidades vulnerables o con recursos limitados. Es importante garantizar que todas las comunidades tengan acceso equitativo y continuo a la electricidad, independientemente de los cambios en la infraestructura tecnológica.

Responsabilidad Social Corporativa: EMELNORTE tiene la responsabilidad de operar de manera ética y contribuir al bienestar de la comunidad. Es importante que se consideró cómo la separación de redes IT y tecnologías operativas OT pudo afectar el cumplimiento de esta responsabilidad y con ello se pudo mitigar los impactos negativos.

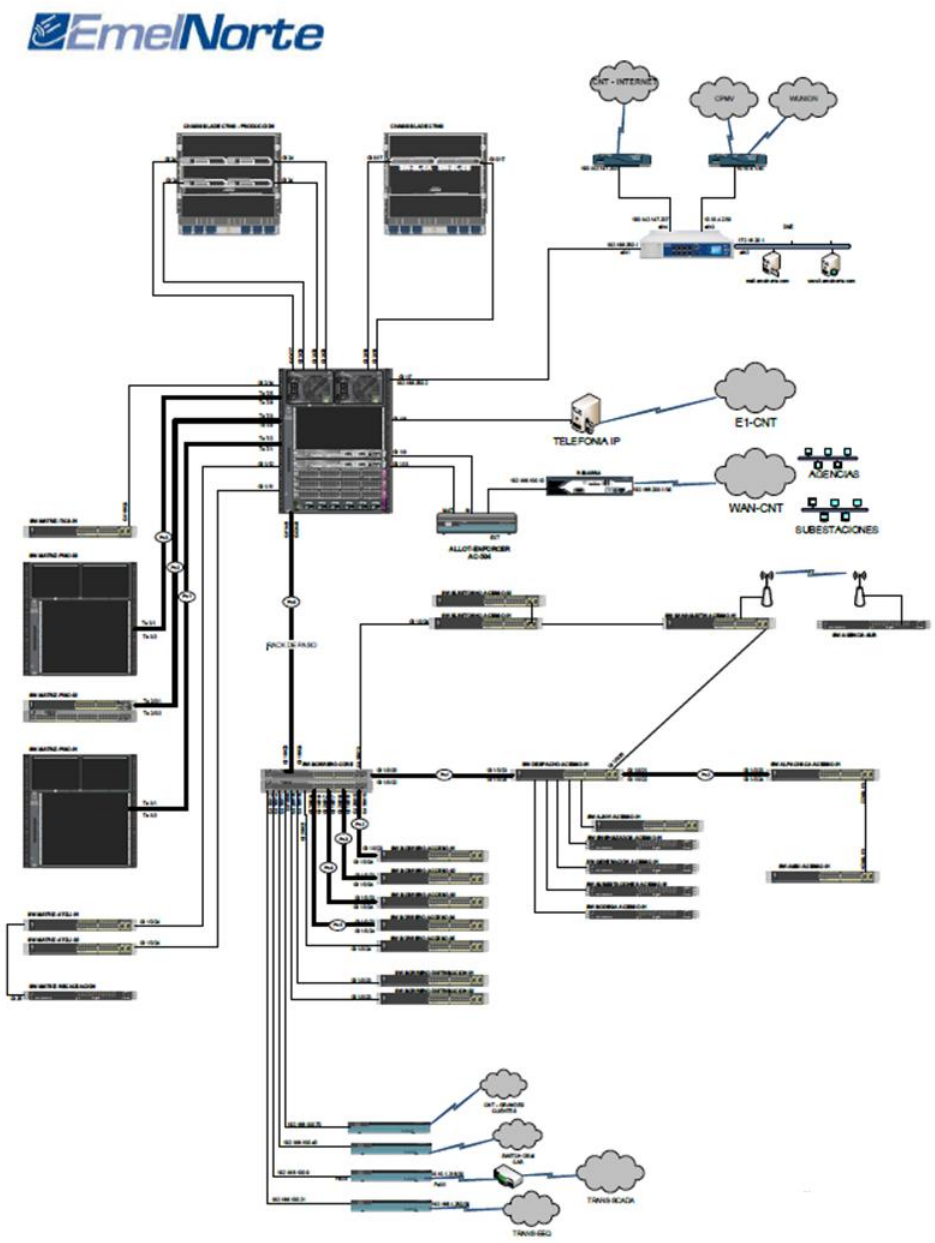
CAPITULO IV

4.1. Evaluación de arquitectura actual de red de EMELNORTE

El objetivo de la evaluación de arquitectura de red en el contexto del plan de separación de servicios IT (Tecnología de la Información) y OT (Tecnología Operativa) en la Empresa Eléctrica Regional Norte S.A. (EMELNORTE) es analizar la infraestructura de red existente para identificar áreas de integración entre servicios IT y OT, así como posibles vulnerabilidades de seguridad asociadas. Esta evaluación busca proporcionar una comprensión detallada de la arquitectura de red actual, destacando los puntos críticos que podrían afectar la ciberseguridad y la eficiencia operativa. Con estos hallazgos, se pretende informar la implementación de medidas de separación de servicios IT y OT para mejorar la seguridad y la gestión operativa de la red de EMELNORTE.

Se examina la estructura y disposición de los dispositivos de red, incluyendo routers, switches, firewalls y servidores, para comprender cómo están interconectados y cómo fluye el tráfico de datos entre ellos.

Ilustración 18. Diagrama de Red Actual



4.1.1. Descripción de los hallazgos

En la arquitectura de red de EMELNORTE se puede observar que no se sigue el modelo Purdue de referencia para arquitecturas de control industrial.

Se pueden señalar diferencias en la estructura y organización de la red en comparación con las capas definidas en el modelo Purdue, como la falta de una

separación clara entre las capas de proceso, supervisión y control, y la capa de negocios/empresa.

Identificación de interconexiones directas entre los sistemas de IT y los sistemas OT sin una segmentación clara entre ellas.

Puntos donde los sistemas de TI, como servidores de administración y aplicaciones corporativas, están conectados directamente a los sistemas de control industrial, lo que indica una integración no adecuada y un riesgo potencial para la seguridad.

Observación de comunicaciones directas entre dispositivos y sistemas de IT y OT sin pasar por dispositivos de seguridad intermedios, como firewalls o gateways, lo que aumenta el riesgo de ataques cibernéticos y fallos operativos.

La ausencia de segmentación de redes físicas o lógicas entre los entornos de IT y OT facilita la propagación de amenazas y la interferencia entre sistemas críticos de producción y sistemas empresariales.

Para evitar las conexiones entre las redes IT y OT, se cuenta con la configuración de listas de acceso en el Switch de Core que no es lo óptimo porque se experimenta complejidad en la configuración. Esto puede requerir un conocimiento detallado de la red y de los requisitos de seguridad, así como un tiempo considerable para su implementación y gestión. Las listas de acceso pueden afectar el rendimiento del switch de core al procesar el tráfico de red y aplicar las reglas definidas en las ACLs. Esto puede provocar una degradación del rendimiento, especialmente en switches con recursos limitados o cuando se aplican reglas complejas que implican un procesamiento intensivo. Además, la configuración incorrecta de las ACLs puede resultar en errores que podrían afectar la conectividad de la red y comprometer su

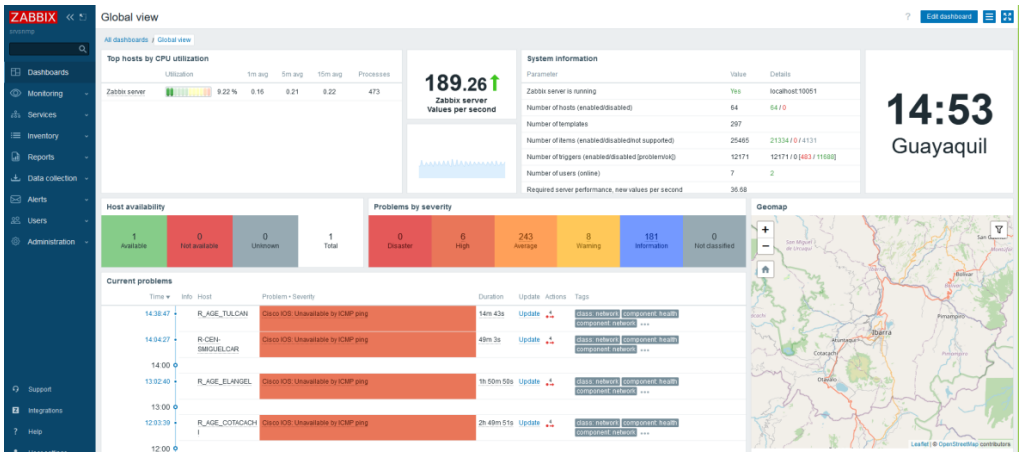
seguridad. Por ejemplo, una regla mal configurada podría bloquear el tráfico legítimo o permitir el acceso no autorizado a recursos sensibles.

4.1.2. Análisis de Tráfico

Con la finalidad de definir los equipos necesarios para la ejecución adecuada de la separación de redes IT y OT se analizaron los tráficos de red actuales, con la ayuda de herramientas existentes en EMELNORTE.

Se realizó la revisión de los enlaces para analizar el tráfico en recibido que permite validar el thoughput de EMELNORTE, mediante la aplicación ZABBIX.

Ilustración 19. Pantalla Principal ZABBIX



Para determinar el throughput se tomó la información de un año y se consideró el crecimiento del 5 % anual, a continuación, el detalle:

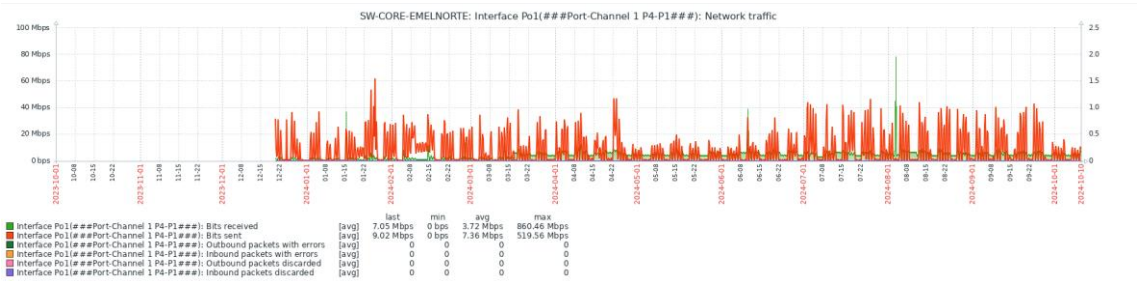
Ilustración 20. Resumen Throughput de Enlaces

Nro	Port Chanel	Descripción	MAX recieved	
1	Po1	P4-P1	860,46	Mbps
2	Po2	P4-P2	845,86	Mbps
3	Po3	P4-P3	959,18	Mbps
4	Po4	P4-4500	1239,04	Mbps
5	Po5	P4-3800	1064,96	Mbps
6	Po6	BORRERO B	544,32	Mbps
7	Po7	WLC	513,86	Mbps
8	Po8	TRUNK MX	996,90	Mbps
9	Po9	P4-9300	469,98	Mbps
10	Te 1/0/6	CHK	323,91	Mbps
11	Te 2/0/6	CHK	100,71	Mbps
12	CNT - WAN		31,34	Mbps
13	Internet - Backup		150,00	Mbps

TOTAL Po		8100,52	Mbps
Crecimiento 25%		2025,13	Mbps
CON CRECIMIENTO		10125,65	Mbps

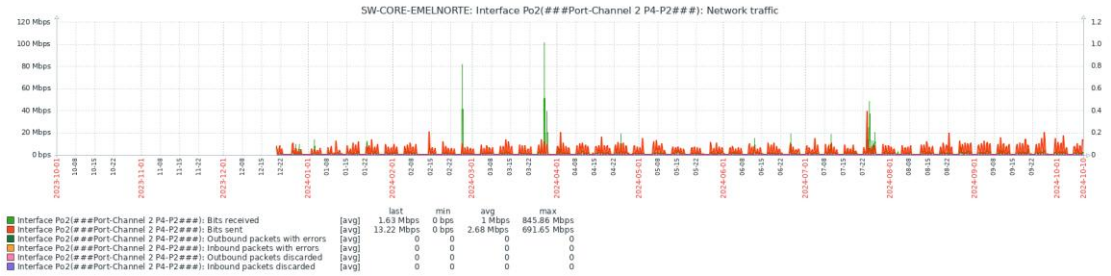
Throughput máximo recibido	9,89	**Gbps**

Ilustración 21. Tráfico SW-CORE: Po1 (PISO_4 – PISO_1)



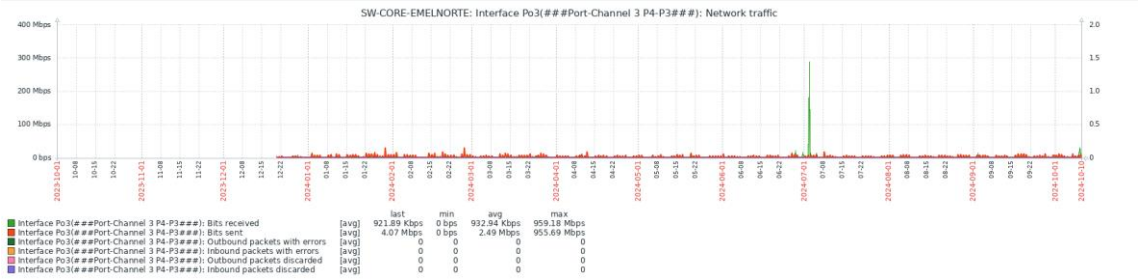
Tráfico de red entre el switch de core del piso 4 y el switch de acceso del piso 1, la medición se realizó en el enlace EtherChannel Po1.

Ilustración 22. Tráfico SW-CORE: Po2 (PISO_4 – PISO_2)



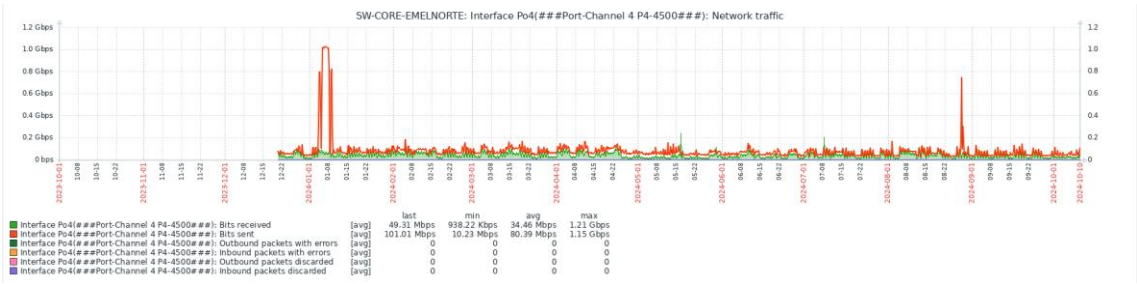
Tráfico de red entre el switch de core del piso 4 y el switch de acceso del piso 2, la medición se realizó en el enlace EtherChannel Po2.

Ilustración 23. Tráfico SW-CORE: Po3 (PISO_4 – PISO_3)



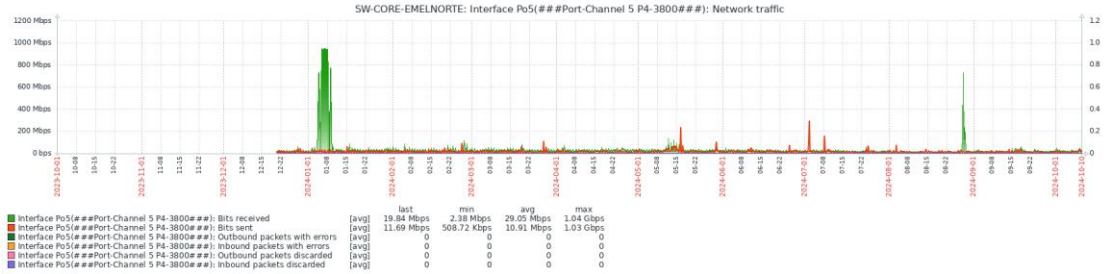
Tráfico de red entre el switch de core del piso 4 y el switch de acceso del piso 3, la medición se realizó en el enlace EtherChannel Po3.

Ilustración 24. Tráfico SW-CORE: Po4 (PISO_4 - SW_DISTRIBUCIÓN_1)



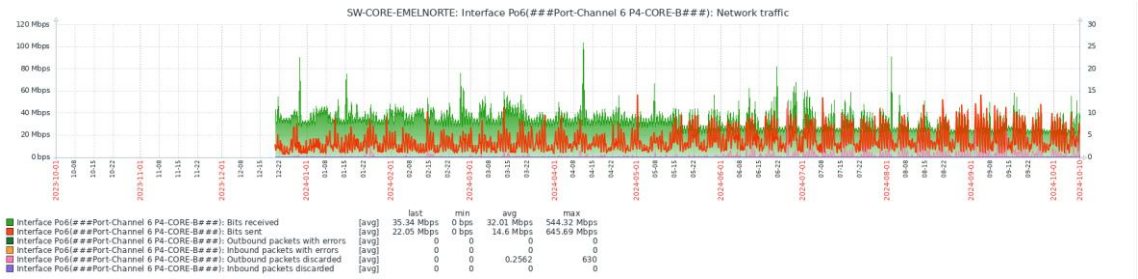
Tráfico de red entre el switch de core del piso 4 y el switch de distribución uno del piso 4, la medición se realizó en el enlace EtherChannel Po4.

