Informe “El Reto” enerTIC

Comité de Expertos de Innovación para la eficiencia en Infraestructuras IT del Sector Energético

El reto del dato como infraestructura crítica: implicaciones energéticas y de seguridad



Septiembre 2026

Sumario

Resumen ejecutivo 3

Reconocimientos 5

Identificación del reto por el Comité de Expertos 6

DECALOGO

1. El dato como activo estratégico e infraestructura crítica 7

2. Gobernanza, calidad y confiabilidad del dato 12

3. Ciberseguridad, resiliencia y gestión del riesgo: más allá de NIS2 17

4. Convergencia real IT/OT 21

5. Inteligencia operacional e IA aplicada 26

6. Implicaciones para la flexibilidad del sistema eléctrico 31

7. Nuevas fuentes de información para una observabilidad ampliada del sistema energético 35

8. Soberanía tecnológica y seguridad de la cadena de suministro 40

9. Datos sintéticos y honestidad algorítmica 44

10. Infraestructuras digitales para un sistema energético más competitivo y escalable 49

Resultados esperados 54

Anexo: Marcos normativos, certificaciones y *frameworks* de referencia 59

Informes El Reto 2026 60

Acerca de enerTIC 63

Resumen ejecutivo

La digitalización de las redes, la electrificación, la generación distribuida y el crecimiento de la inteligencia artificial están aumentando el volumen, la diversidad y la criticidad de la información que sostiene el sistema energético. El dato ha dejado de ser un recurso auxiliar para convertirse en una infraestructura que conecta activos físicos, plataformas digitales, organizaciones y decisiones. Su disponibilidad, calidad y seguridad condicionan directamente la operación, la planificación y la capacidad de integrar nuevos recursos y consumos.

El informe identifica una prioridad central: evolucionar desde entornos fragmentados y orientados a usos concretos hacia un **ecosistema de datos gobernado, interoperable, seguro y confiable**. Esto exige coordinar IT y OT, reforzar la resiliencia, controlar las dependencias tecnológicas y aplicar la inteligencia artificial con trazabilidad, evitando que la automatización, la proliferación de fuentes o el crecimiento de la información introduzcan nuevos riesgos sobre la continuidad operativa.

El decálogo plantea cinco prioridades de actuación:

- **Tratar el dato como una infraestructura crítica**. Las organizaciones deben conocer qué información resulta esencial, dónde se genera, quién la utiliza y de qué sistemas depende. Inventarios, clasificación, linaje, responsables y políticas de ciclo de vida permiten proteger su disponibilidad y convertirlo en un activo reutilizable para la operación, la planificación y el desarrollo de nuevos servicios.
- **Construir una gobernanza conectada con la realidad operacional**. La calidad debe definirse según el uso y mantenerse desde la captura hasta la decisión. Los modelos comunes de activos, la interoperabilidad semántica y la convergencia IT/OT permiten relacionar información técnica, energética y empresarial sin eliminar las diferencias de criticidad, tiempos de respuesta y seguridad propias de cada entorno.
- **Reforzar la resiliencia y controlar las dependencias**. La ciberseguridad debe integrar prevención, detección, respuesta, recuperación y continuidad, superando una aproximación centrada únicamente en el cumplimiento de NIS2. También resulta necesario conocer la cadena de suministro, evaluar concentraciones de riesgo y disponer de alternativas, portabilidad y planes de salida ante proveedores y tecnologías críticas.
- **Convertir la información en inteligencia operacional y flexibilidad**. La analítica, la inteligencia artificial, los gemelos digitales y las nuevas fuentes de observación pueden mejorar previsiones, mantenimiento, capacidad de red y respuesta ante incidencias. Su aplicación debe vincularse a decisiones concretas e incorporar validación física, supervisión humana y mecanismos de abstención cuando la evidencia resulte insuficiente.
- **Escalar preservando la confiabilidad y el significado del dato**. Las organizaciones deben distinguir claramente entre información observada, inferida, reconstruida y sintética, comunicando procedencia, incertidumbre y limitaciones. Arquitecturas modulares, estándares y componentes reutilizables permiten ampliar capacidades sin multiplicar integraciones, costes y riesgos ni convertir la propia infraestructura digital en un nuevo cuello de botella.

Estas prioridades deben aplicarse según la madurez, la criticidad y las necesidades de cada organización. No todas requieren gemelos digitales avanzados, automatización en tiempo real o grandes plataformas de inteligencia artificial. En algunos casos, la prioridad será completar inventarios, asignar responsables, normalizar modelos de activos o reforzar copias y recuperación; en otros, integrar nuevas fuentes, desplegar previsiones avanzadas o coordinar demanda, almacenamiento y generación distribuida.

El criterio para priorizar es claro: **comenzar por la decisión o el proceso que se quiere mejorar, identificar los datos y dependencias que lo sostienen y definir después la arquitectura, los controles y el grado de automatización adecuados**. Cada iniciativa debe contar con una línea de base, responsables, métricas de resultado, validación sobre datos reales, límites operativos y mecanismos de reversión y continuidad.

Este enfoque permite convertir el dato en una capacidad estructural para utilizar mejor los activos existentes, anticipar restricciones, acelerar proyectos y coordinar un sistema energético cada vez más distribuido. La finalidad no es acumular más información ni desplegar el mayor número de modelos, sino construir una infraestructura digital que contribuya de forma verificable a la **eficiencia, la competitividad, la resiliencia, la soberanía y la sostenibilidad del sistema energético**.

Reconocimientos

Este informe ha sido posible gracias a la colaboración de los miembros del Comité y de su Presidente, cuya experiencia y compromiso han enriquecido el análisis y las conclusiones aquí presentadas.

Comité de Expertos de Innovación para la eficiencia en Infraestructuras IT del Sector Energético

Presidente



Claudio Fernández
Babel

Miembros titulares



Andoni Saiz
Ayesa



Rafael Bolívar
Enagás



David Leiva
Google



Gonzalo Valle
IFS



Pedro Puche
SAS



Ignacio Moreno
Telespazio



Javier Mazo
Hiberus



Jhon Medina
NTT Data



Guillermo Viguera
CIC Consulting Informático

Otros expertos participantes

Alexandra Vega
Teknei

Bruno Gerlic
Baobab AI

Juan Herranz
Esri

Pilar Papadopolo
S2Grupo

Eleany Restrepo
Grupo Amper

Identificación del Reto

Las organizaciones del sector energético dependen de un volumen creciente de información para operar activos, anticipar la demanda, integrar generación renovable, gestionar incidencias y planificar inversiones. Sin embargo, desde el Comité de Expertos identificamos una brecha entre esa dependencia y la capacidad de muchas organizaciones para gobernar, proteger y utilizar sus datos con la calidad y la rapidez necesarias. El dato se ha convertido en una infraestructura crítica, pero todavía se gestiona con frecuencia como un recurso fragmentado y subordinado a sistemas o proyectos concretos.

Esta brecha se aprecia cuando distintas áreas mantienen versiones incompatibles de un mismo activo; cuando se desconoce la procedencia o transformación de la información; cuando los datos operativos no pueden combinarse con fuentes empresariales, meteorológicas o territoriales; o cuando una pérdida de conectividad impide acceder a capacidades esenciales. También aparece al incorporar nuevas plataformas sin resolver integraciones anteriores, generando duplicidades, dependencias y puntos de fallo difíciles de identificar.

El reto tiene una dimensión organizativa y de seguridad. La responsabilidad sobre los datos se distribuye entre operación, mantenimiento, IT, OT, ciberseguridad, negocio y proveedores, sin que siempre exista una visión compartida de su criticidad y sus usos. A ello se suman cadenas de suministro tecnológicas cada vez más complejas, en las que una vulnerabilidad, una interrupción de servicio o una dependencia difícil de sustituir puede trasladarse rápidamente desde el entorno digital hasta la continuidad de la infraestructura física.

La expansión de la inteligencia artificial acentúa estas tensiones. Los modelos pueden mejorar previsiones, mantenimiento, flexibilidad y respuesta ante incidencias, pero dependen de información fiable, representativa y contextualizada. Incorporar más datos o generar ejemplos sintéticos no garantiza mejores decisiones si no se preservan la trazabilidad, las restricciones físicas y la incertidumbre. Una inferencia, reconstrucción o simulación presentada como observación puede introducir una apariencia de precisión con consecuencias operativas reales.

Tampoco existe un punto de partida único. Conviven activos recientes con sistemas heredados, infraestructuras altamente instrumentadas con otras de observabilidad limitada y organizaciones con capacidades muy diferentes de gobierno, integración y analítica. La respuesta no puede consistir en centralizar toda la información ni en automatizar indiscriminadamente las decisiones. Debe determinar qué datos son críticos, dónde deben procesarse, qué nivel de disponibilidad necesitan y qué decisiones requieren validación humana o capacidad de operar de forma degradada.

El Comité sitúa aquí el reto central del informe: **gobernar, proteger y aprovechar el dato como una infraestructura crítica capaz de conectar IT y OT, reforzar la inteligencia operacional y acompañar el crecimiento del sistema energético sin comprometer la seguridad, la confiabilidad ni el control**. El decálogo desarrolla las capacidades de gobierno, interoperabilidad, ciberseguridad, inteligencia artificial, soberanía y escalabilidad necesarias para avanzar en esa dirección, contribuyendo a la eficiencia, la competitividad, la resiliencia y la sostenibilidad del sector energético.

1. El dato como activo estratégico e infraestructura crítica

Elevar el dato al nivel de los activos esenciales del sector energético para garantizar resiliencia, capacidad de decisión y autonomía en un entorno cada vez más digitalizado

Durante años, el dato fue considerado principalmente un subproducto de la operación: servía para documentar lo sucedido, elaborar informes o justificar actuaciones. La digitalización ha transformado esta relación. En organizaciones intensivas en activos físicos, la información interviene hoy directamente en la planificación, la operación, el mantenimiento y la coordinación de recursos.

Esta evolución no convierte automáticamente cualquier dato en crítico. Su relevancia depende del proceso al que da soporte, de las decisiones que descansan sobre él y de las consecuencias de su pérdida, alteración o indisponibilidad. Una serie histórica destinada a un informe periódico no presenta la misma criticidad que la telemetría necesaria para supervisar una red o los datos empleados para anticipar la demanda.

En el sector energético, esta dependencia adquiere especial intensidad. Las organizaciones gestionan infraestructuras distribuidas, activos de larga vida útil, mercados dinámicos y procesos sometidos a estrictas exigencias de seguridad y continuidad. Además, deben coordinar generación, transporte, distribución, almacenamiento y consumo en un sistema donde muchas decisiones se adoptan en tiempo real o casi real.

El dato deja así de ser un recurso auxiliar para convertirse en una **capacidad estructural**. Su disponibilidad, calidad y comprensión condicionan la eficiencia operativa, la competitividad, la sostenibilidad y la resiliencia de la organización.

Una infraestructura común con una criticidad particular

La infraestructura lógica no es exclusiva del sector energético. Fábricas, aeropuertos, redes ferroviarias y operadores logísticos también necesitan conectar equipos, recopilar señales y relacionar la información con sus procesos.

Lo diferencial en energía es la profundidad con la que esta infraestructura digital se integra en actividades esenciales y el alcance de las consecuencias que puede provocar su degradación. La energía sostiene la actividad económica y numerosos servicios críticos; por ello, una pérdida de observabilidad, una previsión incorrecta o una decisión tardía pueden afectar a la continuidad del suministro, la seguridad operativa y la utilización de las infraestructuras.

Esta criticidad responde a características como:

- La distribución geográfica de redes, plantas e instalaciones.
- La necesidad de equilibrar continuamente recursos, flujos y demanda.
- La convivencia de activos con tecnologías y ciclos de vida muy diferentes.
- La integración creciente de renovables y recursos energéticos distribuidos.
- La interacción entre operación física, mercados y obligaciones regulatorias.
- El elevado impacto económico y social de las interrupciones.

