

**UNIVERSIDAD SANTO TOMÁS DE AQUINO
SECCIONAL TUNJA**

FACULTAD DE INGENIERÍA ELECTRÓNICA



UNIVERSIDAD
SANTO TOMÁS
TUNJA

VIGILADA MINEDUCACIÓN - SNIES 1732

**ESTUDIO TÉCNICO COMPARATIVO PARA LA SELECCIÓN
DE EQUIPOS Y ARQUITECTURAS DE CIBERSEGURIDAD
IT/OT EN EBSA, BASADO EN LAS NORMAS IEC 62443 E
IEC 62351**

Monografía presentada por:

BARÓN ARIAS JUAN PABLO

Para optar al título de:

INGENIERO ELECTRÓNICO

Tunja, Boyacá Colombia

2026

UNIVERSIDAD SANTO TOMÁS
SECCIONAL TUNJA

FACULTAD DE INGENIERÍA ELECTRÓNICA



UNIVERSIDAD
SANTO TOMÁS
TUNJA

VIGILADA MINEDUCACIÓN - SNIES 1732

**ESTUDIO TÉCNICO COMPARATIVO PARA LA SELECCIÓN
DE EQUIPOS Y ARQUITECTURAS DE CIBERSEGURIDAD
IT/OT EN EBSA, BASADO EN LAS NORMAS IEC 62443 E
IEC 62351**

Monografía presentada por:

Barón Arias Juan Pablo

Director:

Ph.D. William Fabián Chaparro Becerra

Codirectores:

M.Sc. Angélica María Salazar Madrigal

M.Sc. Cristian David Camacho Parra

Tunja, Boyacá Colombia

2026

Dedicatoria

Dedico este trabajo, en primer lugar, a Dios, por brindarme la fortaleza, la sabiduría y la perseverancia necesarias para culminar esta etapa de mi formación profesional. Su guía constante ha sido el fundamento que me permitió superar los desafíos académicos y personales que se presentaron a lo largo de este proceso.

A mi familia y a mi pareja, quienes han sido mi apoyo incondicional en cada momento. Gracias por su comprensión, paciencia y confianza en mí. Su respaldo, consejos y sacrificios han sido la motivación principal para alcanzar esta meta. Cada logro obtenido es también resultado de su amor y acompañamiento permanente.

Este trabajo representa no solo un logro académico, sino también el fruto del esfuerzo compartido con quienes han creído en mí desde el inicio.

Agradecimientos

Agradezco en primer lugar a Dios, por darme la fortaleza, la paciencia y la sabiduría necesarias para culminar esta etapa tan importante de mi vida. En cada momento de dificultad encontré en Él la guía y la motivación para continuar.

A mi familia y a mi pareja, por su apoyo incondicional, por su comprensión en los momentos de dedicación intensa y por creer siempre en mis capacidades. Su amor, sacrificio y confianza han sido el motor que me impulsó a no rendirme y a alcanzar esta meta.

A mi director, Ph.D. William Fabián Chaparro Becerra, por su acompañamiento y orientación académica a lo largo del desarrollo de este proyecto. A los codirectores, M.Sc. Angélica María Salazar Madrigal y M.Sc. Cristian David Parra Camacho, por sus aportes técnicos y su disposición para enriquecer este trabajo.

A la Empresa de Energía de Boyacá (EBSA), por la apertura brindada para el desarrollo del estudio, por el interés en fortalecer sus procesos y por permitir que este trabajo se fundamentara en un contexto real del sector eléctrico. Su disposición fue clave para orientar el enfoque práctico de la investigación.

Finalmente, agradezco a todas las personas que de una u otra manera hicieron parte de este proceso y contribuyeron a mi crecimiento académico y personal.

Índice general

1	Introducción	1
1.1	Planteamiento del problema	2
1.2	Contexto del entorno IT/OT en la Empresa de Energía de Boyacá (EBSA)	3
1.3	Formulación de Pregunta	4
1.4	Justificación	4
2	Objetivos	6
2.1	Objetivo General	6
2.2	Objetivos Específicos	6
3	Marco teórico	7
3.1	Tecnologías de la información (IT) y Tecnologías de la Operación (OT) en empresas del sector energético	7
3.1.1	Tecnologías de la Operación (OT)	7
3.1.2	Tecnologías de la Información (IT)	8
3.1.3	Diferencias fundamentales entre IT y OT	8
3.1.4	Convergencia IT-OT en empresas de energía	9
3.1.5	Activos y flujos de información que requieren protección	9
3.2	Ciberseguridad en infraestructuras críticas	11
3.2.1	Infraestructuras críticas y su relación con la ciberseguridad	11
3.2.2	Particularidades de la ciberseguridad en entornos OT	11
3.2.3	Amenazas cibernéticas en infraestructuras energéticas	12
3.2.4	Enfoques de Protección para infraestructuras críticas	13
3.3	Modelo de ciberseguridad basado en la norma IEC 62443	13
3.3.1	La norma IEC 62443 y su enfoque en infraestructuras industriales	13
3.3.2	Concepto de zonas y conductos (Zones & Conduits)	13
3.3.3	Defensa en profundidad según IEC 62443	14
3.3.4	Niveles de Seguridad (Security Levels - SL)	15
3.3.5	Relación entre IEC 62443 y la selección de equipos	16
3.4	Seguridad de las comunicaciones en sistemas eléctricos	16
3.4.1	La norma IEC 62351 en el contexto del sector eléctrico	16
3.4.2	Alcance de la norma IEC 62351	16
3.4.3	Protección de las comunicaciones basada en TCP-IP (IEC 62351-3)	17
3.4.4	Autenticación, integridad y confidencialidad de la información . .	17
3.4.5	Gestión de claves y certificados digitales	18
3.4.6	Relación entre IEC 62351 y los flujos de información IT-OT	18
3.4.7	Implicaciones de IEC 62351 para la selección de equipos	18
3.5	Marco regulatorio colombiano aplicable a EBSA	19
3.5.1	Comisión de Regulación de Energía y Gas (CREG)	19

3.5.2	Superintendencia de Servicios Públicos Domiciliarios (SSPD)	20
3.5.3	Reglamento Técnico de Instalaciones Eléctricas (RETIE)	20
3.5.4	Política de Protección de Infraestructura Crítica	21
3.5.5	Relación entre el marco regulatorio colombiano y las normas IEC 62443 e IEC 62351	21
4	Metodología	22
4.1	Enfoque y tipo de investigación	22
4.2	Ámbito de aplicación del estudio	22
4.3	Fases Metodológicas	23
4.3.1	Fase 1: Revisión documental y análisis normativo	23
4.3.2	Fase 2: Caracterización conceptual de entornos IT y OT	23
4.3.3	Fase 3: Definición de criterios técnicos de evaluación	24
4.3.4	Fase 4: Evaluación técnica comparativa de alternativas	25
4.3.5	Fase 5: Propuesta de arquitectura de referencia y análisis de resultados	25
4.4	Técnicas e Instrumentos de investigación	26
4.5	Construcción de la matriz de criterios de evaluación	26
4.5.1	Estructura general de la matriz de criterios	26
4.5.1.1	Trazabilidad entre requisitos normativos y criterios de evaluación	27
4.5.2	Criterios de cumplimiento normativo	28
4.5.3	Criterios de arquitectura y segmentación	29
4.5.4	Criterio de seguridad de las comunicaciones	29
4.5.5	Criterios de control, monitoreo y gestión	29
4.5.6	Criterios operativos y de viabilidad	30
4.6	Metodología de evaluación aplicada a las tecnologías	30
4.6.1	Aplicación de la matriz de criterios	30
4.6.2	Escala de evaluación	30
4.7	Alcance del análisis de equipos y arquitecturas de ciberseguridad	31
4.8	Validez, confiabilidad y replicabilidad del método	31
5	Desarrollo de las Fases Metodológicas	33
5.1	Definición del caso de estudio	33
5.2	Caracterización técnica del escenario IT-OT	34
5.2.1	Descripción general del entorno IT	34
5.2.2	Descripción general del entorno OT	35
5.2.3	Clasificación de activos críticos según nivel de criticidad para la empresa EBSA	36
5.2.4	Interacción y flujos de información entre IT y OT	37
5.3	Identificación de activos críticos y flujos de información	38
5.3.1	Identificación de activos IT relevantes	38
5.3.2	Identificación de activos OT relevantes	39
5.3.3	Identificación de flujos de información críticos	40
5.3.4	Riesgos asociados a los flujos IT-OT	41
5.4	Definición de requisitos técnicos de ciberseguridad	41
5.4.1	Requisitos técnicos derivados de la norma IEC 62443	41
5.4.2	Requisitos técnicos derivados de la norma IEC 62351	42
5.4.3	Requisitos técnicos operativos y de continuidad	44

5.4.4	Síntesis de requisitos técnicos de ciberseguridad	44
5.5	Análisis de certificaciones y exigencias normativas aplicables a EBSA . .	44
5.5.1	Relación entre requisitos normativos y aplicación en EBSA	46
5.6	Evaluación técnica comparativa de tecnologías de ciberseguridad	47
5.6.1	Enfoque general de la evaluación	47
5.6.2	Clasificación de tecnologías de ciberseguridad analizadas	48
5.6.2.1	Switches industriales gestionables	48
5.6.2.2	Firewalls industriales - Firewalls OT	48
5.6.2.3	Gateways de seguridad IT-OT	49
5.6.2.4	Dispositivos de cifrado y protección de comunicaciones .	49
5.6.2.5	Sistemas de monitoreo y detección para entornos OT . .	49
5.6.3	Análisis comparativo por tipo de tecnología	49
5.6.3.1	Evaluación comparativa de Switches industriales gestionables	49
5.6.3.2	Evaluación comparativa de Firewalls industriales	54
5.6.3.3	Evaluación comparativa de Gateways IT/OT	59
6	Resultados	64
6.1	Conversión del análisis cualitativo a cuantitativo	64
6.2	Resultados por tipo de tecnología	65
6.2.1	Resultados del análisis cuantitativo de switches industriales	65
6.2.2	Resultados del análisis cuantitativo de firewalls industriales	66
6.2.3	Resultados del análisis cuantitativo de Gateways	67
6.3	Resultados con ayuda de simulación (GNS3)	68
6.3.1	Escenario sin segmentación restrictiva	69
6.3.2	Escenario con segmentación conforme a IEC 62443	70
6.3.3	Análisis técnico de los resultados simulados	70
6.3.3.1	Análisis de indicadores de seguridad	71
6.4	Estimación presupuestaria para la compra de equipos de subestación . .	72
7	Discusión	74
7.1	Validez metodológica del enfoque adoptado	74
7.2	Discusión sobre la matriz de criterios y la ponderación basada en IEC 62443	74
7.3	Importancia de la segmentación IT/OT evidenciada experimentalmente .	75
7.4	Discusión sobre la aplicabilidad real en la empresa	75
7.5	Limitaciones del estudio y trabajos futuros	75
7.6	Aporte del estudio	76
	Conclusiones	77
	Referencias	78

Índice de figuras

Figura 3.1.1	Cuadro comparativo IT-OT	8
Figura 3.1.2	Diagrama causa efecto riesgos de compromiso	10
Figura 3.1.3	Diagrama de Pareto riesgos de compromiso	10
Figura 3.2.1	Riesgos en compromiso en la infraestructura.	11
Figura 3.2.2	Taxonomía de los ataques a la cadena de suministros	12
Figura 3.3.1	Modelo Purdue de un sistema industrial dividido en zonas	14
Figura 3.3.2	Defensa en profundidad	15
Figura 3.3.3	Niveles de seguridad IEC 62443	15
Figura 3.4.1	Componentes de seguridad contemplados por IEC 62351.	17
Figura 3.5.1	Logo EBSA	19
Figura 5.2.1	Entorno IT	35
Figura 5.2.2	Entorno OT	36
Figura 5.3.1	Activos IT	39
Figura 5.3.2	Activos OT presentes	40
Figura 5.3.3	Flujos de información industriales	40
Figura 5.4.1	Infografía-IEC-62443	42
Figura 5.4.2	Infografía-IEC-62351	43
Figura 5.6.1	Switch 1: Siemens RUGGEDCOM RST2228	51
Figura 5.6.2	Switch 2: Hirschmann RSP25	52
Figura 5.6.3	Switch 3: Cisco Industrial Ethernet IE 4000	53
Figura 5.6.4	Siemens SCALANCE S615	56
Figura 5.6.5	Hirschmann EAGLE40/EAGLE One	57
Figura 5.6.6	Firewall 3: Fortinet FortiGate Rugged(FortiGateR)	58
Figura 5.6.7	Gateway 1: Siemens SCALANCE M876	61
Figura 5.6.8	Gateway 2: Hirschmann EAGLE One	61
Figura 5.6.9	Gateway 3: Fortinet FortiGate Rugged Modo Gateway	62
Figura 6.2.1	Ejemplo Matriz con ponderaciones (Cuantitativo)	65
Figura 6.2.2	Calculo Swiches Cuantitativo	65
Figura 6.2.3	Calculo Firewalls Cuantitativo	66
Figura 6.2.4	Calculo Gateways Cuantitativo	67
Figura 6.3.1	Arquitectura del escenario OT crítico basada en zonas (IT/OT) y conductos (Firewall).	68
Figura 6.3.2	Resultado del escaneo de puertos desde la zona IT hacia la red OT con y sin políticas de segmentación activas.	70
Figura 6.3.3	Gráfico de indicadores de seguridad del sistema SCADA Simulado.	71

Índice de tablas

Tabla 4.5.1 Matriz de criterios para la evaluación de tecnologías de ciberseguridad IT/OT	27
Tabla 4.5.2 Trazabilidad entre criterios de evaluación y requisitos normativos .	28
Tabla 5.2.1 Clasificación de activos OT según criticidad e impacto	37
Tabla 5.5.1 Relación entre requisitos IEC y aplicación en EBSA	47
Tabla 5.6.1 Comparación técnica de switches industriales evaluados	50
Tabla 5.6.2 Evaluación cualitativa de switches industriales según la matriz de criterios	54
Tabla 5.6.3 Comparación técnica de firewalls industriales evaluados	55
Tabla 5.6.4 Evaluación cualitativa de firewalls industriales según la matriz de criterios	59
Tabla 5.6.5 Comparación técnica de gateways IT/OT evaluados	60
Tabla 5.6.6 Evaluación cualitativa de gateways IT/OT según la matriz de criterios	63
Tabla 6.4.1 Estimación presupuestal para implementación de arquitectura de ciberseguridad en una subestación	72

Anexos

Anexo 1. Diagrama de pareto y espina de pescado

Enlace de consulta:

https://usantotomaseduco-my.sharepoint.com/:f:/g/personal/juan_baron_usantoto_edu_co/IgD2cSS6x19IR6u6FW0xnxQbAQcYKQxiIf2iFfBBlw74z-o?e=O84j6e

Anexo 2. Análisis Firewalls.

Enlace de consulta:

https://usantotomaseduco-my.sharepoint.com/:f:/g/personal/juan_baron_usantoto_edu_co/IgAsLKtPE_QSSqRTllqfM2IqAQsbBxC931eNffcCqjD7tIs?e=f5NLQh

Anexo 3. Análisis Gateways.

Enlace de consulta:

https://usantotomaseduco-my.sharepoint.com/:f:/g/personal/juan_baron_usantoto_edu_co/IgBcn2v4BH_dTYXxP6MKBPI5AUBffrTlJPh8MF7u9FscPjs?e=dJfUfE

Anexo 4. Análisis Switches.

Enlace de consulta:

https://usantotomaseduco-my.sharepoint.com/:f:/g/personal/juan_baron_usantoto_edu_co/IgBdBtLxUUb8Rq-wPmD1TccxAQzLmPiittysiqWCLK4u__Q?e=CWvupb

Anexo 5. Guía Experimental de Configuración y Validación de Seguridad IT/OT en GNS3.

Enlace de consulta:

https://usantotomaseduco-my.sharepoint.com/:f:/g/personal/juan_baron_usantoto_edu_co/IgAZZfZXGMrITap8fY6lnX64AZvToFYo7MaEfQk9RnYILyc?e=6bgCV9

Lista de abreviaturas y símbolos

IT	Information Technology (Tecnologías de la Información)
OT	Operational Technology (Tecnologías de la Operación)
IEC	International Electrotechnical Commission
IEC 62443	Norma internacional de ciberseguridad industrial
IEC 62351	Norma de seguridad para comunicaciones en sistemas eléctricos
SCADA	Supervisory Control and Data Acquisition
HMI	Human Machine Interface
LAN	Local Area Network
WAN	Wide Area Network
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
TLS	Transport Layer Security
IPsec	Internet Protocol Security
NAT	Network Address Translation
ACL	Access Control List
DoS	Denial of Service
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
GNS3	Graphical Network Simulator 3
CAPEX	Capital Expenditure
OPEX	Operational Expenditure

Resumen

La convergencia entre los entornos de Tecnologías de la Información (IT) y Tecnologías de la Operación (OT) en el sector eléctrico ha incrementado la superficie de exposición a riesgos cibernéticos, comprometiendo la seguridad de los activos críticos, la continuidad operativa y la confidencialidad de la información estratégica. En este contexto, el presente trabajo tuvo como objetivo realizar un estudio técnico comparativo para la selección de equipos y arquitecturas de ciberseguridad aplicables a los entornos IT y OT de la Empresa de Energía de Boyacá (EBSA), fundamentado en los lineamientos establecidos por las normas IEC 62443 e IEC 62351.

Inicialmente, se llevó a cabo la caracterización funcional de los entornos IT y OT, identificando activos críticos, flujos de información y puntos de interconexión susceptibles de riesgo. Posteriormente, se definieron los requisitos técnicos de seguridad a partir de estándares internacionales, traduciéndolos en criterios evaluables mediante una matriz comparativa estructurada. Dicha matriz permitió transformar criterios cualitativos en ponderaciones cuantitativas, reduciendo la subjetividad en la selección tecnológica y facilitando la toma de decisiones basada en evidencia.

Debido a las restricciones propias de una infraestructura crítica, no fue posible realizar pruebas directas sobre la red productiva de la empresa. Por ello, se implementó un entorno de simulación controlado en GNS3, donde se validaron experimentalmente escenarios de segmentación IT/OT, ejecución de ataques de reconocimiento, intentos de acceso no autorizado y generación de tráfico malicioso. Los resultados demostraron que la aplicación de políticas de segmentación basadas en el modelo de zonas y conductos reduce significativamente la superficie de ataque y fortalece la trazabilidad de eventos.

Finalmente, se realizó una estimación presupuestal para la implementación de la arquitectura propuesta en una subestación tipo, evidenciando la viabilidad económica de una modernización progresiva alineada con el ciclo de vida de los activos existentes. El estudio integra análisis técnico, validación experimental y evaluación económica, proporcionando a EBSA una base estructurada para la toma de decisiones en materia de ciberseguridad industrial.

Palabras Clave: Ciberseguridad industrial; Infraestructura crítica; Segmentación IT/OT; IEC 62443; IEC 62351; Redes eléctricas; Evaluación comparativa; Defensa en profundidad; Seguridad en subestaciones; Arquitecturas de red industrial.

Abstract

The convergence between Information Technology (IT) and Operational Technology (OT) environments in the electric power sector has significantly increased exposure to cybersecurity risks, affecting critical assets, operational continuity, and the protection of strategic information. In this context, the objective of this study was to conduct a technical comparative analysis for the selection of cybersecurity equipment and architectures applicable to the IT and OT environments of the Empresa de Energía de Boyacá (EBSA), based on the guidelines established in IEC 62443 and IEC 62351 standards.

Initially, a functional characterization of the IT and OT environments was carried out, identifying critical assets, information flows, and interconnection points susceptible to cyber threats. Subsequently, technical cybersecurity requirements were defined according to international standards and translated into measurable evaluation criteria through a structured comparative matrix. This matrix allowed the transformation of qualitative criteria into quantitative weighted values, reducing subjectivity in the technology selection process and supporting evidence-based decision-making.

Due to the critical nature of the infrastructure, direct testing on the company's production network was not permitted. Therefore, a controlled simulation environment was implemented using GNS3 to experimentally validate IT/OT segmentation scenarios, including reconnaissance scans, unauthorized access attempts, and controlled malicious traffic generation. The results demonstrated that the application of zone-and-conduit segmentation policies significantly reduces the attack surface and improves event traceability.

Finally, a budget estimation was developed for implementing the proposed architecture in a typical substation, demonstrating the economic feasibility of a progressive modernization strategy aligned with the lifecycle of existing assets. This study integrates technical analysis, experimental validation, and economic evaluation, providing EBSA with a structured framework to support cybersecurity decision-making in industrial environments.

Capítulo 1

Introducción

La transformación digital en el sector eléctrico ha impulsado la evolución de las redes tradicionales hacia sistemas inteligentes conocidos como Smart Grids, los cuales integran capacidades avanzadas de monitoreo, control y automatización en tiempo real. Este proceso ha favorecido la convergencia entre las Tecnologías de la Información (IT) y las Tecnologías de la Operación (OT), permitiendo una mayor eficiencia operativa, optimización de recursos y mejora en la calidad del servicio eléctrico. Sin embargo, dicha integración también ha introducido nuevos desafíos en materia de ciberseguridad, al ampliar la superficie de ataque y exponer infraestructuras críticas a amenazas cada vez más sofisticadas. (National Institute of Standards and Technology, 2015)

Diversos estudios han evidenciado que la interconexión entre sistemas IT y OT en infraestructuras críticas incrementa significativamente la exposición a amenazas cibernéticas, incluyendo accesos no autorizados, ataques de denegación de servicio y manipulación de datos. En este contexto, incidentes reales han demostrado el impacto de estas vulnerabilidades; por ejemplo, el Ukraine power grid cyberattack (Lee et al., 2016) evidenció cómo un ataque coordinado puede comprometer la operación de sistemas eléctricos, generando interrupciones del servicio y afectando la seguridad energética. Este tipo de eventos ha puesto en evidencia la necesidad de fortalecer los mecanismos de protección en entornos industriales.

En este contexto, estándares como IEC 62443 y IEC 62351 han sido ampliamente adoptados como referencia para la implementación de estrategias de ciberseguridad en entornos industriales y sistemas eléctricos. La norma IEC 62443 establece un enfoque basado en la segmentación de redes mediante zonas y conductos, así como en el principio de defensa en profundidad, mientras que la IEC 62351 se enfoca en la protección de las comunicaciones, garantizando la confidencialidad, integridad y autenticidad de la información intercambiada en sistemas de potencia. (International Electrotechnical Commission, 2018) (International Electrotechnical Commission, 2013)

A pesar de la existencia de estos marcos normativos, uno de los principales desafíos para las empresas del sector eléctrico radica en la selección adecuada de tecnologías de ciberseguridad que permitan implementar dichos lineamientos de manera efectiva. La diversidad de soluciones disponibles en el mercado, junto con la complejidad de los entornos IT/OT, dificulta la toma de decisiones, especialmente cuando no se cuenta con metodologías estructuradas que permitan evaluar de forma objetiva las diferentes

alternativas tecnológicas.(Knowles et al., 2015)

En el caso de la Empresa de Energía de Boyacá (EBSA), la adopción de sistemas SCADA, redes de telecontrol y dispositivos inteligentes en subestaciones eléctricas ha fortalecido sus capacidades operativas, pero también ha incrementado la necesidad de implementar mecanismos robustos de ciberseguridad. En este escenario, resulta fundamental contar con herramientas que permitan analizar, comparar y seleccionar tecnologías adecuadas, considerando tanto criterios técnicos como normativos.(Empresa de Energía de Boyacá, 2024)

Frente a esta problemática, el presente trabajo propone un estudio técnico comparativo para la selección de equipos y arquitecturas de ciberseguridad aplicables a entornos IT/OT, basado en los lineamientos de las normas IEC 62443 e IEC 62351. La investigación integra la caracterización de los entornos tecnológicos, la identificación de activos críticos, la definición de criterios de evaluación y la aplicación de una matriz comparativa que permite transformar variables cualitativas en resultados cuantitativos.