Ilustración 25. Tráfico SW-CORE: Po5 (PISO_4 - SW_DISTRIBUCIÓN_2)



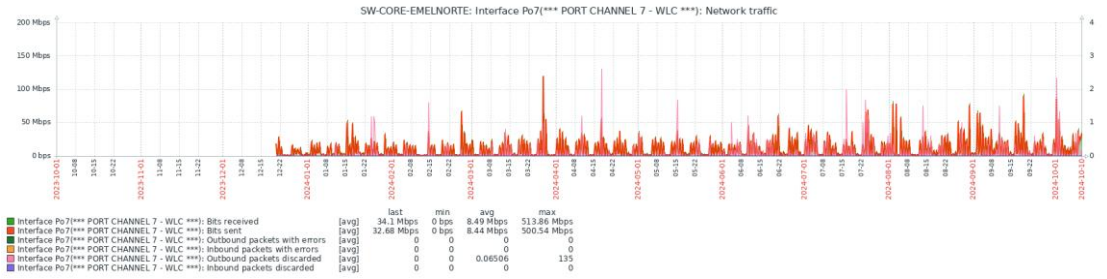
Tráfico de red entre el switch de core del piso 4 y el switch de distribución dos del piso 4, la medición se realizó en el enlace EtherChannel Po5.

Ilustración 26. Tráfico SW-CORE: Po6 (ED_MATRIZ - ED_BORRERO)



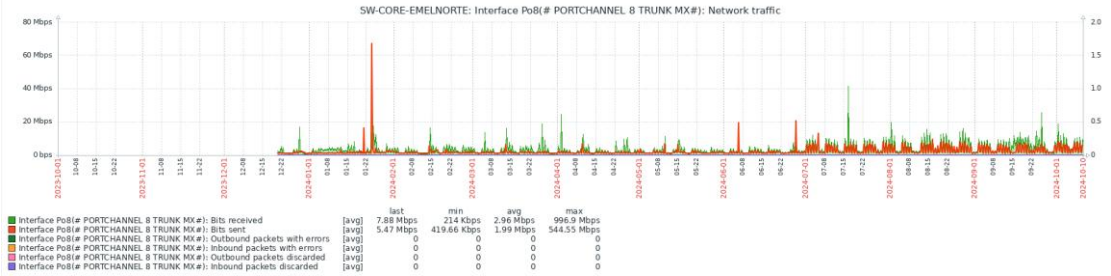
Tráfico de red entre el switch de core del Edificio Matriz y el switch core del Edificio Borrero, la medición se realizó en el enlace EtherChannel Po6.

Ilustración 26. Tráfico SW-CORE: Po7 (WIRELESS_LAN_CONTROLLER)



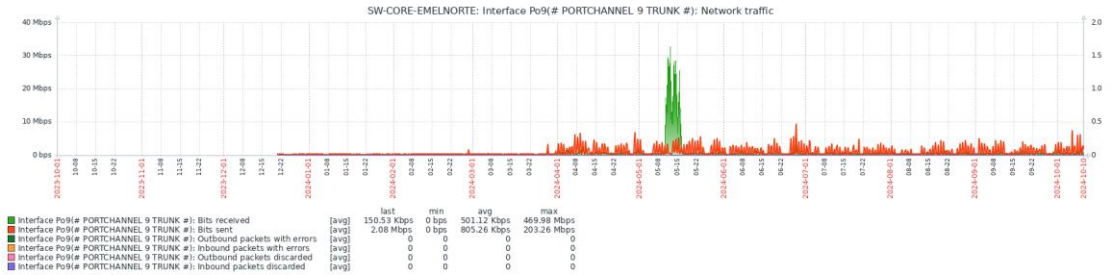
Tráfico de red entre el switch de core del piso 4 y la controladora Wireless, la medición se realizó en el enlace EtherChannel Po7.

Ilustración 27. Tráfico SW-CORE: Po8 (SW_CORE – CHASIS_SERVIDORES_BLADE)



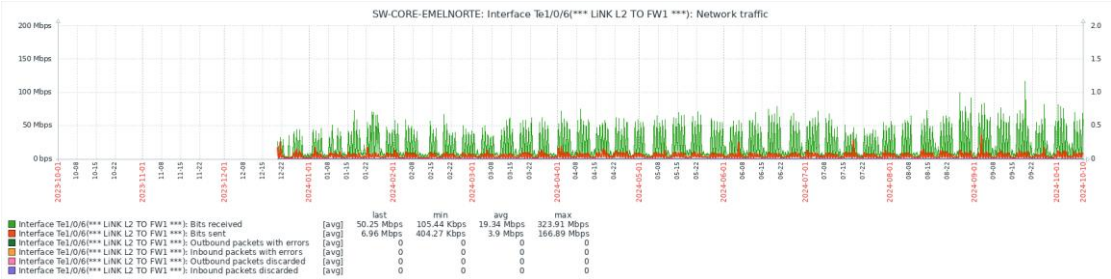
Tráfico de red entre el switch de core del piso 4 y el switch del chasis de servidores, la medición se realizó en el enlace EtherChannel Po8.

Ilustración 28. Tráfico SW-CORE: Po9 (PISO_4 - SW_DISTRIBUCIÓN_3)



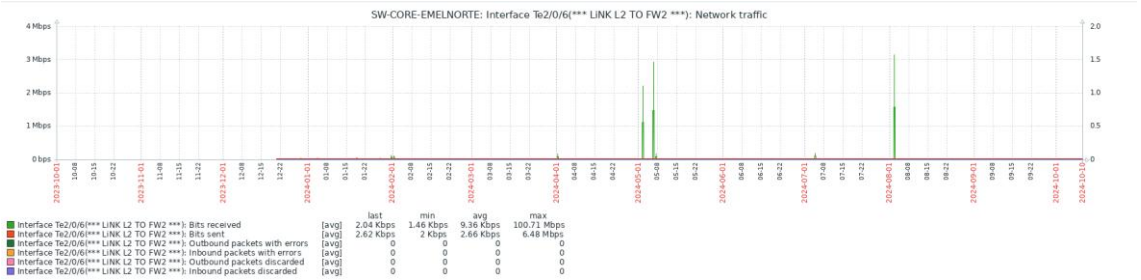
Tráfico de red entre el switch de core del piso 4 y el switch de distribución tres del piso 4, la medición se realizó en el enlace EtherChannel Po9.

Ilustración 29. Tráfico SW-CORE: Interface Te1/0/6 (CONEXIÓN_FIREWALL_1)



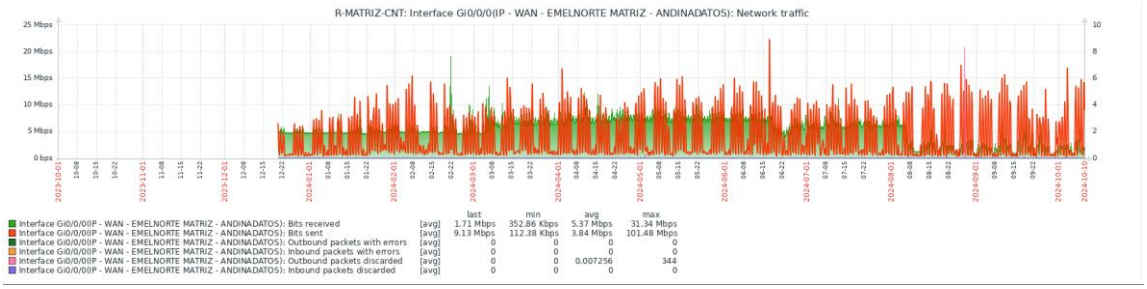
Tráfico de red entre el switch de core del piso 4 y el firewall perimetral 1, la medición se realizó en la interface TenGigabit.

Ilustración 30. Tráfico SW-CORE: Interface Te2/0/6 (CONEXIÓN_FIREWALL_2)



Tráfico de red entre el switch de core del piso 4 y el firewall perimetral 2, la medición se realizó en la interface TenGigabit.

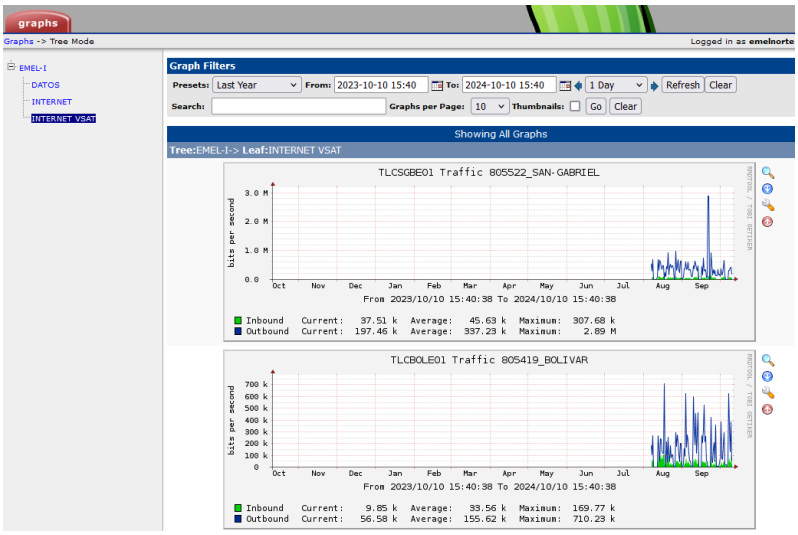
Ilustración 31. Tráfico-MATRIZ-CNT



Tráfico de red en el ruteador que se conecta el Edificio Matriz con las Agencias, Subestaciones y Centrales.

Se realizó la revisión de los enlaces de las subestaciones y centrales para analizar el tráfico en recibido que permite validar el thoughput de la red OT de EMELNORTE, mediante el enlace al CACTI que proporciona CNT para la validación en el enlace: https://cacti-corp.fastboy.com.ec/index.php

Ilustración 32. Pantalla principal CACTI



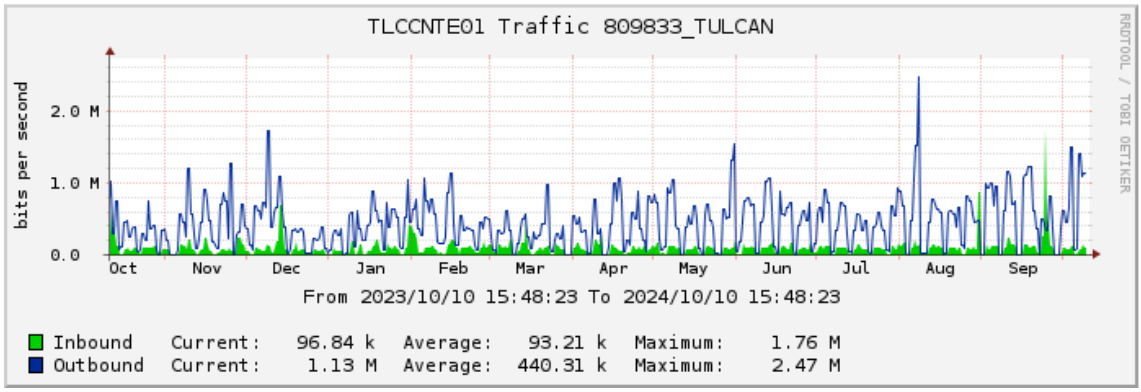
Para la determinación del throughput de los datos de OT se tomó la información de un periodo de año y se consideró el crecimiento del 5 % anual, a continuación, el detalle:

Ilustración 33. Throughput máximo recibido

Nro	Ubicación	MAX Throughput	
1	SUB-TULCAN	2.529,28	Kbps
2	SUB-EL-ROSAL	1.105,92	Kbps
3	SUB-SAN-GABRIEL	200,50	Kbps
4	SUB-ATUNTAQUI	507,69	Kbps
5	SUB-CAYAMBE	493,19	Kbps
6	SUB-EL-ANGEL	269,69	Kbps
7	SUB-LA-CAROLINA	49,73	Kbps
8	SUB-COTACACHI	7.116,80	Kbps
9	SUB-OTAVALO	917,00	Kbps
10	SUB-SAN-VICENTE	210,46	Kbps
11	SUB-LA-ESPERANZA	1.300,48	Kbps
12	SUB-CANANVALLE	288,34	Kbps
13	SUB-EL-CHOTA	1.064,96	Kbps
14	CEN-SAN-MIGUEL-INTERNET	1.802,24	Kbps
15	CEN-BUENOS-AIRES-INTERNET	1.443,84	Kbps
16	CEN-LA-PLAYA	775,14	Kbps
17	CEN-SAN-MIGUEL-DATOS	2.488,32	Kbps
18	CEN-BUENOS-AIRES-DATOS	45,70	Kbps
19	CENTRAL AMBI	91.934,72	Kbps

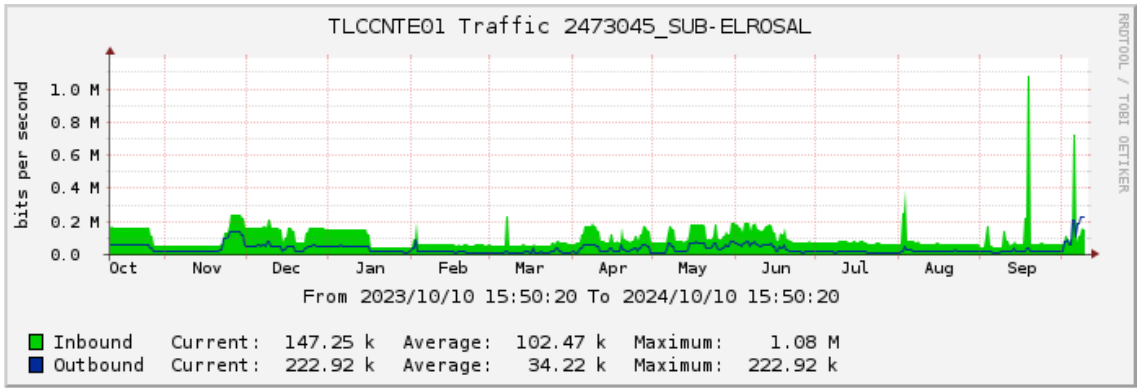
	114544	Kbps
TOTAL SUB Y CEN	111,86	Mbps
Crecimiento 25%	27,96	Mbps
CON CRECIMIENTO	139,82	Mbps

Ilustración 34. Tráfico Subestación Tulcán



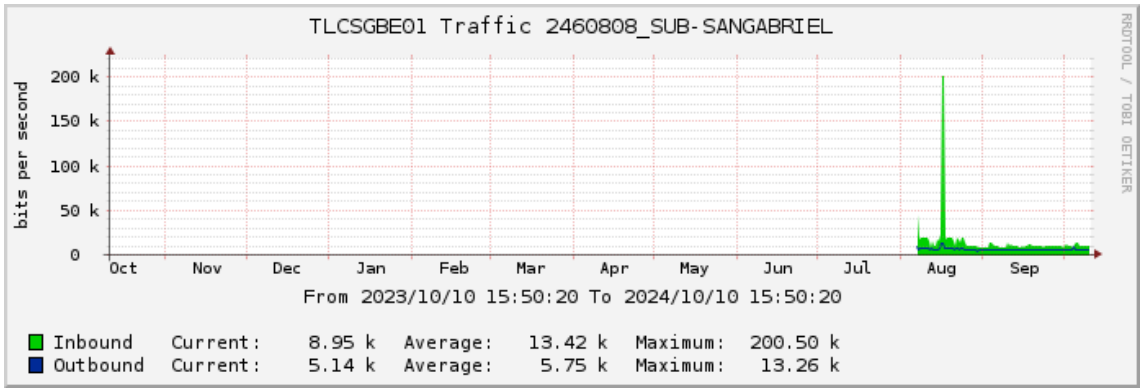
Tráfico de red de entrada y salida en la Subestación Tulcán, datos obtenidos de la plataforma del proveedor.

Ilustración 35. Tráfico Subestación El Rosal



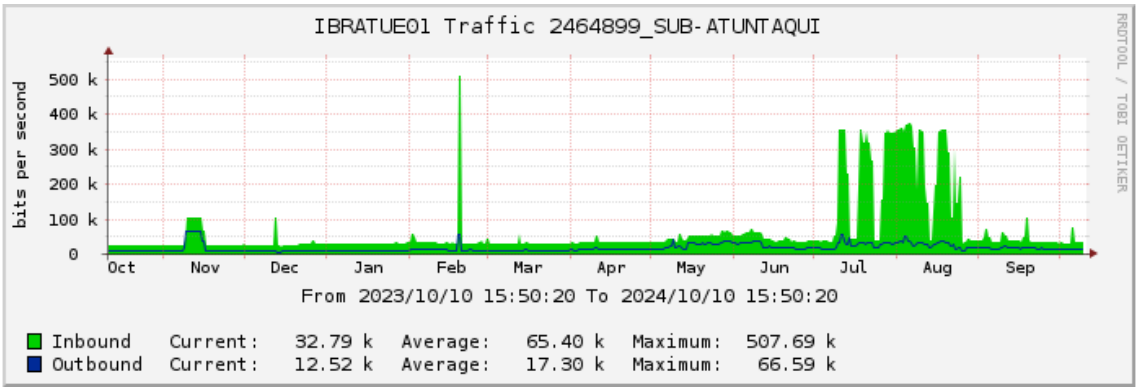
Tráfico de red en la Subestación El Rosal, datos obtenidos de la plataforma del proveedor.

Ilustración 36. Tráfico Subestación San Gabriel



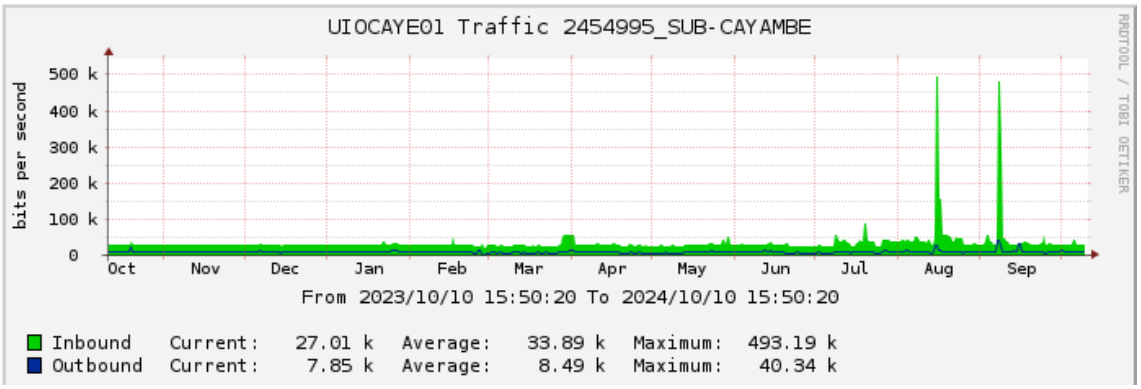
Tráfico de red de entrada y salida en la Subestación San Gabriel, datos obtenidos de la plataforma del proveedor.

