ESTRATEGIAS PARA IMPLEMENTAR IA ÉTICA Y SEGURA EN REDES ELÉCTRICAS CON IoT

Estrategias de Gerencia de Proyectos para la Implementación Ética y Segura de IA en Redes Eléctricas con Integración de IoT

Luis Ferney Ortiz Torres

Corporación Universitaria Minuto de Dios

Rectoría Virtual

Programa Especialización en Gerencia de Proyectos

agosto de 2024

ESTRATEGIAS PARA IMPLEMENTAR IA ÉTICA Y SEGURA EN REDES ELÉCTRICAS CON IoT

Estrategias de Gerencia de Proyectos para la Implementación Ética y Segura de IA en Redes Eléctricas con Integración de IoT

Luis Ferney Ortiz Torres

Trabajo de Grado presentado como requisito para optar al título de Especialista en Gerencia de Proyectos

Asesor(a)
Henry Alberto Rodríguez Guzmán
M.Sc en Administración de Empresas

Corporación Universitaria Minuto de Dios

Rectoría Virtual

Programa Especialización en Gerencia de Proyectos

agosto de 2024

Contenido

Lista de tablas

Lista de figuras

Resumen

Este trabajo de investigación aborda el desarrollo de estrategias para implementar soluciones de inteligencia artificial (IA) de manera ética y segura en la gestión de redes eléctricas, con la integración de dispositivos del Internet de las Cosas (IoT). El objetivo principal es garantizar la privacidad y la seguridad de los datos, así como optimizar la eficiencia operativa de las redes eléctricas. La investigación se enfoca en la identificación de técnicas avanzadas de IA, la evaluación de riesgos y vulnerabilidades, y la adopción de estándares internacionales y mejores prácticas.

***Palabras clave**:* Inteligencia Artificial (IA), Internet de las Cosas (IoT), Privacidad de Datos, Gerencia de Proyectos, Ética en IA.

Estrategias para implementar IA ética y segura en redes eléctricas con IoT

Abstract

This research work addresses the development of strategies to implement artificial intelligence (AI) solutions in an ethical and secure way in the management of power grids, with the integration of Internet of Things (IoT) devices. The main objective is to ensure data privacy and security, as well as to optimize the operational efficiency of power grids. The research focuses on identifying advanced AI techniques, assessing risks and vulnerabilities, and adopting international standards and best practices.

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

Introducción

En el contexto actual de creciente demanda energética y urgencia por reducir las emisiones de carbono, la gestión eficiente de la energía eléctrica se ha convertido en un factor clave para el desarrollo sostenible y el bienestar de las sociedades. Las redes eléctricas, que tradicionalmente han dependido de infraestructuras y métodos convencionales, están experimentando una transformación significativa impulsada por la integración de tecnologías avanzadas como la inteligencia artificial (IA) y el Internet de las Cosas (IoT). Estas innovaciones ofrecen potenciales mejoras en la eficiencia operativa, optimización de la distribución de energía y facilitan la transición hacia fuentes de energía renovable.

Sin embargo, esta evolución tecnológica no está exenta de desafíos. La implementación de soluciones de IA y IoT en redes eléctricas implica la recopilación masiva y el procesamiento de datos en tiempo real, lo cual plantea serias preocupaciones respecto a la privacidad de los usuarios y la seguridad de la información crítica. Este fenómeno aumenta la exposición de las infraestructuras a posibles ciberataques y a vulnerabilidades en la gestión de datos sensibles (Rao, 2018, p. 10). En este contexto, es imperativo desarrollar e implementar estrategias que no solo optimicen el rendimiento de las redes eléctricas, sino que también aseguren la protección de la información y el respeto a los derechos de privacidad.

Las estrategias de gerencia de proyectos desempeñan un papel fundamental para abordar estos desafíos. Un enfoque riguroso en la gestión de proyectos permite garantizar que la integración de tecnologías emergentes como la IA y el IoT se realice de manera ética y eficiente, cumpliendo con las normativas de privacidad y seguridad. Al adoptar prácticas y políticas que promuevan la transparencia, la responsabilidad y el cumplimiento regulatorio, las organizaciones pueden mitigar los riesgos asociados con la integración de dispositivos IoT en redes eléctricas, maximizando a su vez los beneficios que estas tecnologías pueden ofrecer para la sociedad en su conjunto.

1. PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción del problema

En la era contemporánea 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 vital para mejorar la eficiencia operativa y garantizar la confiabilidad del suministro de energía. La aplicación de algoritmos de IA en la optimización de la distribución de energía y en el pronóstico de la demanda energética ha demostrado ser fundamental para responder de manera más ágil y efectiva a las fluctuaciones del mercado y a las condiciones operativas variables (Abd Elazim y Ali, 2016).

Kandukuri et al. (2009) afirman que “la IA juega un papel crucial en la detección y prevención de fallas en la red eléctrica, lo que contribuye significativamente a la reducción de tiempos de inactividad y a la mejora de la calidad del servicio”. Sin embargo, la adopción de tecnologías de IA en el contexto de las redes eléctricas conlleva importantes desafíos en términos de privacidad y seguridad de los datos. La interconexión de dispositivos del Internet de las Cosas (IoT) y sistemas de monitoreo en entornos residenciales e industriales agrega una capa adicional de complejidad y vulnerabilidad (Miraz et al., 2015).

La gran cantidad de datos generados por estos dispositivos, combinada con la capacidad de procesamiento de la IA, plantea preocupaciones sobre la protección de la privacidad de los usuarios y la seguridad de la información sensible (Al-Fuqaha et al., 2015). En este contexto, la gerencia de proyectos desempeña un papel fundamental en la implementación ética y efectiva de soluciones de IA en redes eléctricas. La gestión de riesgos, la planificación estratégica y la adopción de prácticas de seguridad cibernética son aspectos clave que deben ser abordados de manera integral. Además, es fundamental considerar los principios éticos en el diseño e implementación de sistemas de IA, asegurando la transparencia, la equidad y el respeto a la privacidad de los individuos (Floridi et al., 2018, p. 30).

La colaboración entre diferentes partes interesadas, incluidos los reguladores, los expertos en ciberseguridad y los profesionales de la energía, es esencial para garantizar que se aborden adecuadamente los desafíos de privacidad y seguridad de datos en proyectos de IA en redes eléctricas. Este asunto es de naturaleza compleja y demanda una comprensión holística de las consecuencias éticas y prácticas que conlleva la implementación de soluciones de IA en un ámbito tan crucial como el sector energético. La solución a este problema no solo engloba consideraciones técnicas e ingenieriles, sino que también abarca aspectos éticos, legales y de administración de proyectos.

1.2 La pregunta de investigación

¿Cómo puede la gerencia de proyectos asegurar la implementación efectiva y ética de soluciones de inteligencia artificial para abordar los desafíos de privacidad y seguridad de datos en la gestión y optimización de la red eléctrica, particularmente al integrar dispositivos IoT y sistemas de monitorización en entornos residenciales e industriales?

1.3 Los objetivos de investigación

1.3.1 Objetivo general

Establecer un marco de gestión de proyectos para la implementación ética de soluciones de inteligencia artificial en la gestión de la red eléctrica, con un enfoque en la privacidad y seguridad de datos al integrar dispositivos IoT y sistemas de monitorización en entornos residenciales e industriales.

1.3.2 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.**

- Realizar una investigación exhaustiva sobre artículos científicos que aborden diferentes soluciones de inteligencia artificial disponibles en el mercado, considerando su capacidad para abordar los desafíos específicos de la gestión y optimización de la red eléctrica.
- Evaluar las características de privacidad y seguridad de datos de cada solución, prestando especial atención a la forma en que manejan la información sensible y protegen contra posibles amenazas cibernéticas.
- Seleccionar y documentar las soluciones que mejor se ajusten a los requisitos de privacidad y seguridad de datos identificados, priorizando aquellas que cuenten con certificaciones o estándares reconocidos en el campo de la ciberseguridad.

2. **Especificar los requisitos de privacidad y seguridad de datos, identificando posibles vulnerabilidades y riesgos asociados con la integración de dispositivos IoT y sistemas de monitoreo en entornos residenciales e industriales.**
    - Realizar un análisis detallado de los posibles riesgos y vulnerabilidades asociados con la integración de dispositivos IoT y sistemas de monitoreo en entornos residenciales e industriales.
    - Definir los requisitos de privacidad y seguridad de datos que deben cumplir las soluciones de inteligencia artificial seleccionadas, incluyendo medidas específicas para proteger la confidencialidad, integridad y disponibilidad de la información.
    - Identificar y documentar los controles de seguridad necesarios para mitigar los riesgos identificados, asegurando que se apliquen de manera efectiva durante todo el ciclo de vida del proyecto.

3. **Identificar estándares internacionales y mejores prácticas para la implementación ética de soluciones de inteligencia artificial en la gestión de redes eléctricas, enfocándose en la privacidad y seguridad de datos.**
    - Realizar una investigación exhaustiva sobre los estándares internacionales y las mejores prácticas en la implementación ética de inteligencia artificial en redes eléctricas.

- Evaluar la aplicabilidad de estos estándares y prácticas a los requisitos específicos de privacidad y seguridad de datos en entornos residenciales e industriales.
- Seleccionar y documentar las normativas y directrices que mejor se adapten a los principios éticos y necesidades de seguridad de la implementación de inteligencia artificial en la gestión de redes eléctricas.