Adicionalmente, se incorpora un proceso de validación experimental mediante el uso de GNS3, en el cual se simulan escenarios de ataque y se evalúa el impacto de la implementación de mecanismos de segmentación y control de acceso. Este enfoque permite evidenciar de manera práctica la efectividad de las soluciones propuestas y su aplicabilidad en entornos reales.

Finalmente, este estudio busca contribuir al fortalecimiento de la ciberseguridad en infraestructuras críticas del sector eléctrico, proporcionando una metodología estructurada y replicable que facilite la toma de decisiones en la selección de tecnologías, alineada con estándares internacionales y adaptada a las necesidades específicas del contexto colombiano.

1.1. Planteamiento del problema

La transformación digital en el sector eléctrico ha impulsado la integración progresiva entre los entornos de Tecnologías de la Información (IT) y Tecnologías de la Operación (OT), permitiendo mejorar la supervisión, automatización y eficiencia de los procesos de generación, transmisión y distribución de energía. En este contexto, las empresas operadoras de red, como la Empresa de Energía de Boyacá S.A. E.S.P. (EBSA), han fortalecido sus sistemas de supervisión y control mediante la implementación de plataformas SCADA, redes de telecontrol y dispositivos inteligentes de protección y automatización en subestaciones eléctricas.(Stouffer et al., 2011)

Sin embargo, esta convergencia IT/OT ha incrementado significativamente la superficie de exposición a amenazas cibernéticas. Los sistemas OT, tradicionalmente diseñados bajo criterios de disponibilidad y continuidad operativa, no fueron concebidos originalmente con mecanismos robustos de ciberseguridad. La incorporación de protocolos basados en TCP/IP, la interconexión con redes corporativas y el acceso remoto para mantenimiento han generado nuevos vectores de ataque que pueden comprometer la integridad, confidencialidad y disponibilidad de la información

operativa.(Knowles et al., 2015)

En el caso específico de EBSA, como operador de red del Sistema Interconectado Nacional colombiano, la continuidad del servicio eléctrico constituye un requisito esencial regulado por entidades como la Comisión de Regulación de Energía y Gas (CREG) y supervisado por la Superintendencia de Servicios Públicos Domiciliarios (SSPD). Una interrupción significativa derivada de un incidente cibernético en una subestación podría impactar no solo la calidad del servicio y los indicadores regulatorios, sino también la estabilidad operativa y la confianza institucional.(Comisión de Regulación de Energía y Gas, 2018)(Superintendencia de Servicios Públicos Domiciliarios, 2020)

Las subestaciones de distribución, integradas a centros de control mediante protocolos industriales como IEC 60870-5-104, intercambian información crítica relacionada con estados de interruptores, mediciones eléctricas, alarmas y comandos de operación. Si dichos flujos de información no cuentan con mecanismos adecuados de autenticación, segmentación y cifrado, pueden ser objeto de interceptación, manipulación o denegación de servicio.(International Electrotechnical Commission, 2016)

En este escenario, las normas internacionales IEC 62443 e IEC 62351 proporcionan marcos técnicos específicos para la protección de sistemas industriales y comunicaciones eléctricas. La serie IEC 62443 establece principios de segmentación en zonas y conductos, defensa en profundidad y niveles de seguridad (Security Levels), mientras que IEC 62351 define mecanismos de autenticación, integridad y confidencialidad para protocolos eléctricos basados en TCP/IP. No obstante, la aplicación práctica de estos estándares requiere traducir sus requisitos en criterios concretos de selección de equipos y diseño arquitectónico.(International Electrotechnical Commission, 2018),(International Electrotechnical Commission, 2013)

Actualmente, no se cuenta con un estudio técnico comparativo específico que analice, bajo el contexto operativo de EBSA, qué tipos de equipos y arquitecturas de ciberseguridad IT/OT permiten dar cumplimiento efectivo a los lineamientos establecidos por IEC 62443 e IEC 62351, considerando además criterios de viabilidad operativa y coherencia con la infraestructura existente.(Knowles et al., 2015)

Por lo tanto, surge la necesidad de desarrollar un estudio técnico comparativo que permita identificar y evaluar tecnologías de ciberseguridad aplicables a entornos IT y OT en EBSA, con el fin de proponer una arquitectura de referencia alineada con estándares internacionales y adaptada a la realidad operativa de una subestación de distribución típica.

1.2. Contexto del entorno IT/OT en la Empresa de Energía de Boyacá (EBSA)

En el sector eléctrico, las infraestructuras tecnológicas combinan entornos de Tecnologías de la Información (IT) y Tecnologías de Operación (OT), los cuales

permiten la supervisión, control y gestión de los sistemas de generación, transmisión y distribución de energía. En el caso de la Empresa de Energía de Boyacá (EBSA), estas infraestructuras incluyen centros de control, sistemas SCADA, subestaciones eléctricas, equipos de protección, redes de comunicación industrial y plataformas de gestión administrativa. La integración de estos sistemas permite monitorear variables críticas del sistema eléctrico en tiempo real y garantizar la continuidad del servicio energético en la región.(Gungor et al., 2011)

No obstante, la convergencia entre los entornos IT y OT ha incrementado la superficie de ataque de las organizaciones del sector energético. Tradicionalmente, los sistemas OT se diseñaban para operar en redes cerradas y con un nivel limitado de conectividad externa; sin embargo, la digitalización de las infraestructuras eléctricas ha promovido la interconexión con redes corporativas y sistemas de gestión remotos, lo que introduce nuevos riesgos de ciberseguridad. Entre los principales desafíos se encuentran el acceso no autorizado a sistemas de control, la manipulación de información operativa, la interrupción de los procesos industriales y la explotación de vulnerabilidades en dispositivos conectados a la red.(Knowles et al., 2015)

En este contexto, resulta fundamental evaluar arquitecturas de seguridad que permitan fortalecer la protección de los sistemas IT/OT presentes en infraestructuras críticas como las subestaciones eléctricas. La implementación de mecanismos de autenticación robustos, segmentación de red y monitoreo continuo de comunicaciones constituye un elemento clave para reducir la probabilidad de ataques cibernéticos y garantizar la disponibilidad, integridad y confidencialidad de la información que circula en los sistemas de control industrial.(International Electrotechnical Commission, 2018)(National Institute of Standards and Technology, 2015)

1.3. Formulación de Pregunta

¿Cuáles son los equipos y arquitecturas de ciberseguridad IT/OT más adecuados para una subestación de distribución típica en EBSA, que permitan dar cumplimiento a los requisitos establecidos en las normas IEC 62443 e IEC 62351, garantizando segmentación, protección de comunicaciones y continuidad operativa?

1.4. Justificación

La creciente convergencia entre los entornos de tecnologías de la información (IT) y tecnologías de la operación (OT) en el sector eléctrico ha generado nuevos desafíos en materia de ciberseguridad, especialmente en infraestructuras críticas como las subestaciones eléctricas. Este proceso de integración, si bien permite mejorar la eficiencia operativa, la supervisión en tiempo real y la automatización de los sistemas, también incrementa la superficie de ataque y la exposición a amenazas cibernéticas que pueden comprometer la continuidad del servicio eléctrico y la integridad de los activos críticos.(Cherdantseva et al., 2016)

En el caso particular de la Empresa de Energía de Boyacá (EBSA), la modernización tecnológica y la adopción de sistemas SCADA, redes de telecontrol y dispositivos

inteligentes hacen necesario contar con criterios técnicos claros para la selección de equipos y arquitecturas de ciberseguridad que respondan a las exigencias actuales del entorno IT/OT. Sin embargo, la toma de decisiones en este ámbito suele verse afectada por la diversidad de soluciones disponibles en el mercado y la falta de metodologías estructuradas que permitan evaluarlas de manera objetiva.(Wang et al., 2013)

En este contexto, el presente estudio se justifica en la necesidad de proporcionar un enfoque técnico comparativo que facilite la selección de tecnologías de ciberseguridad, basado en estándares internacionales como las normas IEC 62443 e IEC 62351. Estas normas establecen lineamientos fundamentales para la protección de sistemas industriales y de comunicaciones en el sector eléctrico, permitiendo definir criterios de evaluación alineados con buenas prácticas reconocidas a nivel global.

Desde el punto de vista técnico, este trabajo aporta una metodología estructurada que integra la caracterización de entornos IT/OT, la identificación de activos críticos, la definición de requisitos de seguridad y la evaluación comparativa de tecnologías mediante una matriz de criterios. Adicionalmente, la validación experimental en un entorno de simulación (GNS3) permite evidenciar de manera práctica el impacto de la segmentación de redes y la implementación de mecanismos de seguridad en la reducción de riesgos cibernéticos.(Hahn & Govindarasu, 2013)

Desde el punto de vista práctico, los resultados del estudio proporcionan a EBSA una base sólida para la toma de decisiones en la implementación de soluciones de ciberseguridad, contribuyendo a mejorar la protección de sus infraestructuras y a garantizar la continuidad operativa del servicio eléctrico. Asimismo, la estimación presupuestaria incluida permite evaluar la viabilidad económica de la adopción de dichas soluciones en escenarios reales.

Finalmente, desde el ámbito académico, este trabajo contribuye al desarrollo de conocimiento aplicado en el área de la ciberseguridad industrial, particularmente en el contexto de la convergencia IT/OT en sistemas eléctricos, sirviendo como referencia para futuros estudios y proyectos en el sector energético.

Capítulo 2

Objetivos

2.1. Objetivo General

Realizar un estudio técnico comparativo para la selección de equipos y definición de una arquitectura de ciberseguridad IT/OT aplicable a una subestación de distribución tipo en EBSA, alineada con los requisitos establecidos en las normas IEC 62443 e IEC 62351.

2.2. Objetivos Específicos

- Caracterizar los entornos IT y OT de EBSA desde una perspectiva funcional y de seguridad, identificando los activos y flujos de información críticos que requieren protección.
- Definir los requisitos técnicos de ciberseguridad, a partir de los lineamientos establecidos en las normas IEC 62443 e IEC 62351, para su aplicación en arquitecturas IT y OT del sector eléctrico.
- Evaluar comparativamente diferentes alternativas de equipos y arquitecturas de ciberseguridad mediante una matriz de criterios técnicos, operativos y de viabilidad, apoyado en GNS3, con el fin de proponer una arquitectura de referencia aplicable a EBSA.

Capítulo 3

Marco teórico

3.1. Tecnologías de la información (IT) y Tecnologías de la Operación (OT) en empresas del sector energético

La convergencia entre las tecnologías de la información IT y las tecnologías de la operación OT constituye uno de los principales ejes de transformación en las empresas del sector energético, particularmente en aquellas dedicadas a la generación, transmisión y distribución de energía eléctrica. Tradicionalmente, ambos entornos son concebidos y gestionados de forma independiente, respondiendo a objetivos, arquitecturas y prioridades distintas dentro de cada organización. Sin embargo, la evolución tecnológica y la aparición de conceptos como "Smart Grids" han impulsado una integración progresiva entre ambos dominios, generando nuevos retos en términos de gestión, operación y regularidad. (Gungor et al., 2011)(Yan et al., 2012)

3.1.1. Tecnologías de la Operación (OT)

La tecnología Operacional, conocida como OT o Operational Technology, se define como el conjunto de equipos, dispositivos, sensores, actuadores y software utilizados para supervisar y controlar procesos físicos en tiempo real, con el propósito de mantener la integridad y continuidad de los sistemas operativos. En el sector energético, OT abarca sistemas críticos como SCADA, sistemas de control, sistemas de transmisión eléctrica y formas de gestión de energía, los cuales interactúan directamente con activos físicos y procesos de misión crítica. (International Society of Automation, 2018)

Una de las principales características de los sistemas OT es su orientación hacia la disponibilidad, confiabilidad y seguridad operacional, dado que cualquier interrupción puede generar impactos significativos en la operación del sistema eléctrico. Estos sistemas suelen operar bajo condiciones de tiempo real, con arquitecturas basadas en software embebido y con interfaces específicas para operadores e ingenieros, lo que históricamente ha llevado al uso de tecnologías propietarias y a una menor consideración de aspectos de ciberseguridad desde su diseño inicial. (Instituto Nacional de Ciberseguridad, 2019)

3.1.2. Tecnologías de la Información (IT)

Por su parte, las tecnologías de la información IT se refieren al conjunto de recursos, procedimientos y técnicas orientadas al procesamiento, almacenamiento y transmisión de información dentro de la organización. Los sistemas IT están asociados principalmente a la gestión de información corporativa y de procesos de negocio, utilizando arquitecturas lógicas multicapa, bases de datos transaccionales y redes de comunicación LAN y WAN basadas en protocolos estándar. Ejemplos de estos sistemas incluyen plataformas ERP, sistemas de gestión de contenidos, correo electrónico y aplicaciones corporativas. (Laudon & Laudon, 2020)

A diferencia de OT, los entornos IT priorizan aspectos como la confidencialidad, integridad y disponibilidad de la información, así como la escalabilidad y la interoperatividad entre aplicaciones. La gestión de IT suele estar bajo la responsabilidad de áreas especializadas en información y sistemas de información, con procesos consolidados de planeación tecnológica, administración de redes y desarrollo de software. (European Union Agency for Cybersecurity, 2016)

3.1.3. Diferencias fundamentales entre IT y OT

La separación histórica entre IT y OT en empresas del sector energético ha estado motivada por la especialización natural de cada entorno, tanto a nivel organizacional como tecnológico. Mientras que IT se orienta a la automatización de procesos de negocio y a la gestión de información, OT se enfoca en el manejo de activos físicos y el control de procesos industriales. Estas diferencias se reflejan en aspectos como la arquitectura de los sistemas, los tiempos de respuesta, los tiempos de interfaces, los responsables de su gestión y los niveles de tolerancia de riesgo. (Instituto Nacional de Ciberseguridad, 2019)

	IT	OT
Propósito	Gestión de información, Automatización de procesos de negocio	Manejo de activos, Procesos de Control
Arquitectura	Transaccional o Batch, bases de datos relacionales o texto	Tiempo Real, Software embebido
Interfaces	Navegador web, Terminales y teclado	Sensores, Displays codificados
Propietario	CIO, Ingenieros de Informática, Finanzas, Adquisiciones	Ingenieros técnicos, Gerentes de línea de negocios
Conectividad	Red Corporativa, basada IP	Redes de control (en incremento redes IP y wireless)
Ejemplos	ERP, SCM, CRM, E-mail	SCADA, PLCs, Sistemas de Control, Modelamiento

Figura 3.1.1: Cuadro comparativo IT-OT
Fuente: (Instituto Nacional de Ciberseguridad, 2019)

En el caso de OT, la adopción de tecnologías estándar y la integración con redes IP han sido más lentas debido a los altos requerimientos de confiabilidad y a la criticidad de los procesos controlados. No obstante, el incremento en la capacidad de procesamiento, la velocidad de las redes y la introducción de nuevas tecnologías de comunicación han permitido que progresivamente los sistemas OT incorporen arquitecturas y prácticas tradicionalmente asociadas a IT, lo anterior resumido en el cuadro comparativo de la figura 3.1.1. (Centro Criptológico Nacional, 2020)

3.1.4. Convergencia IT-OT en empresas de energía

La convergencia IT-OT se entiende como el proceso mediante el cual se integran tecnologías, prácticas y modelos de gestión de ambos dominios con el fin de mejorar la eficiencia operativa, la interoperatividad de los sistemas y la capacidad de respuesta de la organización. En el sector eléctrico, esta convergencia ha sido un habilitador fundamental para el desarrollo de redes inteligentes, la supervisión avanzada de la operación y el análisis de grandes volúmenes de datos operativos. (Unidad de Planeación Minero Energética, 2020) (Ministerio de Tecnologías de la Información y las Comunicaciones, 2019)

Sin embargo, los autores señalan que la convergencia IT-OT no es únicamente un desafío tecnológico, sino también organizacional y estratégico. La integración requiere marcos de referencia que consideren procesos, roles, gobierno de tecnología y niveles de madurez, con el fin de garantizar una adopción ordenada y controlada que minimice riesgos operativos y de seguridad. (Banco Interamericano de Desarrollo, 2020) (Comisión Económica para América Latina y el Caribe, 2021)

3.1.5. Activos y flujos de información que requieren protección

En un entorno convergente IT-OT, los activos tecnológicos y los flujos de información adquieren un rol central en la operación del sistema eléctrico. Los activos OT incluyen dispositivos de campo, sistemas de control y plataformas de supervisión que interactúan directamente con los procesos físicos, mientras que los activos IT abarcan servidores de información críticos que deben ser protegidos para garantizar la integridad del sistema y la continuidad del servicio. (Cherdantseva et al., 2016)

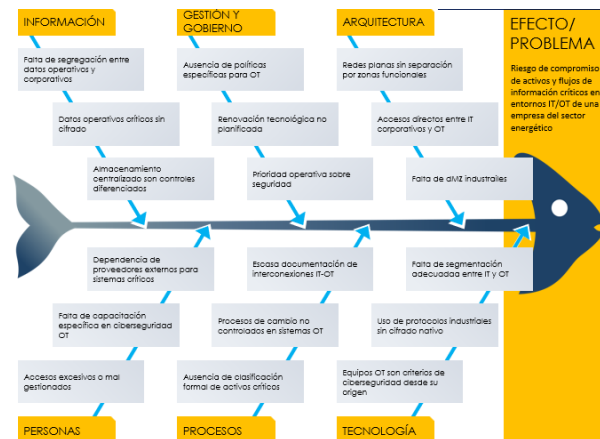


Figura 3.1.2: Diagrama causa efecto riesgos de compromiso
Fuente: (Elaboración propia, 2026)

Con el fin de identificar los principales factores que influyen en la necesidad de proteger los activos y flujos de información en entornos IT y OT con mayor criticidad denotados en la figura 3.1.2 , se empleó un análisis causa-efecto mediante un diagrama de espina de pescado. este análisis permitió agrupar las causas en categorías relacionadas con tecnología, procesos, personas, arquitectura, gestión y gobierno, e información.

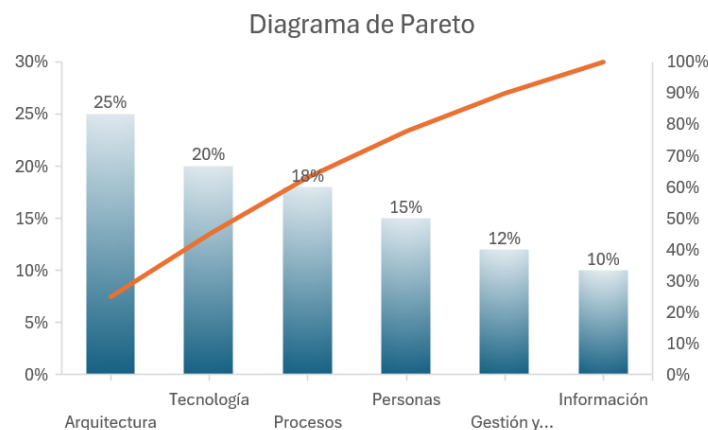


Figura 3.1.3: Diagrama de Pareto riesgos de compromiso
Fuente: (Elaboración propia, 2026)

De manera complementaria, para priorizar las causas identificadas en el análisis de activos y flujos de información, se elaboró un diagrama de Pareto determinado en la figura 3.1.3 a partir de los resultados de los diagramas de causa y efecto. El análisis evidencia que las categorías relacionadas con la arquitectura, la tecnología, los procesos y las personas concentran aproximadamente el 78 % del impacto total sobre el riesgo de compromiso de los activos y flujos de información en entornos IT y OT.

Este resultado indica que la mayoría de los riesgos se originan en un conjunto reducido de factores críticos, lo que permite enfocar los esfuerzos de ciberseguridad en el diseño de arquitecturas adecuadas, la selección de tecnologías compatibles con entornos industriales, la definición de procesos de gestión claros y la capacitación del personal de

acuerdo con los principios establecidos por la norma IEC 62443.(International Electrotechnical Commission, 2018)

Nota: Las versiones de alta resolución de los diagramas de Pareto y espina de pescado se encuentran disponibles en el ***Anexo 1***.

3.2. Ciberseguridad en infraestructuras críticas

3.2.1. Infraestructuras críticas y su relación con la ciberseguridad

Las infraestructuras críticas se definen como aquellos sistemas, instalaciones y activos cuya interrupción o afectación tendría un impacto significativo sobre la seguridad, la economía y el bienestar de la sociedad. Dentro de este grupo se incluyen los sistemas de generación, transmisión y distribución de energía eléctrica, los cuales dependen cada vez más de plataformas digitales para su operación y supervisión . en este contexto, la ciberseguridad se convierte en un componente esencial para garantizar la continuidad del servicio y la protección de los activos físicos y de información.(Alonso et al., 2021)

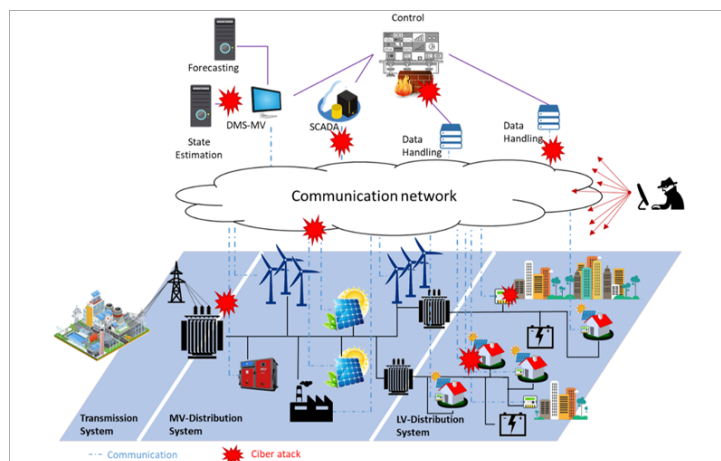


Figura 3.2.1: Riesgos en compromiso en la infraestructura.