Ilustración 37. Tráfico Subestación Atuntaqui



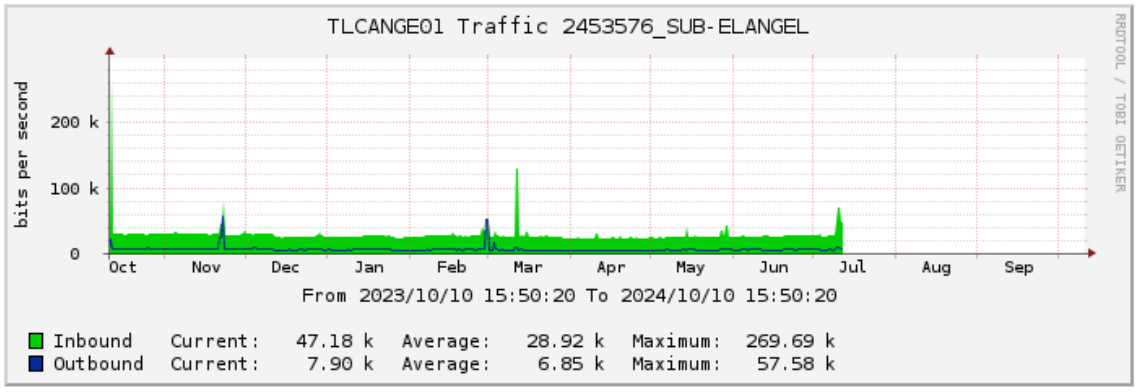
Tráfico de red de entrada y salida en la Subestación Atuntaqui, datos obtenidos de la plataforma del proveedor.

Ilustración 38. Tráfico Subestación Cayambe



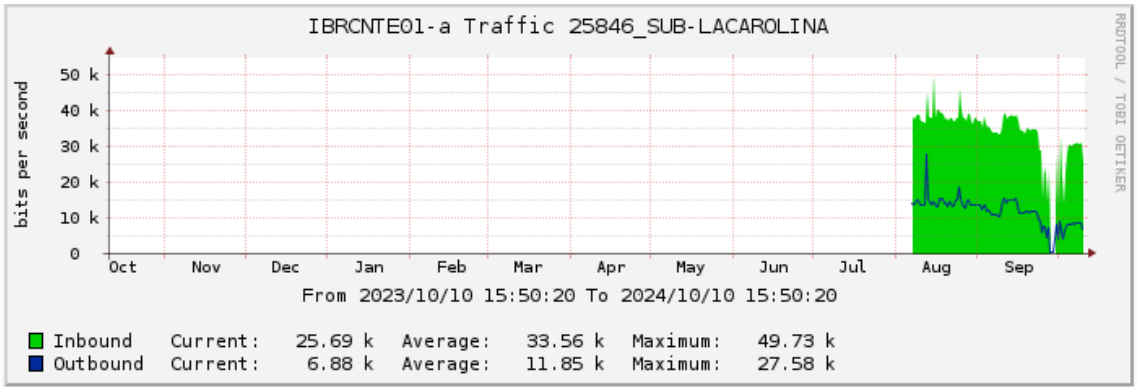
Tráfico de red de entrada y salida en la Subestación Cayambe, datos obtenidos de la plataforma del proveedor.

Ilustración 39. Tráfico Subestación El Ángel



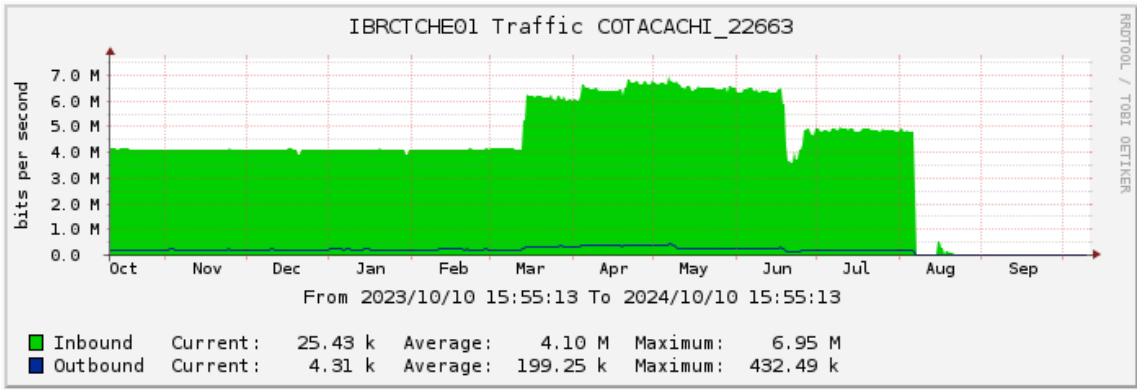
Tráfico de red de entrada y salida en la Subestación El Ángel, datos obtenidos de la plataforma del proveedor.

Ilustración 40. Tráfico Subestación La Carolina



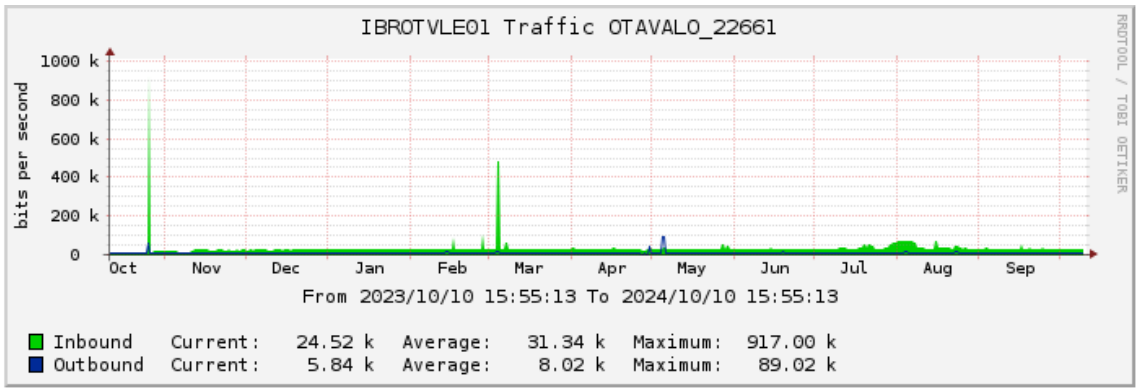
Tráfico de red de entrada y salida en la Subestación La Carolina, datos obtenidos de la plataforma del proveedor.

Ilustración 41. Tráfico Subestación Cotacachi



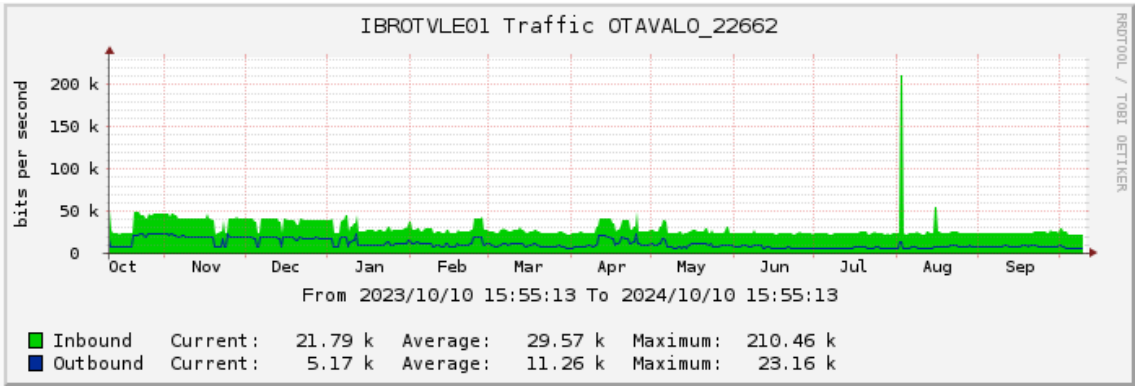
Tráfico de red de entrada y salida en la Subestación Cotacachi, datos obtenidos de la plataforma del proveedor.

Ilustración 42. Tráfico Subestación Otavalo



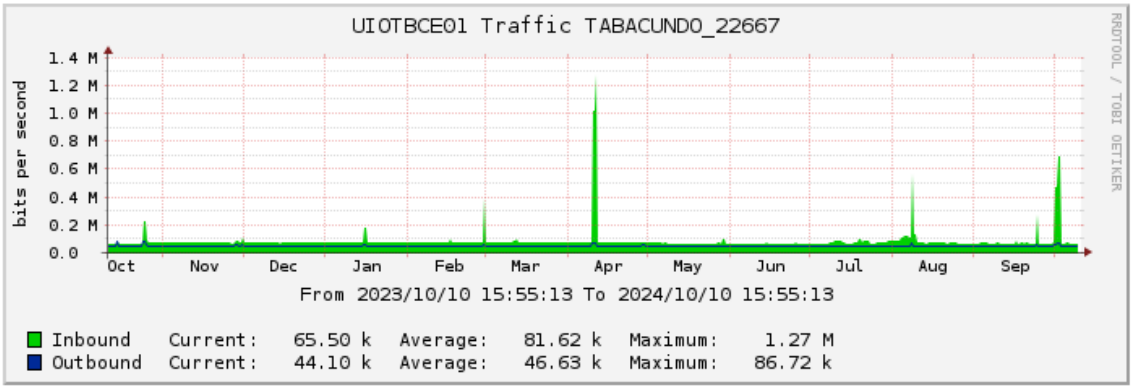
Tráfico de red de entrada y salida en la Subestación Otavalo, datos obtenidos de la plataforma del proveedor.

Ilustración 43. Tráfico Subestación San Vicente



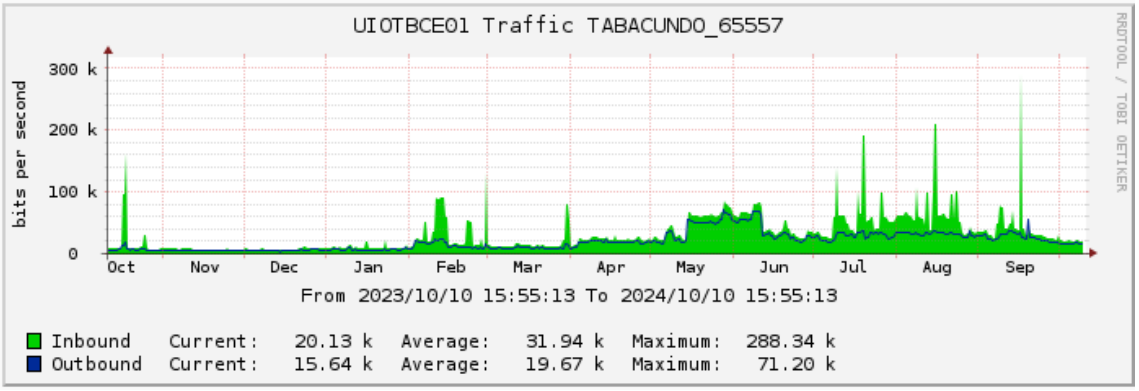
Tráfico de red de entrada y salida en la Subestación San Vicente, datos obtenidos de la plataforma del proveedor.

Ilustración 44. Tráfico Subestación La Esperanza



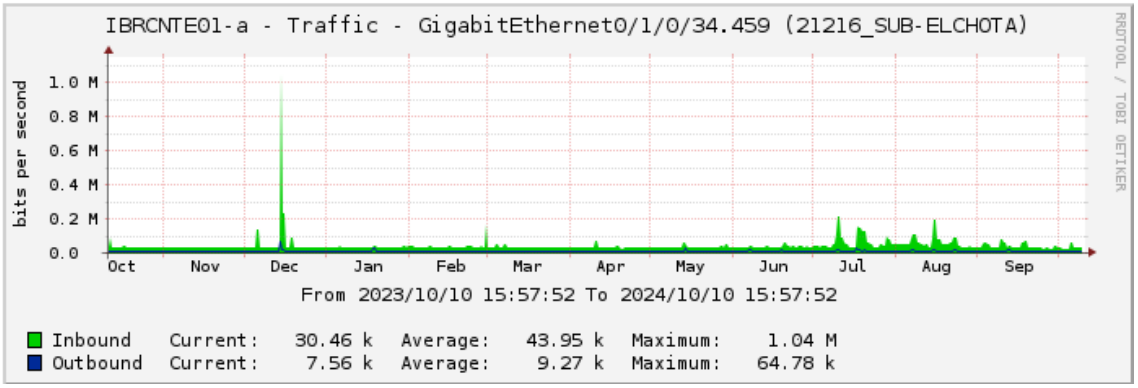
Tráfico de red de entrada y salida en la Subestación La Esperanza, datos obtenidos de la plataforma del proveedor.

Ilustración 45. Tráfico Subestación Cananvalle



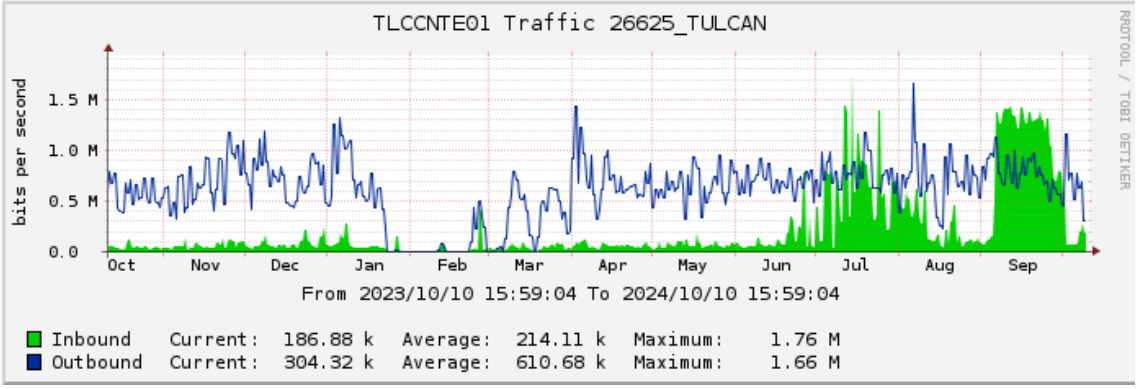
Tráfico de red de entrada y salida en la Subestación Cananvalle, datos obtenidos de la plataforma del proveedor.

Ilustración 46. Tráfico Subestación El Chota



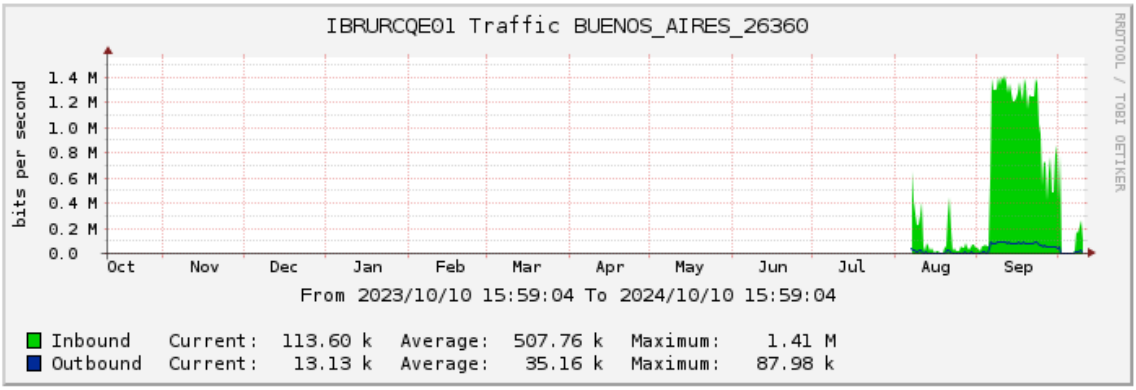
Tráfico de red de entrada y salida en la Subestación El Chota, datos obtenidos de la plataforma del proveedor.

Ilustración 47. Tráfico Central San Miguel de Car – Internet



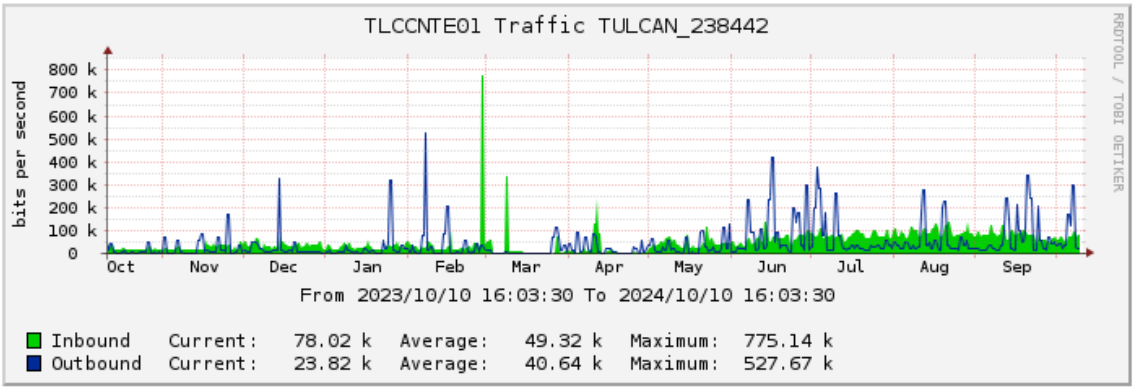
Tráfico de red, enlace de internet de entrada y salida en la Central San Miguel de Car, datos obtenidos de la plataforma del proveedor.