También se manifiesta de manera diferente en cada segmento. En electricidad, los datos permiten equilibrar el sistema y gestionar restricciones; en gas, conocer flujos, presiones, capacidades y existencias; en renovables, prever la producción; y en almacenamiento, determinar el estado del activo y decidir cómo utilizar su capacidad.

La conclusión es común: **la capacidad física ya no puede aprovecharse plenamente sin una capacidad digital equivalente**. El valor de una red, una planta o una batería depende cada vez más de la información disponible para operarla, mantenerla y coordinarla.

Los habilitadores de una infraestructura antes inviable

La consolidación de esta infraestructura no responde a una única innovación, sino a la convergencia de diversos avances. La reducción del coste de sensores ha ampliado la monitorización a activos que antes quedaban fuera de la supervisión continua. Al mismo tiempo, las comunicaciones inalámbricas han facilitado la conexión de instalaciones remotas, móviles o distribuidas.

La estandarización de protocolos y modelos de comunicación, mediante tecnologías como IEC 61850, OPC UA, MQTT o las APIs, ha reducido algunas barreras entre equipos, sistemas operacionales y aplicaciones empresariales. A ello se suman:

- Mayor capacidad de almacenamiento y procesamiento.
- Arquitecturas cloud e híbridas capaces de escalar según la carga.
- Procesamiento edge para reducir tráfico y tiempos de respuesta.
- Plataformas orientadas a eventos y flujos continuos.
- Sistemas GIS que incorporan la dimensión territorial.
- Herramientas analíticas para combinar series temporales y fuentes heterogéneas.

Esta evolución ha hecho viable recopilar información de más activos, durante más tiempo y con mayor frecuencia. Sin embargo, también ha creado un nuevo desequilibrio: **la capacidad para capturar datos crece más rápido que la capacidad para convertirlos en información útil**.

La infraestructura crítica del dato no puede reducirse, por tanto, a sensores, conectividad y almacenamiento. El valor depende de que la información conserve una relación comprensible con el activo, el proceso y la decisión a los que sirve.

De una sucesión de plataformas a una infraestructura lógica

Las organizaciones energéticas no suelen partir de una arquitectura homogénea. En sus ecosistemas conviven ERP, EAM, APM, GIS, *historians*, SCADA, centros de control, herramientas de planificación, aplicaciones de mercado, repositorios documentales, entornos analíticos, plataformas *cloud* y dispositivos de campo.

Cada sistema aporta una parte de la realidad, pero ninguno ofrece por sí solo una visión completa. La infraestructura lógica aparece cuando estas piezas pueden relacionarse para construir una representación coherente del activo y su contexto.

Una señal adquiere mayor valor cuando se vincula con:

- El activo, su modelo y su localización.
- Su historial de funcionamiento y mantenimiento.
- Las intervenciones realizadas.
- Las condiciones ambientales.
- El servicio que presta y los elementos que dependen de él.
- Las consecuencias de su posible indisponibilidad.

Esta relación permite pasar de la acumulación de registros a una **representación operativa de la realidad**. Ya no se trata únicamente de detectar que una variable ha cambiado, sino de comprender qué activo está afectado, si el comportamiento resulta anómalo y qué actuación puede ser necesaria.

Una infraestructura lógica madura conecta el presente del activo con su historia y con las decisiones que condicionarán su futuro. Las señales muestran qué está sucediendo; los históricos permiten identificar patrones y degradaciones; y la información económica, contractual o de mantenimiento ayuda a seleccionar la respuesta más adecuada.

No todos los datos son críticos de la misma manera

Elevar el dato a la categoría de activo estratégico no implica proteger toda la información con el mismo nivel de exigencia. La criticidad debe evaluarse según el impacto de su indisponibilidad, pérdida de integridad o utilización incorrecta.

DIMENSIÓN	FUNCIONES AFECTADAS	EXIGENCIA PRINCIPAL
Operativa	Supervisión, maniobras, incidencias y seguridad	Disponibilidad, baja latencia e integridad
Analítica	Predicción, mantenimiento y evaluación de escenarios	Históricos completos, consistentes y comparables
Económica	Mercados, contratos, costes e ingresos	Precisión, actualidad y trazabilidad
Estratégica	Planificación, inversión y gestión de riesgos	Información integrada y contexto suficiente
Regulatoria	Cumplimiento, auditoría y justificación	Evidencias verificables y conservación adecuada

Para determinar la criticidad conviene preguntar:

- ¿Qué proceso perdería eficacia o dejaría de funcionar sin ese dato?
- ¿Qué decisiones dependen de su exactitud y actualidad?
- ¿Durante cuánto tiempo puede operar la organización sin él?
- ¿Qué impacto operativo, económico o regulatorio produciría un error?
- ¿Existe una fuente alternativa o un procedimiento de contingencia?
- ¿Qué sistemas, áreas o agentes dependen posteriormente de esa información?

Esta clasificación permite priorizar inversiones y establecer niveles de servicio, recuperación y conservación acordes con el impacto real sobre la actividad.

Una infraestructura para decidir en todos los niveles

Los datos respaldan decisiones en toda la organización, aunque las necesidades varían según el perfil y el horizonte temporal.

NIVEL	DECISIONES HABITUALES	NECESIDADES DE INFORMACIÓN
Operativo	Supervisar, detectar desviaciones y responder ante eventos	Alta frecuencia, baja latencia y contexto para actuar
Táctico	Priorizar trabajos, programar paradas y asignar recursos	Visión integrada del activo, riesgos, costes y disponibilidad
Estratégico	Planificar capacidad, evaluar escenarios y asignar inversiones	Información consolidada, comparable y multidimensional

Esta diferenciación evita convertir el tiempo real en un objetivo indiscriminado. Una señal puede necesitar procesarse en milisegundos para proteger un activo, en segundos para respaldar una maniobra, en horas para programar una intervención o en meses para orientar una inversión.

También cambia la granularidad. Un operador puede requerir señales individuales; un gestor de activos, indicadores agregados de salud y rendimiento; y la dirección, in-

formación comparable sobre disponibilidad, riesgo y retorno. La infraestructura debe permitir que todos trabajen sobre una **base coherente**, sin imponer la misma representación a necesidades diferentes.

Cuando perder el dato significa perder capacidad de actuación

La indisponibilidad de información no siempre detiene inmediatamente un activo, pero puede reducir de forma sustancial la capacidad para operarlo. Una red puede seguir energizada tras perder parte de su observabilidad y una planta continuar funcionando sin un modelo predictivo, aunque la organización pase a actuar con mayor incertidumbre y menor capacidad de anticipación.

La pérdida de datos puede obligar a adoptar criterios más conservadores, aumentar las inspecciones manuales, mantener mayores reservas o limitar determinadas maniobras. También puede impedir detectar una degradación temprana, reducir la precisión de las previsiones y dificultar la priorización de intervenciones.

Entre sus consecuencias se encuentran:

- Pérdida de observabilidad sobre redes, activos e instalaciones.
- Menor capacidad para detectar fallos o restricciones emergentes.
- Deterioro de las previsiones de demanda, generación o precios.
- Incremento de falsas alarmas y actuaciones innecesarias.
- Programación menos eficiente del mantenimiento.
- Mayor exposición a indisponibilidades, penalizaciones y costes.

La **integridad** resulta tan importante como la disponibilidad. Recibir información de forma continua no evita decisiones incorrectas si las mediciones están alteradas, descontextualizadas o asociadas al activo equivocado. Un dato erróneo que aparenta ser confiable puede resultar más peligroso que una interrupción evidente.

También debe preservarse la continuidad histórica. Sin ella, la organización puede conocer el presente, pero pierde parte de su capacidad para interpretar la evolución de los activos y anticipar su comportamiento.

Por ello, la resiliencia no debe medirse únicamente mediante la disponibilidad técnica de una plataforma. La pregunta relevante es **qué decisiones pueden seguir adoptándose, con qué confianza y mediante qué alternativas**.

Del dato al resultado empresarial

Capturar más información o aumentar el almacenamiento no constituye por sí mismo una mejora. El valor aparece cuando los datos permiten aprovechar mejor los activos, reducir riesgos, evitar pérdidas y decidir con mayor rapidez y precisión.

En gestión de activos, ayudan a anticipar degradaciones y ajustar el mantenimiento; en operación, a detectar restricciones y coordinar recursos; en mercados, a mejorar previsiones; y en planificación, a reducir la incertidumbre sobre demanda, capacidad e inversiones.

Los resultados pueden evaluarse mediante indicadores como:

- Disponibilidad e indisponibilidad de los activos.
- MTBF, MTTR y antelación en la detección de fallos.
- Precisión de las previsiones de demanda, generación y precios.
- Reducción de pérdidas, restricciones y vertidos de renovables.
- Capacidad flexible identificada y realmente movilizada.
- Costes evitados, ingresos capturados y utilización de infraestructuras.

Estos resultados no dependen únicamente de la tecnología. También intervienen la calidad de la información, los procesos y la actuación de las personas. No obstante, los indicadores permiten comprobar si la infraestructura digital contribuye al desempeño o permanece desconectada de las necesidades reales del negocio.

La dimensión física y organizativa del dato

Aunque el dato sea intangible, la infraestructura que lo sostiene es material. Su captura requiere sensores; su transmisión, redes; y su almacenamiento y procesamiento, servidores, centros de datos, refrigeración y un suministro energético fiable.

La relación es bidireccional: **la energía sostiene la infraestructura digital y la infraestructura digital permite gestionar mejor la energía**. El crecimiento de la inteligencia artificial y del procesamiento aumenta la demanda energética, mientras que los datos ayudan a integrar y optimizar esos nuevos consumos.

Por ello, no toda la información debe conservarse con la máxima resolución ni procesarse permanentemente en entornos de alta capacidad. La arquitectura debe decidir dónde procesar cada dato, durante cuánto tiempo almacenarlo y qué disponibilidad requiere. La protección del dato debe equilibrarse con el coste, el consumo energético y el valor generado.

La responsabilidad tampoco puede recaer exclusivamente en IT. Los expertos en operación, mantenimiento, mercados y planificación deben definir qué información necesitan, cómo interpretarla y qué consecuencias tendría su degradación.

Las organizaciones necesitan:

- Traducir los objetivos operativos y empresariales en requisitos de información.
- Involucrar a los expertos de dominio en el diseño y la validación.
- Adaptar las herramientas a cada perfil y nivel de decisión.
- Formar a los profesionales para interpretar indicadores e incertidumbres.
- Integrar los datos en los procedimientos reales de trabajo.
- Medir el valor generado y revisar los casos de uso sin resultados.

Proporcionar más información no mejora automáticamente la capacidad de actuación. Si los datos no están priorizados y contextualizados, pueden incrementar la carga cognitiva, multiplicar las alarmas y ocultar las situaciones verdaderamente relevantes.

El dato como capacidad estructural del sistema energético

Considerar el dato como infraestructura crítica implica reconocer el papel que ya desempeña. Las organizaciones energéticas dependen de él para conocer sus activos, anticipar su comportamiento, coordinar recursos y responder ante escenarios complejos. Su pérdida no supone únicamente un problema informático, sino una **reducción de la capacidad para decidir, operar y competir**.

Esta visión no debe conducir a acumular información indiscriminadamente. El objetivo es identificar qué datos resultan necesarios, qué decisión respaldan, con qué latencia y granularidad deben estar disponibles y qué impacto tendría su degradación.

