ISSN: 1692-7257 - Volumen 2 – Número 46 - 2025

RCTA
Revista Colombiana de Tecnologías de Avanzada
UNIPAMPLONA

Digital Object Identifier: 10.24054/rcta.v2i46.4101

Subestaciones digitales: impulsando la sostenibilidad y ciberseguridad para el sector eléctrico a partir de soluciones emergentes

Digital substations: driving sustainability and cybersecurity in the power sector through emerging solutions

MSc. Oscar Andrés Tobar Rosero [1], MSc. Luis Fernando Quintero Henao [2]
PhD. Ernesto Pérez González [1]

[1] ***Universidad Nacional de Colombia***, *sede Medellín, Medellín, Antioquia, Colombia.*
[2] ***Enterprise Innovation,*** *Medellín, Antioquia, Colombia.*

Correspondencia: *oatobarr@unal.edu.co*

Recibido: *24 abril 2025.* ***Aceptado:*** *03 julio 2025.* ***Publicado:*** *21 julio 2025.*

Cómo citar: *O. A. Tobar Rosero, L. F. Quintero Henao, y E. Pérez González, «Subestaciones digitales: impulsando la sostenibilidad y ciberseguridad para el sector eléctrico a partir de soluciones emergentes», RCTA, vol. 2, n.º 46, pp. 132–140, jul. 2025. Recuperado de https://ojs.unipamplona.edu.co/index.php/rcta/article/view/4101*

Resumen: la digitalización de las subestaciones eléctricas, basada en el estándar IEC 61850, representa un eje fundamental en la modernización de las redes eléctricas hacia sistemas más sostenibles, eficientes y seguros. Este artículo examina el papel de las subestaciones digitales y el impacto de tecnologías emergentes como Software-Defined Networking (SDN), Blockchain, aprendizaje automático (ML) y la virtualización de funciones de red (NFV) en la automatización, análisis en tiempo real y resiliencia frente a amenazas cibernéticas. Se abordan los desafíos asociados a su implementación, incluyendo la interoperabilidad con sistemas legados, los riesgos de ciberseguridad y los costos de modernización, con énfasis en economías emergentes. Asimismo, se identifican oportunidades para avanzar hacia redes más descentralizadas e inteligentes, destacando el caso colombiano como referencia. El análisis ofrece una visión integral sobre las barreras y beneficios de estas tecnologías en la transición hacia infraestructuras eléctricas digitales, interoperables y resilientes.

Palabras clave: subestaciones digitales, ciberseguridad, tecnologías emergentes, sistemas de comunicación, sistemas eléctricos, transformación digital.

Abstract: the digitalization of electrical substations, guided by the IEC 61850 standard, is a key pillar in modernizing power grids toward more sustainable, efficient, and secure systems. This article examines the role of digital substations and the impact of emerging technologies, including Software-Defined Networking (SDN), Blockchain, machine learning (ML), and Network Function Virtualization (NFV), in enabling automation, real-time analytics, and resilience against cyber threats. It addresses the challenges of implementation, including the interoperability of legacy systems, cybersecurity risks, and modernization costs, particularly in emerging economies. The paper also explores opportunities for developing more decentralized and intelligent power networks, with

Colombia highlighted as a reference case. The analysis provides a comprehensive view of both the barriers and advantages of these technologies in the transition toward digital, interoperable, and resilient electrical infrastructures.

Keywords: digital substations, cybersecurity, emerging technologies, communication systems, electric power systems, digital transformation.

1. INTRODUCCIÓN

Las subestaciones digitales (SDs) han emergido como un pilar fundamental en la transformación digital del sector eléctrico, impulsando la modernización de las redes de energía hacia sistemas más eficientes, seguros y sostenibles [1]. Este proceso se enmarca en un contexto global de transición energética, donde la integración de tecnologías avanzadas es clave para responder a la creciente demanda de energía renovable y a los desafíos de ciberseguridad asociados [2].

La digitalización de subestaciones eléctricas configura uno de los principales cambios del sector eléctrico en los últimos años. Apalancada en el uso de estándares abiertos como IEC 61850, la implementación de SDs ha dado lugar al desarrollo de nuevos sistemas y soluciones tecnológicas orientadas a mejorar las capacidades de respuesta, la atención a eventos y la automatización de múltiples procesos operativos [3].

A su vez, las SDs han incentivado la integración de otros tipos de sistemas de generación, monitoreo, gestión y uso final de energía eléctrica (ver Fig. 1). Dadas las características del estándar IEC 61850, es posible llevar a cabo la supervisión, protección y control centralizados de sistemas de generación distribuida, microrredes y sistemas heredados; además de brindar la oportunidad de gestionar datos de operación y gestionar la ciberseguridad de este tipo de sistemas [4].