Ilustración 48. Tráfico Central Buenos Aires – Internet



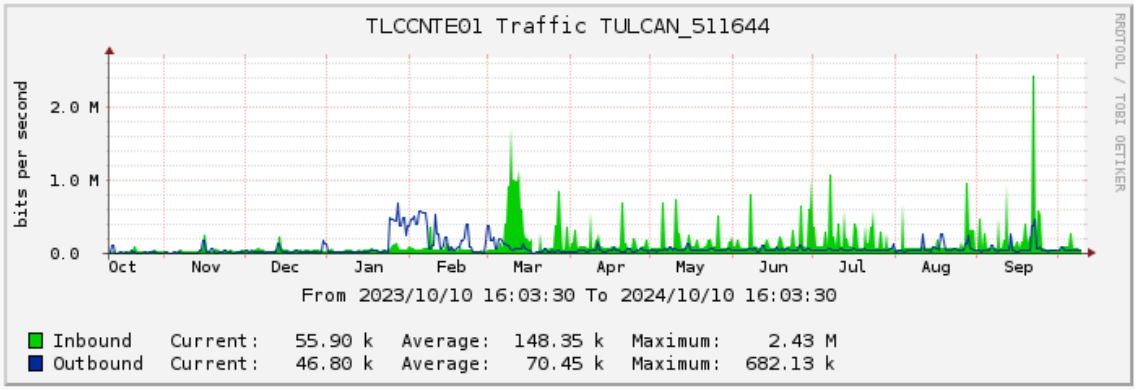
Tráfico de red, enlace de internet de entrada y salida en la Central Buenos Aires, datos obtenidos de la plataforma del proveedor.

Ilustración 49. Tráfico Central La Playa



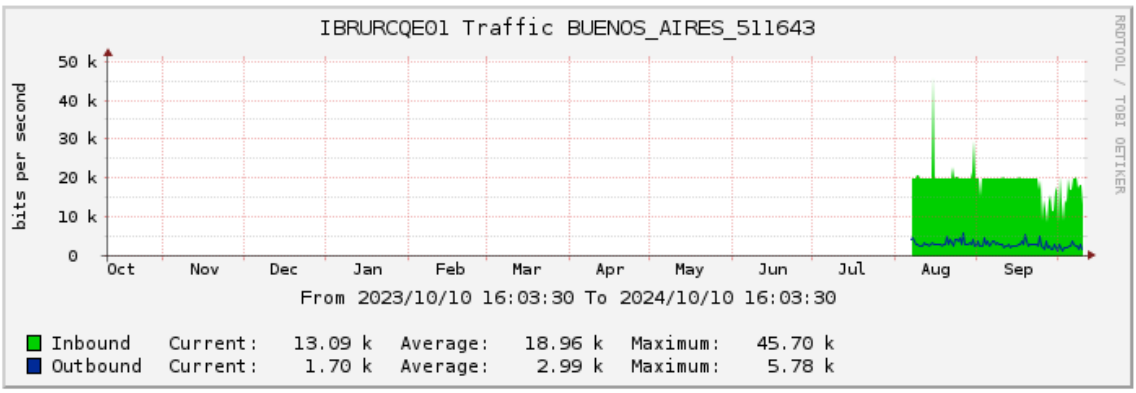
Tráfico de red de entrada y salida en la Central La Playa, datos obtenidos de la plataforma del proveedor.

Ilustración 50. Tráfico Central San Miguel de Car – Datos



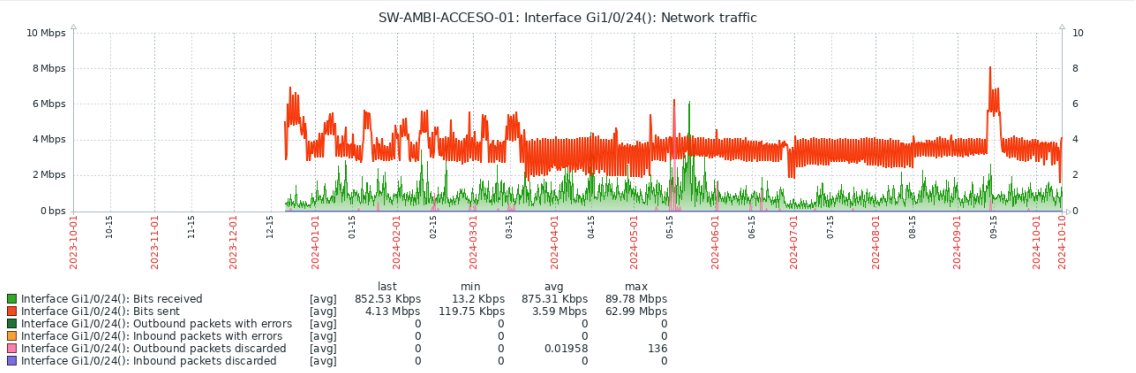
Tráfico de red de datos de entrada y salida en la Central San Miguel de Car, datos obtenidos de la plataforma del proveedor.

Ilustración 51. Tráfico Central Buenos Aires – Datos



Tráfico de red de datos de entrada y salida en la Central San Miguel de Car, datos obtenidos de la plataforma del proveedor.

Ilustración 52. Tráfico Central Ambi



Tráfico de red de datos de entrada y salida en la Central Ambi, datos obtenidos de la plataforma del proveedor.

4.2. Diseño de la arquitectura de red que permita la segmentación de los servicios de IT (Information Technology) (IT) y tecnologías operativas OT (Operational Technology) (OT)

El diseño propuesto para la arquitectura de redes en el contexto del plan de separación de servicios de IT y OT en EMELNORTE se fundamenta en varios principios clave para garantizar una separación efectiva y segura entre estas dos áreas tecnológicas críticas. A continuación, se proporciona una explicación detallada del modelo de arquitectura de redes diseñado, resaltando los elementos esenciales y la lógica subyacente:

4.2.1. Segmentación de redes

La base de la arquitectura de redes diseñada implica la segmentación clara y definida de las redes de IT y OT. Esto implica la creación de redes separadas y distintas para cada una de estas áreas tecnológicas. La segmentación permite aislar los sistemas y dispositivos de IT de aquellos utilizados en las operaciones operativas, reduciendo así el riesgo de intrusiones no autorizadas y minimizando la superficie de ataque.

4.2.2. Implementación de firewalls

Se propone la implementación de firewalls como una medida clave para reforzar la separación entre las redes IT y OT. Estos dispositivos permitirán controlar y filtrar el tráfico entre ambas redes, asegurando que solo se autorice el paso de datos legítimos y bloqueando cualquier intento de comunicación no autorizada. Además, los

firewalls permiten aplicar políticas avanzadas de seguridad, como la inspección profunda de paquetes (DPI), detección y prevención de intrusiones (IPS/IDS), así como la segmentación granular de redes. Para garantizar altos estándares de protección, se considera el uso de soluciones de fabricantes reconocidos en el Cuadrante Mágico de Gartner, como Palo Alto Networks y CheckPoint, los cuales ofrecen plataformas robustas y ampliamente validadas para entornos críticos de IT y OT.

4.2.3. Medidas de seguridad adicionales

Además de los firewalls, se considera la implementación de otras medidas de seguridad complementarias para fortalecer la separación de servicios de IT y OT. Esto puede incluir sistemas de detección y prevención de intrusiones (IDS/IPS), sistemas de gestión de identidad y acceso (IAM), sistemas de gestión de eventos e información de seguridad (SIEM). Estas medidas ayudan a monitorear y proteger las redes contra amenazas internas y externas.

4.2.4. Infraestructura de red adecuada

El diseño de la arquitectura de redes también requiere una infraestructura de red robusta y escalable que admita la separación efectiva de servicios de IT y OT. Esto puede implicar la implementación de tecnologías de red como VLANs (Virtual LANs), enrutadores y conmutadores configurados para garantizar el tráfico segregado entre las redes de IT y OT. Además, se pueden considerar tecnologías de virtualización de red para facilitar la gestión y la flexibilidad operativa.

4.2.5. Amenazas específicas identificadas

El análisis de riesgos y vulnerabilidades asociados con la integración de los servicios de IT y OT en la red actual de EMELNORTE es crucial para comprender los posibles peligros y amenazas que podrían afectar la seguridad y operación del sistema. Se pueden presentar ataques de malware y ransomware, accesos no autorizados y ataques de denegación de servicio (DDoS).

4.2.6. Posibles impactos en la seguridad y operación del sistema

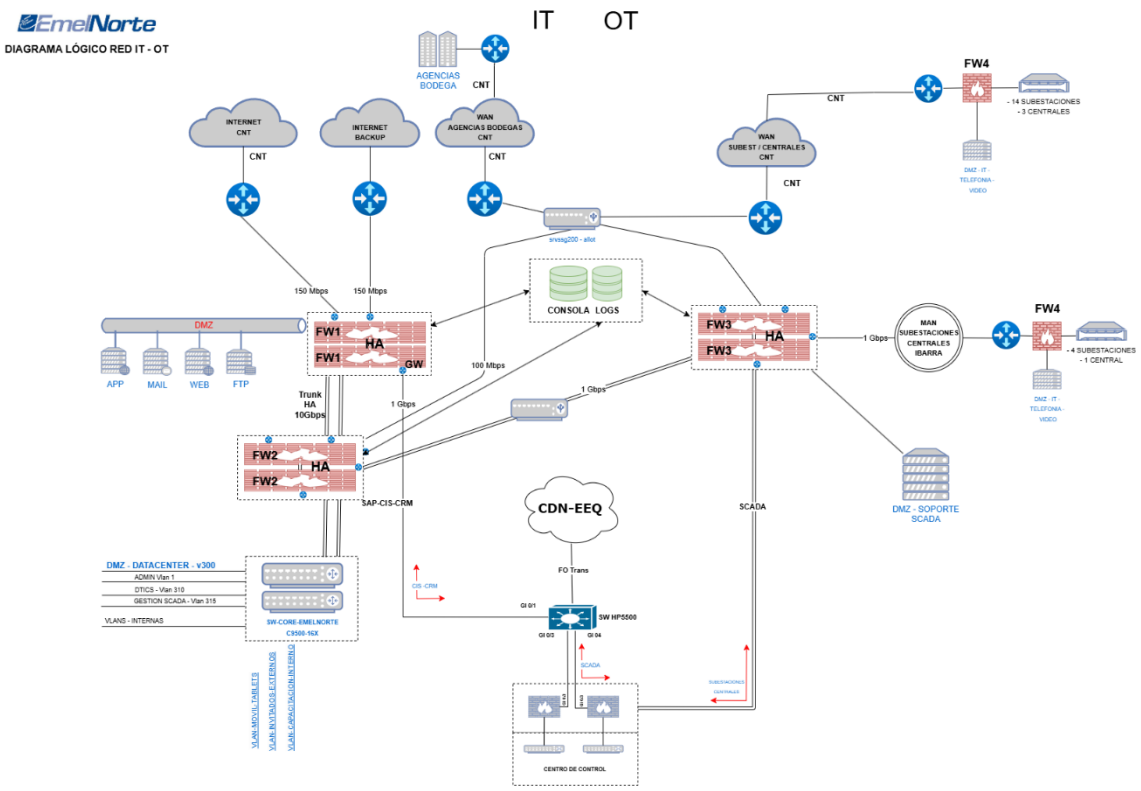
Se podrían presentar interrupciones en el servicio eléctrico, pérdida de datos críticos y daños en la reputación de la empresa.

4.2.7. Recomendaciones para mitigar los riesgos identificados

Se recomienda la implementación de medidas de seguridad robustas, como es la implantación de firewalls, sistemas de detección de intrusos, sistemas de prevención de intrusos y soluciones antivirus actualizadas para proteger tanto los sistemas de IT como de OT. Además de debe aplicar una segmentación adecuada de redes para limitar la comunicación entre los sistemas de IT y OT, reduciendo así la superficie de ataque y mitigando el impacto de posibles intrusiones. También es fundamental capacitar al personal sobre las mejores prácticas de seguridad cibernética, incluyendo la identificación de correos electrónicos de phishing, el uso seguro de contraseñas y la detección de actividad sospechosa en la red.

A continuación, se presenta la propuesta de arquitectura de red, considerando mitigar los riegos en la red de EMELNORTE.

Ilustración 53. Diagrama de Red Propuesto



4.2.8. Mejores prácticas y estándares de la industria

La separación efectiva de los servicios de IT y OT es fundamental para garantizar la seguridad cibernética y la eficiencia operativa en entornos industriales y de infraestructura crítica. Esta práctica es ampliamente recomendada por organismos como el National Institute of Standards and Technology (NIST), la International Society of Automation (ISA) y el Center for Internet Security (CIS), los cuales promueven arquitecturas segmentadas y controles estrictos entre dominios IT y OT. Entre las mejores prácticas y estándares recomendados se incluyen:

4.2.8.1. IEC 62443

Es una serie de estándares internacionales desarrollados por la Comisión Electrotécnica Internacional (IEC) que se centran en la ciberseguridad de los sistemas de automatización y control industrial (IACS, por sus siglas en inglés). Estos

estándares proporcionan directrices y mejores prácticas para proteger los sistemas de control industrial contra amenazas cibernéticas. En términos de arquitectura de redes para la separación efectiva de servicios de IT y OT, los estándares IEC 62443 ofrecen las siguientes recomendaciones:

Segmentación de Redes: IEC 62443 enfatiza la importancia de segmentar las redes de IT y OT para limitar la exposición a amenazas cibernéticas. Se recomienda implementar zonas de seguridad y demarcar claramente los límites entre las redes de IT y OT.

Acceso Controlado: Los estándares IEC 62443 sugieren implementar mecanismos de control de acceso para restringir el acceso a los sistemas y dispositivos de OT solo a usuarios autorizados. Esto incluye la autenticación robusta y la autorización basada en roles.

Monitoreo y Detección de Intrusiones: Se recomienda implementar sistemas de monitoreo y detección de intrusiones tanto en las redes de IT como de OT para identificar actividades sospechosas y responder rápidamente a posibles amenazas cibernéticas.

Gestión de Identidad y Acceso: IEC 62443 propone establecer políticas de gestión de identidad y acceso para garantizar que solo los usuarios autorizados tengan acceso a los sistemas de OT. Esto incluye la implementación de contraseñas seguras, la autenticación multifactor y la revisión regular de los permisos de acceso.

Resiliencia y Continuidad Operativa: Los estándares IEC 62443 abogan por la implementación de medidas de resiliencia y continuidad operativa para garantizar la disponibilidad continua de los sistemas de OT en caso de incidentes cibernéticos o desastres.

Actualizaciones y Parches de Seguridad: Se recomienda establecer procesos de gestión de parches y actualizaciones de seguridad para garantizar que los sistemas de OT estén protegidos contra vulnerabilidades conocidas.

Tabla 4. IEC 62443

Criterio de Evaluación	IEC 62443	Prioridad	Recomendaciones	Ciberseguridad y Eficiencia Operativa
Gestión de Accesos	Control estricto entre zonas	Alta	Implementar Autenticación Multifactor MFA	Mayor protección contra accesos no autorizados
Segmentación de Redes	Zonas y conductos	Alta	Firewalls y VLANs	Reducción de propagación de ataques
Monitoreo y Detección	Análisis de eventos	Media	SIEM y IDS/IPS	Mayor visibilidad de amenazas
Respuesta a Incidentes	Estrategia de mitigación	Alta	Simulaciones y DRP	Reducción de tiempo de recuperación
Seguridad de Comunicaciones	Encriptación de tráfico OT	Alta	TLS/IPSec	Protección contra interceptación de datos

4.2.8.2. NIST SP 800-82

Una de las guías más reconocidas a nivel internacional en cuanto a la seguridad de sistemas de control industrial (ICS) es la NIST Special Publication 800-82, desarrollada por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos. Esta publicación proporciona recomendaciones detalladas sobre la gestión de riesgos y el fortalecimiento de la seguridad en entornos OT. En lo que

respecta a la arquitectura de redes, promueve la separación efectiva de redes IT y OT como una medida crítica para reducir la superficie de ataque y limitar la propagación de amenazas (NIST, 2015).

Además del NIST, otras organizaciones también promueven esta buena práctica como parte de estándares y marcos de referencia reconocidos internacionalmente:

Segmentación de Redes: El documento recomienda la segmentación de redes para separar claramente los sistemas de IT de los sistemas de OT. Esto implica establecer zonas de seguridad y cortafuegos entre las redes de IT y OT para limitar la propagación de amenazas cibernéticas.

Definición de Perímetros de Seguridad: Se sugiere establecer perímetros de seguridad para controlar el tráfico entre las redes de IT y OT. Esto puede incluir el uso de dispositivos de seguridad como firewalls, gateways y proxies para filtrar y supervisar el tráfico entre las dos redes.

Control de Acceso Basado en Políticas: El NIST SP 800-82 recomienda implementar políticas de control de acceso para regular el acceso a los sistemas y dispositivos de OT. Esto implica establecer políticas de autenticación y autorización para garantizar que solo los usuarios autorizados tengan acceso a los recursos de OT.

Gestión de Identidad y Acceso: Se enfatiza la importancia de implementar una sólida gestión de identidad y acceso para garantizar que los usuarios sean autenticados de manera segura antes de acceder a los sistemas de OT. Esto puede incluir la implementación de autenticación multifactor y la revisión regular de los permisos de acceso.

Monitoreo y Detección de Intrusiones: Se recomienda implementar sistemas de monitoreo y detección de intrusiones para detectar actividades maliciosas en las redes de OT. Esto puede incluir la supervisión del tráfico de red, la detección de anomalías y la generación de alertas en caso de actividad sospechosa.

Gestión de Incidentes y Respuesta: El documento sugiere establecer procesos de gestión de incidentes y respuesta para manejar de manera efectiva los incidentes de seguridad que afecten a los sistemas de OT. Esto implica la preparación de planes de respuesta a incidentes y la capacitación del personal para responder rápidamente a las amenazas cibernéticas.