La cadena de valor conecta directamente el mundo físico con la actuación:

- Los activos y procesos generan señales, eventos y registros.
- La infraestructura digital captura, transmite y procesa la información.
- El contexto convierte los datos en una representación comprensible.
- Las personas y los sistemas utilizan esa representación para decidir.

- Las decisiones se traducen en actuaciones sobre activos, recursos y mercados.
- Los resultados permiten revisar y mejorar el proceso.

Sobre esta base pueden desarrollarse capacidades avanzadas de gobierno, integración, predicción, optimización e inteligencia operacional. Sin ella, la sofisticación analítica carece de cimientos sólidos; con ella, el dato se convierte en un multiplicador de la eficiencia y en una fuente de resiliencia y ventaja competitiva.

El reto consiste en gestionar la infraestructura lógica con una atención proporcional a su impacto sobre la infraestructura física. Las organizaciones energéticas no competirán únicamente por disponer de mejores activos o mayor capacidad de generación, sino también por **comprender mejor su sistema, anticipar su evolución y transformar la información en decisiones** que impulsen la eficiencia, la competitividad y la sostenibilidad.

2. Gobernanza, calidad y confiabilidad del dato

Construir una infraestructura lógica fiable, contextualizada y orientada al propósito que permita convertir la información en decisiones operativas y empresariales

La digitalización energética ha multiplicado el volumen, la frecuencia y la diversidad de la información. Sensores, sistemas SCADA, plataformas GIS, aplicaciones corporativas y fuentes externas generan flujos continuos de datos. El desafío ya no es capturarlos, sino garantizar que **representen correctamente la realidad y puedan utilizarse con confianza**.

Una infraestructura lógica exige datos definidos, contextualizados, trazables y sometidos a controles proporcionales a las decisiones que respaldan. Sin esas condiciones, acumular registros no proporciona una visión fiable de los activos.

Esta distinción resulta decisiva ante el crecimiento de la analítica y la inteligencia artificial. Los algoritmos detectan patrones a gran escala, pero no corrigen definiciones ambiguas, mediciones descalibradas o asociaciones incorrectas. Una base débil puede hacer que la sofisticación analítica **acelere y extienda conclusiones erróneas**.

CAPA	FUNCIÓN	PREGUNTA FUNDAMENTAL	RIESGO PRINCIPAL
Infraestructura tecnológica	Capturar, transmitir, almacenar y procesar	¿Podemos obtener la información?	Pérdida de cobertura o disponibilidad
Infraestructura lógica	Definir, contextualizar, relacionar y trazar	¿Comprendemos el dato y confiamos en él?	Inconsistencias e interpretaciones erróneas
Analítica e IA	Detectar patrones, predecir y recomendar	¿Qué conocimiento podemos obtener?	Automatización de errores
Decisión y actuación	Convertir el conocimiento en respuesta	¿Qué debe hacerse y con qué límites?	Inacción o actuaciones incorrectas

La gobernanza se concentra en la segunda capa, pero conecta toda la cadena para que la información conserve su significado, integridad y utilidad hasta convertirse en una actuación.

De acumular datos a construir confianza

Las fuentes conectadas y el volumen almacenado describen la escala tecnológica, pero no determinan si los datos son aptos para decidir. Los usuarios deben conocer qué representa cada dato, su procedencia, transformaciones, limitaciones y usos validados.

En energía, una previsión basada en históricos incompletos incrementa los desvíos; una medición asociada al activo equivocado provoca intervenciones innecesarias; y una estimación incorrecta de flexibilidad puede comprometer una capacidad inexistente.

La confiabilidad se apoya en varios atributos:

- **Exactitud**: correspondencia con la realidad representada.
- **Completitud**: cobertura de los campos, activos y periodos necesarios.
- **Consistencia**: coherencia entre sistemas que describen una misma entidad.
- **Actualidad**: disponibilidad dentro del plazo requerido.
- **Contexto**: relación con el activo, el momento, la ubicación y el proceso.
- **Trazabilidad**: conocimiento del origen y las transformaciones.
- **Disponibilidad**: acceso autorizado cuando resulta necesario.
- **Interpretación inequívoca**: definiciones, unidades y criterios comunes.

La importancia de cada atributo depende del propósito. En supervisión pueden primar continuidad y latencia; en planificación, profundidad histórica y comparabilidad; y en modelos predictivos, representatividad y etiquetado. **La calidad es la adecuación del dato al uso previsto**, no un valor absoluto.

Calidad vinculada al activo y a la decisión

Detectar campos vacíos, formatos incorrectos o duplicados resulta necesario, pero insuficiente. Una medición puede superar las validaciones informáticas y ser físicamente improbable o incompatible con el estado operativo del activo. Los controles deben incorporar conocimiento técnico:

- Rangos y velocidades de cambio según el activo y su régimen de funcionamiento.
- Comparación entre sensores redundantes y variables relacionadas.
- Detección de señales congeladas, periodos sin datos y frecuencias irregulares.
- Verificación de unidades, escalas, marcas temporales y sincronización.
- Identificación de descalibración o envejecimiento de sensores.
- Contraste con la topología, las condiciones ambientales y el estado operativo.

DIMENSIÓN	CONTROL ORIENTATIVO	RIESGO EMPRESARIAL	KPI POSIBLE
Exactitud	Contraste con sensores o reglas físicas	Diagnósticos incorrectos	Mediciones dentro de tolerancia
Completitud	Cobertura de variables y periodos	Modelos sesgados	Datos esperados recibidos
Consistencia	Comparación entre SCADA, GIS y EAM	Versiones contradictorias	Discrepancias entre sistemas
Actualidad	Tiempo desde la captura	Detección tardía	Edad máxima del dato
Contextualización	Asociación con activo y modo operativo	Interpretación errónea	Datos correctamente vinculados
Trazabilidad	Registro de origen y transformaciones	Resultados inexplicables	Flujos con linaje documentado

Los umbrales deben ajustarse a la criticidad. La organización necesita definir qué desviaciones pueden advertirse al usuario y cuáles obligan a bloquear un dato para impedir que alimente una decisión o un proceso automatizado.

Contextualización, normalización y semántica

Un valor aislado aporta poca información. Una temperatura de 80 grados o una caída de presión no pueden interpretarse sin conocer el activo, su configuración, su régimen de funcionamiento y las condiciones de la medición. **El contexto convierte una señal en información** y permite diferenciar una condición normal de una anomalía.

La contextualización debe incorporar varias dimensiones:

- Técnica y operativa: activo, modelo, configuración, carga, estado y consignas.
- Temporal y geográfica: instante, frecuencia, secuencia, ubicación y entorno.
- Topológica: conexiones, dependencias y posición dentro del sistema.
- Empresarial: propietario, contrato, criticidad, coste y nivel de servicio.

Esta visión exige relacionar fuentes: el GIS aporta ubicación y topología; el EAM, identidad e historial; el SCADA, comportamiento operacional; y los sistemas corporativos, dimensión económica. No es necesario centralizarlo todo, pero sí definir identificadores y relaciones comunes.

La coexistencia de plataformas y generaciones tecnológicas provoca que un activo tenga códigos, unidades o taxonomías diferentes. La normalización debe establecer identificadores persistentes, unidades y reglas de conversión, jerarquías de activos, taxonomías de estados y definiciones compartidas de variables e indicadores.

Los datos maestros proporcionan referencias comunes; los modelos semánticos describen relaciones; y los metadatos explican origen, propiedad y uso. El objetivo es crear un **lenguaje común para intercambiar información**, preservando la precisión de cada dominio.

Trazabilidad, latencia y granularidad

La información suele atravesar dispositivos, *gateways*, procesos de integración, repositorios y capas analíticas antes de llegar a una aplicación. Durante ese recorrido puede filtrarse, agregarse, corregirse o combinarse. El linaje debe permitir conocer:

- Qué dispositivo o sistema generó la información.
- Qué momento representa y cuándo fue recibida.
- Qué transformaciones y controles se aplicaron.
- Quién autorizó los cambios relevantes.
- Qué informes, modelos y procesos la consumen.
- Qué decisiones quedarían afectadas por una modificación.

La trazabilidad permite reconstruir resultados y evaluar cambios. Los catálogos, el versionado y el *data lineage* ayudan, pero las transformaciones manuales no documentadas crean puntos ciegos.

Un dato exacto también puede perder su valor si llega tarde o con una frecuencia insuficiente. La latencia real comprende el tiempo transcurrido entre la producción física del evento, su captura, recepción, procesamiento, presentación y conversión en una decisión. Diferenciar estas etapas permite localizar el origen de los retrasos.

NIVEL DE DECISIÓN	HORIZONTE	INFORMACIÓN REQUERIDA	EXIGENCIA PRINCIPAL
Operativo automático	Segundos o menos	Señales y estados inmediatos	Muy baja latencia y alta frecuencia
Operativo humano	Segundos, minutos u horas	Estado, eventos y contexto	Detalle suficiente para diagnosticar
Táctico	Días, semanas o meses	Tendencias, rendimiento e históricos	Agregación controlada y contexto
Estratégico	Meses o años	Escenarios, costes y riesgos	Comparabilidad y profundidad histórica

La máxima frecuencia no siempre es la mejor solución. Una resolución innecesaria incrementa volumen, consumo y complejidad sin mejorar la decisión. Además, reutilizar un dato para un nuevo propósito exige comprobar nuevamente su aptitud: **estar disponible no significa servir para cualquier análisis**.

Responsabilidades compartidas

La gobernanza fracasa cuando se concibe como una función exclusivamente tecnológica. IT administra plataformas y accesos, pero los expertos de dominio determinan si una medición representa correctamente el activo y qué margen de error resulta aceptable.

ROL	RESPONSABILIDAD PRINCIPAL
Data Owner	Define prioridades, usos y niveles de calidad
Data Steward	Mantiene definiciones, metadatos y reglas
Data Custodian	Garantiza acceso, controles y conservación
Experto de dominio	Valida coherencia física y relación con los procesos
Consumidor del dato	Comunica requisitos, limitaciones e incidencias
Comité de gobierno	Establece estándares y resuelve conflictos

Los roles pueden adaptarse, pero no quedar implícitos. Sin un responsable, los errores persisten y aparecen soluciones paralelas. Los proveedores también deben asumir requisitos contractuales sobre formatos, frecuencia, calidad y acceso.

KPIs orientados al negocio

El número de políticas, términos documentados o fuentes catalogadas muestra actividad, pero no demuestra que la información sea más fiable. Los indicadores deben combinar:

- **Salud del dato**: exactitud, completitud, consistencia, actualidad y trazabilidad.
- **Eficacia operativa**: detección y resolución de incidencias, automatización y reducción de tareas manuales.
- **Impacto empresarial**: mejora de previsiones, reducción de falsas alarmas y menor número de decisiones afectadas.

Entre los KPIs aplicables figuran los activos contextualizados, las variables críticas con controles automáticos, las incidencias detectadas a tiempo, el plazo de resolución, los flujos con linaje y las reconciliaciones manuales eliminadas.

La relación con el resultado debe ser explícita. Normalizar identificadores debería reducir discrepancias entre GIS, EAM y SCADA; mejorar la sincronización temporal tendría que favorecer la detección de anomalías; y corregir deficiencias debería aumentar la precisión de las previsiones.

Gobernar sin frenar la innovación

Un exceso de procedimientos puede ralentizar el acceso y favorecer circuitos informales. El extremo contrario genera deuda de datos, métricas contradictorias e integraciones difíciles de mantener. El equilibrio exige controles proporcionales al riesgo:

- Reglas mínimas y plantillas reutilizables desde el inicio.
- Validaciones automáticas integradas en los flujos.
- Catálogos que faciliten descubrir y reutilizar información.
- Controles priorizados según criticidad.
- Gestión ágil de excepciones y revisión de reglas sin valor.

