innova SCIENCE JOURNAL ISSN:3091-1680

OM EDITORIAL

Artículo Científico

Seguridad y confiabilidad en los sistemas eléctricos de infraestructuras digitales críticas

Safety and reliability of critical digital infrastructure power systems

Guerrero-Calero, Juan Manuel [1]; Toaza-Iza, Jimmy Xavier [2]; Calero-Silva, Mayckel Sebastián [3].

[1] Universidad Estatal del Sur de Manabí; Ecuador, Portoviejo; https://orcid.org/0000-0002-1356-0475; juan.guerrero@unesum.edu.ec

[2] Universidad Técnica de Cotopaxi; Ecuador, Latacunga; https://orcid.org/0000-0002-5859-3385; jimmy.toaza1062@utc.edu.ec

[3] Universidad de las Fuerzas Armadas; Ecuador, Sangolqui; https://orcid.org/0000-0001-5454-9777; mscalero1@espe.edu.ec

[1] Autor Correspondencia

https://doi.org/10.63618/omd/isj/v2/n1/33

Cita: Guerrero-Calero, J. M., Toaza-Iza, J. X., & Calero-Silva, M. S. (2024). Seguridad y confiabilidad en los sistemas eléctricos de infraestructuras digitales críticas. *Innova Science Journal*, *2*(1), 58-72. https://doi.org/10.63618/omd/isj/v2n1/33.

Recibido: 02/12/2023
Aceptado: 29/12/2023
Publicado: 31/01/2024

Resumen: El crecimiento de las infraestructuras digitales ha intensificado la dependencia de sistemas eléctricos confiables, cuya seguridad es esencial para la continuidad operativa de sectores estratégicos. Este estudio analiza la optimización de la confiabilidad eléctrica, el impacto de la variabilidad del suministro y las amenazas cibernéticas en infraestructuras críticas. Mediante un enfoque exploratorio y revisión bibliográfica, se identificaron estrategias de compensación reactiva, predicción de fallos con inteligencia artificial y almacenamiento energético para estabilizar la red. Los resultados evidencian que la integración de tecnologías de monitoreo y protección dinámica mejora la resiliencia de estos sistemas, mitigando interrupciones y riesgos operativos. Se destaca la necesidad de implementar esquemas de ciberseguridad avanzados para enfrentar amenazas digitales, incluyendo el uso de inteligencia artificial en la detección de anomalías. A pesar de los avances, persisten desafíos en la integración de soluciones sostenibles y la actualización constante de los protocolos de seguridad. La investigación concluye que la combinación de optimización energética, respaldo eléctrico y estrategias de ciberseguridad es clave para garantizar la estabilidad y sostenibilidad de las infraestructuras digitales críticas, requiriendo un desarrollo continuo de tecnologías innovadoras y normativas adaptadas a la evolución del entorno eléctrico y digital.

Palabras clave: confiabilidad eléctrica; ciberseguridad; infraestructura digital; inteligencia artificial; almacenamiento energético.

Abstract: The growth of digital infrastructures has intensified the dependence on reliable electrical systems, whose security is essential for the operational continuity of strategic sectors. This study analyzes the optimization of electrical reliability, the impact of supply variability and cyber threats on critical infrastructures. Through an exploratory approach and literature review, reactive compensation, artificial intelligence fault prediction and energy storage strategies were identified to stabilize the grid. The results show that the integration of monitoring and dynamic protection technologies improves the resilience of these systems, mitigating interruptions and operational risks. It highlights the need to implement advanced cybersecurity schemes to address digital threats, including the use of artificial intelligence in anomaly detection. Despite advances, challenges remain in integrating sustainable solutions and constantly updating security protocols. The research concludes that the combination of energy optimization, power backup and cybersecurity strategies is key to ensure the stability and sustainability of critical digital infrastructures, requiring continuous development of innovative technologies and regulations adapted to the evolving electrical and digital environment.

Keywords: electrical reliability; cybersecurity; digital infrastructure; artificial intelligence; energy storage.

1. Introducción

El crecimiento exponencial de las infraestructuras digitales ha traído consigo una dependencia cada vez mayor de los sistemas eléctricos para garantizar su funcionamiento continuo y seguro. En la actualidad, sectores estratégicos como las telecomunicaciones, la banca, la salud y la industria dependen de redes eléctricas confiables para operar de manera eficiente (Velasco et al., 2023). Sin embargo, estos sistemas están expuestos a múltiples riesgos que comprometen su estabilidad, como fallos en la distribución de energía, fluctuaciones en la calidad del suministro y amenazas cibernéticas que pueden afectar su control y supervisión. En este contexto, la seguridad y confiabilidad de los sistemas eléctricos en infraestructuras críticas se han convertido en una preocupación clave para garantizar la continuidad operativa y mitigar los efectos de interrupciones imprevistas.

Las afectaciones a la seguridad y confiabilidad de los sistemas eléctricos en infraestructuras digitales críticas pueden manifestarse de diversas formas. Uno de los principales problemas es la variabilidad en la calidad del suministro eléctrico, lo que genera problemas de estabilidad en los circuitos electrónicos y provoca daños en los equipos (Villafuerte Ávila, 2021). Además, la falta de estrategias óptimas para la compensación reactiva en los sistemas eléctricos puede generar pérdidas energéticas significativas, disminuyendo la eficiencia operativa de las infraestructuras (Velasco et al., 2023). Por otro lado, la creciente digitalización ha llevado a una mayor integración de sistemas electrónicos embebidos en infraestructuras críticas, lo que a su vez incrementa la vulnerabilidad a ataques cibernéticos y fallos operativos (Giler Cevallos, 2021). Estas afectaciones no solo comprometen la continuidad del servicio, sino que también pueden generar costos económicos elevados y poner en riesgo la seguridad de los datos y la integridad de los procesos industriales.