4. **Documentar la gestión de riesgos, la planificación estratégica y las prácticas de seguridad cibernética 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.**
    - Realizar una búsqueda exhaustiva de los diferentes marcos de gestión de proyectos adaptados a las necesidades específicas de la implementación de soluciones de inteligencia artificial en redes eléctricas, incorporando procesos claros y prácticas recomendadas para abordar los riesgos relacionados con la privacidad y seguridad de datos.
    - Validar actividades específicas para la identificación, evaluación y mitigación de riesgos en un plan de proyecto, que permitan la asignación de responsabilidades claras y estableciendo plazos realistas para su ejecución.
    - Integrar y documentar conforme la investigación anterior, la gestión de riesgos, la planificación estratégica y las prácticas de seguridad cibernética 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.

1.4 Justificación de la investigación

El desarrollo e implementación de soluciones basadas en inteligencia artificial (IA) para la gestión de redes eléctricas representan un avance significativo con el potencial de mejorar la eficiencia operativa y la confiabilidad del suministro energético. No obstante, esta integración tecnológica plantea desafíos importantes en términos de privacidad y seguridad de los datos, especialmente en un entorno de creciente interconexión de dispositivos IoT en entornos residenciales e industriales.

Este proyecto de investigación surge de la necesidad de establecer un enfoque sistemático y estructurado para la implementación de soluciones de IA en la gestión de redes eléctricas. Este enfoque debe no solo garantizar la mejora en la eficiencia operativa, sino también asegurar la protección de la privacidad y la seguridad de los datos, minimizando los riesgos asociados con la vulnerabilidad de los sistemas ante posibles ataques cibernéticos.

Implementar un marco de gestión de proyectos específicamente diseñado para este propósito permitirá a las organizaciones afrontar los desafíos técnicos, éticos y regulatorios asociados con la integración de soluciones de IA en contextos energéticos complejos. Además, asegurará que la adopción de estas tecnologías se realice de manera transparente, eficiente y ética, alineándose con las mejores prácticas internacionales en gestión de proyectos y estándares de seguridad. De este modo, se contribuirá a una implementación más segura y confiable de soluciones tecnológicas innovadoras en las redes eléctricas, reforzando la confianza pública y promoviendo un desarrollo sostenible.

2. Marco de Referencia

El marco de referencia explora diferentes conceptos desde la gerencia de proyectos, la tecnología, ética, normativas y la protección de los datos, lo que enmarca un panorama holístico, con el fin de obtener una base sólida para validar desde la gerencia de proyectos la implementación efectiva y ética de soluciones de inteligencia artificial.

El presente estado del arte abarca diferentes referencias que ponen en evidencia la necesidad de desarrollar marcos éticos sólidos para guiar el desarrollo y la implementación de la inteligencia artificial (IA). Estos marcos éticos deben tener en cuenta no solo los aspectos técnicos de estas tecnologías, sino también sus implicaciones sociales, legales y éticas.

En particular, es crucial que las organizaciones consideren cómo la IA puede afectar los derechos individuales y la autonomía humana. La recopilación y el uso de datos personales por parte de sistemas de IA plantean desafíos importantes en términos de privacidad y consentimiento informado. Además, la necesidad de abordar sesgos y errores en los algoritmos de toma de decisiones algorítmicas es un área crítica de investigación.

"Antes de implementar una nueva herramienta de IA, una organización debe desarrollar principios éticos claves para guiar la toma de decisiones sobre la adopción y el uso de la herramienta. La Organización Mundial de la Salud proporciona una serie de principios clave que pueden considerarse, incluido el principio de evitar daños y la protección de la autonomía humana, entre otros".

"Si una IA debe tomar decisiones en nombre de un individuo o una sociedad, necesita conocer las preferencias de ese individuo o sociedad. Dado que se ha demostrado que una multitud de factores sociales, como el altruismo, el egoísmo y la reciprocidad, median el juego de las personas en interacciones estratégicas, esto comprende algoritmos de aprendizaje y modelado de preferencias sociales"(Klockmann et al., 2022).

"Incluso si el diseño de los sistemas de IA y los datos con los que se entrenan son de alta calidad (algo difícil de determinar en sí mismo), entonces la forma en que se utiliza la IA se convierte en un problema importante. Incluso una IA bien diseñada que utilice datos precisos puede utilizarse de forma maliciosa. La IA ya se está utilizando para limitar aún más los objetivos geoestratégicos y económicos y, de hecho, para llevar a cabo delitos cibernéticos"(Burton, 2023).

Ahora, una de las particularidades de la IA es que debe complementarse con herramientas físicas como sensores, los cuales se han catalogado en el término de IoT. A continuación, en el presente estado del arte se describe un poco de esta tecnología y su implicación en el contexto de esta investigación.

IoT es el elemento clave para llevar un sistema existente a los estándares de la Industria 4.0; sin embargo, los sistemas de IoT son propensos a sufrir riesgos de seguridad.

"Una anomalía en el contexto de IoT se refiere a los efectos mensurables de un cambio inesperado en el estado de un sistema que se desvía de su comportamiento habitual, ya sea a nivel local o global (Trilles et al., 2024).

"Aunque los dispositivos IoT ofrecen numerosas ventajas, también presentan desafíos debido a su susceptibilidad a amenazas y ataques a la seguridad" (Ksibi et al., 2023).

"La clonación de dispositivos se refiere a la imitación de dispositivos para realizar actividades maliciosas en el entorno de IoT. La suplantación de sensores se ha presentado como un tipo de ataque de canal lateral" (Vidhate, 2017).

Dado que las personas están rodeadas de un número cada vez mayor de sensores inteligentes, resulta complicado expresar sus opciones de consentimiento de privacidad de forma electrónica. "La mayoría de los dispositivos utilizados para recopilar datos en entornos de edificios inteligentes orientados a la IoT tienen recursos limitados, funcionan con baterías o son pasivos, es decir, sin ninguna interfaz de usuario" (Pathmabandu et al., 2023).

Como señala Davidson (2019), "el consentimiento es especialmente problemático para la IA, ya que la opacidad es inherente cuando se hace referencia a datos recopilados previamente".

"Además de ser importante en sí mismo, dotar a los sistemas de IA de valores y directrices éticas también será crucial, ya que una dependencia cada vez mayor de la IA hará que las normas y acciones existentes de las empresas sean más transparentes para el mundo exterior. Un sistema de inteligencia artificial que haya sido entrenado con datos sesgados o erróneos formalizará y amplificará dichos errores" (Haenlein, 2020).

Este análisis del estado del arte destaca la creciente importancia de desarrollar marcos éticos sólidos para guiar el desarrollo y la implementación de la inteligencia artificial (IA). Los autores subrayan la necesidad de considerar no solo los aspectos técnicos de la IA, sino también sus implicaciones sociales, legales y éticas. Coinciden en la importancia de proteger los derechos

individuales y la autonomía humana, así como en la necesidad de abordar desafíos como la privacidad de los datos, la transparencia en los algorítmicos y el uso incorrecto de la IA.

2.1.Marco de Antecedentes

La implementación de soluciones de inteligencia artificial (IA) en la gestión y optimización de redes eléctricas representa una oportunidad significativa para mejorar la eficiencia, la resiliencia y la seguridad de estas infraestructuras críticas. Este marco de antecedentes se centra en evaluar las investigaciones previas y las prácticas actuales en el campo, con un enfoque particular en la privacidad y la seguridad de los datos, así como en la gestión de riesgos y la implementación ética de estas tecnologías.

La investigación sobre la aplicación de la IA en redes eléctricas ha mostrado avances importantes en diversas áreas. Según Mohammadi et al. (2018), las técnicas de aprendizaje profundo y aprendizaje automático han permitido desarrollar sistemas avanzados de predicción de demanda y detección de anomalías, mejorando significativamente la eficiencia operativa y la capacidad de respuesta de las redes eléctricas. Estos sistemas utilizan grandes volúmenes de datos generados por sensores y dispositivos IoT para optimizar la distribución de energía y reducir las pérdidas.

Sin embargo, la integración de dispositivos IoT en redes eléctricas también introduce riesgos significativos en términos de privacidad y seguridad de los datos. Murugan, (2018) señala que “la expansión de la superficie de ataque debido a la proliferación de dispositivos conectados incrementa el riesgo de ciberataques, que pueden tener consecuencias catastróficas para la estabilidad y seguridad de las redes eléctricas”. En este contexto, es crucial realizar una evaluación exhaustiva de las características de privacidad y seguridad de cada solución de IA.

Chehri et al. (2021) destacan la necesidad de incorporar medidas robustas de seguridad en las soluciones de IA para redes eléctricas, incluyendo el cifrado de datos, la autenticación multifactor y el monitoreo continuo de la red. Estos enfoques ayudan a proteger la información sensible y a mitigar las amenazas cibernéticas. Además, la selección de soluciones que cumplan

con certificaciones y estándares reconocidos en el campo de la ciberseguridad, como ISO/IEC 27001, es esencial para garantizar la confiabilidad y la seguridad de la implementación.

La definición de requisitos de privacidad y seguridad es otro aspecto crítico en la implementación de soluciones de IA en redes eléctricas. Según Babar et al. (2010), es fundamental identificar y documentar los controles de seguridad necesarios para mitigar los riesgos asociados con la integración de dispositivos IoT. Estos controles deben aplicarse de manera efectiva durante todo el ciclo de vida del proyecto, desde la definición de requisitos hasta la implementación y operación continua de las soluciones de IA.