Tratar determinados conjuntos como **productos de datos** ayuda a definir quién responde por ellos, qué consumidores atienden y qué nivel de servicio ofrecen. La gobernanza también necesita formación, incentivos y herramientas integradas en el trabajo cotidiano. El conocimiento de operadores y técnicos debe incorporarse a reglas y modelos para evitar que permanezca concentrado en personas concretas.

Una base fiable para escalar la capacidad digital

La gobernanza no es una iniciativa temporal ni un trámite previo a la inteligencia artificial. Constituye una capacidad permanente que debe evolucionar con los activos, las plataformas y los procesos. La organización debe poder responder:

- ¿Qué representa exactamente cada dato?
- ¿De dónde procede y qué transformaciones ha experimentado?
- ¿Con qué calidad y actualidad está disponible?
- ¿Para qué decisiones ha sido validado?
- ¿Quién responde por su mantenimiento y utilización?

Cuando estas preguntas no tienen respuesta, la organización acumula información, pero no construye confianza. Cuando sí la tienen, los datos se reutilizan con mayor rapidez, las incidencias se detectan antes y disminuye la dependencia de reconciliaciones manuales.

La ventaja no procederá de disponer de más datos, sino de **saber cuáles son adecuados para cada propósito, qué limitaciones presentan y qué decisiones pueden respaldar**. Esa confianza permite anticipar mejor, reducir incertidumbre y escalar la digitalización sin multiplicar el riesgo.

3. Ciberseguridad, resiliencia y gestión del riesgo: más allá de NIS2

Evolucionar desde una visión centrada en el cumplimiento hacia una gestión estratégica del riesgo capaz de preservar los activos digitales, los datos y los procesos que sustentan el sector energético

La transformación digital desplaza parte de la criticidad energética hacia una infraestructura interconectada. Sistemas corporativos, entornos OT, arquitecturas cloud, dispositivos de campo y servicios de terceros condicionan la capacidad para operar los activos físicos.

La ciberseguridad debe entenderse como una **capacidad para preservar el funcionamiento del negocio**. Su objetivo es mantener los servicios esenciales, proteger la integridad de las decisiones y recuperar las capacidades afectadas dentro de límites aceptables.

La resiliencia amplía la prevención. La madurez consiste en reducir la probabilidad de incidentes, limitar su alcance, detectarlos con rapidez y conservar capacidad operativa durante la recuperación.

Del riesgo tecnológico al impacto empresarial

Vulnerabilidades y alertas deben relacionarse con los procesos afectados. Una debilidad grave puede tener impacto limitado si está aislada, mientras que otra menor puede alterar datos operativos o comprometer una identidad privilegiada.

La evaluación debe combinar **amenaza, exposición, criticidad y capacidad de respuesta**. Así, el riesgo se expresa en términos de pérdida de observabilidad, indisponibilidad, interrupción de ingresos, daños sobre activos o deterioro de la seguridad.

Capacidad comprometida	Consecuencia	Impacto empresarial	Prioridad
Observabilidad	Pérdida de telemetría y alarmas	Mayor incertidumbre y operación conservadora	Recuperar fuentes críticas
Integridad del dato	Mediciones o previsiones alteradas	Decisiones incorrectas	Aislar fuentes y reconstruir información fiable
Control remoto	Imposibilidad de ejecutar maniobras	Menor agilidad y más intervención local	Activar operación degradada
Gestión de activos	Pérdida de históricos u órdenes	Mantenimiento ineficiente	Recuperar mínimos y priorizar activos
Mercados y previsión	Degradación de cálculos o comunicaciones	Desvíos y penalizaciones	Aplicar modelos alternativos

Estas relaciones deben conocerse antes de una crisis. Si durante el incidente todavía se investigan las dependencias de cada plataforma, se perderá un tiempo decisivo.

NIS2 como base, no como meta

NIS2 refuerza el enfoque basado en el riesgo, la responsabilidad directiva y la notificación de incidentes. Su aportación principal es incorporar la ciberseguridad al gobierno corporativo y vincularla con la continuidad.

El cumplimiento documental no garantiza resiliencia. Pueden existir políticas correctas junto a activos desconocidos, copias no verificadas o tiempos de recuperación incompatibles con el negocio.

ÁMBITO	APLICACIÓN OPERATIVA	EVIDENCIA DE MADUREZ
Gestión del riesgo	Relacionar amenazas con procesos esenciales	Inventario crítico y escenarios priorizados
Incidentes	Detectar, contener y comunicar	Procedimientos probados y responsables definidos
Continuidad	Mantener o recuperar capacidades prioritarias	BCP, DRP y restauraciones verificadas
Identidades	Limitar privilegios y movimientos laterales	MFA, IAM, PAM y revisión de permisos
Proveedores	Controlar el riesgo introducido por terceros	Requisitos contractuales y supervisión
Eficacia	Comprobar los controles en condiciones reales	Auditorías, simulaciones y mejoras completadas

La resiliencia exige demostrar que las medidas funcionan, que los responsables saben aplicarlas y que la organización puede mantener los procesos críticos cuando la realidad no coincide exactamente con los procedimientos.

Conocer y reducir la exposición

No es posible proteger activos cuya existencia, configuración o dependencia se desconoce. El inventario debe superar el listado de equipos y recoger:

- Identidad, ubicación, función, versión y estado de soporte.
- Propietarios tecnológico y empresarial.
- Comunicaciones, dependencias y servicios asociados.
- Usuarios, privilegios y accesos remotos.
- Vulnerabilidades, controles y criticidad.
- Posibilidades de aislamiento, sustitución y recuperación.

La visibilidad debe actualizarse continuamente en entornos donde conviven sistemas corporativos, tecnologías OT, componentes *legacy* y servicios *cloud*. Las herramientas de descubrimiento deben evitar interferencias con equipos sensibles.

La identidad constituye otro perímetro. Zero Trust exige verificar accesos, aplicar el mínimo privilegio y asumir posibles compromisos. Las prioridades incluyen IAM, PAM, autenticación multifactor, revisión de permisos y accesos de proveedores individualizados y temporales.

En OT, estas medidas deben respetar la disponibilidad y las limitaciones técnicas. Cualquier conexión necesita **una identidad verificable, un propósito autorizado y privilegios limitados**, sin introducir bloqueos incompatibles con la operación.

Proteger el dato y la confianza en las decisiones

Los datos describen activos, capacidades y patrones de demanda. Su protección debe garantizar confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad durante todo el ciclo de vida.

La integridad merece especial atención: una información manipulada puede aparentar normalidad y provocar una actuación incorrecta. A medida que aumenta la automatiza-

ción, el incidente puede propagarse desde la capa de datos hasta el entorno físico. Cifrado, segregación, control de acceso, firmas, auditoría y monitorización deben aplicarse de acuerdo con la criticidad.

De las alertas a la conciencia situacional

La detección eficaz combina señales de distintas capas mediante SIEM, SOAR, EDR/XDR, NDR, inteligencia de amenazas, gestión de vulnerabilidades y observabilidad de entornos híbridos y operacionales. Su valor no reside en acumular alertas, sino en **convertir señales técnicas en una interpretación del riesgo empresarial**.

CAPACIDAD	PREGUNTA	RESULTADO ESPERADO
Visibilidad	¿Qué activos, identidades y comunicaciones existen?	Superficie conocida
Detección	¿Qué comportamiento se desvía de lo esperado?	Identificación temprana
Contextualización	¿Qué procesos podrían verse afectados?	Priorización por impacto
Orquestación	¿Qué acciones pueden automatizarse?	Menor tiempo de respuesta
Decisión	¿Qué medida debe adoptarse y quién la autoriza?	Contención coordinada

Los analistas conocen amenazas y patrones de ataque; los equipos operativos, los activos y las consecuencias de aislarlos. La conciencia situacional exige combinar ambos conocimientos.

Responder sin agravar el incidente

Una respuesta precipitada puede ampliar el impacto. Aislar un sistema o bloquear una cuenta puede contener la amenaza e interrumpir simultáneamente una función esencial. Las medidas deben estar predefinidas, probadas y adaptadas a IT y OT.

La respuesta debe cubrir:

- Identificación, validación y clasificación del incidente.
- Contención y limitación de movimientos laterales.
- Análisis del origen, persistencia y activos afectados.
- Erradicación y recuperación controlada.
- Verificación de datos, identidades y configuraciones.
- Comunicación interna, regulatoria y a terceros.
- Revisión posterior y aplicación de mejoras.

Los procedimientos deben establecer quién autoriza cada actuación y prever la caída de canales habituales. La notificación requiere clasificación, conservación de evidencias y coordinación jurídica. Los ejercicios permiten detectar ambigüedades antes de una crisis.

Continuidad orientada a capacidades críticas

Recuperar no significa encender todos los sistemas cuanto antes, sino restablecer las capacidades esenciales en el orden adecuado. Los planes BCP y DRP deben definir:

- RTO y RPO coherentes con el impacto empresarial.
- Orden y dependencias de restauración.

- Capacidades mínimas para operar de forma degradada.
- Procedimientos alternativos, responsables y recursos.
- Criterios para regresar a la operación normal.

Las copias deben estar aisladas, utilizar credenciales separadas y ser inmutables cuando proceda. Es necesario probar restauraciones y verificar tiempos y consistencia.

La **operación degradada** permite mantener funciones limitadas y seguras mientras se recupera la automatización. Los equipos deben conocer qué decisiones pueden adoptar, qué información continúa siendo fiable y qué límites no deben superar.

KPIs para medir resiliencia

El número de herramientas, alertas o vulnerabilidades registradas no mide por sí mismo la resiliencia. Los indicadores deben mostrar si la organización conoce su exposición, detecta con rapidez, limita el impacto y recupera las funciones prioritarias.

DIMENSIÓN	KPI ORIENTATIVO	Precaución
Cobertura	Activos críticos inventariados y monitorizados	Cobertura no equivale a buena telemetría
Detección	MTTD y permanencia no detectada	Segmentar por criticidad y entorno
Respuesta	Tiempo de clasificación y contención	Rapidez no garantiza una decisión correcta
Recuperación	MTTR y cumplimiento de RTO/RPO	Verificar mediante pruebas reales
Identidades	Privilegios protegidos y revisados	Evaluar la calidad de las revisiones
Copias	Restauraciones completadas con éxito	Una copia sin probar genera falsa confianza
Preparación	Hallazgos de ejercicios corregidos	Simular sin mejorar aporta poco valor

Los KPIs deben vincularse con la indisponibilidad evitada, la contención y la preservación de los datos. Medir solo vulnerabilidades cerradas puede relegar exposiciones críticas.

Gobierno, personas y terceros

La resiliencia requiere coordinación entre dirección, ciberseguridad, IT, OT, continuidad, comunicación, áreas jurídicas y negocio. La dirección debe definir la tolerancia al riesgo, aprobar recursos, supervisar excepciones, participar en ejercicios y asegurar que las mejoras se completan.

La formación debe adaptarse a cada perfil. Una cultura madura facilita comunicar errores sin penalizaciones que retrasen la respuesta e incorpora la seguridad a los objetivos de proyectos y operaciones.

Los proveedores amplían la exposición. Sus accesos deben ser limitados, temporales, protegidos con MFA y registrados. Los contratos deben exigir notificación, cooperación y revocación rápida. La dependencia tecnológica se desarrolla en el capítulo 8.

La ciberseguridad como inversión en continuidad

Ir más allá de NIS2 significa utilizar el cumplimiento como punto de partida para cinco capacidades conectadas: conocer, proteger, detectar, responder y recuperar.

La ciberseguridad genera valor cuando reduce la probabilidad y el impacto de las interrupciones, protege la integridad de las decisiones y permite innovar sobre una base confiable. En un entorno donde la digitalización aumenta simultáneamente la capacidad operativa y la exposición, la resiliencia deja de ser una función de soporte: se convierte en una condición para seguir operando, decidir y recuperarse cuando la prevención no ha sido suficiente.

