eISSN 2938-1487
Universitat Autònoma de Barcelona
Journal of Human Security and Global Law 2026, vol. 5
129-155

El impacto del Reglamento Europeo de Inteligencia Artificial en el sector energético

The Impact of the EU Artificial Intelligence Regulation on the Energy Sector

Cristina Blasi Casagran
Universitat Autònoma de Barcelona
cristina.blasi@uab.cat
0000-0002-4327-2212

Recepción: 19/1/2026
Aceptación: 21/1/2026
Publicación: 20/2/2026

Citación recomendada: Blasi Casagran, Cristina (2026). «El impacto del Reglamento Europeo de Inteligencia Artificial en el sector energético». *Journal of Human Security and Global Law*, 5, 129-155. <https://doi.org/10.5565/rev/jhsgl.74>

Resumen

Este artículo analiza cómo el nuevo Reglamento Europeo de Inteligencia Artificial afecta al sector energético e identifica tanto las oportunidades tecnológicas como los desafíos regulatorios. La IA tiene un gran potencial para optimizar redes eléctricas, mejorar la predicción de la producción de energías renovables, aplicar mantenimiento predictivo y personalizar servicios al consumidor. Estas aplicaciones prometen aumentar la eficiencia operativa, reducir costes y avanzar hacia un modelo energético más sostenible. Sin embargo, el Reglamento impone exigencias significativas, en especial para los sistemas de alto riesgo, como los usados en infraestructuras críticas. Se detallan algunos de sus artículos clave, como los relativos a la gestión de riesgos (art. 9), gobernanza de datos (art. 10), transparencia (art. 11), supervisión humana (art. 14), robustez y seguridad (art. 15) y obligaciones para proveedores y distribuidores (arts. 22-26). Las empresas deben implementar sistemas seguros, explicables y conformes a la normativa, lo que implica inversiones en tecnología, formación del personal y cambios organizativos. Entre los desafíos más relevantes destacan la dificultad técnica de garantizar transparencia en sistemas complejos, las restricciones del RGPD en el uso de datos, la escasez de personal cualificado y el consumo energético de los propios sistemas de IA. A pesar de ello, el artículo concluye afirmando que el Reglamento no debe ser visto como una barrera, sino como una oportunidad para innovar con responsabilidad y fortalecer la confianza en el sector. Se incluyen diez apartados con recomenda-

ciones prácticas para guiar a las empresas en una implementación conforme, ética y sostenible de la IA.

Palabras clave: regulación de la IA; sector energético; alto riesgo; transparencia; gobernanza de datos

Abstract

This article examines how the EU's new AI regulation affects the energy sector, identifying both technological opportunities and regulatory challenges. AI has strong potential to optimise power grids, improve forecasting of renewable energy production, enable predictive maintenance, and personalise consumer services. These applications promise to increase operational efficiency, reduce costs, and advance toward a more sustainable energy model. However, the regulation imposes significant requirements, especially for high-risk systems such as those used in critical infrastructures. The article outlines key provisions of the regulation, including those related to risk management (Art. 9), data governance (Art. 10), transparency (Art. 11), human oversight (Art. 14), robustness and security (Art. 15), and obligations for providers and distributors (Arts. 22–26). Companies must implement safe, explainable, and compliant systems, which entails investments in technology, staff training, and organisational changes. Among the most important challenges are the technical difficulty of ensuring transparency in complex systems, GDPR restrictions on data use, the shortage of qualified personnel, and the energy consumption of AI systems themselves. Despite these hurdles, the article concludes that the regulation should not be seen as a barrier but as an opportunity to innovate responsibly and strengthen trust in the sector. It includes ten sections with practical recommendations to guide companies in the compliant, ethical, and sustainable implementation of AI.

Keywords: AI regulation; energy sector; high risk; transparency; data governance

1. Introducción

El Reglamento Europeo de Inteligencia Artificial —en adelante, el Reglamento de IA— (Unión Europea, 2024) es la primera normativa integral sobre inteligencia artificial en el mundo que, aprobada en 2024, persigue el objetivo de mitigar los riesgos que la IA puede suponer para la seguridad y los derechos fundamentales de las personas.

El sector energético europeo, inmerso en una transformación digital y verde, se encuentra en el punto de mira de esta nueva regulación. La aplicación de IA en energía abarca desde redes eléctricas inteligentes que equilibran la oferta y la demanda en tiempo real (Estebsari et al., 2022), hasta la optimización de fuentes renovables (como predecir la generación eólica y la solar) (Islam et al., 2023) y la gestión eficiente del

consumo. Estas innovaciones prometen mejorar la eficiencia y la sostenibilidad del sistema energético, pero también introducen riesgos si no se controlan adecuadamente. Un algoritmo defectuoso o sesgado en la operación de una red eléctrica podría, por ejemplo, causar interrupciones de suministro a gran escala. Conscientes de ello, los legisladores europeos han clasificado a muchas aplicaciones de IA en energía dentro de las de «alto riesgo» y han sido sometidas a obligaciones estrictas. De hecho, el Reglamento de IA identifica expresamente como sistemas de IA de alto riesgo aquellos utilizados en la gestión de infraestructuras críticas, incluyendo los empleados en el suministro de agua, gas y electricidad. En otras palabras, si una IA interviene en tareas donde un fallo podría comprometer servicios energéticos esenciales o la seguridad de las personas, estará sujeta a un escrutinio regulatorio elevado.

Aunque el Reglamento de IA fue publicado en el *Diario Oficial de la Unión Europea* en julio de 2024 y entró en vigor el 1 de agosto de 2024, sus disposiciones no se aplican de inmediato en su totalidad. La normativa prevé un período transitorio para que los actores públicos y privados se adapten. Con carácter general, las obligaciones principales serán exigibles a partir de agosto de 2026, sin perjuicio de que determinadas disposiciones entren en aplicación con anterioridad o posterioridad según el tipo de sistema de IA y el riesgo asociado. Este margen de adaptación es especialmente relevante en el sector energético, donde las empresas deberán preparar con antelación sus sistemas y procesos de IA para cumplir con los nuevos requisitos legales.

En este artículo se explora cómo impacta el Reglamento Europeo de IA en el ámbito energético, analizando las implicaciones prácticas para las empresas energéticas y proporcionando recomendaciones para cumplir la normativa sin frenar la innovación. Esta aproximación integral busca ofrecer una versión enriquecida y clara del análisis del impacto del Reglamento de IA de la UE en el sector energético, así como una serie de recomendaciones para las empresas energéticas.

2. Marco legal: IA de alto riesgo en energía y obligaciones del Reglamento Europeo de IA

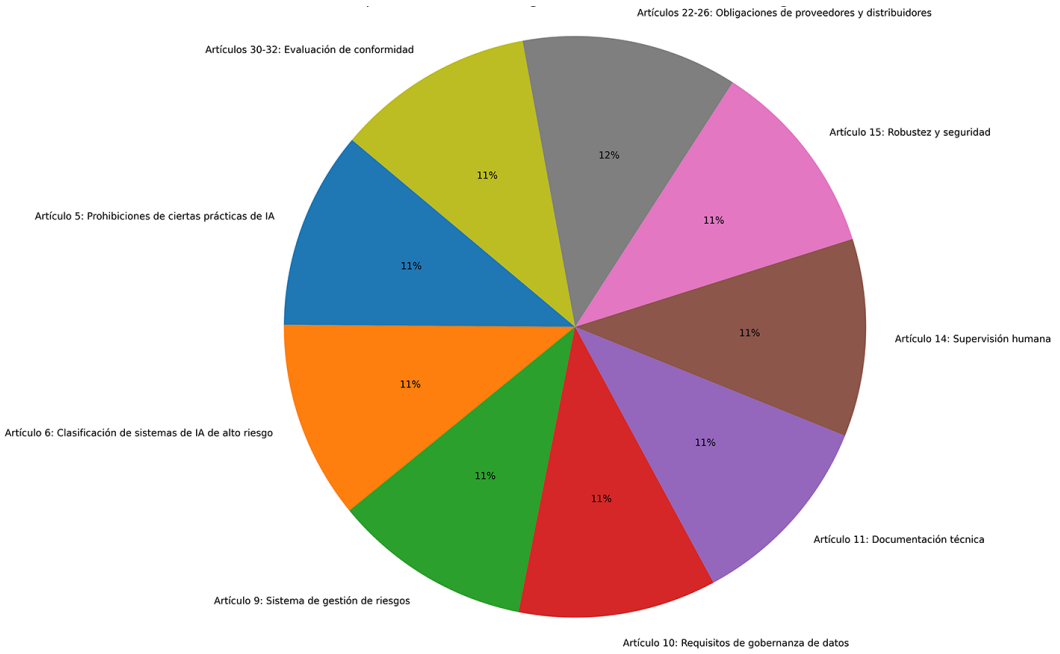
El Reglamento de IA establece un marco legal integral para el desarrollo, la comercialización y el uso de sistemas de inteligencia artificial dentro del mercado único europeo. Su objetivo principal es garantizar que los sistemas de IA sean seguros, transparentes, éticos y respetuosos con los derechos fundamentales y los valores de la UE (artículo 1). Entre otros aspectos, el Reglamento introduce un enfoque basado en el riesgo, clasificando los sistemas de IA en diferentes categorías según su nivel

