Intelética 1(2) (2024), 27-50
Revista de Inteligencia Artificial, Ética y Sociedad

INTELETICA

https://inteletica.iberamia.org/

Marco de Gerencia de Proyectos para la Implementación Ética y Segura de Soluciones de Inteligencia Artificial en Redes Eléctricas con Integración de IoT

Luis Ferney Ortiz Torres [1], Luis Alberto Cárdenas Otaya [2]

[1] Investigador independiente.
[2] Corporación Universitaria Minuto de Dios – Minuto de DIOS.

[1] luis.ortiz-torr@uniminuto.edu.co
[2] luis.cardenas.o@uniminuto.edu.co

"Artículo revisado y recomendada su publicación por el Dr. Dany Mauricio López Santiago Director de I+D+i de la empresa Potencia y Tecnologías Incorporadas S.A. BIC, y por el M.Sc. Héctor García Arana Coordinador del programa académico Tecnología en Electrónica Industrial en la Universidad del Valle seccional Tuluá".

Abstract This research presents a framework for the ethical and secure implementation of Artificial Intelligence (AI) solutions in the management of power grids, integrating Internet of Things (IoT) devices. The study focuses on ensuring data privacy and security while optimizing the operational efficiency of power grids. Advanced AI techniques are identified, risks and vulnerabilities are assessed, and best practices based on international standards are proposed.

Resumen Esta investigación presenta un marco para la implementación ética y segura de soluciones de Inteligencia Artificial (IA) en la gestión de redes eléctricas, integrando dispositivos del Internet de las Cosas (IoT). El estudio se centra en asegurar la protección de la privacidad y la seguridad de los datos, así como en optimizar la eficiencia operativa de las redes eléctricas. Se identifican técnicas avanzadas de IA, se evalúan riesgos y vulnerabilidades, y se proponen mejores prácticas basadas en estándares internacionales.

Keywords: Artificial Intelligence (AI), Internet of Things (IoT), Data Privacy, Project Management, AI Ethics.

Palabras clave: Inteligencia Artificial (IA), Internet de las Cosas (IoT), Privacidad de Datos, Gestión de Proyectos, Ética de la Inteligencia Artificial.

1 Introducción

En la actualidad, la creciente demanda energética y la necesidad de reducir las emisiones de carbono han impulsado la búsqueda de soluciones innovadoras para optimizar la eficiencia y sostenibilidad de las redes eléctricas. La transición hacia infraestructuras más inteligentes, facilitada por la incorporación de tecnologías como la Inteligencia Artificial (IA) y el Internet de las Cosas (IoT), permite una gestión más efectiva de la distribución de energía y promueve el uso de fuentes renovables. No obstante, esta integración tecnológica plantea importantes desafíos en términos de privacidad, seguridad y gobernanza de datos.

La implementación de IA y IoT en redes eléctricas implica la recolección y procesamiento de grandes volúmenes de datos en tiempo real, lo que expone a las infraestructuras críticas a vulnerabilidades ante posibles ciberataques. Según Rao (2018), la falta de medidas adecuadas de ciberseguridad en redes eléctricas puede aumentar el riesgo de accesos no autorizados y la manipulación de información sensible, generando amenazas significativas a la estabilidad del sistema.

ISSN: 3020-7444

Ante este contexto, el presente estudio propone un marco de gestión de proyectos que aborda la integración ética y segura de soluciones de IA en redes eléctricas, con el fin de mitigar los riesgos asociados y garantizar la protección de la privacidad de los usuarios. Para ello, se identifican técnicas avanzadas de IA, se evalúan los riesgos y vulnerabilidades potenciales, y se sugieren mejores prácticas basadas en estándares internacionales como el Reglamento General de Protección de Datos (GDPR) y el NIST Cybersecurity Framework (McIntosh et al., 2024).

El enfoque propuesto enfatiza la importancia de la gestión estratégica de riesgos y la adaptación de políticas organizacionales que aseguren una implementación ética y eficiente. De esta manera, el artículo contribuye al desarrollo de un modelo de gobernanza que permita a las organizaciones maximizar los beneficios de estas tecnologías sin comprometer la seguridad y el bienestar de los individuos y la sociedad en su conjunto.

1.1 Planteamiento del Problema

1.1.1. Descripción del problema

En la era actual de digitalización y automatización, la integración de soluciones basadas en Inteligencia Artificial (IA) en la gestión de redes eléctricas se ha convertido en un componente fundamental para mejorar la eficiencia operativa y la fiabilidad del suministro de energía. La aplicación de algoritmos de IA permite optimizar la distribución de energía, así como predecir la demanda con mayor precisión, respondiendo de manera más ágil a las fluctuaciones del mercado y a las condiciones operativas variables (Abd Elazim y Ali, 2016). Sin embargo, esta adopción también introduce desafíos significativos relacionados con la privacidad y la seguridad de los datos.

La interconexión de dispositivos del Internet de las Cosas (IoT) y sistemas de monitoreo en entornos residenciales e industriales crea una superficie de ataque ampliada que expone a las redes eléctricas a posibles ciberataques. Según Miraz et al. (2015), el aumento de dispositivos conectados genera vulnerabilidades que pueden ser explotadas para acceder a información sensible, comprometiendo así la estabilidad y la seguridad del sistema.

Por otro lado, Kandukuri et al. (2009) destacan que la IA desempeña un papel crucial en la detección y prevención de fallos en la red eléctrica, contribuyendo significativamente a la reducción de tiempos de inactividad y a la mejora de la calidad del servicio. Sin embargo, la falta de medidas de ciberseguridad adecuadas puede derivar en accesos no autorizados y manipulación de datos críticos (Rao, 2018). A su vez, la implementación de sistemas de IA sin considerar principios éticos puede generar sesgos y decisiones automatizadas que no siempre prioricen el bienestar y la privacidad de los usuarios (Floridi et al., 2018).

Ante este panorama, es necesario desarrollar estrategias de gerencia de proyectos que aseguren una integración ética y segura de soluciones de IA en redes eléctricas. Esto implica no solo la aplicación de prácticas de ciberseguridad, sino también la adopción de principios éticos y normativas internacionales como el Reglamento General de Protección de Datos (GDPR) y el NIST Cybersecurity Framework, para mitigar riesgos y garantizar la protección de la información sensible (McIntosh et al., 2024). La presente investigación aborda estas problemáticas mediante la propuesta de un marco de gerencia de proyectos que facilite la implementación de soluciones de IA, considerando aspectos de privacidad, seguridad y ética, con el fin de maximizar los beneficios tecnológicos al tiempo que se minimizan los riesgos asociados.

1.1.2. La pregunta de investigación

¿Cómo puede un marco de gerencia de proyectos facilitar la integración ética y segura de soluciones de inteligencia artificial (IA) en la gestión de redes eléctricas, abordando los riesgos asociados a la privacidad y la seguridad de datos, especialmente en la implementación de dispositivos del Internet de las Cosas (IoT) en entornos residenciales e industriales?

1.1.3. Los objetivos de investigación

Objetivo general

Establecer un marco de gestión de proyectos para la implementación ética y segura de soluciones de inteligencia artificial en la gestión de redes eléctricas, con un enfoque en la protección de la privacidad y la seguridad de los

datos, particularmente en la integración de dispositivos del Internet de las Cosas (IoT) en entornos residenciales e industriales.

Objetivos específicos

1. Determinar las soluciones de inteligencia artificial más adecuadas para abordar los desafíos específicos de la gestión y optimización de la red eléctrica, considerando los aspectos de privacidad y seguridad de datos.

2. Identificar los riesgos y vulnerabilidades asociados con la integración de dispositivos IoT y sistemas de monitoreo en redes eléctricas, y definir los requisitos de privacidad y seguridad de datos necesarios para garantizar la protección de la información en estos entornos.

3. Evaluar los estándares internacionales y las mejores prácticas aplicables a la implementación ética de soluciones de inteligencia artificial en la gestión de redes eléctricas, con énfasis en la privacidad y seguridad de datos.

4. Desarrollar un marco de gestión de proyectos que integre prácticas de seguridad cibernética y gestión de riesgos en todas las etapas del ciclo de vida del proyecto, desde la definición de requisitos hasta la implementación y operación continua de las soluciones de inteligencia artificial.

1.1.4. Justificación de la investigación

El desarrollo e implementación de soluciones basadas en inteligencia artificial (IA) para la gestión de redes eléctricas representa un avance significativo con el potencial de mejorar la eficiencia operativa y la confiabilidad del suministro energético. Sin embargo, esta integración tecnológica presenta desafíos importantes relacionados con la privacidad y seguridad de los datos, especialmente debido a la creciente interconexión de dispositivos IoT en entornos residenciales e industriales.

El uso de IA en la gestión de redes eléctricas permite optimizar el consumo y distribución de energía, así como predecir la demanda con mayor precisión, lo que contribuye a la sostenibilidad y eficiencia del sistema energético. No obstante, la implementación de estas tecnologías también implica la recolección y análisis de grandes volúmenes de datos en tiempo real, exponiendo a las infraestructuras críticas a vulnerabilidades ante posibles ciberataques (Rao, 2018). En este sentido, se hace necesario desarrollar un marco ético y normativo que garantice la protección de la privacidad y la seguridad de los datos, tal como lo indican Cintuglu et al. (2017) y Floridi et al. (2018), quienes subrayan la necesidad de adoptar estándares internacionales como el Reglamento General de Protección de Datos (GDPR) y el NIST Cybersecurity Framework para asegurar la interoperabilidad y la seguridad de las soluciones de IA.

La presente investigación busca establecer un marco de gerencia de proyectos que integre principios éticos, seguridad cibernética y gestión de riesgos, con el fin de asegurar una implementación efectiva y segura de la IA en redes eléctricas. Este enfoque permitirá a las organizaciones abordar los desafíos técnicos, éticos y regulatorios asociados con la integración de IA y IoT, y garantizará que se maximicen los beneficios tecnológicos sin comprometer la seguridad y el bienestar de los usuarios. Implementar un marco de gestión de proyectos específicamente diseñado para este propósito contribuirá a la protección de la información sensible y a la reducción de riesgos en la adopción de estas tecnologías innovadoras, promoviendo así un desarrollo sostenible en el sector energético.

1.2 Marco de Referencia

1.2.1. Marco de Antecedentes

El marco de referencia de esta investigación abarca una amplia gama de conceptos relacionados con la gerencia de proyectos, tecnología, ética, normativas y protección de datos, con el propósito de ofrecer una visión integral que permita validar la implementación efectiva y ética de soluciones de inteligencia artificial (IA) desde la perspectiva de la gerencia de proyectos. El estado del arte revisa diversas fuentes que subrayan la necesidad de desarrollar marcos éticos sólidos para guiar el diseño y uso de la IA, considerando no solo sus aspectos técnicos, sino también las implicaciones sociales, legales y éticas que surgen de su aplicación.

Es fundamental que las organizaciones evalúen cómo la IA puede impactar los derechos individuales y la autonomía humana. La recopilación y uso de datos personales por sistemas de IA plantea desafíos significativos en términos de privacidad y consentimiento informado. Además, la corrección de sesgos y errores en los algoritmos de toma de decisiones se ha convertido en un área prioritaria de investigación. Como indica la Organización Mundial de la Salud, antes de implementar una nueva herramienta de IA, es esencial desarrollar principios éticos que orienten su uso y adopción, considerando el principio de evitar daños y respetar la autonomía humana.

El análisis de Klockmann et al. (2022) sugiere que para que una IA pueda tomar decisiones en nombre de un individuo o una sociedad, debe comprender sus preferencias. Debido a que el comportamiento humano en interacciones estratégicas está mediado por factores sociales como el altruismo y la reciprocidad, los algoritmos de aprendizaje y modelado de preferencias sociales deben ser diseñados cuidadosamente para evitar malinterpretaciones. Además, Burton (2023) destaca que incluso una IA bien diseñada y entrenada con datos de alta calidad puede ser utilizada de forma maliciosa, lo cual subraya la importancia de implementar medidas de seguridad robustas.