Fuente: (Alonso et al., 2021)

En las empresas del sector energético, la digitalización y la convergencia IT-OT han permitido mejorar la eficiencia operativa y la capacidad de monitoreo; sin embargo, también han introducido nuevas superficies de ataque como las que se observan en la figura 3.2.1 denotadas de color rojo. La interconexión de sistemas corporativos con sistemas de control industrial implica que los incidentes originados en el entorno IT pueden propagarse hacia entornos OT, generando consecuencias que trascienden la pérdida de información y pueden afectar directamente procesos físicos críticos.(Alonso et al., 2021)

3.2.2. Particularidades de la ciberseguridad en entornos OT

A diferencia de los entornos IT tradicionales, la ciberseguridad en OT presenta características específicas que condicionan el diseño e implementación de controles de seguridad. En primer lugar, los sistemas OT priorizan la disponibilidad y la

confiabilidad operacional por encima de la confidencialidad, dado que una interrupción en la operación puede generar fallas masivas en el suministro eléctrico. En segundo lugar, muchos de estos sistemas fueron diseñados sin considerar las amenazas cibernéticas modernas, utilizando protocolos propietarios o sin mecanismos de autenticación y cifrado robustos.(Humayed et al., 2017)

Adicionalmente, los ciclos de vida de los equipos OT suelen ser considerablemente más largos que los de IT, lo que limita la posibilidad de actualizaciones frecuentes y la adopción inmediata de nuevas tecnologías de seguridad. Estas restricciones hacen necesario adoptar enfoques de ciberseguridad específicos para infraestructuras críticas, basados en arquitectura, segmentación y gestión del riesgo, en lugar de soluciones genéricas orientadas exclusivamente a IT.(Krause et al., 2015)

3.2.3. Amenazas cibernéticas en infraestructuras energéticas

Las infraestructuras energéticas son objetivos atractivos para los diferentes tipos de amenazas cibernéticas, debido a su relevancia estratégica y al impacto potencial de un ataque exitoso. Entre las amenazas más relevantes se encuentran el acceso no autorizado a sistemas de control, la manipulación de datos operativos, los ataques de denegación de servicio y el uso de malware especializado para entornos industriales. Casos documentados a nivel internacional han demostrado que los ataques dirigidos a sistemas eléctricos pueden provocar interrupciones del servicio y afectar la estabilidad del sistema energético. Algunas de las taxonomías que utilizan para alterar el sistemas se presentan con ayuda del siguiente cuadro, comparando el proveedor contra el cliente.(Instituto Nacional de Ciberseguridad, 2019)

Proveedor		Cliente	
Técnicas de ataque utilizadas para comprometer la cadena de suministro	Activos de los proveedores objeto del ataque a la cadena de suministro	Técnicas de ataque utilizadas para comprometer al cliente	Activos de los clientes objeto del ataque a la cadena de suministro
Infección por malware	Software preexistente	Relación de confianza	Datos
Ingeniería social	Bibliotecas informáticas	[T1199]	Datos personales
Ataque de fuerza bruta	Código	Compromiso Drive-by [T1189]	Propiedad intelectual
Aprovechamiento de la vulnerabilidad del software	Configuraciones	Phishing [T1566]	Software
Aprovechamiento de la vulnerabilidad de la configuración	Datos	Infección por malware	Procesos
Inteligencia de fuentes abiertas (OSINT)	Procesos	Ataque físico o modificación	Ancho de banda
	Hardware	Falsificación	Finanzas
	Personas		Personas
	Proveedor		

Figura 3.2.2: Taxonomía de los ataques a la cadena de suministros

Fuente: (Instituto Nacional de Ciberseguridad, 2019)

La evolución de las amenazas ha dado lugar a técnicas que combinan tácticas propias del entorno IT con conocimiento específico de procesos industriales, lo que refuerza la necesidad de modelos de defensa en profundidad y de una clara separación entre dominios IT y OT. En este sentido, la identificación de activos críticos, flujos de información y posibles vectores de ataque constituye un paso fundamental en el análisis de seguridad de la cadena de suministro, tal como se ilustra en la figura 3.2.2.,

constituye un paso fundamental para el diseño de estrategias de ciberseguridad en infraestructuras críticas.(Organización de los Estados Americanos, 2019)

3.2.4. Enfoques de Protección para infraestructuras críticas

Para hacer frente a las amenazas descritas, diversos organismos y estándares internacionales proponen enfoques de protección basados en la gestión del riesgo, la segmentación de redes y la defensa en profundidad. Estos enfoques buscan limitar la propagación de incidentes, reducir la superficie de ataque y garantizar la continuidad operativa incluso ante eventos de seguridad.(European Union Agency for Cybersecurity, 2016)

En el sector energético, dichos enfoques se materializan en arquitecturas que separan funcionalmente los entornos IT y OT, definen zonas de seguridad con diferentes niveles de criticidad y controlan los flujos de información entre ellas. la ciberseguridad en infraestructuras críticas no se concibe unicamente como la implementación de dispositivos tecnológicos, sino como un conjunto de políticas, procesos y controles técnicos alineados con la operación del sistema y con estándares internacionales.(Red Eléctrica de España, 2018)

3.3. Modelo de ciberseguridad basado en la norma IEC 62443

3.3.1. La norma IEC 62443 y su enfoque en infraestructuras industriales

La serie de normas IEC 62443 constituye el principal marco internacional para la ciberseguridad de sistemas de automatización y control industrial(IACS). Su enfoque está orientado a la protección en entornos OT, considerando las particularidades operativas de los procesos industriales y de infraestructuras críticas como el sector energético. A diferencia de otros estándares de seguridad de la información, IEC 62443 no se limita a la gestión organizacional, sino que define requisitos técnicos, arquitectónicos y operativos aplicables a sistemas, redes y dispositivos industriales.(International Electrotechnical Commission, 2018)

En el contexto de empresas de energía, IEC 62443 resulta especialmente relevante debido a que permite estructurar la ciberseguridad desde una perspectiva de arquitectura, priorizando la disponibilidad, la confiabilidad y la seguridad operacional. La norma propone un enfoque de defensa en profundidad, mediante la aplicación de múltiples capas de protección, con el objeto de reducir la probabilidad de una amenaza comprometa activos críticos del sistema.(International Electrotechnical Commission, 2018)

3.3.2. Concepto de zonas y conductos (Zones & Conduits)

Uno de los pilares fundamentales de la norma IEC 62443 es el modelo de zonas y conductos, el cual permite segmentar la infraestructura en función de la criticidad de los

activos y controlar los flujos de información entre diferentes dominios de seguridad.(International Electrotechnical Commission, 2018)

Una zona se define como un conjunto lógico o físico de activos que comparten requisitos de seguridad similares, mientras que un conducto corresponde al medio controlado a través del cual se permite la comunicación entre zonas. Este modelo facilita la aplicación de controles específicos para cada segmento de la red, limitando la propagación de incidentes de seguridad y reduciendo la superficie de ataque.(International Electrotechnical Commission, 2018)

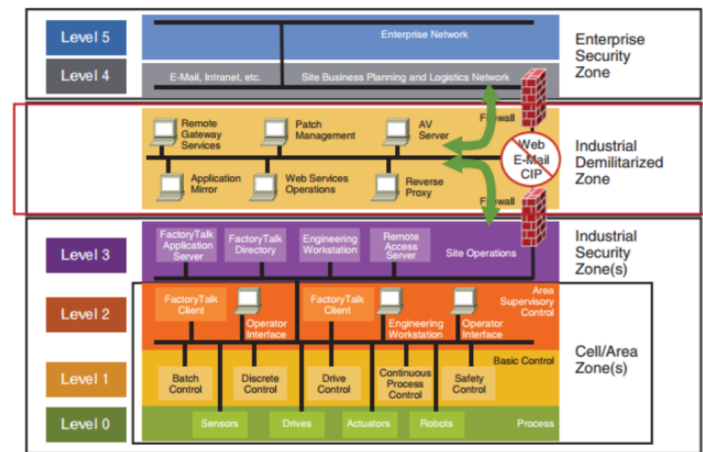


Figura 3.3.1: Modelo Purdue de un sistema industrial dividido en zonas

Fuente: (Northwind Technical Services, 2026)

El modelo Purdue ilustrado en la figura 3.3.1 una de la primeras arquitecturas que se implementaron o se tomaron como referencia para los sistemas de control industrial, el cual provee una perspectiva para entender cómo construir un sistema de control industrial enfocado en la seguridad de zonas. En entornos IT-OT del sector energético, las zonas pueden representar, por ejemplo, el entorno corporativo IT, la zona de operaciones OT, una zona de control de subestaciones o una zona de acceso remoto, mientras que los conductos corresponden a los enlaces de comunicación entre zonas.(Northwind Technical Services, 2026)

3.3.3. Defensa en profundidad según IEC 62443

La defensa en profundidad es un principio central de la norma IEC 62443 y se basa en la implementación de múltiples capas de seguridad distribuidas a lo largo de la arquitectura del sistema, con una jerarquía como se ilustra en la figura 3.3.2. Este enfoque reconoce que ningún control de seguridad es infalible por sí solo, por lo que la combinación de medidas técnicas, organizacionales y operativas incrementa la resiliencia del sistema frente a ataques cibernéticos.(International Electrotechnical Commission, 2018)

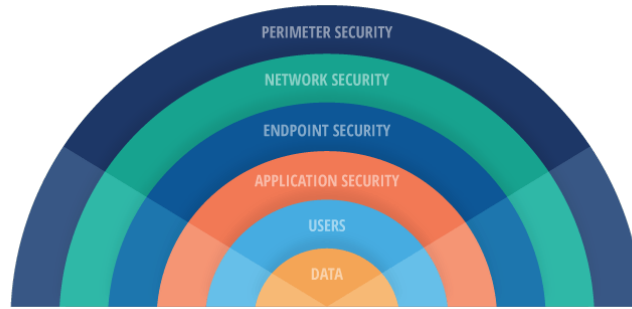


Figura 3.3.2: Defensa en profundidad
Fuente: (Rodriguez, 2022)

La infraestructura crítica del sector energético, la defensa en profundidad se traduce en la aplicación de controles en diferentes niveles, tales como dispositivos de segmentación de red, mecanismos de autenticación, cifrado de comunicaciones, monitores continuo y procedimientos de gestión de incidentes. Este enfoque permite mitigar tanto amenazas externas como internas, y es especialmente adecuado para entornos OT donde las interrupciones operativas deben evitarse.(Rodriguez, 2022)

3.3.4. Niveles de Seguridad (Security Levels - SL)

IEC 62443 introduce el concepto de niveles de seguridad (SL), los cuales permiten clasificar el grado de protección requerido para una zona o sistemas en función de las amenazas esperadas. La norma define diferentes niveles de seguridad que van desde la protección contra amenazas no intencionales hasta la defensa frente a atacantes altamente sofisticados, como se identifican en la figura 3.3.3.(International Electrotechnical Commission, 2018)

Este enfoque es particularmente útil en entornos energéticos, ya que no todos los activos requieren el mismo nivel de protección. La asignación de niveles de seguridad permite priorizar recursos y aplicar controles adecuados a la criticidad de cada zona, evitando soluciones sobre dimensionadas o insuficientes.

Nivel de seguridad (SL)	Objetivo	Habilidades	Motivación	Medios	Recursos
SL1	Violaciones casuales o accidentales	Sin habilidades para atacar	Ninguna, por error	No intencionales	Un individuo
SL2	Delincuentes informáticos, hackers	Genéricas	Baja	Simple	Bajos (individuo aislado)
SL3	Hackers activistas, terroristas	Específicas de ICS	Moderada	Sofisticados (ataque)	Moderados (grupo de hackers)
SL4	Estado nacional	Específicas de ICS	Alta	Sofisticados (campana)	Extensos (equipos multidisciplinarios)

Figura 3.3.3: Niveles de seguridad IEC 62443
Fuente: (Schneider Electric, 2026)

3.3.5. Relación entre IEC 62443 y la selección de equipos

Uno de los aportes más relevantes de IEC 62443 para el presente trabajo es que la norma no prescribe tecnologías específicas, sino que establece requisitos de seguridad que deben cumplirse a nivel del sistema, zona o componente. Esto implica que la selección de equipos de ciberseguridad debe realizarse a partir de un análisis técnico comparativo, evaluando qué soluciones permiten cumplir con los requisitos definidos para cada zona y conducto.

En este sentido, IEC 62443 sirve como marco de referencia para la definición de criterios de evaluación de equipos, tales como capacidades de segmentación, control de flujos, autenticación, cifrado y monitoreo, lo cual se alinea directamente con la matriz de criterios planteada en el desarrollo de este proyecto.

3.4. Seguridad de las comunicaciones en sistemas eléctricos

3.4.1. La norma IEC 62351 en el contexto del sector eléctrico

La norma IEC 62351 forma parte del conjunto de estándares internacionales desarrollados para fortalecer la seguridad de los sistemas de gestión, supervisión y control del sector eléctrico. A diferencia de la serie IEC 62443, que se enfoca en la arquitectura y en los requisitos de seguridad de sistemas industriales, IEC 62351 está orientada específicamente a la protección de las comunicaciones y del intercambio de información entre los diferentes componentes de los sistemas eléctricos. (International Electrotechnical Commission, 2013)

La empresa del sector energético, las comunicaciones constituyen un elemento crítico para la operación segura y eficiente del sistema, ya que permiten el intercambio de información entre centros de control, subestaciones, sistemas de telecontrol y plataformas corporativas. La norma IEC 62351 surge como respuesta a la necesidad de proteger estos flujos de información frente a amenazas como interpretación, manipulación de datos, suplantación de identidad y accesos no autorizados, sin afectar la disponibilidad y el desempeño del sistema eléctrico. (Alonso et al., 2021)

3.4.2. Alcance de la norma IEC 62351

La serie IEC 62351 abarca múltiples partes, cada una orientada a la protección de distintos aspectos de las comunicaciones en sistemas eléctricos. Entre sus principales alcances se encuentran la autenticación de dispositivos y usuarios, la integridad de los mensajes, la confidencialidad de la información transmitida y la gestión segura de claves y certificados digitales. (International Electrotechnical Commission, 2013)

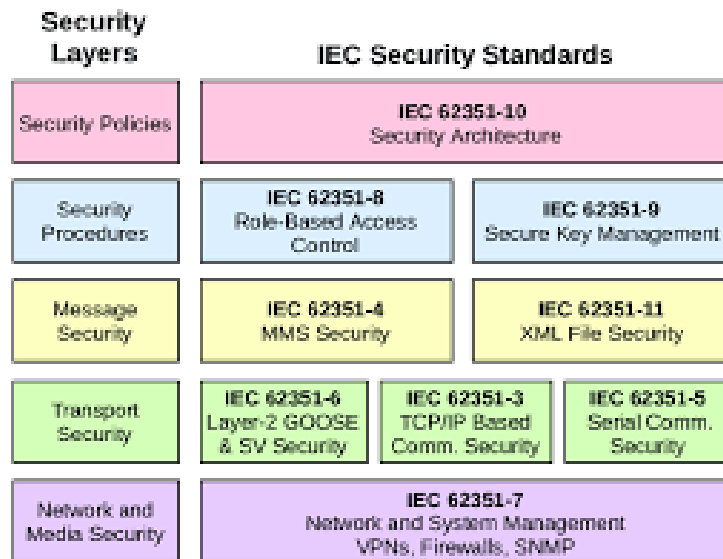


Figura 3.4.1: Componentes de seguridad contemplados por IEC 62351.

Fuente: (ResearchGate, 2026b)

En Particular, IEC 62351 define mecanismos de seguridad aplicables a protocolos ampliamente utilizados en el sector eléctrico, estableciendo perfiles y recomendaciones que permiten adaptar tecnologías de seguridad estándar a las restricciones propias de los entornos OT. De esta manera, la norma busca equilibrar la necesidad de protección con los requerimientos de tiempo real y confiabilidad característicos de las infraestructuras energéticas.

3.4.3. Protección de las comunicaciones basada en TCP-IP (IEC 62351-3)

Uno de los componentes más relevantes de la norma es IEC 62351-3, la cual define el uso de Transport Layer Security (TLS) para proteger las comunicaciones basadas en TCP-IP en sistemas eléctricos. Este enfoque permite garantizar la confidencialidad, integridad y autenticación de las comunicaciones entre dispositivos y sistemas, mitigando riesgos asociados a ataques de tipo man-in-the-middle, espionaje de tráfico y modificación de mensajes.(International Electrotechnical Commission, 2013)

La aplicación de TLS en entornos del sector eléctrico debe considerar las particularidades operativas de los sistemas OT, tales como la latencia permitida, la capacidad de procesamiento de los dispositivos y las disponibilidad continua del servicio. Por esta razón, IEC 62351-3 no se limita a recomendar el uso cifrado, sino que establece perfiles y lineamientos específicos para su implementación en infraestructuras eléctricas.(International Electrotechnical Commission, 2013)

3.4.4. Autenticación, integridad y confidencialidad de la información

La norma IEC 62351 establece que la protección de las comunicaciones no debe limitarse únicamente al cifrado, sino que debe complementar mecanismos de

autenticación robusta y verificación de integridad de los mensajes. La autenticación permite asegurar que los dispositivos y sistemas que intercambian información son legítimos, mientras que la verificación de integridad garantiza que los datos no han sido alterados durante su transmisión.

En el contexto de infraestructuras críticas, estos mecanismos son fundamentalmente para evitar la ejecución de comandos no autorizados, la manipulación de datos operativos y la generación de decisiones incorrectas basadas en información comprometida. La correcta implementación de estos controles contribuye directamente a la confiabilidad del sistema eléctrico y a la prevención de incidentes con impacto operativo.

3.4.5. Gestión de claves y certificados digitales

Un aspecto crítico por IEC 62351 es la gestión segura de claves criptográficas y certificados digitales, los cuales son esenciales para la implementación de mecanismos de autenticación y cifrado. En entornos del sector eléctrico, la gestión de certificados debe realizarse de manera controlada, Considerando la gran cantidad de dispositivos, su distribución geográfica y sus limitaciones técnicas.

La norma enfatiza la necesidad de establecer procesos adecuados para la generación, distribución, almacenamiento y renovación de certificados, de modo que se mantenga un nivel de seguridad adecuado a lo largo del ciclo de vida de los sistemas. Una gestión deficiente de claves puede comprometer la efectividad de los mecanismos de seguridad, incluso cuando se utilizan algoritmos criptográficos robustos.

3.4.6. Relación entre IEC 62351 y los flujos de información IT-OT

La norma IEC 62351 cobra especial relevancia en escenarios de convergencia IT-OT, donde los flujos de información atraviesan diferentes dominios de seguridad. En estos casos, la protección de las comunicaciones permite reducir el riesgo de que una vulnerabilidad en entorno IT afecte directamente a los sistemas OT, asegurando que los datos transmitidos entre zonas mantengan su confidencialidad e integridad.

Desde el punto de vista del presente estudio, IEC 62351 proporciona los lineamientos necesarios para definir los requisitos técnicos asociados al cifrado de datos, autenticación de dispositivos y protección de enlaces de comunicación, los cuales se integran con el enfoque arquitectónico propuesto por IEC 62443. De esta manera, ambas normas se complementan para ofrecer una visión integral de la ciberseguridad en infraestructuras del sector energético.

3.4.7. Implicaciones de IEC 62351 para la selección de equipos

Al igual que IEC 62443, la norma IEC 62351 no impone marcas o tecnologías específicas, sino que define requisitos funcionales que deben ser considerados al momento de seleccionar equipos y soluciones de ciberseguridad. En este sentido, los dispositivos de red, gateways y sistemas de comunicación deben ser evaluados en función de su

capacidad para soportar mecanismos de cifrado, autenticación y gestión segura de certificados, conforme a los lineamientos de la norma.

Este enfoque refuerza la necesidad de realizar un estudio técnico comparativo, en el cual se analicen las capacidades de diferentes alternativas tecnológicas para cumplir con los requisitos de seguridad de las comunicaciones, sin comprometer la operación ni la continuidad del sistema eléctrico.

3.5. Marco regulatorio colombiano aplicable a EBSA



Figura 3.5.1: Logo EBSA

Fuente: (Empresa de Energía de Boyacá, 2024)

El presente estudio técnico no solo se fundamenta en estándares internacionales como IEC 62443 e IEC 62351, sino que también debe enmarcarse dentro del contexto regulatorio colombiano aplicable a empresas operadoras de red como la Empresa de Energía de Boyacá S.A. E.S.P. (EBSA). En Colombia, el sector eléctrico se encuentra regulado y supervisado por diversas entidades que establecen lineamientos técnicos, operativos y de calidad del servicio, los cuales inciden indirectamente en la gestión de la ciberseguridad IT/OT.

3.5.1. Comisión de Regulación de Energía y Gas (CREG)

La Comisión de Regulación de Energía y Gas (CREG) es el organismo encargado de regular la prestación del servicio público de energía eléctrica en Colombia, conforme a lo establecido en la Ley 142 de 1994 y la Ley 143 de 1994.

Entre sus funciones principales se encuentran:

- Definir el marco regulatorio técnico y tarifario.
- Establecer indicadores de calidad del servicio (SAIDI, SAIFI).
- Regular obligaciones de los operadores de red.
- Establecer lineamientos de continuidad y confiabilidad del servicio.

En este contexto, aunque la CREG no emite regulación específica en ciberseguridad industrial, sí exige el cumplimiento de estándares de calidad y continuidad operativa. Un incidente cibernético que afecte la disponibilidad de una subestación o interrumpa el suministro eléctrico podría impactar directamente los indicadores regulatorios y generar consecuencias económicas para la empresa.(Comisión de Regulación de Energía y Gas, 2018)

Por lo tanto, la implementación de arquitecturas de ciberseguridad alineadas con IEC 62443 e IEC 62351 contribuye indirectamente al cumplimiento de las obligaciones regulatorias establecidas por la CREG.

3.5.2. Superintendencia de Servicios Públicos Domiciliarios (SSPD)

La Superintendencia de Servicios Públicos Domiciliarios (SSPD) es la entidad encargada de vigilar, inspeccionar y controlar la gestión de las empresas prestadoras de servicios públicos, incluyendo operadores de red como EBSA.

La SSPD puede:

- Imponer sanciones administrativas.
- Exigir planes de mejora.
- Aplicar multas económicas.
- Intervenir empresas en casos graves.

Si un incidente derivado de una vulnerabilidad en entornos IT/OT afectara la continuidad del servicio eléctrico, la empresa podría ser objeto de investigaciones administrativas. En este sentido, la ciberseguridad deja de ser únicamente un asunto técnico para convertirse en un factor de cumplimiento regulatorio y gestión del riesgo corporativo.(Superintendencia de Servicios Públicos Domiciliarios, 2026)

3.5.3. Reglamento Técnico de Instalaciones Eléctricas (RETIE)

El Reglamento Técnico de Instalaciones Eléctricas (RETIE), adoptado mediante resoluciones del Ministerio de Minas y Energía, establece requisitos obligatorios en materia de seguridad eléctrica. Aunque el RETIE se enfoca principalmente en seguridad física y eléctrica, su objetivo es proteger la vida humana, la integridad de los bienes y la continuidad del servicio. Una afectación en sistemas de protección o control producto de un incidente cibernético podría comprometer la operación segura de instalaciones eléctricas.(Ministerio de Minas y Energía, 2013)

Por tanto, la protección de sistemas de control industrial mediante arquitecturas de ciberseguridad adecuadas se alinea con el espíritu del RETIE en cuanto a seguridad y confiabilidad de las instalaciones.

3.5.4. Política de Protección de Infraestructura Crítica

Colombia ha desarrollado lineamientos relacionados con la protección de infraestructura crítica, particularmente a través del Ministerio de Defensa y el CONPES 3854 de 2016 (Política Nacional de Seguridad Digital).

El CONPES 3854 establece la necesidad de fortalecer la gestión del riesgo digital en sectores estratégicos, incluyendo el sector energético. En este marco, las empresas operadoras de red deben implementar medidas preventivas frente a amenazas cibernéticas que puedan afectar servicios esenciales.

La adopción de estándares como IEC 62443 e IEC 62351 se encuentra alineada con los objetivos de esta política nacional, al fortalecer la resiliencia de infraestructuras críticas frente a amenazas digitales.(Departamento Nacional de Planeación, 2016)

3.5.5. Relación entre el marco regulatorio colombiano y las normas IEC 62443 e IEC 62351

Si bien las normas IEC 62443 e IEC 62351 no son de obligatorio cumplimiento por disposición legal directa en Colombia, su adopción voluntaria constituye una práctica recomendada para fortalecer la seguridad de infraestructuras industriales y eléctricas.

En el ámbito de EBSA, la implementación de arquitecturas alineadas con dichos estándares contribuye a:

- Reducir el riesgo de incidentes que afecten indicadores regulatorios.
- Fortalecer la continuidad del servicio.
- Mejorar la gestión del riesgo corporativo.
- Aumentar la resiliencia de infraestructura crítica.

En consecuencia, el presente estudio técnico comparativo se desarrolla no solo como una iniciativa de mejora tecnológica, sino como un aporte estratégico a la gestión integral del riesgo operativo y regulatorio de la empresa.