La importancia de abordar estos desafíos radica en la necesidad de garantizar la resiliencia de los sistemas eléctricos en infraestructuras críticas. La optimización de la compensación reactiva, el análisis de señales en circuitos electrónicos y la implementación de sistemas de monitoreo avanzados son estrategias fundamentales para mejorar la estabilidad y eficiencia de estas redes (Velasco et al., 2023). Asimismo, la implementación de tecnologías emergentes como la inteligencia artificial y el aprendizaje automático en el análisis y predicción de fallos en los sistemas eléctricos podría proporcionar soluciones efectivas para fortalecer la confiabilidad operativa de estas infraestructuras. La presente revisión bibliográfica busca consolidar información relevante sobre estrategias y metodologías empleadas en la mejora de la seguridad y confiabilidad de los sistemas eléctricos en infraestructuras digitales críticas, proporcionando una base teórica para futuras investigaciones y aplicaciones prácticas en el sector.

Desde un punto de vista metodológico, este estudio se fundamenta en la recopilación y análisis de fuentes científicas que abordan la optimización de sistemas eléctricos y el desarrollo de tecnologías de monitoreo y control en infraestructuras críticas. La viabilidad de la investigación radica en la accesibilidad a literatura científica de alto impacto, así como en la creciente disponibilidad de herramientas y metodologías que permiten evaluar la estabilidad de los sistemas eléctricos en entornos digitales. Al analizar estudios previos sobre compensación reactiva, señales en circuitos electrónicos

y aplicaciones de microcontroladores en sistemas eléctricos, se pretende identificar patrones y tendencias que contribuyan al desarrollo de soluciones innovadoras y eficientes en este ámbito (Giler Cevallos, 2021; Villafuerte Ávila, 2021).

El objetivo principal de esta investigación es analizar el estado del arte en torno a la seguridad y confiabilidad de los sistemas eléctricos en infraestructuras digitales críticas, con énfasis en estrategias de optimización, detección de fallos y mitigación de riesgos. A través de una revisión bibliográfica exhaustiva, se busca identificar los principales desafíos y avances tecnológicos en este campo, así como proponer líneas de investigación futuras que permitan fortalecer la resiliencia de estos sistemas ante escenarios adversos. Esta investigación no solo contribuye al conocimiento teórico sobre el tema, sino que también proporciona información valiosa para la formulación de políticas y estrategias destinadas a mejorar la seguridad y confiabilidad de los sistemas eléctricos en entornos digitales de alta criticidad.

2. Materiales y Métodos

El presente estudio se desarrolla bajo un enfoque exploratorio y se basa en un análisis bibliográfico exhaustivo de fuentes científicas y académicas especializadas en la seguridad y confiabilidad de los sistemas eléctricos en infraestructuras digitales críticas. La metodología empleada tiene como objetivo identificar, analizar y sintetizar la información disponible en la literatura con el fin de comprender el estado actual del conocimiento en esta área y destacar los principales avances, desafíos y tendencias tecnológicas.

Para la selección de las fuentes, se consideraron artículos científicos, tesis académicas y publicaciones indexadas en bases de datos reconocidas, priorizando aquellas que abordan temáticas relacionadas con la optimización de sistemas eléctricos, la detección de fallos en infraestructuras digitales y las estrategias de mitigación de riesgos. Se establecieron criterios de inclusión y exclusión con el propósito de garantizar la pertinencia y calidad de los documentos analizados. Entre los criterios de inclusión, se seleccionaron estudios publicados en los últimos años que presentaran metodologías rigurosas y aplicables al contexto de infraestructuras digitales críticas. Como criterio de exclusión, se descartaron fuentes con información desactualizada, de baja fiabilidad o sin una fundamentación teórica y metodológica clara.

El proceso de recolección de datos se llevó a cabo mediante la consulta de bases de datos académicas y repositorios institucionales, empleando palabras clave estratégicas relacionadas con la temática de estudio. Una vez recopiladas las fuentes pertinentes, se realizó un análisis cualitativo de los contenidos, identificando patrones, similitudes y diferencias en las perspectivas de los distintos autores. Posteriormente, se llevó a cabo una clasificación de los hallazgos en función de su relevancia, aplicabilidad y contribución al conocimiento en el área de la seguridad y confiabilidad de los sistemas eléctricos.

Para la organización de la información, se utilizó una matriz de análisis que permitió estructurar los principales aportes de cada fuente en categorías temáticas. Esta estrategia facilitó la comparación de resultados y la identificación de enfoques innovadores que pueden servir como referencia para futuras investigaciones. Además,

se realizó un proceso de síntesis y discusión de los hallazgos con el fin de establecer relaciones entre los diferentes estudios y proponer líneas de investigación emergentes.

Dado el carácter exploratorio del estudio, no se llevó a cabo la recolección de datos empíricos ni la aplicación de metodologías experimentales. En su lugar, el análisis se centró en la interpretación y discusión de información previamente documentada, lo que permitió generar un marco teórico sólido sobre la temática abordada. La validez del estudio se fundamenta en la rigurosidad del proceso de selección y análisis de las fuentes, asegurando que las conclusiones obtenidas reflejen una visión integral y actualizada del estado del arte en seguridad y confiabilidad de los sistemas eléctricos en infraestructuras digitales críticas.

3. Resultados

3.1. Estrategias de optimización para la confiabilidad en sistemas eléctricos

La confiabilidad en los sistemas eléctricos que sustentan infraestructuras digitales críticas es un factor determinante para la continuidad operativa y la seguridad de los servicios tecnológicos. La creciente digitalización de los procesos industriales, financieros y gubernamentales ha incrementado la dependencia de redes eléctricas estables y eficientes, por lo que es esencial desarrollar estrategias de optimización que minimicen el impacto de fallos y fluctuaciones energéticas. En este contexto, la implementación de metodologías para la compensación reactiva y la integración de modelos de predicción basados en inteligencia artificial y aprendizaje automático han emergido como soluciones clave para mejorar la estabilidad y eficiencia del suministro eléctrico en entornos críticos.