Para que la IA cumpla con su propósito, debe complementarse con herramientas físicas como los sensores, los cuales están enmarcados en el concepto del Internet de las Cosas (IoT). Aunque el IoT es esencial para alcanzar los estándares de la Industria 4.0, también introduce riesgos de seguridad. Según Trilles et al. (2024), una anomalía en el IoT se refiere a un cambio inesperado en el estado de un sistema que se desvía de su comportamiento habitual, lo que puede ocurrir tanto a nivel local como global. Este tipo de incidentes, junto con la clonación de dispositivos y la suplantación de sensores, representa un peligro latente que debe abordarse.

En este sentido, Pathmabandu et al. (2023) indican que, dada la gran cantidad de sensores inteligentes presentes en la vida cotidiana, las personas encuentran difícil gestionar su consentimiento de privacidad de forma efectiva. Además, Davidson (2019) enfatiza que el consentimiento es particularmente problemático en la IA debido a la opacidad inherente de los datos ya recopilados. Asimismo, Haenlein (2020) resalta que dotar a la IA de valores éticos no solo es relevante en sí mismo, sino que es crucial para hacer más transparentes las acciones de las empresas que dependen de estas tecnologías.

Por lo tanto, la implementación de soluciones de IA en la gestión y optimización de redes eléctricas representa una oportunidad significativa para mejorar la eficiencia, resiliencia y seguridad de estas infraestructuras críticas. Sin embargo, esta integración también conlleva desafíos importantes en términos de privacidad y seguridad de los datos. Mohammadi et al. (2018) señalan que las técnicas de aprendizaje profundo han facilitado el desarrollo de sistemas avanzados para predecir la demanda de energía y detectar anomalías, mejorando la eficiencia operativa y la capacidad de respuesta de las redes eléctricas. No obstante, Murugan (2018) alerta que la proliferación de dispositivos IoT incrementa el riesgo de ciberataques con potenciales consecuencias catastróficas.

Chehri et al. (2021) enfatizan la importancia de implementar medidas de seguridad como el cifrado de datos y la autenticación multifactor en las soluciones de IA para proteger la información sensible y mitigar las amenazas cibernéticas. Además, la selección de soluciones que cumplan con certificaciones internacionales, como ISO/IEC 27001, es crucial para garantizar la seguridad y confiabilidad del sistema. A su vez, Babar et al. (2010) sostienen que la definición de controles de seguridad debe abarcar todo el ciclo de vida del proyecto, desde la planificación hasta la operación continua.

Para garantizar una implementación ética y segura de la IA en redes eléctricas, se debe adoptar un marco que combine estándares técnicos y principios éticos, como sugiere Floridi et al. (2018). Esto es necesario para proteger los derechos de los usuarios y mitigar los riesgos asociados con el uso incorrecto de la IA. Además, Cintuglu et al. (2017) recomiendan la adopción de normativas internacionales, como el IEEE 1547 y el NIST Cybersecurity Framework, para asegurar la interoperabilidad y seguridad de las soluciones de IA, proporcionando un conjunto de directrices que garanticen la resiliencia ante ciberataques.

En última instancia, la gestión de riesgos y la planificación estratégica son componentes esenciales para el éxito de estas implementaciones. Según Frame (2003), los marcos de gestión de proyectos deben adaptarse a las características únicas de las tecnologías avanzadas, validando actividades específicas para la identificación, evaluación y mitigación de riesgos, con asignación clara de responsabilidades y plazos. Finalmente, Sommerville (2011) resalta la importancia de integrar prácticas de seguridad cibernética en cada fase del ciclo de vida del

proyecto, desde la definición de requisitos hasta la implementación y operación continua, para asegurar la continuidad y protección de las soluciones de IA.

1.2.2. Marco Teórico

Esta investigación se fundamenta en la teoría de la administración científica de Frederick Winslow Taylor, debido a su influencia histórica, su enfoque en la mejora de la eficiencia y su aplicabilidad interdisciplinaria en la gestión de proyectos tecnológicos. La teoría de Taylor, propuesta a principios del siglo XX, se centra en la optimización de las tareas laborales mediante un análisis científico que busca identificar métodos eficientes y eliminar el desperdicio de tiempo y recursos (Taylor, 1911). Estos principios de gestión han sido ampliamente adoptados en la práctica de la gestión de proyectos, facilitando la planificación, ejecución y control de actividades con el fin de mejorar el desempeño organizacional.

Aplicación de la Teoría de la Administración Científica de Taylor en la Gestión de Proyectos de IA e IoT

La gestión de proyectos enfocados en la implementación de soluciones de inteligencia artificial (IA) en la red eléctrica, que además integran dispositivos del Internet de las Cosas (IoT), se beneficia de los principios de Taylor. El enfoque de eficiencia propuesto por Taylor se adapta bien a la planificación estratégica y operativa de estos proyectos, donde la optimización de procesos y la reducción de ineficiencias son objetivos prioritarios. A continuación, se detallan las principales áreas de aplicación de estos principios en el contexto de la investigación:

- **Análisis de Tiempos y Movimientos:** La aplicación de la técnica de análisis de tiempos y movimientos permite examinar de manera minuciosa los procesos involucrados en la integración de dispositivos IoT y sistemas de monitoreo en entornos residenciales e industriales. Como afirman Gilbreth & Gilbreth (1916), este análisis facilita la identificación de cuellos de botella y la implementación de estrategias más productivas que optimicen la ejecución de tareas (p.34). En el contexto de la IA e IoT, este enfoque es fundamental para diseñar procesos eficientes y prever posibles interrupciones en la operación de las redes eléctricas.

- **Diseño de Métodos Eficientes:** Una vez detectadas las áreas de mejora a través del análisis de tiempos y movimientos, se pueden establecer métodos más eficientes para ejecutar las tareas relacionadas con la integración de soluciones de IA en la gestión de redes eléctricas (Smith, 1794, p.23). Esto incluye la estandarización de procesos y la adopción de mejores prácticas, las cuales pueden ser esenciales para asegurar la consistencia y calidad en la implementación de estas tecnologías emergentes.

- **División del Trabajo:** La asignación clara de responsabilidades a cada miembro del equipo de proyecto, basada en sus habilidades y especializaciones, permite maximizar la eficiencia y reducir los tiempos de ejecución. Según Taylor, la división del trabajo facilita una mayor especialización, lo que se traduce en una ejecución más ágil y una menor redundancia en tareas operativas. Esta práctica es particularmente relevante en proyectos de IA, donde la colaboración de múltiples disciplinas es crucial para el éxito del proyecto.

- **Colaboración entre Gerencia y Trabajadores:** La colaboración estrecha entre la gerencia y los equipos de trabajo es un factor crítico en la implementación de proyectos que involucran tecnología avanzada como la IA y el IoT. Según Mayo (1946), la gerencia debe proporcionar el apoyo y recursos necesarios, mientras que los trabajadores aportan una perspectiva práctica sobre la viabilidad de las soluciones propuestas (p.10). Esta dinámica colaborativa fomenta un entorno donde las ideas se pueden evaluar de manera integral y las soluciones se pueden adaptar de acuerdo con las necesidades identificadas en el campo.

- **Incentivos Salariales Basados en Productividad:** El uso de un sistema de incentivos basado en la productividad no solo motiva a los miembros del equipo a alcanzar los objetivos del proyecto de manera eficiente, sino que también promueve una cultura de alto rendimiento orientada a resultados. Al reconocer y recompensar el desempeño excepcional, se crea un entorno de trabajo donde se valoran las contribuciones individuales y colectivas, mejorando la cohesión del equipo y su compromiso con la ejecución exitosa del proyecto.

En el contexto de esta investigación, los principios de la administración científica de Taylor se aplican para estructurar un marco de gestión que no solo optimice los procesos operativos, sino que también asegure que la implementación de soluciones de IA e IoT en redes eléctricas se lleve a cabo de manera ética, eficiente y segura. Integrar estos principios permite a las organizaciones afrontar los desafíos inherentes a la adopción de tecnologías avanzadas, maximizando el rendimiento operativo sin comprometer la privacidad, seguridad y el bienestar de los usuarios.

1.2.3. Marco Conceptual

Las estrategias de gestión de proyectos para la implementación ética y efectiva de soluciones de inteligencia artificial (IA) en redes eléctricas con dispositivos del Internet de las Cosas (IoT) se basan en varios principios fundamentales. Primero, es esencial establecer políticas claras de privacidad y protección de datos, ya que estas forman la base para un manejo seguro de la información. Además, se deben implementar medidas técnicas robustas, como el cifrado de datos y la autenticación de dispositivos, para proteger los sistemas ante posibles amenazas cibernéticas. La transparencia y la rendición de cuentas son otros aspectos clave que requieren mecanismos de auditoría y supervisión para monitorear el cumplimiento de las políticas de privacidad y seguridad de datos.

Privacidad de los Datos

A continuación, se presentan algunas definiciones propuestas por diferentes autores que abordan la privacidad de los datos:

- **Dwork y Roth (2013)** definen la privacidad de los datos como "el derecho fundamental de los individuos a controlar la información sobre sí mismos y a decidir cómo se recopila, utiliza, comparte y almacena esa información por parte de terceros".
- **Solove (2008)** expresa que "la privacidad de los datos es el derecho de las personas a determinar qué información desean revelar, con quién quieren compartirla y bajo qué condiciones".
- **Nissenbaum (2011)** señala que "la privacidad de los datos se refiere a proteger la autonomía individual y el control sobre la información personal, preservando así la capacidad de las personas para decidir cómo se les percibe y cómo interactúan con su entorno".

En general, los autores coinciden en varios aspectos de la privacidad de los datos:

- Reconocen la privacidad como un derecho humano fundamental.
- Destacan la importancia del control que el individuo tiene sobre su información personal.
- Consideran la privacidad como un proceso que abarca la recopilación, uso, compartición y almacenamiento de datos por parte de terceros.

No obstante, también presentan ciertas diferencias en sus enfoques:

- **Dwork y Roth (2013)** enfatizan el control de los individuos sobre su información y cómo estos deciden quién la maneja.
- **Solove (2008)** subraya la capacidad de las personas para decidir qué información revelar, con quién compartirla y bajo qué condiciones, lo que implica un enfoque más orientado hacia la toma de decisiones individuales.
- **Nissenbaum (2011)** destaca la autonomía individual y el control sobre la información personal, abarcando aspectos más amplios que incluyen la percepción social y la interacción del individuo con su entorno.

Para esta investigación, se entiende la privacidad de los datos como: *el derecho fundamental de las personas a controlar qué información personal se recopila, cómo se utiliza, quién tiene acceso a ella y con qué fines, tanto en el ámbito digital como en el físico. Implica garantizar la confidencialidad, integridad y disponibilidad de los datos personales, así como el respeto a la autonomía y dignidad de los individuos en relación con su información privada.*

Ética en la Inteligencia Artificial

Existen varias definiciones de ética en la inteligencia artificial, entre ellas:

- **Floridi y Sanders (2004)** indican que "la ética en la inteligencia artificial se centra en los principios y valores que guían el diseño, desarrollo y uso de sistemas de IA, con el objetivo de garantizar que estos sistemas actúen de manera ética y respeten los derechos y la dignidad de las personas".

- **Dignum (2018)** explica que "la ética en la inteligencia artificial implica el análisis y la reflexión sobre cómo las decisiones y acciones de los sistemas de IA afectan a los individuos, las sociedades y el medio ambiente, y cómo podemos garantizar que estas tecnologías se utilicen de manera justa y responsable".
- **González et al. (2024)** afirman que "la ética en la inteligencia artificial se centra en el desarrollo y la aplicación de marcos éticos y normativos para guiar la toma de decisiones y el comportamiento de los sistemas de inteligencia artificial, asegurando su alineación con los valores humanos fundamentales".