Además, la digitalización contribuye a la optimización de la gestión de activos y a la reducción de costos operativos mediante la incorporación de sensores y sistemas de monitoreo avanzados. Esta capacidad abre un abanico de oportunidades en el sector eléctrico, facilitando respuestas rápidas ante fallas, automatización avanzada, mantenimiento predictivo optimizado y una mayor resiliencia de la infraestructura crítica [5], [6]. En países como Colombia, las SDs se perfilan como herramientas clave para la modernización del sistema eléctrico, en línea con las estrategias nacionales de ciberseguridad y sostenibilidad energética.

En este contexto, la ciberseguridad emerge como un componente central en la digitalización de infraestructuras críticas, como el sector eléctrico. La creciente interconexión y automatización de las SDs, junto con su dependencia de sistemas de comunicación en tiempo real, las hace especialmente vulnerables a ciberamenazas. Desde ataques de denegación de servicio hasta intrusiones que comprometen la integridad de los datos operativos, la protección de estas infraestructuras requiere medidas especializadas, normativas actualizadas y la integración de soluciones tecnológicas avanzadas [7]. Así, la ciberresiliencia se convierte en un pilar indispensable para garantizar la sostenibilidad de estos sistemas, asegurando con esto una continuidad y seguridad operativa en entornos eléctricos digitalizados.

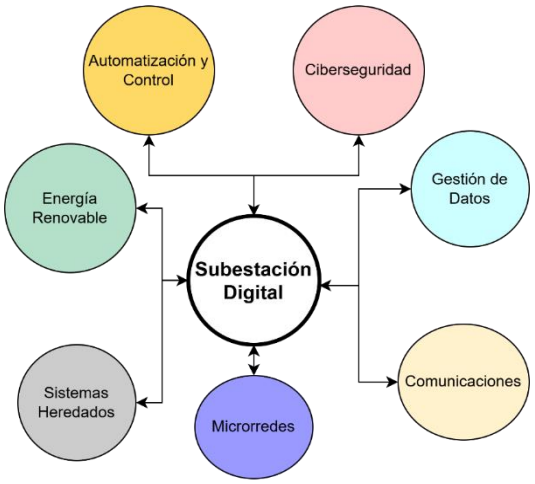

***Fig. 1**. Subestación digital como punto de integración de múltiples sistemas y soluciones tecnológicas para el sector eléctrico. **Fuente:** elaboración propia.*

Este artículo analiza el papel estratégico de las SDs en dicha transformación, explorando las soluciones emergentes que facilitan su implementación, su impacto en la transición energética y los retos y oportunidades asociados. Se examina su evolución desde modelos convencionales basados en componentes analógicos hacia arquitecturas digitales soportadas por el estándar IEC 61850, que optimizan la comunicación y el control en tiempo real. Esta transición mejora la interoperabilidad,

automatización y disponibilidad de datos para análisis avanzados, transformando las subestaciones en nodos inteligentes dentro de la red eléctrica. Finalmente, se introduce el análisis de tecnologías emergentes aplicables a las SDs, orientadas a la mitigación de vulnerabilidades y la optimización de procesos mediante capacidades digitales especializadas.

2. CONTEXTO Y ENFOQUE METODOLÓGICO

Las subestaciones eléctricas permiten transformar, controlar y distribuir la energía eléctrica dentro de la red, garantizando el equilibrio entre la generación y el consumo. En ellas convergen múltiples sistemas tanto de generación como de uso final, los cuales deben ser monitoreados, controlados y protegidos, al igual que la infraestructura eléctrica asociada [1]. En este contexto, la transición de subestaciones eléctricas convencionales a digitales ha representados un cambio paradigmático, dando lugar al uso de sistemas de comunicación para enlazar los diferentes componentes de protección, control, automatización y monitoreo en las subestaciones eléctricas.

Sin embargo, esta transformación tiene diversas implicaciones, especialmente desde el punto de vista de la ingeniería de sistemas eléctricos. La operación y mantenimiento de subestaciones digitales requiere de una comprensión de los sistemas de comunicación, los protocolos empleados para el intercambio de información entre sistemas y un conocimiento cuando menos básico para la gestión adecuada de la infraestructura de comunicación (ver Fig. 2) [8]. A su vez, los esquemas de redundancia física y lógica, junto con la gestión de ciberseguridad son pilares esenciales en el adecuado desarrollo de subestaciones eléctricas digitales seguras y confiables [9]. De aquí que existan diversas investigaciones y planteamientos sobre el desempeño de estos sistemas, retos de confiabilidad y análisis de vulnerabilidades a partir de múltiples configuraciones en SDs [10].

A través de múltiples investigaciones, se han identificado debilidades o vulnerabilidades críticas en los sistemas de comunicación, esenciales para el desarrollo de subestaciones digitales. Un ejemplo notable es la limitada capacidad de gestión de la infraestructura de comunicación empleada en las actuales tecnologías operativas, lo que restringe la escalabilidad y eficiencia en la transmisión de datos en tiempo real [11]. Asimismo, un análisis detallado de los protocolos de comunicación estandarizados bajo el marco IEC 61850 revela que, aunque facilitan el intercambio de información entre dispositivos, también presentan vulnerabilidades significativas [12]. La falta de mecanismos robustos de autenticación en estos protocolos puede ser explotada mediante diversos ataques, comprometiendo la integridad de los datos y, en consecuencia, la operación segura de las SDs.