Capítulo 4

Metodología

4.1. Enfoque y tipo de investigación

El presente estudio adopta un enfoque metodológico mixto, integrando elementos cualitativos y cuantitativos. El componente cualitativo se fundamenta en la revisión normativa (IEC 62443 e IEC 62351), la caracterización de los entornos IT/OT y la identificación de requisitos de ciberseguridad.

Por su parte, el componente cuantitativo se desarrolla mediante la construcción y aplicación de una matriz de evaluación, en la cual se asignan valores ponderados a diferentes criterios técnicos, permitiendo comparar de manera objetiva las tecnologías analizadas. Este enfoque permite reducir la subjetividad en la selección de equipos y facilita la toma de decisiones basada en evidencia.

4.2. Ámbito de aplicación del estudio

El presente estudio técnico comparativo se desarrolla tomando como referencia el entorno operativo de la Empresa de Energía de Boyacá S.A. E.S.P. (EBSA), en su condición de Operador de Red (OR) del Sistema Interconectado Nacional colombiano.

El análisis se centra particularmente en la interacción entre los entornos de Tecnologías de la Información (IT) y Tecnologías de la Operación (OT), considerando como escenario representativo una subestación de distribución típica de nivel de tensión 34.5 kV / 13.2 kV integrada a un centro de control mediante protocolos industriales sobre TCP/IP, tales como IEC 60870-5-104.

Dado que por razones de seguridad y confidencialidad no se dispone de acceso directo a configuraciones internas específicas de la empresa, el estudio modela una arquitectura técnicamente coherente con la operación estándar de subestaciones de distribución utilizadas por operadores de red en Colombia, incluyendo activos como IEDs, RTUs, switches industriales gestionables, firewalls industriales, gateways IT/OT y sistemas de monitoreo.

El alcance del estudio se limita al análisis técnico de selección de equipos y definición de arquitectura de referencia de ciberseguridad, alineada con los requisitos establecidos

en las normas IEC 62443 e IEC 62351, sin intervenir sistemas reales ni realizar pruebas en infraestructura operativa de la empresa.

4.3. Fases Metodológicas

La metodología se estructura en cinco fases secuenciales, las cuales permiten dar cumplimiento a los objetivos planteados y asegurar las coherencia entre el marco teórico, el análisis realizado y los resultados obtenidos.

4.3.1. Fase 1: Revisión documental y análisis normativo

Actividades desarrolladas en la fase

- **1.** Recolección de normas internacionales relacionadas con la ciberseguridad industrial y del sector eléctrico.
- **2.** Revisión de guías técnicas y marcos de referencia en ciberseguridad OT.
- **3.** Análisis de literatura científica especializada en infraestructuras críticas y convergencia IT-OT.

En esta fase se realiza la recopilación y el estudio detallado de normas internacionales que sirven como base para la ciberseguridad en infraestructuras industriales y eléctricas. La recolección de normas se enfoca principalmente en la serie IEC 62443, utilizada para definir requisitos de seguridad en sistemas de automatización y control industrial, y en la norma IEC 62351, orientada a la protección de las comunicaciones en sistemas eléctricos. Cada norma es analizada para identificar sus objetivos, su alcance, los requisitos que establece y su aplicabilidad en entornos IT y OT.

Adicionalmente, se revisan guías técnicas y documentos de referencia en ciberseguridad OT, los cuales permiten complementar el enfoque normativo con buenas prácticas ampliamente aceptadas en el sector. Estas guías aportan criterios para la gestión del riesgo, la segmentación de redes y la protección de sistemas críticos, facilitando la interpretación práctica de los requisitos normativos.

Finalmente, se analizan artículos académicos y estudios especializados relacionados con ciberseguridad en infraestructuras críticas, con el fin de identificar enfoques utilizados en proyectos similares, tendencias tecnológicas y principales desafíos reportados en la literatura. El resultado de esta fase es la consolidación del marco normativo y conceptual que sustentan el desarrollo del estudio comparativo.

4.3.2. Fase 2: Caracterización conceptual de entornos IT y OT

Actividades desarrolladas en la fase:

- **1.** identificación conceptual de activos IT y OT relevantes en empresas del sector energético.
- **2.** Análisis de los flujos de información entre entornos IT y OT.

- **3.** Identificación y priorización de factores que influyen en la protección de activos y flujos de información.

En esta fase se realiza la caracterización de los entornos IT y OT tomando como referencia el contexto operativo de EBSA, identificando activos típicos presentes en una subestación de distribución y su integración con el centro de control. Se describen elementos tales como sistemas SCADA, RTUs, IEDs de protección y control, dispositivos de red industriales, servidores corporativos y mecanismos de interconexión IT-OT, con el fin de analizar los flujos de información críticos y su impacto en la continuidad del servicio eléctrico.

Posteriormente, se analizan los flujos de información que se generan entre dichos activos, prestando especialmente atención a aquellos flujos que atraviesan la frontera IT-OT y que pueden representar un mayor riesgo desde el punto de vista de la ciberseguridad. Este análisis permite comprender cómo circula la información operativa y corporativa dentro de una empresa del sector eléctrico.

Como complemento, se emplean herramientas de análisis cuantitativo, como el diagrama de causa-efecto y el diagrama de Pareto, para identificar y priorizar los factores que influyen en la necesidad de proteger los activos y flujos de información. Esta priorización permite enfocar el estudio en aquellos aspectos que generan mayor impacto sobre el riesgo cibernético, al finalizar esta fase se da cumplimiento al primer objetivo específico.

4.3.3. Fase 3: Definición de criterios técnicos de evaluación

Actividades desarrolladas en la fase:

- **1.** Identificación de requisitos de seguridad derivados de las normas IEC 62443 e IEC 62351.
- **2.** Clasificación de criterios técnicos, operativos y de viabilidad.
- **3.** Construcción de la matriz de criterios para la evaluación comparativa.

En esta fase se extraen y sistematizan los requisitos técnicos de ciberseguridad establecidos en las normas IEC 62443 e IEC 62351, tales como segmentación de redes, control de flujos, autenticación, cifrado de comunicaciones, monitoreo y continuidad operativa. Cada requisito es interpretado en función de su aplicabilidad en entornos IT y OT del sector energético.

A partir de estos requisitos, se definen criterios de evaluación que consideran no solo aspectos técnicos, sino también factores operativos y de viabilidad, como la compatibilidad con sistemas existentes y la posibilidad de implementación progresiva. Estos criterios se organizan de manera estructurada en una matriz de evaluación, la cual constituye el instrumento central para el análisis comparativo de alternativas tecnológicas, al finalizar esta fase se da cumplimiento al segundo objetivo específico.

4.3.4. Fase 4: Evaluación técnica comparativa de alternativas

Actividades desarrolladas en la fase:

- 1. Identificación de tipos de equipos y arquitecturas de ciberseguridad aplicables a entornos IT y OT.
- 2. Análisis de capacidades funcionales y técnicas de cada alternativa.
- 3. Comparación de las alternativas utilizando la matriz de criterios definida.

En esta fase, se identifican diferentes tipos de equipos y arquitecturas de ciberseguridad que pueden ser utilizados para la protección de entornos IT y OT, tales como soluciones de segmentación de red y dispositivos de protección y monitoreo.

Cada alternativa es analizada en función de sus capacidades técnicas y funcionales, evaluando su alineación con los criterios definidos en la fase anterior. La comparación se realiza de manera cualitativa, sin considerar marcas o fabricantes específicos, con el objetivo de mantener un enfoque objetivo y normativo. El resultado de esta fase es la identificación de fortalezas, limitaciones y posibles escenarios de la aplicación de cada alternativa.

La evaluación incluye tecnologías representativas disponibles en el mercado industrial, considerando fabricantes reconocidos en entornos de automatización eléctrica, con el fin de analizar su alineación con los requisitos normativos establecidos en IEC 62443 e IEC 62351.

4.3.5. Fase 5: Propuesta de arquitectura de referencia y análisis de resultados

Actividades desarrolladas en la fase:

- 1. Integración y síntesis de los resultados obtenidos en la evaluación comparativa.
- 2. Definición de una arquitectura de referencia de ciberseguridad para un entorno simulado con ayuda del software GNS3.
- 3. Análisis e interpretación de los resultados en relación con el marco teórico

En esta fase final se integran los resultados del análisis comparativo para proponer una arquitectura de referencia de ciberseguridad, alineada con los principios de defensa en profundidad y segmentación definidos por la norma IEC 62443, e incorporando los mecanismos de protección de comunicaciones establecidos en IEC 62351.

La arquitectura propuesta tiene un carácter conceptual y busca servir como guía para la toma de decisiones técnicas, considerando la renovación tecnológica progresiva y las restricciones operativas propias del sector energético. Finalmente, se realiza un análisis de los resultados obtenidos, relacionándolos con el marco teórico y con estudios previos, lo que permite sustentar las conclusiones y recomendaciones del trabajo, al finalizar esta fase se da cumplimiento al tercer objetivo específico.

4.4. Técnicas e Instrumentos de investigación

Para el desarrollo de la presente monografía se emplean técnicas de investigación de tipo documental y analítico-comparativo. La técnica documental se utiliza para la revisión sistemática de normas internacionales, guías técnicas y literatura científica relacionada con la ciberseguridad en infraestructuras críticas del sector energético, permitiendo la identificación de conceptos, requisitos y enfoques relevantes para el estudio.

Como instrumentos de investigación se utilizan matrices de análisis y evaluación, las cuales permiten organizar y comparar de manera estructurada los criterios técnicos, operativos y de viabilidad definidos a partir de las normas IEC 62443 e IEC 62351. Estas matrices constituyen la herramienta principal para la evaluación comparativa de alternativas de ciberseguridad.

Adicionalmente, se emplean representaciones gráficas como diagramas de arquitectura, diagramas de causa-efecto y diagramas de Pareto, con el fin de apoyar el análisis cualitativo de activos, flujos de información y factores de riesgo. Para la organización y sistematización de la información se utilizan herramientas ofimáticas, las cuales facilitan la consolidación de resultados y su posterior análisis.

4.5. Construcción de la matriz de criterios de evaluación

La construcción de la matriz de criterios de evaluación constituye una etapa central dentro del estudio técnico comparativo, ya que permite traducir los requisitos técnicos de ciberseguridad definidos previamente en un instrumento sistemático para el análisis de alternativas tecnológicas. En el contexto de infraestructuras críticas del sector energético, la selección de equipos y arquitecturas de ciberseguridad no pueden basarse únicamente en características comerciales, sino que debe responder a criterios técnicos, normativos y operativos claramente definidos.

La matriz desarrollada en este estudio se fundamenta en los requisitos derivados de las normas IEC 62443 e IEC 62351, así como en consideraciones operativas propias de los entornos IT y OT. Su objetivo es proporcionar un marco objetivo y reproducible que permita comparar diferentes tecnologías de ciberseguridad de manera estructurada, sirviendo como base para la posterior evaluación de soluciones específicas.

4.5.1. Estructura general de la matriz de criterios

La matriz de criterios se estructura en categorías que agrupan requisitos con características comunes. Cada categoría responde a un aspecto clave de la ciberseguridad en infraestructuras críticas y permite evaluar en forma integral las capacidades de las tecnologías analizadas.

La ponderación y selección de criterios responde a las necesidades técnicas y operativas del entorno de subestación considerado en EBSA, priorizando segmentación,

disponibilidad y control de flujos conforme a los lineamientos de IEC 62443.

La categorías definidas en la matriz corresponden a:

- Cumplimiento Normativo.
- Arquitectura y segmentación de red.
- Seguridad de las comunicaciones.
- Control de accesos y gestión.
- Monitoreo y Respuesta.
- Requisitos operativos y de continuidad.

Esta estructura permite asegurar que la evaluación no se limite a un único aspecto técnico, sino que considere de manera equilibrada los diferentes factores que influyen en la viabilidad de una solución de ciberseguridad en entornos IT-OT. La matriz se presenta en la tabla numero 5.4.1, denominada matriz de criterios para la evaluación de tecnologías de ciberseguridad IT-OT.

Tabla 4.5.1: Matriz de criterios para la evaluación de tecnologías de ciberseguridad IT/OT

Categoría	Criterio	Descripción	Referencia
Cumplimiento normativo	Alineación IEC 62443	Soporte para segmentación, zonas y conductos, defensa en profundidad	IEC 62443
Arquitectura	Segmentación de red	Capacidad de crear separación lógica o física entre dominios IT y OT	IEC 62443
Seguridad de comunicaciones	Cifrado	Soporte de TLS u otros mecanismos criptográficos	IEC 62351
Gestión y monitoreo	Registro de eventos	Generación y exportación de logs de seguridad	Buenas prácticas OT
Operación	Alta disponibilidad	Soporte para redundancia y tolerancia a fallos	Sector energético
Viabilidad	Implementación progresiva	Posibilidad de adopción gradual según ciclo de vida	Estrategia EBSA

4.5.1.1. Trazabilidad entre requisitos normativos y criterios de evaluación

Con el propósito de garantizar que la metodología de evaluación utilizada se encuentre alineada con los estándares internacionales aplicables a la ciberseguridad industrial, se estableció una trazabilidad directa entre los requisitos identificados en las normas IEC 62443 e IEC 62351 y los criterios empleados en la matriz de evaluación de tecnologías.

La norma IEC 62443 proporciona los lineamientos para la protección de sistemas de automatización y control industrial mediante conceptos como segmentación por zonas y conductos, defensa en profundidad, control de acceso, monitoreo de eventos de seguridad y gestión de riesgos. Por su parte, la norma IEC 62351 complementa estos requisitos mediante mecanismos específicos para la protección de las comunicaciones en sistemas eléctricos, incorporando controles de autenticación, cifrado, integridad de mensajes y gestión de certificados digitales.

La Tabla 4.5.2 presenta la relación establecida entre los principales criterios de evaluación considerados en este estudio y los requisitos normativos asociados.

Tabla 4.5.2: Trazabilidad entre criterios de evaluación y requisitos normativos

Criterio de evaluación	IEC 62443	IEC 62351
Segmentación de redes IT/OT	IEC 62443-3-2 (Zonas y Conductos)	No aplica directamente
Control de acceso y autenticación	IEC 62443-3-3 SR 1	IEC 62351-8
Monitoreo y registro de eventos	IEC 62443-3-3 SR 6	Soporte complementario
Protección de comunicaciones	IEC 62443-3-3 SR 3	IEC 62351-3 y IEC 62351-5
Cifrado de información	Requisito general de seguridad	IEC 62351-3 (TLS)
Gestión de certificados digitales	Requisito organizacional	IEC 62351-9
Integridad de mensajes	IEC 62443-3-3 SR 3	IEC 62351-5 e IEC 62351-6
Defensa en profundidad	IEC 62443-3-3	Complementa la protección de protocolos

Esta trazabilidad permitió justificar la selección de los criterios empleados en la matriz comparativa y asegurar que la evaluación de las tecnologías analizadas estuviera fundamentada en requisitos internacionalmente reconocidos para la protección de infraestructuras críticas y sistemas eléctricos de potencia.

Las ponderaciones asignadas a los criterios de evaluación fueron definidas considerando la criticidad de los requisitos identificados en IEC 62443 e IEC 62351, priorizando aquellos relacionados con segmentación, autenticación, protección de comunicaciones y defensa en profundidad.

4.5.2. Criterios de cumplimiento normativo

Los criterios de cumplimiento normativo permiten evaluar el grado en que tecnología o equipo de ciberseguridad se alinea con los lineamientos establecidos en las normas IEC

62443 e IEC 62351. Estos criterios no buscan certificar formalmente los equipos, sino verificar que sus capacidades técnicas permitan cumplir con los requisitos normativos aplicables.

Desde la perspectiva del estudio, este grupo de criterios resulta fundamental para garantizar que las soluciones evaluadas sean compatibles con estándares internacionales ampliamente aceptados y que puedan integrarse en arquitecturas de ciberseguridad alineadas con buenas prácticas del sector energético.

4.5.3. Criterios de arquitectura y segmentación

Los criterios de arquitectura y segmentación evalúan la capacidad de las tecnologías para implementar el modelo de zonas y conductos propuesto por IEC 62443. Estos criterios permiten analizar si una solución facilita la separación de dominios IT y OT, el control de flujos de información y la aplicación de políticas de seguridad diferenciadas según la criticidad de los activos.

En infraestructuras del sector energético, una arquitectura mal segmentada puede permitir la propagación de incidentes desde sistemas corporativos hacia sistemas de control industrial. Por esa razón, los criterios de este grupo tienen un peso significativo dentro de la matriz de evaluación.

4.5.4. Criterio de seguridad de las comunicaciones

Este grupo de criterios se deriva principalmente de la norma IEC 62351 y se orienta a evaluar la capacidad de las tecnologías para proteger los flujos de información críticos. Se consideran aspectos como el cifrado de comunicaciones, la autenticación de dispositivos y la verificación de integridad de los datos.

la inclusión de estos criterios permite analizar si las soluciones evaluadas pueden proteger adecuadamente las comunicaciones entre centros de control, subestaciones y sistemas de gestión, sin afectar la disponibilidad ni el desempeño operativo del sistema eléctrico.

4.5.5. Criterios de control, monitoreo y gestión

Los criterios de control, monitoreo y gestión evalúa la capacidad de las tecnologías para administrar accesos, registrar eventos y proporcionar visibilidad sobre el estado de la infraestructura. En entornos OT, estos criterios deben considerar la necesidad de monitoreo pasivo y la mínima interferencia con los procesos operativos.

Este grupo de criterios resulta clave para fortalecer la detección temprana de incidentes y la trazabilidad de eventos, aspectos fundamentales para una gestión efectiva de la ciberseguridad en infraestructuras críticas.

4.5.6. Criterios operativos y de viabilidad

Finalmente, los criterios operativos y de viabilidad permiten evaluar si las tecnologías analizadas pueden ser implementadas de manera realista en entornos del sector energético. Estos criterios consideran factores como la compatibilidad con sistemas existentes, la alta disponibilidad, el impacto en la latencia y la posibilidad de implementación progresiva.

La inclusión de este grupo de criterios asegura que las soluciones evaluadas no solo sean técnicamente adecuadas, sino también viables desde el punto de vista operativo y estratégico.

4.6. Metodología de evaluación aplicada a las tecnologías

4.6.1. Aplicación de la matriz de criterios

La aplicación de la matriz de criterios se realiza de forma individual para cada alternativa tecnológica, evaluando su capacidad para cumplir con los requisitos establecidos en cada categoría. Para ello, se analizan las especificaciones técnicas y funcionales de las tecnologías a partir de documentación oficial, como fichas técnicas, manuales de referencia y documentos técnicos publicados por fabricantes y proveedores reconocidos.

Cada criterio es evaluado de manera independiente, verificando si las tecnología:

- Cumple plenamente el requisito con el requisito.
- Cumple de manera parcial.
- No cumple con el requisito definido.

Este enfoque permite reflejar de forma clara las fortalezas y limitaciones de cada alternativa, sin forzar comparaciones directas entre tecnologías con funciones diferentes.

4.6.2. Escala de evaluación

Con el fin de facilitar la interpretación de los resultados, se adopta una escala de evaluación cualitativa compuesta por tres niveles:

- **Cumple(C):** La tecnología satisface completamente el criterio evaluado conforme a los requisitos definidos.
- **Cumple Parcialmente(CP):** La tecnología satisface el criterio de manera limitada o requiere configuraciones adicionales para su cumplimiento.
- **No cumple (NC):** La tecnología no dispone de las capacidades necesarias para satisfacer el criterio evaluado.

Esta escala se complementa con observaciones técnicas, en las cuales se justifica la calificación asignada a cada criterio. Dichas observaciones permiten contextualizar los resultados y aportar claridad sobre las condiciones bajo las cuales una tecnología podría ser utilizada.

4.7. Alcance del análisis de equipos y arquitecturas de ciberseguridad

El presente estudio se delimita al análisis técnico de equipos y arquitecturas de ciberseguridad aplicables a entornos de redes industriales y sistemas de supervisión utilizados en subestaciones eléctricas. El análisis se centrará principalmente en tecnologías que permitan fortalecer la autenticación de dispositivos, la segmentación de red y el control de acceso a los recursos críticos del sistema.

Dentro de este alcance se considerarán dispositivos de infraestructura de red tales como routers, switches industriales, gateways de comunicación y puntos de acceso inalámbrico, así como soluciones de seguridad orientadas a la protección de redes industriales, incluyendo firewalls industriales, mecanismos de autenticación y plataformas de monitoreo de tráfico de red.

El análisis se enfocará en evaluar la aplicabilidad de estas tecnologías en escenarios representativos de una subestación eléctrica conectada a un centro de control, considerando tanto las necesidades operativas del sistema eléctrico como los requerimientos de seguridad establecidos para infraestructuras críticas.

4.8. Validez, confiabilidad y replicabilidad del método

El enfoque metodológico adoptado en el presente estudio garantiza su validez, confiabilidad y replicabilidad mediante la integración de estándares internacionales, criterios técnicos estructurados y procedimientos documentados.

En cuanto a la validez, esta se sustenta en el uso de marcos normativos ampliamente reconocidos en el ámbito de la ciberseguridad industrial, como las normas IEC 62443 y IEC 62351. Estos estándares proporcionan lineamientos técnicos para la protección de infraestructuras críticas y sistemas eléctricos, permitiendo que los criterios definidos en la matriz de evaluación estén alineados con buenas prácticas internacionales. De esta manera, las variables analizadas (segmentación de red, control de accesos, seguridad de las comunicaciones, monitoreo, entre otras) reflejan condiciones reales de seguridad en entornos IT/OT.

Respecto a la confiabilidad, esta se garantiza mediante la definición clara y estructurada de criterios de evaluación, así como por la aplicación uniforme de una matriz comparativa a todas las tecnologías analizadas. La asignación de ponderaciones a cada criterio permite reducir la subjetividad del análisis, asegurando que la evaluación se base en parámetros consistentes y reproducibles. Además, la utilización de una escala de valoración homogénea facilita la comparación objetiva entre diferentes soluciones

tecnológicas.

En relación con la replicabilidad, el método propuesto ha sido documentado de manera detallada en cada una de sus fases, incluyendo la construcción de la matriz de evaluación, los criterios utilizados, la metodología de ponderación y el entorno experimental implementado en GNS3. Esto permite que otros investigadores o profesionales del sector puedan aplicar la misma metodología en contextos similares, adaptando los criterios a sus necesidades específicas sin perder la coherencia del enfoque.

En conjunto, estos elementos consolidan un método robusto, aplicable y fundamentado, que no solo permite analizar tecnologías de ciberseguridad en el contexto de la Empresa de Energía de Boyacá (EBSA), sino que también puede ser extendido a otras infraestructuras críticas del sector energético.

Capítulo 5

Desarrollo de las Fases Metodológicas

El presente capítulo desarrolla el estudio técnico comparativo propuesto en la monografía, con el fin de evaluar alternativas de ciberseguridad aplicables entornos IT y OT en el contexto de una empresa del sector energético. El análisis se fundamenta en los conceptos, principios y requisitos establecidos en el marco teórico, así como en los lineamientos definidos por las normas IEC 62443 e IEC 62351.

El desarrollo del estudio se realiza de manera progresiva, iniciando con la caracterización técnica del escenario IT-OT y la identificación de activos y flujos de información críticos, para luego definir los requisitos de ciberseguridad que deben ser satisfechos. A partir de estos requisitos, se construye una matriz de criterios que permite realizar una evaluación técnica comparativa de diferentes alternativas tecnológicas, sin considerar marcas o fabricantes específicos.