Destaca la importancia de la segmentación de redes, el control de acceso, la monitorización de seguridad y la gestión de incidentes como parte de una estrategia integral de ciberseguridad para entornos industriales.

Tabla 5. NIST SP 800-82

Criterio de Evaluación	NIST SP 800-82	Prioridad	Recomendaciones	Ciberseguridad y Eficiencia Operativa
Gestión de Accesos	Basado en roles y riesgos	Alta	Implementar Autenticación Multifactor MFA	Mayor protección contra accesos no autorizados
Segmentación de Redes	Defensa en profundidad	Alta	Firewalls y VLANs	Reducción de propagación de ataques

Monitoreo y Detección	Supervisión continua	Media	SIEM y IDS/IPS	Mayor visibilidad de amenazas
Respuesta a Incidentes	Planes de respuesta	Alta	Simulaciones y DRP	Reducción de tiempo de recuperación
Seguridad de Comunicaciones	Segmentación de tráfico	Alta	TLS/IPSec	Protección contra interceptación de datos

4.2.8.3. Modelo Purdue

El Modelo Purdue, también conocido como Purdue Enterprise Reference Architecture (PERA), es un marco de referencia ampliamente adoptado para la arquitectura de sistemas de control industrial. Fue originalmente desarrollado por la Universidad Purdue en la década de 1990 y posteriormente formalizado como parte del estándar ISA-95 por la International Society of Automation (ISA), con el propósito de facilitar la integración entre los sistemas OT e IT (ISA, 2000).

Este modelo propone una estructura jerárquica de cinco niveles funcionales (extendida en algunas versiones a siete), que va desde el nivel de campo (sensores y actuadores) hasta el nivel empresarial (ERP), y ha sido clave para establecer zonas de segmentación y zonas de control en la infraestructura de red, lo cual es fundamental para una separación segura y eficaz entre los entornos IT y OT.

Autores como Stouffer (Stouffer K. P., Guide to Industrial Control Systems (ICS) Security: NIST SP 800-82 Revision 2., 2015) del NIST recomiendan explícitamente el uso del Modelo Purdue en su guía de seguridad para sistemas de control industrial (NIST SP 800-82 Rev. 2), señalando que este modelo permite diseñar controles de seguridad adaptados a cada nivel, facilitando la defensa en profundidad (defense-in-depth). Asimismo, (Langner, 2011), al analizar el ataque Stuxnet, destacó cómo la ausencia de segmentación efectiva entre IT y OT permitió la propagación del malware, lo que reforzó la necesidad de arquitecturas basadas en Purdue.

En la práctica, empresas como Siemens, Rockwell Automation y Schneider Electric han incorporado principios del Modelo Purdue en sus soluciones de ciberseguridad industrial, promoviendo su adopción como una mejor práctica de la industria. Por ejemplo, en el informe de Cisco sobre ciberseguridad en entornos industriales (Cisco, 2019), se describe cómo el modelo Purdue sirve de base para implementar arquitecturas Zero Trust en sistemas OT.

Las características más relevantes del Modelo Purdue para la separación efectiva de redes IT/OT son:

Niveles Jerárquicos: El Modelo Purdue define una jerarquía de niveles que van desde el nivel de campo hasta el nivel empresarial. Cada nivel tiene su propia función y responsabilidades en el proceso de producción, desde el control y monitoreo en el nivel de campo hasta la planificación y la gestión en el nivel empresarial.

Separación de Funciones: Cada nivel en el Modelo Purdue tiene funciones específicas y está diseñado para gestionar diferentes aspectos del proceso de producción. Por ejemplo, el nivel de campo está destinado a la adquisición de datos y

el control en tiempo real, mientras que los niveles superiores están más centrados en la supervisión, la planificación y la toma de decisiones.

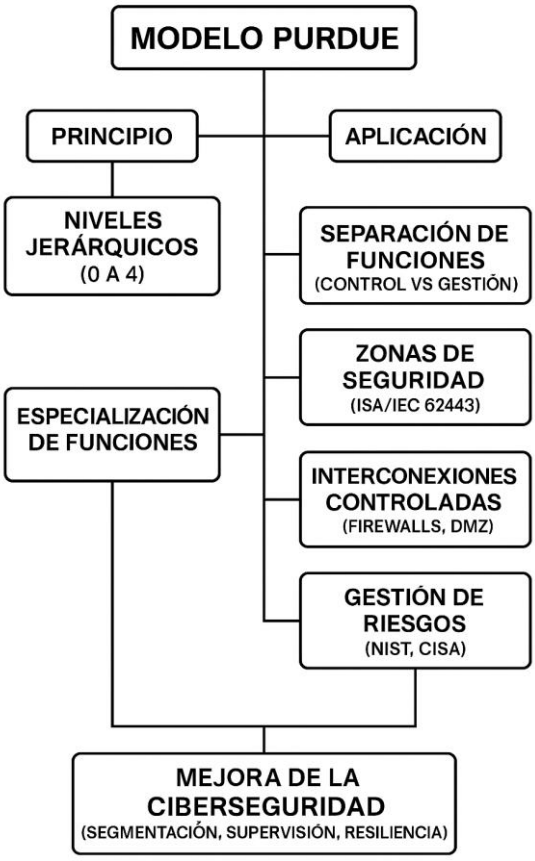
Zonas de Seguridad: El Modelo Purdue permite la definición de zonas de seguridad en diferentes niveles de la jerarquía para separar claramente los sistemas de IT y OT. Estas zonas de seguridad actúan como barreras físicas y lógicas para limitar el acceso no autorizado y proteger los sistemas críticos de producción.

Interconexiones Controladas: Si bien el Modelo Purdue reconoce la necesidad de interconectar los sistemas de IT y OT para facilitar la comunicación y la colaboración, también establece controles estrictos para gestionar estas interconexiones. Se recomienda implementar cortafuegos y dispositivos de seguridad en los puntos de conexión entre los diferentes niveles para filtrar y supervisar el tráfico de red.

Gestión de Riesgos: El Modelo Purdue promueve la gestión proactiva de riesgos para identificar y mitigar posibles amenazas a la seguridad y la integridad de los sistemas de IT y OT. Se recomienda realizar evaluaciones de riesgos regulares y establecer medidas de seguridad adecuadas en cada nivel de la jerarquía.

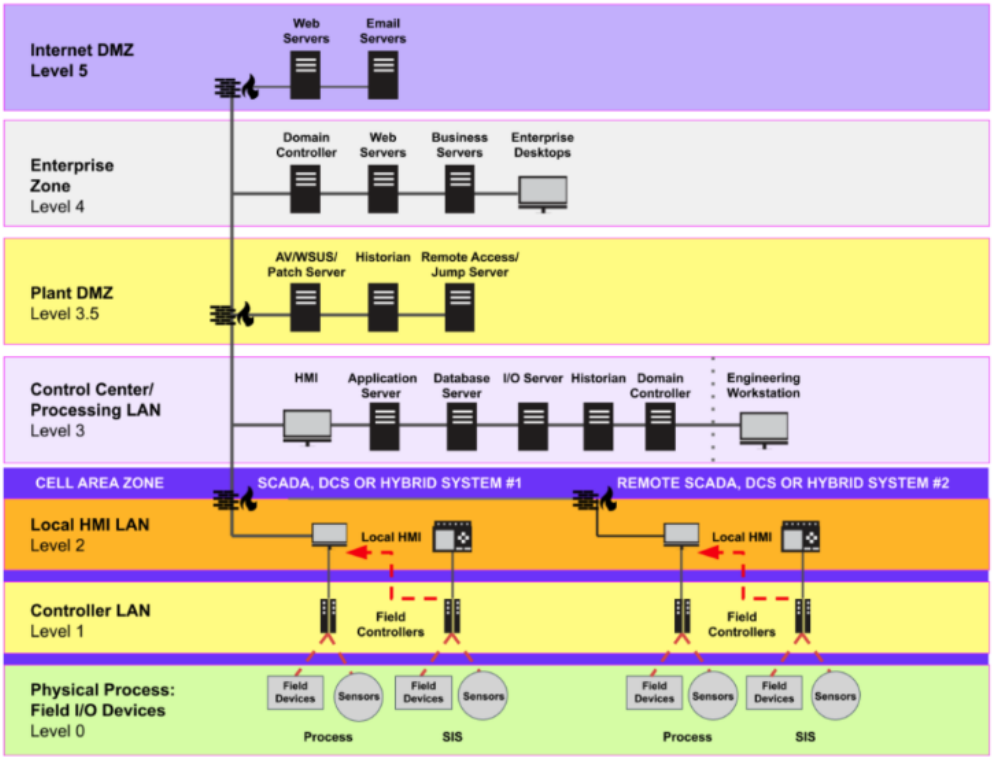
Proporciona una estructura jerárquica que organiza los sistemas de control en capas, desde los niveles de proceso hasta los niveles corporativos, con el objetivo de proporcionar una separación clara entre los sistemas OT y los sistemas IT.

Ilustración 54. Modelo Purdue



El modelo Purdue recomienda la segmentación de redes entre las diferentes capas para minimizar los riesgos de seguridad y garantizar la confiabilidad y la disponibilidad de los sistemas de control.

Ilustración 55. Modelo Pudue. Autor Claroty



4.3. Definición de medidas de seguridad cibernética en redes IT y OT

La definición de medidas de seguridad permite fundamentar la necesidad y efectividad de las medidas de seguridad propuestas para garantizar la protección de la infraestructura crítica de la organización.

La separación efectiva de redes IT y OT contribuye a una mejora sustancial en la ciberseguridad, reduciendo la superficie de ataque.

La reducción de riesgos de ataques dirigidos, minimizando la posibilidad de intrusiones a sistemas críticos.

Los beneficios en la disponibilidad y confiabilidad de los sistemas SCADA, asegurando la operatividad de la empresa sin interrupciones.

4.3.1. Segmentación de redes

Se debe establecer segmentos de red bien definidos para IT y OT, minimizando la interdependencia y reduciendo el riego de propagación de ataques.

Configuración de firewalls y una DNZ para restringir el tráfico entre IT y OT, permitiendo solo comunicaciones autorizadas.

4.3.2. Control de acceso y autenticación

Es indispensable contar con autenticación multifactorial (MFA) en sistemas críticos, reforzando la seguridad en accesos sensibles.

La aplicación de políticas de acceso basado en roles (RBAC), garantizando que solo usuarios autorizados puedan acceder a sistemas específicos según sus funciones.

Se debe considerar mecanismos de seguridad para cuentas de usuarios y dispositivos, como la gestión centralizada de credenciales y la reducción de privilegios innecesarios.

4.3.3. Monitoreo y detección de amenazas

La implementación de un sistema para la correlación de eventos de seguridad y la detección proactiva de amenazas.

Despliegue de IDS/IPS en redes OT para identificar intrusiones y comportamientos anómalos en el tráfico de red.

Estrategias de respuesta ante incidentes basadas en plane de acción y ejercicios de simulación de ataques.

4.3.4. Gestión de parches y actualizaciones

Desarrollo de una estrategia de actualización segura en sistemas OT, considerando los requisitos de alta disponibilidad.

Evaluación de riesgo antes de aplicar parches en sistemas SCADA, garantizando la estabilidad operativa.

4.3.5. Protección de datos y comunicación

Implementación de cifrado de datos en tránsito y en reposo, minimizando el riego de exfiltración de información sensible.

Uso de protocolos seguros de comunicación entre IT y OT, incluyendo VPNs para la protección de la integridad de los datos.

Definición de políticas de respaldo y recuperación ante desastres, asegurando la continuidad del negocio en caso de incidentes.

Ilustración 56. Medidas de Seguridad

4.4. Evaluar el impacto del plan de separación de redes en la eficiencia operativa y la ciberseguridad de EMELNORTE, mediante la realización de pruebas de concepto tendientes a verificar la efectividad de las medidas implementadas y proponer ajustes necesarios para mejorar la protección de los sistemas y datos críticos.

4.4.1. Definición de ejes y criterios

Los ejes evaluados en el plan de separación de redes en la eficiencia operativa y ciberseguridad de EMELNORTE, son: Tecnológico, Institucional, Económico y Ambiental.

Tabla 6. Criterios de Evaluación

Eje	Criterios de Evaluación	Peso (%)
Tecnológico (T)	- Segmentación efectiva de redes	30%
	- Reducción de la superficie de ataque	
	- Implementación de protocolos seguros (IEC 62443, NIST 800-82)	
	- Rendimiento de la red post-separación	
Institucional (I)	- Adopción de nuevas políticas y normativas	25%
	- Capacitación y conciencia del personal	
	- Coordinación entre equipos de TI y OT	
	- Cumplimiento de normativas regulatorias	
Económico (E)	- Costos de implementación	25%
	- Retorno de inversión en seguridad y eficiencia	
	- Costos operativos post-implementación	
	- Ahorros por reducción de incidentes de ciberseguridad	
Ambiental (A)	- Consumo energético de la infraestructura post-separación	20%
	- Impacto ambiental de nuevos equipos	
	- Gestión de residuos tecnológicos	
	- Continuidad operativa en escenarios de contingencia	

4.4.2. Metodología de Evaluación

Cada criterio se evaluará en una escala del 1 al 5.

Tabla 7. Evaluación de Criterios

1	Impacto muy bajo
2	Impacto bajo
3	Impacto medio
4	Impacto alto
5	Impacto muy alto

Para evaluar la efectividad de la separación de redes IT y OT en un entorno industrial, se han definido cuatro ejes principales que permiten un análisis integral: tecnológico, institucional, económico y ambiental. Cada eje agrupa criterios específicos que permiten valorar su aporte al éxito del proyecto. A continuación, se describen detalladamente los ejes de evaluación:

Eje Tecnológico (T): Evalúa la implementación técnica de la separación, considerando aspectos como la segmentación de redes, la reducción de la superficie de ataque, el uso de protocolos seguros y el rendimiento general de la red tras la intervención.

Eje Institucional (I): Mide el grado de adaptación organizacional, incluyendo la adopción de nuevas políticas, el nivel de capacitación del personal, la coordinación entre equipos de TI y OT, y el cumplimiento de las normativas regulatorias.

Eje Económico (E): Analiza la viabilidad financiera del proyecto, considerando tanto los costos de implementación y operación como los beneficios derivados, tales como el retorno de inversión y los ahorros por reducción de incidentes de ciberseguridad.

Eje Ambiental (A): Valora los impactos ambientales de la separación, como el consumo energético, el uso de nuevos equipos, la gestión de residuos tecnológicos y la continuidad operativa en situaciones de contingencia.

Tabla 8. Evaluación por Criterio

Eje	Criterios de Evaluación	Calificación (1-5)	Peso (%)	Puntaje Ponderado
Tecnológico (T)	Segmentación efectiva de redes	4	10%	0.40
	Reducción de la superficie de ataque	5	8%	0.40
	Implementación de protocolos seguros	4	6%	0.24
	Rendimiento de la red post-separación	3	6%	0.18
Subtotal Tecnológico			**30%**	**1.22**
Institucional (I)	Adopción de nuevas políticas y normativas	4	7%	0.28
	Capacitación y conciencia del personal	3	6%	0.18
	Coordinación entre equipos de TI y OT	3	6%	0.18
	Cumplimiento de normativas regulatorias	5	6%	0.30
Subtotal Institucional			**25%**	**0.94**
Económico (E)	Costos de implementación	3	7%	0.21
	Retorno de inversión en seguridad y eficiencia	4	6%	0.24
	Costos operativos post-implementación	3	6%	0.18

	Ahorros por reducción de incidentes de ciberseguridad	4	6%	0.24
Subtotal Económico			**25%**	**0.87**
Ambiental (A)	Consumo energético post-separación	3	5%	0.15
	Impacto ambiental de nuevos equipos	4	5%	0.20
	Gestión de residuos tecnológicos	3	5%	0.15
	Continuidad operativa en escenarios de contingencia	4	5%	0.20
Subtotal Ambiental			**20%**	**0.70**

Cálculo del puntaje ponderado total

Cada criterio se evalúa en una escala del 1 al 5, se multiplica por su respectivo peso porcentual, y se obtiene el puntaje ponderado. Luego, los puntajes ponderados de todos los criterios se agrupan por eje, y finalmente se suman los subtotales de cada eje para obtener el puntaje total:

$$\textbf{Puntaje Total} = \sum \textbf{(Calificación} \times \textbf{Peso)}$$

Puntaje Total = 1.22 (T) + 0.94 (I) + 0.87 (E) + 0.70 (A) = **3.73 *sobre* 5.0**

Para escalar a 100 puntos:

3.73 × 20 = 74.6 puntos.

Con un puntaje total de 3.73 sobre 5.0, equivalente a 74.6 puntos sobre 100, la evaluación integral clasifica el impacto del plan de separación de redes IT y OT como **ALTO**. Esta clasificación no solo refleja un cumplimiento satisfactorio de los objetivos técnicos y organizacionales, sino que además respalda la viabilidad del plan desde una perspectiva operativa, económica y de sostenibilidad.

El resultado evidencia que la segmentación efectiva de redes y la reducción de la superficie de ataque están logrando mejoras tangibles en la postura de ciberseguridad de la organización. Asimismo, la implementación de protocolos seguros ha fortalecido las comunicaciones entre sistemas críticos, disminuyendo significativamente los vectores de ataque.

Desde el enfoque institucional, el alto puntaje en cumplimiento de normativas regulatorias y la adopción de nuevas políticas indican una madurez creciente en la gobernanza de la ciberseguridad. Aunque aún existen oportunidades de mejora en la coordinación entre equipos TI y OT, los resultados muestran avances positivos en la gestión del cambio organizacional.

En el plano económico, los datos sugieren que el plan no solo es viable, sino que está comenzando a generar retornos medibles en términos de reducción de incidentes y mejora de la eficiencia operativa, lo cual compensa gradualmente los costos iniciales de implementación.