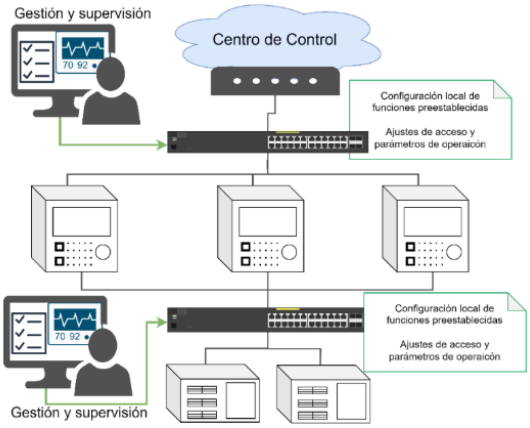

Fig. 2**. Arquitectura básica para una subestación digital, compuesta por los niveles de proceso, protección y control, y el nivel de supervisión.* ***Fuente: *elaboración propia.*

Si bien se cuenta con estándares como IEC 62443 e IEC 62351 que brindan pautas para asegurar la integración segura en sistemas industriales y redes inteligentes, los requerimientos de desempeño planteados para garantizar la confiabilidad de las SDs limitan en muchos casos la adopción de protocolos y configuraciones robustas de ciberseguridad en estos sistemas [13], [14].

Este artículo adopta un enfoque metodológico mixto, cualitativo y cuantitativo, para analizar tecnologías emergentes en sistemas de comunicación y ciberseguridad, identificando su impacto en la digitalización de subestaciones eléctricas. Las etapas contempladas en este enfoque se describen a continuación:

- Revisión sistemática de literatura
- Análisis: Casos de uso y evolución tecnológica
- Caracterización de tecnologías emergentes
- Discusión: Oportunidades y retos para para el sector eléctrico a partir de las tecnologías emergentes.

La investigación se basa en una revisión sistemática de la literatura científica, técnica y normativa reciente sobre subestaciones digitales, con un enfoque en los protocolos de comunicación

considerados en el estándar IEC 61850 y sus implicaciones en materia de ciberseguridad. Adicionalmente, se complementa este proceso con un análisis sobre estudios de caso destacados con implementación de subestaciones digitales en distintas regiones, haciendo énfasis en experiencias de América Latina, como el caso colombiano.

Producto de este análisis, se expone una visión general sobre la evolución de las subestaciones eléctricas convencionales hacia entornos digitalizados, destacando la relevancia de los sistemas de comunicación como eje estructural. A su vez, se identifican y describen algunas de las principales tecnologías emergentes que pueden integrarse en subestaciones digitales, destacando sus atributos fundamentales y sus potenciales beneficios para el sector eléctrico.

Finalmente, se plantea una discusión alrededor de los principales retos y oportunidades derivados de la transformación digital en el sector eléctrico y las soluciones tecnológicas emergentes analizadas.

3. SOSTENIBILIDAD Y CIBERSEGURIDAD EN EL SECTOR ELÉCTRICO MEDIANTE LA DIGITALIZACIÓN DE SISTEMAS

Para hablar de sostenibilidad y ciberseguridad es fundamental establecer en primer lugar el nivel de adopción tecnológica en torno a las subestaciones digitales. Esto, nos lleva a identificar como a nivel global se puede establecer un grado de madurez media a alta, a partir de los múltiples despliegues documentados principalmente en Europa, Estados unidos y Asia.

Por ejemplo, operadores como Landsnet en Islandia han desplegado un importante número subestaciones completamente digitales (220–66 kV) durante 2023, basadas en IEC 61850, con transformadores de instrumentación de baja potencia y sistemas de control multimarca [15]. Por su parte, en Estados Unidos y Reino Unido, el despliegue de subestaciones digitales se enmarca en los programas gubernamentales de modernización de redes. Además, National Grid (Reino Unido) y CFE (México) han adoptado soluciones IEC 61850 con GOOSE, MMS, Sampled Values y redundancia PRP en múltiples proyectos [16], [17].

Viendo un poco más hacia la región, en América Latina ISA-CTEEP (Brasil) ha destacado por sus iniciativas de innovación, tal como es la primera “subestación 4.0” inaugurada en Sao Paulo; la cual, hace parte de un programa de digitalización en varias subestaciones de la empresa [18], [19].

Países como México, Perú y Chile, también han evidenciado avances importantes en la implementación de subestaciones digitales, en algunos casos planteando incluso un marco normativo preliminar que apoya los procesos de adopción de tecnologías digitales para subestaciones eléctricas [20].