En general, los autores coinciden en:

- La importancia de la ética en la IA como un campo interdisciplinario que aborda cuestiones éticas y morales relacionadas con el diseño, desarrollo e implementación de sistemas de IA.
- La necesidad de reflexionar sobre cómo las decisiones y acciones de los sistemas de IA afectan a las personas, las sociedades y el medio ambiente.
- La promoción de un uso justo, responsable y alineado con los valores humanos.

Las diferencias se manifiestan en:

- **Floridi y Sanders (2004)** presentan la ética en la IA como un campo interdisciplinario enfocado en promover el bienestar humano y social.
- **Dignum (2018)** se centra en la reflexión y análisis de las decisiones y acciones de los sistemas de IA.
- **González et al. (2024)** destacan el desarrollo de marcos éticos y normativos para guiar la toma de decisiones y comportamiento de los sistemas de IA.

Para esta investigación, la ética en la inteligencia artificial se define como: *un campo interdisciplinario que abarca los principios y valores que guían el diseño, desarrollo, implementación y uso de sistemas de IA, con el objetivo de garantizar que estos sistemas actúen de manera ética y respeten los derechos y la dignidad de las personas.*

Internet de las Cosas (IoT)

Las siguientes definiciones proporcionan una visión general del concepto de IoT:

- Oriwoh et al. (2013) define el IoT como "la interconexión de dispositivos físicos a través de la internet, permitiendo la recopilación y el intercambio de datos para realizar tareas automatizadas y mejorar la eficiencia y la comodidad en diversos contextos".
- **Gubbi et al. (2013)** explican que "el IoT es un paradigma emergente que se refiere a la conexión y comunicación de objetos físicos a través de la internet, facilitando la monitorización, el control y la gestión remota de estos objetos".
- **Atzori et al. (2010)** describen el IoT como "la infraestructura global de información y comunicación que integra objetos físicos y virtuales, habilitada por la generación de información sensorial, la comunicación inalámbrica y el procesamiento inteligente".

En general, los autores concuerdan en que el IoT:

- Es un paradigma emergente que involucra la interconexión de dispositivos físicos.
- Permite la recopilación, intercambio y procesamiento de datos entre dispositivos conectados.
- Facilita la automatización de tareas, la monitorización y el control remoto de objetos físicos.

Las diferencias entre sus definiciones radican en:

- **Oriwoh et al. (2013)** resalta la eficiencia y comodidad que el IoT aporta en diversos contextos.
- **Gubbi et al. (2013)** subrayan la importancia de la comunicación y la gestión remota de los dispositivos conectados.
- **Atzori et al. (2010)** enfatizan la generación de información sensorial y el procesamiento inteligente como aspectos clave del IoT.

Para esta investigación, el IoT se define como: *una infraestructura global de información y comunicación que integra objetos físicos y virtuales, con el potencial de transformar sectores como la industria, la salud, la agricultura y el transporte.*

1.3. Marco normativo

El marco normativo para la implementación de inteligencia artificial (IA) en la gestión de redes eléctricas con dispositivos del Internet de las Cosas (IoT) se estructura en torno a un conjunto de normas y leyes que abordan la privacidad, la ética y la seguridad de la información. Estas regulaciones y principios éticos establecen las pautas

para el uso responsable de la IA, protegiendo los derechos de los individuos y promoviendo la transparencia y la equidad en la gestión de datos. La Tabla 1 presenta un resumen de las principales normas y leyes que guían la implementación de la IA en diversos ámbitos, incluidas las especificaciones para la protección de la privacidad y la transparencia en el uso de datos:

Tabla 1

Normas y leyes establecidas para la abordar la implementación de la inteligencia artificial en diferentes ámbitos.

Norma/Ley	Año de Publicación	Descripción	Referencia
Principios de Ética de la IA de la Unión Europea (UE)	2019	Establece principios para el desarrollo y uso ético de la inteligencia artificial en la Unión Europea.	(COMISIÓN EUROPEA, 2020)
Principios de Ética de la IA de la OECD	2019	Define principios para promover la innovación responsable y la confianza en la IA a nivel internacional.	(OECD, 2023)
Principios de Ética de la IA de la UNESCO	2021	Proporciona un marco global para el desarrollo y despliegue de la inteligencia artificial, centrado en los derechos humanos y la justicia.	(UNESCO, 2021)
Directrices Éticas de la AAAI	2017	Ofrece directrices para la investigación y el desarrollo ético de la IA, promoviendo la responsabilidad social y profesional.	(An et al., 2017)
Principios Éticos de la IJCAI	2017	Establece principios éticos para la investigación y desarrollo de la IA, incluyendo la transparencia y la responsabilidad.	(De Montalvo, s. f.)
Código Ético de la ACM	2018	Contiene pautas éticas para los profesionales de la computación, incluyendo consideraciones sobre la IA.	(Association for Computing Machinery (ACM), 2018)
Reglamento General de Protección de Datos (GDPR)	2018	Regula la protección de datos personales en la Unión Europea, incluyendo aquellos utilizados en sistemas de IA.	(Diario Oficial de la Unión Europea, 2018)
Ley de Protección de la Privacidad del Consumidor de California (CCPA)	2018	Establece derechos de privacidad para los consumidores de California y regula el uso de datos personales, incluyendo en sistemas de IA.	(CCPA, 2018)
Ley de Transparencia en la IA de la Unión Europea (UE)	2021	Exige transparencia en los sistemas de IA, asegurando que los usuarios sean informados sobre su funcionamiento y decisiones.	(Parliament, 2016)
Ley de Acceso Digital de Estados Unidos (DAA)	2021	Promueve el acceso a la tecnología digital y establece principios para el desarrollo y despliegue ético de la IA.	(Barrio, 2022)

Nota: Recopilación de las leyes actuales que están planteando los límites para la incorporación de la IA y salvaguardar los derecho y privacidad de los datos y que pueda afectar la vida de las personas.

Principios Éticos: La Tabla 1 también destaca la inclusión de principios éticos, como los establecidos por la Unión Europea (UE), la OECD y la UNESCO, que guían el desarrollo y uso de la IA de manera justa y responsable. Estos principios promueven la confianza en la IA y aseguran que las tecnologías se desarrollen respetando los derechos humanos y la justicia social. Además, directrices como las de la AAAI y la IJCAI definen principios para la investigación y desarrollo ético de la IA, promoviendo la transparencia y responsabilidad en el uso de estas tecnologías (An et al., 2017; De Montalvo, s. f.).

Responsabilidad Legal: La responsabilidad legal en la implementación de IA abarca aspectos como la responsabilidad por productos defectuosos, el uso indebido de datos y las posibles consecuencias de decisiones automatizadas. Normas como el Código Ético de la ACM y la Ley de Acceso Digital de Estados Unidos (DAA) establecen criterios para definir las responsabilidades de las partes involucradas, asegurando que se adopten medidas adecuadas para mitigar los riesgos legales y éticos. La Ley de Protección de la Privacidad del Consumidor de

California (CCPA) también desempeña un papel crucial en la regulación del uso de datos personales, estableciendo responsabilidades legales claras para los proveedores de tecnologías de IA (CCPA, 2018).

Gobernanza y Supervisión: La gobernanza y supervisión adecuada de los sistemas de IA es esencial para garantizar el cumplimiento de regulaciones y principios éticos. La creación de comités de ética, la auditoría de algoritmos y la participación de diversas partes interesadas son mecanismos recomendados para monitorear el cumplimiento de estos principios y normas, como se establece en las Directrices Éticas de la AAAI y en los Principios de Ética de la IA de la UNESCO (UNESCO, 2021).

Seguridad Cibernética: El desarrollo de medidas robustas de seguridad cibernética es fundamental para proteger las redes eléctricas contra posibles amenazas y ciberataques. Normas como el **NIST Cybersecurity Framework** proporcionan directrices específicas para la protección de datos e infraestructuras críticas. La implementación de políticas de seguridad de la información y la respuesta a incidentes se basan en marcos establecidos para la seguridad de la IA y la protección de datos en sistemas interconectados de IoT.

2 Metodología

La presente investigación se fundamenta en un análisis documental, una metodología cualitativa que permite la revisión, evaluación y síntesis de información proveniente de fuentes secundarias. El objetivo principal de esta metodología es entender las tendencias, normas y desafíos éticos en la implementación de soluciones de inteligencia artificial (IA) en la gestión de redes eléctricas, considerando aspectos de ciberseguridad, privacidad de datos y principios éticos. Este enfoque metodológico facilita la integración de conceptos teóricos y normativos en un marco de referencia que guía la implementación ética y efectiva de soluciones de IA.

Justificación del Análisis Documental

El análisis documental se seleccionó como la metodología principal de la investigación debido a su capacidad para examinar exhaustivamente las normativas, principios éticos y prácticas de implementación de IA desde un enfoque crítico. La revisión de documentos como leyes, marcos regulatorios y principios éticos internacionales proporciona un contexto amplio y detallado para evaluar la viabilidad y las implicaciones de la implementación de IA en redes eléctricas.
Al utilizar esta metodología, se garantiza un proceso sistemático de recopilación, organización y análisis de la información existente, permitiendo identificar vacíos normativos, tendencias emergentes y desafíos éticos. Además, el análisis documental facilita la comparación de distintas normativas y principios éticos, lo cual es fundamental para comprender cómo se alinean o difieren en sus enfoques para abordar la privacidad, seguridad y gobernanza de la IA.

2.1. Aplicación del Análisis Documental en el Contexto de la Investigación

La investigación se estructuró en dos componentes principales para abordar sus objetivos:

- **Revisión de Normativas y Principios Éticos Internacionales:** Este componente se centró en la recopilación y análisis de documentos que abordan la regulación de la inteligencia artificial y su impacto en la gestión de redes eléctricas. Se analizaron documentos como el Reglamento General de Protección de Datos (GDPR), las Directrices de Ética de la OECD y la Ley de Protección de la Privacidad del Consumidor de California (CCPA). La comparación de estas normativas permitió identificar principios comunes y divergencias en cuanto a la protección de datos y la seguridad de la información en sistemas de IA.

- **Estudio de Casos y Prácticas Actuales en la Implementación de IA:** Se revisaron documentos y estudios de caso que describen la implementación de soluciones de IA en diferentes sectores, incluyendo el energético, con especial atención a la integración de dispositivos del Internet de las Cosas (IoT). Este análisis documental permitió identificar buenas prácticas, desafíos y estrategias de mitigación que pueden ser aplicadas al contexto de redes eléctricas.

Con esta metodología, la investigación busca proporcionar un marco comprensivo para la gestión de proyectos que incorpore las mejores prácticas y normativas aplicables, asegurando una implementación ética, eficiente y segura de soluciones de IA en la gestión de redes eléctricas.

2.2. Estructura del Análisis Documental

El análisis documental se llevó a cabo en tres fases, cada una enfocada en recopilar, organizar y analizar información relevante para los objetivos de la investigación. A continuación, se describe la estructura y el proceso detallado seguido en cada fase:

Fase de Revisión de Literatura y Normativas La primera fase se centró en la recopilación de documentos y fuentes secundarias relacionadas con la regulación y gestión de la inteligencia artificial en el contexto de redes eléctricas. Se incluyeron documentos normativos, principios éticos y estudios de casos que abordan aspectos de ciberseguridad y privacidad en sistemas de IA. La selección de fuentes se realizó con base en los siguientes criterios:

- **Relevancia**: Se seleccionaron documentos que abordan específicamente la implementación de IA en el sector energético, la gestión de proyectos tecnológicos y la protección de datos en entornos interconectados.
- **Actualidad**: Se priorizó la inclusión de documentos publicados en los últimos cinco años para reflejar las normativas y avances más recientes en el campo.
- **Fiabilidad**: Se consultaron fuentes académicas, informes de organismos internacionales (como la OECD y la Unión Europea) y marcos normativos establecidos (por ejemplo, el GDPR y la CCPA).