Uno de los principales desafíos en la confiabilidad de los sistemas eléctricos es la gestión de la potencia reactiva, la cual puede generar pérdidas energéticas significativas si no se administra adecuadamente. La compensación reactiva permite optimizar el factor de potencia del sistema eléctrico, reduciendo las pérdidas de energía y mejorando la estabilidad de la red. Entre las metodologías más utilizadas para este propósito se encuentran la instalación de bancos de condensadores, dispositivos de compensación estática y tecnologías avanzadas de regulación de voltaje, las cuales ajustan de manera dinámica la distribución de la energía reactiva en función de la demanda del sistema. Estudios recientes han demostrado que la correcta implementación de estas tecnologías no solo incrementa la eficiencia operativa de las infraestructuras eléctricas, sino que también contribuye a prolongar la vida útil de los equipos al reducir el estrés eléctrico en los componentes críticos del sistema (Betancourt Proaño, 2023).

Además, la digitalización y automatización de los procesos de supervisión energética han permitido optimizar aún más la compensación reactiva mediante el uso de modelos predictivos avanzados. La integración de herramientas de monitoreo en tiempo real basadas en tecnologías de inteligencia artificial facilita la identificación de patrones de consumo y fluctuaciones en la calidad del suministro eléctrico. Estos modelos, al analizar grandes volúmenes de datos, pueden anticipar variaciones en la demanda energética y ajustar automáticamente los mecanismos de compensación reactiva para garantizar una operación más eficiente y estable. En este sentido, se han desarrollado estrategias que combinan técnicas de aprendizaje automático con redes neuronales

artificiales para mejorar la precisión en la predicción de fallos y optimizar el uso de los recursos eléctricos disponibles (Betancourt Proaño, 2023).

Otro enfoque clave para fortalecer la confiabilidad de los sistemas eléctricos es la implementación de modelos de predicción de fallos mediante inteligencia artificial y aprendizaje automático. Estas tecnologías han demostrado ser altamente eficaces en la detección temprana de anomalías en la red eléctrica, permitiendo una respuesta proactiva ante posibles fallos que podrían comprometer la operatividad de infraestructuras digitales críticas. A través del análisis de datos históricos y la identificación de patrones de comportamiento en la red, los modelos predictivos pueden anticipar fallas en transformadores, variaciones anómalas en la calidad de la energía y posibles interrupciones en el suministro. Este enfoque resulta fundamental para la gestión del mantenimiento preventivo, ya que permite reducir costos operativos y minimizar el impacto de cortes de energía inesperados (Castro Thompson, Ramírez Molina, Salazar Carmona & Pablo Olivares, 2021).

Asimismo, la aplicación de estos modelos predictivos no solo mejora la confiabilidad del sistema eléctrico, sino que también fortalece la seguridad de la infraestructura digital. La creciente interconectividad de los sistemas eléctricos con plataformas digitales de monitoreo y control los ha hecho vulnerables a amenazas cibernéticas que pueden comprometer su estabilidad. En este sentido, la inteligencia artificial puede utilizarse no solo para la predicción de fallos físicos en la red, sino también para la detección de patrones sospechosos que podrían indicar la presencia de ataques informáticos dirigidos a los sistemas de gestión eléctrica. La combinación de estas estrategias con auditorías de seguridad y estándares de preservación digital ha demostrado ser una práctica efectiva para mitigar los riesgos asociados a la operación de infraestructuras críticas (Bodero Poveda, De Giusti & Morales, 2022).

Además, la optimización de la confiabilidad en los sistemas eléctricos requiere la implementación de modelos de preservación y planificación estratégica que aseguren la sostenibilidad a largo plazo de la infraestructura. La gestión eficiente de la energía eléctrica debe ir acompañada de estándares de operación y auditoría que permitan evaluar la madurez de los sistemas eléctricos y su capacidad de respuesta ante escenarios de riesgo. En este contexto, las metodologías basadas en el modelo de referencia OAIS (Open Archival Information System) han sido aplicadas en diversos sectores para estructurar planes de preservación digital y garantizar la disponibilidad de información crítica en entornos altamente dinámicos. Estos modelos pueden adaptarse a la gestión de sistemas eléctricos, proporcionando un marco de referencia para la planificación y optimización de los recursos energéticos en infraestructuras digitales críticas (Ochoa-Gutiérrez, Giraldo & Tamayo, 2021).

En conclusión, la confiabilidad en los sistemas eléctricos de infraestructuras digitales críticas puede mejorarse significativamente mediante la implementación de estrategias de optimización que incluyan metodologías avanzadas de compensación reactiva y modelos de predicción de fallos basados en inteligencia artificial. La integración de tecnologías de monitoreo en tiempo real, la aplicación de estándares de seguridad y la planificación estratégica de la gestión energética son factores clave para garantizar la estabilidad y eficiencia de estos sistemas. No obstante, para lograr una implementación efectiva de estas estrategias, es necesario continuar desarrollando investigaciones que

permitan adaptar estas soluciones a los requerimientos específicos de cada entorno digital y eléctrico.

3.2. Impacto de la variabilidad del suministro eléctrico en infraestructuras digitales

Las infraestructuras digitales dependen de un suministro eléctrico estable y confiable para garantizar su operatividad continua. Sin embargo, la variabilidad en la calidad de la energía representa un desafío significativo que puede afectar la estabilidad de los sistemas electrónicos, generando fallos en el equipamiento, interrupciones en los servicios y pérdida de datos. Las fluctuaciones en el voltaje, la presencia de armónicos, las caídas de tensión y los transitorios eléctricos pueden comprometer la integridad de los sistemas, lo que hace necesario el desarrollo de estrategias para mitigar estos efectos y garantizar un suministro de energía estable.