de riesgo: riesgo inaceptable, alto riesgo, riesgo limitado y mínimo riesgo. Esta clasificación determina las obligaciones y los requisitos que deben cumplir los proveedores y los usuarios de sistemas de IA (capítulos II y III del Reglamento).

Dado que en el sector energético muchas aplicaciones de IA inciden directamente en servicios críticos (electricidad o gas) o en infraestructuras cuya interrupción podría afectar a millones de personas, gran parte de estas aplicaciones quedan clasificadas en categorías de «alto riesgo». Ya se ha mencionado que la ley incluye explícitamente bajo este paraguas a los sistemas de IA utilizados en la gestión u operación de infraestructuras críticas, tales como la red eléctrica. Por ejemplo, un sistema de IA que gestione la distribución eléctrica o modifique la inyección de energía en la red en tiempo real será considerado de alto riesgo. Esto significa básicamente que la UE trata este tipo de IA con la misma precaución con la que trataría un equipamiento de seguridad industrial: exige que antes de su uso se demuestre que es fiable y seguro, debido al enorme impacto que tendría un fallo.

En la figura 1 se identifican y se analizan los artículos del Reglamento que podrían ejercer un impacto directo o indirecto en las empresas del sector energético.

Figura 1. Principales artículos del Reglamento de IA con impacto en el sector energético



Fuente: elaboración propia.

2.1. Prohibiciones de ciertas prácticas de IA (artículo 5)

El artículo 5 del Reglamento prohíbe el uso de sistemas de IA que representen un riesgo inaceptable, como aquellos que manipulan el comportamiento humano de manera perjudicial o permiten realizar una vigilancia masiva indiscriminada. En consecuencia, las empresas energéticas deben asegurarse de que sus aplicaciones de IA no infrinjan estas prohibiciones, especialmente en sistemas que recopilan datos de usuarios o que podrían influir en el comportamiento de los consumidores.

Por ejemplo, si una empresa energética utiliza un sistema de IA para gestionar los datos de consumo de energía de sus clientes y ofrecer recomendaciones personalizadas sobre cómo reducir el uso de energía, dicho sistema debe evitar prácticas que puedan ser consideradas una manipulación del comportamiento de los usuarios, como la presión para que estos adopten ciertos hábitos de consumo a través de notificaciones repetitivas o invasivas. Además, el sistema de IA no puede involucrarse en una vigilancia masiva de los usuarios, recopilando y monitoreando sus datos de forma indiscriminada y sin el consentimiento explícito del afectado.

2.2. Clasificación de sistemas de IA de alto riesgo (artículo 6)

El artículo 6 define los criterios para considerar un sistema de IA como de alto riesgo. Los sistemas que se utilizan en la gestión y operación de infraestructuras críticas, como las redes eléctricas y de gas, se clasifican como de alto riesgo.

¿Qué implica que un sistema de IA sea «de alto riesgo»? En términos prácticos, implica que fabricantes, proveedores y usuarios profesionales de dicha IA deben cumplir una serie de requisitos legales estrictos antes de ponerla en el mercado o en operación. El Reglamento impone obligaciones que abarcan el ciclo completo de vida del sistema de IA, desde su diseño hasta su implementación. Entre estas obligaciones destacan: realizar evaluaciones de riesgos y aplicar medidas de mitigación apropiadas; garantizar la alta calidad de los datos de entrenamiento para minimizar sesgos o resultados discriminatorios; llevar un registro automático de las actividades del sistema (*logs*) para asegurar la trazabilidad de sus decisiones; documentar detalladamente el sistema, proporcionando información suficiente sobre su finalidad y su funcionamiento para que las autoridades puedan evaluarlo; asegurar que se brinde información clara y adecuada al usuario o implementador sobre el sistema; establecer medidas de supervisión humana cuando corresponda (es decir, mantener «un humano en el circuito» monitorizando o validando

las decisiones de la IA en casos sensibles), y garantizar la robustez, la ciberseguridad y la precisión del sistema, de modo que funcione de forma confiable incluso ante condiciones cambiantes (*La Ley de Inteligencia Artificial…*, 2024). Estas exigencias recuerdan a las que ya existen en campos regulados tradicionales (por ejemplo, los ensayos y las certificaciones que requieren los equipos en centrales eléctricas), trasladando ese rigor al ámbito algorítmico. El cumplimiento deberá demostrarse a través de evaluaciones de conformidad. En muchos casos será el propio proveedor quien realice una autoevaluación de conformidad, aunque para ciertas aplicaciones críticas podría exigirse una intervención de entidades notificadas (organismos externos acreditados), similar a como ocurre con la certificación de equipos de alto riesgo bajo otras normativas de la UE.

Por lo tanto, las empresas que utilizan sistemas de IA para gestionar infraestructuras energéticas deben cumplir con requisitos estrictos. Esto implicaría una revisión exhaustiva de los sistemas vigentes y posibles actualizaciones para cumplir con los estándares establecidos. Por ejemplo, imaginemos que una empresa de energía utiliza un sistema de inteligencia artificial para gestionar su red eléctrica inteligente (*smart grid*), que optimiza la distribución de electricidad a hogares y empresas en función de la demanda en tiempo real. Este sistema de IA monitorea continuamente el uso de energía y ajusta el flujo eléctrico para reducir pérdidas y mejorar la eficiencia. Además, predice fallos en el sistema para realizar mantenimientos preventivos. Con la entrada en vigor del Reglamento de IA esta empresa debería cumplir con una serie de requisitos estrictos, como los siguientes:

a) Evaluación de conformidad, mediante la cual la empresa debe realizar una auditoría completa de su sistema de IA para asegurarse de que cumple con los estándares de seguridad, transparencia y ética establecidos por la UE (por ejemplo, debe demostrar que su sistema de IA no discrimina en la asignación de energía entre diferentes barrios o usuarios).
b) Gestión de riesgos, ya que la empresa está obligada a identificar y gestionar los riesgos asociados al uso de la IA en la red eléctrica (por ejemplo, el sistema debe ser capaz de explicar las decisiones críticas que toma, como reducir el suministro a ciertas áreas en momentos de alta demanda).
c) Revisión de sistemas actuales y actualizaciones.

Si el sistema de IA no cumple con alguno de los nuevos requisitos del Reglamento, la empresa tendrá que hacer actualizaciones para alinearse con los estándares. Esto podría implicar la modificación de algorit-

mos de decisión para asegurar una mayor transparencia o introducir nuevas capas de seguridad para prevenir ataques cibernéticos.

De esta manera, la empresa no solo asegura la eficiencia operativa de su red, sino también el cumplimiento normativo con las nuevas exigencias del Reglamento de IA, lo que protege tanto a sus usuarios como a la infraestructura crítica.

2.3. Sistema de gestión de riesgos (artículo 9)

El artículo 9 establece que los proveedores de sistemas de IA de alto riesgo deben implementar un sistema de gestión de riesgos para identificar y mitigar posibles peligros asociados con el uso de IA. En base a este artículo, las empresas energéticas deben desarrollar protocolos para gestionar riesgos específicos de la IA, como errores en la predicción (también conocidos como *alucinaciones*) de la demanda energética o fallos en sistemas automatizados de control, lo que puede requerir inversiones en nuevas herramientas y formación del personal.