Además de los aspectos técnicos, la implementación ética de soluciones de IA en la gestión de redes eléctricas requiere la adopción de estándares internacionales y mejores prácticas. Cintuglu et al. (2017) sugieren que "la adopción de estándares como el IEEE 1547 y el NIST Cybersecurity Framework es crucial para garantizar la interoperabilidad y la seguridad de las soluciones de IA" (p.20). Estas normativas proporcionan directrices claras para la protección de la privacidad y la seguridad de los datos, así como para la resiliencia ante ciberataques.

Floridi et al. (2018) abogan por una combinación de estándares técnicos y principios éticos en la implementación de IA, enfatizando la necesidad de proteger los derechos y la seguridad de los usuarios. La documentación de las normativas y directrices que mejor se adapten a los principios éticos y necesidades de seguridad es fundamental para una implementación efectiva y responsable.

Finalmente, la gestión de riesgos y la planificación estratégica son componentes esenciales en la implementación de soluciones de IA en redes eléctricas. Kerzner (2009) resalta la importancia de adaptar los marcos de gestión de proyectos para abordar los riesgos únicos asociados con la implementación de tecnologías avanzadas en infraestructuras críticas. Esto incluye la validación de actividades específicas para la identificación, evaluación y mitigación de riesgos, así como la asignación de responsabilidades claras y la definición de plazos realistas.

Sommerville (2011) enfatiza en la importancia de documentar detalladamente la gestión de riesgos y la planificación estratégica en todas las etapas del ciclo de vida del proyecto. La integración de prácticas de seguridad cibernética, desde la definición de requisitos hasta la

implementación y operación continua, es crucial para asegurar la continuidad y protección de las soluciones de IA.

2.2. Marco Teórico

Esta investigación se basa en la teoría de la administración de Tylor, debido a su importancia histórica, su relevancia continua, su enfoque en la eficiencia y su aplicabilidad interdisciplinaria.

Teoría de la administración de Tylor. "La teoría de la administración científica, propuesta por Frederick Winslow Taylor a principios del siglo XX, se centra en la eficiencia y la productividad en el trabajo" (Taylor, 1911). Taylor abogaba por el análisis científico de las tareas laborales para identificar los métodos más eficientes y eliminar el desperdicio de tiempo y recursos. Sus principios de gestión han sido ampliamente adoptados en la gestión de proyectos para mejorar la planificación, ejecución y control de las actividades.

Aplicación en la Gestión de Proyectos de IA e IoT. La gestión de proyectos relacionados con la implementación de soluciones de inteligencia artificial (IA) en la gestión de la red eléctrica puede beneficiarse de los principios de la administración científica de Taylor, los cuales se centran en mejorar la eficiencia y la productividad en el trabajo industrial. En este contexto, se pueden destacar varias áreas de aplicación de estos principios:

1. Análisis de tiempos y movimientos: "la aplicación de esta técnica permite analizar detalladamente los procesos involucrados en la integración de dispositivos del Internet de las Cosas (IoT) y sistemas de monitorización en entornos residenciales e industriales" (Gilbreth, 2006, p.34). Analizar los periodos y acciones requeridos para cada labor, facilita la detección de fallos operativos y permite idear estrategias más productivas.

2. Diseño de métodos eficientes: una vez identificadas las áreas de mejora a través del análisis de tiempos y movimientos, se pueden diseñar métodos más eficientes para llevar a cabo las tareas necesarias en la implementación de soluciones de IA (Smith, 1794, p.

23). Lo anterior, puede incluir la estandarización de procesos y la implementación de mejores prácticas.

3. División del trabajo: asignar responsabilidades específicas a los miembros del equipo de proyecto con base en sus habilidades y especializaciones, permite maximizar la eficiencia en la ejecución del proyecto. Cada miembro del equipo se enfocará en tareas específicas, lo que agiliza el proceso y reduce los tiempos de ejecución.

4. Colaboración entre gerencia y trabajadores: promover una estrecha colaboración entre la gerencia y los trabajadores es fundamental para implementar con éxito las mejoras propuestas. “La gerencia puede proporcionar el apoyo necesario y los recursos adecuados, mientras que los trabajadores pueden ofrecer perspectivas valiosas sobre la viabilidad y eficacia de las soluciones propuestas” (mayo, 1946, p.10).

5. Incentivos salariales: implementar un sistema de incentivos salariales basado en la productividad puede motivar a los miembros del equipo a alcanzar los objetivos del proyecto de manera eficiente y oportuna. Reconocer y recompensar el desempeño excepcional fomenta un ambiente de trabajo colaborativo y orientado a resultados.

2.3. Marco Conceptual

Las estrategias de gerencia de proyectos para la implementación ética y efectiva de soluciones de IA en redes eléctricas con dispositivos IoT se basan en varios principios fundamentales. En primer lugar, es crucial establecer políticas claras de privacidad y protección de datos. Además, se deben implementar medidas técnicas robustas, como el cifrado de datos y la autenticación de dispositivos, para proteger contra amenazas cibernéticas. La transparencia y la rendición de cuentas también son aspectos clave, con la necesidad de establecer 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 de autores:

Según Dwork Roth (2013) "la privacidad de los datos se refiere al 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".

Según Solove (2008) "la privacidad de los datos es el derecho de las personas a determinar qué información sobre ellas mismas quieren revelar, con quién quieren compartirla y bajo qué condiciones".

Según Nissenbaum (s. f.) "la privacidad de los datos se trata de proteger la autonomía individual y el control sobre la información personal, preservando así la capacidad de las personas para determinar cómo se les percibe y cómo interactúan con su entorno".

Los autores coinciden en varios aspectos relacionados con la definición de la privacidad de los datos:

1. Reconocen la importancia de la privacidad de los datos como un derecho humano fundamental.
2. Destacan el papel del individuo en el control de su información personal.
3. Se refieren al proceso de recopilación, uso, compartición y almacenamiento de datos por parte de terceros.

A continuación, se describen algunas diferencias en sus definiciones:

1. Dwork Roth (2013) enfatizan en el control que tienen los individuos sobre su información, así como su capacidad para decidir cómo se manejan sus datos por parte de terceros.
2. Solove (2008)coloca énfasis en la capacidad de las personas para determinar qué información desean revelar, con quién desean compartirla y en qué condiciones, lo que sugiere un enfoque más orientado hacia las decisiones individuales.
3. Nissenbaum (s. f.) resalta la protección de la autonomía individual y el control sobre la información personal, con un enfoque más amplio que incluye la percepción social y la interacción del individuo con su entorno.

Para esta investigación se entenderá la privacidad de los datos como: el derecho fundamental que tienen las personas para controlar qué información personal suya se recopila, cómo se utiliza, quién tiene acceso a ella y con qué fines se utiliza, 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. A continuación, se presentan algunas definiciones propuestas de autores:

Según Floridi y Sanders (2004) indica 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)expresa 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) manifiesta 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, con el fin de asegurar su alineación con los valores humanos fundamentales".

Estos autores coinciden en varios aspectos relacionados con la definición de ética en la Inteligencia Artificial (IA):

1. Todos los autores reconocen la importancia de la ética en la inteligencia artificial (IA) como un campo interdisciplinario que aborda cuestiones éticas y morales relacionadas con el diseño, desarrollo, implementación y uso de sistemas de IA.
2. Todos enfatizan la necesidad de analizar y reflexionar sobre cómo las decisiones y acciones de los sistemas de IA afectan a los individuos, las sociedades y el medio ambiente.
3. Cada definición busca garantizar que las tecnologías de IA se utilicen de manera justa, responsable y alineada con los valores humanos fundamentales.

   Diferencias:

1. Enfoque de la definición: Floridi (2019) presenta la ética en la IA como un campo interdisciplinario que busca promover el bienestar humano y social. Dignum (2018) se

enfoca en el análisis y reflexión sobre las decisiones y acciones de los sistemas de IA y cómo garantizar su uso justo y responsable. González et al. (2024) 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 IA.

2. Alcance de la ética: Mientras que Floridi (2019) y González et al. (2024) se enfocan en aspectos más generales de la ética en la IA, Dignum (2018) se centra específicamente en cómo las decisiones y acciones de los sistemas de IA afectan a los individuos, las sociedades y el medio ambiente.
3. Objetivo final: Floridi (2019) y González et al. (2024) buscan promover el bienestar humano y social a través de la ética en la IA, mientras que Dignum (2018) busca garantizar el uso justo y responsable de estas tecnologías.

Para esta investigación se entenderá la ética en la inteligencia artificial como: La ética en la inteligencia artificial es 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). A continuación, se presentan algunas definiciones propuestas de autores:

Ashton (2009) "El Internet de las cosas se refiere a 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) "El Internet de las cosas es un paradigma emergente que se refiere a la conexión y la comunicación de objetos físicos a través de la internet, permitiendo la monitorización, el control y la gestión remota de estos objetos".

Atzori et al. (2010) "El Internet de las cosas se refiere a la infraestructura global de información y comunicación, habilitada para la interconexión y la integración de objetos físicos y virtuales basada en la capacidad de generación de información sensorial, la comunicación inalámbrica y el procesamiento inteligente".

Estos autores coinciden en varios aspectos relacionados con la definición del Internet de las cosas (IoT):

1. Todos reconocen al IoT como un paradigma emergente que implica la interconexión de dispositivos físicos a través de la internet.
2. Coinciden en que el IoT permite la recopilación, intercambio y procesamiento de datos entre los dispositivos conectados.
3. Todos destacan que el IoT facilita la automatización de tareas y procesos, así como la monitorización y el control remoto de objetos físicos.