En Colombia se han evidenciado proyectos muy relevantes liderados por las principales empresas de servicios públicos del país, tal es el caso de la digitalización en la subestación Chinú, con el primer sistema con bus de proceso interoperable, la subestación Portugal (Bogotá) que representa el primer proyecto de subestación completamente digital en el país y posteriormente se suman proyectos en Tolima, Valle del Cauca y Antioquia [21], [22]. Esto evidencia la tendencia en adopción de nuevas tecnologías y la transformación que actualmente se adelanta en el sector.

A partir esto, y considerando los desafíos y oportunidades que conlleva la implementación de subestaciones digitales en el sector eléctrico, resulta esencial mantenerse actualizado respecto a las múltiples investigaciones que se desarrollan a nivel global en esta área [9], [23]. Estas investigaciones han impulsado la aparición de soluciones emergentes que, si bien presentan nuevos retos, también abren posibilidades significativas para acelerar la transformación digital y avanzar en los objetivos de sostenibilidad energética.

Una de las estrategias más prometedoras consiste en la integración de tecnologías emergentes que podrían mejorar tanto la funcionalidad operativa de las SDs como su nivel de protección frente a amenazas cibernéticas. Entre estas tecnologías, se destacan:

- **Software-Defined Networking (SDN):** permite una gestión dinámica y eficiente de las redes de comunicación en SDs bajo IEC 61850. La separación del plano de control y datos brinda mayor flexibilidad para la administración del tráfico y la implementación de esquemas de redundancia, mejorando así la resiliencia ante ataques cibernéticos y optimizando la comunicación en tiempo real [24], [25].
- **Blockchain:** ofrece mecanismos de registro inmutable y descentralizado, útiles para preservar la integridad de la información

operativa y de configuración en las SDs, reduciendo la posibilidad de manipulaciones maliciosas o errores involuntarios [26], [27].

- **Aprendizaje Automático (ML):** facilita el análisis de flujos de datos en tiempo real mediante algoritmos capaces de identificar patrones anómalos, detectar intrusiones y clasificar eventos críticos, aportando valor a la toma de decisiones en ciberseguridad y mantenimiento predictivo [28], [29].
- **Network Virtualization Functions (NFV):** permite reducir la complejidad física de la infraestructura mediante la implementación de funciones de red sobre plataformas virtualizadas. Esto puede repercutir en una simplificación la infraestructura de SDs, permitiendo incrementa la flexibilidad operativa, facilita la integración de soluciones heterogéneas y permite una evolución escalable de la red eléctrica [30], [31].

La convergencia entre sostenibilidad y ciberseguridad en el sector eléctrico exige un enfoque integral que combine innovación tecnológica con rigurosidad operativa. La adopción de soluciones como SDN, Blockchain, ML y NFV permite avanzar hacia subestaciones más inteligentes, resilientes y eficientes, capaces de responder a los crecientes desafíos energéticos y de seguridad del entorno digital actual [28].

La adopción de tecnologías emergentes en subestaciones digitales no solo responde a una necesidad técnica frente a los desafíos de modernización y ciberseguridad, sino que también ha dado lugar a una serie de experiencias prácticas y estudios aplicados que validan su funcionalidad en entornos reales. Diversos casos de uso han sido documentados en la literatura científica, demostrando la aplicabilidad de soluciones como SDN, ML, NFV y, en menor medida, Blockchain, en contextos de operación de subestaciones bajo el estándar IEC 61850.

Una de las experiencias más destacadas es el trabajo desarrollado por Girdhar et al. (2024), quienes propusieron un marco de restauración cibernética en subestaciones IEC 61850 basado en SDN [32]. Esta arquitectura incluye detección de intrusos (IDS), un controlador SDN centralizado y un sistema dinámico de gestión de puertos. Validada a través de pruebas en tiempo real bajo esquemas hardware-in-the-loop (HIL), la solución demostró ser capaz de mantener la continuidad operativa durante ataques cibernéticos, reforzando así la resiliencia del sistema.

De forma complementaria, los mismos autores desarrollaron un marco híbrido de ciberseguridad que combina SDN e IDS para mitigar ataques mediante inyección maliciosa de mensajes GOOSE. Esta solución permite detectar eventos anómalos y ejecutar bloqueos automáticos de puertos comprometidos, asegurando la integridad de la red de comunicaciones [33].

En cuanto al uso de NFV, el proyecto VirtuWind (2019) constituye un referente importante [34]. Esta iniciativa diseñó una arquitectura para redes industriales críticas, aplicable a subestaciones digitales, en la que se integran SDN y NFV para garantizar calidad de servicio (QoS), escalabilidad y aislamiento de funciones. La arquitectura permite una gestión eficiente de servicios en tiempo real, esencial para sistemas eléctricos complejos.

Desde una perspectiva de automatización de subestaciones, Leal et al. (2021) propusieron la arquitectura S3N (Smart Solution for Substation Networks), que segmenta la red en tres capas funcionales: infraestructura, virtualización y funcionalidades [35]. Esta propuesta facilita la auto-configuración de IEDs, la segmentación dinámica del tráfico y la adaptación de servicios, mostrando un avance significativo hacia la evolución de subestaciones inteligentes.