4. Convergencia real IT/OT

Conectar la operación y el negocio mediante arquitecturas interoperables que preserven el contexto, la seguridad y las exigencias propias de los activos energéticos

IT y OT han evolucionado con prioridades y ritmos diferentes. Los entornos corporativos han incorporado *cloud*, APIs y ciclos rápidos de desarrollo, mientras que los sistemas operacionales priorizan la disponibilidad, la estabilidad y la seguridad de procesos físicos cuya interrupción puede afectar al suministro, los activos o las personas.

Esta diferencia responde a la naturaleza de cada dominio. Una aplicación corporativa puede admitir actualizaciones o reinicios; un sistema de control puede operar durante décadas y exigir pruebas específicas antes de cualquier cambio. El problema surge cuando esa separación impide relacionar información operacional, económica, geográfica y de mantenimiento.

La convergencia IT/OT debe permitir **compartir datos y responsabilidades sin eliminar las particularidades de cada entorno**. No busca convertir OT en IT ni conectar indiscriminadamente los activos, sino utilizar la información operacional allí donde aporte valor, manteniendo la seguridad y la autonomía del control.

DIMENSIÓN	IT	OT	IMPLICACIÓN
Objetivo	Gestionar información y procesos	Supervisar y controlar activos	Integrar sin alterar el control
Prioridad	Confidencialidad, integridad y disponibilidad	Seguridad física, disponibilidad y respuesta	Adaptar los controles al impacto operacional
Ciclo de vida	Renovación frecuente	Décadas de servicio	Desacoplar ritmos tecnológicos
Actualizaciones	Regulares y automatizables	Ventanas limitadas y pruebas exhaustivas	Coordinar cambios
Latencia	Variable	Puede ser determinista	Mantener procesamiento local cuando sea necesario
Responsabilidad	Tecnología y áreas corporativas	Operación, ingeniería y mantenimiento	Establecer gobierno compartido

Converger no significa conectarlo todo

La madurez no se mide por el número de conexiones, sino por la utilidad y el control de los flujos. Cada integración debe responder:

- ¿Qué decisión necesita el dato y cuál es su fuente autorizada?
- ¿Qué latencia, frecuencia y granularidad requiere?
- ¿El flujo debe ser unidireccional o actuar sobre OT?
- ¿Qué ocurriría si se interrumpiera o transmitiera información incorrecta?
- ¿Puede la operación continuar de forma autónoma?
- ¿Quién valida y mantiene la integración?

Tampoco toda la información debe trasladarse al *cloud*. La carga puede procesarse en el dispositivo cuando exige respuesta inmediata; en el *edge* para filtrar o agregar; en plataformas OT para supervisar; en la capa corporativa para combinarla con datos empresariales; o en *cloud* y centros de datos cuando requiere elasticidad y cálculo intensivo.

La arquitectura debe distribuir capacidades según el propósito y mantener las funciones esenciales cuando fallen una comunicación o una plataforma externa.

El dato como punto de encuentro

OT aporta señales, alarmas, estados y series temporales; IT incorpora costes, órdenes de trabajo, contratos, inventarios, localización y previsiones. Cuando ambas perspectivas permanecen aisladas, operación conoce el estado inmediato del equipo, pero no siempre su impacto económico; mantenimiento dispone de órdenes e inventarios, pero puede carecer de variables que anticipen una degradación.

Su integración permite identificar qué activos se degradan, relacionar anomalías con intervenciones, priorizar trabajos según criticidad, comparar coste e indisponibilidad y evaluar qué inversiones mejoran el rendimiento.

El dato operacional adquiere valor empresarial cuando se **vincula con el activo, su contexto y las consecuencias de su comportamiento**. La información corporativa permite priorizar decisiones que no pueden tomarse observando únicamente variables físicas.

Arquitecturas desacopladas y seguras

Las conexiones punto a punto resuelven necesidades inmediatas, pero generan dependencias difíciles de mantener. El desacoplamiento permite publicar información mediante interfaces controladas para que los consumidores no dependan de las particularidades del origen.

PATRÓN	USO ADECUADO	VENTAJA	PRECAUCIÓN
API	Consulta de información actualizada	Control y reutilización	Evitar dependencia inmediata del origen
Historian o plataforma de datos	Explotación de series temporales	Preserva históricos	Mantener tiempo, calidad y contexto
Event streaming	Distribución continua de eventos	Escala a múltiples consumidores	Gestionar orden y duplicados
Gateway industrial	Integración de equipos *legacy*	Extiende la vida de los activos	Controlar latencia y funciones
Transferencia unidireccional	Extracción desde zonas críticas	Reduce el riesgo de retorno	No permite interacción bidireccional
Edge	Filtrado y análisis local	Reduce latencia y tráfico	Gestionar versiones y operación distribuida

Debe diferenciarse el plano de información del plano de control. Compartir datos de OT no implica permitir que una aplicación corporativa actúe directamente sobre los activos. Las órdenes necesitan validaciones, autorizaciones y límites acordes con su impacto. La arquitectura debe mantener una frontera explícita entre **observar, recomendar, autorizar y actuar**.

La segmentación por zonas y conductos, las DMZ industriales y las capas de integración controlan qué sistemas se comunican, mediante qué protocolos y con qué propósito. Una estructura funcional distingue:

- Campo y control local: sensores, actuadores, PLC, RTU e IED.
- Supervisión operacional: SCADA, DCS, EMS, DMS y centros de control.
- Integración industrial: historians, gateways, brokers y DMZ.
- Plataformas empresariales: GIS, EAM, APM, ERP y planificación.
- Datos y analítica: plataformas de datos y capacidad de cálculo.
- Consumo y decisión: aplicaciones, cuadros de mando y flujos de trabajo.

Esta separación evita que una aplicación corporativa acceda directamente a dispositivos de campo y permite preservar la operación local.

Interoperabilidad técnica y semántica

Transmitir datos no garantiza que el receptor los interprete correctamente. La interoperabilidad técnica permite mover información; la semántica preserva su significado. Estándares como IEC 61850, OPC UA, MQTT y las APIs proporcionan mecanismos de intercambio, pero deben conservar:

- Identidad y jerarquía del activo.
- Variable, unidad, escala y precisión.
- Marca temporal y origen del evento.
- Calidad y validez de la medición.
- Estado operativo y relación topológica.
- Transformaciones y versión del modelo utilizado.

Los contratos de datos formalizan estructura, frecuencia, nivel de servicio y gestión de cambios. Así se evita que una modificación en OT rompa silenciosamente procesos corporativos o modelos analíticos.

Los sistemas *legacy* requieren *gateways*, adaptadores o capas de abstracción que extraigan la información sin convertirlos en el centro permanente de la arquitectura. La decisión debe valorar criticidad, vida útil, soporte, riesgo, coste y alternativas de modernización. Los componentes temporales necesitan responsables, documentación, monitorización y un plan de retirada.

Latencia, granularidad y dirección del flujo

Una plataforma corporativa puede trabajar con cierres diarios, mientras que OT procesa señales en segundos o milisegundos. No toda información necesita conservar su frecuencia original: el *edge* puede filtrar ruido, agregar valores o publicar cambios relevantes sin eliminar los patrones necesarios para interpretar el activo.

La dirección del flujo determina el riesgo:

- **OT hacia IT**: telemetría, estados e históricos para análisis y mantenimiento.
- **IT hacia OT**: órdenes, límites o consignas autorizadas.

- **Bidireccional**: procesos con retroalimentación continua.
- **Unidireccional**: extracción desde entornos que no admiten retorno.
- **Local**: decisiones ejecutadas sin depender de capas superiores.

Los flujos hacia OT requieren controles reforzados. Una recomendación económica o analítica puede influir en la operación, pero debe pasar por los responsables autorizados. Además, un sistema OT no debería perder funciones esenciales porque fallen una plataforma analítica, un servicio *cloud* o una comunicación corporativa.

Del intercambio de datos al valor empresarial

La convergencia genera valor cuando mejora decisiones, no cuando aumenta el volumen transferido. Sus aplicaciones incluyen:

- Mantenimiento basado en el estado real de los activos.
- Priorización de intervenciones según criticidad e impacto.
- Reducción de paradas no planificadas.
- Correlación entre rendimiento técnico y coste.
- Optimización de repuestos, recursos y desplazamientos.
- Detección de pérdidas e ineficiencias.
- Mejor coordinación entre operación, mantenimiento y planificación.

Integrar SCADA, EAM y GIS, por ejemplo, permite asociar una anomalía con el activo correcto, su historial y su ubicación. Esto acelera el diagnóstico, prepara mejor la intervención y elimina reconciliaciones manuales.

OBJETIVO	KPI ORIENTATIVO	RESULTADO ESPERADO
Ampliar visibilidad	Activos críticos con datos integrados	Menor incertidumbre
Reducir latencia	Tiempo desde el evento hasta su disponibilidad	Respuesta más rápida
Eliminar tareas manuales	Horas de extracción y conciliación	Menor coste y mayor trazabilidad
Mejorar mantenimiento	Tiempo desde detección hasta orden de trabajo	Menor indisponibilidad
Aumentar resiliencia	Funciones OT autónomas ante pérdida de IT	Continuidad operacional
Acelerar casos de uso	Tiempo para incorporar una fuente	Mayor capacidad de innovación

Los KPIs deben ser compartidos por IT, OT y las áreas beneficiarias. Integrar más activos carece de valor si los datos no son fiables; reducir la latencia no mejora la decisión si se pierde el contexto; y automatizar un proceso defectuoso puede extender sus errores.

Gobierno común y responsabilidades claras

IT aporta capacidades de arquitectura, integración y escalabilidad; OT, conocimiento del proceso físico, criticidad y restricciones operativas; mantenimiento y negocio, la perspectiva necesaria para convertir información en resultados.

La gobernanza conjunta debe cubrir:

- Priorización de casos de uso y beneficios.
- Arquitecturas, estándares y patrones reutilizables.
- Responsabilidad sobre fuentes, interfaces y modelos.
- Gestión de cambios entre dominios.
- Validación operacional, seguridad y continuidad.
- Seguimiento de KPIs y retirada de integraciones obsoletas.

La colaboración no debe diluir la responsabilidad: cada sistema necesita un propietario y las decisiones sobre activos deben permanecer bajo responsables autorizados. Los equipos multidisciplinares ayudan a contrastar desde el inicio la tecnología con las condiciones reales de uso.

La gestión del cambio debe acercar culturas diferentes. IT necesita comprender las restricciones operacionales y OT, las capacidades y riesgos de las nuevas arquitecturas. Las herramientas deben presentar a operadores, técnicos, arquitectos, responsables de negocio y equipos de seguridad únicamente el contexto necesario para actuar.

Avanzar mediante casos de uso y una arquitectura común

La convergencia progresa mejor con problemas concretos, pero cada iniciativa no debe crear su propia arquitectura. Una evolución ordenada comprende:

1. Identificar un problema con impacto medible.
2. Mapear activos, sistemas, datos y responsables.
3. Definir latencia, dirección y criticidad de los flujos.
4. Seleccionar componentes reutilizables.
5. Validar la integración en un entorno controlado.
6. Medir resultados y documentar aprendizajes.
7. Incorporar los componentes a la arquitectura común.
8. Escalar a otros activos o procesos.

La convergencia real aparece cuando IT y OT comparten una comprensión de los activos, los procesos y los resultados, manteniendo las fronteras necesarias para proteger la operación. Su avance se mide por **decisiones más completas, rápidas y fiables**, no por el número de sistemas conectados. Sobre esta base pueden crecer la inteligencia operacional, la predicción y la automatización sin sacrificar estabilidad, resiliencia ni seguridad.