Sin embargo, también presentan algunas diferencias sutiles en sus definiciones:

1. Ashton hace hincapié en la eficiencia y comodidad que el IoT aporta en diversos contextos.
2. Gubbi et al. (2013)subrayan la importancia de la comunicación y la gestión remota de los objetos conectados.
3. Atzori et al. (2010) enfatizan la capacidad de generación de información sensorial y el procesamiento inteligente como aspectos clave del IoT.

Para esta investigación se entenderá IoT 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, entre otros

2.4. Marco normativo

A continuación, se explorarán algunas dimensiones legales y éticas relacionadas con el marco legal y ético para garantizar una implementación efectiva y ética de la IA en el sector eléctrico.

1. Regulaciones y Legislación

La regulación de la IA en el contexto de la gestión de la red eléctrica está influenciada por diversas normativas y leyes que abordan la protección de datos, la ciberseguridad y la privacidad. “Es fundamental considerar regulaciones internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, así como legislaciones nacionales y locales específicas en el ámbito de la energía y la tecnología” (Diario Oficial de la Unión Europea, 2016, p. 60).

2. Principios Éticos

"Los principios éticos guían el desarrollo y uso de la IA en la gestión de la red eléctrica, incluyendo la transparencia, la responsabilidad, la equidad y el respeto a la privacidad y los derechos humanos. Estos principios proporcionan un marco ético para la toma de decisiones y la implementación de tecnologías de IA de manera ética y responsable" (Floridi y Sanders, 2004).

3. Responsabilidad Legal

La responsabilidad legal en el contexto de la IA abarca cuestiones como la responsabilidad civil, la responsabilidad por productos defectuosos y la responsabilidad por el uso indebido de datos. Es crucial determinar las responsabilidades legales de las partes involucradas en la implementación y operación de sistemas de IA en la red eléctrica.

4. Gobernanza y Supervisión

La gobernanza y supervisión adecuadas son esenciales para garantizar el cumplimiento de las regulaciones y principios éticos en el uso de IA en la gestión de la red eléctrica. Esto puede implicar la creación de comités de ética, la auditoría de algoritmos y la participación de múltiples partes interesadas en el proceso de toma de decisiones (Ospino, 2023, p.56).

5. Seguridad Cibernética

La seguridad cibernética es fundamental para mitigar los riesgos asociados con la integración de dispositivos IoT y sistemas de monitorización en la red eléctrica. Se deben implementar medidas de seguridad de la información, detección de intrusiones y respuesta a incidentes de seguridad para proteger los datos y sistemas críticos.

Tecnología de la información y comunicación

Uno de los principales enfoques de la IA en este contexto es el uso de algoritmos de aprendizaje automático para analizar grandes volúmenes de datos generados por los dispositivos IoT. Estos algoritmos pueden identificar patrones y anomalías en tiempo real, lo que permite una detección temprana de posibles problemas en la red eléctrica y una respuesta rápida para mitigarlos.

Además, la IA se utiliza para desarrollar sistemas de detección de intrusiones avanzados que pueden identificar y responder a ataques cibernéticos de manera proactiva. Estos sistemas pueden detectar comportamientos maliciosos y tomar medidas correctivas antes de que causen daños significativos a la infraestructura eléctrica.

Experiencias y mejores prácticas

La implementación de inteligencia artificial (IA) en la gestión de redes eléctricas, especialmente al integrar dispositivos IoT y sistemas de monitorización, ha sido fundamental para abordar desafíos de privacidad y seguridad de datos en entornos residenciales e industriales. Algunas experiencias y mejores prácticas destacadas incluyen:

Detección temprana de fallas: "los algoritmos de IA pueden analizar grandes volúmenes de datos recopilados por dispositivos IoT para identificar patrones anómalos que sugieran posibles fallas en la red eléctrica. Esto permite una intervención rápida y eficiente para prevenir interrupciones del suministro eléctrico" (Franco et al., 2017, p. 45).

Gestión proactiva de la carga: "la IA puede predecir la demanda de energía en diferentes momentos del día en base a datos históricos y patrones de uso para maximizar la eficiencia energética" (Ruiz, s. f.)

Seguridad cibernética avanzada: mediante el uso de algoritmos de aprendizaje automático, se pueden desarrollar sistemas de detección de intrusiones que identifiquen y respondan a posibles ataques cibernéticos en tiempo real (Pineda et al., 2022). Estos sistemas pueden detectar comportamientos maliciosos y tomar medidas correctivas para proteger la red eléctrica contra amenazas externas.

Protección de datos sensibles: "la IA puede cifrar datos sensibles recopilados por dispositivos IoT y sistemas de monitorización para proteger la privacidad de los usuarios finales" (García, 2012, p. 27). Además, los algoritmos de IA pueden identificar intentos de acceso no autorizado y prevenir fugas de información mediante la monitorización continua de la red.

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.	(Comité Interamericano, 2021)

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

3. Metodología

1. **Objetivo Específico 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.**

    - **Investigación Exhaustiva**

        1. **Actividad:** Revisar literatura científica y artículos relevantes sobre soluciones de inteligencia artificial en la gestión de redes eléctricas.
        2. **Resultados Esperados:** Informe con un análisis detallado de las diferentes soluciones de IA disponibles en el mercado y su capacidad para abordar desafíos específicos.

    - **Evaluación de Privacidad y Seguridad de Datos**

        1. **Actividad:** Evaluar las características de privacidad y seguridad de cada solución de IA, con especial atención a la gestión de información sensible y protección contra amenazas cibernéticas.
        2. **Resultados Esperados:** Documento con la evaluación de privacidad y seguridad de cada solución de IA.

    - **Selección y Documentación de Soluciones**

        1. **Actividad:** Seleccionar las soluciones de IA que mejor se ajusten a los requisitos de privacidad y seguridad de datos, priorizando aquellas con certificaciones o estándares reconocidos en ciberseguridad.
        2. **Resultados Esperados:** Informe con la selección y documentación de las soluciones de IA adecuadas.

2. **Objetivo Específico 2: Especificar los requisitos de privacidad y seguridad de datos, identificando posibles vulnerabilidades y riesgos asociados con la integración de dispositivos IoT y sistemas de monitoreo en entornos residenciales e industriales.**

1. **Análisis de Riesgos y Vulnerabilidades**
    - **Actividad:** Realizar un análisis detallado de los posibles riesgos y vulnerabilidades asociados con la integración de dispositivos IoT y sistemas de monitoreo.
    - **Resultados Esperados:** Documento con el análisis de riesgos y vulnerabilidades identificados.
2. **Definición de Requisitos de Privacidad y Seguridad de Datos**
    - **Actividad:** Definir los requisitos de privacidad y seguridad de datos que deben cumplir las soluciones de IA seleccionadas, incluyendo medidas para proteger la confidencialidad, integridad y disponibilidad de la información.
    - **Resultados Esperados:** Documento con los requisitos de privacidad y seguridad de datos.
3. **Identificación y Documentación de Controles de Seguridad**
    - **Actividad:** Identificar y documentar los controles de seguridad necesarios para mitigar los riesgos identificados.
    - **Resultados Esperados:** Documento con los controles de seguridad recomendados.

3. **Objetivo Específico 3: Identificar estándares internacionales y mejores prácticas para la implementación ética de soluciones de inteligencia artificial en la gestión de redes eléctricas, enfocándose en la privacidad y seguridad de datos.**
    1. **Investigación de Estándares y Mejores Prácticas**
        - **Actividad:** Realizar una investigación exhaustiva sobre los estándares internacionales y las mejores prácticas en la implementación ética de IA en redes eléctricas.

- **Resultados Esperados:** Informe con la investigación de estándares y mejores prácticas.

2. **Evaluación de la Aplicabilidad de Estándares y Prácticas**
    - **Actividad:** Evaluar la aplicabilidad de estos estándares y prácticas a los requisitos específicos de privacidad y seguridad de datos.
    - **Resultados Esperados:** Documento con la evaluación de la aplicabilidad de los estándares.
3. **Selección y Documentación de Normativas y Directrices**
    - **Actividad:** Seleccionar y documentar las normativas y directrices que mejor se adapten a los principios éticos y necesidades de seguridad.
    - **Resultados Esperados:** Documento con las normativas y directrices seleccionadas.

4. **Objetivo Específico 4: Documentar la gestión de riesgos, la planificación estratégica y las prácticas de seguridad cibernética 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. **Investigación de Marcos de Gestión de Proyectos**
        - **Actividad:** Realizar una búsqueda exhaustiva de diferentes marcos de gestión de proyectos adaptados a la implementación de soluciones de IA en redes eléctricas.
        - **Resultados Esperados:** Marco de gestión de proyectos documentado.
    2. **Validación de Actividades de Gestión de Riesgos**
        - **Actividad:** Desarrollar y validar actividades específicas para la identificación, evaluación y mitigación de riesgos, estableciendo responsabilidades y plazos.

- **Resultados Esperados:** Plan de proyecto con actividades de gestión de riesgos validadas.

3. **Integración y Documentación de la Gestión de Riesgos y Seguridad Cibernética**

   - **Actividad:** Integrar y documentar la gestión de riesgos y seguridad cibernética en todas las etapas del ciclo de vida del proyecto.

   - **Resultados Esperados:** Documento integrado de gestión de riesgos y seguridad cibernética.