Tabla 1

Estrategias para mitigar el impacto de las fluctuaciones en la calidad del suministro eléctrico en infraestructuras digitales

Estrategia	Descripción	Beneficios	Tecnologías involucradas
Monitoreo y control en redes eléctricas	Implementación de sistemas de protección avanzada y algoritmos adaptativos para detectar anomalías y ajustar dinámicamente la respuesta del sistema.	Reducción de fallos en el suministro, mejora en la identificación temprana de problemas y optimización del uso energético.	Redes de protección avanzada, algoritmos de control adaptativo, sensores de medición sincronizada.
Monitoreo térmico y visual	Uso de drones y sensores infrarrojos para inspeccionar la infraestructura eléctrica y detectar puntos críticos antes de fallos.	Prevención de interrupciones, identificación de sobrecalentamientos y reducción del tiempo de respuesta ante incidentes.	Drones con sensores infrarrojos, cámaras térmicas, análisis de imágenes con inteligencia artificial.
Almacenamiento de energía	Implementación de baterías de iones de litio y supercondensadores para estabilizar la red y proporcionar energía de respaldo.	Mitigación de fluctuaciones, continuidad operativa en caso de cortes eléctricos y optimización del consumo energético.	Baterías de iones de litio, supercondensadores, sistemas de almacenamiento distribuido.
Integración de energías renovables y	Uso de estándares como la norma IEC 61850 para facilitar la	Mayor estabilidad del suministro, reducción de la dependencia de	Norma IEC 61850, sistemas de gestión de redes inteligentes,

Estrategia	Descripción	Beneficios	Tecnologías involucradas
modelos interoperables	integración de fuentes renovables en la red eléctrica.	fuentes convencionales y mejora en la gestión energética.	integración de energías renovables.
Sistemas de monitoreo a gran escala	Aplicación de tecnologías de medición y control en redes eléctricas para mejorar la detección temprana de fallos y optimizar la distribución de la energía.	Mejora en la confiabilidad operativa, optimización de la distribución eléctrica y reducción del impacto de fluctuaciones en la red.	Sensores de medición sincronizada, inteligencia artificial, sistemas SCADA.

Nota: La tabla presenta un análisis de las estrategias tecnológicas y operativas utilizadas para reducir el impacto de las variaciones en la calidad de la energía en infraestructuras digitales críticas. Se incluyen los principales enfoques, sus beneficios y las tecnologías involucradas.

El análisis de las estrategias para mitigar el impacto de las fluctuaciones en la calidad del suministro eléctrico en infraestructuras digitales demuestra la importancia de un enfoque integral basado en monitoreo avanzado, almacenamiento de energía y control inteligente de redes. La combinación de sensores de medición sincronizada, algoritmos adaptativos y sistemas de protección avanzada permite mejorar la estabilidad del suministro y reducir la vulnerabilidad de las infraestructuras críticas ante variaciones en la calidad de la energía. Además, la incorporación de tecnologías emergentes, como la inteligencia artificial y la integración de fuentes renovables, facilita una gestión más eficiente del suministro eléctrico, optimizando el consumo y garantizando la operatividad de los sistemas digitales.

Uno de los principales efectos de las fluctuaciones en la calidad de la energía es la inestabilidad de los sistemas electrónicos. Las variaciones en el voltaje y la frecuencia pueden causar sobrecargas en los dispositivos eléctricos, reduciendo su vida útil y generando fallas en el procesamiento de datos en infraestructuras digitales críticas. La implementación de algoritmos adaptativos para la protección contra sobrecorriente ha demostrado ser una estrategia efectiva para minimizar el impacto de estas fluctuaciones, ya que permite detectar anomalías en el suministro y ajustar dinámicamente la protección de los equipos. Estudios han demostrado que los sistemas de monitoreo y control basados en redes de protección avanzadas pueden mejorar significativamente la respuesta ante variaciones inesperadas en la calidad del suministro eléctrico, permitiendo una rápida identificación y corrección de fallos antes de que afecten la operatividad del sistema (Montoya-Arias, Tobar-Rosero, Zapata-Madrigal & García-Sierra, 2019).

Asimismo, la inestabilidad del suministro eléctrico puede comprometer la eficiencia operativa de los sistemas de distribución y subtransmisión de energía. La implementación de diagnósticos visuales y térmicos mediante el uso de tecnologías

avanzadas, como drones equipados con sensores infrarrojos, ha permitido identificar puntos críticos en la infraestructura eléctrica y prevenir fallos antes de que se conviertan en interrupciones del servicio. Este tipo de monitoreo ha resultado especialmente útil en redes de alta demanda energética, donde cualquier anomalía en la distribución puede generar impactos significativos en infraestructuras digitales críticas, como centros de datos y redes de telecomunicaciones (Varas Alava, 2022).

Para mitigar el impacto de las fluctuaciones en el suministro eléctrico, se han desarrollado soluciones basadas en el almacenamiento de energía y sistemas de respaldo. Los sistemas de almacenamiento, como baterías de iones de litio y supercondensadores, han demostrado ser eficaces para estabilizar la red eléctrica y proporcionar energía de respaldo en caso de interrupciones. Estos sistemas pueden integrarse con tecnologías de monitoreo en tiempo real, permitiendo una gestión eficiente del suministro eléctrico y optimizando el consumo energético en infraestructuras digitales críticas. Además, el desarrollo de sistemas de control basados en modelos de intercambio de datos interoperables, como los definidos por la norma IEC 61850, facilita la integración de fuentes de energía renovable en la red eléctrica, mejorando la estabilidad del sistema ante fluctuaciones en la demanda y el suministro (Yongli, Dewen, Yan & Wenqing, 2009).