Los documentos seleccionados se clasificaron en categorías temáticas, tales como privacidad de datos, seguridad de la información, principios éticos y gestión de riesgos en la implementación de IA.

Fase de Categorización y Organización de Información Una vez recopilada la información, se procedió a su categorización para facilitar el análisis posterior. Los documentos se organizaron de acuerdo con los siguientes temas:

- **Normativas y Leyes Aplicables**: Incluye regulaciones internacionales, leyes nacionales y principios éticos que influyen en la implementación de IA y la protección de datos personales.
- **Estándares Técnicos y Prácticas de Implementación**: Se agrupan documentos que abordan la integración de IA e IoT en la gestión de redes eléctricas, con especial énfasis en estándares como el NIST Cybersecurity Framework y otros marcos técnicos.
- **Estudios de Casos y Aplicaciones Prácticas**: Documentos que describen la implementación de IA en proyectos tecnológicos y su evaluación en términos de eficiencia y seguridad.

Para cada documento, se elaboró una ficha técnica que contiene la referencia completa, el resumen del contenido y las principales implicaciones para la investigación.

Fase de Análisis Comparativo y Síntesis de Información En la fase final, se realizó un análisis comparativo de los documentos categorizados, identificando puntos de convergencia y divergencia entre las distintas normativas y prácticas de implementación de IA. El análisis se centró en:

- **Identificación de Vacíos Normativos**: Comparación de las normativas aplicables para detectar lagunas en la regulación de la IA, especialmente en lo relativo a la seguridad y privacidad de los datos en entornos interconectados.
- **Evaluación de la Implementación Ética de IA**: Análisis de los principios éticos que guían el desarrollo y uso de la IA, considerando cómo se alinean con la gestión de riesgos en redes eléctricas.
- **Desarrollo de Recomendaciones**: A partir del análisis documental, se desarrollaron recomendaciones para mejorar el marco de gestión de proyectos, basadas en las mejores prácticas identificadas en los documentos revisados.

2.3. Herramientas Utilizadas para la Organización de la Información

La investigación se apoyó en un conjunto de herramientas para facilitar la recolección, organización y análisis de la información obtenida de los documentos revisados. Estas herramientas fueron seleccionadas por su capacidad para gestionar grandes volúmenes de datos, su compatibilidad con formatos de citación académica y su funcionalidad para el análisis cualitativo. A continuación, se describen las principales herramientas empleadas:

2.3.1. Gestores Bibliográficos (Zotero y Mendeley):

Se utilizaron para organizar las referencias bibliográficas y generar fichas de cada documento, permitiendo una rápida recuperación de la información y asegurando la coherencia en las citas y referencias a lo largo del documento.

Estas herramientas facilitaron la categorización de los documentos según su tipo (artículos académicos, informes técnicos, documentos normativos) y temática (ciberseguridad, privacidad de datos, ética en IA).

2.3.2. Software de Análisis Cualitativo (NVivo):

Se empleó para codificar y categorizar la información contenida en los documentos revisados. Esta herramienta permitió identificar temas recurrentes, patrones y relaciones entre las diferentes categorías establecidas. La codificación se basó en las categorías definidas previamente (normativas, principios éticos, estándares técnicos) y en variables como el enfoque metodológico, resultados y recomendaciones de cada documento.

2.3.3. Procesadores de Texto (Microsoft Word y Google Docs):

Utilizados para la redacción y revisión continua del documento de investigación. Estas plataformas permitieron la colaboración y la retroalimentación en tiempo real, facilitando la coherencia y la corrección de la estructura del documento.

2.4. Técnicas para la Síntesis de Información

Para asegurar una correcta integración de los hallazgos documentales, se aplicaron las siguientes técnicas de análisis y síntesis de información:

- **Codificación y Categorización:** Se realizó una codificación abierta de los documentos, identificando las ideas y conceptos principales. Posteriormente, se categorizaron los fragmentos de información en grupos temáticos, lo cual facilitó la comparación y el contraste de los hallazgos. La codificación axial permitió establecer relaciones entre categorías, identificando vínculos entre normas éticas, estándares de ciberseguridad y prácticas de implementación de IA.
- **Análisis Comparativo:** Se llevó a cabo un análisis comparativo entre las normativas revisadas y los estudios de caso seleccionados, para evaluar cómo las distintas regulaciones abordan los desafíos éticos y de seguridad en la implementación de IA en redes eléctricas. Esta técnica permitió identificar vacíos en las normativas y divergencias en la aplicación de principios éticos en diferentes contextos geográficos y normativos.
- **Triangulación de Información:** La triangulación se aplicó al integrar los hallazgos de diferentes fuentes, verificando la consistencia y validez de la información obtenida. Este enfoque metodológico aseguró una mayor robustez en las conclusiones y recomendaciones presentadas en el documento.

2.5. Proceso de Selección de Documentos

El proceso de selección de documentos para el análisis documental se desarrolló en cinco etapas, cada una diseñada para garantizar la relevancia y calidad de los artículos incluidos en la investigación:

Definición de Palabras Clave y Cadenas de Búsqueda: Se establecieron cadenas de búsqueda específicas para cada base de datos (Scopus, Springer, ScienceDirect, IEEE Xplorer), con el objetivo de identificar artículos que abordaran la implementación de IA en redes eléctricas, ciberseguridad y privacidad de datos. Estas cadenas incluyeron términos como "gestión de proyectos", "implementación efectiva", "ética", "IA", "privacidad de datos" y "seguridad de datos"(Formato_Inteletica-Word…).

Búsqueda Inicial en Bases de Datos Se realizó una búsqueda exhaustiva en cada una de las bases de datos utilizando las cadenas de búsqueda definidas. Los artículos encontrados se clasificaron según su título y resumen para realizar una evaluación preliminar de su relevancia.

Tabla 2

Cadenas consideradas en el proceso de búsqueda.

Base de datos	Cadena de búsqueda
Scopus	TÍTULO-ABS-CLAVE ("gestión de proyectos" Y "implementación efectiva" Y "ética" Y "soluciones de inteligencia artificial" Y "privacidad de datos" Y "seguridad de datos" Y "red eléctrica" Y "IoT" Y "sistemas de monitorización" Y "entornos residenciales" Y "entornos industriales")
Springer	("gestión de proyectos" AND "implementación efectiva" AND "ética" AND "soluciones de inteligencia artificial" AND "privacidad de datos" AND "seguridad de datos" AND "red eléctrica" AND "IoT" AND "sistemas de monitorización" AND "entornos residenciales" AND "entornos industriales")

ScienceDirect	TITLE-ABS-KEY ("gestión de proyectos" AND "implementación efectiva" AND "ética" AND "soluciones de inteligencia artificial" AND "privacidad de datos" AND "seguridad de datos" AND "red eléctrica" AND "IoT" AND "sistemas de monitorización" AND "entornos residenciales" AND "entornos industriales")
IEEE Xplorer	("gestión de proyectos" AND "implementación efectiva" AND "ética" AND "soluciones de inteligencia artificial" AND "privacidad de datos" AND "seguridad de datos" AND "red eléctrica" AND "IoT" AND "sistemas de monitorización" AND "entornos residenciales" AND "entornos industriales")

Nota. Elaboración propia.

Revisión de Títulos y Resúmenes: Durante esta etapa, se revisaron los títulos y resúmenes de cada documento para identificar su pertinencia con los objetivos de la investigación. Se incluyeron artículos que trataban específicamente sobre la implementación de IA en la gestión de redes eléctricas, con un enfoque en privacidad y seguridad de datos.
Aplicación de Criterios de Inclusión y Exclusión: Para asegurar la calidad y relevancia de los documentos seleccionados, se aplicaron criterios específicos de inclusión y exclusión:

- **Criterios de Inclusión:**
  - Artículos revisados por pares.
  - Publicados entre 2019 y 2024.
  - Estudios empíricos o revisiones teóricas relevantes que abordaran la gestión de proyectos, privacidad de datos y seguridad de datos en redes eléctricas.
  - Publicaciones en revistas académicas de alto impacto.
- **Criterios de Exclusión:**
  - Editoriales, notas de opinión y artículos de divulgación.
  - Artículos duplicados.
  - Estudios que no se centraran específicamente en el contexto de IA y redes eléctricas.
  - Ponencias de congresos y documentos de trabajo no revisados por pares (Formato_Inteletica-Word…).

Análisis de Contenido: Los artículos seleccionados pasaron a una fase de lectura detallada y análisis de contenido para confirmar su relevancia y calidad. En esta etapa se verificó que los artículos abordaran directamente los desafíos y soluciones relacionadas con la implementación efectiva y ética de IA para la privacidad y seguridad de datos en redes eléctricas. Además, se evaluó la metodología, los resultados y las conclusiones de cada artículo para asegurar su aporte significativo al campo de estudio.

Justificación de los Criterios de Selección: La definición de criterios de inclusión y exclusión se realizó para asegurar que los artículos seleccionados fueran rigurosos y relevantes para los objetivos de la investigación. Dado que el enfoque del estudio se centra en la implementación ética de IA en la gestión de redes eléctricas, se priorizó la inclusión de artículos recientes que reflejen los avances tecnológicos y normativos en esta área.
Los criterios de exclusión, por otro lado, ayudaron a filtrar documentos que no cumplieran con los estándares de calidad requeridos o que no se alinearan con los objetivos de la investigación. De esta manera, se garantizó la obtención de un conjunto de documentos coherente y representativo para el análisis

3 Resultados

La revisión de literatura se centró en analizar el estado actual de las Estrategias de Gerencia de Proyectos para la Implementación Ética y Segura de Inteligencia Artificial (IA) en Redes Eléctricas con Integración de IoT, con un énfasis especial en ciberseguridad y privacidad de datos en contextos residenciales e industriales. Para ello, se seleccionaron estudios relevantes de bases de datos académicas como Springer, Scopus, IEEE Xplorer y ScienceDirect, considerando artículos publicados entre 2019 y 2024.

3.1. Soluciones de Inteligencia Artificial para Abordar los Desafíos Específicos de la Gestión y Optimización de la Red Eléctrica

Uno de los grandes desafíos que ha enfrentado la red eléctrica tradicional durante décadas es la dificultad para almacenar la energía generada. La electricidad se produce en función de la demanda, lo que convierte en una prioridad para los operadores contar con información precisa y recursos disponibles para evitar inestabilidades en

la red ocasionadas por fluctuaciones en el consumo. Esta tarea se ha vuelto aún más compleja con la incorporación de tecnologías emergentes, como los vehículos eléctricos, que representan un alto consumo de energía, pero al mismo tiempo pueden ser utilizados como sistemas de almacenamiento a gran escala, contribuyendo a la estabilidad de la red.

Además, la integración de energías renovables ha introducido un cambio significativo en la infraestructura energética, desplazando plantas de generación tradicionales basadas en combustibles no renovables por recursos energéticos distribuidos (DER, por sus siglas en inglés). Esta transición hacia fuentes de energía más sostenibles ha creado la necesidad de modernizar las infraestructuras eléctricas y su gestión para responder a los desafíos actuales de la transición energética (Ortiz-Torres et al., 2024).

3.1.1. Aplicación de Tecnologías IoT en la Industria de la Energía Eléctrica

La industria de la energía eléctrica se estructura en torno a tres componentes principales:

- **Generación de Energía:** Transformación de fuentes primarias en electricidad.
- **Transmisión de Energía:** Transporte de electricidad desde los sitios de generación hasta los centros de consumo.
- **Distribución de Energía:** Entrega de electricidad a los usuarios finales.