Este enfoque metodológico permite asegurar que la selección de equipos y arquitecturas de ciberseguridad se encuentre alineada con las necesidades operativas, las restricciones tecnológicas y los estándares internacionales aplicables al sector energético, proporcionando una base técnica sólida para la propuesta de una arquitectura de referencia

5.1. Definición del caso de estudio

El caso de estudio considerado en el presente trabajo corresponde a una subestación de distribución típica de operador de red colombiano, con nivel de tensión 34.5 kV / 13.2 kV, integrada a un centro de control mediante protocolo IEC 60870-5-104 sobre TCP/IP. La subestación incluye dispositivos de protección (IED), unidad terminal remota (RTU), red de comunicaciones industrial basada en switches gestionables y un perímetro de interconexión IT/OT.

La subestación considerada se clasifica como infraestructura crítica dentro del sistema de distribución de EBSA, debido a que su indisponibilidad podría afectar la continuidad del servicio eléctrico a usuarios residenciales, comerciales e industriales del área de influencia. En este sentido, la protección de sus activos y flujos de información adquiere carácter estratégico.

5.2. Caracterización técnica del escenario IT-OT

La caracterización técnica del escenario IT-OT constituye el punto de partida del estudio técnico comparativo, ya que permite contextualizar el entorno tecnológico sobre el cual se definirán los requisitos de ciberseguridad y se evaluarán las alternativas disponibles. En empresas del sector energético, la coexistencia de sistemas IT y OT responde a necesidades operativas y de gestión diferenciadas, pero interdependientes, lo que exige un análisis estructurado de sus componentes, interacciones y flujos de información.

En este apartado describe de manera general los entornos IT y OT, así como los mecanismos de interacción entre ambos, sin hacer referencia a configuraciones específicas ni a tecnologías propietarias. El objetivo es establecer un escenario representativo y genérico, alineado con las prácticas del sector eléctrico, que sirva como base para el análisis posterior conforme a los lineamientos de las normas IEC 62443 e IEC 62351.

5.2.1. Descripción general del entorno IT

En entornos de tecnologías de la información IT en una empresa del sector energético está orientado a la gestión de información corporativa, administrativa y de soporte a la toma de decisiones. Este entorno agrupa sistemas como plataformas de gestión empresarial, servidores de base de datos, aplicaciones corporativas, sistemas de correo electrónico y redes de comunicación LAN y WAN, los cuales operan principalmente sobre arquitecturas IP y protocolos estándar.

Desde el punto de vista técnico, los sistemas IT se caracterizan por su enfoque en la confidencialidad, integridad y disponibilidad de la información, así como por su capacidad de integración y escalabilidad. La infraestructura IT suele contar con mecanismos de seguridad tradicionales, como firewalls perimetrales, sistemas de autenticación centralizada y políticas de control de acceso, diseñados para proteger información sensible y garantizar la continuidad de los servicios corporativos.

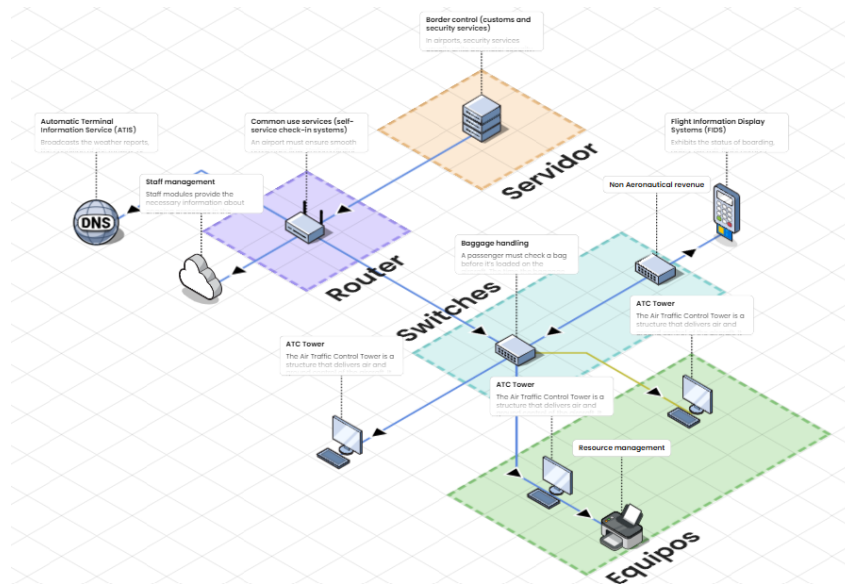


Figura 5.2.1: Entorno IT
Fuente: (Elaboración propia, 2026)

No obstante, en escenarios de convergencia IT-OT, el entorno IT también actúa como punto de entrada para flujos de información operativa, lo que incrementa su relevancia desde la perspectiva de la ciberseguridad industrial. Esta situación hace necesario considerar el entorno IT ilustrado en la figura 5.2.1 no solo como un sistema corporativo aislado, sino como un componente activo dentro de la arquitectura global de la empresa.

5.2.2. Descripción general del entorno OT

El entorno de tecnologías de operación OT comprende los sistemas y dispositivos encargados de supervisar y controlar procesos físicos asociados a la generación, transmisión y distribución de energía eléctrica. Este entorno incluye sistemas SCADA, unidades terminales remotas (RTU), controladores lógicos programables (PLC), dispositivos de protección y equipos de campo, los cuales interactúan directamente con activos físicos del sistema eléctrico.

Desde una perspectiva técnica, los sistemas OT se distinguen por operar en tiempo real o casi real, con estrictos requisitos de disponibilidad y confiabilidad. La arquitectura OT suele estar diseñada para mantener la estabilidad del proceso, priorizando la continuidad operativa sobre otros criterios, lo que históricamente ha limitado la incorporación de mecanismos avanzados de ciberseguridad.

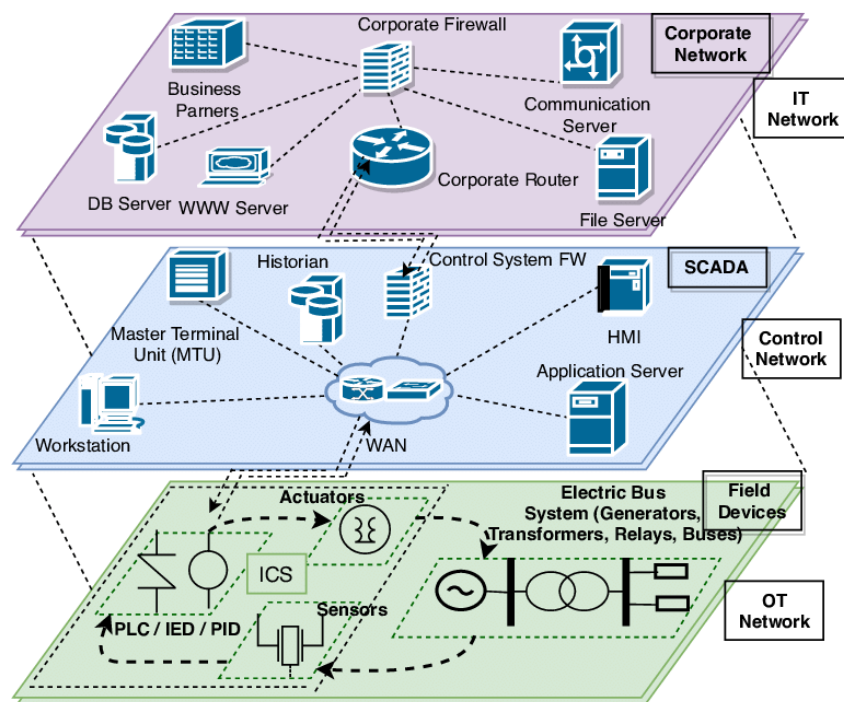


Figura 5.2.2: Entorno OT
Fuente: (ResearchGate, 2026a)

La interconexión progresiva ilustrada en la figura 5.2.2 sistemas OT con redes IP y plataformas de gestión ha permitido mejorar la visibilidad y el control de la operación, pero también ha introducido nuevos riesgos. En este contexto, el entorno OT debe analizarse considerando sus limitaciones técnicas, sus largos ciclos de vida y su dependencia de comunicaciones confiables, factores que condicionan la selección de soluciones de ciberseguridad.

5.2.3. Clasificación de activos críticos según nivel de criticidad para la empresa EBSA

Con el fin de estructurar la gestión de activos desde una perspectiva de riesgo, se realiza una clasificación de los activos OT identificados en la subestación tipo analizada. Esta clasificación considera el impacto potencial sobre la operación del sistema eléctrico en caso de compromiso del activo. (Empresa de Energía de Boyacá, 2024)

Tabla 5.2.1: Clasificación de activos OT según criticidad e impacto

Activo	Función	Nivel de criticidad	Impacto potencial
IED de protección	Protección de alimentadores y transformadores	Alta	Desconexión incorrecta, daño a equipos, interrupción del servicio
RTU	Comunicación con centro de control	Alta	Pérdida de supervisión y control remoto
Switch industrial OT	Interconexión de dispositivos	Media-Alta	Interrupción de comunicaciones internas
Firewall industrial	Segmentación y control de flujos	Alta	Propagación de amenazas IT-OT
Gateway IT/OT	Interconexión controlada	Alta	Acceso no autorizado desde red corporativa
Servidor SCADA	Supervisión y gestión operativa	Alta	Pérdida de visibilidad operativa y control
Estaciones de ingeniería	Configuración y mantenimiento	Media	Alteraciones de configuración no autorizadas

5.2.4. Interacción y flujos de información entre IT y OT

La interacción entre los entornos IT y OT se produce a través de flujos de información que permiten el intercambio de datos operativos, eventos, alarmas y reportes de gestión. Estos flujos son esenciales para la supervisión integral del sistema eléctrico y para la toma de decisiones a nivel operativo y estratégico. Sin embargo, también representan uno de los principales vectores de riesgo desde el punto de vista de la ciberseguridad.(Alonso et al., 2021)

Técnicamente, los flujos IT-OT pueden atravesar múltiples dominios de seguridad, incluyendo redes corporativas, zonas intermedias y redes operativas. La ausencia de una segmentación adecuada o de controles específicos sobre estos flujos puede facilitar la propagación de incidentes desde el entorno IT hacia sistemas OT, con potencial impacto en la operación del sistema eléctrico.(Alonso et al., 2021)

Por esta razón, la identificación y comprensión de los flujos de información entre IT y OT resulta fundamental para definir requisitos de seguridad, establecer zonas de protección y controlar los conductos de comunicación conforme a la norma IEC 62443.

Este análisis permite además identificar puntos críticos donde se requiere la aplicación de mecanismos de cifrado, autenticación y monitoreo, en concordancia con los lineamientos de la norma IEC 62351.

5.3. Identificación de activos críticos y flujos de información

La identificación de activos críticos y de los flujos de información asociados constituye un paso fundamental para el desarrollo del estudio técnico comparativo, ya que permite determinar que elementos del entorno IT-OT requieren mayores niveles de protección desde la perspectiva de la ciberseguridad. En infraestructuras del sector energético, los activos tecnológicos y los flujos de información están estrechamente vinculados a la operación del sistema eléctrico, por lo que su compromiso puede generar impactos significativos en la continuidad del servicio.

Esta sección ofrece una identificación conceptual y general de los activos OT e IT, además de los flujos informativos críticos que surgen entre ambos, sin mencionar configuraciones particulares de la compañía. El análisis se ajusta a los lineamientos de las normas IEC 62443 e IEC 62351 y a los principios de gestión del riesgo, lo que permite la determinación posterior de requisitos relacionados con la ciberseguridad. (International Electrotechnical Commission, 2018) (International Electrotechnical Commission, 2013)

5.3.1. Identificación de activos IT relevantes

Los activos IT en una empresa del sector energético corresponden a los sistemas y componentes tecnológicos utilizados para la gestión de información corporativa, administrativa y de soporte a la operación. Entre estos activos se incluye servidores de aplicaciones y bases de datos, plataformas de gestión empresarial, sistemas de respaldo y recuperación, dispositivos de red corporativos y estaciones de trabajo de usuarios.

Desde el punto de vista de ciberseguridad, estos activos son críticos debido a que almacenan y procesan información sensible, como datos operativos consolidados, información financiera, registros históricos y credenciales de acceso. Además, en escenarios de convergencia IT-OT, los sistemas IT suelen actuar como intermediarios para el acceso a información proveniente del entorno OT, lo que incrementa su relevancia dentro de la arquitectura de seguridad.



Figura 5.3.1: Activos IT
Fuente: (Elaboración propia, 2026)

La protección de los activos debe considerar no solo amenazas externas, sino también riesgos asociados a accesos indebidos, configuraciones incorrectas y fallas en los mecanismos de autenticación y control de privilegios. Por esta razón, la identificación clara de estos activos resulta esencial para establecer controles adecuados y evitar que vulnerabilidades en el entorno IT se conviertan en vectores de ataque hacia sistemas operativos críticos.

5.3.2. Identificación de activos OT relevantes

Los activos OT corresponden a los sistemas y dispositivos encargados de la supervisión y control de los procesos físicos asociados al sistema eléctrico. Estos activos incluyen sistemas SCADA, unidades terminales remotas(RTU), controladores lógicos programables (PLC), dispositivos de protección, relés digitales y equipos de comunicación industrial.

A diferencia de los activos IT, los activos OT interactúan directamente con el proceso físico, por lo que su compromiso puede tener consecuencias inmediatas sobre la operación del sistema eléctrico. Estos sistemas suelen operar bajo estrictos requisitos de disponibilidad y confiabilidad, y presentan limitaciones técnicas que dificultan la aplicación de mecanismos de seguridad tradicionales.



Figura 5.3.2: Activos OT presentes
Fuente: (Elaboración propia, 2026)

5.3.3. Identificación de flujos de información críticos

Los flujos de información representan los canales mediante los cuales se intercambian datos entre IT y OT, y constituyen uno de los principales elementos a proteger en entornos convergentes. En empresas del sector energético, estos flujos incluyen la transmisión de datos de supervisión, comandos de control, alarmas, eventos, reportes operativos y datos históricos.

Desde el punto de vista de la ciberseguridad, los flujos críticos son aquellos cuya interrupción, manipulación o interpretación puede afectar la operación del sistema eléctrico o comprometer la integridad de la información. Estos flujos pueden atravesar diferentes dominios de seguridad, incluyendo redes corporativas, zonas intermedias y redes operativas, lo que incrementa su exposición a amenazas. (Gavilán, 2019)

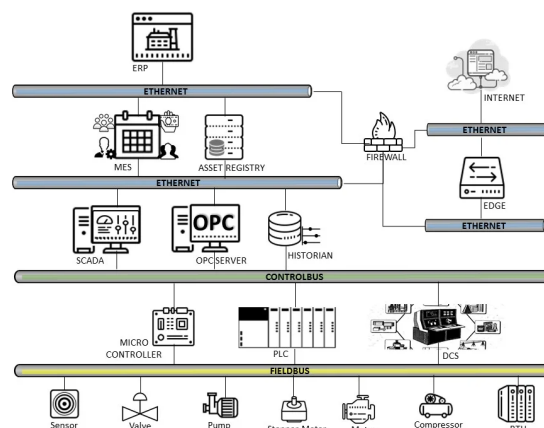


Figura 5.3.3: Flujos de información industriales
Fuente: (Gavilán, 2019)

La identificación de los flujos de información críticos permite determinar dónde se

requiere mecanismos de protección adicionales, como cifrado, autenticación y control de acceso, conforme a los lineamientos de la norma IEC 62351. Asimismo, este análisis facilita la definición de conductos de comunicación controlados según el modelo propuesto por la norma IEC 62443.

5.3.4. Riesgos asociados a los flujos IT-OT

Los flujos información entre entornos IT y OT introducen riesgos específicos que deben ser considerados en el diseño de arquitecturas de ciberseguridad. Entre estos riesgos se encuentran el acceso no autorizado a sistemas operativos, la manipulación y la propagación de incidentes desde el entorno IT hacia sistemas OT.

La falta de segmentación adecuada, el uso de protocolos sin mecanismos de seguridad robustos y la ausencia de controles sobre los flujos de información pueden facilitar la materialización de estos riesgos. En este sentido, el análisis de riesgos asociados a los flujos IT-OT permite justificar la necesidad de enfoques de protección basados en arquitectura, segmentación y defensa en profundidad.

Este análisis se complementa con el uso de herramientas como el diagrama causa-efecto y el diagrama de Pareto, anteriormente anexados, los cuales permiten visualizar y priorizar los factores que influyen en el riesgo de compromiso de los activos y flujos de información. Los resultados obtenidos en este apartado sirven como insumo directo para la definición de requisitos técnicos de ciberseguridad en el siguiente capítulo.

5.4. Definición de requisitos técnicos de ciberseguridad

La definición de requisitos técnicos de ciberseguridad constituye el vínculo entre la caracterización del escenario IT-OT y la evaluación comparativa de alternativas tecnológicas. En infraestructura del sector energético, dichos requisitos deben responder tanto a los lineamientos normativos internacionales como a las restricciones operativas propias de los sistemas industriales. En este sentido, los requisitos definidos en el presente estudio se fundamentan principalmente en las normas IEC 62443 e IEC 62351, complementados con consideraciones operativas orientadas a la continuidad del servicio.

El objetivo de este capítulo es establecer un conjunto estructurado de requisitos técnicos que permitan evaluar de manera objetiva las alternativas de ciberseguridad, asegurando que estas sean viables desde el punto de vista normativo.

5.4.1. Requisitos técnicos derivados de la norma IEC 62443

La norma IEC 62443 establece un marco integral para la ciberseguridad de sistemas de automatización y control industrial, basados en principios arquitectónicos y en la defensa en profundidad. A partir de esta norma, se derivan requisitos técnicos orientados principalmente a la segmentación de la infraestructura, el control de accesos y la protección de los flujos de información entre zonas.

Uno de los requisitos fundamentales derivados de IEC 62443 es la segmentación del sistema en zonas de seguridad, de acuerdo con la criticidad de los activos y los riesgos

asociados. Cada zona debe agrupar activos con requisitos de seguridad similares, permitiendo la aplicación de controles específicos y reduciendo la superficie de ataque. Este requisito implica la necesidad de soluciones que soporten separación lógica o física de redes, así como mecanismos de control de tráfico entre zonas.

Asociado a la segmentación, la norma establece la necesidad de definir y proteger los conductos de comunicación entre zonas, garantizando que los flujos de información estén estrictamente controlados. Esto se traduce en requisitos técnicos relacionados con las inspección de tráfico, el filtrado de comunicaciones y la aplicación de políticas de seguridad entre dominios.

Adicionalmente, IEC 62443 introduce requisitos ilustrados en la figura 5.4.1 relacionados con el control de accesos, incluyendo la autenticación de usuarios y dispositivos, las gestión de privilegios y la restricción de accesos no autorizados. Estos requisitos son especialmente relevantes en entornos OT, donde el acceso indebido a sistemas de control puede generar impactos operativos significativos. (Bureau Veritas, 2026)

Finalmente, la norma contempla requisitos de monitoreo y registro de eventos, orientados a la detección de comportamientos anómalos y a la trazabilidad de incidentes de seguridad. Estos requisitos permiten mejorar la capacidad de respuesta ante incidentes y fortalecer la gestión del riesgo cibernético.

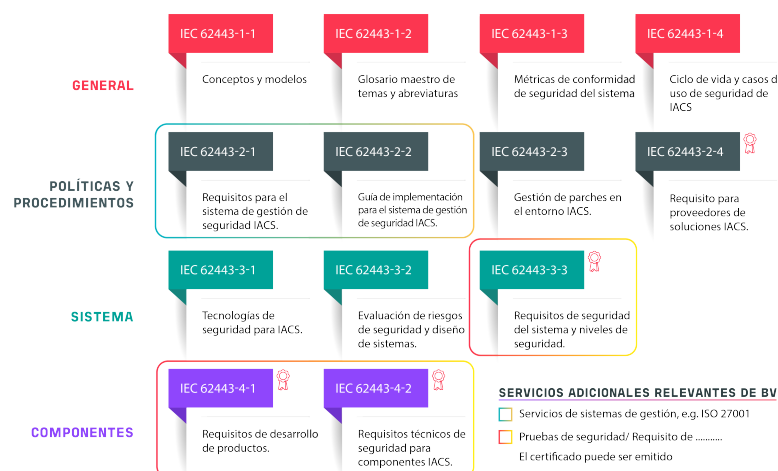


Figura 5.4.1: Infografía-IEC-62443
Fuente: (Bureau Veritas, 2026)

5.4.2. Requisitos técnicos derivados de la norma IEC 62351

La norma IEC 62351 complementa el enfoque arquitectónico de IEC 62443 al definir requisitos específicos para la protección de las comunicaciones en sistemas eléctricos. A partir de esta norma, se derivan requisitos técnicos orientados a garantizar la confidencialidad, integridad y autenticación de la información intercambiada entre los diferentes componentes del sistema.

uno de los principales requisitos establecidos por IEC 62351 es la protección de las comunicaciones mediante mecanismos criptográficos, tales como el uso de TLS en comunicaciones basadas en TCP-IP. Este requisito implica que los dispositivos y sistemas de comunicación deben ser capaces de soportar cifrado robusto sin afectar el desempeño operativo del sistema eléctrico.

Asimismo, la norma ilustrada en la figura 5.4.2 define requisitos de autenticación de dispositivos y sistemas, con el fin de asegurar que únicamente entidades legítimas puedan intercambiar información dentro de la infraestructura. Este aspecto resulta crítico para prevenir ataques de suplantación de identidad y accesos no autorizados a sistemas de control.

Otro requisito relevante es la verificación de la integridad de los mensajes, que permite detectar modificaciones no autorizadas en la información transmitida. En sistemas eléctricos, la integridad de los datos es esencial para garantizar que las decisiones operativas se basen en información confiable.

Finalmente, IEC 62351 introduce requisitos relacionados con la gestión de claves y certificados digitales, los cuales son fundamentales para la implementación efectiva de mecanismos de cifrado y autenticación. La adecuada gestión de estos elementos es un factor clave para la sostenibilidad de la seguridad de las comunicaciones a lo largo del ciclo de vida del sistema.

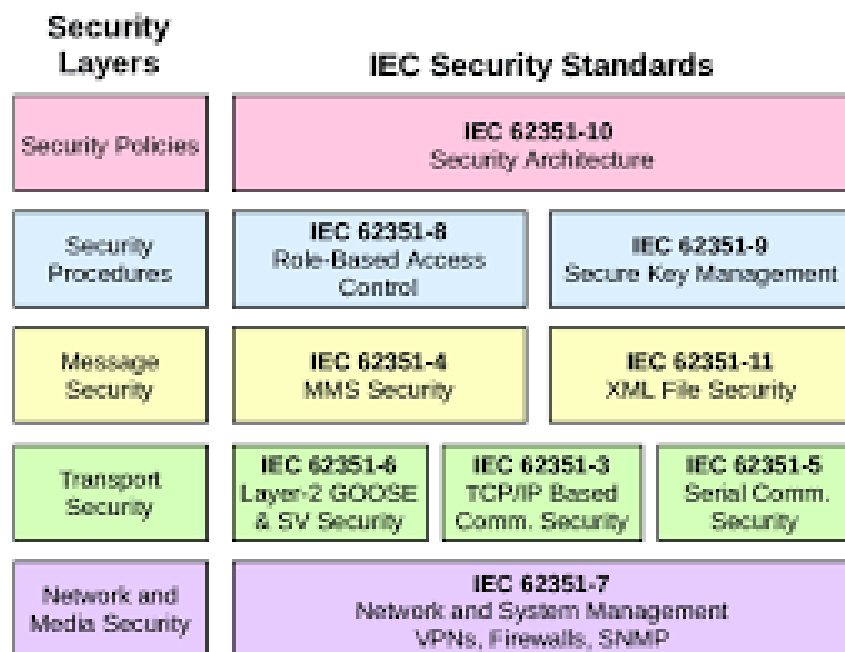


Figura 5.4.2: Infografía-IEC-62351

Fuente: (ResearchGate, 2026c)

La aplicación de la norma IEC 62351 resulta especialmente relevante en protocolos ampliamente utilizados en sistemas eléctricos modernos, tales como IEC 60870-5-104, DNP3 e IEC 61850. Estas tecnologías son empleadas para la supervisión, control y automatización de subestaciones eléctricas y centros de operación. En este contexto, IEC 62351 establece mecanismos de autenticación, cifrado, gestión de certificados y

protección de integridad que permiten mitigar ataques de interceptación, modificación de mensajes y accesos no autorizados. Por esta razón, dentro de los criterios de selección de tecnologías de ciberseguridad se consideró la compatibilidad de los equipos con mecanismos TLS, VPN IPsec, gestión de certificados digitales y funcionalidades de autenticación robusta alineadas con los requerimientos de la norma.