Otro enfoque para garantizar la continuidad del suministro eléctrico en infraestructuras digitales es el uso de sistemas de monitoreo a gran escala basados en tecnologías de protección y control en redes eléctricas. Las técnicas de monitoreo en áreas extensas han permitido mejorar la detección temprana de fallos en la red y optimizar la distribución de la energía en función de la demanda. La implementación de tecnologías de protección avanzada en redes de energía eléctrica ha facilitado la identificación de vulnerabilidades en el sistema y la implementación de estrategias de control en tiempo real para mitigar el impacto de las fluctuaciones en la calidad de la energía. En este sentido, el desarrollo de herramientas de monitoreo de amplio alcance, como sensores de medición sincronizada y sistemas de control basados en inteligencia artificial, ha permitido mejorar la confiabilidad operativa de infraestructuras digitales críticas, garantizando un suministro eléctrico estable y seguro (Terzija et al., 2011).

En síntesis, la variabilidad en la calidad del suministro eléctrico representa un desafío significativo para la estabilidad de infraestructuras digitales críticas. La implementación de estrategias de protección avanzadas, el uso de tecnologías de monitoreo térmico y visual, y la integración de sistemas de almacenamiento de energía han demostrado ser soluciones efectivas para mitigar los efectos negativos de las fluctuaciones eléctricas. Además, el desarrollo de modelos de monitoreo a gran escala y la aplicación de estándares de interoperabilidad han permitido optimizar la distribución y control de la energía en entornos digitales altamente exigentes. La combinación de estas estrategias es fundamental para garantizar la operatividad continua de las infraestructuras digitales y minimizar los riesgos asociados a la inestabilidad del suministro eléctrico.

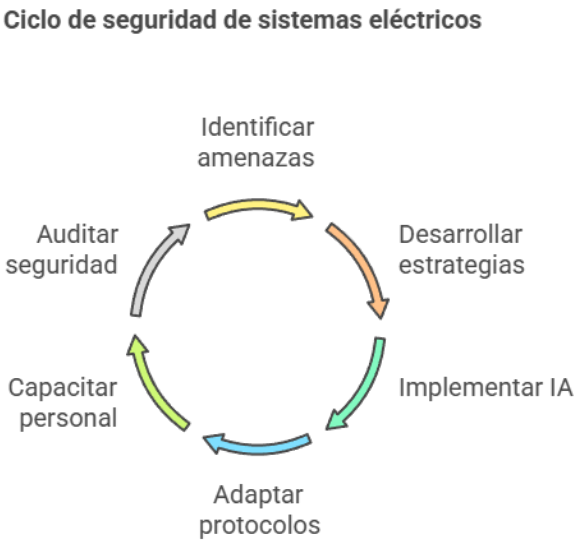
3.3. Seguridad en sistemas eléctricos y vulnerabilidades en entornos digitales

La seguridad en los sistemas eléctricos que sustentan infraestructuras digitales críticas es un aspecto fundamental en la era de la transformación digital. A medida que estos sistemas dependen cada vez más de tecnologías conectadas, su vulnerabilidad ante amenazas cibernéticas se incrementa, lo que puede comprometer la integridad y

continuidad del suministro eléctrico. La identificación de amenazas y el desarrollo de estrategias de ciberseguridad son esenciales para fortalecer la resiliencia de estos sistemas frente a ataques externos y fallos operativos.

Figura 1

Ciclo de seguridad en sistemas eléctricos



Nota: La figura representa un ciclo continuo de seguridad en sistemas eléctricos, abarcando desde la identificación de amenazas hasta la auditoría de seguridad. Cada fase es clave para garantizar la protección y eficiencia del sistema.

Uno de los principales riesgos en los sistemas eléctricos modernos es la creciente exposición a ataques cibernéticos. La digitalización de la infraestructura eléctrica, con la implementación de sistemas de monitoreo en tiempo real y redes de control automatizadas, ha facilitado la operación eficiente de estos sistemas, pero también ha abierto nuevas brechas de seguridad. Los ataques dirigidos a infraestructuras críticas pueden manifestarse en diferentes formas, como intrusiones en redes de control industrial, manipulación de datos operativos y sabotaje de sistemas de protección. En este sentido, la inteligencia artificial ha demostrado ser una herramienta clave en la identificación y mitigación de amenazas cibernéticas, al permitir la detección temprana de patrones anómalos y la automatización de respuestas ante incidentes de seguridad (Erazo-Luzuriaga, Ramos-Secaira, Galarza-Sánchez & Boné-Andrade, 2023).

La implementación de esquemas de protección dinámica ha sido una de las estrategias más efectivas para garantizar la seguridad en entornos digitales de sistemas eléctricos. Estos esquemas permiten adaptar los protocolos de seguridad en función del análisis en tiempo real del comportamiento de la red, facilitando la detección de intentos de acceso no autorizado y la activación de medidas de contención. La integración de algoritmos avanzados para la gestión de amenazas, combinada con el uso de redes neuronales artificiales y sistemas de aprendizaje automático, ha mejorado significativamente la capacidad de los sistemas eléctricos para prevenir fallos inducidos por ataques cibernéticos. En este contexto, la ciberseguridad no solo debe centrarse en la protección de los datos operativos, sino también en la preservación de la estabilidad

del suministro eléctrico en infraestructuras críticas (Fernández, Carvajal, Uribe, Madrigal & Rosero, 2023).

Otro aspecto clave en la seguridad de los sistemas eléctricos es la implementación de protocolos de protección ante ataques externos. A medida que los sistemas de distribución y control eléctrico se interconectan con plataformas digitales, se hace imprescindible el desarrollo de estrategias que garanticen la integridad y confidencialidad de los datos. La adopción de normas internacionales de seguridad, el uso de cifrado avanzado en las comunicaciones y la segmentación de redes críticas han demostrado ser enfoques efectivos para reducir el riesgo de ataques cibernéticos. Además, la capacitación del personal en materia de ciberseguridad y la implementación de auditorías de seguridad periódicas son factores determinantes para fortalecer la resiliencia de la infraestructura eléctrica ante amenazas emergentes (Sánchez-Caguana, Philco-Reinozo, Salinas-Arroba & Pico-Lescano, 2024).