Por ejemplo, si una empresa energética utiliza IA para predecir la demanda de su producto y controlar automáticamente el suministro de energía renovable a la red, deberá asumir un riesgo de que un fallo en la predicción de la demanda provoque un desequilibrio en la distribución de energía, lo que podría generar sobrecargas o apagones. Por ello, para cumplir con el artículo 9 del Reglamento de IA, dicha empresa debería implementar un sistema de gestión de riesgos que incluyese la monitorización continua del desempeño del sistema de IA, simulaciones de escenarios de fallo y la incorporación de un sistema de respaldo manual en caso de emergencia. Además, debería invertir en herramientas avanzadas para detectar anomalías y capacitar al personal para responder eficazmente ante cualquier fallo en el sistema, minimizando el impacto en la estabilidad de la red.

2.4. Requisitos de gobernanza de datos (artículo 10)

El artículo 10 enfatiza la necesidad de garantizar la calidad y la gestión adecuada de los datos utilizados por los sistemas de IA. Dado que las aplicaciones de IA en el sector dependen en gran medida de datos operativos y de consumo, las empresas deben asegurar la integridad, la exactitud y la seguridad de estos datos, cumpliendo además con regulaciones de protección de datos como el RGPD.

En este sentido, si la empresa de energía renovable utiliza un sistema de IA para optimizar la distribución de su producto en función de los datos de consumo de sus clientes y de las condiciones meteorológicas,

buscará predecir la demanda y ajustar el suministro de energía de manera eficiente. Para cumplir con el artículo 10 del Reglamento de IA, esta empresa debería implementar un sistema de gobernanza de datos que asegurase la calidad, la integridad y la seguridad de los datos utilizados por la IA. Esto incluiría lo siguiente:

a) Un control de calidad de datos, asegurando que no se utilicen algunos que sean corruptos o incorrectos y puedan afectar a las decisiones del sistema de IA.
b) Políticas estrictas de cumplimiento con el Reglamento General de Protección de Datos (RGPD) (Unión Europea, 2016), garantizando así que los datos de los consumidores están protegidos mediante medidas de seguridad tales como encriptación y almacenamiento seguro.
c) Llevar a cabo auditorías regulares para asegurar que los datos gestionados por el sistema de IA cumplen con los estándares de seguridad y precisión, lo que permite a la empresa mantener la confianza de los consumidores y cumplir con las normativas, tanto del Reglamento de IA como del RGPD.

2.5. Documentación técnica (artículo 11)

El artículo 11 requiere que los proveedores de sistemas de IA de alto riesgo elaboren una documentación técnica detallada. Así pues, las empresas del sector energético que utilicen IA deben documentar exhaustivamente sus sistemas, incluyendo detalles sobre el diseño, la finalidad, los algoritmos utilizados y las pruebas realizadas. Esto puede suponer una carga administrativa adicional y requerir recursos especializados. Esta documentación también debería detallar cómo el sistema ha sido entrenado y validado para evitar errores críticos, lo que garantiza su conformidad con las normativas y facilita auditorías futuras.

2.6. Supervisión humana (artículo 14)

El artículo 14 establece que los sistemas de IA de alto riesgo deben diseñarse para permitir una supervisión humana apropiada. Las empresas energéticas deben, pues, asegurar que haya mecanismos para que los operadores humanos intervengan o anulen decisiones tomadas por sistemas de IA, especialmente en situaciones críticas que afecten al suministro o a la seguridad energética.

Imaginemos, por ejemplo, que un sistema de IA utilizado para gestionar la red eléctrica de Cataluña controla el flujo de energía entre plantas

generadoras y los consumidores de la región. En un día de alta demanda energética, el sistema de IA podría decidir reducir el suministro en ciertas áreas para evitar la sobrecarga de la red. Sin embargo, en una situación grave, como la pérdida de energía en un hospital o en una instalación de emergencia, los operadores humanos deberían tener la capacidad de intervenir, anulando la decisión de la IA para priorizar el suministro en estos lugares críticos. Este tipo de supervisión humana es clave para asegurar que las decisiones automatizadas no comprometan la seguridad o el bienestar de los usuarios finales.

2.7. Robustez y seguridad (artículo 15)

El artículo 15 exige que los sistemas de IA sean robustos, seguros y precisos. En este sentido, las empresas del sector energético deben garantizar que sus sistemas de IA puedan manejar errores y resistir ataques cibernéticos. Esto es especialmente relevante para infraestructuras críticas que podrían ser vulnerables a ciberataques, por lo que requerirían medidas adicionales de ciberseguridad.

Así pues, el artículo 15 enfatiza la necesidad de que las empresas del sector energético implementen medidas de ciberseguridad que protejan la integridad y la disponibilidad de sus sistemas. Esto incluye el uso de IA para detectar y mitigar vulnerabilidades en tiempo real, evitar ataques de denegación de servicio (DDoS) y garantizar que los sistemas puedan seguir funcionando de manera segura ante fallos o intrusiones.

Un ejemplo relevante es el proyecto Darktrace, una empresa de ciberseguridad que ha aplicado inteligencia artificial para proteger infraestructuras críticas incluyendo el sector energético. Darktrace implementó su tecnología de IA en una importante compañía de energía en Europa que gestiona una red eléctrica extensa y diversa. El sistema de IA detectó una anomalía inusual en las comunicaciones internas de la red que no fue identificada por los sistemas de seguridad tradicionales. Resultó ser un intento de ataque que buscaba desestabilizar el suministro de energía. La IA no solo detectó el comportamiento anómalo antes de que causara daño, sino que automáticamente aisló las partes afectadas de la red, previniendo una interrupción masiva (Darktrace, 2023).

Este caso demuestra cómo los sistemas de IA en el sector energético, si son diseñados bajo principios de robustez y seguridad como lo estipula el artículo 15 del Reglamento de IA, pueden ser claves para resistir ataques cibernéticos complejos. Además, garantiza que los sistemas puedan gestionar errores, adaptarse a comportamientos imprevistos y responder eficazmente a situaciones de amenaza, protegiendo así infraestructuras críticas del sector energético.

2.8. Obligaciones de los proveedores, los distribuidores y los responsables del despliegue de sistemas de IA (artículos 22 a 26)

Los artículos 22 a 26 del Reglamento de IA de la UE establecen obligaciones específicas para proveedores, importadores, distribuidores y responsables del despliegue de sistemas de IA de alto riesgo, lo cual tiene importantes implicaciones para las empresas del sector energético que utilizan IA en infraestructuras críticas.

Así, si una empresa de fuera de la UE (por ejemplo, de EE. UU.) quiere introducir un sistema de IA para gestionar redes eléctricas o para optimizar el consumo energético en hogares europeos, deberá nombrar un representante autorizado en la UE para garantizar el cumplimiento normativo y facilitar la interacción con las autoridades (artículo 22). Este representante en la UE será responsable de presentar la documentación requerida y cooperar con las autoridades de vigilancia del mercado en caso de problemas con el sistema.

Igualmente, los importadores son responsables de garantizar que los sistemas de IA de alto riesgo que ingresan en el mercado de la UE cumplan con los requisitos del Reglamento (artículo 23). Por ejemplo, si una empresa energética importa un sistema de IA para gestionar el almacenamiento de energía renovable, el importador debe asegurarse de que el sistema cumpla con las normativas, incluyendo la documentación y la evaluación de conformidad, antes de que pueda comercializarse en la UE. Esto incluye verificar que el proveedor haya elaborado la documentación técnica, así como asegurar que el sistema lleve el marcado CE.

Los distribuidores de sistemas de IA de alto riesgo también deben asegurarse de que el producto lleve el marcado CE, vaya acompañado de la declaración de conformidad y que tanto el proveedor como el importador hayan cumplido sus obligaciones. Así pues, un distribuidor de sistemas de IA en España que gestiona la integración de energía solar en la red eléctrica debe comprobar que los sistemas cumplen con todos los requisitos antes de ofrecerlos al mercado.