5.4.3. Requisitos técnicos operativos y de continuidad

Además de los requisitos normativos, en el sector energético es necesario considerar requisitos técnicos orientados a la continuidad operativa y a la viabilidad técnica de las soluciones de ciberseguridad. Estos requisitos no siempre están explícitamente definidos en las normas, pero son fundamentales para su correcta aplicación en entornos OT.

Uno de estos requisitos es la alta disponibilidad, que implica que los mecanismos de ciberseguridad no deben introducir puntos únicos de falla ni afectar la operación continua del sistema eléctrico. Las soluciones evaluadas deben ser compatibles con esquemas de redundancia y tolerancia a fallos.

Otro requisito clave se considera de baja latencia y el impacto mínimo en el desempeño, ya que los sistemas de control industrial requieren tiempos de respuesta estrictos. Los mecanismos de seguridad implementados no deben interferir con la operación normal de los procesos. Finalmente, se incluye como requisito la posibilidad de implementación progresiva, de modo que las soluciones de ciberseguridad puedan adoptarse de manera gradual, conforme al ciclo de vida de los equipos y a la planificación estratégica de la organización.

5.4.4. Síntesis de requisitos técnicos de ciberseguridad

La integración de los requisitos derivados de las normas IEC 62443 e IEC 62351, junto con los requisitos operativos y de continuidad, permite definir un conjunto coherente de criterios técnicos que servirán como base para la evaluación comparativa de alternativas de ciberseguridad.

Esta síntesis facilita la traducción de los lineamientos normativos en requisitos evaluables, permitiendo analizar de manera objetiva la capacidad de diferentes equipos y arquitecturas para proteger los activos y flujos de información identificados previamente. Asimismo, establece una conexión directa entre el marco normativo y la matriz de criterios que se desarrollará en el siguiente capítulo.

5.5. Análisis de certificaciones y exigencias normativas aplicables a EBSA

Las normas IEC 62443 e IEC 62351 tienen como objetivo establecer un marco técnico para la protección de sistemas de automatización industrial y de comunicaciones en sistemas eléctricos, respectivamente. Su propósito no es únicamente definir controles técnicos aislados, sino estructurar un modelo integral de ciberseguridad basado en gestión del riesgo, segmentación de arquitectura, protección de comunicaciones y

monitoreo continuo.

En el contexto del sector eléctrico, estas normas buscan garantizar la disponibilidad, integridad y confidencialidad de la información operativa, minimizando el impacto de incidentes cibernéticos sobre la continuidad del servicio.

Desde el punto de vista de certificación, la serie IEC 62443 contempla diferentes niveles de evaluación:

- Certificación de productos (IEC 62443-4-2): exige que los dispositivos cumplan requisitos técnicos como autenticación robusta, control de acceso, registro de eventos, integridad del sistema y protección contra uso indebido.
- Certificación de procesos de desarrollo seguro (IEC 62443-4-1): exige prácticas de desarrollo seguro por parte del fabricante.
- Certificación de integradores de sistemas (IEC 62443-2-4): exige competencia técnica en implementación de soluciones de ciberseguridad industrial.
- Evaluación de programas de seguridad (IEC 62443-2-1): exige la implementación de políticas, gestión de activos, gestión de riesgos, control de cambios y respuesta a incidentes.

Para el caso de EBSA, los criterios más relevantes desde la perspectiva de certificación y cumplimiento normativo incluyen:

- Implementación del modelo de zonas y conductos.
- Segmentación efectiva entre IT y OT.
- Gestión formal de activos OT.
- Control de accesos basado en roles.
- Monitoreo y registro de eventos de seguridad.
- Protección criptográfica de comunicaciones críticas conforme a IEC 62351.
- Gestión de vulnerabilidades y actualización controlada de firmware.

Estos criterios no solo responden a los estándares internacionales, sino que constituyen elementos fundamentales para demostrar madurez en ciberseguridad industrial ante auditorías técnicas o regulatorias.

Las auditorías en empresas del sector eléctrico pueden realizarse mediante evaluaciones internas, auditorías externas especializadas en ciberseguridad industrial o revisiones regulatorias. En el marco de estándares como IEC 62443, las auditorías evalúan aspectos como:

- Existencia de inventario actualizado de activos.
- Evidencia de segmentación de red.

- Políticas formales de control de acceso.
- Registro y trazabilidad de eventos de seguridad.
- Procedimientos de gestión de incidentes.

La evidencia documental y técnica constituye un elemento fundamental para demostrar cumplimiento y madurez organizacional.

5.5.1. Relación entre requisitos normativos y aplicación en EBSA

La siguiente tabla establece una relación directa entre los principales requisitos derivados de las normas IEC 62443 e IEC 62351, la evidencia técnica esperada en un proceso de auditoría y su aplicación en el contexto operativo de EBSA.

Tabla 5.5.1: Relación entre requisitos IEC y aplicación en EBSA

Requisito Normativo	Evidencia Técnica Esperada	Aplicación en EBSA
Segmentación en Zonas y Conductos (IEC 62443)	Diagramas de arquitectura segmentada, reglas de firewall documentadas, separación lógica IT-OT	Implementación de segmentación entre red corporativa y red de subestación mediante firewalls industriales y VLAN
Control de Acceso y Autenticación (IEC 62443-4-2)	Políticas de control de acceso, autenticación basada en roles, registros de acceso	Definición de perfiles de usuario diferenciados para operadores, ingenieros y personal de mantenimiento
Gestión de Activos (IEC 62443-2-1)	Inventario actualizado de dispositivos OT, control de firmware, gestión de cambios	Registro formal de IED, RTU y equipos de red presentes en la subestación tipo analizada
Registro y Monitoreo de Eventos (IEC 62443)	Logs de seguridad, sistemas de monitoreo pasivo, alertas documentadas	Implementación de monitoreo de tráfico OT y exportación de registros hacia sistemas de análisis
Cifrado de Comunicaciones (IEC 62351)	Soporte de TLS, certificados digitales, gestión de claves	Protección de comunicaciones IEC 60870-5-104 mediante mecanismos criptográficos en gateways o firewalls
Alta Disponibilidad y Continuidad	Arquitectura redundante, tolerancia a fallos, pruebas de conmutación	Uso de switches industriales con protocolos de redundancia y alimentación dual

5.6. Evaluación técnica comparativa de tecnologías de ciberseguridad

5.6.1. Enfoque general de la evaluación

Para sostener la objetividad del estudio, la evaluación se realiza por tipo de tecnología (p. ej., switches industriales, firewalls OT, gateways IT-OT), y

posteriormente se analizarán alternativas específicas soportadas por documentación técnica oficial. Las fuentes utilizadas para sustentar las capacidades de cada alternativa corresponderán principalmente a documentación pública por fabricantes y proveedores reconocidos (Fichas técnicas, manuales de referencia y white papers), complementadas con literatura científica y guías técnicas aplicables al sector. Esta restricción metodológica busca garantizar que los resultados del análisis sean verificables y replicables.

Finalmente, los resultados de la evaluación se presentarían a través de tablas comparativas, donde cada alternativa será valorada frente a los criterios definidos en la matriz. Dependiendo del criterio, se empleará una escala cualitativa (Cumple - Parcialmente cumple - No cumple) acompañada de observaciones técnicas justificadas. Esta estrategia permite integrar tanto el cumplimiento normativo como la viabilidad técnica y operativa, generando un insumo sólido para la síntesis de resultados y para la propuesta de arquitectura de referencia desarrollada en el capítulo siguiente.

5.6.2. Clasificación de tecnologías de ciberseguridad analizadas

5.6.2.1. Switches industriales gestionables

Los switches gestionables constituyen un elemento fundamental en la red OT, ya que permiten la interconexión de dispositivos de control y comunicación en ambientes con condiciones operativas exigentes. A diferencia de los switches tradicionales de entorno IT, estos equipos están diseñados para operar rangos amplios de temperatura, son de alta disponibilidad y soporte para protocolos industriales.

Desde la perspectiva de la ciberseguridad, los switches industriales gestionables desempeñan un rol clave en la segmentación de la red, mediante el uso de VLAN, control de tráfico y mecanismos de priorización. Estas capacidades los convierten en componentes relevantes para la implementación de zonas de seguridad conforme al modelo de IEC 62443, especialmente en niveles de acceso y distribución dentro del entorno OT.

5.6.2.2. Firewalls industriales - Firewalls OT

Los firewalls industriales, también conocidos como firewalls OT, están diseñados específicamente para proteger redes de automatización y control industrial. Estos dispositivos permiten controlar y filtrar el tráfico entre diferentes zonas de seguridad, aplicando políticas de acceso acordes con requisitos operativos de los sistemas OT.

A diferencia de los firewalls tradicionales de IT, los firewalls OT incorporan funciones orientadas a entornos industriales, como la inspección de protocolos específicos, el soporte para arquitecturas redundantes y la operación con mínima latencia. En el contexto del presente estudio, estos equipos son considerados elementos centrales para la protección de los conductos de comunicación definidos por IEC 62443.

5.6.2.3. Gateways de seguridad IT-OT

los gateways de seguridad IT-OT actúan como puntos de interconexión controlada entre los entornos corporativos y operativos. Su función principal es permitir el intercambio seguro de información entre dominios con diferentes niveles de criticidad, aplicando controles de seguridad adicionales sobre los flujos de datos.

Estos dispositivos suelen integrar capacidades de filtrado, traducción de protocolos, autenticación y, en algunos casos, cifrado de comunicaciones. Su evaluación resulta especialmente relevante en escenarios de convergencia IT-OT, donde los flujos de información atraviesan múltiples dominios y requieren controles específicos para evitar la propagación de incidentes desde el entorno IT hacia el entorno OT.

5.6.2.4. Dispositivos de cifrado y protección de comunicaciones

Los dispositivos de cifrado y protección de comunicaciones están orientados a garantizar la confidencialidad, integridad y autenticación de los datos transmitidos entre sistemas eléctricos. Estos equipos pueden operar como dispositivos dedicados o como funcionalidades integradas en otros elementos de red, y su evaluación se fundamenta principalmente en los requisitos establecidos por la norma IEC 62351.

En el contexto del sector energético, estos dispositivos resultan especialmente relevantes para la protección de enlaces de comunicación críticos, como aquellos que conectan centros de control, subestaciones y sistemas de tele-control. Su correcta selección permite mitigar riesgos asociados a la interpretación y manipulación de información sensible.

5.6.2.5. Sistemas de monitoreo y detección para entornos OT

Los sistemas de monitoreo y detección para entornos OT permiten obtener visibilidad sobre el comportamiento de la red y de los dispositivos industriales, facilitando la detección temprana de eventos anómalos o potenciales incidentes de ciberseguridad. Estos sistemas suelen operar de manera pasiva, con el fin de no interferir con los procesos operativos.

Desde el punto de vista el estudio comparativo, estos sistemas se consideran complementarios a los mecanismos de protección perimetral y de segmentación, ya que fortalecen la capacidad de respuesta ante incidentes y contribuyen a la gestión del riesgo cibernético. Su evaluación se enfoca en la capacidad de monitoreo, generación de alertas y compatibilidad con entornos OT.

5.6.3. Análisis comparativo por tipo de tecnología

5.6.3.1. Evaluación comparativa de Switches industriales gestionables

Previo al análisis individual de los switches industriales seleccionados, se establece un conjunto de parámetros técnicos que permiten realizar una comparación objetiva entre las alternativas evaluadas. Estos parámetros no fueron definidos de manera arbitraria, sino que responden a criterios de ingeniería aplicados al contexto de subestaciones eléctricas y a los lineamientos establecidos en la norma IEC 62443 en

materia de segmentación y disponibilidad.

Los criterios técnicos considerados incluyen el tipo de dispositivo (L2/L3), el rango de alimentación, los mecanismos de gestión, las capacidades de segmentación, los protocolos de redundancia y la aplicación típica dentro de una arquitectura IT/OT. La selección de estos parámetros se fundamenta en su relevancia para garantizar la disponibilidad operativa, la resiliencia de la red y la implementación efectiva del modelo de zonas y conductos.

En el contexto de una subestación eléctrica, aspectos como el rango de alimentación y la tolerancia ambiental resultan críticos debido a las condiciones propias del entorno industrial. De igual manera, las capacidades de segmentación mediante VLAN y control de tráfico son esenciales para cumplir con los principios de defensa en profundidad definidos en IEC 62443.

Por otra parte, los mecanismos de redundancia adquieren especial importancia en sistemas de protección y control, donde la interrupción de comunicaciones puede impactar directamente la continuidad del servicio eléctrico.

En la Tabla 5.6.1 se presenta la comparación técnica de los switches industriales evaluados, con el propósito de identificar las características funcionales y operativas que inciden en su adecuación dentro de una arquitectura de ciberseguridad para EBSA.

Tabla 5.6.1: Comparación técnica de switches industriales evaluados

Parámetro	RUGGEDCOM RST2228	Hirschmann RSP25	Cisco IE 4000
Tipo	Switch industrial L2	Switch industrial L2/L3	Switch industrial L2/L3
Alimentación	88–300 VDC / 85–264 VAC	60–250 VDC / 110–230 VAC	9.6–60 VDC
Gestión	CLI (ROS), gestión central	CLI / Web / SNMP	CLI (IOS), consola
Segmentación	VLAN, control por puerto	VLAN, control avanzado	VLAN, políticas
Redundancia	Protocolos industriales	PRP / HSR (IEC 62439)	Redundancia básica
Aplicación típica	Subestaciones	Subestaciones IEC 61850	IT/OT convergente

■ Switch 1: Siemens RUGGEDCOM RST2228

El RUGGEDCOM RST2228 es un switch industrial gestionable de capa 2, diseñado específicamente para aplicaciones críticas en subestaciones y redes eléctricas. Su diseño está orientado a ambientes de alta exigencia operativa, lo que lo hace especialmente adecuado para el sector energético.

Desde el punto de vista técnico, este equipo destaca por su amplio rango de alimentación, que permite operar directamente con tensiones típicas de subestación, y por el uso del sistema operativo Rugged Operating System (ROS), el cual ofrece administración segura mediante interfaz de línea de comandos CLI y herramientas de gestión centralizada. Estas características facilitan su integración

en arquitecturas segmentadas conforme a la IEC 62443, evidenciado en la figura 5.6.1

El RST2228 ha sido reportado en aplicaciones de subestaciones eléctricas bajo arquitecturas de la IEC 61850, donde se emplea para conformar redes de comunicación resilientes que soportan tráfico crítico de protección y control, lo que evidencia su madurez tecnológica y adecuación en el sector.(Siemens, 2026a)



Figura 5.6.1: Switch 1: Siemens RUGGEDCOM RST2228
Fuente: (Siemens, 2026a)

Justificación de uso de empresa de energía:

Se prioriza este switch cuando el entorno presenta alimentación AC-DC de alta tensión, condiciones ambientales severas y necesidades de alta confiabilidad, siendo la segmentación de red el principal mecanismo de ciberseguridad a nivel de acceso y distribución OT.

■ Hirschmann RSP25 (familia RSP)

La familia Hirschmann RSP corresponde a switches industriales gestionables ampliamente utilizados en redes eléctricas, especialmente en arquitecturas basadas en IEC 61850. El modelo RSP25 representa esta familia y se caracteriza por su enfoque en alta disponibilidad y comunicaciones sin interrupción.

Un aspecto diferenciador de estos switches es su soporte para protocolos de redundancia PRP y HSR (IEC 62439), los cuales permiten comunicaciones determinísticas y tolerantes a fallos, requisitos crítico en redes de protección y control. Desde la perspectiva de ciberseguridad, estas capacidades refuerzan el principio de disponibilidad definido en IEC 62443, evidenciado en la figura 5.6.2

La alimentación redundante y el bajo consumo energético los hacen adecuados para instalaciones distribuidas, mientras que sus capacidades de segmentación y

gestión permiten su uso dentro de zonas OT con diferentes niveles de criticidad.



Figura 5.6.2: Switch 2: Hirschmann RSP25
Fuente: (Belden Inc., 2026)

Justificación de uso de empresa de energía:

Este tipo de Switch es priorizado en subestaciones digitales y redes donde la continuidad del tráfico es crítica, incluso ante fallas de enlace, siendo especialmente relevante cuando la arquitectura OT exige redundancia sin tiempos de recuperación.

■ **Switch 3: Cisco Industrial Ethernet IE 4000**

El Cisco IE 4000 es un switch industrial diseñado para entornos de automatización y convergencia IT-OT. Su arquitectura combina robustez industrial con capacidades de gestión alineadas al ecosistema de redes corporativas, lo que hace adecuado para escenarios donde la integración IT y OT es más estrecha.

Este equipo opera con alimentación DC típica de entornos industriales y ofrece administración mediante interfaces de consola y CLI, permitiendo una gestión consistente con prácticas IT. Aunque no está orientado específicamente a subestaciones de alta tensión, su fortaleza radica en la estandarización operativa y en su facilidad de integración con sistemas de gestión de red existentes, determinado en la figura 5.6.3.

Desde la óptica de IEC 62443, el IE 4000 aporta capacidades de segmentación y control que resultan útiles en zonas intermedias IT-OT, donde se requiere una separación lógica robusta sin sacrificar la interoperabilidad.



Figura 5.6.3: Switch 3: Cisco Industrial Ethernet IE 4000
Fuente: (Cisco Systems, 2026; Sin fecha, 2026)

Justificación de uso de empresa de energía:

Se prioriza en escenarios de convergencia IT-OT, redes de telecontrol o infraestructura WAN industrial, donde la alineación con arquitecturas corporativas y la gestión centralizada son factores determinantes.

Un caso reportado en la literatura técnica del sector eléctrico describe la implementación de una red de subestación IEC 61850 basada en switches industriales RUGGEDCOM, configurados en topología redundante para garantizar comunicaciones confiables entre dispositivos de protección y control. Este tipo de aplicación demuestra que dichas tecnologías no solo cumplen con requisitos normativos, sino que han sido validadas en entornos operativos reales del sector energético.

En el análisis técnico indexado en la tabla 5.6.1, se evidencia que no solo existe un único switch óptimo para todos los escenarios, sino que la selección depende de la arquitectura y del entorno operativo:

- **Arquitectura OT crítica:** RUGGEDCOM RST2228 o Hirschmann RSP.

- **Alta disponibilidad sin interrupción:** Hirschmann RSP (PRP-HSR).
- **Convergencia IT-OT y gestión corporativa:** Cisco IE 4000.

Esta conclusión refuerza la necesidad de un estudio técnico comparativo, en el cual la arquitectura y la segmentación, priorizadas por la IEC 62443, se convierten en el criterio dominante para la selección de switches industriales en empresas de energía.

Tabla 5.6.2: Evaluación cualitativa de switches industriales según la matriz de criterios

Criterio	RST2228	RSP25	IE 4000
Alineación IEC 62443	C	C	CP
Segmentación de red	C	C	C
Cifrado	NC	NC	NC
Registro de eventos	CP	CP	CP
Alta disponibilidad	C	C	CP
Implementación progresiva	C	C	C

Los resultados en la tabla 5.6.2 evidencian la evaluación cualitativa que los switches industriales cumplen principalmente con criterios de arquitectura y operación, lo cual es coherente con su rol dentro de una arquitectura de ciberseguridad basada en IEC 62443. El criterio de cifrado presenta un nivel de no cumplimiento en todos los casos evaluados, dado que esta funcionalidad no corresponde al alcance típico de este tipo de dispositivos, sino a tecnologías complementarias como firewalls industriales o gateways de seguridad. Para un análisis detallado de los resultados, consúltase el ***Anexo 2***.

5.6.3.2. Evaluación comparativa de Firewalls industriales

Antes de realizar la evaluación cualitativa de los firewalls industriales mediante la matriz de criterios, se procede a establecer una comparación técnica preliminar basada en parámetros funcionales y operativos relevantes para entornos de subestaciones eléctricas.

Los criterios seleccionados no obedecen a consideraciones comerciales, sino a principios de ingeniería aplicados a arquitecturas OT y a los lineamientos establecidos en la norma IEC 62443, particularmente en lo referente a la definición y protección de conductos de comunicación entre zonas de seguridad.

Entre los parámetros considerados se encuentran el tipo de firewall (orientación OT o convergente IT/OT), el rango de alimentación industrial, los mecanismos de gestión, las capacidades de segmentación y control de tráfico, los esquemas de redundancia y su aplicación típica dentro de arquitecturas industriales. Estos factores resultan determinantes para evaluar la idoneidad de un firewall en contextos donde la disponibilidad, la baja latencia y la confiabilidad operativa son prioritarias.

En entornos de subestación, el firewall constituye el elemento central para la implementación de conductos protegidos conforme al modelo de zonas y conductos definido por IEC 62443. Por ello, la capacidad de segmentación, control granular de tráfico y soporte para alta disponibilidad adquieren especial relevancia técnica.

En la Tabla 5.6.3 se presenta la comparación técnica de los firewalls industriales evaluados, con el objetivo de identificar sus características funcionales y su orientación dentro de arquitecturas OT puras o entornos de convergencia IT/OT.

Tabla 5.6.3: Comparación técnica de firewalls industriales evaluados

Parámetro	Siemens SCALANCE S615	Hirschmann EAGLE	FortiGate Rugged
Tipo	Firewall industrial OT	Firewall industrial OT	Firewall industrial IT/OT
Alimentación	Industrial AC/DC	Industrial AC/DC	Industrial DC
Gestión	CLI / Web (industrial)	CLI / Web (industrial)	CLI / Web / gestión central
Segmentación	Control de conductos IEC 62443	Segmentación perimetral OT	Segmentación granular IT/OT
Redundancia	Alta disponibilidad OT	Alta disponibilidad OT	Alta disponibilidad según modelo
Aplicación típica	Subestaciones y redes OT	Perímetro OT / zonas críticas	IT/OT convergente

■ Firewall 1: Siemens SCALANCE S615

El SCALANCE S615 es un firewall industrial diseñado específicamente para la protección de redes OT y subestaciones eléctricas. Este equipo está orientado a la implementación de zonas y conductos conforme a IEC 62443, permitiendo el control del tráfico entre segmentos con diferentes niveles de criticidad, evidenciado en la figura 5.6.4.

Desde el punto de vista técnico, el SCALANCE S615 soporta funciones de firewall industrial, segmentación de red y administración segura, manteniendo un enfoque conservador en términos de inspección para no afectar la latencia de procesos críticos. Su diseño industrial y compatibilidad con entornos eléctricos lo convierten en una solución adecuada para aplicaciones OT pura.



Figura 5.6.4: Siemens SCALANCE S615
Fuente: (Siemens, 2026a)

Justificación de uso de empresa de energía:

Se prioriza en subestaciones y redes OT donde el objetivo principal es controlar estrictamente los flujos entre zonas, sin introducir complejidad excesiva ni impacto en la operación.

■ **Firewall 2: Hirschmann EAGLE40/EAGLE One**

Los firewalls industriales Hirschmann EAGLE están diseñados para la segmentación y protección de redes industriales críticas. Estos dispositivos ofrecen capacidades de firewall, NAT y control de tráfico, con un enfoque orientado a la seguridad perimetral OT, determinado en la figura 5.6.5.