El desarrollo de tecnologías innovadoras también ha permitido mejorar la protección de los sistemas eléctricos ante vulnerabilidades digitales. La inteligencia artificial, aplicada al análisis de seguridad, ha facilitado la optimización de los mecanismos de detección de amenazas, permitiendo una respuesta más rápida y eficiente ante incidentes. Asimismo, la integración de tecnologías de automatización y monitoreo avanzado ha transformado la gestión de la seguridad en entornos eléctricos digitales, reduciendo la dependencia de procesos manuales y mejorando la capacidad de reacción ante posibles intrusiones (Silva-Peñafiel, Castillo-Parra, Tixi-Gallegos & Urgiles-Rodríguez, 2024).

Para concluir, la seguridad en los sistemas eléctricos de infraestructuras digitales críticas enfrenta desafíos significativos debido al incremento de amenazas cibernéticas y vulnerabilidades en entornos digitales. La implementación de esquemas de protección dinámicos, la adopción de protocolos de seguridad avanzados y el uso de inteligencia artificial para la detección de amenazas han demostrado ser estrategias clave para fortalecer la resiliencia de estos sistemas. Sin embargo, la evolución constante de los riesgos cibernéticos requiere una actualización continua de las medidas de seguridad y una mayor inversión en tecnologías innovadoras que permitan garantizar la integridad y confiabilidad de la infraestructura eléctrica en el futuro.

4. Discusión

La seguridad y confiabilidad de los sistemas eléctricos en infraestructuras digitales críticas constituyen un desafío multifacético que requiere un enfoque integral basado en la optimización energética, la mitigación de interrupciones y el fortalecimiento de la ciberseguridad. La creciente digitalización y automatización de estos sistemas han traído consigo beneficios operativos significativos, pero también han incrementado su vulnerabilidad a fluctuaciones energéticas y amenazas cibernéticas. En este sentido, la presente revisión ha identificado diversas estrategias tecnológicas y metodológicas que contribuyen a mejorar la resiliencia de estas infraestructuras ante escenarios adversos.

Uno de los principales factores que afectan la confiabilidad de los sistemas eléctricos es la variabilidad en la calidad del suministro energético, lo que genera pérdidas de eficiencia y riesgos operacionales en infraestructuras críticas. La compensación reactiva se ha consolidado como una solución clave para mitigar estos problemas, ya que

permite estabilizar los niveles de voltaje y reducir el consumo de potencia reactiva, optimizando así la operación del sistema (Betancourt Proaño, 2023). Sin embargo, la implementación de esta estrategia requiere de una supervisión constante y de modelos predictivos avanzados que permitan ajustar dinámicamente la distribución de la energía en función de la demanda y las condiciones del sistema. En este contexto, el uso de inteligencia artificial y algoritmos de aprendizaje automático ha demostrado ser una herramienta eficiente para mejorar la gestión energética y reducir los impactos negativos de las fluctuaciones eléctricas (Erazo-Luzuriaga, Ramos-Secaira, Galarza-Sánchez & Boné-Andrade, 2023).

La estabilidad de los sistemas electrónicos dentro de infraestructuras digitales críticas depende en gran medida de la continuidad del suministro eléctrico. Las interrupciones y variaciones en la calidad de la energía pueden causar fallos en equipos sensibles, lo que compromete la integridad de la información y la operatividad de los servicios digitales. Para enfrentar estos desafíos, se han desarrollado soluciones basadas en almacenamiento de energía, tales como baterías de iones de litio y sistemas de respaldo híbridos, los cuales han demostrado su efectividad en la estabilización de redes eléctricas de alto consumo (Yongli, Dewen, Yan & Wenqing, 2009). Además, la implementación de técnicas de monitoreo térmico y visual mediante drones ha permitido mejorar la detección temprana de fallos en infraestructuras de distribución y subtransmisión, optimizando los procesos de mantenimiento y reduciendo el riesgo de interrupciones prolongadas (Varas Alava, 2022).

Desde la perspectiva de la ciberseguridad, la integración de sistemas digitales en la infraestructura eléctrica ha aumentado la exposición a amenazas cibernéticas, que pueden comprometer tanto la estabilidad del suministro como la integridad de los datos operativos. En este sentido, la identificación de vulnerabilidades en redes de control industrial y la implementación de esquemas de protección dinámica han sido estrategias fundamentales para mitigar los riesgos asociados a los ciberataques (Fernández, Carvajal, Uribe, Madrigal & Rosero, 2023). La inteligencia artificial ha jugado un papel crucial en la detección y respuesta ante incidentes de seguridad, al permitir el análisis en tiempo real de patrones anómalos y la automatización de protocolos de protección. Asimismo, la adopción de normativas internacionales y la segmentación de redes críticas han demostrado ser enfoques efectivos para garantizar la seguridad en entornos eléctricos interconectados (Sánchez-Caguana, Philco-Reinozo, Salinas-Arroba & Pico-Lescano, 2024).

A pesar de los avances tecnológicos en la optimización y seguridad de los sistemas eléctricos en infraestructuras críticas, persisten desafíos que requieren una evolución constante de las estrategias de mitigación de riesgos. La creciente complejidad de los sistemas eléctricos interconectados exige una mayor integración de herramientas avanzadas de monitoreo, control y predicción, con el fin de mejorar la capacidad de respuesta ante eventos adversos. En este sentido, el desarrollo de tecnologías emergentes, como la inteligencia artificial y los sistemas de análisis de big data, se perfila como una solución prometedora para fortalecer la resiliencia de estas infraestructuras y garantizar su operatividad en escenarios de alta demanda energética y riesgos cibernéticos (Silva-Peñafiel, Castillo-Parra, Tixi-Gallegos & Urgiles-Rodríguez, 2024).