Finalmente, los responsables del despliegue de sistemas de IA de alto riesgo, como las empresas energéticas, deben tomar medidas para asegurar que aquellos se usen conforme a las instrucciones proporcionadas (artículo 26), vigilando su funcionamiento y garantizando que los operadores tengan la formación adecuada para supervisar los sistemas. Además, si el sistema presenta un riesgo o sufre un incidente, deberán informar a las autoridades competentes. Por ejemplo, una empresa eléctrica que despliega IA para optimizar la distribución de electricidad debe garantizar que sus operadores humanos estén capacitados para supervisar el sistema y que los datos de entrada sean precisos. Si detectan un fallo en el sistema que podría provocar apagones, deberán sus-

pender el uso de la IA y notificarlo a las autoridades para evitar riesgos adicionales.

2.9. Evaluación de conformidad (artículos 30 a 32)

Los artículos 30 a 32 del Reglamento establecen que los sistemas de IA de alto riesgo deben someterse a una evaluación de conformidad antes de ser comercializados o puestos en servicio. En este sentido, las empresas energéticas deben realizar o encargar evaluaciones de conformidad, lo que puede implicar costes y retrasos en la implementación de nuevos sistemas de IA.

Por ejemplo, una empresa energética quiere implementar un nuevo sistema de IA para optimizar la operación de sus parques eólicos. Dado que este sistema se considera de alto riesgo por su influencia en una infraestructura crítica, la empresa debería contratar a un organismo notificado para llevar a cabo la evaluación, la cual tendría que incluir la revisión de los algoritmos, la calidad de los datos utilizados y las pruebas rigurosas de seguridad. La evaluación de conformidad garantiza, pues, la robustez y la fiabilidad del sistema, minimizando los riesgos para la red eléctrica y cumpliendo con las normativas europeas.

Al comprender y abordar todos estos artículos relevantes del Reglamento de IA, las empresas del sector energético pueden no solo garantizar su cumplimiento legal, sino también fortalecer la confianza de los consumidores y las partes interesadas, posicionándose como líderes en la adopción responsable de tecnologías avanzadas.

3. Implicaciones de la IA para el sector energético

Una vez que se han revisado los principales artículos del Reglamento de IA relevantes para el sector energético, es crucial identificar las oportunidades y los desafíos que las empresas energéticas enfrentarán al incorporar sistemas de inteligencia artificial. Estas oportunidades y desafíos están enmarcados no solo en el cumplimiento de las normativas, sino también en el aprovechamiento de las ventajas tecnológicas que la IA ofrece al sector. A continuación, se analizan las principales oportunidades y desafíos de la IA en el sector energético.

3.1. Oportunidades de la IA para el sector energético

Las oportunidades que la IA presenta para el sector energético son amplias y van desde la mejora de la eficiencia operativa hasta la creación de nuevas formas de interacción con los clientes.

Una de las mayores oportunidades es la capacidad de la IA para optimizar las redes eléctricas y gestionar la demanda de manera dinámica (Ahmad et al., 2022). La IA permite realizar el análisis de grandes volúmenes de datos en tiempo real, lo que posibilita una distribución más eficiente de la energía. Al predecir el consumo y ajustar el suministro en función de los patrones de demanda, las redes eléctricas pueden operar con mayor estabilidad, reduciendo las pérdidas y mejorando la eficiencia energética (Joint Research Center, 2024; KPMG, 2024). Esto es especialmente relevante en la transición hacia un modelo energético más descentralizado, con una mayor dependencia de fuentes renovables (Sun et al., 2023).

En segundo lugar, el uso de IA también puede mejorar en la predicción de la producción de energías renovables, al analizar grandes conjuntos de datos meteorológicos y operativos. Esto permite realizar una integración más efectiva de fuentes renovables en la red y una planificación más precisa (Demertzis, 2023). Por ejemplo, el proyecto europeo SustainML (2022-2025) se centra en desarrollar modelos de aprendizaje automático para predecir la generación de energía renovable y optimizar su uso, contribuyendo a facilitar una mayor eficiencia y sostenibilidad en el sector energético[1].

En tercer lugar, cabe destacar la posibilidad de establecer un mantenimiento predictivo de infraestructuras energéticas. Cada vez hay más compañías energéticas que están utilizando IA para el mantenimiento predictivo de infraestructuras. Mediante el análisis de datos en tiempo real y el monitoreo continuo, la IA ayuda a predecir fallos y a programar mantenimientos, reduciendo costos y evitando interrupciones (Hamdan et al., 2024; KPMG, 2024). Por ejemplo, el proyecto europeo ELIAS (2022-2025) utiliza inteligencia artificial para mejorar el mantenimiento de infraestructuras energéticas, aplicando técnicas avanzadas para detectar anomalías y anticipar necesidades de mantenimiento[2].

Finalmente, otra oportunidad que brinda la IA es la personalización de servicios al cliente y la eficiencia energética (Susanto y Khaq, 2024). En este sentido, el proyecto europeo dAIEDGE (2023-2026) trabaja en implementar soluciones de IA en el borde de la red para ofrecer servicios personalizados y mejorar la eficiencia energética, permitiendo a los clientes gestionar mejor su consumo[3].

3.2. Límites y desafíos de la IA para el sector energético

Si bien las oportunidades de la IA son significativas, también conllevan desafíos que las empresas energéticas deben enfrentar para cum-

1. <https://sustainml.eu>.
2. <https://elias-ai.eu>.
3. <https://daiedge.eu>.

plir con las nuevas normativas y asegurar la viabilidad de sus proyectos de IA.

Desde la perspectiva legal, el impacto inmediato para las empresas energéticas que emplean IA es la necesidad de incorporar nuevos procesos de cumplimiento normativo. Las áreas legales y de cumplimiento de las compañías eléctricas, petroleras o de redes inteligentes deberán familiarizarse con los detalles del Reglamento de IA y posiblemente crear sistemas internos de gobernanza de IA. Las dinámicas de implementación de dicho tipo de proyectos pueden ralentizarse ligeramente al inicio, debido a los nuevos pasos requeridos. Un proyecto piloto de IA en una empresa de energía ahora no solo tendrá que demostrar su viabilidad técnica, sino también preparar su eventual certificación legal: desde el comienzo habrá que pensar en cómo documentar el modelo, qué riesgos evaluar, etc. Esto podría alargar los tiempos de desarrollo en el corto plazo. No obstante, una vez que las metodologías de cumplimiento se integren en la rutina (y con la ayuda de estándares y plantillas comunes), es probable que la innovación retome su ritmo, esta vez en un entorno más controlado. Un beneficio importante es que, con el Reglamento en vigor, disminuirá la incertidumbre regulatoria. Hasta ahora, algunas empresas quizá dudaban en invertir mucho en IA por temor a futuras prohibiciones o reglas contradictorias entre países. Ahora tienen un marco estable que seguir a nivel europeo. Incluso aplicaciones potencialmente polémicas (como sistemas automatizados de fijación de tarifas energéticas o IA para recomendar cortes rotativos en caso de crisis) podrán explorarse sabiendo qué criterios legales deben cumplir.

De hecho, algunas empresas europeas han comenzado ya a prepararse voluntariamente, adoptando estándares y certificaciones alineados con el uso ético y seguro de la IA. Un ejemplo notable es Iberdrola (España), que se convirtió en 2025 en la primera empresa en certificar con AENOR su Sistema de Gestión de la Inteligencia Artificial conforme a la norma internacional ISO/IEC 42001 («Iberdrola, primera empresa…», 2025). Esta certificación acredita que Iberdrola ha implantado procesos para un uso responsable y seguro de las herramientas de IA en sus operaciones internas, anticipándose en buena medida a las exigencias regulatorias. Tales iniciativas de autorregulación indican que el sector entiende la importancia de generar confianza en las soluciones de IA que despliega. Además, más de un centenar de empresas europeas (incluyendo actores energéticos como la propia Iberdrola, junto con compañías tecnológicas como Telefónica, Siemens, etc.) han firmado el Pacto Europeo por una IA Confiable y Segura[4], un marco voluntario promovido por la Comisión Europea para que la industria aplique los principios

4. <https://digital-strategy.ec.europa.eu/en/policies/ai-pact>.

del Reglamento de IA incluso antes de su entrada en vigor. Los firmantes de este pacto se comprometen a adoptar estrategias internas para la introducción de la IA que cumplan con la legislación emergente, identificando sus sistemas de IA de alto riesgo, formando a su personal en alfabetización de IA y garantizando en general un desarrollo ético y responsable de esta tecnología en sus organizaciones.