5. Inteligencia operacional e IA aplicada

Evolucionar desde la monitorización y el análisis retrospectivo hacia capacidades capaces de anticipar comportamientos, decidir bajo incertidumbre y actuar dentro de límites controlados

Durante años, la analítica energética se apoyó en plataformas de *Business Intelligence* destinadas a consolidar históricos, elaborar indicadores y explicar resultados. Estas capacidades siguen siendo necesarias, pero resultan insuficientes en un sistema cada vez más distribuido, dinámico e interdependiente.

Las organizaciones necesitan conocer qué sucede, anticipar la evolución de los activos y comparar posibles actuaciones. La inteligencia operacional conecta estas capacidades con los procesos reales de decisión. Su valor no reside en detectar una anomalía o generar una previsión, sino en **reducir indisponibilidades, evitar costes, gestionar riesgos y asignar mejor los recursos**.

De describir el pasado a intervenir sobre el futuro

La inteligencia operacional representa una progresión de capacidades, exigencias y responsabilidades:

NIVEL	PREGUNTA	CAPACIDAD	EJEMPLO	PAPEL HUMANO
Descriptivo	¿Qué ocurrió?	Indicadores e históricos	Evolución del consumo	Interpretar desviaciones
Diagnóstico	¿Por qué?	Correlación y análisis causal	Relación entre parada y operación	Validar causas
Predictivo	¿Qué puede ocurrir?	*Forecasting* y detección temprana	Demanda o probabilidad de fallo	Evaluar riesgo y confianza
Prescriptivo	¿Qué conviene hacer?	Simulación y optimización	Priorizar una intervención	Comparar y autorizar
Agéntico	¿Qué puede ejecutarse?	Planificación y actuación controlada	Crear una orden de trabajo	Definir límites y excepciones

No todos los procesos deben alcanzar la máxima autonomía ni necesitan IA. Las reglas ofrecen respuestas deterministas; los modelos físicos representan activos y redes; la estadística estima relaciones e incertidumbre; el machine *learning* detecta patrones complejos; la optimización compara alternativas; y los agentes coordinan tareas y herramientas. **La solución más sencilla que resuelva el problema con robustez suele ser la adecuada**.

Conciencia situacional y mantenimiento predictivo

La conciencia situacional combina telemetría, alarmas, eventos, topología, históricos, mantenimiento y condiciones externas. Su objetivo no es mostrar más datos, sino filtrar, correlacionar y priorizar lo relevante, evitando que el exceso de señales aumente la carga cognitiva.

Las capacidades principales incluyen:

- Procesamiento continuo de eventos y series temporales.
- Correlación de señales y supresión de alarmas redundantes.
- Identificación de cambios de régimen.

- Priorización según criticidad, probabilidad e impacto.
- Presentación adaptada a cada usuario.
- Indicación expresa de datos ausentes o resultados inciertos.

En mantenimiento, los modelos basados en condición adaptan las intervenciones al estado real del activo, mientras la analítica predictiva estima su evolución. Pueden combinar variables operativas, fallos anteriores, características técnicas, condiciones ambientales, repuestos disponibles y consecuencias de una indisponibilidad.

El valor depende de la capacidad para actuar. Una alerta precisa que llega tarde puede ser menos útil que otra algo más incierta que permite preparar recursos. También debe equilibrarse el coste del error: un falso negativo oculta una degradación; demasiados falsos positivos saturan a los equipos y destruyen la confianza.

La predicción debe integrarse en el proceso: validar la alerta, asociarla al activo, consultar trabajos existentes, estimar la criticidad y convertirla, cuando proceda, en una recomendación u orden.

El *forecasting* como capacidad estructural

La predicción sustenta continuamente decisiones sobre demanda, renovables, precios, disponibilidad, consumo y restricciones. Por ello, debe gestionarse como un servicio empresarial con niveles definidos de disponibilidad, frecuencia, calidad, trazabilidad y soporte.

Una infraestructura de *forecasting* necesita datos gobernados, modelos por horizonte, ejecución programada, previsiones probabilísticas, registro de versiones, comparación con la realidad, recalibración e interfaces de distribución.

ÁMBITO	HORIZONTE	DECISIÓN ASOCIADA	EVALUACIÓN
Demanda	Minutos a años	Operación, compras y capacidad	MAE, RMSE, MAPE o WAPE
Renovables	Minutos a días	Programación y reservas	Error por horizonte y meteorología
Precios	Intradiario a medio plazo	Compra, cobertura y arbitraje	Error y rentabilidad frente a referencia
Activos	Horas a meses	Mantenimiento y capacidad	Precisión, calibración y antelación
Sistema	Años o décadas	Red e inversiones	Robustez y sensibilidad de escenarios

Ninguna métrica es universal. La evaluación debe considerar el horizonte, el tipo de serie y el impacto económico. Una pequeña mejora durante periodos de congestión, precios elevados o baja disponibilidad puede aportar más valor que una reducción mayor del error medio.

Decidir bajo incertidumbre

La demanda, la meteorología, los precios y la disponibilidad varían de forma inesperada. La IA debe ayudar a gestionar esa incertidumbre, no presentar una predicción única como certeza. Las previsiones probabilísticas, los escenarios y la optimización estocástica permiten comparar alternativas considerando restricciones, costes y riesgos.

El sistema debería mostrar:

- Escenario central y alternativas relevantes.
- Probabilidad o nivel de confianza.
- Variables que más influyen en el resultado.

- Sensibilidad ante cambios.
- Restricciones utilizadas.
- Coste o riesgo de cada alternativa.
- Condiciones que invalidarían la recomendación.

La función de la IA es ampliar la capacidad para explorar opciones y actualizar escenarios. La responsabilidad sobre decisiones de gran impacto debe permanecer asignada y contar con supervisión proporcional al riesgo.

De la recomendación a la IA agéntica

Un agente puede perseguir objetivos, consultar sistemas, elaborar planes, iniciar flujos y comprobar resultados. En mantenimiento podría detectar una degradación, revisar el historial y los repuestos y proponer una intervención. Actuar directamente sobre una infraestructura física, sin embargo, exige límites mucho más estrictos que automatizar una tarea administrativa.

NIVEL	CAPACIDAD	Ejemplo	CONTROL
0.Observación	Presenta información	Cuadro operacional	Validación de datos
1.Asistencia	Detecta y explica anomalías	Alerta enriquecida	Revisión humana
2.Recomendación	Propone alternativas	Intervención recomendada	Autorización responsable
3.Ejecución supervisada	Actúa tras aprobación	Orden de trabajo	Registro y cancelación
4.Autonomía acotada	Actúa dentro de límites	Ajuste autorizado	Guardarraíles y reversión
5.Autonomía ampliada	Coordina varias acciones	Reconfiguración dinámica	Condiciones estrictas y supervisión reforzada

En muchos procesos, la recomendación o la ejecución supervisada ofrecen el mejor equilibrio. Los agentes deben aplicar mínimo privilegio, separar análisis, autorización y ejecución, registrar sus acciones, comprobar resultados y escalar ante ambigüedad o baja confianza. También necesitan mecanismos para detenerse, revertir actuaciones y probarse antes en entornos controlados.

Objetivos, límites y comportamientos indeseados

Un optimizador actúa según los objetivos y restricciones definidos. Si son incompletos, puede encontrar una solución matemáticamente eficiente y perjudicial: reducir costes de mantenimiento aumentando el riesgo, maximizar el arbitraje acelerando la degradación de una batería o reducir consumo comprometiendo la producción.

Los objetivos deben incorporar:

- Límites físicos y de seguridad.
- Compromisos contractuales y regulatorios.
- Costes directos y consecuencias indirectas.
- Impacto sobre disponibilidad, degradación y sostenibilidad.
- Tolerancia al riesgo y condiciones de escalado humano.

Expertos de negocio y operación deben traducir la intención empresarial a funciones objetivo y restricciones verificables. La inteligencia operacional también debe hacer visibles los intercambios entre mantenimiento, disponibilidad inmediata y rentabilidad.

Industrializar mediante MLOps

Un modelo preciso en un piloto todavía no es una capacidad operacional. MLOps aporta automatización, versionado, pruebas, despliegue y observabilidad durante todo el ciclo de vida.

Debe contemplar:

- Versionado de datos, variables, código y modelos.
- Registro de experimentos y criterios de selección.
- Pruebas técnicas, estadísticas y operativas.
- Separación de desarrollo, validación y producción.
- Despliegue controlado y reversión.
- Monitorización de precisión, deriva, latencia y disponibilidad.
- Reentrenamiento, comparación *champion-challenger* y retirada de versiones.

Un modelo puede ejecutarse correctamente y haber perdido validez porque cambian los activos, los mercados o los hábitos de consumo. La monitorización debe incluir el resultado empresarial y disponer de alternativas: modelo anterior, regla conservadora, modelo físico o decisión humana.

Explicabilidad y confianza

La explicación debe aportar a cada usuario el contexto necesario para valorar el resultado. Un técnico necesita conocer qué variables activaron una alerta; un operador, las restricciones de una recomendación; un responsable de mercado, los escenarios y el riesgo; y la dirección, rendimiento, límites e incidencias.

Debe permitir responder:

- ¿Qué factores influyen en el resultado y con qué confianza?
- ¿Trabaja el modelo dentro de las condiciones validadas?
- ¿Qué alternativas y restricciones se consideraron?
- ¿Qué consecuencias tendría no actuar?
- ¿Cuándo debe intervenir una persona?

La confianza se construye comparando predicciones con resultados, mostrando errores e involucrando a los usuarios en la mejora. Ocultar las limitaciones para favorecer la adopción suele producir el efecto contrario.

Horizontes de decisión conectados

La misma infraestructura puede respaldar decisiones diferentes, pero no debe utilizar idénticos modelos y controles en todos los casos:

- **Operativo**: segundos o minutos, con prioridad en latencia, disponibilidad y límites físicos.
- **Táctico**: días o meses para optimizar mantenimiento, recursos y planificación.
- **Estratégico**: años para comparar inversiones, tecnologías y evolución de la demanda.

La operación genera evidencias sobre los activos; mantenimiento las convierte en planes; y la planificación las incorpora a las inversiones. Esta continuidad evita que una decisión inmediata perjudique la vida útil o que una estrategia de largo plazo ignore restricciones conocidas por los equipos de campo.

KPIs para medir inteligencia aplicada

El número de modelos o usuarios no demuestra valor. Los KPIs deben combinar calidad analítica, adopción, impacto empresarial y control.

ÁMBITO	KPI ANALÍTICO	KPI EMPRESARIAL	SEÑAL DE ALERTA
Forecasting	Error y calibración	Coste de desvíos	Mejora media que oculta periodos críticos
Mantenimiento	Precisión, *recall* y antelación	Disponibilidad, MTBF y MTTR	Alertas imposibles de atender
Optimización	Mejora frente a referencia	Coste evitado o ingreso adicional	Beneficio que ignora riesgo o degradación
Recomendación	Aceptación y rechazo	Tiempo y resultado de la decisión	Rechazo elevado sin analizar causas
Agentes	Éxito, excepciones y reversiones	Tiempo ahorrado y cumplimiento	Acciones fuera de política
MLOps	Deriva, latencia y actualización	Continuidad del servicio	Modelos sin propietario o validación reciente

Las métricas deben compararse con el procedimiento anterior, una regla o un modelo simple. También deben contabilizar preparación de datos, infraestructura, licencias, supervisión y mantenimiento para comprobar la sostenibilidad económica.

Organización y escalado

La inteligencia operacional requiere equipos de operación, mantenimiento, negocio, datos, arquitectura, ciberseguridad y experiencia de usuario. Cada modelo necesita propietario empresarial, responsable técnico, expertos de validación y usuarios autorizados para aceptar o rechazar recomendaciones.