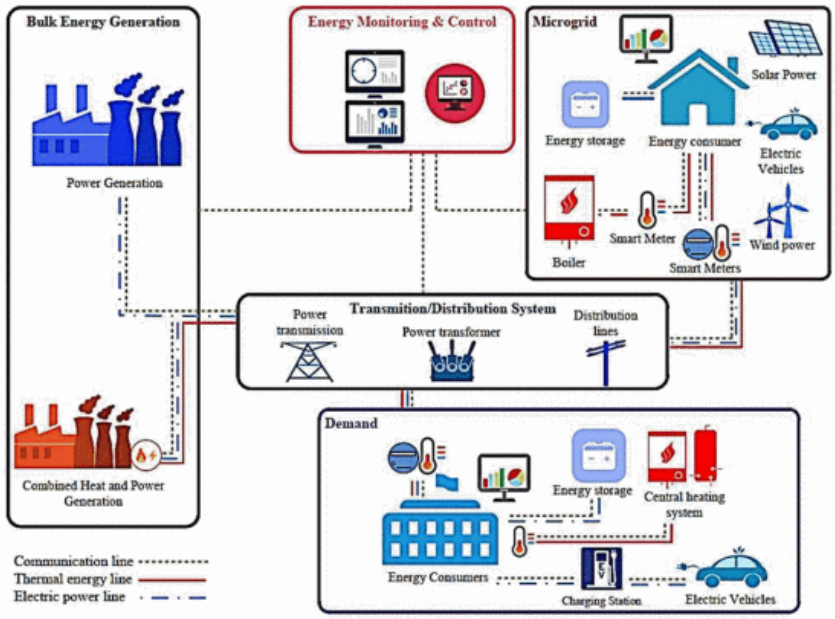
La implementación de sistemas IoT integrados tiene el potencial de optimizar cada uno de estos componentes al permitir una mejor monitorización y control en tiempo real de las operaciones. Esto no solo mejora la eficiencia y la capacidad de respuesta de las redes eléctricas, sino que también promueve una mayor interacción con los usuarios finales, dando lugar al concepto de redes inteligentes (Saleem et al., 2019).

Las redes inteligentes, o *smart grids*, se definen como sistemas eléctricos que incorporan diferentes tecnologías para optimizar la eficiencia de la red y facilitar la comunicación bidireccional entre las compañías eléctricas y los usuarios. Sin embargo, la creciente conectividad y la proliferación de dispositivos IoT han introducido nuevos desafíos en términos de ciberseguridad.

Ansaria (2024) destacan que, si bien los dispositivos conectados han impulsado mejoras significativas en la red, también han generado amenazas complejas para la ciberseguridad, en las que la ausencia de políticas de seguridad corporativa y la falta de adopción de requisitos específicos han resultado en incidentes importantes, como el ciberataque a la infraestructura eléctrica de Ucrania.

Figura 1

Esquema del sistema energético, incluidas las infraestructuras eléctricas, térmicas y de comunicación.

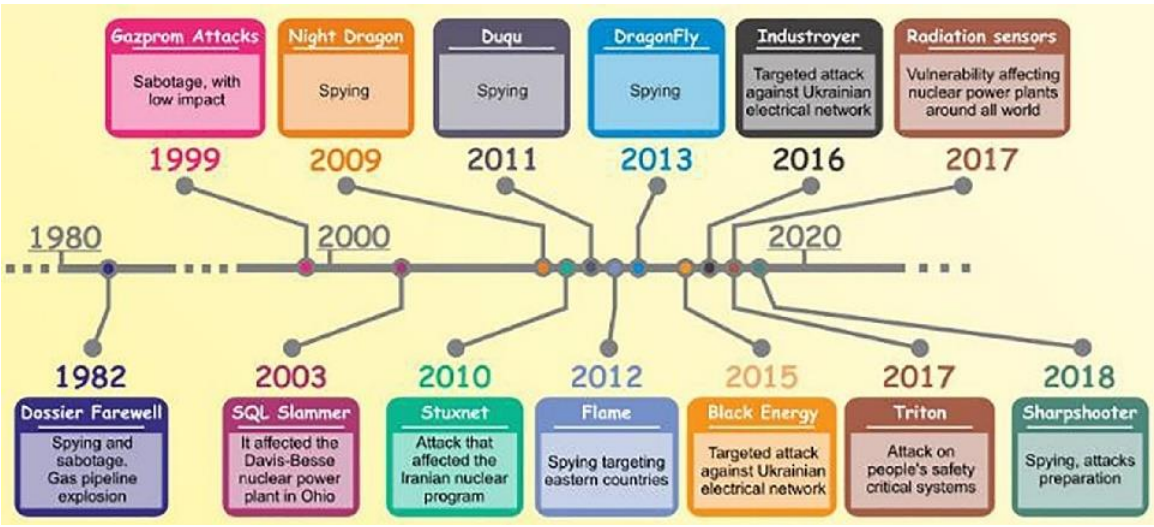


Nota. Actualidad del sistema energético con diferentes actores aportando a este y por otro lado aumento de la demanda con más dispositivos y tecnologías de consumo. Tomado de *Internet of things-aided smart grid: technologies, architectures, applications, prototypes, and future research directions* (p. 10), por Saleem et al., 2019, Ieee Access, 7, 62962-63003.

El Internet de las Cosas (IoT) conecta una amplia variedad de dispositivos inteligentes, como sensores, sistemas de posicionamiento global (GPS), dispositivos portátiles y teléfonos móviles. Su adopción en sectores como la automatización del hogar, la seguridad, la videovigilancia y la gestión de bienes ha impulsado un crecimiento fenomenal en el número de dispositivos conectados a nivel global. Según Holland et al. (2021), las conexiones máquina a máquina (M2M) se incrementarán 2,4 veces, pasando de 6.100 millones en 2018 a 14.700 millones en 2023, mientras que las conexiones móviles M2M se cuadruplicarán, de 1.200 millones en 2018 a 4.400 millones en 2023, alcanzando una tasa compuesta anual del 30% (Holland et al., 2021, p. 6). Este crecimiento también se ve reflejado en un aumento sustancial de los dispositivos IoT en comparación con aquellos que no se consideran IoT. Gupta y Quamara (2020) estiman una tasa de crecimiento anual del 10% desde 2018, con una proyección que apunta a 21,5 mil millones de dispositivos IoT para el año 2025, lo cual es tres veces mayor al número registrado en 2018 (Gupta y Quamara, 2020, p. 40).

Los dispositivos IoT pueden comunicarse e interconectarse entre sí para intercambiar datos, lo que permite una conectividad masiva que involucra a miles de millones de dispositivos conectados que se comunican a través de la Internet. Con su rápida adopción, estos dispositivos se encuentran en una variedad de entornos, como hogares, oficinas, transporte, atención médica, telecomunicaciones e industrias, entre otros. Sin embargo, la mayoría de estos dispositivos presentan limitaciones en términos de recursos, como capacidad de procesamiento, memoria y batería, lo que los convierte en blancos potenciales para ataques cibernéticos.
Debido a su popularidad, uso generalizado y naturaleza distribuida, la seguridad de IoT plantea un desafío complejo que difiere considerablemente del de las redes tradicionales. Los dispositivos IoT utilizan múltiples protocolos de comunicación, lo que, sumado a la falta de estándares de seguridad universales, aumenta su vulnerabilidad ante ataques maliciosos. Además, la gran cantidad de dispositivos conectados y la creciente movilidad de los mismos han incrementado la superficie de ataque, haciendo que la protección de estos entornos requiera un enfoque multifacético. En la Figura 2, se presenta una cronología de incidentes cibernéticos que han afectado al sector energético, destacando la relevancia de la ciberseguridad en este ámbito.

Figura 2
Cronología con las incidencias de intrusiones más importantes sobre las redes eléctricas.



Nota. Cronología de los diferentes ataques con mayor relevancia que se han hecho sobre el sector eléctrico a nivel mundial. A systematic approach to analysis for assessing the security level of cyber-physical systems in the electricity sector (p. 12), por Sánchez et al., 2021, Microprocessors and Microsystems, 87, 104352.

3.1.2. Potencial de la IA en la Protección de Redes Eléctricas con Despliegue IoT

Las tecnologías de inteligencia artificial han demostrado un gran potencial para mejorar la seguridad y resiliencia de las redes eléctricas en entornos IoT. En particular, los sistemas de detección de intrusiones basados en IA representan una solución innovadora para superar las limitaciones de los enfoques de seguridad tradicionales. Estos sistemas son capaces de analizar grandes volúmenes de datos en tiempo real y detectar patrones anómalos que puedan indicar amenazas emergentes, respondiendo de manera rápida y precisa. Además, los sistemas basados en

IA tienen la capacidad de adaptarse a entornos cambiantes y aprender de la experiencia acumulada, lo que los hace especialmente efectivos en la gestión de la seguridad de redes dinámicas y complejas.
Al integrar IA con dispositivos IoT, las redes eléctricas pueden beneficiarse de capacidades avanzadas de detección y respuesta ante incidentes de seguridad, optimizando así su resiliencia frente a ataques cibernéticos. Esta capacidad de adaptación y aprendizaje es particularmente relevante en el contexto de redes eléctricas interconectadas, donde las amenazas son cada vez más sofisticadas y difíciles de prever mediante métodos tradicionales.
Al aprovechar el potencial de la inteligencia artificial (IA), los sistemas de detección de intrusiones pueden llenar los vacíos que dejan los enfoques tradicionales de seguridad y brindar una protección más integral y efectiva en entornos de IoT. La IA contribuye a mejorar la seguridad de IoT mediante la implementación de tres capacidades fundamentales:

- **Aprendizaje Supervisado:** Se utiliza cuando los modelos de IA son entrenados con datos previamente etiquetados. Esta técnica permite que el sistema aprenda a clasificar y predecir comportamientos basados en patrones conocidos. Por ejemplo, las máquinas de vectores de soporte (SVM) se emplean para clasificar dispositivos autorizados y no autorizados en la red, detectando posibles accesos no autorizados y comportamientos anómalos.
- **Aprendizaje No Supervisado:** A diferencia del aprendizaje supervisado, esta técnica permite extraer conocimiento oculto de los datos sin necesidad de etiquetado previo. El aprendizaje no supervisado es especialmente útil para detectar patrones emergentes o actividades inusuales en dispositivos IoT que puedan indicar la presencia de amenazas en la red, incluso cuando no se tiene un conocimiento previo de estas amenazas.
- **Aprendizaje por Refuerzo:** Este modelo se basa en la técnica de recompensa y castigo para mejorar continuamente el comportamiento del sistema a lo largo del tiempo. El aprendizaje por refuerzo permite a los sistemas de detección de intrusiones adaptarse dinámicamente a entornos cambiantes, aprendiendo de sus propias acciones para optimizar la seguridad y minimizar riesgos. Zarca et al. (2019) destacan que esta capacidad de adaptación es crucial para la protección de redes eléctricas en entornos IoT.