En segundo lugar, las empresas del sector energético deberán cumplir con los requisitos de transparencia y explicabilidad de los sistemas de IA. El Reglamento de IA, en su artículo 50, establece que los sistemas de IA deben ser transparentes y explicables, especialmente aquellos clasificados como de alto riesgo. En el sector energético, donde las decisiones pueden afectar a la seguridad y al suministro, es crucial que los algoritmos sean auditables y que sus resultados puedan ser interpretados por humanos. Esto plantea desafíos técnicos, ya que muchos procedimientos avanzados de IA, como las redes neuronales profundas, son inherentemente opacos y pueden entrar en conflicto con el rendimiento de los sistemas de IA, ya que los modelos más precisos suelen ser los menos interpretables (Custers y Vergouw, 2021).

Un tercer desafío sería la gestión de datos y la privacidad en aplicaciones de IA en el sector energético. El Parlamento Europeo ya ha advertido que el acceso limitado a datos de calidad y las estrictas regulaciones de privacidad en la UE, como el RGPD, pueden dificultar el desarrollo y la implementación de sistemas de IA en el sector energético. Las empresas enfrentan desafíos para recopilar y procesar datos sensibles, lo que puede obstaculizar la innovación y la eficiencia (Voss, 2024). En la misma línea, la Comisión Europea ha enfatizado la importancia de equilibrar la innovación en IA con la protección de datos y la privacidad. Se promueve el desarrollo de sistemas de IA que respeten los derechos fundamentales y garanticen la seguridad y la confidencialidad de los datos, lo cual es esencial en el manejo de información sensible en el sector energético (Comisión Europea, 2024a).

En quinto lugar, sería necesario que las empresas energéticas introdujeran cursos de adaptación y formación del personal en nuevas tecnologías. Actualmente, hay una falta de habilidades digitales y de conocimiento sobre IA entre el personal en muchas de estas empresas, lo cual es un obstáculo significativo. Así, las empresas energéticas deben invertir en programas de formación y desarrollo profesional para capacitar a sus empleados en el uso y el mantenimiento de sistemas de IA, facilitando así la transición hacia operaciones más automatizadas y eficientes (KPMG, 2024). Precisamente, el proyecto europeo dAIEDGE mencionado anteriormente resalta la importancia de preparar a la fuerza laboral para la adopción de tecnologías de IA en el borde de la red. Este proyecto promueve iniciativas de formación y creación de competencias

para garantizar que el personal pueda gestionar y aprovechar eficazmente las nuevas herramientas tecnológicas.

Un sexto desafío a tener en cuenta consistiría en las posibles restricciones en el uso de IA para ciertas aplicaciones de alto riesgo, por ejemplo, tecnologías que impliquen decisiones autónomas sin intervención humana (Liakeas et al., 2024), tal y como se ha indicado en el apartado 2. El Reglamento de IA introduce categorías de riesgo para aplicaciones de IA (artículo 6), imponiendo restricciones y requisitos estrictos para aquellas consideradas de alto riesgo. En el sector energético, esto podría afectar el despliegue de sistemas de IA en operaciones críticas, como la gestión de redes eléctricas o sistemas de control industrial, debido a las implicaciones de seguridad y fiabilidad.

Finalmente, no se pueden olvidar los posibles riesgos que presenta la IA para la sostenibilidad y el medio ambiente. De hecho, la sostenibilidad y la eficiencia también están presentes en la regulación: el Reglamento de IA enfatiza la necesidad de transparencia en el consumo energético de ciertos sistemas de IA y alude a la protección del medio ambiente como parte de sus objetivos. Las empresas deben equilibrar los beneficios de la IA con los objetivos de desarrollo sostenible (ODS) de las Naciones Unidas, así como las políticas de medio ambiente de la UE. En este sentido, el Reglamento de IA complementa otras grandes iniciativas europeas, como el Pacto Verde Europeo (Comisión Europea, 2019) y la Década Digital 2030 (Comisión Europea, 2024d), que buscan una transición ecológica apoyada en tecnología de vanguardia. La convergencia de la agenda verde y la digital (*twin transition*) significa que la IA en energía tiene un rol importante que jugar para lograr objetivos climáticos (reducción de emisiones, eficiencia energética e integración de renovables) y que Europa quiere liderar esa sinergia de forma segura. Prueba de ello es la financiación de proyectos de I+D específicos, por ejemplo los mencionados en apartados anteriores y otros, como el proyecto europeo I-NERGY[5], que reunió a empresas y a centros de investigación para desarrollar aplicaciones de *IA-as-a-service* en energía, desde gemelos digitales de la red hasta optimización de activos renovables. El Reglamento de IA viene precisamente a subsanar la fragmentación normativa, proporcionando un marco común que, a largo plazo, debería facilitar que las innovaciones de IA exitosas en un país europeo puedan replicarse en otros con menos trabas legales. En suma, desde un punto de vista estratégico, el sector energético europeo se encuentra ante la oportunidad de consolidar un ecosistema de IA robusto y confiable, en el que las empresas que inviertan en cumplimiento y calidad probablemente cosecharán ventajas competitivas y reputacionales significativas.

5. <https://i-nergy.eu/>.

En conclusión, mientras que la IA ofrece al sector energético oportunidades sin precedentes para mejorar la eficiencia, la sostenibilidad y la personalización de los servicios, también impone desafíos que deben ser abordados cuidadosamente para garantizar el cumplimiento normativo y la seguridad operativa. Las empresas tienen que adoptar un enfoque equilibrado que considere tanto la innovación como la responsabilidad social y ambiental en el uso de estas tecnologías emergentes.

4. Recomendaciones para empresas del sector energético sobre el uso de la IA conforme al Reglamento de IA

Dado el análisis anterior, surge la pregunta siguiente: ¿cómo pueden las empresas del sector energético prepararse y adaptarse con éxito en referencia al Reglamento de IA? A continuación, se presentan una serie de recomendaciones prácticas, concebidas tanto para empresas eléctricas y gasistas consolidadas como para nuevos entrantes y empresas emergentes del ámbito de la energía inteligente. El objetivo es ayudar a cumplir con la normativa de manera eficiente, al tiempo que se sigue aprovechando el potencial transformador de la IA en el negocio energético.

A continuación, se presentan diez apartados con las recomendaciones principales para utilizar la IA de manera conforme al reglamento, cada una de ellas con una lista de acciones que las empresas pueden implementar para asegurar su cumplimiento con el nuevo reglamento.

4.1. Clasificar los sistemas de IA según su nivel de riesgo

Es esencial identificar y categorizar los sistemas de IA utilizados en función de los niveles de riesgo definidos por el Reglamento: riesgo inaceptable, alto, limitado y mínimo.

Como primer paso, es fundamental que cada empresa realice un inventario exhaustivo de las soluciones de IA que utiliza o planea utilizar en sus operaciones. Por cada sistema, se debe evaluar preliminarmente si entra en la categoría de alto riesgo según el Reglamento (¿está involucrado en una infraestructura crítica?, ¿toma decisiones automatizadas que pueden afectar significativamente a personas u operaciones?). Este «mapeo» interno fue precisamente uno de los compromisos asumidos por las empresas firmantes del Pacto Europeo de IA mencionado anteriormente. A partir de esta evaluación, se puede priorizar la adaptación: los sistemas identificados como de alto riesgo requerirán mayor atención (quizá rediseño o mejoras), mientras que otros de bajo riesgo simplemente deberán documentarse y monitorearse para asegurar que no escalen en criticidad.

Si se identifica un sistema de riesgo alto, una práctica útil puede ser crear listas de validación inspiradas en los requisitos del Reglamento. Antes de desplegar un nuevo algoritmo en la operación diaria, pasar la lista de chequeo: ¿tiene evaluación de riesgos?, ¿está la documentación técnica completa?, ¿hemos probado los peores casos? Este proceso, que al principio puede parecer burocrático, con el tiempo se vuelve parte natural del flujo de trabajo de desarrollo y evita problemas mayores.

Acciones recomendadas	• Llevar a cabo un mapeo de sistemas de IA y una evaluación de riesgos. • Realizar una auditoría interna para clasificar los sistemas de IA existentes. • Implementar procesos para evaluar el riesgo antes de desarrollar o adquirir nuevos sistemas de IA.