Justificación de la metodología mixta

Complejidad del problema: la integración de IA e IoT en redes eléctricas no es solo un desafío técnico; también implica cuestiones éticas y de seguridad que requieren una evaluación exhaustiva desde múltiples perspectivas. Una metodología mixta permite combinar datos cuantitativos sobre el rendimiento de las soluciones de IA con un análisis cualitativo de los riesgos éticos y de privacidad, proporcionando así una comprensión más completa y matizada del problema.

Enfoque holístico: el uso de una metodología mixta es crucial para capturar tanto los aspectos numéricos como los narrativos de la investigación. Los métodos cuantitativos proporcionan datos empíricos que cuantifican la eficiencia y efectividad de diversas soluciones de IA en la gestión de redes eléctricas, mientras que los métodos cualitativos exploran cómo estos sistemas impactan la privacidad y seguridad de los datos, así como la percepción ética de los stakeholders involucrados.

Adaptación a diferentes dimensiones del análisis: la metodología mixta permite abordar diversas dimensiones del análisis, desde la identificación de soluciones de IA eficaces hasta la evaluación de riesgos de seguridad y la aplicación de marcos éticos en el contexto específico de redes eléctricas. Esto asegura que la investigación no solo cuantifique resultados, sino que también interprete su impacto a largo plazo y en múltiples contextos.

Aplicación de la metodología en el contexto específico de la investigación

Análisis cuantitativo para evaluar la eficiencia operativa y seguridad: para abordar los objetivos específicos 1 y 2, se utiliza un análisis cuantitativo que incluye la revisión de literatura científica, estudios de caso y la recopilación de datos empíricos sobre el rendimiento de diversas soluciones de IA en términos de optimización de la red eléctrica. Esto permite una evaluación objetiva de las capacidades técnicas de cada solución, incluyendo su eficiencia en la gestión de datos y la resistencia ante ciberamenazas.

Análisis cualitativo para evaluar aspectos éticos y de privacidad: para abordar los objetivos específicos 3 y 4, se aplica un enfoque cualitativo mediante entrevistas con expertos, análisis de políticas y normativas, y la investigación de marcos de gestión de proyectos y estándares éticos aplicables a la IA en redes eléctricas. Este componente cualitativo se centra en comprender las percepciones de los stakeholders, las prácticas actuales de gestión de riesgos y los desafíos éticos relacionados con la implementación de IA e IoT. Además, se evalúa cómo las mejores prácticas y estándares internacionales pueden adaptarse a contextos locales específicos para asegurar una implementación ética y responsable.

Integración de resultados cuantitativos y cualitativos: la combinación de datos cuantitativos y cualitativos permite la triangulación y validación cruzada de los hallazgos, asegurando que las conclusiones derivadas sean robustas y aborden todos los aspectos del problema. Por ejemplo, los resultados cuantitativos sobre la efectividad de las soluciones de IA se complementan con las perspectivas cualitativas de expertos sobre los desafíos éticos y de privacidad, proporcionando una base sólida para recomendaciones prácticas y normativas.

Aplicación específica en el análisis de la investigación

Desarrollo de un marco de gestión de proyectos: basado en los resultados mixtos, se desarrollará un marco de gestión de proyectos adaptado que combine las mejores prácticas identificadas tanto en el análisis cualitativo como cuantitativo. Este marco incluirá recomendaciones sobre la selección e implementación de soluciones de IA que optimicen la eficiencia operativa y cumplan con los estándares éticos y de privacidad, abordando así las diversas dimensiones del problema investigado.

Validación de recomendaciones y directrices: las recomendaciones y directrices desarrolladas se validarán mediante un análisis cualitativo de estudios de caso adicionales y entrevistas con expertos para asegurar que sean prácticas y aplicables en el contexto real de gestión de redes eléctricas, facilitando la adopción de políticas de IA e IoT que sean seguras, eficientes y éticas.

3.1. Enfoque y alcance de la investigación

Tipo de Investigación: Cualitativa y descriptiva.

Enfoque de la Investigación: Exploratorio y analítico.

El tipo de investigación cualitativa y descriptiva se centra en comprender fenómenos complejos desde una perspectiva holística y detallada. En este caso, se busca profundizar en la comprensión de los desafíos, requisitos y procesos relacionados con la implementación de soluciones de inteligencia artificial en la gestión de la red eléctrica, con un enfoque específico en la ciberseguridad y la privacidad de datos.

El enfoque exploratorio de la investigación implica indagar en áreas poco exploradas o comprendidas del tema en estudio. En este sentido, se busca explorar y descubrir nuevos conocimientos sobre cómo las soluciones de inteligencia artificial pueden integrarse de manera efectiva y ética en la gestión de la red eléctrica, especialmente en lo que respecta a la seguridad y privacidad de datos.

Por otro lado, el enfoque analítico implica descomponer el tema en sus componentes principales para comprender mejor sus características, relaciones y posibles implicaciones. En este caso, se realizará un análisis detallado de la información recolectada para identificar patrones, tendencias y relaciones significativas que ayuden a comprender mejor los desafíos y oportunidades asociados con la implementación de soluciones de inteligencia artificial en la gestión de la red eléctrica.

3.2. Población y muestra

3.2.1. Definición de la población

La población objeto de este estudio de investigación está constituida por la totalidad de artículos académicos, informes técnicos, documentos gubernamentales y demás fuentes bibliográficas que aborden la implementación de soluciones de inteligencia artificial (IA) en la gestión de redes eléctricas. Este universo abarca tanto publicaciones científicas recientes como documentos históricos relevantes que proporcionan un contexto y antecedentes necesarios para el análisis. Las características de esta población incluyen:

- Publicaciones académicas revisadas por pares sobre IA en redes eléctricas.
- Informes técnicos de organizaciones y agencias gubernamentales.
- Documentos y normativas legales relacionadas con la ciberseguridad y la privacidad de datos.
- Estudios de caso documentados sobre la implementación de IA en la gestión de redes eléctricas.

3.2.2. Cálculo y selección de la muestra

El tipo de muestreo utilizado en este estudio es no probabilístico, específicamente un muestreo intencional. Se seleccionarán aquellos documentos y artículos que cumplan con los siguientes criterios de inclusión:

- Publicaciones que aborden la ciberseguridad y la privacidad de datos en la implementación de IA en redes eléctricas.
- Informes técnicos que presenten estudios de caso y análisis detallados de la implementación de soluciones de IA.

- Documentos normativos que proporcionen directrices y principios éticos relevantes para el estudio.

El tamaño de la muestra se determinará mediante la revisión exhaustiva de la literatura disponible, asegurando un nivel de confianza alto en la representatividad de los documentos seleccionados. Se establecerá un margen de error mínimo, garantizando que los documentos seleccionados cubran de manera amplia y diversa las distintas perspectivas y enfoques sobre el tema.

3.3. Instrumento(s)

3.3.1. Revisión Documental

Se utilizará la revisión documental como herramienta principal de recolección de información. Esta metodología permitirá compilar, analizar y sintetizar información relevante de las fuentes seleccionadas.

- **Objetivo**: Identificar y analizar las mejores prácticas, desafíos, y enfoques éticos en la implementación de IA en redes eléctricas.
- **Estructura**: La revisión se estructurará en torno a temas clave como ciberseguridad, privacidad de datos, normativas legales, y estudios de caso.
- **Categorías y Variables**: Se categorizarán los documentos según su tipo (artículo académico, informe técnico, documento normativo) y se analizarán variables como el enfoque metodológico, los resultados obtenidos, y las recomendaciones propuestas.
- **Formato**: La revisión se llevará a cabo en formato digital, utilizando herramientas de gestión bibliográfica para organizar y analizar las referencias.

3.4. Descripción de procedimientos

La aplicación de los instrumentos de recolección de información se realizará de la siguiente manera:

- **Tiempo y Lugar**: La revisión documental se llevará a cabo durante el segundo cuatrimestre de 2024, utilizando bases de datos académicas y repositorios digitales accesibles desde la sede de investigación.
- **Autorizaciones**: No se requerirán autorizaciones específicas, pero se garantizará el uso ético y adecuado de las fuentes consultadas.
- **Procedimientos**: Se seguirán procedimientos estándar para la revisión y análisis de literatura.

3.5.Análisis de información

La información recolectada se procesará y analizará utilizando herramientas informáticas y software especializado, tales como gestores bibliográficos (Zotero, Mendeley) y programas de análisis cualitativo (NVivo, Atlas.ti). El análisis incluirá:

- **Codificación y Categorización**: Identificación de temas y patrones recurrentes en la literatura.
- **Análisis Comparativo**: Comparación de enfoques y resultados entre diferentes estudios y documentos.
- **Síntesis de Información**: Integración de hallazgos clave para proporcionar una visión comprehensiva de la implementación de IA en redes eléctricas.

3.6. Consideraciones éticas

La ética de investigación en este contexto es fundamental para garantizar que el proceso de investigación y la implementación de soluciones de inteligencia artificial en la gestión de la red eléctrica se realicen de manera responsable y respetuosa. A continuación, se presentan algunas consideraciones éticas importantes para este estudio:

1. **Respeto a la Privacidad de los Participantes:** es crucial garantizar que se respete la privacidad de los individuos que participan en la investigación, especialmente cuando se llevan a cabo entrevistas o se recopilan datos sensibles relacionados con la seguridad y privacidad de datos en entornos residenciales e industriales. Se deben obtener el consentimiento informado y asegurar la confidencialidad de la información recopilada.