En el campo del aprendizaje automático (ML), también se han desarrollado iniciativas relevantes. Por ejemplo, Yegorov et al. (2023) y Eynawi et al. (2024) demostraron la aplicación de algoritmos de detección de anomalías y selección de características en subestaciones digitales para detectar intrusiones, ataques tipo spoofing en GOOSE, y fallas operativas, aportando un enfoque proactivo en la gestión de la ciberseguridad [36], [37].

Por su parte, muchas aplicaciones basadas en Blockchain se encuentran en etapas iniciales o en proceso de desarrollo. Aunque existen propuestas arquitectónicas orientadas a la gestión de ajustes de protección mediante registros distribuidos, su adopción a gran escala en subestaciones digitales aún es limitada, debido principalmente a restricciones operativas, latencia y requisitos de interoperabilidad [38].

Los casos de uso documentados en la literatura reciente confirman la viabilidad técnica de integrar soluciones como SDN, ML y NFV en subestaciones digitales bajo IEC 61850, contribuyendo a una mayor automatización, resiliencia operativa y

ciberseguridad. Estas experiencias constituyen una base sólida para la evolución futura de estas infraestructuras críticas, abriendo camino hacia redes eléctricas más inteligentes, seguras y sostenibles.

En un contexto local, la digitalización de subestaciones en Colombia ha potenciado la adopción de energías renovables, alineándose con las metas nacionales de reducción de emisiones. Sin embargo, la implementación de SDs y otras tecnologías emergentes presenta retos significativos, como la necesidad de garantizar la interoperabilidad con sistemas heredados y mitigar riesgos de ciberseguridad, junto con oportunidades para innovar en la gestión de redes eléctricas sostenibles.

De esta manera, el presente capítulo expone un análisis preliminar sobre el panorama que afronta el sector eléctrico a partir de la transformación digital de múltiples sistemas. Como caso particular, se destaca el rol de las subestaciones digitales en la redefinición de los paradigmas operativos del sistema eléctrico, contribuyendo no solo a una mayor eficiencia y seguridad, sino también a la consolidación de un modelo energético más sostenible, descentralizado y resiliente frente a futuras contingencias, especialmente apalancado de tecnologías emergentes.

4. DISCUSIÓN – RETOS Y OPORTUNIDADES

La implementación de sistemas de comunicación avanzados y la integración de soluciones tecnológicas, como las descritas anteriormente, no solo modernizan las subestaciones eléctricas, sino que las transforman en sistemas dinámicos y adaptativos. Estas infraestructuras son clave para responder a los requerimientos de la transición energética, particularmente en lo relativo al uso creciente de fuentes de energía renovable y el avance hacia una economía descarbonizada.

La digitalización de las subestaciones constituye un eje estratégico en este proceso, ya que permite optimizar la gestión de microrredes y facilitar una transición eficiente hacia redes eléctricas descentralizadas. En este contexto, la capacidad analítica de las soluciones digitales mejora la predicción de patrones de consumo y generación, aportando información crítica para la formulación de políticas energéticas sostenibles.

No obstante, este avance conlleva una serie de desafíos técnicos y estratégicos que deben abordarse con rigurosidad. Entre ellos destacan los siguientes:

- **Ciberseguridad:** La creciente conectividad de los sistemas digitales expone a las subestaciones a riesgos significativos, como ataques de denegación de servicio distribuido o la explotación de vulnerabilidades en protocolos de comunicación.
- **Costos de modernización:** Las inversiones necesarias en hardware especializado y capacitación técnica pueden representar una barrera significativa, especialmente en economías emergentes.
- **Interoperabilidad:** La coexistencia de sistemas heredados con tecnologías modernas genera problemas de compatibilidad, retrasando la implementación efectiva y a gran escala de soluciones digitales.

Por otra parte, las oportunidades derivadas del proceso de digitalización son igualmente relevantes. Tecnologías emergentes como las SDN y Blockchain habilitan el desarrollo de sistemas eléctricos más seguros, resilientes y eficientes, capaces de responder de manera ágil a condiciones operativas cambiantes y a amenazas cibernéticas sofisticadas. La Tabla 1 expone una síntesis de los principales retos y oportunidades analizados desde diferentes enfoques o categorías.