4.2. Garantizar la transparencia y la explicabilidad de los sistemas de IA

La transparencia es crucial para generar confianza y cumplir con los requisitos legales, especialmente en sistemas de alto riesgo (Custers y Vergouw, 2021). El sector energético suele estar bajo escrutinio público, y tecnologías como los contadores inteligentes, la gestión automática de la demanda o la predicción de cortes de suministro mediante IA pueden generar preocupaciones ciudadanas si no hay transparencia. El Reglamento obligará a proporcionar información adecuada sobre los sistemas de IA, lo cual incluye en ciertos casos notificar a las personas cuándo interactúan con una IA o explicar de forma comprensible cómo toma decisiones relevantes. Esto debería traducirse en una mayor transparencia de las empresas energéticas hacia sus clientes y reguladores respecto al uso de IA. Por ejemplo, una comercializadora que utilice IA para fijar precios dinámicos de la electricidad tal vez deba informar a los consumidores de la existencia de ese algoritmo y asegurarse de que no sea discriminatorio. En la medida en que las compañías gestionen bien esa comunicación y cumplan estándares éticos, es probable que aumente la confianza del público en las soluciones de IA aplicadas a la energía (lo cual es vital para su adopción masiva, pues de poco sirve una mejor IA si los usuarios finales —ciudadanos, empresas o reguladores nacionales— no confían en ella).

Acciones recomendadas	• Implementar técnicas de IA explicable (XAI) para facilitar la interpretación de los resultados. • Documentar detalladamente los algoritmos y los procesos utilizados. • Proporcionar información clara a los usuarios sobre el funcionamiento del sistema.

4.3. Asegurar el cumplimiento en materia de protección de datos y privacidad

El manejo de datos personales debe cumplir con el RGPD y otras normativas relevantes (Comisión Europea, 2024a). En concreto, el RGPD sigue siendo plenamente aplicable a los sistemas de IA y exige, entre otros principios, minimización de datos, limitación de la finalidad, exactitud y transparencia. En la práctica, esto implica que las empresas deben asegurarse de que no recogen más datos de los necesarios, que los usan solo para las finalidades específicas informadas a los usuarios y que los mantienen actualizados y protegidos frente a accesos no autorizados.

Además, cuando se trata de sistemas de IA que tomen decisiones automatizadas con efectos significativos para las personas (como ajustes automáticos en las tarifas o interrupciones del servicio), el RGPD establece derechos adicionales como el de no ser objeto de decisiones exclusivamente automatizadas y el derecho a una intervención humana significativa (art. 22, RGPD). Esto refuerza la necesidad de realizar una supervisión humana exigida también por el Reglamento de IA.

Un reto añadido es que muchos algoritmos requieren entrenamiento previo con datos históricos, lo que obliga a revisar cuidadosamente los conjuntos de datos para evitar que contengan información identificable o sesgada. Por ejemplo, un sistema que aprenda patrones de consumo energético no debe inferir o exponer sin control hábitos personales sensibles, como presencia en el hogar o problemas económicos del usuario.

Acciones recomendadas	• Implementar medidas de anonimización y seudonimización de datos. • Establecer políticas claras de consentimiento y gestión de datos. • Realizar evaluaciones de impacto en la protección de datos (DPIA) para nuevos sistemas de IA.

4.4. Invertir en formación y desarrollo de competencias del personal

La adopción efectiva de la IA requiere que el personal esté capacitado y familiarizado con las nuevas tecnologías (KPMG, 2024). Sería útil asignar formación específica a los equipos involucrados: desde cursos de sensibilización para directivos (entendiendo el porqué de la regulación) hasta capacitación técnica para ingenieros en metodologías de Machine Learning Operations (MLOps) que incorporen requerimientos de documentación y prueba continua.

Igualmente, a nivel organizativo, las empresas energéticas podrían reforzar sus equipos multidisciplinarios. El cumplimiento del Reglamento de IA no recaerá únicamente en el departamento legal, sino que

involucrará a expertos en datos, ingenieros de IA, personal de operaciones y altos directivos.

Acciones recomendadas	• Ofrecer programas de formación continua en IA y análisis de datos. • Fomentar una cultura de innovación y aprendizaje dentro de la organización multidisciplinaria. • Colaborar con instituciones educativas y proyectos europeos para mantenerse actualizado.

4.5. Establecer un marco ético para el desarrollo y el uso de la IA

La ética debe ser un pilar fundamental en la estrategia de IA de las empresas (Comisión Europea, 2024a), las cuales deberían designar responsables o crear comités específicos para la gobernanza de la IA. Esto incluye establecer políticas internas claras sobre desarrollo y uso de IA (alineadas con los principios europeos: legalidad, ética, robustez técnica, seguridad, privacidad, transparencia y acción correctiva), similares a las políticas de seguridad de datos que surgieron tras el Reglamento General de Protección de Datos – RGPD). Un buen modelo a seguir son las empresas que ya cuentan con una política de uso responsable de IA pública —por ejemplo, Iberdrola dispone de una política corporativa donde garantiza que sus sistemas de IA serán transparentes, seguros y fiables (Iberdrola, 2025)—. Estas políticas deben descender a procedimientos, por ejemplo: definir que ningún modelo de IA de alto riesgo se pondrá en producción sin pasar por una validación de un comité técnico-ético.

Así pues, muchas compañías crearán probablemente comités internos de IA o ampliarán las funciones de sus comités de ética y cumplimiento para incluir la supervisión de inteligencia artificial. Al igual que el RGPD impulsó la figura del Delegado en Protección de Datos (DPD), el Reglamento de IA podría incentivar la aparición de responsables de cumplimiento de IA o roles semejantes dentro de las empresas, encargados de verificar que cada sistema de IA que se utilice haya pasado las evaluaciones necesarias y tenga las salvaguardas requeridas.

Acciones recomendadas	• Definir un código ético específico para el uso de IA. • Crear comités o grupos de trabajo interdisciplinarios para supervisar el cumplimiento ético. • Asegurar que los sistemas de IA no perpetúen sesgos o discriminación.

4.6. Implementar medidas de seguridad robustas

La ciberseguridad es crucial para proteger los sistemas de IA y los datos manejados (Joint Research Center, 2024). Un reto técnico adicional, pues,

será asegurar la ciberseguridad y la robustez de los sistemas de IA. Las redes eléctricas y gasistas forman parte de la infraestructura crítica nacional y han sido tradicionalmente objeto de estrictos estándares de seguridad industrial. Al introducir IA en estos entornos, las empresas deberán garantizar que un atacante no pueda manipular el algoritmo (por ejemplo, alimentándole con datos falsos) para causar disrupciones (Diaba et al., 2023). El Reglamento de IA exige explícitamente un alto nivel de seguridad y resiliencia ante ataques o intentos de manipulación, lo que probablemente estimulará inversiones en ciberseguridad específica para sistemas de IA. Pensemos en algoritmos de redes inteligentes (*smart grids*) que deciden reconfiguraciones de la red: deben estar protegidos contra intrusiones que alteren sus cálculos. Para ello, las empresas colaborarán con expertos en IA segura, aplicando técnicas como entornos aislados de prueba (*sandboxing*), prueba de penetración (*penetration testing*) adaptada a algoritmos y validaciones adicionales cuando la IA reciba datos externos. Organismos europeos como la Agencia de Ciberseguridad de la UE (ENISA) ya han señalado la importancia de este tema, y es previsible la emisión de guías sectoriales al respecto (ENISA, 2012; ENISA, 2013).

Acciones recomendadas	• Adoptar estándares internacionales de seguridad de la información (como ISO/IEC 27001). • Realizar pruebas de penetración y auditorías de seguridad periódicas. • Establecer protocolos de respuesta ante incidentes de seguridad.