Para resumir, la seguridad y confiabilidad de los sistemas eléctricos en infraestructuras digitales críticas dependen de un enfoque multidimensional que abarque la optimización de la eficiencia energética, la implementación de soluciones de almacenamiento y respaldo, y el desarrollo de estrategias avanzadas de ciberseguridad. La combinación de estas estrategias con tecnologías innovadoras permitirá no solo mejorar la estabilidad operativa de estos sistemas, sino también anticipar y mitigar los riesgos derivados de fluctuaciones energéticas y amenazas digitales. No obstante, para garantizar la efectividad de estas soluciones, es fundamental continuar promoviendo la investigación en este campo y la adopción de estándares tecnológicos que aseguren la sostenibilidad y seguridad de la infraestructura eléctrica en el futuro.

5. Conclusiones

La seguridad y confiabilidad en los sistemas eléctricos de infraestructuras digitales críticas representan un pilar fundamental para garantizar la estabilidad y operatividad de múltiples sectores estratégicos. La creciente digitalización y automatización de estos sistemas han mejorado significativamente la eficiencia energética y la gestión operativa, pero también han incrementado la vulnerabilidad ante fluctuaciones en la calidad del suministro eléctrico y amenazas cibernéticas. En este sentido, es imprescindible desarrollar estrategias avanzadas que permitan optimizar la gestión energética, fortalecer la resiliencia de los sistemas ante interrupciones y mitigar los riesgos asociados a ataques externos.

La optimización de los sistemas eléctricos es un componente clave para garantizar su confiabilidad y eficiencia. La compensación reactiva y la reducción de pérdidas energéticas han demostrado ser estrategias eficaces para mejorar la estabilidad de la red y minimizar el impacto de fluctuaciones en la calidad de la energía. Estas técnicas permiten ajustar dinámicamente la distribución de la energía y optimizar el uso de los recursos disponibles, lo que se traduce en una mayor eficiencia operativa y una reducción en el desgaste de los componentes eléctricos. Sin embargo, la correcta implementación de estos mecanismos requiere un monitoreo constante y el uso de modelos predictivos avanzados que faciliten la detección temprana de posibles fallos en la red.

Por otro lado, la variabilidad en el suministro eléctrico continúa representando una amenaza para las infraestructuras digitales críticas, ya que cualquier interrupción en la energía puede afectar la operatividad de sistemas esenciales, desde centros de datos hasta plataformas industriales automatizadas. La implementación de soluciones basadas en almacenamiento de energía y sistemas de respaldo ha sido una estrategia efectiva para mitigar estos riesgos. Tecnologías como baterías de alta capacidad, supercondensadores y sistemas híbridos han permitido mejorar la continuidad del suministro eléctrico, asegurando que los sistemas críticos puedan seguir funcionando incluso en escenarios de contingencia. No obstante, es necesario seguir avanzando en el desarrollo de estas tecnologías y en su integración con fuentes de energía renovable, con el fin de garantizar la sostenibilidad del suministro y reducir la dependencia de fuentes convencionales.

La seguridad cibernética se ha convertido en un factor determinante en la protección de los sistemas eléctricos en infraestructuras digitales. La interconectividad de estos sistemas con plataformas digitales ha incrementado la exposición a ataques cibernéticos que pueden comprometer la integridad de los datos operativos y la estabilidad del suministro energético. Para abordar estos desafíos, es fundamental implementar esquemas de protección dinámicos, el uso de inteligencia artificial para la detección de amenazas y la adopción de normativas de seguridad avanzadas. La automatización de la detección y respuesta ante incidentes de ciberseguridad ha permitido mejorar la resiliencia de los sistemas eléctricos, reduciendo el tiempo de respuesta ante posibles intrusiones y minimizando el impacto de ataques dirigidos. Sin embargo, el panorama de amenazas evoluciona constantemente, por lo que es crucial mantener una actualización continua de los protocolos de seguridad y promover una cultura organizacional enfocada en la ciberseguridad.

El desarrollo de infraestructuras eléctricas resilientes requiere un enfoque integral que combine tecnologías avanzadas, estrategias de gestión eficiente y medidas de seguridad robustas. La integración de inteligencia artificial, big data y sistemas de monitoreo en tiempo real ha permitido optimizar la operación y mantenimiento de estos sistemas, asegurando una mayor confiabilidad y reducción de riesgos. A pesar de estos avances, es necesario continuar investigando y desarrollando soluciones innovadoras que permitan anticipar y mitigar posibles amenazas, tanto en el ámbito energético como en el de la seguridad informática.

En el futuro, la evolución de las infraestructuras eléctricas estará marcada por la convergencia de la automatización, la inteligencia artificial y las energías renovables. La capacidad de adaptación de estos sistemas a los cambios tecnológicos y regulatorios será determinante para garantizar su sostenibilidad y eficiencia a largo plazo. Además, la colaboración entre el sector público, la industria y el ámbito académico será clave para fomentar la investigación y el desarrollo de soluciones que permitan afrontar los retos emergentes en materia de seguridad y confiabilidad eléctrica.

En conclusión, la seguridad y confiabilidad de los sistemas eléctricos en infraestructuras digitales críticas es un desafío complejo que exige un enfoque multidisciplinario. La optimización energética, el almacenamiento eficiente de energía y el fortalecimiento de la ciberseguridad son elementos fundamentales para garantizar la estabilidad operativa de estos sistemas. Si bien se han logrado avances significativos en estas áreas, el dinamismo del entorno tecnológico y la creciente sofisticación de las amenazas requieren una mejora continua en las estrategias de gestión y protección. La implementación de soluciones innovadoras y la adopción de estándares internacionales de seguridad serán determinantes para asegurar la resiliencia de estas infraestructuras y su capacidad de respuesta ante los desafíos del futuro.