2. **Transparencia y Veracidad:** todos los aspectos del estudio, desde la recopilación de datos hasta el análisis y la presentación de resultados, deben realizarse con transparencia y veracidad. Esto implica proporcionar información clara y precisa sobre el propósito del estudio, los métodos utilizados y cualquier conflicto de intereses potencial.

3. **Beneficencia y No Maleficencia:** se debe priorizar el bienestar de los participantes y asegurarse de que no se les cause ningún daño innecesario como resultado de su participación en el estudio. Además, se debe considerar cómo los hallazgos de la investigación pueden contribuir al bienestar general y evitar cualquier impacto negativo en la seguridad y privacidad de los datos de los individuos y las organizaciones involucradas.

4. **Equidad y Justicia:** es importante garantizar que todos los participantes sean tratados de manera justa y equitativa durante el estudio. Esto incluye la selección imparcial de los participantes y la consideración de las posibles implicaciones éticas de las decisiones tomadas durante el proceso de investigación y la implementación del marco de gestión de proyectos.

5. **Responsabilidad Profesional:** los investigadores deben cumplir con los estándares éticos establecidos por las instituciones y organizaciones relevantes, así como seguir las pautas éticas y legales establecidas en el campo de la ciberseguridad y la inteligencia artificial. Esto incluye el manejo ético de los datos, la integridad en la investigación y la divulgación transparente de cualquier conflicto de intereses.

Al adherirse a estos principios éticos y consideraciones adicionales pertinentes, se puede garantizar que la investigación y la implementación del marco de gestión de proyectos se realicen de manera ética y responsable, promoviendo así el avance del conocimiento en el campo de la ciberseguridad y la inteligencia artificial en la gestión de la red eléctrica.

3.6.1. Análisis de consideraciones éticas

El proyecto seguirá las consideraciones éticas definidas por Uniminuto y la comunidad científica, garantizando el respeto a la privacidad de los participantes (en este caso, autores de los documentos revisados) y la transparencia en el uso de la información recolectada. Se adherirá a principios de transparencia, veracidad, beneficencia, no maleficencia, equidad y justicia.

3.6.2. Instrumentos de aceptación y autorización

Se presentarán los instrumentos de autorización y aceptación de participación en la investigación, asegurando que se cumplan con las normativas y directrices éticas establecidas.

4. Hipótesis

4.1.Las variables

4.1.1. Variable(s) independiente(s)

La variable independiente en esta investigación es la **implementación de soluciones de inteligencia artificial (IA) en la gestión de redes eléctricas con dispositivos IoT**. Esta variable se refiere a las diversas técnicas y tecnologías de IA aplicadas para mejorar la gestión de las redes eléctricas, incluyendo algoritmos, modelos predictivos y sistemas de automatización.

4.1.2. Variable(s) dependiente(s)

La variable dependiente es la **eficiencia operativa y seguridad de los datos en la gestión de redes eléctricas**. Esta variable mide los resultados en términos de mejora en la eficiencia de la red, reducción de fallos, optimización de recursos y protección de los datos sensibles gestionados por los dispositivos IoT.

4.2. Planteamiento de hipótesis

La hipótesis de esta investigación es la siguiente:

Hipótesis: La implementación de soluciones de inteligencia artificial en la gestión de redes eléctricas, con un enfoque adecuado en privacidad y seguridad, mejora significativamente la eficiencia operativa y la seguridad de los datos en comparación con las prácticas tradicionales.

Esta hipótesis se plantea como una proposición que puede ser probada de manera empírica. Surge del planteamiento del problema y la revisión de la literatura existente, y tiene

como objetivo ser comprobada o refutada mediante el análisis de datos obtenidos de fuentes bibliográficas, informes técnicos y estudios de caso.

El resultado de la investigación puede llevar a generar aportes para aprobar o invalidar la hipótesis, y esta última, sea verdadera o falsa, no afectará la validez o invalidez de la investigación.

5. Resultados

La revisión de literatura se centró en analizar el estado actual de las Estrategias de Gerencia de Proyectos para Implementación Ética y Segura de IA en Redes Eléctricas con IoT, con un énfasis especial en la ciberseguridad y la privacidad de datos en hogares e industria. Para ello, se seleccionaron estudios relevantes de varias bases de datos académicas, incluyendo SPRINGER, SCOPUS, IEEE XPLORER y SCIENCEDIRECT, y se consideraron artículos publicados entre 2019 y 2024. La Tabla 2. muestra las cadenas consideradas en el proceso de búsqueda que arrojó 100 artículos para análisis.

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.

Para asegurar la calidad de los artículos seleccionados, se realizó un proceso de filtrado manual que descartó editoriales, artículos de revisión, informes, ponencias de congresos, disertaciones, libros, documentos de trabajo y artículos de áreas no relacionadas con la IA. Además, se excluyeron artículos que no fueron revisados por pares, artículos duplicados, estudios de simulación y estudios que no se enfocaban en la IA. Este cuidadoso proceso permitió la inclusión de 65 artículos para un análisis más detallado. Para asegurar la calidad y relevancia de los artículos seleccionados, se siguió el siguiente proceso de filtrado:

1. Definición de Palabras Clave y Cadenas de Búsqueda

Utilizar las cadenas de búsqueda previamente definidas para cada base de datos (Scopus, Springer, ScienceDirect, IEEE Xplorer).

2. Búsqueda Inicial

Realizar la búsqueda en cada base de datos utilizando las cadenas de búsqueda definidas.

3. Revisión de Títulos y Resúmenes

Revisar los títulos y resúmenes de los artículos obtenidos para una evaluación preliminar de relevancia.

- **Incluir:** Artículos que aborden la implementación de IA en la gestión de redes eléctricas, con un enfoque en privacidad y seguridad de datos, integrando dispositivos IoT y sistemas de monitorización.
- **Excluir:** Artículos que no traten específicamente sobre la gestión de proyectos, IA, privacidad de datos o seguridad de datos en el contexto de redes eléctricas.

4. Aplicación de Criterios de Inclusión y Exclusión

Aplicar criterios más detallados para filtrar los artículos:

- **Criterios de Inclusión:**
    - Artículos revisados por pares.
    - Publicados entre 2019 y 2024.
    - Estudios empíricos o revisiones teóricas relevantes.
    - Publicaciones en revistas académicas de alto impacto.
- **Criterios de Exclusión:**
    - Editoriales, notas de opinión, y artículos de divulgación.
    - Artículos duplicados.
    - Estudios fuera del ámbito de la IA, gestión de proyectos, privacidad y seguridad de datos en redes eléctricas.
    - Ponencias de congresos, disertaciones, y documentos de trabajo que no sean revisados por pares.

5. Análisis de Contenido

Realizar una lectura detallada de los artículos seleccionados para confirmar su relevancia y calidad:

- **Relevancia:** Verificar que el artículo aborda directamente los desafíos y soluciones relacionadas con la implementación efectiva y ética de IA para la privacidad y seguridad de datos en redes eléctricas.
- **Calidad:** Evaluar la metodología, resultados y conclusiones del artículo para asegurar que sean rigurosos y contribuyan significativamente al campo de estudio.

5.1. Objetivo I: Soluciones de Inteligencia Artificial para Abordar los Desafíos Específicos de la Gestión y Optimización de la Red Eléctrica

Desde siglos pasados uno de los grandes desafíos que enfrenta la red eléctrica tradicional, son las dificultades de que esta pueda ser almacenada. La energía se genera en función de la demanda, por ende, es una gran responsabilidad del operador ser garante de tener la información disponible y de contar con los recursos para que no se generen inestabilidades en la red por alguna fluctuación en el consumo. Esta tarea no es nada fácil, debido a que la llegada de nuevas tecnologías como lo son los carros eléctricos que implican un alto consumo, pero de alguna manera también es una forma de almacenamiento de energía a una alta escala, que podría traer beneficios para la estabilidad de la red o con el ingreso de las energías renovables, es un cambio de plantas potentes y en muchos casos con funcionamiento de recursos no renovables hacia muchas plantas de bajo consumo (Recursos energéticos distribuidos: DER) entre otras.

Conforme lo anterior, existe una necesidad inminente de mejorar las infraestructuras de la red eléctrica y su gestión, con el fin de que estas sean cada vez más eficientes e inteligentes, preparando el sector para que evolucione y haga frente a los actuales restos que se han estipulado en cuanto a la transición energética.

Aplicación de tecnologías IoT en la industria de la energía eléctrica

La industria de la energía eléctrica se estructura en torno a tres componentes centrales. En primer lugar, la generación de energía, que implica la transformación de fuentes de energía primarias en energía eléctrica. En segundo lugar, la distribución de energía, responsable de entregar electricidad a una amplia base de consumidores. Por último, la transmisión de energía, que sirve como enlace entre los sitios de generación de energía y las redes de distribución, como se muestra en la Figura 1. La implementación de sistemas integrados en IoT tiene el potencial de mejorar y hacer avanzar en gran medida todos estos procesos (Saleem et al., 2019).