4.7. Fomentar la eficiencia energética y la sostenibilidad en el uso de IA

Dado que la IA puede consumir grandes cantidades de energía, es importante considerar su impacto ambiental (Demertzis, 2023). Se trata de alinear la revolución digital con la transición verde. Esto significa que los desarrolladores de IA (especialmente de modelos de propósito general o de gran escala) deberán documentar y, potencialmente, optimizar la huella energética de sus algoritmos. En el contexto de la energía, esto crea un doble vínculo virtuoso: utilizamos IA para mejorar la eficiencia energética del sistema, pero a su vez monitorizamos que la propia IA sea eficiente energéticamente. Por ejemplo, proveedores de grandes modelos de IA tendrán que reportar la energía consumida durante el entrenamiento y la operación de esos modelos, información que las autoridades podrán requerir y auditar (Hickman et al., 2025). Existe, pues, una clara necesidad de desarrollar sistemas de IA que sean energéticamente eficientes y de bajo consumo, lo cual añade otro nivel de desafío para las empresas que deben cumplir con estándares ambientales además de las regulaciones de IA (Comisión Europea, 2024b). De hecho, ya hay doctrina que argu-

menta que el impacto del uso de IA en el consumo energético puede contradecir los objetivos de sostenibilidad (Demertzis, 2023).

Acciones recomendadas	• Optimizar los algoritmos para reducir el consumo energético. • Utilizar hardware eficiente y considerar la huella de carbono de los centros de datos. • Integrar fuentes de energía renovable en las operaciones de tecnologías de la información.

4.8. Garantizar la supervisión humana en sistemas de alto riesgo

Un elemento crucial es la supervisión humana. La normativa enfatiza que, en sistemas de alto riesgo, debe haber mecanismos para que un humano supervise o intervenga en ellos cuando sea necesario. En el contexto energético, donde tradicionalmente ha habido operadores humanos controlando redes y plantas, esto se traduce en mantener al personal «en el circuito». Así, si una IA recomienda desconectar cierta línea eléctrica para evitar una sobrecarga, el sistema puede requerir la confirmación de un ingeniero antes de ejecutar la acción.

Muchas empresas ya siguen esta filosofía de automatización con respaldo humano. Por ejemplo, la empresa TenneT, gestora del sistema de transmisión eléctrica en los Países Bajos y parte de Alemania, ha desarrollado una herramienta de IA para la gestión de congestiones en la red (ayudando a decidir acciones ante sobrecargas en ciertas líneas). Este sistema opera como herramienta de apoyo en la toma de decisiones de los operadores, y no como un control autónomo total de la red (Viebahn et al., 2024). De esta forma, TenneT explota las capacidades predictivas de la IA para mejorar la confiabilidad del suministro, pero conservando la validación humana en cada paso crítico. Otro ejemplo es RTE (el operador de red en Francia), que ha introducido asistentes inteligentes (chatbots y sistemas de análisis llamados ORIGAMI) para ayudar a los ingenieros de control de red en la interpretación de datos y procedimientos (RTE, 2023). Estos asistentes aceleran tareas rutinarias y aportan recomendaciones, pero las decisiones finales siguen pasando por personal autorizado. Casos así muestran cómo las compañías energéticas europeas integran IA de forma gradual y segura, en consonancia con las exigencias de supervisión humana y responsabilidad que ahora refuerza el Reglamento.

Acciones recomendadas	• Diseñar sistemas que permitan la intervención humana en situaciones críticas. • Establecer procedimientos claros para la revisión y la validación de decisiones tomadas por la IA.

4.9. Prepararse para posibles auditorías y evaluaciones

Cumplir con la normativa no es un ejercicio de «marcar casillas» una sola vez. El Reglamento exige que los sistemas de IA de alto riesgo sean evaluados a lo largo de todo su ciclo de vida. En el dinámico sector energético, donde las condiciones cambian (nuevas pautas de consumo, integración de más renovables, ciberamenazas emergentes), es esencial establecer mecanismos de monitorización continua de los algoritmos. Así, sería recomendable implantar procesos de auditado periódico de los resultados de la IA. Por ejemplo, cada ciertos meses revisar con datos reales si un modelo de predicción de demanda mantiene la precisión esperada y no ha derivado en sesgos inaceptables. Si se detectan desviaciones, activar protocolos de recalibración (Zollo et al., 2024) o incluso apagar temporalmente funciones automatizadas hasta corregirlas. Esta mentalidad de mejora continua no solo ayudará a cumplir la ley (que obliga a reaccionar ante riesgos imprevistos), sino que también mejorará la calidad del servicio energético prestado.

Acciones recomendadas	• Mantener registros detallados de las operaciones y las decisiones de los sistemas de IA. • Establecer canales de comunicación con autoridades regulatorias. • Realizar autoevaluaciones periódicas del cumplimiento normativo.

4.10. Abordar el acceso y la calidad de los datos

La calidad de los datos es fundamental para el rendimiento y la confiabilidad de los sistemas de IA (Voss, 2024). Así como Iberdrola optó por certificar su sistema de gestión de IA según la ISO/IEC 42001, otras empresas pueden beneficiarse de seguir estándares internacionales emergentes. Si bien la ISO 42001 (sistema de gestión de IA) es voluntaria, proporciona un marco para asegurar la calidad y la gobernanza de la IA que encaja con las exigencias del Reglamento. Existen también guías, como la del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), sobre diseño ético de algoritmos (Morandín-Ahuerma, 2023) y estándares europeos CEN/CENELEC[6]. Cumplir con estos estándares «de buena práctica» no garantiza automáticamente la conformidad legal, pero facilita demostrar a reguladores y a terceros que la empresa está actuando diligentemente. En licitaciones o colaboraciones contar con certificaciones de este tipo puede convertirse en un factor diferenciador positivo.

6. <https://www.cencenelec.eu/european-standardization/european-standards/>.

Acciones recomendadas	• Establecer prácticas sólidas de gestión de datos, incluyendo la verificación y la limpieza de datos. • Resolver problemas de acceso a datos, posiblemente colaborando con otras entidades para compartir información de manera legal y ética.

5. Conclusiones

Este artículo ha analizado las principales cláusulas del Reglamento de IA que deberían tener en cuenta las empresas energéticas, y también examina los principales desafíos y oportunidades que estas empresas deberán tener en cuenta cuando adopten sus desarrollos de IA a los requisitos del Reglamento.

Por lo que respecta a los desafíos, el Reglamento exige garantizar la calidad y la representatividad de estos datos, lo que podría requerir esfuerzos adicionales de depuración, gobierno del dato y reducción de sesgos. Esto probablemente impulsará la adopción de buenas prácticas de ingeniería de IA en el sector energético, como la documentación exhaustiva de los conjuntos de datos y modelos usados, la validación cruzada de algoritmos y la realización de pruebas piloto controladas para evaluar el comportamiento del sistema en escenarios adversos. Por otro lado, el Reglamento también introduce otros desafíos que las empresas deben gestionar cuidadosamente, como la necesidad de garantizar la transparencia y la explicabilidad de los sistemas de IA, especialmente en aplicaciones de alto riesgo, lo que plantea complejidades técnicas. Además, las restricciones en el acceso a datos y las estrictas normativas de privacidad, como el RGPD, requieren que las empresas implementen sistemas de gestión de datos sólidos que equilibren la innovación con la protección de la privacidad. Finalmente, el Reglamento subraya la importancia de la formación y la capacitación del personal, ya que el éxito en la adopción de IA depende en gran medida de contar o no con una fuerza laboral capacitada para manejar estas tecnologías emergentes.

Como oportunidades destacadas, la IA permite a las empresas del sector energético optimizar sus operaciones mediante la mejora de la eficiencia de las redes eléctricas, la gestión de la demanda y la integración de energías renovables. Además, la IA facilita la implementación de mantenimiento predictivo, lo que contribuye a reducir costos y evita interrupciones en el servicio. Asimismo, la capacidad de personalizar servicios al cliente y mejorar la eficiencia energética presenta beneficios, tanto para las empresas como para los consumidores, puesto que ayuda a avanzar hacia un modelo energético más sostenible.

Este análisis concluye con la propuesta de varias recomendaciones que buscan ayudar a las empresas europeas del sector energético a inte-

grar la inteligencia artificial de manera responsable y conforme al marco regulatorio vigente, aprovechando sus beneficios mientras se minimizan los riesgos y se garantiza el respeto a los derechos fundamentales.

En conclusión, la implementación de la IA en el sector energético muestra un gran potencial para impulsar la innovación y mejorar la eficiencia operativa de las compañías eléctricas. Sin embargo, estas deben adoptar un enfoque responsable, eficiente y efectivo que combine el cumplimiento normativo con implantaciones ágiles en su seno, con equipos bien entrenados y multidisciplinarios capaces de aumentar la productividad y las labores empresariales mediante estas tecnologías.