Su arquitectura permite la implementación de políticas de acceso entre zonas de seguridad y su integración con redes industriales existentes. Estos equipos son comúnmente utilizados en entornos de automatización industrial y energía, donde la robustez y la confiabilidad son requisitos clave.



Figura 5.6.5: Hirschmann EAGLE40/EAGLE One
Fuente: (Belden Inc., 2026)

Justificación de uso de empresa de energía:

Adecuados para entornos OT donde se requiere una protección perimetral clara entre segmentos, con un balance entre seguridad y simplicidad operativa.

■ Firewall 3: Fortinet FortiGate Rugged(FortiGateR)

Los FortiGate Rugged representan una familia de firewalls industriales que incorporan capacidades avanzadas de seguridad, incluyendo inspección profunda y soporte de cifrado. A diferencia de firewalls OT más conservadores, estos dispositivos ofrecen un enfoque más cercano al mundo IT, adaptado a condiciones industriales, evidenciado en la figura 5.6.6.

Estos equipos permiten implementar políticas de seguridad complejas y protección de comunicaciones cifradas, siendo especialmente útiles en escenarios de convergencia IT/OT o interconexión con redes corporativas.



Figura 5.6.6: Firewall 3: Fortinet FortiGate Rugged(FortiGateR)
Fuente: (Fortinet, 2026)

Justificación de uso de empresa de energía:

Se prioriza en escenarios donde existen interacción frecuente entre IT y OT, y donde se requiere mayor visibilidad y control avanzado de tráfico.

En el análisis técnico evidenciado en la tabla 5.6.3, se observa que los firewalls industriales evaluados presentan enfoques diferenciados según el entorno de aplicación. Mientras que soluciones como SCALANCE S615 y Hirschmann EAGLE están orientadas principalmente a la protección de zonas y conductos en entornos OT críticos, alternativas como FortiGate Rugged ofrecen mayores capacidades para escenarios de convergencia IT/OT.

En consecuencia, no existe un firewall óptimo universal, sino que su selección depende de la arquitectura de red y del grado de integración entre los entornos IT y OT.

Tabla 5.6.4: Evaluación cualitativa de firewalls industriales según la matriz de criterios

Criterio	SCALANCE S615	EAGLE	FortiGate Rugged
Alineación IEC 62443	C	C	CP
Segmentación de red	C	C	C
Cifrado	CP	CP	C
Registro de eventos	CP	CP	C
Alta disponibilidad	C	C	CP
Implementación progresiva	C	C	C

En la tabla 5.6.4 se evidencia la evaluación cualitativa evidencia que los firewalls industriales cumplen un rol central en la protección de los conductos definidos por IEC 62443. Mientras que soluciones OT puras como SCALANCE y EAGLE priorizan la segmentación y la disponibilidad, plataformas como FortiGate Rugged aportan capacidades adicionales de cifrado y registro de eventos, siendo más adecuadas para escenarios de convergencia IT/OT. Para un análisis detallado de los resultados, consúltese el *Anejo 3*.

5.6.3.3. Evaluación comparativa de Gateways IT/OT

Previo a la evaluación cualitativa de los gateways IT/OT mediante la matriz de criterios, se realiza una comparación técnica preliminar orientada a identificar las capacidades funcionales que inciden directamente en la protección de los flujos de información entre dominios con diferente nivel de criticidad.

La selección de los parámetros evaluados no responde a criterios comerciales, sino a fundamentos de ingeniería de redes industriales y a los lineamientos establecidos en las normas IEC 62443 e IEC 62351. En el contexto de una subestación de distribución integrada a un centro de control, el gateway constituye el punto estratégico donde convergen los entornos IT y OT, por lo que su adecuada caracterización resulta determinante para la seguridad global de la arquitectura.

Entre los parámetros considerados se incluyen el tipo de dispositivo (orientación OT pura o convergente IT/OT), el rango de alimentación industrial, los mecanismos de gestión, las capacidades de segmentación y control de conductos, los esquemas de redundancia y la aplicación típica dentro de arquitecturas industriales. Estos aspectos permiten evaluar si el dispositivo puede implementar controles adecuados sobre los flujos que atraviesan la frontera IT-OT.

Desde la perspectiva de IEC 62443, el gateway debe garantizar la protección de los conductos definidos entre zonas de seguridad. Complementariamente, desde el enfoque de IEC 62351, debe permitir la implementación de mecanismos de cifrado, autenticación y control de integridad en las comunicaciones basadas en TCP/IP, como las utilizadas

en protocolos de telecontrol.

En la Tabla 5.6.5 se presenta la comparación técnica de los gateways IT/OT evaluados, con el propósito de identificar su orientación arquitectónica y su adecuación para la interconexión segura entre la subestación y el entorno corporativo de EBSA.

Tabla 5.6.5: Comparación técnica de gateways IT/OT evaluados

Parámetro	SCALANCE M876	Hirschmann EAGLE One	FortiGate Rugged
Tipo	Gateway industrial IT/OT	Gateway / Firewall OT	Gateway industrial IT/OT
Alimentación	Industrial AC/DC	Industrial AC/DC	Industrial DC
Gestión	CLI / Web (industrial)	CLI / Web (industrial)	CLI / Web / gestión central
Segmentación	Control de conductos IEC 62443	Segmentación OT perimetral	Segmentación granular IT/OT
Redundancia	Alta disponibilidad industrial	Alta disponibilidad OT	Alta disponibilidad según modelo
Aplicación típica	Enlace OT-IT seguro	Zona intermedia OT	Convergencia IT/OT

■ Gateway 1: Siemens SCALANCE M876

El SCALANCE M876 es una gateway industrial orientado a la interconexión segura de redes OT con redes externas o corporativas. Incorpora funciones de firewall industrial y soporte de comunicaciones seguras, manteniendo un enfoque conservador en términos de latencia y estabilidad operativa, determinado en la figura 5.6.7.



Figura 5.6.7: Gateway 1: Siemens SCALANCE M876
Fuente: (Siemens, 2026b; Sin fecha, 2026)

Justificación de uso de empresa de energía:

Adecuado para enlaces OT-IT controlados, subestaciones y redes de campo donde se requiere comunicación segura sin introducir complejidad excesiva.

■ **Gateway 2: Hirschmann EAGLE One**

El Hirschmann EAGLE One combina funciones de gateway industrial y firewall OT, permitiendo la segmentación y el control de tráfico entre dominios. Su diseño está orientado a redes industriales críticas, priorizando disponibilidad y simplicidad operativas, determinado en la figura 5.6.8.



Figura 5.6.8: Gateway 2: Hirschmann EAGLE One
Fuente: (Belden Inc., 2026)

Justificación de uso de empresa de energía:

Apropiado para zonas intermedias IT/OT, donde se requiere protección perimetral y control de flujos con mínima intervención operativa.

■ **Gateway 3: Fortinet FortiGate Rugged (Modo Gateway)**

Los FortiGate Rugged, además de operar firewalls, pueden configurarse como gateways IT/OT, integrando capacidades avanzadas de inspección, cifrado y control de tráfico. Su enfoque es más flexible y cercano al mundo IT, adaptado a condiciones industriales, el cual se puede determinar en la figura 5.6.9.



Figura 5.6.9: Gateway 3: Fortinet FortiGate Rugged Modo Gateway
Fuente: (Belden Inc., 2026)

Justificación de uso de empresa de energía:

Recomendado para escenarios de convergencia IT/OT, accesos remoto seguro y enlaces con centros de control corporativos.

El análisis cualitativo en la tabla 5.6.5 muestra que los gateways IT/OT cumplen un rol fundamental en la protección de los flujos de información entre dominios con diferentes niveles de criticidad. Soluciones orientadas a OT, como SCALANCE M876 y EAGLE One, priorizan la disponibilidad y el control básico de conductos, mientras que plataformas como FortiGate Rugged ofrecen capacidades adicionales de cifrado y monitoreo, siendo más adecuadas para escenarios de convergencia IT/OT.

Tabla 5.6.6: Evaluación cualitativa de gateways IT/OT según la matriz de criterios

Criterio	SCALANCE M876	EAGLE One	FortiGate Rugged
Alineación IEC 62443	C	C	CP
Segmentación de red	C	C	C
Cifrado	CP	CP	C
Registro de eventos	CP	CP	C
Alta disponibilidad	C	C	CP
Implementación progresiva	C	C	C

Es importante señalar que la evaluación comparativa determinada en la tabla 5.6.6 se basa en documentación técnica pública de los fabricantes, sin acceso a configuraciones reales implementadas en EBSA. No obstante, el análisis permite establecer una base objetiva para la selección de tecnologías alineadas con los estándares internacionales aplicables. Para un análisis detallado de los resultados, consúltese el ***Anexo 4***.

Capítulo 6

Resultados

6.1. Conversión del análisis cualitativo a cuantitativo

En esta sección se presentan los resultados derivados de la conversión del análisis cualitativo de las tecnologías evaluadas hacia un análisis cuantitativo, con el fin de facilitar la comparación objetiva entre alternativas. Inicialmente, cada tecnología fue evaluada mediante la matriz cualitativa basada en los criterios definidos (Cumple, Cumple Parcialmente y No Cumple), en coherencia con los lineamientos normativos y operativos establecidos en el estudio.

Posteriormente, los resultados cualitativos fueron transformados en valores numéricos mediante una escala de conversión previamente definida, asignando un puntaje unitario a los criterios que cumplen, un puntaje intermedio a los que cumplen parcialmente y un valor nulo a aquellos que no cumplen. Esta conversión permitió ponderar cada criterio según su nivel de importancia dentro del sector energético y obtener un puntaje total representativo para cada tecnología analizada.

Los resultados cuantitativos se representan mediante gráficos, como el ilustrado en la figura correspondiente, donde se visualiza la contribución de cada criterio al puntaje total obtenido. Este tipo de representación gráfica permite identificar de manera clara cuáles criterios aportan mayor peso al resultado final y evidencia que aspectos como la segmentación de red, la alta disponibilidad y la alineación con la norma IEC 62443 concentran la mayor proporción del puntaje, reafirmando su relevancia en la selección de tecnologías de ciberseguridad para entornos IT/OT.

En conjunto, este enfoque facilita la interpretación de los resultados, permitiendo comparar distintas tecnologías bajo una misma base metodológica y sirviendo como fundamento para el análisis de escenarios de implementación y simulación que se presentan en las secciones posteriores.

6.2. Resultados por tipo de tecnología

Cálculo SCALANCE S615			
Criterio	Peso	Valor	Resultado
Segmentación	30	C (1)	30
Alta disponibilidad	25	C (1)	25
IEC 62443	20	C (1)	20
Cifrado	10	CP (0.5)	5
Logs	10	CP (0.5)	5
Implementación	5	C (1)	5
Total			90
Total ideal			100

Figura 6.2.1: Ejemplo Matriz con ponderaciones (Cuantitativo)

Fuente: (Elaboración propia, 2026)

Con el fin de fortalecer el análisis comparativo, se asignaron ponderaciones a cada criterio de evaluación, como se muestra en la figura 6.2.1, en función de su impacto en la seguridad de entornos IT/OT. Esta ponderación que se muestra es un ejemplo claro de los varios realizados, que permite priorizar aspectos críticos como el cumplimiento normativo y la segmentación de red, alineados con los principios de la norma IEC 62443. Para un análisis detallado de los resultados, consúltese el *Anexo 2*, *Anexo 3 y Anexo 4*.

6.2.1. Resultados del análisis cuantitativo de switches industriales

Con el fin de facilitar la interpretación de los resultados obtenidos mediante la matriz ponderada, se consolidan los puntajes finales de los switches industriales evaluados en una única representación gráfica comparativa. Esta gráfica permite visualizar de manera directa el desempeño relativo de cada alternativa bajo los mismos criterios y ponderación previamente definidos.

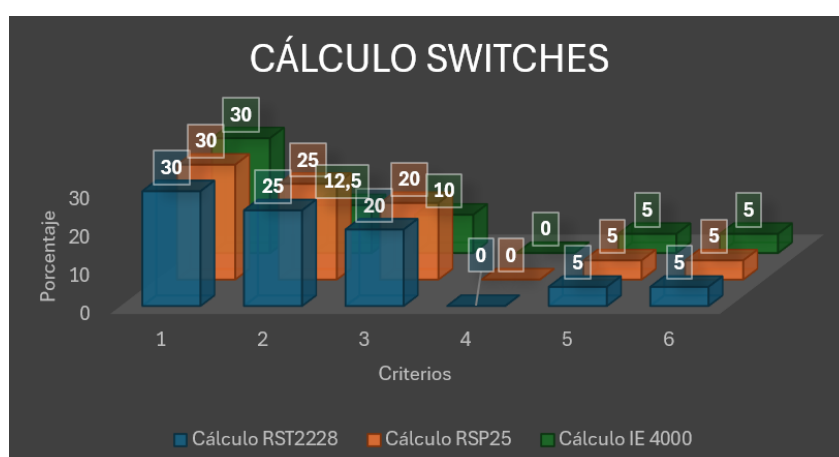


Figura 6.2.2: Calculo Swiches Cuantitativo

Fuente: (Elaboración propia, 2026)

Como se observa en la figura 6.2.2, los switches SCALANCE S615 y Hirschmann RSP25 presentan un porcentaje más alto dentro del análisis, tomando valores de un

85 %, lo cual evidencia una fuerte alineación con los criterios priorizados para el sector energetico, especialmente en aspectos relacionados son segmentación de red, alta disponibilidad y cumplimiento de IEC 62443.

Por su parte, el Cisco IE 4000 presenta un puntaje inferior en comparación con las soluciones orientadas estrictamente a entornos OT, aunque mantiene un desempeño adecuado dentro del rango evaluado. Esta diferencia se debe principalmente a su enfoque hacia escenarios con convergencia IT-OT, donde la integración con redes corporativas adquiere mayor relevancia que los requerimientos estrictos de subestación eléctrica.

La comparación global permite concluir que, desde una perspectiva cuantitativa, las tecnologías diseñadas específicamente para entornos industriales críticos obtienen mejores resultados cuando los criterios de arquitectura y disponibilidad tienen mayor ponderación. No obstante, la elección final dependerá del ambiente de implementación que la empresa EBSA determine como prioritario, ya sea un entorno OT crítico, un entorno OT estructurado o un entorno de convergencia IT-OT. Esta representación consolidada refuerza la validez del método aplicado, al demostrar de manera clara y objetiva las diferentes técnicas entre las alternativas evaluadas bajo una misma base metodológica.

6.2.2. Resultados del análisis cuantitativo de firewalls industriales

Con el propósito de consolidar los resultados obtenidos mediante la matriz ponderada, se presenta una representación gráfica comparativa de los firewalls industriales evaluados. Esta gráfica integra los puntajes finales obtenidos por cada alternativa bajo los mismos criterios y ponderaciones definidos previamente, permitiendo una visualización clara del desempeño relativo de cada tecnología.

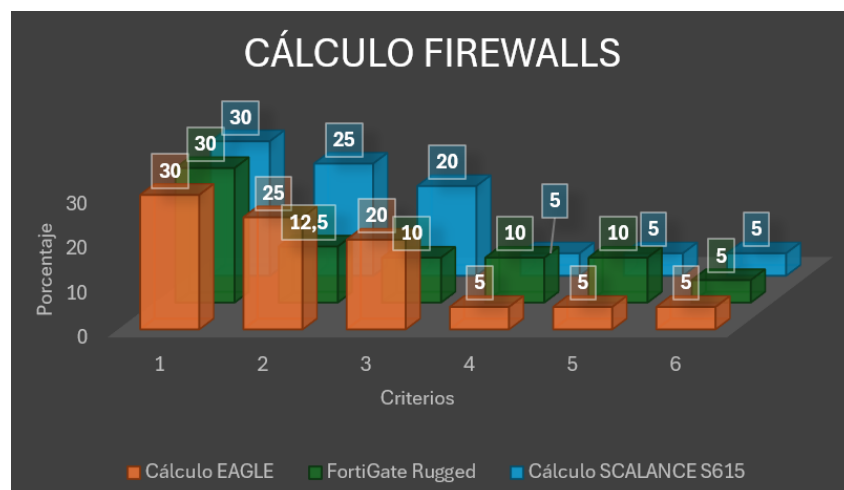


Figura 6.2.3: Calculo Firewalls Cuantitativo
Fuente: (Elaboración propia, 2026)

Los resultados en la figura 6.2.3 muestran que los firewalls orientados específicamente a entornos OT, como SCALANCE S615 y Hirschmann EAGLE,

alcanzan puntajes superiores dentro del análisis, evidenciando una fuerte alineación con los criterios de mayor peso, particularmente en segmentación de red, alta disponibilidad y cumplimiento de IEC 62443. Estos dispositivos están diseñados para operar en infraestructuras críticas, priorizando estabilidad y control de conductos por encima de funciones avanzadas de inspección.

Por su parte, la solución FortiGate Rugged presenta un desempeño competitivo, especialmente en criterios asociados a cifrado y registro de eventos, lo cual refleja su enfoque hacia escenarios de convergencia IT-OT. Sin embargo, al aplicarse una ponderación donde arquitectura y disponibilidad tienen mayor peso (Como es en el caso del sector energético), las soluciones OT puras mantienen una ligera ventaja en el puntaje total.

La gráfica comparativa figura 6.2.3 permite evidenciar que la selección de firewall no depende únicamente del puntaje final, sino del ambiente operativo donde será implementado. En entornos OT críticos, se priorizan soluciones con alta estabilidad y alineación estricta con IEC 62443, mientras que en escenarios de integración IT-OT pueden resultar más convenientes plataformas con mayores capacidades de inspección y cifrado. Esta consolidación gráfica reafirma la coherencia del método aplicado, demostrando que la ponderación de criterios influye directamente en la posición relativa de cada tecnología y validando la necesidad de contextualizar la selección en función del entorno especificado de la empresa EBSA.

6.2.3. Resultados del análisis cuantitativo de Gateways

La siguiente gráfica integra los puntajes finales obtenidos por cada alternativa bajo los mismos criterios y ponderaciones definidos previamente, permitiendo una visualización clara del desempeño relativo de cada tecnología dentro del estudio.

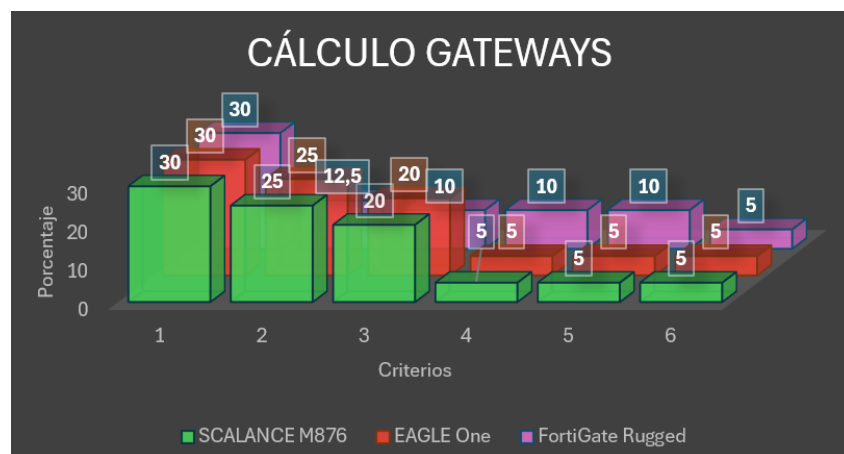


Figura 6.2.4: Calculo Gateways Cuantitativo

Fuente: (Elaboración propia, 2026)

Los resultados en la figura 6.2.4 evidencian que las soluciones orientadas específicamente a entornos industriales, como SCALANCE M676 y Hirschmann EAGLE One, mantienen un desempeño sólido en los criterios de mayor ponderación,

particularmente en segmentación de red, alta disponibilidad y alineación con la norma IEC 62443. Estas características los posicionan como las alternativas adecuadas para la protección de conductos entre zonas OT y para la implementación de arquitecturas industriales estructuradas.

Por su parte, la solución FortiGate Rugged, aunque presenta un puntaje competitivo, destaca principalmente en criterios asociados a cifrado y registro de eventos, lo cual refleja su orientación hacia escenarios de convergencia IT-OT. No obstante, al aplicarse una ponderación donde la arquitectura y la disponibilidad operativa tiene mayor pesos (Como ocurre en el sector energético) las soluciones de enfoque OT puro muestra una ligera ventaja en el resultado global. La representación gráfica permite concluir que la selección del gateway IT-OT debe realizarse en función del ambiente de implementación definido por la empresa EBSA, ya que el desempeño relativo de cada tecnología esta directamente influenciado por la ponderación de los criterios y por el contexto operativo donde se aplique.

6.3. Resultados con ayuda de simulación (GNS3)

Con el propósito de validar técnicamente la efectividad del modelo de segmentación propuesto, se implementó un entorno de simulación controlado en la plataforma GNS3 evidenciado en la figura 6.3.1, el cual permitió reproducir un escenario representativo de infraestructura IT/OT con ayuda de equipos similares a los del estudio realizado. La arquitectura experimental estuvo compuesta por un router en la zona IT, un firewall perimetral (pfSense), un router en la zona OT y un servidor interno que simuló un activo crítico operacional.

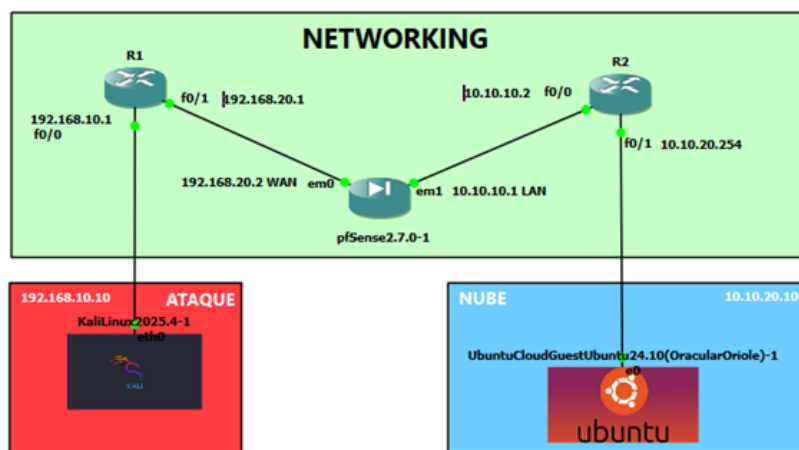


Figura 6.3.1: Arquitectura del escenario OT crítico basada en zonas (IT/OT) y conductos (Firewall).

Fuente: (Elaboración propia, 2026)

El objetivo principal de la simulación fue evaluar el comportamiento del sistema ante intentos de acceso no autorizado desde la zona IT hacia la red OT, comparando dos escenarios: uno sin políticas restrictivas activas y otro con segmentación

implementada conforme a los principios de la norma IEC 62443, específicamente en lo referente a zonas y conductos.

La validación experimental se desarrolló mediante el entorno de simulación GNS3, implementando una arquitectura IT/OT segmentada conforme a los principios de zonas y conductos establecidos por la norma IEC 62443. Debido a la extensión de los procedimientos de configuración, comandos ejecutados, evidencias de captura y registros generados durante las pruebas, la documentación técnica completa se presenta en el ***Anexo 5: Guía Experimental de Configuración y Validación de Seguridad IT/OT en GNS3.***

Dicho anexo incluye la topología detallada utilizada, configuración individual de los dispositivos (Kali Linux, Router Cisco 3725, pfSense y servidor Ubuntu), reglas aplicadas en el firewall, comandos de validación, ejecución de ataques de reconocimiento, fuerza bruta y escaneo avanzado, así como las evidencias experimentales obtenidas y el análisis de los resultados.