El escalado debe seguir una secuencia común:

1. Seleccionar un problema con impacto y usuarios identificados.
2. Establecer una referencia y validar los datos.
3. Diseñar con expertos de dominio.
4. Integrar la salida en una decisión real.
5. Definir límites, supervisión y respaldo.
6. Medir valor, adopción, errores y costes.
7. Industrializar componentes reutilizables.
8. Extender o retirar según los resultados.

La inteligencia aplicada avanza del registro a la conciencia situacional, de la alarma a la anticipación, de la previsión a la decisión bajo incertidumbre y del piloto a una capacidad gobernada. **El propósito debe permanecer por encima de la tecnología**: los modelos han de responder a necesidades concretas, respetar restricciones físicas y proporcionar a las personas información suficiente para ejercer su responsabilidad.

6. Implicaciones para la flexibilidad del sistema eléctrico

Convertir los datos en una capacidad para coordinar generación, almacenamiento y demanda, gestionar congestiones y extraer mayor valor de los recursos energéticos disponibles

La incorporación de renovables variables, almacenamiento, electrificación y grandes consumidores aumenta los recursos que deben coordinarse y reduce la validez de algunos patrones históricos de operación.

La flexibilidad es la capacidad de modificar temporalmente la generación o el consumo, almacenar o liberar energía y adaptar el comportamiento ante una necesidad del sistema. Debe aportar una potencia, duración, velocidad de respuesta y localización determinadas. Una capacidad que no puede activarse donde y cuando se necesita posee un valor limitado.

La dimensión física tampoco basta. Es necesario conocer la capacidad, estimar su disponibilidad, comunicar una instrucción, comprobar la respuesta y valorar sus consecuencias. **El dato convierte una posibilidad técnica en un recurso identificable, coordinable y verificable**.

Una capacidad física, digital y contractual

Un activo puede modificar su comportamiento y, aun así, no estar disponible: quizá esté comprometido con otro servicio, carezca de telemetría, no disponga de activación o esté condicionado por el proceso.

NIVEL	SIGNIFICADO
Flexibilidad teórica	Capacidad física máxima del activo
Técnica	Capacidad utilizable respetando seguridad y límites operativos
Disponible	Parte no comprometida y activable en un periodo concreto
Habilitada	Capacidad integrada y autorizada para participar
Activada	Modificación solicitada al recurso
Entregada	Respuesta medida y validada

Las diferencias pueden ser importantes. Una batería puede carecer del estado de carga requerido; una industria, estar limitada por la producción; y un centro de datos, reservar su almacenamiento para continuidad. La flexibilidad debe expresarse mediante potencia, energía, duración, rampas, localización, sentido de activación y capacidad de repetición.

RECURSO	APORTACIÓN	RESTRICCIONES PRINCIPALES	DATOS NECESARIOS
Baterías	Carga, descarga y reserva	Estado, degradación y compromisos	SoC, SoH, temperatura, ciclos y precios
Industria	Reducción o desplazamiento	Producción, calidad y coste de oportunidad	Consumo, planificación y capacidad productiva
Centros de datos	Baterías, refrigeración y cargas gestionables	SLA, continuidad y respaldo	Carga IT, consumo, SoC y condiciones térmicas
Vehículos eléctricos	Modulación y posible descarga	Movilidad y hora de salida	Disponibilidad, SoC y preferencias
Recursos distribuidos	Coordinación de generación y consumo	Necesidades locales y control	Producción, demanda y punto de conexión
Generación	Modulación o reserva	Rampas y compromisos	Disponibilidad, previsiones y estado

El ciclo digital de la flexibilidad

Convertir activos distribuidos en recursos gestionables exige una cadena coordinada:

1. Inventariar activos y capacidades.
2. Observar su estado y disponibilidad.
3. Predecir generación, demanda y condiciones.
4. Calcular la flexibilidad disponible.
5. Optimizar su utilización.
6. Comunicar la activación.
7. Medir y verificar la respuesta.
8. Liquidar el servicio y actualizar los modelos.

FASE	Pregunta	Resultado
Identificación	¿Qué activos pueden responder?	Cartera de recursos
Estimación	¿Qué capacidad estará disponible?	Flexibilidad por periodo
Optimización	¿Cómo conviene utilizarla?	Estrategia de despacho
Activación	¿Qué recurso debe responder?	Instrucción trazable
Medición	¿Qué modificación se produjo?	Respuesta observada
Verificación	¿Se entregó lo comprometido?	Capacidad validada
Liquidación y aprendizaje	¿Qué valor corresponde y cómo mejorar?	Remuneración y modelos recalibrados

La interoperabilidad resulta esencial porque los activos pertenecen a fabricantes, propietarios y agregadores diferentes. Definiciones, marcas temporales y niveles de calidad deben ser compatibles en todo el ciclo.

Almacenamiento: optimizar sin ignorar la degradación

Las baterías pueden desplazar energía, reducir picos, aportar respaldo y participar en distintos servicios. Su optimización debe combinar *SoC*, SoH, temperatura, potencia, previsiones, límites de red, compromisos, degradación y riesgo.

Una oportunidad inmediata puede impedir otra posterior, y cada ciclo afecta a la vida útil. Por ello, la función objetivo debe incorporar el coste de envejecimiento, las reservas necesarias y la tolerancia al riesgo. El *revenue stacking* puede mejorar la rentabilidad, pero exige evitar que una misma capacidad se venda para servicios incompatibles.

Los resultados deben compararse con una estrategia de referencia mediante ingresos adicionales, costes evitados, reducción de picos y utilización, descontando degradación, operación y penalizaciones.

Demanda flexible y centros de datos

La demanda puede reducirse, desplazarse, modularse o incrementarse de forma controlada, pero su disponibilidad depende del proceso al que sirve. Deben considerarse consumo mínimo, velocidad y duración del cambio, recuperación, efecto rebote, coste de oportunidad e impacto sobre calidad y seguridad.

En industria, integrar datos energéticos y productivos permite conocer cuándo una carga es realmente flexible. El beneficio puede proceder de reducir picos, desplazar consumo, aprovechar autoconsumo, participar en servicios y coordinarse con almacenamiento. Los incentivos internos deben repartir el beneficio y el riesgo entre energía y producción.

Los centros de datos presentan posibilidades específicas: programar cargas no críticas, optimizar refrigeración, coordinar baterías y generación local o reducir picos. Sin embargo, **la continuidad del servicio debe prevalecer**. La reserva de respaldo, los SLA, la residencia de los datos y la latencia limitan qué cargas pueden desplazarse. La flexibilidad debe medirse por su disponibilidad real, no inferirse de la potencia contratada.

Gestionar congestiones con información locacional

La congestión aparece cuando la red no puede transportar toda la generación o demanda sin superar límites. La flexibilidad solo ayuda si se encuentra en el nodo adecuado; por ello, localización y tiempo son tan importantes como potencia.

Su gestión requiere:

- Estado y topología de la red.
- Previsiones de generación y demanda por ubicación.
- Anticipación de restricciones.
- Identificación de recursos capaces de modificar el flujo.
- Optimización bajo límites eléctricos y operativos.
- Medición del efecto sobre la congestión.

Almacenamiento, demanda flexible o cambios de configuración pueden reducir restricciones y *curtailment*. Esta capacidad mejora la utilización de la red, pero no elimina los refuerzos cuando la limitación es estructural.

Plataformas para coordinar recursos distribuidos

Las plataformas cumplen funciones complementarias:

- **EMS**: optimiza una instalación o cartera.
- **DERMS**: observa y coordina recursos distribuidos respecto a la red.
- **VPP**: agrega activos para operarlos comercialmente.
- **Plataforma de agregación**: canaliza recursos de distintos propietarios.
- **BMS**: supervisa y protege técnicamente la batería.
- **Optimizador**: calcula la estrategia según objetivos y restricciones.

Si varios sistemas influyen sobre un activo, deben existir jerarquías, arbitraje y una autoridad final. La coordinación exige una fuente autorizada para estado y disponibilidad, reserva previa de capacidad, límites locales, registro de consignas y operación degradada ante pérdida de comunicaciones. **La conectividad no resuelve por sí sola los conflictos entre objetivos**.

Medir, verificar y liquidar

Los mercados intercambian servicios energéticos, pero dependen de datos para demostrar que la capacidad existía y fue entregada. La línea base estima qué habría consumido o generado el activo sin activación; su precisión condiciona la remuneración, los incumplimientos y la confianza.

La medición debe registrar:

- Capacidad ofrecida y disponibilidad declarada.
- Momento, potencia y duración de la instrucción.
- Línea base y respuesta observada.

- Desviación respecto a la consigna y efecto rebote.
- Incidencias y causas de indisponibilidad.

La trazabilidad desde la oferta hasta la liquidación reduce disputas y mejora futuras estimaciones. Debe contemplar resolución temporal, sincronización, pérdidas de datos y condiciones excepcionales.

Horizontes, autonomía y resiliencia

La flexibilidad combina decisiones automáticas, operativas, comerciales y estratégicas:

HORIZONTE	DECISIÓN	RIESGO PRINCIPAL
Segundos o minutos	Responder a una consigna	Superar límites o responder mal
Intradiario	Reprogramar recursos	Error de previsión o doble compromiso
Diario o semanal	Planificar mantenimiento y ofertas	Perder oportunidades o degradar activos
Mensual o estacional	Reservar capacidad y contratar	Comprometer flexibilidad inexistente
Largo plazo	Evaluar inversiones	Sobredimensionar o infravalorar recursos

Una decisión comercial debe respetar restricciones operativas, y una activación inmediata, la disponibilidad posterior. Los controles locales pueden automatizarse dentro de límites; las decisiones con impacto sobre producción o vida útil pueden requerir autorización.

Flexibilidad y resiliencia no son equivalentes. La capacidad comercializable debe diferenciarse de la reserva de continuidad, la capacidad de emergencia y los márgenes de seguridad. Los activos deben conservar comportamientos seguros si se pierde la conexión con el agregador o el optimizador.

KPIs de disponibilidad, entrega y valor

La potencia instalada no determina la flexibilidad utilizable. Los indicadores deben mostrar cuánto puede activarse, cuánto se entrega y qué resultado produce.

DIMENSIÓN	KPI ORIENTATIVO	PRECAUCIÓN
Capacidad	MW teóricos, disponibles y habilitados	No confundir potencia nominal y flexibilidad
Entrega	Porcentaje de consigna cumplida	Segmentar los fallos críticos
Respuesta	Tiempo hasta alcanzar la potencia	Comprobar también la duración
Previsión	Error de disponibilidad y demanda	El promedio puede ocultar extremos
Congestión	Horas, energía y coste de restricciones	Analizar por nodo y causa
Almacenamiento	SoH, ciclos y coste de degradación	Evitar maximizar ingresos a corto plazo
Economía	Ingresos, costes evitados y margen neto	Incluir operación y penalizaciones

Los KPIs deben segmentarse por recurso, ubicación, servicio y periodo. También conviene medir la capacidad no utilizada y distinguir si la barrera es física, tecnológica, contractual u organizativa.

Organización, incentivos e inversión

Operación protege la estabilidad; mantenimiento, la salud del activo; mercados, las oportunidades; producción, sus compromisos; y tecnología, la coordinación. El modelo debe definir quién calcula, compromete y autoriza la flexibilidad, qué límites prevalecen y cómo se reparten ingresos, costes y penalizaciones.

La flexibilidad puede reducir restricciones, mejorar la infraestructura existente y aplazar ciertos refuerzos cuando la congestión es temporal, existe capacidad fiable y su coste total es menor. La inversión física seguirá siendo necesaria ante limitaciones estructurales o crecimiento sostenido de la demanda.