Por último, en el eje ambiental, se ha evidenciado un equilibrio entre el despliegue de nueva infraestructura y el control de impactos como el consumo energético y la gestión de residuos tecnológicos. La continuidad operativa en

escenarios de contingencia también fue calificada positivamente, lo cual refuerza la resiliencia del sistema frente a eventos disruptivos.

En conjunto, esta puntuación alta valida la estrategia de separación de redes como una intervención crítica y efectiva para organizaciones que operan infraestructuras críticas, como en el caso de empresas del sector eléctrico. Además, el resultado obtenido proporciona una base técnica y objetiva para la toma de decisiones futuras, tanto en escalamiento del proyecto como en su replicabilidad en otras empresas eléctricas.

4.4.3. Ajustes y Recomendaciones

Mejorar el rendimiento post-separación: Revisar latencias y optimizar la configuración de VLANs y firewalls.

Aumentar la capacitación del personal: Realizar más simulaciones de ciberataques y entrenamientos especializados en seguridad OT.

Optimizar costos operativos: Identificar oportunidades para automatizar la gestión de redes y reducir gastos en mantenimiento.

Reducir consumo energético: Evaluar la actualización de hardware a equipos más eficientes.

CAPITULO V

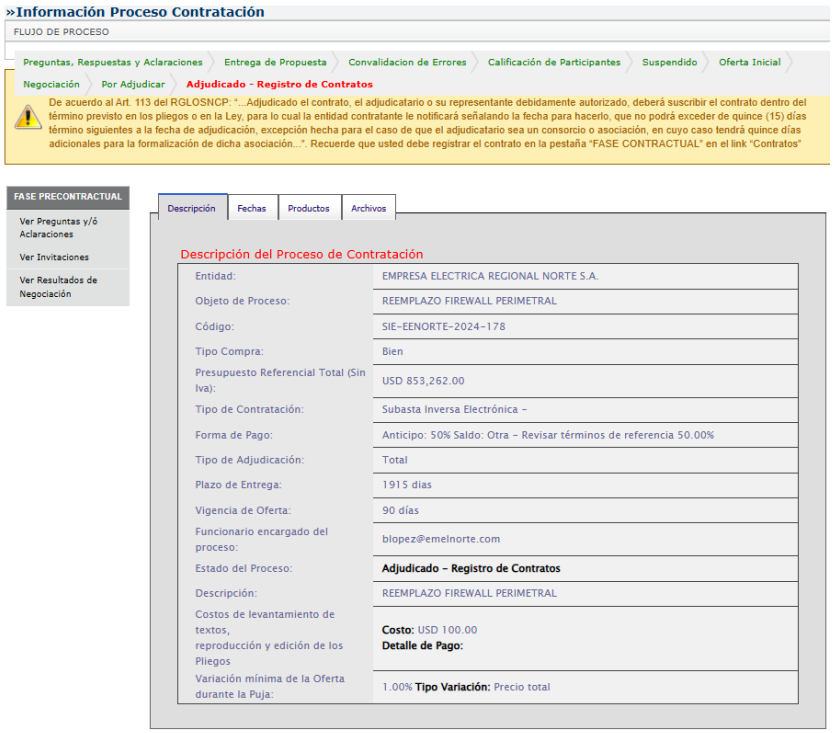
5. PROPUESTA

Los beneficios esperados incluyen una mayor resistencia ante ataques cibernéticos, una reducción del impacto de incidentes de seguridad, un control más preciso sobre el tráfico de datos y una optimización de los procesos operativos mediante la disminución de latencias y cuellos de botella en la comunicación entre sistemas.

ETAPA PRECONTRACTUAL

Se publicó en el portal de compras públicas el proyecto de Reemplazo de Firewall Perimetral con el código SIE-EENORTE-2024-178, en el que consta el PLAN DE SEPARACIÓN DE LOS SERVICIOS DE RED IT Y OT ENFOCADOS A LA CIBERSEGURIDAD Y EFICIENCIA OPERATIVA EN LA EMPRESA ELÉCTRICA REGIONAL NORTE S.A. EMELNORTE.

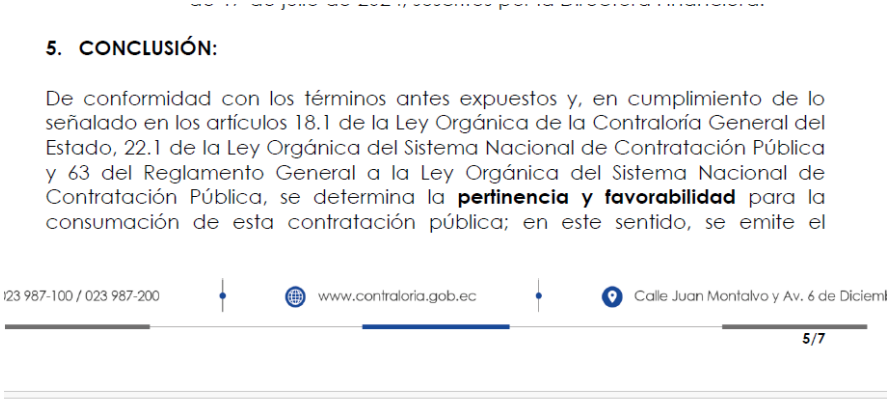
Ilustración 57. Portal de Compras Públicas



En la sección de Archivos se encuentra publicada toda la documentación precontractual, donde consta el Informe de Necesidad, Resolución de Inicio, Certificaciones Presupuestarias, Informe de Pertinencia Favorable, Autorizaciones de los entes de control, Pliegos, Acta de Calificación, Resolución de Adjudicación, entre otros.

Ilustración 58. Archivos Portal de Compras Públicas

Ilustración 59. Informe de pertinencia Contraloría General del Estado



5. CONCLUSIÓN:

De conformidad con los términos antes expuestos y, en cumplimiento de lo señalado en los artículos 18.1 de la Ley Orgánica de la Contraloría General del Estado, 22.1 de la Ley Orgánica del Sistema Nacional de Contratación Pública y 63 del Reglamento General a la Ley Orgánica del Sistema Nacional de Contratación Pública, se determina la **pertinencia y favorabilidad** para la consumación de esta contratación pública; en este sentido, se emite el

presente **Informe de Pertinencia**, mismo que deberá ser publicado por la entidad contratante en el Portal Compras Públicas.

5.1. Propuesta de equipos

Se requieren firewalls de próxima generación (NGFW) con capacidades avanzadas de inspección de tráfico, segmentación, detección de amenazas y alta disponibilidad y que cumpla con necesidades de EMELNORTE de acuerdo con los análisis de tráfico realizados.

5.1.1. Red IT

Según el diagrama propuesto los equipos sugeridos deben estar en alta disponibilidad.

Deben tener las siguientes funcionalidades: Firewall, VPN, Red y Clustering, Identificación de Usuarios, IPS, Control de Aplicaciones, Filtrado basado en URLs, Seguridad DNS, Prevención de Amenazas, Control de dispositivos IoT y Calidad de Servicio.

5.1.1.1.Firewall Perimetral

Tabla 9. Especificaciones Básicas Firewall Perimetral

FIREWALL PERIMETRAL	
DATOS DE FABRICACIÓN	**CONDICIONES**
Cantidad	2
Marca	Especificar
Modelo	Especificar
Tipo	El hardware de la plataforma de seguridad NGFW en alta disponibilidad debe ser de tipo Appliance (hardware y software integrados del mismo fabricante). (No se aceptan soluciones virtualizadas).
Montaje	Los equipos deben ser de tipo rackeable. Se debe incluir todos los accesorios para el montaje en rack.

Equipos	Nuevos, no remanufacturados de reciente fabricación (al menos en los 2 últimos años y de última generación).
Alta disponibilidad	Tiene que operar en alta disponibilidad, se entiende por alta disponibilidad una solución redundante de por lo menos 2 (dos) firewalls en modo activo/activo o activo/pasivo. Sin que se afecte el rendimiento y requerimientos solicitados.
Compatibilidad	Diponer de hiperescalabilidad con orquestador del mismo fabricante.
DESCRIPCIÓN	
El fabricante de la solución deberá contar con certificaciones de seguridad ISO 27001, ISO27017 e ISO27018.	
Los modelos ofertados no podrán estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. Se deberá adjuntar el link público del fabricante que verifique que los modelos propuestos no están en ese listado.	
CAPACIDADES	**CANTIDADES**
Throughput de Firewall con logging activo.	>= 19 Gbps
Throughput de Prevención de Amenazas con todas las funcionalidades habilitadas simultáneamente (Firewall, Control de Aplicaciones, URL Filtering, IPS, Antivirus, Anti-Bot, Sandboxing) con logging activo.	>= 6.5 Gbps
Número de conexiones simultaneas soportadas	>= 2 M
Nuevas sesiones por segundo soportadas	>=200000
Interfaces de red ethernet 10/100/1000	>= 8
Interfaces de red 1/10 Gbps SFP/SFP+	>= 8
Incluir 6 (seis) transceivers de 10 Gbps tipo SFP+ por cada equipo.	Requerido
Interfaz de red para administración.	>= 1
Interfaz de tipo consola o similar.	>= 1
Interfaz de red dedicada para alta disponibilidad (HA) y sincronización clúster.	>=1
Velocidad de la interfaz para alta disponibilidad (HA) y sincronización clúster.	>=1 Gbps
Disco de estado sólido interno.	>= 480 GB
El equipo de seguridad deberá soportar la capacidad de crear firewalls virtuales.	>= 4

Fuente de alimentación redundante con todos los accesorios. Requerido

FUNCIONALIDADES GENERALES
El equipo tipo appliance debe contar con un acceso fuera de banda a través de la consola web provista por la interfaz solicitada.
Las funcionalidades de Firewall, VPN, QoS, NATs, Identificación de usuarios, Geolocalización debe de estar embebido en el sistema operativo de manera permanente sin necesidad de una licencia que active las mismas.
El firmware deberá ser ofrecido en su versión más estable y/o más actual.
Debe ser posible la gestión y configuración completa, integración total a la herramienta de la solución propuesta.

5.1.1.2.Firewall de Data Center

Tabla 10. Especificaciones Básicas Firewall Data Center

FIREWALL DATA CENTER	
DATOS DE FABRICACIÓN	**CONDICIONES**
Cantidad	2
Marca	Especificar
Modelo	Especificar
Tipo	El hardware de la plataforma de seguridad NGFW en alta disponibilidad debe ser de tipo Appliance (hardware y software integrados del mismo fabricante). (No se aceptan soluciones virtualizadas).
Montaje	Los equipos deben ser de tipo rackeable. Se debe incluir todos los accesorios para el montaje en rack.
Equipos	Nuevos, no remanufacturados de reciente fabricación (al menos en los 2 últimos años y de última generación).
Alta disponibilidad	Tiene que operar en alta disponibilidad, se entiende por alta disponibilidad una solución redundante de por lo menos 2 (dos) firewalls en modo activo/activo o activo/pasivo. Sin que se afecte el rendimiento y requerimientos solicitados.
Compatibilidad	Disponer de hiperescalabilidad con

	orquestador del mismo fabricante.
DESCRIPCIÓN	
El fabricante de la solución deberá contar con certificaciones de seguridad ISO 27001, ISO27017 e ISO27018.	
Los modelos ofertados no podrán estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. Se deberá adjuntar el link público del fabricante que verifique que los modelos propuestos no están en ese listado.	
CAPACIDADES	**CANTIDADES**
Throughput de Firewall con logging activo	>= 28 Gbps
Throughput de Prevención de Amenazas con todas las funcionalidades habilitadas simultáneamente (Firewall, Control de Aplicaciones, URL Filtering, IPS, Antivirus, Anti-Bot, Sandboxing) logging activo.	>= 9 Gbps
Número de conexiones simultaneas soportadas.	>= 2,5 M
Nuevas sesiones por segundo soportadas.	>= 240000
Interfaces de red 10/100/1000	>= 8
Interfaces de red 1/10 Gbps SFP/SFP+	>= 8
Se deben incluir 8 (ocho) transceivers de 10 Gbps tipo SFP+ por cada equipo.	Requerido
Interfaz de red para administración.	>= 1
Interfaz de tipo consola o similar.	>= 1
Interfaz de red dedicada para alta disponibilidad (HA) y sincronización clúster.	>=1
Velocidad de la interfaz para alta disponibilidad (HA) y sincronización clúster.	>=1 Gbps
Disco de estado sólido interno.	>= 480 GB
El equipo de seguridad deberá soportar la capacidad de crear firewalls virtuales.	>= 4
Fuente de alimentación redundante con todos los accesorios.	Requerido
FUNCIONALIDADES GENERALES	
El equipo tipo appliance debe contar con un acceso fuera de banda a través de la consola web provista por la interfaz solicitada.	
Las funcionalidades de Firewall, VPN site-to-site, QoS, NATs, Identificación de usuarios, Geolocalización debe de estar embebido en el sistema operativo de manera permanente sin necesidad de una licencia que active las mismas.	
El firmware deberá ser ofrecido en su versión más estable y/o más actual.	
Debe ser posible la gestión y configuración completa, integración total a la herramienta de la solución propuesta.	

5.1.2. Red OT

Deben tener las siguientes funcionalidades: Firewall, VPN, Red y Clustering, Identificación de Usuarios, IPS, Control de Aplicaciones, Filtrado basado en URLs,

Seguridad DNS, Prevención de Amenazas, Funcionalidades de OT, Control de dispositivos IoT y Calidad de Servicio.

5.1.2.1.Firewall de OT

Tabla 11. Especificaciones Básicas Firewall OT

FIREWALL OT	
DATOS DE FABRICACIÓN	**CONDICIONES**
Cantidad	2
Marca	Especificar
Modelo	Especificar
Tipo	El hardware de la plataforma de seguridad NGFW en alta disponibilidad debe ser de tipo Appliance (hardware y software integrados del mismo fabricante). (No se aceptan soluciones virtualizadas).
Montaje	Los equipos deben ser de tipo rackeable. Se debe incluir todos los accesorios para el montaje en rack.
Equipos	Nuevos, no remanufacturados de reciente fabricación (al menos en los 2 últimos años y de última generación).
Alta disponibilidad	Tiene que operar en alta disponibilidad, se entiende por alta disponibilidad una solución redundante de por lo menos 2 (dos) firewalls en modo activo/activo o activo/pasivo. Sin que se afecte el rendimiento y requerimientos solicitados.
Compatibilidad	Compatibilidad de hiperescalabilidad con orquestador del mismo fabricante.
DESCRIPCIÓN	
El fabricante de la solución deberá contar con certificaciones de seguridad ISO 27001, ISO27017 e ISO27018.	
Los modelos ofertados no podrán estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. Se deberá adjuntar el link público del fabricante que verifique que los modelos propuestos no están en ese listado.	
CAPACIDADES	**CANTIDADES**
Throughput de Firewall con logging activo.	>= 14 Gbps

Throughput de Prevención de Amenazas con todas las funcionalidades habilitadas simultáneamente (Firewall, Control de Aplicaciones, URL Filtering, IPS, Antivirus, Anti-Bot, Sandboxing) logging activo.	>= 4.9 Gbps
Número de conexiones simultaneas soportadas.	>= 1.4 M
Nuevas sesiones por segundo soportadas.	>=145000
Interfaces de red 10/100/1000.	>= 8
Interfaces de red 1/10 Gbps SFP/SFP+.	>= 8
Se deben incluir 6 (seis) transceivers de 1 Gbps tipo SFP por cada equipo.	Requerido
Interfaz de red para administración.	>= 1
Interfaz de tipo consola o similar.	>= 1
Interfaz de red dedicada para alta disponibilidad (HA) y sincronización clúster.	>=1
Velocidad de la interfaz para alta disponibilidad (HA) y sincronización clúster.	>=1 Gbps
Disco de estado sólido interno	>= 480 GB
El equipo de seguridad deberá soportar la capacidad de crear firewalls virtuales.	>= 4
Fuente de alimentación redundante con todos los accesorios.	Requerido
FUNCIONALIDADES GENERALES	
El equipo tipo appliance debe contar con un acceso fuera de banda a través de la consola web provista por la interfaz solicitada.	
Las funcionalidades de Firewall, VPN site-to-site, QoS, NATs, Identificación de usuarios, Geolocalización debe de estar embebido en el sistema operativo de manera permanente sin necesidad de una licencia que active las mismas.	
El firmware deberá ser ofrecido en su versión más estable y/o más actual.	
Debe ser posible la gestión y configuración completa, integración total a la herramienta de la solución propuesta.	
FUNCIONALIDADES DE OT	**CONDICIONES**
Debe proteger los sistemas OT, ICS y SCADA al bloquear o restringir el acceso a protocolos industriales:	Requerido
• DNP3	Requerido
• IEC 61850	Requerido
• Modbus	Requerido
• Ethernet/IP	Requerido
• OPC	Requerido
• PROFINET	Requerido
• Safety NET	Requerido

• IEC 60870-6 (TASE.2) /ICCP	Requerido
• IEC 60870-5-104	Requerido
Debe tener la capacidad de entender protocolos SCADA y aplicar firmas de IPS sobre este tipo de tráfico.	Requerido
Debe soportar dispositivos OT sobre IPv4.	Requerido
FUNCIONALIDADES DE IoT	
La solución debe tener la capacidad de brindar prevención para dispositivos tipo IoT (internet de las cosas) como, por ejemplo, cámaras IP, Smart TV, impresoras entre otros.	
La solución debe poder descubrir automáticamente los dispositivos IoT en la red.	
La solución debe poder aplicar una política de seguridad sobre los dispositivos IoT.	
La solución debe poder brindar sobre los dispositivos IoT una protección autónoma basado en el principio de ZTNA (zero Trust Network Access).	