3.1.3. Técnicas Recomendadas para la Gestión y Optimización de la Red Eléctrica

Las técnicas modernas como el aprendizaje automático (Machine Learning, ML) y el aprendizaje de refuerzo profundo (Deep Reinforcement Learning, DRL) son esenciales para analizar y tomar decisiones en redes eléctricas inteligentes que utilizan IoT. Estas técnicas permiten gestionar grandes volúmenes de datos de manera eficiente, asegurando decisiones óptimas y escalables. A continuación, se detallan las principales técnicas aplicadas:

- **Aprendizaje Supervisado:** Se emplea para clasificar y predecir comportamientos en la red eléctrica. Las SVM y los árboles de decisión son ejemplos de técnicas que pueden identificar dispositivos autorizados y no autorizados, clasificando el tráfico de red y detectando comportamientos inusuales con alta precisión.
- **Aprendizaje No Supervisado:** Se utiliza para detectar patrones y anomalías sin necesidad de datos etiquetados. Esta técnica permite la identificación de actividades anormales en dispositivos IoT que podrían indicar intrusiones o accesos no autorizados, proporcionando una capa adicional de seguridad.
- **Aprendizaje por Refuerzo (RL):** Permite mejorar continuamente los modelos de seguridad a medida que el sistema interactúa con su entorno, adaptándose a nuevas amenazas y entornos complejos.
- **Aprendizaje Profundo (Deep Learning, DL):** Se centra en el manejo de grandes volúmenes de datos y mejora la precisión en la detección de amenazas. Las redes neuronales profundas son capaces de analizar datos complejos y no estructurados, detectando intrusiones con alta efectividad.
- **Aprendizaje de Refuerzo Profundo (DRL):** Combina el aprendizaje profundo con el aprendizaje por refuerzo, optimizando el proceso de toma de decisiones en la red eléctrica al responder rápidamente a cambios en la demanda y la oferta de energía, así como a amenazas cibernéticas emergentes.
- **Evaluación de Privacidad y Seguridad de Datos en Redes Eléctricas con IoT**

Para garantizar la protección de información sensible y la capacidad de respuesta ante amenazas cibernéticas, es fundamental implementar soluciones de IA que aseguren un alto nivel de privacidad y seguridad de datos. A continuación, se presentan las características clave que deben cumplir estas soluciones:

- **Reconocimiento de Patrones y Detección de Conductas Anormales:** Utilizar métodos supervisados y no supervisados para identificar actividades inusuales en la red eléctrica. Por ejemplo, el uso de SVM permite clasificar dispositivos y detectar accesos no autorizados en tiempo real, proporcionando una respuesta rápida a incidentes de seguridad.

- **Capacidades de Protección y Aprendizaje Autónomo:** Implementar técnicas de aprendizaje no supervisado para manejar datos sin etiquetar, permitiendo la identificación de amenazas emergentes sin la necesidad de información previa. Además, el aprendizaje por refuerzo permite una mejora continua de los modelos de seguridad a medida que se actualizan con nuevos datos y experiencias.
- **Procesamiento Eficaz de Grandes Cantidades de Datos:** Emplear modelos de aprendizaje profundo que aseguren la eficiencia y precisión en la detección de amenazas, incluso en entornos con grandes volúmenes de datos complejos. Estas técnicas permiten gestionar la complejidad de la información generada por dispositivos IoT conectados en la red eléctrica.
- **Alta Precisión y Robustez del Modelo:** Utilizar algoritmos supervisados y redes neuronales profundas para garantizar una detección precisa de ataques. La robustez del modelo se evalúa mediante técnicas como SVM y bosques aleatorios, que ofrecen una capacidad de generalización sólida y un rendimiento constante en escenarios diversos y complejos.
- **Certificaciones y Estándares de Ciberseguridad:** Es fundamental priorizar soluciones de IA que cumplan con certificaciones y estándares reconocidos, como ISO/IEC 27001 para la gestión de seguridad de la información. Estas certificaciones garantizan que las soluciones han sido evaluadas y cumplen con requisitos de seguridad rigurosos.

3.2. Requisitos de Privacidad y Seguridad de Datos con la Integración de Dispositivos IoT en Entornos Residenciales e Industriales.

En la actualidad, las cuestiones de privacidad relacionadas con la IoT doméstica e industrial se están debatiendo activamente. Kowatsch Maass (s. f.) demostró que la aceptación de los servicios de IoT en el hogar e industrias, se ve afectada por diversos factores que van desde los riesgos de privacidad y los intereses personales hasta la legislación, la seguridad de la información y la transparencia del uso de la información.
Khidzir et al. (2010) clasificó los factores de vulnerabilidad en treinta categorías basadas en la literatura pertinente. Estas categorías pueden clasificarse a su vez en cuatro tipos: vulnerabilidades tecnológicas (fallas y debilidades en el diseño del sistema), vulnerabilidades del proveedor (fiabilidad y responsabilidad), vulnerabilidades de la ley (aplicación insuficiente de la ley) y vulnerabilidades del usuario (ignorancia y negligencia descuidada). La tabla 3 muestra un ejemplo de los cuatro factores de riesgo y vulnerabilidad en un entorno de IoT doméstico e industrial.

Tabla 3
Ejemplos de cuatro factores de riesgo y vulnerabilidad en entornos domésticos e industriales.

Vulnerabilidad	Ejemplos	Referencias
Tecnología	• Piratería informática e invasión de la privacidad utilizando vulnerabilidades de seguridad de las tecnologías de la información y la comunicación (por ejemplo, Bluetooth, Wifi, Z-wave). • Marco de seguridad y soluciones débiles para los dispositivos conectados.	(Jacobsson et al., 2020; Lee, 2020)
Ley	• Penas débiles o evasión de castigos debido a leyes insuficientes. • Falta de marco legal para la instalación de equipos IoT domésticos e industriales y estándares técnicos.	(Losavio et al., 2018)
Proveedor	• No hay acuerdos de usuario, ni actualizaciones del sistema para eliminar la vulnerabilidad. • Recopilación de información personal de los usuarios para otros fines comerciales o uso no autorizado. • Medidas de seguridad débiles y piezas de hardware debido al costo.	(Jackson y Orebaugh, 2020)
Usuario	• Incumplimiento de las políticas de seguridad (contraseñas simples y sin cambios). • Mal uso y gestión de dispositivos IoT domésticos e industriales debido a antigüedad o inexperiencia.	(Boer et al., 2020)

Nota. Elaboración propia.

3.2.1. Vulnerabilidades y Riesgos Asociados

- **Amenazas cibernéticas:** los dispositivos IoT y los sistemas de monitoreo pueden ser vulnerables a ataques cibernéticos como malware, phishing, ataques de denegación de servicio (DDoS) e interceptación de datos, lo que podría comprometer la confidencialidad, integridad y disponibilidad de la información.
- **Privacidad de datos:** la recopilación, almacenamiento y uso de datos personales por parte de los sistemas IoT pueden generar inquietudes sobre la privacidad individual, especialmente si no se implementan prácticas de manejo de datos transparentes y responsables.
- **Fallos de seguridad física:** los dispositivos IoT pueden ser susceptibles a manipulaciones físicas o robos, lo que podría exponer datos confidenciales o permitir la toma de control no autorizada de los sistemas.
- **Errores humanos:** la configuración incorrecta, el uso inadecuado o la falta de actualizaciones de software en los dispositivos IoT pueden crear vulnerabilidades que podrían ser explotadas por actores maliciosos.

3.2.2. Requisitos de seguridad para soluciones de inteligencia artificial

- **Protección de datos:** implementar medidas robustas para proteger la confidencialidad, integridad y disponibilidad de los datos utilizados para entrenar y operar los sistemas de inteligencia artificial.
- **Transparencia y explicabilidad:** asegurar que los algoritmos de inteligencia artificial sean transparentes y explicables, permitiendo comprender cómo se toman las decisiones y cómo se procesan los datos.
- **Robustez y confiabilidad**: diseñar sistemas de inteligencia artificial robustos y confiables que sean resistentes a manipulaciones, sesgos y errores algorítmicos.
- **Gestión de riesgos:** implementar un proceso de gestión de riesgos para identificar, evaluar y mitigar los riesgos potenciales asociados con el uso de la inteligencia artificial.

3.2.3. Controles de seguridad para mitigar riesgos

- **Autenticación y control de acceso:** implementar mecanismos robustos de autenticación y control de acceso para restringir el acceso a dispositivos IoT, sistemas de monitoreo y datos asociados solo a usuarios y entidades autorizadas.
- **Cifrado de datos:** Cifrar los datos en reposo y en tránsito para protegerlos contra accesos no autorizados e interceptaciones.
- **Actualizaciones de software:** implementar un proceso regular de actualizaciones de software para dispositivos IoT y sistemas de monitoreo para corregir vulnerabilidades y proteger contra nuevas amenazas.
- **Segmentación de redes:** segmentar las redes en las que se encuentran los dispositivos IoT para aislarlos de otros sistemas y reducir el alcance potencial de las amenazas.
- **Conciencia y capacitación del usuario:** educar a los usuarios sobre las prácticas de seguridad adecuadas para dispositivos IoT y sistemas de monitoreo, incluyendo la creación de contraseñas seguras, la identificación de ataques de phishing y la importancia de las actualizaciones de software.

3.3. Estándares Internacionales y Prácticas para la Implementación Ética de Soluciones de Inteligencia Artificial en la Gestión de Redes Eléctricas.

La integración de la inteligencia artificial (IA) en la gestión de redes eléctricas presenta un gran potencial para optimizar la eficiencia, la confiabilidad y la seguridad de los sistemas eléctricos. Sin embargo, es crucial garantizar que la implementación de estas soluciones se realice de manera ética y responsable, considerando los aspectos de privacidad y seguridad de datos.

3.3.1. Estándares Internacionales

- Recomendación de la UNESCO sobre la Ética de la Inteligencia Artificial: Este documento establece principios éticos generales para el desarrollo y uso de la IA, incluyendo la no discriminación, la rendición de cuentas, la transparencia y la responsabilidad (UNESCO, 2022).

- Principios de la OCDE sobre Inteligencia Artificial: Estos principios abordan aspectos como la robustez, la transparencia, la explicabilidad, la equidad, la seguridad y la responsabilidad de los sistemas de IA (OECD, 2024).
- ISO/IEC 27001:2022 - Sistemas de gestión de la seguridad de la información: Este estándar proporciona un marco para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI) en una organización (ISO, 2022).
- UNE-EN IEC 62443-3-3:2020 - Redes de comunicaciones industriales. Seguridad de la red y del sistema. Parte 3-3: Requisitos de seguridad del sistema y niveles de seguridad (Atkins & Lawson, 2021). La IEC 62443 complementa así a la norma ISO 27001, que abarca principalmente las regulaciones para la seguridad IT. Sumadas, ambas normas ofrecen de forma integral una opción amplia de protección en hogares, industrias y empresas frente a las amenazas cibernéticas.

3.3.2. Mejores Prácticas Recomendadas para Abordar los Riesgos Relacionados con la Privacidad y Seguridad de Datos

- Enfoque en el diseño desde la privacidad: Incorporar principios de privacidad desde las primeras etapas del diseño de las soluciones de IA, minimizando la recopilación y el almacenamiento de datos personales.
- Transparencia y explicabilidad: Proporcionar información clara y comprensible sobre cómo funcionan los sistemas de IA, incluyendo los datos utilizados, los algoritmos empleados y las decisiones tomadas.
- Gestión responsable de datos: Implementar prácticas robustas de gestión de datos para garantizar la confidencialidad, integridad y disponibilidad de los datos, incluyendo medidas de control de acceso, cifrado y eliminación segura de datos.
- Evaluación de impacto y mitigación de riesgos: Realizar evaluaciones de impacto de la privacidad y la seguridad de datos para identificar y mitigar los riesgos potenciales asociados con la implementación de soluciones de IA.
- Gobernanza y supervisión: Establecer mecanismos de gobernanza y supervisión para garantizar el cumplimiento de los principios éticos, los estándares y las regulaciones aplicables.

3.3.3. Aplicabilidad en Entornos Residenciales e Industriales

Los estándares y las mejores prácticas mencionadas anteriormente son aplicables tanto a entornos residenciales como industriales. Sin embargo, es importante considerar las particularidades de cada contexto al implementar soluciones de IA en la gestión de redes eléctricas.

En entornos residenciales

- Privacidad de los datos del consumidor: Es crucial proteger la privacidad de los datos de consumo de energía y otros datos personales asociados con los residentes.
- Seguridad de los dispositivos IoT: Los dispositivos IoT utilizados en el hogar deben ser seguros y resistentes a ataques cibernéticos.