Referencias Bibliográficas

Betancourt Proaño, D. A. (2023). *Análisis de la trayectoria de la impedancia de falla vista por el relé de distancia en sistemas eléctricos ante oscilaciones de potencia* (Master's thesis). http://dspace.ups.edu.ec/handle/123456789/26516

Bodero Poveda, E., De Giusti, M. R., & Morales, C. (2022). Preservación digital a largo plazo: estándares, auditoría, madurez y planificación estratégica. *Revista Interamericana de Bibliotecología*, *45*(2). https://doi.org/10.17533/udea.rib.v45n2e344178

Castro Thompson, A., Ramírez Molina, A. Y., Salazar Carmona, J. A., & Pablo Olivares, L. (2021). Estrategias de preservación digital: casos de estudio. *Biblioteca universitaria*, *24*(1), 13-25. https://biblat.unam.mx/hevila/Bibliotecauniversitaria/2021/vol24/no1/3.pdf

Erazo-Luzuriaga, A. F., Ramos-Secaira, F. M., Galarza-Sánchez, P. C., & Boné-Andrade, M. F. (2023). La inteligencia artificial aplicada a la optimización de programas informáticos. Journal of Economic and Social Science Research, 3(1), 48–63. https://doi.org/10.55813/gaea/jessr/v3/n1/61

Fernández, J. S. C., Carvajal, G. D. R., Uribe, C. A. M., Madrigal, G. D. Z., & Rosero, Ó. A. T. (2023). Esquema dinámico de protección en un entorno digital de sistemas eléctricos. *Encuentro Internacional de Educación en Ingeniería*. https://doi.org/10.26507/paper.3369

Galarza-Sánchez, P. C., Agualongo-Yazuma, J. C., & Jumbo-Martínez, M. N. (2022). Innovación tecnológica en la industria de restaurantes del Cantón Pedro Vicente Maldonado. Journal of Economic and Social Science Research, 2(1), 31–43. https://doi.org/10.55813/gaea/jessr/v2/n1/45

GILER CEVALLOS, K. K. (2021). *Sistemas electrónicos embebidos con microcontroladores PIC para mejorar la enseñanza de Electrónica Digital en la Carrera de Tecnologías de la Información de la Universidad Estatal del Sur de Manabí* (Bachelor's thesis, Jipijapa. UNESUM). https://repositorio.unesum.edu.ec/bitstream/53000/3390/1/KIMBERLY%20KARINA%20GILER%20CEVALLLOS.pdf

Montoya-Arias, J. A., Tobar-Rosero, O. A., Zapata-Madrigal, G. D., & García-Sierra, R. (2019). Algoritmo adaptativo para protecciones de sobrecorriente en el caso de estudio IEEE9. TecnoLógicas, 22(45), 45–58. https://doi.org/10.22430/22565337.1335

Ochoa-Gutiérrez, J., Giraldo, R. A. S., & Tamayo, T. T. (2021, March). Experiencias de gestión de los procesos de preservación digital a partir del modelo OAIS en repositorios institucionales. In *Anales de Documentación* (Vol. 24, No. 1). Facultad de Comunicación y Documentación y Servicio de Publicaciones de la Universidad de Murcia. https://doi.org/10.6018/analesdoc.428141

Sánchez-Caguana, D. F., Philco-Reinozo, M. A., Salinas-Arroba, J. M., & Pico-Lescano, J. C. (2024). Impacto de la Inteligencia Artificial en la Precisión y Eficiencia de los Sistemas Contables Modernos. Journal of Economic and Social Science Research, 4(3), 1–12. https://doi.org/10.55813/gaea/jessr/v4/n3/117

Silva-Peñafiel, G. E., Castillo-Parra, B. F., Tixi-Gallegos, K. G., & Urgiles-Rodríguez, B. E. (2024). La Revolución de la Inteligencia Artificial en la Educación Superior. Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.71

Terzija, V., Valverde, G., Cai, D., Regulski, P., Madani, V., Fitch, J., Skok, S., Begovic, M. M., & Phadke, A. (2011). Wide-area monitoring, protection, and control of future electric power networks. Proceedings of the IEEE, 99(1), 80–93. https://doi.org/10.1109/JPROC.2010.2060450

Varas Alava, J. A. (2022). *Diagnóstico Visual-térmico en sistemas eléctricos de subtransmisión y distribución con el uso de drones para efectuar*

mantenimientos (Bachelor's thesis). http://dspace.ups.edu.ec/handle/123456789/22503

Velasco, A. N. C., Fiallos, J. N. C., Caiza, C. I. Q., & Collaguazo, E. F. G. (2023). Optimización de la compensación reactiva en sistemas eléctricos por el método CRITIC. *Ciencia digital*, *7*(2), 64-81. https://doi.org/10.33262/cienciadigital.v7i2.2540

Velasco, A. N. C., Fiallos, J. N. C., Caiza, C. I. Q., & Collaguazo, E. F. G. (2023). Optimización de la compensación reactiva en sistemas eléctricos por el método CRITIC. *Ciencia digital*, *7*(2), 64-81. https://doi.org/10.33262/cienciadigital.v7i2.2540

VILLAFUERTE AVILA, D. K. (2021). *Análisis De Señales De Ondas En Circuitos Electrónicos Digitales Mediante Simulador Virtual Para El Laboratorio De Electrónica De La Carrera De Ingeniería En Computación Y Redes* (Bachelor's thesis, Jipijapa. UNESUM). http://repositorio.unesum.edu.ec/handle/53000/3057

Yongli, Z., Dewen, W., Yan, W., & Wenqing, Z. (2009). Study on Interoperable Exchange of IEC 61850 Data Model. 4031. https://doi.org/10.1109/ICIEA.2009.5138698

Zapata-Mendoza, P. C. O., Villalta-Arellano, S. R., Berrios-Zevallos, A. A., Atto-Coba, S. R., & Berrios-Tauccaya, O. J. (2023). *Sostenibilidad ambiental en el diseño arquitectónico de plantas procesadoras de alimentos.* Editorial Grupo AEA. https://doi.org/10.55813/egaea.l.2022.59

CONFLICTO DE INTERESES

“Los autores declaran no tener ningún conflicto de intereses”.