5.1.2.2.Firewalls Subestaciones y Centrales

Tabla 12. Especificaciones Básicas Firewall Subestaciones y Centrales

FIREWALL SUBESTACIONES Y CENTRALES	
DATOS DE FABRICACIÓN	**CONDICIONES**
Cantidad	12
Marca	Especificar
Modelo	Especificar
Tipo	El hardware de la plataforma de seguridad NGFW en alta disponibilidad debe ser de tipo Appliance (hardware y software integrados del mismo fabricante). (No se aceptan soluciones virtualizadas).
Equipos	Nuevos, no remanufacturados de reciente fabricación (al menos en los 2 últimos años y de última generación).
DESCRIPCIÓN	
El fabricante de la solución deberá contar con certificaciones de seguridad ISO 27001, ISO27017 e ISO27018.	
Los modelos ofertados no podrán estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. Se deberá adjuntar el link público del fabricante que verifique que los modelos propuestos no están en ese listado.	
CAPACIDADES	**CANTIDADES**
Throughput de Firewall con logging activo.	>= 1000 Mbps

Throughput de Prevención de Amenazas con todas las funcionalidades habilitadas simultáneamente (Firewall, Control de Aplicaciones, URL Filtering, IPS, Antivirus, Anti-Bot, Sandboxing) logging activo.	>= 440 Mbps
Número de conexiones simultaneas soportadas.	>= 200000
Nuevas sesiones por segundo soportadas.	>=10000
Interfaces de red 10/100/1000.	>= 6
Interfaz de red para administración.	>= 1
Interfaz de tipo consola o similar.	>= 1
Almacenamiento interno	>= 64 GB
Fuente de alimentación con todos los accesorios.	Requerido
FUNCIONALIDADES GENERALES	
Las funcionalidades de Firewall, VPN site-to-site, QoS, NATs, Identificación de usuarios, Geolocalización debe de estar embebido en el sistema operativo de manera permanente sin necesidad de una licencia que active las mismas.	
El firmware deberá ser ofrecido en su versión más estable y/o más actual.	
Debe ser posible la gestión y configuración completa, integración total a la herramienta de la solución propuesta.	
FUNCIONALIDADES DE OT	**CONDICIONES**
Debe proteger los sistemas OT, ICS y SCADA al bloquear o restringir el acceso a protocolos industriales:	Requerido
• DNP3	Requerido
• IEC 61850	Requerido
• Modbus	Requerido
• Ethernet/IP	Requerido
• OPC	Requerido
• PROFINET	Requerido
• Safety NET	Requerido
• IEC 60870-6 (TASE.2) /ICCP	Requerido
• IEC 60870-5-104	Requerido
Debe tener la capacidad de entender protocolos SCADA y aplicar firmas de IPS sobre este tipo de tráfico.	Requerido
Debe soportar dispositivos OT sobre IPv4.	Requerido
Debe ofrecer recomendaciones de políticas de seguridad específicas para dispositivos IoT.	Requerido
Debe crear atributos de dispositivos IoT de forma automática para ser utilizados en reglas de firewalls.	Requerido
La solución debe incluir de forma nativa la protección de protocolos SCADA, sin requerir un licenciamiento de OT adicional.	Requerido

5.1.3. Consola de Administración

Tabla 13. Especificaciones Básicas Consola de Administración

CONSOLA DE ADMINISTRACIÓN	
ESPECIFICACIONES	**CONDICIONES**
Cantidad	1
Marca	Cien por ciento compatible con los Firewalls.
Hardware	El hardware será provisto por EMELNORTE en un ambiente virtual con hipervisor VMware 8.
Ambiente de Virtualización	EMELNORTE cuenta con una plataforma de virtualización VMware 8.
Software	El software deberá ser ofrecido en su versión más estable y/o más avanzada.
ESPECIFICACIONES GENERALES	
La solución debe contar con una consola de administración, monitoreo y reportería centralizada, haciendo posible la administración para varios equipos de firewall de nueva generación.	
La consola de gestión debe estar en la capacidad de administrar los 18 gateways contemplados en la solución:	
2 Firewalls Tipo Perimetral	
2 Firewalls Data Center	
2 Firewalls OT	
12 Firewalls Subestaciones y Centrales	
La consola de administración de logs y reportería debe contar con interfaz gráfica de usuario (GUI), vía Web por HTTP y/o HTTPS o disponer de un cliente instalable.	
La solución debe incluir una interfaz basada en línea de comando (CLI) usando SSH.	
La solución debe contar con una API abierta (Open API)	
La solución debe centralizar la administración de gateways de seguridad, políticas y objetos usando una única interfaz de administración.	
La consola debe permitir la administración basado en roles, debe permitir roles granulares para: acceso de escritura, acceso de lectura, creación de usuarios, delimitar las funciones de configuraciones.	
La solución debe contar con la capacidad de asignar un perfil de administración basado en roles que permita delimitar las funciones del equipo que pueden gerenciar y afectar.	
Debe permitir monitorear los eventos de la plataforma vía SNMP.	
Debe permitir la generación de logs de auditoria detallados, informando de la configuración realizada, el administrador que la realizo, su IP y el horario de la alteración.	

Generar alertas automáticas vía	Email
	SNMP
	Syslog
La administración debe permitir/hacer	Creación y administración de políticas de firewall y control de aplicaciones.
	Creación y administración de políticas de IPS y Antispyware o Anti-Bot.
	Creación y administración de políticas de filtro de URL.
	Monitoreo de logs.
	Herramientas de investigación de logs.
	Debugging
	Captura de paquetes
La solución de administración debe mostrar en la misma ventana de configuración de políticas los logs referentes a la regla para facilitar las tareas de administración.	
Debe permitir el acceso concurrente, en modo lectura y escritura de varios administradores.	
La administración de la solución debe posibilitar la recolección de estadísticas de todo el tráfico que pasa por los dispositivos de seguridad.	
Debe ser posible exportar los logs en CSV y/o PDF.	
POLÍTICAS	
Debe permitir administrar todas las políticas, reglas y objetos para todos los gateways que componen la plataforma de seguridad, usando una única interfaz de administración.	
La solución poder unificar objetos IPv4 e IPv6 en una misma regla.	
Permitir la creación y administración de políticas de control de acceso (fw, vpn, aplicaciones, url);	
Permitir la creación y administración de políticas de threat prevention (Antivirus, Anti-bot, sandboxing).	
La solución debe ser capaz de segmentar la política en un conjunto de reglas (capa) en la que solo el tráfico relevante sea inspeccionado por es capa, de esta manera segmentando la basa de reglas para mejorar el troubleshooting.	

5.1.4. Consola de Logs

Tabla 14. Especificaciones Básicas Logs y Reportes

LOGS Y REPORTES

ESPECIFICACIONES	CONDICIONES
Cantidad	1
Marca	Cien por ciento compatible con los Firewalls ofertados en este proceso.
Hardware	El hardware será provisto por EMELNORTE en un ambiente virtual con hipervisor VMware 8.
Ambiente de Virtualización	EMELNORTE cuenta con una plataforma de virtualización VMware 8.
Software	El oferente deberá proporcionar el software de administración de logs y reportería.
	El software deberá ser ofrecido en su versión más estable y/o más avanzada.
Capacidad	No se debe limitar la capacidad de almacenamiento de logs diarios.
Arquitectura	El virtual appliance de gestión de logs debe ser independiente de la consola de administración.
ADMINISTRACIÓN DE LOGS	**CONDICIONES**
La consola de gestión debe estar en la capacidad de administrar los 18 gateways contemplados en la solución:	
2 Firewalls Tipo Perimetral	
2 Firewalls Data Center	
2 Firewalls OT	
12 Firewalls Subestaciones y Centrales	
El Visor de logs debe tener la capacidad de ver todos los logs de seguridad (firewall, vpn, IPS, control de aplicaciones, filtrado url, antivirus, antibot) en un panel de visualización.	
La solución ofertada no debe limitar la capacidad de log por día o mes.	
Los logs deben ser transferidos con seguridad entre el clúster de Gateway de Seguridad y la consola de administración de logs.	
El Visor de logs debe tener la capacidad de crear un filtro utilizando los objetos predefinidos (hosts, red, grupos, usuarios, etc.).	
Debe permitir la creación de reportes personalizados.	
El Visor de logs debe permitir generar estadísticas(tops) de logs por orígenes, destinos, servicios, protocolos, usuarios, etc.	

5.2. Tareas preliminares

- Identificación y clasificación de activos IT y OT.
- Definición de ubicaciones de IT y OT.
- Disponibilidad de enlace de internet principal y backup.
- Elaborar diagrama a detalle de la configuración de red.
- Revisión de VLANs y definición de DMZ.
- Revisión de segmentos de red de Agencias, Subestaciones y Centrales.
- Depuración de usuarios de Active Directory.
- Depuración de DHCP.
- Implementación de firewalls.
- Configuración de acceso remoto seguro con VPNs y MFA.
- Aplicación de estrategias de monitoreo y detección de amenazas.
- Realización de pruebas piloto y evaluación de impacto.
- Capacitación de equipos IT y OT en nuevas políticas de seguridad.
- Auditorías de cumplimiento normativo y documentación de procedimientos.

ETAPA CONTRACTUAL

Dentro de la etapa contractual se emitió la Notificación de Adjudicación No. 015-2025, con fecha 18 de febrero de 2025.

Se firmó el contrato Nro. EMELNORTE-034-2025 “REEMPLAZO FIREWALL PERIMETRAL”, con fecha 13 de marzo de 2025.

Se realizó la entrega de los equipos que comprenden el proyecto para el Plan de Separación de Redes IT y OT de EMELNORTE.

Ilustración 60. Entrega de Equipos Firewall

Ilustración 61. Firewall Perimetral

Ilustración 62. Firewall DataCenter

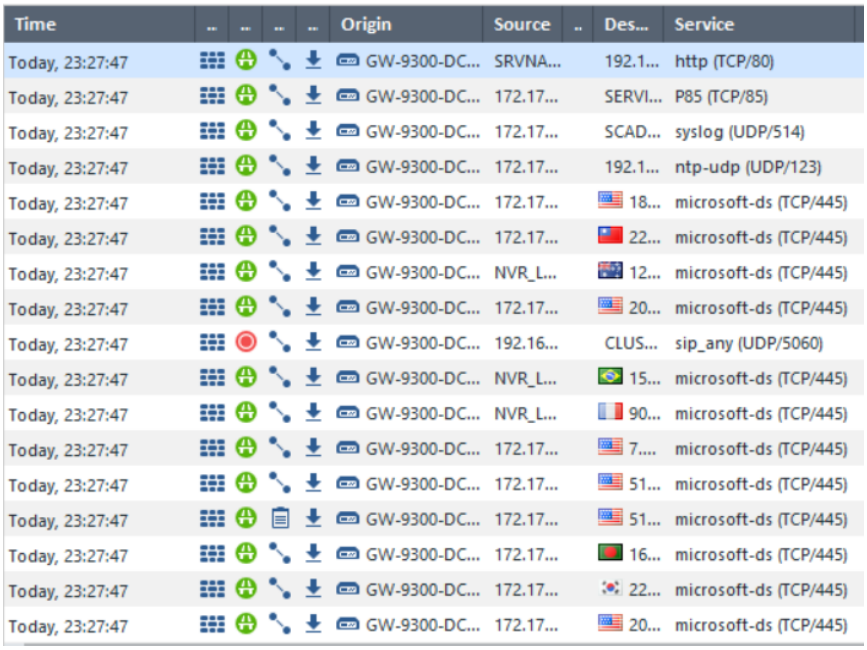
Ilustración 63. Firewall OT

Ilustración 64. Firewall de Subestaciones y Centrales

Ilustración 65. Consola de gestión

Status	Name
✓	CL-MTZ-01
✓	CLUSTER-9100-FWOT
✓	GW-9100-OT-01
✓	GW-9100-OT-02
✓	CLUSTER-9200-PERIMETRAL
✓	GW-9200-PER-01
✓	GW-9200-PER-02
✓	CLUSTER-9300-DATACENTER
✓	GW-9300-DC-01
✓	GW-9300-DC-02
✓	GW-1800-CE-PLAYA-01
✓	GW-1800-CE-SMCAR-01
✓	GW-1800-SE-ANGEL-01
✓	GW-1800-SE-CANAN-01
✓	GW-1800-SE-CHOTA-01
✓	GW-1800-SE-COTAC-01

Ilustración 66. Consola de Logs



Time	Origin	Source	Des...	Service
Today, 23:27:47	GW-9300-DC...	SRVNA...	192.1...	http (TCP/80)
Today, 23:27:47	GW-9300-DC...	172.17...	SERVI...	P85 (TCP/85)
Today, 23:27:47	GW-9300-DC...	172.17...	SCAD...	syslog (UDP/514)
Today, 23:27:47	GW-9300-DC...	172.17...	192.1...	ntp-udp (UDP/123)
Today, 23:27:47	GW-9300-DC...	172.17...	18...	microsoft-ds (TCP/445)
Today, 23:27:47	GW-9300-DC...	172.17...	22...	microsoft-ds (TCP/445)
Today, 23:27:47	GW-9300-DC...	NVR_L...	12...	microsoft-ds (TCP/445)
Today, 23:27:47	GW-9300-DC...	172.17...	20...	microsoft-ds (TCP/445)
Today, 23:27:47	GW-9300-DC...	192.16...	CLUS...	sip_any (UDP/5060)
Today, 23:27:47	GW-9300-DC...	NVR_L...	15...	microsoft-ds (TCP/445)
Today, 23:27:47	GW-9300-DC...	NVR_L...	90...	microsoft-ds (TCP/445)
Today, 23:27:47	GW-9300-DC...	172.17...	7....	microsoft-ds (TCP/445)
Today, 23:27:47	GW-9300-DC...	172.17...	51...	microsoft-ds (TCP/445)
Today, 23:27:47	GW-9300-DC...	172.17...	51...	microsoft-ds (TCP/445)
Today, 23:27:47	GW-9300-DC...	172.17...	16...	microsoft-ds (TCP/445)
Today, 23:27:47	GW-9300-DC...	172.17...	22...	microsoft-ds (TCP/445)
Today, 23:27:47	GW-9300-DC...	172.17...	20...	microsoft-ds (TCP/445)

CONCLUSIONES

Los resultados del estudio confirman que la separación de los servicios de red IT y OT en EMELNORTE contribuye significativamente a mejorar la ciberseguridad y la eficiencia operativa. En función de los objetivos planteados, se concluye que:

Evaluación de la arquitectura actual: El diagnóstico de la arquitectura de red original evidenció una integración excesiva entre los entornos IT y OT, con escasa segmentación y múltiples puntos de exposición a ciberamenazas. Esta situación representaba un riesgo alto para la infraestructura crítica de la organización. El análisis permitió identificar las principales vulnerabilidades y justificar técnicamente la necesidad de una separación estructural entre ambos dominios.

Diseño de una arquitectura de red segmentada: Se diseñó una arquitectura basada en el modelo Purdue y en buenas prácticas internacionales como las definidas por NIST SP 800-82 e ISA/IEC 62443. El nuevo diseño establece segmentos de red bien definidos para IT y OT, con zonas de demilitarización (DMZ), firewalls, políticas de acceso estrictas y rutas de comunicación controladas. La segmentación mejora la visibilidad, el control y la resiliencia de la red ante incidentes.

Implementación de medidas de seguridad cibernética: Se aplicaron controles de seguridad orientados a la defensa en profundidad, incluyendo firewalls industriales, autenticación reforzada, protocolos seguros y control de tráfico interzonal. La implementación fue evaluada mediante un sistema de puntuación multicriterio que asignó un **puntaje total de 3.73 sobre 5.0 (74.6%)**, clasificando el impacto como **ALTO**. Esta valoración confirma que las medidas adoptadas redujeron la superficie de ataque y elevaron el nivel de protección del entorno OT.

Evaluación del impacto de la eficiencia operativa: La separación de redes no solo reforzó la ciberseguridad, sino que también contribuyó positivamente a la eficiencia operativa. Se evidenciaron mejoras en la disponibilidad de los sistemas, reducción de incidentes técnicos, y mejor respuesta ante contingencias. Además, el análisis económico mostró un balance favorable entre costos y beneficios, destacando la reducción de riesgos como una fuente indirecta de ahorro y continuidad operativa.

RECOMENDACIONES

Realizar evaluaciones periódicas para validar la efectividad de las medidas de seguridad.

Fortalecer la concienciación en ciberseguridad para los equipos de IT y OT.

Explorar tecnologías emergentes como inteligencia artificial para detección de amenazas.

Revisar periódicamente las políticas de control de acceso y aplicación de actualizaciones.

Desarrollar estrategias de continuidad del negocio en caso de incidentes.

Referencias

Ackerman, R. (2018). *Cybersecurity Risks to the Electric Grid: NISTIR 7628 Revision 1*. *National Institute of Standards and Technology*.

Amiri, A., Steindl, G., & Hollerer, S. (2024). Integrated safety and security by design in the IT/OT convergence of industrial cyber-physical systems: A graph-based approach. En Proceedings of the 7th IEEE International Conference on Industrial Cyber-Physical Systems (pp. 1-2). IEEE. https://doi.org/10.1109/ICPS59941.2024.10640023

Arguello, B., Johnson, E. S., & Gearhart, J. L. (2021). A trilevel model for segmentation of the power transmission grid cyber network. arXiv. https://arxiv.org/abs/2108.10958

Bhole, M., Kastner, W., & Sauter, T. (2024). IT security solutions for IT/OT integration: Identifying gaps and opportunities. En Proceedings of the 2024 IEEE 29th International Conference on Emerging Technologies and Factory Automation (pp. 1-8). IEEE. https://doi.org/10.1109/ETFA61755.2024.10710968

Cisco. (2019). *Cybersecurity for Industry 4.0: A Cisco Perspective on Securing the Industrial Network.* Cisco Systems, Inc.: https://www.cisco.com/c/dam/en/us/solutions/collateral/industry-solutions/white-paper-c11-739565.pdf

Commission, I. E. (2018). *ISA/IEC 62443-3-3: Security for industrial automation and control systems — System security requirements and security levels*. https://webstore.iec.ch/publication/60225

Commission, I. E. (2024). *https://www.iec.ch/standards*.

Commission, I. O. (2024). *https://www.iso.org/standard/85056.html*.