En entornos industriales

- Seguridad de la infraestructura crítica: La seguridad de la infraestructura crítica de la red eléctrica debe ser una prioridad absoluta.
- Confiabilidad y disponibilidad de la red: Los sistemas de IA deben diseñarse para garantizar la confiabilidad y disponibilidad de la red eléctrica.

3.3.4. Selección de Normativas y Directrices

La selección de las normativas y directrices más adecuadas dependerá de los requisitos específicos de cada proyecto. Sin embargo, algunas de las normativas y directrices más relevantes incluyen:

- Reglamento General de Protección de Datos (RGPD) de la Unión Europea: El RGPD establece un marco legal para la protección de datos personales en la Unión Europea.
- Ley de Protección de Datos Personales y Hábeas Data de Colombia: Esta ley establece un marco legal para la protección de datos personales en Colombia (Azuero, 2023).

- NIST Cybersecurity Framework (CSF): El CSF proporciona un marco para la gestión de riesgos de ciberseguridad en organizaciones (McIntosh et al., 2024).

3.4. Gestión Integral de Riesgos y Seguridad en Proyectos de IA para Redes Eléctricas

Para asegurar la implementación efectiva de soluciones de inteligencia artificial (IA) en redes eléctricas, es fundamental identificar y adoptar marcos de gestión de proyectos que se adapten a las necesidades específicas de este contexto. A continuación, se detallan los marcos más relevantes y su evaluación:

- **PMBOK (Project Management Body of Knowledge):**
  - **Descripción:** Proporciona una guía exhaustiva para la gestión de proyectos basada en procesos.
  - **Adaptabilidad:** PMBOK es altamente adaptable y puede incluir consideraciones específicas de privacidad y seguridad de datos mediante la integración de procesos personalizados (Yilmaz et al., 2024).
- **PRINCE2 (Projects IN Controlled Environments):**
  - **Descripción:** Ofrece un enfoque estructurado para la gestión de proyectos, con énfasis en la justificación continua del negocio.
  - **Adaptabilidad:** Permite la adaptación de sus principios para incorporar prácticas específicas de IA y ciberseguridad (Kous, 2023).
- **Agile:**
  - **Descripción:** Enfocado en la flexibilidad y la adaptabilidad, ideal para proyectos que requieren iteraciones y mejoras continuas.
  - **Adaptabilidad:** Agile puede ser ajustado para integrar evaluaciones continuas de privacidad y seguridad de datos, permitiendo respuestas rápidas a posibles riesgos.
- **ISO 21500 (Guidance on Project Management)**
  - **Descripción:** Proporciona directrices para la gestión de proyectos basadas en las mejores prácticas internacionales.
  - **Adaptabilidad:** Es compatible con la incorporación de estándares específicos de ciberseguridad y privacidad (Bernabé-Custodio et al., 2024).

3.4.1. Validación de actividades de gestión de riesgos

Para asegurar una gestión de riesgos efectiva, es necesario desarrollar y validar actividades específicas que se incorporarán en el plan del proyecto. Estas actividades deben incluir:

- **Identificación de Riesgos:**
  - **Actividad:** Utilizar herramientas como análisis FODA (Fortalezas, Oportunidades, Debilidades, Amenazas) y diagramas de causa-efecto para identificar riesgos.
  - **Resultado:** Lista exhaustiva de riesgos potenciales.
- **Evaluación de Riesgos:**
  - **Actividad:** Aplicar matrices de probabilidad e impacto para priorizar riesgos.
  - **Resultado:** Evaluación detallada de cada riesgo según su probabilidad e impacto.
- **Mitigación de Riesgos:**
  - **Actividad:** Desarrollar planes de mitigación que incluyan medidas preventivas y correctivas.
  - **Resultado:** Planes de mitigación documentados.
- **Asignación de Responsabilidades:**
  - **Actividad:** Asignar claramente las responsabilidades a miembros del equipo y definir plazos para la ejecución de acciones de mitigación.
  - **Resultado:** Registro de responsabilidades y cronograma de actividades.

3.4.2. Integración y documentación de la gestión de riesgos, la planificación estratégica y las prácticas de seguridad cibernética

La integración y documentación deben cubrir todas las etapas del ciclo de vida del proyecto, desde la definición de requisitos hasta la operación continua de las soluciones de IA:

- **Definición de Requisitos:**
  - **Actividad:** Documentar los requisitos específicos de privacidad y seguridad de datos.

- **Resultado:** Documento de requisitos iniciales.
- **Planificación Estratégica:**
  - **Actividad:** Desarrollar un plan estratégico con objetivos claros, estrategias de implementación y métricas de éxito.
  - **Resultado:** Plan estratégico documentado.
- **Implementación y Monitoreo:**
  - **Actividad:** Desarrollar e integrar soluciones de IA, realizar pruebas, validaciones y monitorear el rendimiento.
  - **Resultado:** Soluciones de IA implementadas y validadas con informes de monitoreo continuo.
- **Documentación Continua:**
  - **Actividad:** Mantener una documentación detallada y actualizada de todas las fases del proyecto.
  - **Resultado:** Documentación accesible y completa que incluye:
    - ✓ Definición de requisitos
    - ✓ Planificación estratégica
    - ✓ Actividades de gestión de riesgos
    - ✓ Prácticas de seguridad cibernética

4 Conclusiones y recomendaciones

La presente investigación se centra en la implementación ética y segura de la inteligencia artificial (IA) y el Internet de las Cosas (IoT) en la gestión de redes eléctricas, un campo que combina la innovación tecnológica con la gestión de riesgos éticos y de seguridad. El estudio aporta una perspectiva integral al fusionar principios de gerencia de proyectos con tecnologías avanzadas de IA e IoT, proporcionando un enfoque sistemático para optimizar la eficiencia operativa, la privacidad y la seguridad de los datos en las redes eléctricas.
Uno de los principales hallazgos es el desarrollo de un marco de gestión de proyectos adaptado específicamente para la integración de IA y IoT en redes eléctricas. Este marco se fundamenta en la recopilación de datos a partir de estudios de caso en entornos residenciales e industriales, donde se han implementado soluciones de IA para monitorear y optimizar el consumo energético. Los resultados indican que la implementación de IA no solo mejora significativamente la eficiencia en la distribución de energía, sino que también refuerza la resiliencia de las redes eléctricas frente a ciberataques, gracias a la capacidad de los sistemas de IA para aprender y adaptarse a nuevas amenazas en tiempo real.

El enfoque que se propone expone técnicas de aprendizaje automático supervisado y no supervisado, así como algoritmos de aprendizaje profundo, que permiten identificar patrones anómalos en el consumo de energía y el comportamiento de la red. Esto facilita una respuesta más rápida y precisa ante posibles fallos o ataques de seguridad. La capacidad de estos sistemas para adaptarse dinámicamente a cambios en el entorno operativo representa una mejora significativa respecto a los métodos tradicionales de gestión de redes, que a menudo dependen de procesos manuales y respuestas reactivas.

Además de los avances tecnológicos, la investigación contribuye significativamente al marco ético y de seguridad para la gestión de redes eléctricas. La integración de dispositivos IoT implica la recopilación y análisis de grandes volúmenes de datos personales y operativos, lo que plantea desafíos importantes en términos de privacidad y seguridad de la información. Este estudio propone un conjunto de directrices éticas y normativas, basadas en estándares internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, para garantizar que las implementaciones de IA cumplan con las normativas de privacidad y seguridad, protegiendo así los derechos de los usuarios.

El marco de gestión de proyectos desarrollado también incluye la aplicación de medidas de seguridad robustas, como el cifrado de datos, la autenticación multifactorial y el monitoreo continuo de las redes, para proteger la información sensible de los usuarios y minimizar el riesgo de violaciones de datos. Este enfoque holístico no solo aborda los aspectos técnicos de la seguridad, sino que también enfatiza la importancia de la transparencia, la responsabilidad y la protección de los derechos de privacidad de los individuos.

Este trabajo de investigación abre la puerta a varias áreas potenciales para futuros estudios. Se recomienda investigar cómo los principios y marcos desarrollados aquí pueden aplicarse a otros sectores críticos, como el transporte y la salud, donde la integración de IA e IoT también puede ofrecer mejoras significativas en la eficiencia

operativa y la seguridad. Además, futuras investigaciones deberían explorar cómo las diferencias en los marcos legales y éticos entre diversas jurisdicciones podrían afectar la implementación de soluciones tecnológicas en redes eléctricas y otros contextos industriales. Esto ayudaría a desarrollar estrategias de implementación más adaptables y culturalmente sensibles que puedan ser aplicadas en múltiples escenarios globales.

Asimismo, el marco de gestión de proyectos propuesto puede servir como base para la creación de nuevas regulaciones que aborden los desafíos específicos de la integración de IA e IoT en infraestructuras críticas. Las políticas futuras podrían beneficiarse de este marco para establecer directrices claras y consistentes que aseguren una implementación segura, ética y eficiente de estas tecnologías, apoyando a los legisladores y reguladores en la formulación de políticas basadas en la evidencia.

En definitiva, esta investigación proporciona un aporte significativo al campo de la gestión de proyectos para la implementación de IA e IoT en redes eléctricas, proponiendo un marco que equilibra la eficiencia operativa con la seguridad y la privacidad de los datos, y establece una base sólida para el desarrollo de futuras investigaciones y políticas en este ámbito.

Referencias

Abd Elazim, S. M., y Ali, E. S. (2016). Optimal Power System Stabilizers design via Cuckoo Search algorithm. International Journal of Electrical Power and Energy Systems, 75, 99–107. https://doi.org/10.1016/j.ijepes.2015.08.018

An, J., Ciampaglia, G. L., Grinberg, N., Joseph, K., Mantzarlis, A., Maus, G., Menczer, F., Proferes, N., y Welles, B. F. (2017). Reports of the workshops held at the 2017 international AAAI conference on web and social media. AI Magazine, 38(4), 93–98. https://doi.org/10.1609/aimag.v38i4.2772

Ansaria, N. A. (2024). Analysis of Ukraine power grid cyber-attack 2015. World Journal Of Advanced Engineering Technology And Sciences, 11(1), 410-412. https://doi.org/10.30574/wjaets.2024.11.1.0024

Atkins, S., & Lawson, C. (2021). An improvised patchwork: success and failure in cybersecurity policy for critical infrastructure. Public Administration Review, 81(5), 847-861. https://doi.org/10.1111/puar.13322

Association for Computing Machinery (ACM). (2018). Ingeniería de software Código de Ética y Práctica Profesional 5.2. http://seeri.etsu.edu/Codes/SpanishVersionSECode.htm

Atzori, L., Iera, A., y Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787–2805. https://doi.org/https://doi.org/10.1016/j.comnet.2010.05.010

Azuero, J. S. C. (2023). Personal data processing and compliance in Colombia; [Tratamiento de datos personales y compliance en Colombia]. Revista de La Facultad de Derecho y Ciencias Politicas, 53(138), 1 – 25. https://doi.org/10.18566/rfdcp.v53n138.a2

Babar, S., Mahalle, P., Stango, A., Prasad, N., y Prasad, R. (2010). Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT). In N. Meghanathan, S. Boumerdassi, N. Chaki, & D. Nagamalai (Eds.), Recent Trends in Network Security and Applications (pp. 420–429). Springer Berlin Heidelberg.