Referencias bibliográficas

Ahmad, T.; Madonski, R.; Zhang, D.; Huang, C. y Mujeeb, A. (2022). «Data-driven probabilistic machine learning in sustainable smart energy/smart energy systems: Key developments, challenges, and future research opportunities in the context of smart grid paradigma». *Renewable and Sustainable Energy Reviews*, 160 (mayo), 112128. <https://doi.org/10.1016/j.rser.2022.112128>

Comisión Europea (2019). «Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Green Deal», *COM*(2019), 640 final (11 de diciembre).

— (2024a). *Excellence and trust in artificial intelligence*. Recuperado de <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/excellence-and-trust-artificial-intelligence_en>

— (2024b). *Artificial Intelligence Act: Call for tenders to measure and foster energy efficient and low emission artificial intelligence in the EU*. Recuperado de <https://digital-strategy.ec.europa.eu/en/node/12977/printable/pdf>

— (2024c). *European approach to artificial intelligence*. Recuperado de <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>

— (2024d). *2030 Digital Decade: Report on the State of the Digital Decade 2023* (2 de julio).

Consejo y Parlamento Europeo (2024). *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial*. Recuperado de <https://www.bdo.es/es-es/publicaciones/articulos/normas-armonizadas-inteligencia-artificial-doue>

Custers, B. y Vergouw, B. (2021). «Governing AI in Electricity Systems: Reflections on the EU Artificial Intelligence Act». *Frontiers in Artificial Intelligence*, 4. <https://doi.org/10.3389/frai.2021.690237>

Darktrace (2023). *Darktrace Publishes 2022 Cyber-Attack Trend Data for Energy, Healthcare & Retail Sectors Globally* [Comunicado de prensa] (12 de enero). Recuperado de <https://ir.darktrace.com/press-releases/2023/1/12/de3cfe253f30cae21dcaa5c4c891728ec7729e5c3e7fe1962b2c967c8ff980a3>

Demertzis, M. (2023). *Artificial intelligence and energy consumption*. Bruselas: Bruegel. Recuperado de <https://www.bruegel.org/comment/artificial-intelligence-and-energy-consumption>

Diaba, S. Y.; Shafie-Khah, M. y Elmusrati, M. (2023). «Cyber Security in Power Systems Using Meta-Heuristic and Deep Learning Algorithms». *IEEE Access*, 11, 18660-18672. <https://doi.org/10.1109/ACCESS.2023.3247193>

ENISA (2012). *Smart Grid Security: Recommendations for Europe and Member States* (1 de julio).

— (2013). *Smart Grid Threat Landscape and Good Practice Guide* (9 de diciembre).

Estebsari, A.; Mazzarino, P. R.; Bottaccioli, L. y Patti, E. (2022). «IoT-Enabled Real-Time Management of Smart Grids with Demand Response Aggregators». *IEEE Transactions on Industry Applications*, 58(1) (enero-febrero), 102-112. <https://doi.org/10.1109/TIA.2021.3121651>

Hamdan, A.; Ibekwe, K. I.; Ilojianya, V. I.; Sonko, S. y Etukudoh, E. A. (2024). «AI in renewable energy: A review of predictive maintenance and energy optimization». *International Journal of Science and Research Archive*, 11(1), 718-729.

Hickman, T.; Burmeister, T.; Erasmus, H.; Kistner, P. K. y Jha, A. (2025). «Energy efficiency requirements under the EU AI Act». *White&Case* (14 de abril). Recuperado de <https://www.whitecase.com/insight-alert/energy-efficiency-requirements-under-eu-ai-act#:~:text=Against%20this%20backdrop%2C%20emerging%20AI,It%20is%20also%20anticipated>

Iberdrola (2025). *Iberdrola garantiza el uso responsable, transparente, seguro y fiable de los sistemas de inteligencia artificial y de los algoritmos* (25 de marzo). Recuperado de <https://www.iberdrola.com/gobierno-corporativo/sistema-gobernanza-sostenibilidad/politicas-compromiso-social/politica-herramientas-inteligencia-artificial-algoritmos#:~:text=,y%20de%20los%20algoritmos>

«Iberdrola, primera empresa en certificar su Sistema de Gestión de la Inteligencia Artificial con Aenor». *El Periódico de la Energía* (17 de febrero de 2025). Recuperado de <https://elperiodicodelaenergia.com/iberdrola-primera-empresa-en-certificar-su-sistema-de-gestion-de-la-inteligencia-artificial-con-aenor/>

Islam, M. K.; Hassan, N. M. S.; Rasul, M. G.; Emami, K. y Chowdhury, A. A. (2023). «Forecasting of Solar and Wind Resources for Power Generation». *Energies*, 16, 6247. <https://doi.org/10.3390/en16176247>

Joint Research Center (2024). *AI and the energy sector*. Recuperado de <https://ses.jrc.ec.europa.eu/ai-and-energy-sector>

KPMG (2024). *Global Tech Report 2023: Energy sector insights*. Recuperado de <https://kpmg.com/uk/en/home/insights/2024/02/kpmg-global-tech-report-2023-energy-sector-insights.html>

La Ley de Inteligencia Artificial europea (Reglamento europeo 2024/1689, de 13 de junio de 2024), establece normas en materia de IA. ApudActa.com (18 de febrero de 2025). Recuperado de <https://apudacta.com/la-ley-de-inteligencia-artificial-europea/#:~:text=Los%20sistemas%20de%20IA%20de,de%20robustez%2C%20ciberseguridad%20y%20precisi%C3%B3n>

Liakeas, K.; Rachels, S. y Marshall, T. (2024). *The EU AI Act: A strategic framework for responsible AI in energy* (17 de julio). Recuperado de <https://www.capco.com/intelligence/capco-intelligence/eu-ai-act-energy-implications>

Morandín-Ahuerma, F. (2023). «IEEE: Un estándar global como iniciativa ética de la IA». En: *Principios normativos para una ética de la Inteligencia Artificial*. Puebla, México: Consejo de Ciencia y Tecnología del Estado de Puebla (CONCYTEP), 127-136.

Niet, I.; Van Est, R. y Veraart, E. (2021). «Governing AI in Electricity Systems: Reflections on the EU Artificial Intelligence Bill». *Front. Artif. Intell*, 4. <https://doi.org/10.3389/frai.2021.690237>

RTE (2023). «AI for the French Transmission System Operator». *Le Reseau de Transport d'Electricité*. Recuperado de <https://www.enlit.world/wp-content/uploads/2024/01/Vincent-Lefieux-AI-Machine-Learning-Robotics.pdf>

Sun, Y.; Gao, P. y Razzaq, A. (2023). «How does fiscal decentralization lead to renewable energy transition and a sustainable environment?: Evidence from highly decentralized economies». *Renewable Energy*, 206 (abril), 1064-1074. <https://doi.org/10.1016/j.renene.2023.02.069>

Susanto, E. y Khaq, Z. D. (2024). «Enhancing Customer Service Efficiency in Start-Ups with AI: A Focus on Personalization and Cost Reduction». *Journal of Management and Informatics*, 3(2). <https://doi.org/10.51903/jmi.v3i2.34>

Unión Europea (2016). «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)». *Diario Oficial de la Unión Europea*, L 119 (4 de mayo), 1.

— (2024). «Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial) y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial)». *Diario Oficial de la Unión Europea*, 1689 (12 de julio), 1-44. Recuperado de <https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81079>

Viebahn, J.; Kop, S.; Van Dijk, J.; Budaya, H.; Streefland, M.; Barbieri, D.; Champion, P.; Jothy, M.; Renault, V. y Tindemans, F. S. (2024). «C2 - Grid-Options Tool: Real-World Day-Ahead Congestion Management using Topological Remedial Actions». *CIGRE Science and Engineering*, 35 (diciembre).

Voss, A. (2024). «Data access is limiting AI-optimised energy production in the EU». *The Parliament Magazine*. Recuperado de <https://www.theparliamentmagazine.eu/news/article/ai-artificial-intelligence-data-energy-production-eu>

Zollo, T. P.; Deng, Z.; Snell, J. C.; Pitassi, T. y Zemel, R. (2024). *Improving Predictor Reliability with Selective Recalibration*. Cornell University (7 de octubre). Recuperado de <https://arxiv.org/abs/2410.05407>