Tabla 1: *Base de reglas*

Categoría	Retos	Oportunidades
Seguridad	Vulnerabilidad ante ciberataques (DDoS, spoofing, explotación de protocolos IEC 61850)	Aplicación de tecnologías como SDN y Blockchain para aumentar la resiliencia y seguridad de los sistemas
Económica	Altos costos de modernización (hardware avanzado, capacitación de personal técnico)	Optimización operativa y reducción de pérdidas a mediano y largo plazo
Técnica	Problemas de interoperabilidad entre sistemas heredados y tecnologías digitales modernas	Implementación de arquitecturas flexibles y escalables con NFV y SDN
Operativa	Dificultad para integrar tecnologías en entornos con limitada infraestructura o soporte regulatorio	Mejora en la gestión de microrredes, predicción de demanda, y operación descentralizada mediante análisis de datos y ML
Ambiental / Social	Necesidad de políticas que acompañen la	Apoyo a la transición energética y cumplimiento de metas

Categoría	Retos	Oportunidades
	adopción tecnológica con enfoque sostenible	de descarbonización mediante digitalización y simulación con gemelos digitales (digital twins)

En conjunto, estos elementos configuran un escenario complejo pero prometedor. El desarrollo de subestaciones digitales no solo puede mejorar el desempeño técnico del sistema eléctrico, sino que también fortalece su capacidad de adaptación frente a desafíos energéticos y climáticos del siglo XXI. La transformación digital, apoyada por una infraestructura cibersegura y tecnologías emergentes, representa una oportunidad estratégica para avanzar hacia un modelo energético más sostenible, resiliente y eficiente.

5. CONCLUSIONES

La transformación digital del sector eléctrico, particularmente en el ámbito de las subestaciones, representa un hito clave hacia la construcción de sistemas más eficientes, resilientes y sostenibles. Las subestaciones digitales, soportadas por el estándar IEC 61850, han demostrado ser fundamentales para integrar funciones de supervisión, protección y control en plataformas unificadas que permiten una gestión más flexible, automatizada y segura de la infraestructura eléctrica.

El presente artículo ha evidenciado cómo tecnologías emergentes como SDN, Blockchain, ML y NFV pueden fortalecer significativamente las capacidades técnicas y de ciberseguridad de las SDs. Estas herramientas no solo permiten una mayor adaptabilidad frente a condiciones operativas variables, sino que también mejoran la eficiencia del sistema, facilitan la integración de energías renovables y refuerzan la resiliencia frente a amenazas cibernéticas.

No obstante, la digitalización de subestaciones conlleva retos técnicos, económicos y normativos que deben ser abordados de forma integral. La interoperabilidad con sistemas legados, los altos costos de modernización y la necesidad de personal capacitado constituyen barreras significativas, particularmente en contextos de economías emergentes. Además, garantizar la ciberseguridad en infraestructuras críticas exige una evolución de las prácticas tradicionales de protección, así como la implementación de nuevos enfoques centrados en la detección proactiva de amenazas y la gestión dinámica del riesgo.

El caso colombiano, junto con diversas experiencias internacionales revisadas en este artículo, demuestra que la transición hacia subestaciones digitales es no solo factible, sino estratégica para modernizar los sistemas eléctricos y cumplir con los compromisos globales de descarbonización y sostenibilidad. Para lograrlo, será clave fortalecer el marco regulatorio, fomentar la inversión en innovación tecnológica y promover esquemas colaborativos entre industria, gobierno y academia.

Las subestaciones digitales, habilitadas por tecnologías emergentes, ofrecen una plataforma transformadora para enfrentar los desafíos del siglo XXI en el sector eléctrico. Su implementación efectiva permitirá avanzar hacia redes eléctricas más inteligentes, seguras, adaptativas y alineadas con los principios de sostenibilidad energética y ciberresiliencia.

RECONOCIMIENTO

Un agradecimiento especial al equipo de trabajo del Laboratorio de Automatización y Comunicaciones Industriales de la Universidad nacional de Colombia sede Medellín, quienes han apoyado este proceso de investigación, aportando sus experiencias y recomendaciones.

REFERENCIAS

[1] G. R. Santos, E. Zancul, G. Manassero, and M. Spinola, “From conventional to smart substations: A classification model,” Electric Power Systems Research, vol. 226, p. 109887, Jan. 2024, doi: 10.1016/J.EPSR.2023.109887.

[2] O. A. Tobar-Rosero, E. Pérez González, G. D. Zapata Madrigal, and J. F. Botero Vega, “Subestaciones digitales y ciberseguridad como factores claves en la transformación digital del sector eléctrico colombiano,” Encuentro Internacional de Educación en Ingeniería, pp. 1–12, Sep. 2023, doi: 10.26507/PAPER.3277.

[3] A. Rahman, O. Yilmaz, O. Vaze, and A. Mandal, “Smart Substation Control and Protection Facilitating the Virtualization of Multiple Protection and Control,” 2023 IEEE International Conference on Energy Technologies for Future Grids, ETFG 2023, p. Wollongong, 2023, doi: 10.1109/ETFG55873.2023.10407293.

[4] C. P. Vineetha and C. A. Babu, “Smart grid challenges, issues and solutions,” Proceedings of 2014 International Conference on Intelligent Green Building and Smart Grid, IGBSG 2014, 2014, doi: 10.1109/IGBSG.2014.6835208.