Barrio Andrés, M. (2022). La regulación del derecho a la protección de datos en los Estados Unidos: hacia un RGPD norteamericano. CUADERNOS DE DERECHO TRANSNACIONAL, 14(2), 186-193. https://doi.org/10.20318/cdt.2022.7181

Bernabé, M. W., Gonzales, G. R., Campos, H., Lioo, F. de M., Vellón, V. I., de Salinas, F., Solano, T., y Caro, F. G. (2024). Project management based on ISO 21500, to improve productivity in the industry; [Gestión de proyectos basado en la ISO 21500, para mejorar la productividad en la industria]. Salud, Ciencia y Tecnologia - Serie de Conferencias, 3. https://doi.org/10.56294/sctconf2024928

Burton, J. (2023). Algorithmic extremism? The securitization of artificial intelligence (AI) and its impact on radicalism, polarization and political violence. Technology in Society, 75, 102262. https://doi.org/https://doi.org/10.1016/j.techsoc.2023.102262

CCPA. (2018). Cumplimiento de la Ley de Privacidad del Consumidor de California (CCPA).

Chehri, A., Fofana, I., y Yang, X. (2021). Security Risk Modeling in Smart Grid Critical Infrastructures in the Era of Big Data and Artificial Intelligence. Sustainability, 13(6). https://doi.org/10.3390/su13063196

Cintuglu, M. H., Mohammed, O. A., Akkaya, K., & Uluagac, A. S. (2017). A Survey on Smart Grid Cyber-Physical System Testbeds. IEEE Communications Surveys & Tutorials, 19(1), 446–464. https://doi.org/10.1109/COMST.2016.2627399

COMISIÓN EUROPEA. (2020). Dictamen del Comité Económico y Social Europeo sobre la «Propuesta de Reglamento del Consejo relativo a la apertura y el modo de gestión de contingentes arancelarios autónomos de la Unión para las importaciones de determinados productos de la pesca en las islas Canarias desde 2021 hasta 2027. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020AE4203

De Boer, P. S., Van Deursen, A., y Van Rompay, T. (2020). Accepting the Internet-of-Things in our homes: The role of user skills. Telematics and Informatics, 36, 147–156. https://doi.org/10.1016/j.tele.2018.12.004

De Montalvo, F. (n.d.). Principios éticos de la inteligencia artificial. https://plato.stanford.edu/entries/ethics-ai/.

Diario Oficial de la Unión Europea. (2022). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

Dignum, V. (2018). Ethics in artificial intelligence: introduction to the special issue. Ethics and Information Technology, 20(1), 1–3. https://doi.org/10.1007/s10676-018-9450-z

Dwork, C., & Roth, A. (2013). The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science, 9(3–4), 211–487. https://doi.org/10.1561/0400000042

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., y Vayena, E. (2018). AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. Minds and Machines, 28(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5

Floridi, L., & Sanders, J. W. (2004). On the Morality of Artificial Agents. Minds and Machines, 14(3), 349–379. https://doi.org/10.1023/B:MIND.0000035461.63578.9d

Frame, J. D. (2003). Book Review: Project Management: A Systems Approach to Planning, Scheduling, and Controlling. 8TH Edition. Project Management Journal, 34(4), 59-59. https://doi.org/10.1177/875697280303400409

Gilbreth, F. B., & Gilbreth, L. M. (1916). The Effect of Motion Study Upon the Workers. *The ANNALS of the American Academy of Political and Social Science*, *65*(1), 272-276. https://doi.org/10.1177/000271621606500130

González, A., Moreno, M., Román, A., Fernández, Y., y Pérez, N. (2024). Ethics in Artificial Intelligence: an Approach to Cybersecurity. Inteligencia Artificial, 27(73), 38–54. https://doi.org/10.4114/intartif.vol27iss73pp38-54

Gubbi, J., Buyya, R., Marusic, S., y Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645–1660. https://doi.org/https://doi.org/10.1016/j.future.2013.01.010

Gupta, B., y Quamara, M. (2020). Internet of Things Security: Principles, Applications, Attacks, and Countermeasures. CRC Press. https://doi.org/10.1201/9780429353529

Holland, J., Schmitt, P., Feamster, Nick y Mittal, P. 2021. New Directions in Automated Traffic Analysis. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS '21). Association for Computing Machinery, New York, NY, USA, 3366–3383. https://doi.org/10.1145/3460120.3484758.

ISO. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. https://doi.org/10.13140/RG.2.2.36267.52005

Jackson, C., y Orebaugh, A. (2020). A study of security and privacy issues associated with the Amazon Echo. International Journal of Internet of Things and Cyber-Assurance, 1(1), 91–100. https://doi.org/10.1504/IJITCA.2018.090172

Jacobsson, A., Boldt, M., y Carlsson, B. (2020). A risk analysis of a smart home automation system. Future Generation Computer Systems, 56, 719–733. https://doi.org/10.1016/j.future.2015.09.003

Jog, V., y Murugan, T. (2018). A Critical Analysis on the Security Architectures of Internet of Things: The Road Ahead. 27(2), 149–162. https://doi.org/doi:10.1515/jisys-2016-0032

Kandukuri, B., Ramakrishna ,V., y Rakshit, A. (2009). Cloud Security Issues. IEEE International Conference on Services Computing, 517–520. https://doi.org/10.1109/SCC.2009.84

Kaplan, A., y Haenlein, M. (2020). Rulers of the world, unite! The challenges and opportunities of artificial intelligence. Business Horizons, 63(1), 37–50. https://doi.org/https://doi.org/10.1016/j.bushor.2019.09.003

Khidzir, N., Mohamed, A., y Arshad, N. (2010). Information security risk factors: Critical threats vulnerabilities in ICT outsourcing. 2010 International Conference on Information Retrieval & Knowledge Management (CAMP), Shah Alam, Malaysia, 2010, pp. 194-199, doi: 10.1109/INFRKM.2010.5466918.

Klockmann, V., von Schenk, A., y Villeval, M. C. (2022). Artificial intelligence, ethics, and intergenerational responsibility. Journal of Economic Behavior & Organization, 203, 284–317. https://doi.org/https://doi.org/10.1016/j.jebo.2022.09.010

Kous, K. (2023). Process-oriented model for managing software development projects using the PRINCE2 method. In Innovation, Strategy, and Transformation Frameworks for the Modern Enterprise (pp. 30–59). https://doi.org/10.4018/979-8-3693-0458-7.ch002

Kowatsch, T., y Maass, W. (n.d.). Critical Privacy Factors of Internet of Things Services: An Empirical Investigation with Domain Experts [Discurso principal]. The 7th Mediterranean Conference on Information Systems (MCIS 2012), Zurich, Suiza. DOI:10.1007/978-3-642-33244-9_14

Lee, H. (2020). Home IoT resistance: Extended privacy and vulnerability perspective. Telematics and Informatics, 45-49. https://doi.org/10.1016/j.tele.2020.101377

Losavio, M., Chow, K., Koltay, A., y James, J. (2018). The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security. Security and Privacy, 1(3), e23. https://doi.org/10.3390/s23073681

Mayo, E. (1946). The Human Problems of an Industrial Civilization (1st ed.). Routledge. https://doi.org/10.4324/9780203487273.

McIntosh, T., Susnjak, T., Liu, T., Watters, P., Xu, D., Liu, D., Nowrozy, R., y Halgamuge, M. N. (2024). From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models. Computers and Security, 144. https://doi.org/10.1016/j.cose.2024.103964

Miraz, M., Ali, M., Excell, P., y Picking, R. (2015). A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT). 2015 Internet Technologies and Applications (ITA), 219–224. https://doi.org/10.1109/ITechA.2015.7317398

Mohammadi, M., Al-Fuqaha, A., Sorour, S., & Guizani, M. (2018). Deep Learning for IoT Big Data and Streaming Analytics: A Survey. IEEE Communications Surveys & Tutorials, 20(4), 2923–2960. https://doi.org/10.1109/COMST.2018.2844341

Nissenbaum, H. (2011). Privacidad en contexto: tecnología, política e integridad de la vida social. J Value Inquiry 45 , 97–102 (2011). https://doi.org/10.1007/s10790-010-9251-z

OECD. (2023). Artificial intelligence. https://doi.org/10.1787/dee339a8-en

OECD. (2024). Explanatory memorandum on the updated OECD definition of an AI system.OECD Artificial Intelligence Papers No.8, https://doi.org/10.1787/623da898-en.

Oriwoh, E., Sant, P., & Epiphaniou, G. (2013). Guidelines for Internet of Things Deployment Approaches – The Thing Commandments. Procedia Computer Science, 21, 122-131. https://doi.org/10.1016/j.procs.2013.09.018

Ortiz-Torres, L. F., Gómez-Luna, E., & Marlés-Sáenz, E. (2024). Estudio del uso y contribución de la inteligencia artificial para la operación en redes eléctricas. *Revista UIS Ingenierías*, *23*(2). https://doi.org/10.18273/revuin.v23n2-2024003

Parliament, E. (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. In Official Journal of the European Union. Office for Official Publications of the European Union Luxembourg.

Pathmabandu, C., Grundy, J., Chhetri, M. B., y Baig, Z. (2023). Privacy for IoT: Informed consent management in Smart Buildings. Future Generation Computer Systems, 145, 367–383. https://doi.org/https://doi.org/10.1016/j.future.2023.03.045

Rao, M. A. (2018). Security and Privacy in IoT-Based Smart Grid: A Survey. In Proceedings of the International Conference on Wireless Communications, Signal Processing and Networking (pp. 185-192). Springer, Singapore. doi:10.1007/978-981-10-8363-6_18

Saleem, Y., Crespi, N., Rehmani, M., y Copeland, R. (2019). Internet of things-aided smart grid: technologies, architectures, applications, prototypes, and future research directions. IEEE Access, 7, 62962–63003. doi: 10.1109/ACCESS.2019.2913984.

Sánchez, M., Bermejo, J., Bermejo, J, Sicilia, J., y González, R. (2021). A systematic approach to analysis for assessing the security level of cyber-physical systems in the electricity sector. Microprocessors and Microsystems, 87, 104352. https://doi.org/https://doi.org/10.1016/j.micpro.2021.104352

Smith, A. (1794). An Inquiry into the Nature and Causes of the Wealth of Nations (pp.23). En Valladolid: en la Oficina de la Viuda e Hijos de Santander. 10.7208/chicago/9780226763750.001.0001

Solove, D. (2008). Understanding Privacy. https://doi.org/10.3366/elr.2010.0323

Sommerville, I. (2011). Software engineering. (9a edición, pp. 45 -50). Pearson. https://gc.scalahed.com/recursos/files/r161r/w25469w/ingdelsoftwarelibro9_compressed.pdf

Taylor, F. (1911). Principios de la administración científica. New York: Harper & Brothers Publishers. First edition

Trilles, S., Hammad, S., y Iskandaryan, D. (2024). Anomaly detection based on Artificial Intelligence of Things: A Systematic Literature Mapping. Internet of Things, 25, 101063. https://doi.org/https://doi.org/10.1016/j.iot.2024.101063

UNESCO. (2021). UNESCO's Input in reply to the OHCHR report on the Human Rights Council Resolution 47/23 entitled "New and emerging digital technologies and human rights" UNESCO Recommendation on the Ethics of Artificial Intelligence. https://www.broadbandcommission.org/ai-capacity-building/

UNESCO. (2022). Recommendation on the Ethics of Artificial Intelligence. www.unesco.org/open-

Winter, J., y Davidson, E. (2019). Governance of artificial intelligence and personal health information. Digital Policy, Regulation and Governance, 21(3), 280–290. https://doi.org/10.1108/DPRG-08-2018-0048

Yilmaz, S., Kumar, D., Hada, S., Demirkesen, S., Zhang, C., y Li, H. (2024). A PMBOK-based construction cost management framework for BIM integration in construction projects. International Journal of Construction Management. https://doi.org/10.1080/15623599.2024.2371626

Zarca, A., Bernabe, J., Trapero, R., Rivera, D., Villalobos, J., Skarmeta, A., Bianchi, S., Zafeiropoulos, A., y Gouvas, P. (2019). Security Management Architecture for NFV/SDN-Aware IoT Systems. IEEE Internet of Things Journal, 6(5), 8005–8020. https://doi.org/10.1109/JIOT.2019.2904123