Control Engineering. (2021, abril 8). What the IEC 62443 standard does for industrial cybersecurity. Control Engineering. Recuperado de https://www.controleng.com (Ofrece una visión integral del ciclo de vida ICS/OT: evaluación, implementación, mantenimiento y protección de redes eléctricas industriales usadas en infraestructura crítica)

Dehlaghi-Ghadim, A., Balador, A., Helali Moghadam, M., Hansson, H., & Conti, M. (2022). ICSSIM – A framework for building industrial control systems security simulation testbeds. arXiv. https://doi.org/10.48550/arXiv.2210.13325

Device Authority. (2025, marzo 4). Securing industrial IoT and OT with the Purdue model. DirectorsTalk. Recuperado de https://directorstalk.net/securing-industrial-iot-and-ot-with-the-purdue-model

Dragos. (2023). *ICS/OT Cybersecurity Year in Review*. https://www.dragos.com/year-in-review/2023

Goodchild, P. (2020). *Cyber Security and the Electric Power Industry: Industry Practices and Future Challenges. Electric Power Research Institute*.

Hossain, M. S., Islam, M. S., & Rahman, M. A. (2024). A cyber range framework for emulating secure and private IT/OT consumer service verticals toward 6G. IEEE Transactions on Consumer Electronics, 70(2), 4709-4716. https://doi.org/10.1109/TCE.2024.3387055

ISA. (2000). *Enterprise-Control System Integration - Part 1: Models and Terminology*. International Society of Automation.

Jaén, F. S. (2021). *Ciberseguridad Industrial e Infraestructuras Críticas*. RA-MA Editorial.

Kampa, T., Müller, C. K., & Großmann, D. (2024). Interlocking IT/OT security for edge cloud-enabled manufacturing. Ad Hoc Networks, 154, Art. 103384. https://doi.org/10.1016/j.adhoc.2023.103384

Kandasamy, K. W. (2020). *Cybersecurity risks in IT/OT convergence: A threat modeling approach. Journal of Cybersecurity, 6(1), 1–12*. https://doi.org/10.1093/cybsec/tyaa005

Keyfactor. (2024). Mastering IEC 62443: A guide to securing industrial automation and control systems. Recuperado de https://www.keyfactor.com (Particularmente IEC 62443-4-2 para componentes IACS, autentificación, cifrado, respuesta a incidentes)

Kheddar, H., Himeur, Y., & Awad, A. I. (2023). Deep transfer learning for intrusion detection in industrial control networks: A comprehensive review. arXiv. https://doi.org/10.48550/arXiv.2304.10550

Kumar, S., & Vardhan, H. (2025). Cyber security of OT networks: A tutorial and overview. arXiv. https://arxiv.org/abs/2502.14017

Landis+Gyr / Rhebo. (2025). Cyber security according to IEC 62443 in the energy sector. Recuperado de https://eu.landisgyr.com (Destaca la aplicación del capítulo 3-2 de evaluación de riesgos en infraestructuras eléctricas, mapeo de red, anomalías y segmentación)

Lee, C., & Kim, D. (2021). "Securing Operational Technology Networks: Best Practices and Case Studies". 89-102.

National Institute of Standards and Technology. (2023). Guide to operational technology (OT) security (NIST SP 800-82 Rev. 3). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-82r3

National Institute of Standards and Technology. (2023, abril 6). Security segmentation in a small manufacturing environment (NIST CSWP 28). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.28

OWASPFoundation. (2021). *OWASP TOP 10:2021*. https://owasp.org/Top10/

Serrano, M. A., Fernández-Medina, E., Alcaraz, C., De Castro, N., & Calvo, G. (2021). Investigación en ciberseguridad: Actas de las VI Jornadas Nacionales (JNIC2021 LIVE). Ediciones de la Universidad de Castilla La Mancha.

Smith, J., & Johnson, A. (2020). "Security Challenges in Operational Technology Networks: A Review". *8*(2), 123-137.

Standardization, I. O. (2022). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. https://www.iso.org/standard/82875.html

Stouffer, K. F. (2011). *Guide to Industrial Control Systems (ICS) Security. National Institute of Standards and Technology (NIST) Special Publication 800-82*.

Stouffer, K. P. (2022). *Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity*. . https://doi.org/NIST

Technology, N. I. (2023). *https://doi.org/10.6028/NIST.SP.800-82r3*.

Vacca, J. R. (2020). *Cyber Security and IT Infrastructure Protection. Syngress*.

Varghese, S. A., Dehlaghi Ghadim, A., Balador, A., Alimadadi, Z., & Papadimitratos, P. (2022). Digital twin-based intrusion detection for industrial control systems. arXiv. https://doi.org/10.48550/arXiv.2207.09999

Waclawek, H., Schäfer, G., Binder, C., Hirsch, E., & Huber, S. (2023). Digital twins of business processes as enablers for IT/OT integration. En Proceedings of the 2023 IEEE 21st International Conference on Industrial Informatics. IEEE.

Wang, Q., & Chen, S. (2019). "Cybersecurity Framework for Critical Infrastructure Protection in Operational Technology Environments". 2000-2012.

Wetzels, J., dos Santos, D., & Ghafari, M. (2023). Insecure by design in the backbone of critical infrastructure. arXiv. https://arxiv.org/abs/2303.12340

Zahran, B., Hussaini, A., & Ali-Gombe, A. (2023). Security of IT/OT convergence: Design and implementation challenges. arXiv. https://arxiv.org/abs/2302.09426

Zhang, Y. D. (2021). *Industrial control system security: Threats, challenges and solutions*. Computers & Security, 102, 102148.: https://doi.org/10.1016/j.cose.2020.102148

ANEXOS

Ilustración 67. Encuesta funcionario 1 Página 1

EmelNorte

Encuesta sobre la Separación de Redes IT y OT

Objetivo: Conocer el nivel de conocimiento, percepción de riesgos y prácticas en la segmentación de redes IT y OT en servicios críticos.

1. ¿Qué nivel de conocimiento tiene sobre la separación de redes IT y OT?

   - [x] Básico
   - [ ] Intermedio
   - [ ] Avanzado

2. ¿Cuáles considera que son los principales riesgos de no separar las redes IT y OT? (Seleccione hasta 3 opciones)

   - [x] Ciberataques
   - [ ] Pérdida de datos
   - [ ] Interrupción operativa
   - [ ] Acceso no autorizado
   - [ ] Otros (especificar) _____

3. ¿Su empresa ha implementado una estrategia de segmentación de redes IT y OT?

   - [x] Sí
   - [ ] No
   - [ ] En proceso

Dir. Matriz
Grijalva 654 y Olmedo, Ibarra - Ec.
Telf.: (06) 2997 100
Call Center: 136

www. emelnorte.com

Ilustración 68. Encuesta funcionario 1 Página 2

EmelNorte

4. ¿Qué estándares o normativas de seguridad considera más relevantes para la segmentación de redes IT y OT? (Seleccione hasta 3 opciones)

   - [x] ISO/IEC 27001
   - [ ] NIST SP 800-82
   - [x] IEC 62443
   - [ ] CIS Controls
   - [ ] Otros (especificar) _____

5. ¿Considera que su organización tiene suficiente capacitación en ciberseguridad industrial?

   - [x] Sí
   - [ ] No
   - [ ] Parcialmente

Dir. Matriz
Grijalva 654 y Olmedo, Ibarra - Ec.
Telf.: (06) 2997 100
Call Center: 136

www.emelnorte.com

Ilustración 69. Encuesta funcionario 2 Página 1

EmelNorte

Encuesta sobre la Separación de Redes IT y OT

Objetivo: Conocer el nivel de conocimiento, percepción de riesgos y prácticas en la segmentación de redes IT y OT en servicios críticos.

1. ¿Qué nivel de conocimiento tiene sobre la separación de redes IT y OT?

   ☐ Básico

   ☒ Intermedio

   ☐ Avanzado

2. ¿Cuáles considera que son los principales riesgos de no separar las redes IT y OT?

   (Seleccione hasta 3 opciones)

   ☒ Ciberataques

   ☐ Pérdida de datos

   ☒ Interrupción operativa

   ☐ Acceso no autorizado

   ☐ Otros (especificar) _____

3. ¿Su empresa ha implementado una estrategia de segmentación de redes IT y OT?

   ☐ Sí

   ☒ No

   ☐ En proceso

Dir. Matriz
Grijalva 654 y Olmedo, Ibarra - Ec.
Telf.: (06) 2997 100
Call Center: 136

www. emelnorte.com

Ilustración 70. Encuesta funcionario 2 Página 2

EmelNorte

4. ¿Qué estándares o normativas de seguridad considera más relevantes para la segmentación de redes IT y OT? (Seleccione hasta 3 opciones)

   ☐ ISO/IEC 27001

   ☒ NIST SP 800-82

   ☐ IEC 62443

   ☒ CIS Controls

   ☐ Otros (especificar) _____

5. ¿Considera que su organización tiene suficiente capacitación en ciberseguridad industrial?

   ☐ Sí

   ☒ No

   ☐ Parcialmente

Dir. Matriz
Grijalva 654 y Olmedo, Ibarra - Ec.
Telf.: (06) 2997 100
Call Center: 136

www.emelnorte.com

Ilustración 71. Encuesta funcionario 3 Página 1

EmelNorte

Encuesta sobre la Separación de Redes IT y OT

Objetivo: Conocer el nivel de conocimiento, percepción de riesgos y prácticas en la segmentación de redes IT y OT en servicios críticos.

1. ¿Qué nivel de conocimiento tiene sobre la separación de redes IT y OT?

   ☐ Básico

   ☐ Intermedio

   ☒ Avanzado

2. ¿Cuáles considera que son los principales riesgos de no separar las redes IT y OT? (Seleccione hasta 3 opciones)

   ☒ Ciberataques

   ☒ Pérdida de datos

   ☐ Interrupción operativa

   ☒ Acceso no autorizado

   ☐ Otros (especificar) _____

3. ¿Su empresa ha implementado una estrategia de segmentación de redes IT y OT?

   ☐ Sí

   ☐ No

   ☒ En proceso

Dir. Matriz
Grijalva 654 y Olmedo, Ibarra - Ec.
Telf.: (06) 2997 100
Call Center: 136

www.emelnorte.com

Ilustración 72. Encuesta funcionario 3 Página 2

EmelNorte

4. ¿Que estandares o normativas de seguridad considera mas relevantes para la segmentacion de redes IT y OT? (Seleccione hasta 3 opciones)

- ☐ ISO/IEC 27001
- ☒ NIST SP 800-82
- ☒ IEC 62443
- ☐ CIS Controls
- ☐ Otros (especificar) _____

5. ¿Considera que su organización tiene suficiente capacitación en ciberseguridad industrial?

- ☐ Si
- ☐ No
- ☒ Parcialmente

Dir. Matriz
Urgalva 656 y Olmedo, Ibarra - Ec
Telf.: (06) 2997 300
Call Center: 156

www.emelnorte.com

Ilustración 73. Encuesta funcionario 4 Página 1

EmelNorte

Encuesta sobre la Separación de Redes IT y OT

Objetivo: Conocer el nivel de conocimiento, percepción de riesgos y prácticas en la segmentación de redes IT y OT en servicios críticos.

1. ¿Qué nivel de conocimiento tiene sobre la separación de redes IT y OT?

   - ☐ Básico
   - ☒ Intermedio
   - ☐ Avanzado

2. ¿Cuáles considera que son los principales riesgos de no separar las redes IT y OT? (Seleccione hasta 3 opciones)

   - ☐ Ciberataques
   - ☒ Pérdida de datos
   - ☒ Interrupción operativa
   - ☐ Acceso no autorizado
   - ☐ Otros (especificar) _____

3. ¿Su empresa ha implementado una estrategia de segmentación de redes IT y OT?

   - ☒ Sí
   - ☐ No
   - ☐ En proceso

Dir. Matriz
Grijalva 654 y Olmedo, Ibarra - Ec.
Telf.: (06) 2997 100
Call Center: 136

www.emelnorte.com

Ilustración 74. Encuesta funcionario 4 Página 2

EmelNorte

4. ¿Qué estándares o normativas de seguridad considera más relevantes para la segmentación de redes IT y OT? (Seleccione hasta 3 opciones)

   - [x] ISO/IEC 27001
   - [ ] NIST SP 800-82
   - [ ] IEC 62443
   - [x] CIS Controls
   - [ ] Otros (especificar) _____

5. ¿Considera que su organización tiene suficiente capacitación en ciberseguridad industrial?

   - [x] Sí
   - [ ] No
   - [ ] Parcialmente

Dir. Matriz
Grijalva 654 y Olmedo, Ibarra - Ec.
Telf.: (06) 2997 100
Call Center: 136

www.emelnorte.com

Ilustración 75. Encuesta funcionario 5 Página 1

EmelNorte

Encuesta sobre la Separación de Redes IT y OT

Objetivo: Conocer el nivel de conocimiento, percepción de riesgos y prácticas en la segmentación de redes IT y OT en servicios críticos.

1. ¿Qué nivel de conocimiento tiene sobre la separación de redes IT y OT?

   - [x] Básico
   - [ ] Intermedio
   - [ ] Avanzado

2. ¿Cuáles considera que son los principales riesgos de no separar las redes IT y OT?

   (Seleccione hasta 3 opciones)

   - [x] Ciberataques
   - [ ] Pérdida de datos
   - [x] Interrupción operativa
   - [ ] Acceso no autorizado
   - [ ] Otros (especificar) _____

3. ¿Su empresa ha implementado una estrategia de segmentación de redes IT y OT?

   - [ ] Sí
   - [x] No
   - [ ] En proceso

Dir. Matriz
Grijalva 654 y Olmedo, Ibarra - Ec.
Telf.: (06) 2997 100
Call Center: 136

www.emelnorte.com

Ilustración 76. Encuesta funcionario 5 Página 2

EmelNorte

4. ¿Qué estándares o normativas de seguridad considera más relevantes para la segmentación de redes IT y OT? (Seleccione hasta 3 opciones)

   - [X] ISO/IEC 27001
   - [ ] NIST SP 800-82
   - [X] IEC 62443
   - [ ] CIS Controls
   - [ ] Otros (especificar) _____

5. ¿Considera que su organización tiene suficiente capacitación en ciberseguridad industrial?

   - [ ] Sí
   - [X] No
   - [ ] Parcialmente

Dir. Matriz
Grijalva 654 y Olmedo, Ibarra - Ec.
Telf.: (06) 2997 100
Call Center: 136

www.emelnorte.com

Ilustración 77. Encuesta funcionario 6 Página 1

EmelNorte

Encuesta sobre la Separación de Redes IT y OT

Objetivo: Conocer el nivel de conocimiento, percepción de riesgos y prácticas en la segmentación de redes IT y OT en servicios críticos.

1. ¿Qué nivel de conocimiento tiene sobre la separación de redes IT y OT?

   ☐ Básico

   ☐ Intermedio

   ☒ Avanzado

2. ¿Cuáles considera que son los principales riesgos de no separar las redes IT y OT? (Seleccione hasta 3 opciones)

   ☒ Ciberataques

   ☐ Pérdida de datos

   ☐ Interrupción operativa

   ☒ Acceso no autorizado

   ☐ Otros (especificar) _____

3. ¿Su empresa ha implementado una estrategia de segmentación de redes IT y OT?

   ☒ Sí

   ☐ No

   ☐ En proceso

Dir. Matríz
Grijalva 654 y Olmedo. Ibarra - Ec.
Telf.: (06) 2997 100
Call Center: 136

www. emelnorte.com

Ilustración 78. Encuesta funcionario 6 Página 2

EmelNorte

4. ¿Qué estandares o normativas de seguridad considera más relevantes para la segmentacion de redes IT y OT? (Seleccione hasta 3 opciones)

- ☐ ISO/IEC 27001
- ☒ NIST SP 800-82
- ☒ IEC 62443
- ☐ CIS Controls
- ☐ Otros (especificar) _____

5. ¿Considera que su organización tiene suficiente capacitación en ciberseguridad industrial?

- ☐ Si
- ☐ No
- ☒ Parcialmente

Dir. Matriz
Grijalva 6-56 y Olmedo, Ibarra - Ec
Telf.: (06) 2997 300
Call Center: 156

www.emelnorte.com

Ilustración 79. Encuesta funcionario 7 Página 1

EmelNorte

Encuesta sobre la Separación de Redes IT y OT

Objetivo: Conocer el nivel de conocimiento, percepción de riesgos y prácticas en la segmentación de redes IT y OT en servicios críticos.

1. ¿Qué nivel de conocimiento tiene sobre la separación de redes IT y OT?

   ☐ Básico

   ☒ Intermedio

   ☐ Avanzado

2. ¿Cuáles considera que son los principales riesgos de no separar las redes IT y OT? (Seleccione hasta 3 opciones)

   ☒ Ciberataques

   ☒ Pérdida de datos

   ☐ Interrupción operativa

   ☐ Acceso no autorizado

   ☐ Otros (especificar) _____

3. ¿Su empresa ha implementado una estrategia de segmentación de redes IT y OT?

   ☐ Sí

   ☐ No

   ☒ En proceso

Dir. Matriz
Grijalva 654 y Olmedo, Ibarra - Ec.
Telf.: (06) 2997 100
Call Center: 136

www.emelnorte.com

Ilustración 80. Encuesta funcionario 7 Página 2

EmelNorte

4. ¿Qué estándares o normativas de seguridad considera más relevantes para la segmentación de redes IT y OT? (Seleccione hasta 3 opciones)

   ☐ ISO/IEC 27001

   ☒ NIST SP 800-82

   ☐ IEC 62443

   ☒ CIS Controls

   ☐ Otros (especificar) _____

5. ¿Considera que su organización tiene suficiente capacitación en ciberseguridad industrial?

   ☐ Sí

   ☒ No

   ☐ Parcialmente

Dir. Matríz
Grijalva 654 y Olmedo, Ibarra - Ec.
Telf.: (06) 2997 100
Call Center: 136

www.emelnorte.com