[5] O. A. Tobar-Rosero, J. H. Vargas-Días, R. G. Sierra, G. D. Z. madrigal, and J. E. Candelo-Becerra, “Herramientas de Gestión de Protecciones para Optimizar Procesos Operativos y de Mantenimiento en Empresas del Sector Eléctrico,” Inge CuC, vol. 20, no. 2, Oct. 2024, doi: 10.17981/INGECUC.20.2.2024.03.

[6] D. Álvarez-Osorio, O. Arenas-Crespo, P. Arregocés-Guerra, J. C. R. Suárez, O. A. Tobar-Rosero, and G. D. Zapata-Madrigal, “Modernización del Sistema de Diagnóstico Automático de Eventos en Líneas de Transmisión y Subtransmisión de Energía Eléctrica,” Revista EIA, vol. 22, no. 43, p. 4335 pp. 1–41, Jan. 2025, doi: 10.24050/reia.v22i43.1768.

[7] O. Roa, J. F. Botero, S. A. Gutierrez-Betancur and O. A. Tobar-Rosero, "GOOSEAttacker: Synthetic Attack Generation Tool for IEC61850," 2023 IEEE Latin-American Conference on Communications (LATINCOM), Panama City, Panama, 2023, pp. 1-6, doi: 10.1109/LATINCOM59467.2023.10361897.

[8] J. D. McDonald, Electric Power Substations Engineering, McDonald, John D., vol. Third Edition. 2011.

[9] Y. E. Bouffard-Vercelli and B. Andre, “Future Architectures of Electrical Substations,” Petroleum and Chemical Industry Conference Europe Conference Proceedings, PCIC EUROPE, vol. 2021-June, 2021, doi: 10.23919/PCICEUROPE50407.2021.9805424.

[10] O. A. Tobar-Rosero, O. D. Díaz-Mendoza, P. A. Díaz-Vargas, J. E. Candelo-Becerra, H. A. Florez-Célis, y L. F. Quintero-Henao, «Digital Substations: Optimization Opportunities from Communication Architectures and Emerging Technologies», Sci., vol. 7, n.º 2, p. 63, 2025. doi: 10.3390/sci7020063.

[11] M. Adamiak, D. Baigent, G. E. Digital, E. Ralph, and M. Sisco, “IEC 61850 Communication Networks and Systems In Substations: An Overview for Users,” The Protection and Control Journal, pp. 61–68, 2009.

[12] O. A. Tobar-Rosero et al., “GOOSE Secure: A Comprehensive Dataset for In-Depth Analysis of GOOSE Spoofing Attacks in Digital Substations,” Energies 2024, Vol. 17, Page 6098, vol. 17, no. 23, p. 6098, Dec. 2024, doi: 10.3390/EN17236098.

[13] D. Dolezilek, D. Gammel and W. Fernandes, "Cybersecurity based on IEC 62351 and IEC 62443 for IEC 61850 systems," 15th International Conference on Developments in Power System Protection (DPSP 2020), Liverpool, UK, 2020, pp. 1-6, doi: 10.1049/cp.2020.0016.

[14] P. Kaliappan, S. Sudha and D. Shankar, "International Standards for Cybersecurity in Smart Devices for the Power Sector," 2024 International Conference on Computational Intelligence for Green and Sustainable Technologies (ICCIGST), Vijayawada, India, 2024, pp. 1-5, doi: 10.1109/ICCIGST60741.2024.10717531.

[15] PAC World, “Landsnet’s Road to a Fully Digital Transmission System,” 2023. [En línea]. Disponible en: https://www.pacw.org/

[16] S. R. Patel, “Digital Substation Design and Automation with IEC 61850,” *Keentel Engineering Blog*, May 12, 2025. [Online]. Available: https://keentelengineering.com/digital-substation-design-and-automation-with-iec-61850.

[17] Electric Energy Online, “The Digital Substation: A Catalyst for the U.S. Grid Modernization Initiative,” 2023.

[18] ISA Energía Brasil, “Nuestra Trayectoria,” 2023. [En línea]. Disponible en: https://www.isaenergiabrasil.com.br/

[19] SEL Inc., “CFE México – IEC 61850 Implementation,” 2015. [En línea]. Disponible en: https://www.selinc.com/

[20] A. Domínguez et al., “Restoration Strategies in Digital Distribution Substations,” Energies, vol. 17, no. 16, p. 4154, 2024. DOI: 10.3390/en17164154

[21] Ectricol S.A.S., “Primera Subestación Digital en Colombia,” 2022. [En línea]. Disponible en: https://www.ectricol.com/

[22] La Economía Colombia, “En marcha la primera subestación eléctrica digital del Tolima,” 2022. Disponible en: https://economistacolombia.com/

[23] J. Li, H. Su, Y. Zhang, Q. Yan, L. Liu, and T. Wang, “Smart Digital Inspection and Maintenance of Substations,” 2024 5th International Conference on Power Engineering, ICPE 2024, pp. 388–393, 2024, doi: 10.1109/ICPE64565.2024.10929212.