6.3.1. Escenario sin segmentación restrictiva

En una primera fase, se deshabilitaron temporalmente las políticas de filtrado en el firewall con el fin de observar el comportamiento de la infraestructura ante un intento de reconocimiento de servicios desde la zona IT. Para ello, se empleó la herramienta Nmap desde el equipo ubicado en la red IT, ejecutando un escaneo de puertos hacia el servidor OT, para determinar como se realizo remitirse al ***Anexo 5.***

Los resultados evidenciaron que los servicios expuestos en la red OT eran detectables y accesibles desde la zona IT, lo cual confirma que, en ausencia de mecanismos de control, la red operacional puede quedar expuesta a actividades de reconocimiento, etapa inicial en la mayoría de los ataques cibernéticos dirigidos a infraestructuras críticas.

Esta condición representa un riesgo significativo, dado que permite identificar servicios activos, versiones de software y posibles vectores de explotación como se muestra en la figura 6.3.2.

```
L$ nmap -Pn -sS -p 22,80,443 192.168.20.2
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-16 22:44 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or
specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.20.2
Host is up (0.062s latency).

PORT      STATE SERVICE
22/tcp    filtered ssh
80/tcp    open  http
443/tcp    open  https

Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds

(kali@kali)-[~]
$ nmap -Pn -sS -p 22,80,443 192.168.20.2
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-16 22:44 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or
specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.20.2
Host is up.

PORT      STATE SERVICE
22/tcp    filtered ssh
80/tcp    filtered http
443/tcp    filtered https
```

Figura 6.3.2: Resultado del escaneo de puertos desde la zona IT hacia la red OT con y sin políticas de segmentación activas.

Fuente: (Elaboración propia, 2026)

6.3.2. Escenario con segmentación conforme a IEC 62443

Posteriormente, se activó una política de bloqueo explícita en el firewall, restringiendo el tráfico proveniente de la red IT hacia la red OT. Esta regla fue configurada bajo el principio de denegación por defecto (deny by default), permitiendo únicamente comunicaciones previamente autorizadas.

Tras aplicar la política, se repitió el mismo procedimiento de escaneo desde la zona IT. En esta ocasión, los resultados mostraron que los puertos previamente detectados aparecieron como filtrados o inaccesibles, evidenciando que el firewall interceptó y descartó el tráfico antes de que alcanzara la red OT.

Adicionalmente, el sistema de registros del firewall permitió identificar y documentar los intentos de acceso bloqueados, lo cual aporta trazabilidad y capacidad de monitoreo ante eventos potencialmente maliciosos como se muestra en la figura xxxxx.

6.3.3. Análisis técnico de los resultados simulados

La comparación entre ambos escenarios permite concluir que la implementación del firewall como conducto de seguridad entre las zonas IT y OT reduce significativamente la superficie de ataque, impidiendo actividades de reconocimiento y acceso no autorizado. Este comportamiento es coherente con los lineamientos establecidos en la norma IEC 62443, la cual establece la necesidad de segmentar redes industriales mediante zonas claramente definidas y conductos controlados que regulen estrictamente el flujo de información entre dominios de seguridad.

El ejercicio experimental permitió transformar una evaluación inicialmente cualitativa del modelo de seguridad en evidencia cuantificable, sustentada en resultados

observables tales como el estado de los puertos, la respuesta de los servicios y los registros de eventos generados por el firewall. Asimismo, además del escaneo de puertos presentado en esta sección, se ejecutaron pruebas adicionales que incluyeron intentos de fuerza bruta, generación controlada de tráfico malicioso tipo SYN Flood y validaciones de conectividad bajo diferentes políticas de filtrado. Estas pruebas complementarias, junto con su respectiva configuración técnica y evidencias gráficas, se encuentran descritas de manera detallada en el Anexo 5, donde se documenta paso a paso la programación de los equipos y los resultados obtenidos en cada caso.

6.3.3.1. Análisis de indicadores de seguridad

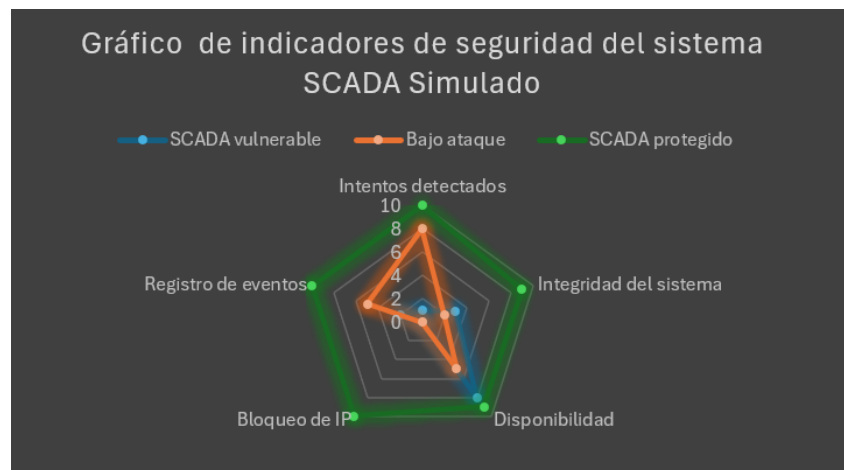


Figura 6.3.3: Gráfico de indicadores de seguridad del sistema SCADA Simulado.

Fuente: (Elaboración propia, 2026)

En la figura 6.3.3 se presenta una comparación de los principales indicadores de seguridad evaluados durante las pruebas experimentales realizadas sobre el entorno SCADA simulado. Se analizan tres escenarios: un sistema vulnerable sin mecanismos de protección, el sistema bajo condiciones de ataque y el sistema con controles de seguridad implementados.

Los resultados evidencian que el sistema vulnerable presenta bajos niveles de detección de ataques y ausencia de mecanismos de mitigación. Durante el escenario de ataque se observa un incremento significativo en los intentos de acceso no autorizado y una disminución en la disponibilidad del servicio.

Tras la implementación del sistema de autenticación y bloqueo automático de direcciones IP, se evidencia una mejora significativa en los indicadores de seguridad, particularmente en la detección de intentos de intrusión, la protección de la integridad del sistema y la generación de registros de eventos de seguridad. Estos resultados demuestran la efectividad de las contramedidas implementadas para fortalecer la seguridad del sistema SCADA.

6.4. Estimación presupuestaria para la compra de equipos de subestación

Con el propósito de dimensionar el impacto económico de la arquitectura propuesta, se realizó una estimación presupuestal considerando la intervención de una subestación eléctrica tipo, incluyendo segmentación de red, implementación de firewall industrial y dispositivos de comunicación seguros conforme a los lineamientos de la norma IEC 62443.

Tabla 6.4.1: Estimación presupuestal para implementación de arquitectura de ciberseguridad en una subestación

Componente	Referencia Industrial	Cantidad	Costo Estimado (USD)
Switch Industrial Gestionable IEC 61850	Hirschmann RSP25 / Siemens RUGGEDCOM	2	11,600
Firewall Industrial Ruggedizado	FortiGate Rugged 60F / Netgate Industrial	1	4,500
Gateway Industrial Seguro	Moxa EDR-G902 / MGate 5105	1	2,900
Licenciamiento y Soporte Anual	IPS, actualizaciones y monitoreo	1	1,800
Ingeniería e Implementación	Diseño, configuración, pruebas FAT/SAT	1	4,000
Total Estimado por Subestación			24,800 USD

El análisis presupuestal realizado en la tabla 6.4.1 permite dimensionar el impacto económico de cada arquitectura evaluada. Se estimaron los costos considerando precios de mercado industrial para el año 2026, incluyendo equipos certificados para entornos eléctricos, licenciamiento, soporte técnico e integración.

El escenario orientado a alta disponibilidad (Escenario A) presenta el mayor costo de implementación, debido a la utilización de equipos certificados IEC 61850 e IEC 62443 para subestaciones críticas. Sin embargo, ofrece el mayor nivel de resiliencia y cumplimiento normativo.

El escenario de convergencia IT-OT (Escenario B) reduce el costo en aproximadamente un 27 %, manteniendo capacidades avanzadas de segmentación y

cifrado, siendo una alternativa viable para centros de control o redes híbridas.

Finalmente, el escenario de implementación progresiva (Escenario C) representa la opción de menor inversión inicial, alineándose con estrategias de renovación gradual conforme al ciclo de vida de los activos, tal como se planteó en la restricción inicial del proyecto. En términos comparativos, el costo estimado por subestación representa una fracción mínima frente al impacto potencial de un evento de indisponibilidad operativa o manipulación maliciosa de sistemas SCADA, cuyo impacto puede superar ampliamente la inversión preventiva propuesta.

Capítulo 7

Discusión

7.1. Validez metodológica del enfoque adoptado

El enfoque metodológico mixto implementado en este estudio permitió integrar de manera efectiva el análisis normativo cualitativo con la evaluación técnica cuantitativa de tecnologías de ciberseguridad. La utilización de estándares internacionales como IEC 62443 e IEC 62351 proporcionó una base sólida para la definición de criterios, asegurando la validez del proceso de evaluación.

Adicionalmente, la transformación de criterios cualitativos en valores ponderados dentro de una matriz estructurada redujo la subjetividad en la toma de decisiones, lo cual es especialmente relevante en entornos industriales donde la selección tecnológica debe estar soportada por evidencia técnica y no únicamente por criterios comerciales o empíricos.

En este sentido, la metodología no solo resulta válida, sino también replicable en otros contextos del sector energético con características similares.

7.2. Discusión sobre la matriz de criterios y la ponderación basada en IEC 62443

La incorporación de una matriz de evaluación permitió establecer un mecanismo sistemático para comparar tecnologías de ciberseguridad bajo criterios homogéneos. La asignación de ponderaciones a cada criterio evidenció que aspectos como el cumplimiento normativo y la capacidad de segmentación tienen un impacto significativamente mayor en la seguridad de entornos IT/OT.

Esto demuestra que no todas las características técnicas tienen el mismo nivel de relevancia en infraestructuras críticas. Por ejemplo, funcionalidades avanzadas de monitoreo pueden resultar útiles, pero sin una adecuada segmentación de red, su efectividad se ve limitada frente a amenazas reales.

Desde una perspectiva práctica, este hallazgo implica que las decisiones de inversión en ciberseguridad deben priorizar arquitecturas robustas antes que funcionalidades

adicionales, alineándose con el principio de defensa en profundidad propuesto por la IEC 62443.

7.3. Importancia de la segmentación IT/OT evidenciada experimentalmente

Los resultados obtenidos en el entorno de simulación evidencian de manera clara el impacto de la segmentación de redes en la reducción de la superficie de ataque. En el escenario sin segmentación, fue posible identificar servicios expuestos y ejecutar actividades de reconocimiento desde la zona IT hacia la red OT. En contraste, al aplicar políticas de segmentación mediante el firewall, el tráfico fue filtrado y los intentos de acceso no autorizado fueron bloqueados.

Este comportamiento confirma que la segmentación no es únicamente una recomendación teórica, sino un mecanismo efectivo para mitigar riesgos en entornos industriales. En términos prácticos, esto se traduce en una mayor protección de sistemas críticos como SCADA, PLCs y dispositivos de protección eléctrica.

Para el caso de EBSA, la implementación de este tipo de arquitectura podría reducir significativamente la probabilidad de incidentes de ciberseguridad que afecten la continuidad del servicio eléctrico.

7.4. Discusión sobre la aplicabilidad real en la empresa

Uno de los aportes más relevantes del estudio radica en su enfoque aplicado. A diferencia de trabajos puramente teóricos, la propuesta desarrollada considera restricciones reales como la imposibilidad de intervenir directamente en la red productiva y la necesidad de evaluar la viabilidad económica de las soluciones.

La estimación presupuestaria realizada demuestra que la implementación de arquitecturas de ciberseguridad puede abordarse de manera progresiva, alineándose con el ciclo de vida de los activos existentes. Esto es fundamental en empresas del sector eléctrico, donde las decisiones de inversión deben balancear seguridad, continuidad operativa y costos.

Asimismo, la metodología propuesta facilita la adaptación a diferentes escenarios dentro de la empresa, permitiendo su aplicación tanto en subestaciones nuevas como en procesos de modernización de infraestructura existente.

7.5. Limitaciones del estudio y trabajos futuros

A pesar de los resultados obtenidos, el estudio presenta algunas limitaciones que deben ser consideradas. En primer lugar, la validación experimental se realizó en un

entorno de simulación (GNS3), lo cual, aunque permite un alto nivel de control, no reproduce completamente la complejidad de una red industrial en operación.

Adicionalmente, la evaluación de tecnologías se basa en información técnica disponible y en criterios definidos dentro de la matriz, lo que implica que factores como la experiencia del usuario, el soporte del fabricante o condiciones específicas de implementación pueden influir en la selección final.

Finalmente, no se contemplaron pruebas de desempeño en condiciones reales de carga, lo cual podría ser considerado en estudios futuros para complementar el análisis.

7.6. Aporte del estudio

El presente trabajo aporta una metodología estructurada para la evaluación y selección de tecnologías de ciberseguridad en entornos IT/OT, integrando análisis normativo, evaluación comparativa y validación experimental.

Su principal contribución radica en la reducción de la subjetividad en la toma de decisiones, mediante la utilización de criterios medibles y alineados con estándares internacionales. Asimismo, proporciona evidencia práctica sobre la efectividad de la segmentación de redes como mecanismo de protección en infraestructuras críticas.

En el contexto de EBSA, este estudio constituye una herramienta de apoyo para la planificación de estrategias de ciberseguridad, contribuyendo al fortalecimiento de la resiliencia operativa y la protección de activos críticos del sistema eléctrico.

Conclusiones

La caracterización funcional y de seguridad de los entornos IT y OT permitió evidenciar que la principal vulnerabilidad no radica únicamente en la tecnología utilizada, sino en la convergencia progresiva entre ambos dominios sin mecanismos estructurados de segmentación. La identificación de activos críticos y flujos de información especialmente aquellos asociados a comunicaciones SCADA, telecontrol y acceso remoto demostró que la superficie de ataque se incrementa cuando no existen conductos claramente definidos entre zonas.

Este análisis permitió establecer que la protección de la infraestructura eléctrica no puede abordarse desde una perspectiva exclusivamente perimetral, sino que requiere una comprensión integral de los procesos operativos, los activos estratégicos y los puntos de interconexión IT/OT. En este sentido, la caracterización desarrollada constituye un insumo fundamental para la toma de decisiones técnicas basadas en riesgo.

La aplicación de los lineamientos establecidos en las normas IEC 62443 e IEC 62351 permitió traducir principios normativos abstractos en requisitos técnicos concretos para el sector eléctrico. La segmentación por zonas y conductos, el control de acceso basado en políticas, el registro de eventos y la implementación de cifrado en comunicaciones críticas se consolidaron como elementos estructurales y no opcionales en arquitecturas IT/OT.

El estudio demostró que el cumplimiento normativo no debe interpretarse únicamente como un ejercicio documental, sino como un marco técnico que orienta la selección de tecnologías y define criterios medibles de seguridad. La matriz desarrollada, basada en estos estándares, permitió convertir requisitos regulatorios en variables evaluables, fortaleciendo la objetividad del análisis comparativo. La evaluación comparativa de alternativas tecnológicas, mediante una matriz ponderada de criterios técnicos, operativos y de viabilidad, permitió transformar un análisis cualitativo en una herramienta cuantificable de toma de decisiones. Este enfoque redujo la subjetividad en la selección de equipos y evidenció diferencias sustanciales entre arquitecturas orientadas exclusivamente a IT y aquellas diseñadas específicamente para entornos industriales.

Los resultados obtenidos muestran que la arquitectura más adecuada no necesariamente corresponde a la de mayor costo, sino a aquella que equilibra cumplimiento normativo, robustez operativa y viabilidad de implementación progresiva. En este contexto, la propuesta de arquitectura de referencia constituye una base técnica adaptable a las restricciones operativas de EBSA, permitiendo una modernización gradual alineada con el ciclo de vida de los activos existentes.

Referencias

- Alonso, M., Amarís, H., Pastrana, S., Turanzas, J., Gálvez, L., & Ledo, Á. T. (2021). Retos en materia de ciberseguridad en smart grids [Comunicación científica]. *VII Congreso Smart Grids*.
<https://www.smartgridsinfo.es/comunicaciones/comunicacion-retos-materia-ciberseguridad-smart-grids>
- Banco Interamericano de Desarrollo. (2020). *Ciberseguridad en infraestructuras críticas en América Latina* (inf. téc.). BID.
- Belden Inc. (2026). *Hirschmann RSP Switch Family: Industrial Managed Ethernet Switches* (inf. téc.) (Ficha técnica del fabricante, consultado en 2026). Belden.
<https://www.belden.com/products/industrial-networking/ethernet-switches/managed/rsp>
- Bureau Veritas. (2026). IEC 62443: Ciberseguridad y protección de datos en sistemas industriales [Consultado en 2026]. <https://www.bureauveritas.es/certificacion/ciberseguridad-y-proteccion-de-datos/IEC-62443>
- Centro Criptológico Nacional. (2020). *Seguridad en Sistemas de Control Industrial (Serie CCN-STIC 800)* (inf. téc.). CCN-CERT. España.
- Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, 56, 1-27.
- Cisco Systems. (2026). Cisco Industrial Ethernet 4000 Series Switches [Ficha técnica del fabricante, consultado en 2026]. <https://www.cisco.com>
- Comisión de Regulación de Energía y Gas. (2018). Marco regulatorio del sector eléctrico colombiano. <https://www.creg.gov.co>
- Comisión Económica para América Latina y el Caribe. (2021). *Transformación digital y gestión de riesgos en sectores estratégicos* (inf. téc.). CEPAL.
- Departamento Nacional de Planeación. (2016). *CONPES 3854 de 2016: Política Nacional de Seguridad Digital* (inf. téc.) (Consultado en 2026). DNP. Colombia. <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>
- Elaboración propia. (2026). Elaboración propia.
- Empresa de Energía de Boyacá. (2024). Información corporativa y servicios de energía eléctrica [Consultado: 2026]. <https://www.ebsa.com.co>
- European Union Agency for Cybersecurity. (2016). *Information Security and Risk Management Practices* (inf. téc.). ENISA.
- Fortinet. (2026). FortiGate Rugged Series [Ficha técnica del fabricante, consultado en 2026]. <https://www.fortinet.com>
- Gavilán, I. (2019, noviembre). Estructura de la planta de automatización [Entrada de blog, consultado en 2026]. <http://bluechip.ignaciogavilan.com/2019/11/estructura-de-la-planta-de.html>

- Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2011). Smart Grid Technologies: Communication Technologies and Standards. *IEEE Transactions on Industrial Informatics*, 7(4), 529-539.
- Hahn, A., & Govindarasu, M. (2013). Cyber attack exposure evaluation framework for the smart grid. *IEEE Transactions on Smart Grid*, 2(4), 835-843.
- Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-Physical Systems Security—A Survey. *IEEE Access*, 5, 18020-18034.
- Instituto Nacional de Ciberseguridad. (2019). *Guía de seguridad en sistemas de control industrial* (inf. téc.). INCIBE. España.
- International Electrotechnical Commission. (2013). IEC 62351 Power systems management and associated information exchange - Data and communications security.
- International Electrotechnical Commission. (2016). IEC 60870-5-104 Telecontrol equipment and systems.
- International Electrotechnical Commission. (2018). IEC 62443 Industrial communication networks - Network and system security.
- International Society of Automation. (2018). *ISA-95 Enterprise-Control System Integration Standard* (inf. téc.). ISA.
- Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection*, 9, 52-80.
- Krause, S., Genge, B., & Haller, P. (2015). Industrial control system security: Current status, challenges and future directions. *Computers & Security*, 47, 30-48.
- Laudon, K. C., & Laudon, J. P. (2020). *Management Information Systems: Managing the Digital Firm*. Pearson.
- Lee, R. M., Assante, M. J., & Conway, T. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid* (inf. téc.). SANS Industrial Control Systems. USA.
- Ministerio de Minas y Energía. (2013). *Reglamento Técnico de Instalaciones Eléctricas (RETIE)* (inf. téc.) (Consultado en 2026). Ministerio de Minas y Energía. Colombia.
https://www.minenergia.gov.co/documents/10180/23517/RETIE_2013.pdf
- Ministerio de Tecnologías de la Información y las Comunicaciones. (2019). Política de transformación digital en Colombia.
- National Institute of Standards and Technology. (2015). *Guide to Industrial Control Systems (ICS) Security (SP 800-82 Rev. 2)* (inf. téc.). NIST. Gaithersburg, MD, USA.
- Northwind Technical Services. (2026). Malware en sistemas de control industrial [Consultado en 2026].
<https://www.northwindts.com/es/malware-industrial-control-system/>
- Organización de los Estados Americanos. (2019). *Informe de ciberseguridad en América Latina* (inf. téc.). OEA.
- Red Eléctrica de España. (2018). *Estrategia de ciberseguridad en el sistema eléctrico* (inf. téc.). REE. España.
- ResearchGate. (2026a). EDS IT, SCADA and OT network [Figura consultada en línea, acceso en 2026]. https://www.researchgate.net/figure/EDS-IT-SCADA-and-OT-network_fig1_337657849

- ResearchGate. (2026b). IEC 62351 security layers [Figura consultada en línea, acceso en 2026]. https://www.researchgate.net/figure/EC-62351-security-layers_fig1_350415102
- ResearchGate. (2026c). IEC 62351 security layers [Figura consultada en línea, acceso en 2026]. https://www.researchgate.net/figure/EC-62351-security-layers_fig1_350415102
- Rodriguez, E. (2022, junio). ¿Qué es la defensa en profundidad? [Artículo en LinkedIn, consultado en 2026]. <https://www.linkedin.com/pulse/qu%C3%A9-es-la-defensa-en-profundidad-eusebio-rodriguez/>
- Schneider Electric. (2026). Visión práctica sobre la implementación de niveles de seguridad según la norma IEC 62443 [Consultado en 2026]. *Revista Automación y Control*. https://www.editoriales-srl.com.ar/revistas/aa/14/schneider_vision_practica_sobre_la_implementacion_de_niveles_de_seguridad_segun_la_norma_iec_62443
- Siemens. (2026a). *RUGGEDCOM RST2228: Managed Ethernet Switch - Technical Data* (inf. téc.) (Ficha técnica del fabricante, consultado en 2026). Siemens AG. <https://support.industry.siemens.com/cs/document/109479566/ruggedcom-rst2228>
- Siemens. (2026b). SCALANCE industrial communication devices [Ficha técnica del fabricante, consultado en 2026]. <https://www.siemens.com>
- Sin fecha. (2026). Fuente sin fecha especificada.
- Stouffer, K., Falco, J., & Scarfone, K. (2011). *Guide to Industrial Control Systems (ICS) Security* (inf. téc.). NIST.
- Superintendencia de Servicios Públicos Domiciliarios. (2020). Supervisión y control del sector eléctrico en Colombia. <https://www.superservicios.gov.co>
- Superintendencia de Servicios Públicos Domiciliarios. (2026). *Funciones de inspección, vigilancia y control de los servicios públicos domiciliarios* (inf. téc.) (Consultado en 2026). SSPD. Colombia. <https://www.superservicios.gov.co>
- Unidad de Planeación Minero Energética. (2020). *Transformación digital del sector energético colombiano* (inf. téc.). UPME. Colombia.
- Wang, W., Xu, Y., & Khanna, M. (2013). A survey on the communication architectures in smart grid. *Computer Networks*, 55(15), 3604-3629.
- Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A survey on cyber security for smart grid communications. *IEEE Communications Surveys & Tutorials*, 14(4), 998-1010.