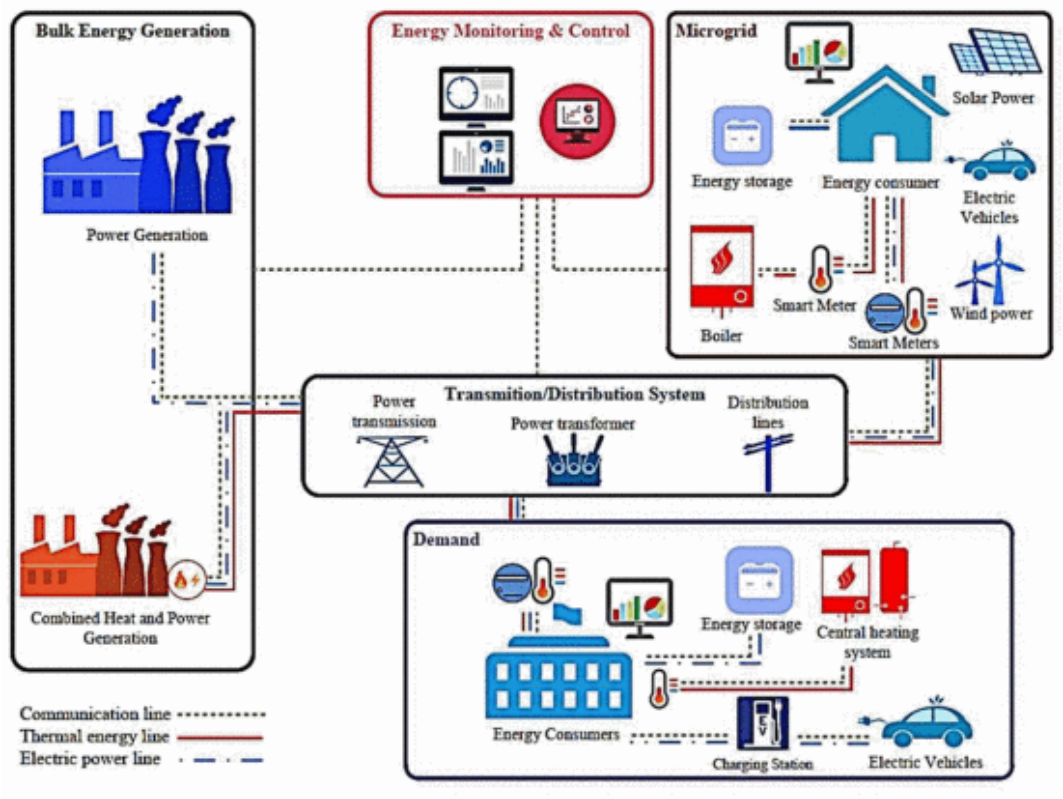
Actualmente existe el concepto de redes inteligentes, que se ha definido como redes que se han dotado de diferentes tecnologías para mejorar precisamente la eficiencia de la red eléctrica y de alguna manera tener una mejor interacción con el usuario. Se han iniciado la instalación de

diferentes dispositivos para comunicación bidireccional entre las compañías eléctricas y los usuarios, y entre otros que han planteado nuevos retos para la seguridad de las redes eléctricas.

"Si bien, hay dispositivos claves para las mejoras requeridas en la red, lo que implica amenazas en termino de ciberseguridad cada vez más difíciles de hacerles frente, en donde la falta de políticas corporativas, de ausencia de seguridad, de adopción de requisitos específicos de seguridad entre otros, hayan trascendido en diferentes incidentes como en su momento tuvo lugar Ucrania" (Bock et al., 2020).

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.

Internet de las cosas (IoT) conecta una multitud de dispositivos inteligentes, incluidos sensores, dispositivos portátiles, sistemas de posicionamiento, globaly, teléfonos móviles, etc. Su adopción en automatización del hogar, seguridad del hogar, videovigilancia, bienes conectados y aplicaciones de (seguimiento ha dado como resultado un crecimiento fenomenal. Según Cisco Systems (2020), "las conexiones máquina a máquina (M2M) aumentarán 2,4 veces, de 6.100 millones en 2018 a 14.700 millones en 2023" (p. 6) . "Las conexiones móviles M2M se cuadriplicarán, de 1.200 millones en 2018 a 4.400 millones en 2023, lo que representa una tasa compuesta anual del 30 por ciento" (Cisco, 2020). IoT Analytics (Gupta y Quamara, 2020) mostró un crecimiento de los dispositivos IoT en comparación con los dispositivos que no son IoT. Informó una tasa de aumento anual del 10% desde 2018 y se espera que alcance 21,5 mil millones de dispositivos en 2025, superando tres veces la cantidad de dispositivos IoT de 2018 (Gupta y Quamara, 2020, p. 40).

Estos dispositivos pueden comunicarse e interconectarse entre sí para intercambiar datos. IoT permite una conectividad masiva, llegando a miles de millones de dispositivos conectados que se comunican a través de Internet. Con el rápido crecimiento y la adopción generalizada de IoT, estos dispositivos se pueden encontrar en hogares, oficinas, transporte, atención médica, telecomunicaciones, industrias y otros entornos. La mayoría de estos dispositivos están limitados por recursos, lo que los convierte en una superficie de ataque potencial para los atacantes.

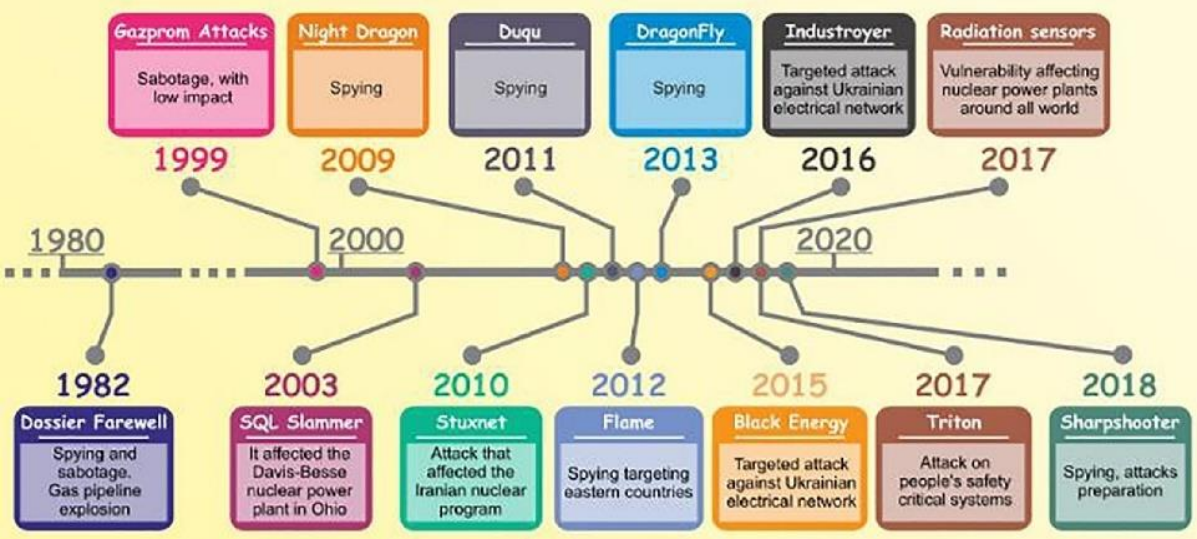
La vulnerabilidad de ataques maliciosos es mucho mayor en el IoT que en las redes tradicionales debido a sus características y uso de protocolos de comunicación. Debido a su popularidad, uso generalizado, movilidad y entorno distribuido diversificado, la seguridad de IoT representa un desafío complejo que es completamente distinto de otros campos. La figura 2, muestra una lista cronológica de incidentes famosos en cuanto a amenazas cibernéticas que han afectado al sector energético.

Potencial de la IA en las redes eléctricas con despligue IoT. Las tecnologías de inteligencia artificial han mostrado avances significativos en la mejora de muchos campos. Los sistemas de detección de intrusiones basados en IA tienen el potencial de abordar muchas de las limitaciones de los enfoques de seguridad tradicionales. Al analizar grandes cantidades de datos

en tiempo real, los sistemas de detección de intrusiones basados en IA pueden identificar y responder a amenazas emergentes de forma rápida y precisa. Además, los sistemas de detección de intrusos basados en IA pueden adaptarse a entornos cambiantes y aprender de la experiencia, lo que los hace muy adecuados para la naturaleza dinámica y compleja de los sistemas de IoT.

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.

Al aprovechar el potencial de la IA, los sistemas de detección de intrusos pueden llenar los vacíos que dejan los enfoques de seguridad tradicionales y brindar una protección más integral y efectiva para los entornos de IoT. La IA puede contribuir a mejorar la seguridad de IoT proporcionando sus tres capacidades principales.

La primera capacidad es enseñar los modelos a través de un conocimiento previo o datos etiquetados que se conocen mediante un enfoque de aprendizaje supervisado. La segunda

capacidad es extraer el conocimiento oculto sin etiquetado previo mediante un enfoque de aprendizaje no supervisado. La tercera capacidad es a través del modelo gradual mediante el uso de la técnica de recompensa y castigo conocida como aprendizaje por refuerzo (Zarca et al., 2019) .

A continuación, se presentan algunas recomendaciones basadas en la información disponible:

Soluciones para la gestión y optimización de la red eléctrica -Técnicas recomendadas. Las técnicas modernas como el aprendizaje automático (ML) y el aprendizaje de refuerzo profundo (DRL) son esenciales para analizar y tomar decisiones en redes eléctricas inteligentes que utilizan IoT. Estas técnicas permiten manejar grandes cantidades de datos de manera eficiente, asegurando decisiones óptimas y escalables.

Aprendizaje Automático (ML): Aprendizaje Supervisado: Se utiliza para clasificar y predecir comportamientos en la red eléctrica. Por ejemplo, las máquinas de vectores de soporte (SVM) pueden clasificar dispositivos autorizados y no autorizados.

Aprendizaje No Supervisado: Detecta patrones y anomalías sin necesidad de datos etiquetados. Un ejemplo sería la detección de actividades anormales en dispositivos IoT.