[24] U. Ghosh, P. Chatterjee, S. Shetty, U. Ghosh, P. Chatterjee, and S. Shetty, “Securing SDN-Enabled Smart Power Grids: SDN-Enabled Smart Grid Security,” https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-6684-3666-0.ch046, vol. 3, pp. 1028–1046, Jan. 1AD, doi: 10.4018/978-1-6684-3666-0.CH046.

[25] M. Girdhar, J. Hong, W. Su, A. Herath, and C.-C. Liu, “SDN-Based Dynamic Cybersecurity Framework of IEC-61850 Communications in Smart Grid,” 2024 IEEE Power & Energy Society General Meeting (PESGM), pp. 1–5,

Jul. 2024, doi: 10.1109/PESGM51994.2024.10688802.

[26] I. Hammouti, A. Addaim, and Z. Guennoun, "Proposed Architecture of Cyber Security in Smart Grids, Blockchain as Solution," 2022 IEEE Information Technologies and Smart Industrial Systems, ITSIS 2022, 2022, doi: 10.1109/ITSIS56166.2022.10118374.

[27] Q. Chai et al., "Relay Protection Setting Management System and Method Based on Blockchain Encryption Technology," Proceedings - 2023 International Conference on Power System Technology: Technological Advancements for the Construction of New Power System, PowerCon 2023, 2023, doi: 10.1109/POWERCON58120.2023.10331237.

[28] P. K. Yegorov, A. Lackovitch, E. Dean, H. M. Mustafa, S. Basumallik, and A. Srivastava, "Analyzing GOOSE Security in IEC61850-based Substation Using ML, SDN and Digital Twin," 2023 North American Power Symposium, NAPS 2023, 2023, doi: 10.1109/NAPS58826.2023.10318551.

[29] A. Eynawi, A. Mumrez, G. Elbez, and V. Hagenmeyer, "Machine Learning-Based Feature Selection for Intrusion Detection Systems in IEC 61850-Based Digital Substations," 2024 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, SmartGridComm 2024, pp. 1–7, 2024, doi: 10.1109/SMARTGRIDCOMM60555.2024.10738031.

[30] A. Fahmin, Y. C. Lai, M. S. Hossain, Y. D. Lin, and D. Saha, "Performance modeling of SDN with NFV under or aside the controller," Proceedings - 2017 5th International Conference on Future Internet of Things and Cloud Workshops, W-FiCloud 2017, vol. 2017-January, pp. 211–216, Nov. 2017, doi: 10.1109/FICLOUDW.2017.76.

[31] K. Kaur, V. Mangat, and K. Kumar, "A review on Virtualized Infrastructure Managers with management and orchestration features in NFV architecture," Computer Networks, vol. 217, p. 109281, Nov. 2022, doi: 10.1016/J.COMNET.2022.109281.

[32] M. Girdhar, J. Hong, W. Su, A. Herath, and C.-C. Liu, "SDN-Based Dynamic Cybersecurity Framework of IEC-61850 Communications in Smart Grid," 2024 IEEE Power & Energy Society General Meeting (PESGM), pp. 1–5, Jul. 2024, doi: 10.1109/PESGM51994.2024.10688802.

[33] M. Girdhar, J. Hong, W. Su, A. Herath, and C.-C. Liu, "Hybrid Intrusion Detection System using SDN and Machine Learning for IEC 61850," arXiv preprint, 2023. [Online]. Available: https://arxiv.org/abs/2311.12205

[34] E. Sakic, V. Kulkarni, V. Theodorou, A. Matsiuk, S. Kuenzer, N. E. Petroulakis, y K. Fysarakis, "VirtuWind – An SDN- and NFV-Based Architecture for Softwarized Industrial Networks," en *Measurement, Modelling and Evaluation of Computing Systems*, R. German, K.-S. Hielscher y U. Krieger, eds., LNCS, vol. 10740, Cham: Springer, 2018, pp. 251–261, doi: 10.1007/978-3-319-74947-1-17.

[35] A. Leal and J. F. Botero, "Arquitectura para redes de comunicaciones en subestaciones de energía basadas en virtualización y SDN," *Revista Facultad de Ingeniería Universidad de Antioquia*, no. 100, pp. 48–66, Mar. 2021, doi: 10.17533/udea.redin.20210321.

[36] P. K. Yegorov et al., "Analyzing GOOSE Security in IEC61850-based Substation Using ML, SDN and Digital Twin," Proc. NAPS 2023, doi: 10.1109/NAPS58826.2023.10318551

[37] Eynawi et al., "Machine Learning-Based Feature Selection for Intrusion Detection Systems in IEC 61850-Based Digital Substations," IEEE SmartGridComm 2024, pp. 1–7, 2024, doi: 10.1109/SMARTGRIDCOMM60555.2024.10738031.

[38] Q. Chai et al., "Relay Protection Setting Management System and Method Based on Blockchain Encryption Technology," Proc. PowerCon 2023, doi: 10.1109/POWERCON58120.2023.10331237.