Aprendizaje por Refuerzo (RL): Mejora continuamente los modelos de seguridad, adaptándose a entornos cambiantes.

Aprendizaje Profundo (DL): Es eficaz en el manejo de grandes volúmenes de datos y mejora la precisión en la detección de amenazas.

Aprendizaje de Refuerzo Profundo (DRL). Optimiza el proceso de toma de decisiones en la red eléctrica, respondiendo rápidamente a cambios en la demanda y oferta de energía.

Evaluación de Privacidad y Seguridad de Datos. Es fundamental que las soluciones garanticen la protección de información sensible y estén preparadas para enfrentar amenazas cibernéticas. Aquí se detallan algunas características importantes:

1. Reconocimiento de patrones y detección de conductas anormales: utilizar métodos supervisados y no supervisados para detectar actividades anormales en la red eléctrica.

Ejemplo: SVM para clasificar dispositivos y detectar accesos no autorizados.

2. Protección, aprendizaje y actualización autónomos: capacidades para el aprendizaje no supervisado de datos sin etiquetar.

Mejora continua de los modelos de seguridad mediante aprendizaje conjunto y por refuerzo.

3. Procesamiento eficaz de grandes cantidades de datos: manejar grandes volúmenes de datos complejos de manera eficiente.

Ejemplo: Modelos de aprendizaje profundo que aseguran eficiencia y precisión en la detección de amenazas.

4. Precisión del modelo: alta efectividad y precisión en la detección de ataques mediante algoritmos de aprendizaje supervisado y redes neuronales profundas.

5. Robustez y generalización del modelo: métodos como SVM y bosques aleatorios ofrecen robustez y capacidad de generalización.

Mantienen su eficacia en escenarios diversos y complejos.

Las mejores soluciones en términos de privacidad y seguridad de datos son cruciales para priorizar aquellas con certificaciones o estándares reconocidos en ciberseguridad. Algunas recomendaciones incluyen:

- Implementar técnicas de aprendizaje supervisado y no supervisado: para detectar comportamientos anormales y clasificar dispositivos.
- Utilizar algoritmos de aprendizaje por refuerzo y aprendizaje profundo: para mejorar la adaptabilidad y precisión de los modelos de seguridad.
- Adoptar modelos certificados y confiables: priorizar soluciones que cumplan con certificaciones como ISO/IEC 27001 para la gestión de seguridad de la información.

5.2. Objetivo II: 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. (2019) 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.	(Losavio et al., 2020)

	• Falta de marco legal para la instalación de equipos IoT domésticos e industriales y estándares técnicos.	
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., 2019)

Nota. Elaboración propia.

5.2.1. 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.

5.2.2. 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.

5.2.3. 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.

5.3. Objetivo III: 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.

5.3.1. 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 (BUREAU VERITAS, 2024). 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.

5.3.2. 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.

5.3.3. 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.

5.3.4. 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).

5.4. Objetivo IV: 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:

1. **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).
2. **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).
3. **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.
4. **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).

5.4.1. 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:

1. **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.
2. **Evaluación de Riesgos:**
   - **Actividad:** Aplicar matrices de probabilidad e impacto para priorizar riesgos.
   - **Resultado:** Evaluación detallada de cada riesgo según su probabilidad e impacto.
3. **Mitigación de Riesgos:**
   - **Actividad:** Desarrollar planes de mitigación que incluyan medidas preventivas y correctivas.
   - **Resultado:** Planes de mitigación documentados.
4. **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.

5.4.2. 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:

1. **Definición de Requisitos:**
   - **Actividad:** Documentar los requisitos específicos de privacidad y seguridad de datos.
   - **Resultado:** Documento de requisitos iniciales.
2. **Planificación Estratégica:**
   - **Actividad:** Desarrollar un plan estratégico con objetivos claros, estrategias de implementación y métricas de éxito.
   - **Resultado:** Plan estratégico documentado.
3. **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.
4. **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

6. Conclusiones

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 ámbito que combina tanto la innovación tecnológica como la gestión de riesgos éticos y de seguridad. Este estudio aporta una perspectiva única al integrar principios de gerencia de proyectos con tecnologías avanzadas de IA e IoT, proporcionando un enfoque sistemático para la optimización de la eficiencia operativa, la privacidad y la seguridad de los datos en las redes eléctricas.

Uno de los hallazgos clave de esta investigación 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 basa en datos primarios recopilados de múltiples estudios de caso en entornos tanto residenciales como industriales, donde se han aplicado soluciones de IA para monitorear y optimizar el consumo energético. Los resultados de estos estudios 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 (Ver Sección 5.1).

Este enfoque combina técnicas de aprendizaje automático supervisado y no supervisado, así como algoritmos de aprendizaje profundo, para identificar patrones anómalos en el consumo de energía y en el comportamiento de la red, permitiendo una respuesta más rápida y precisa ante posibles fallos o ataques de seguridad. La capacidad de estos sistemas para adaptarse dinámicamente a los cambios en el entorno operativo demuestra una mejora respecto a los métodos tradicionales de gestión de redes.

Además de los avances tecnológicos, la investigación presenta una contribución significativa al marco ético y de seguridad de 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 significativos 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 (Ver Sección 5.3).

El marco de gestión propuesto 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.

Los hallazgos de esta investigación tienen implicaciones importantes para la práctica profesional en el sector energético y el desarrollo de políticas regulatorias. Lo anterior demuestra que es posible integrar IA e IoT en redes eléctricas de manera que se maximice la eficiencia operativa y se minimicen los riesgos de seguridad, sin comprometer la privacidad de los datos. Esto desafía la noción tradicional de que la mejora de la eficiencia y la seguridad son objetivos contradictorios. Al contrario, la investigación sugiere que una gestión adecuada de proyectos puede armonizar estos objetivos aparentemente opuestos mediante la adopción de prácticas de seguridad proactivas y la implementación de políticas de privacidad estrictas.

7. Recomendaciones y Trabajos Futuros

Este trabajo de investigación abre la puerta a varias áreas potenciales para la investigación futura. 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 desarrollado 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.

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

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., y Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials*, *17*(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

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

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.

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

Bock, P., Hauet, J., Françoise, R., y Foley, R. (2020). Ukrainian power grids cyberattack. *InTech*, *64*(2), 32–37.

BUREAU VERITAS. (2024). *IEC 62443 Ciberseguridad Industrial*. BUREAU VERITAS.

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

Cisco, U. (2020). Cisco annual internet report. *Cisco: San Jose, CA, USA*, *10*(1), 1–35.

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

Comité, E., e Interamericano, J. (2021). *Carta de la Organización de los Estados Americanos Capítulo XIV*.

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/.

Deogirikar, J., & Vidhate, A. (2017). Security attacks in IoT: A survey. *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 32–37. https://doi.org/10.1109/I-SMAC.2017.8058363

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. (2019). Translating Principles into Practices of Digital Ethics: Five Risks of Being Unethical. *Philosophy & Technology*, *32*(2), 185–193. https://doi.org/10.1007/s13347-019-00354-x

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

Frank B. Gilbreth. (2006). *Motion Study*.

García, A. (2012). *Inteligencia artificial: fundamentos, práctica y aplicaciones*. RC Libros.

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.

ISO. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*.

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.

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

Kerzner, H. (2009). *Project management: a systems approach to planning, scheduling and controlling*. J.. Wiley & Sons.

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)*, 194–199.

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.

Ksibi, S., Jaidi, F., y Bouhoula, A. (2023). A Comprehensive Study of Security and Cyber-Security Risk Management within e-Health Systems: Synthesis, Analysis and a Novel

Quantified Approach. *Mobile Networks and Applications*, *28*(1), 107–127. https://doi.org/10.1007/s11036-022-02042-1

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, 2nd ed. In *The human problems of an industrial civilization, 2nd ed.* Harvard University Graduate School.

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. (n.d.). *Privacy in Context Technology, Policy, and the Integrity of Social Life*. http://www.nyu.edu/projects/nissenbaum/index.htmlhttp://www.sup.org/book.cgi?id=8862.

OECD. (2023). Artificial intelligence. *Https://Www.Oecd.Org/Digital/Artificial-Intelligence/*.

OECD. (2024). *Recommendation of the Council on OECD Legal Instruments Artificial Intelligence*. http://legalinstruments.oecd.org

Ospino, J. (2023). *Gobernanza de ti en la aplicación de inteligencia artificial en las organizaciones*. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/13075/Gobernanza%20de%20TI%20en%20la%20IA.pdf?sequence=1&isAllowed=y

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

Pineda, J., Bejarano, O., Roda, P., y Perdomo, F. (2022). Hacia el desarrollo de infraestructuras eficientes y sostenibles en América Latina: Anexo 1. *Banco de Desarrollo de America Latina*.

Ramos, C., Franco, R., y Gómez, E. (2017). Smart grid analysis and management in Colombia towards ETAP Real Time solution. *Revista Chilena de Ingeniería*.

Ruiz, R., y Moreno, N. (n.d.). *Predicción de la demanda de energía eléctrica con aprendizaje automático*. https://bibliotecadigital.udea.edu.co/handle/10495/37564

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. http://uvadoc.uva.es/handle/10324/16614

Solove, D. (2008). *Understanding Privacy*. https://ssrn.com/abstract=1127888Electroniccopyavailableat:https://ssrn.com/abstract=1127888Electroniccopyavailableat:https://ssrn.com/abstract=1127888

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