El reto consiste en pasar del potencial estimado a una capacidad **disponible, localizable y entregable**. Cuando activos, datos, plataformas, contratos e incentivos se coordinan, la flexibilidad genera ingresos y costes evitados para las organizaciones y contribuye a integrar renovables, gestionar congestiones y reforzar la eficiencia, la competitividad y la sostenibilidad del sistema eléctrico.

7. Nuevas fuentes de información para una observabilidad ampliada del sistema energético

Incorporar datos geoespaciales, remotos y multimodales para conocer el estado de los activos, comprender su entorno y priorizar decisiones de inspección, mantenimiento y gestión del riesgo

Los sistemas SCADA, sensores de campo y aplicaciones corporativas permiten conocer el comportamiento interno de los activos, pero ofrecen una visión limitada de su entorno físico y territorial. Vegetación, movimientos del terreno, inundaciones, incendios, obras próximas o cambios de uso del suelo pueden afectar a la seguridad y disponibilidad sin aparecer inicialmente en la telemetría.

Satélites, drones, LiDAR, cámaras térmicas y sensores multiespectrales amplían esta visión. Su valor no consiste en generar más imágenes, sino en **detectar cambios, priorizar inspecciones y relacionar los activos con las condiciones del territorio**. Una anomalía solo resulta útil cuando se vincula al activo correcto, se evalúa según su criticidad y se transforma en una actuación verificable.

Del activo aislado al activo en su entorno

Una línea puede funcionar dentro de parámetros normales mientras la vegetación invade su corredor; un gasoducto, quedar expuesto a movimientos del terreno; y una planta fotovoltaica, mantener su producción agregada mientras algunos módulos presentan defectos localizados.

La observabilidad ampliada incorpora información sobre vegetación, construcciones, deformaciones, erosión, inundabilidad, anomalías térmicas, accesos, servidumbres, meteorología y cobertura del suelo. Estas fuentes complementan la monitorización operacional: los datos internos describen cómo se comporta el activo; los externos ayudan a comprender qué factores pueden alterar ese comportamiento.

Elegir la fuente según la decisión

Cada tecnología presenta ventajas y límites de cobertura, resolución, frecuencia, coste y condiciones de captura.

FUENTE	CAPACIDAD	VENTAJA	APLICACIONES
Satélite óptico	Imagen visible y multiespectral	Gran cobertura y revisitas	Vegetación, usos del suelo y cambios territoriales
Radar SAR	Deformaciones y estructura	Opera de noche y atraviesa nubes	Movimientos del terreno e inundaciones
Dron RGB	Imagen dirigida de alta resolución	Flexibilidad y detalle	Inspección visual y documentación
Termografía	Patrones térmicos	Localiza puntos calientes	Equipos eléctricos y plantas fotovoltaicas
LiDAR	Geometría tridimensional	Precisión espacial	Distancias, vegetación y topografía
Sensores espectrales	Caracterización de materiales	Diferencia superficies	Vegetación e indicios de emisiones
IoT móvil	Medición próxima y recurrente	Continuidad y rapidez	Condiciones ambientales y estado local

La pregunta operacional debe preceder a la tecnología. Para detectar cambios sobre miles de kilómetros importan cobertura y frecuencia; para evaluar una anomalía concreta, un dron o LiDAR pueden aportar mayor detalle. Una estrategia escalonada combina vigilancia amplia, selección de áreas de riesgo e inspección dirigida.

Resolución, precisión y oportunidad

La calidad no depende únicamente del tamaño del píxel. Debe considerar:

- Resolución espacial, temporal, espectral y radiométrica.
- Precisión posicional y cobertura real.
- Tiempo entre captura y disponibilidad para decidir.
- Condiciones atmosféricas, iluminación y ángulo de observación.
- Calibración y comparabilidad entre capturas.

Una imagen detallada puede llegar demasiado tarde; una fuente frecuente puede no distinguir el objeto relevante; y una captura térmica puede resultar incomparable bajo condiciones ambientales diferentes. La organización debe definir primero **el umbral de detección y la ventana de actuación**.

También debe diferenciar precisión visual y métrica. Reconocer un objeto no implica poder medir distancias o deformaciones con exactitud suficiente. Cuando la decisión depende de una magnitud física, la metodología y la calibración son tan importantes como el sensor.

Casos de uso vinculados a decisiones

Adquirir imágenes sin usuario, umbral ni actuación genera repositorios costosos y poco utilizados. Cada caso debe conectar la fuente con una decisión.

CASO	FUENTES	DECISIÓN HABILITADA	BENEFICIO
Vegetación en corredores	Satélite, LiDAR, dron y GIS	Priorizar podas	Menor riesgo y mejor uso de cuadrillas
Obras y ocupaciones	Imagen y cartografía	Revisar servidumbres	Detección temprana
Movimientos del terreno	SAR, LiDAR y sensores	Inspeccionar activos expuestos	Anticipación geotécnica
Líneas eléctricas	Dron, termografía y LiDAR	Generar inspección	Mayor cobertura y menor coste
Plantas fotovoltaicas	Termografía e imagen	Priorizar módulos	Recuperación de rendimiento
Infraestructuras lineales	Satélite, dron y datos territoriales	Revisar tramos	Gestión de activos dispersos
Riesgo de incendio	Vegetación y meteorología	Reforzar vigilancia	Mantenimiento preventivo

La fuente remota suele identificar un indicio, no cerrar el proceso. El hallazgo puede requerir otra captura, revisión experta o inspección presencial. La observabilidad ampliada ayuda a decidir **dónde mirar, cuándo actuar y con qué prioridad**.

Combinar fuentes y reducir puntos ciegos

La imagen óptica muestra apariencia; el radar, estructura y deformaciones; LiDAR, geometría; la termografía, patrones térmicos; y la telemetría, comportamiento interno. Su combinación permite confirmar anomalías, reducir falsos positivos, relacionar territorio y operación y mantener observación cuando una fuente no está disponible.

La fusión exige gestionar escalas, frecuencias, coordenadas y momentos de captura. Diferencias estacionales o geométricas pueden parecer anomalías. Por ello, deben conservarse los metadatos y el dato original para verificar resultados y distinguir lo capturado de lo derivado.

De la imagen al producto de información

Los usuarios necesitan objetos, cambios, distancias, zonas de riesgo e indicadores asociados a activos concretos, no grandes archivos de imágenes. La industrialización debe crear productos como mapas de vegetación, capas de deformación, activos con anomalías térmicas o tramos priorizados.

Cada producto debe indicar:

- Fuente, fecha, cobertura y activos observados.
- Resolución, precisión y método de procesamiento.
- Hallazgos, confianza y limitaciones.
- Frecuencia de actualización y responsable.
- Proceso y decisión a los que se destina.

Este enfoque reduce la carga de revisión y evita que cada proyecto procese las mismas capturas para obtener resultados similares.

Integración con GIS, EAM y operación

Mantener los hallazgos en una plataforma aislada dificulta que se conviertan en actuaciones. El GIS relaciona activo, territorio y topología; el EAM aporta historial, órdenes y criticidad; y las plataformas operacionales incorporan estado y comportamiento.

ETAPA	PROCESO	CONTROL	SALIDA
Captura	Imagen o medición	Cobertura, calibración y fecha	Dato identificable
Preprocesamiento	Corrección y georreferenciación	Coordenadas y precisión	Dato comparable
Análisis	Detección o medición	Modelo, umbral y validación	Anomalía candidata
Contextualización	Asociación con activos	Identificador y relación espacial	Hallazgo vinculado
Priorización	Evaluación de impacto	Reglas y conocimiento experto	Actuaciones ordenadas
Integración	Envío a GIS, EAM o APM	Trazabilidad y duplicados	Tarea, alerta u orden
Verificación	Revisión remota o presencial	Evidencia y responsable	Confirmación o descarte
Cierre	Registro del resultado	Estado, fecha y causa	Aprendizaje

El flujo debe ser bidireccional: la inspección y la intervención regresan a la plataforma para medir precisión, ajustar umbrales y reducir falsas alarmas.

Industrializar captura, procesamiento e IA

Pasar del piloto a un servicio recurrente exige definir cobertura, frecuencia, niveles de servicio y responsabilidades. La captura puede combinar vigilancia periódica, activación por eventos e inspecciones detalladas en zonas prioritarias. La automatización debe asumir descarga, procesamiento e integración, reservando la revisión humana para excepciones relevantes.

La calidad geoespacial debe controlar coordenadas, georreferenciación, resoluciones, condiciones ambientales, calibración, oclusiones, cobertura y transformaciones. Los umbrales dependen de la decisión: localizar aproximadamente un cambio no exige la misma precisión que medir una distancia de seguridad.

La IA puede segmentar vegetación, detectar objetos, clasificar anomalías, identificar patrones térmicos y comparar fechas. Su rendimiento debe evaluarse por clases, estaciones, terrenos y sensores. Una precisión media elevada puede ocultar fallos en categorías poco frecuentes pero críticas.

Los casos de alta confianza pueden automatizarse; los ambiguos deben revisarse. En decisiones de mayor impacto será necesaria una segunda fuente o validación humana. La inspección remota reduce desplazamientos rutinarios, pero no sustituye todas las comprobaciones de campo.

KPIs de cobertura, precisión y valor

El número de imágenes, vuelos o terabytes no demuestra una mejora. Los indicadores deben conectar observación, detección, actuación y resultado.

DIMENSIÓN	KPI	PRECAUCIÓN
Cobertura	Activos o kilómetros observados	No garantiza resolución suficiente
Frecuencia	Tiempo entre observaciones	Mayor frecuencia puede no justificar el coste
Oportunidad	Tiempo desde captura hasta hallazgo	Medir hasta su disponibilidad operativa
Precisión	Precision, recall y falsos positivos	Segmentar por clase crítica
Posicionamiento	Error respecto al activo	La exigencia depende del caso
Verificación	Hallazgos confirmados y descartados	Registrar ambos resultados
Conversión	Hallazgos que generan actuación	Más órdenes pueden indicar exceso de alertas
Eficiencia	Coste por anomalía confirmada	Comparar con el método anterior

También deben medirse falsos negativos, reducción de inspecciones no dirigidas, tiempo hasta la resolución y reutilización del producto en distintos procesos. La fuente facilita la decisión, pero el resultado depende de la capacidad para intervenir.

Organización y capacidad continua

La observabilidad ampliada conecta GIS, operación, mantenimiento, ingeniería, medioambiente, seguridad, datos y contratación. La organización debe definir quién selecciona fuentes y activos, valida la captura, interpreta hallazgos, genera intervenciones, mantiene los productos y evalúa su retorno.

Los contratos deben fijar cobertura, frecuencia, precisión, formatos, tiempos, derechos de uso y mecanismos de corrección. Los profesionales necesitan competencias geoespaciales y comprensión de la incertidumbre; los especialistas en teledetección, conocimiento de los activos y procesos.

El objetivo es evolucionar desde proyectos de captura hacia **una capacidad de observación continua integrada en la gestión de activos**. Cuando las fuentes remotas se combinan con telemetría, GIS y conocimiento experto, la organización reduce puntos ciegos, anticipa riesgos y concentra sus recursos donde aportan mayor valor, reforzando la eficiencia, la competitividad y la sostenibilidad.

8. Soberanía tecnológica y seguridad de la cadena de suministro

Identificar, gestionar y reducir dependencias críticas para mantener el control sobre las tecnologías, servicios y datos que sustentan la operación energética

La transformación digital ha incrementado la dependencia de fabricantes, operadores *cloud*, integradores y proveedores de comunicaciones. Esta colaboración aporta escala y velocidad, pero desplaza hacia terceros funciones que sostienen la operación.

El riesgo aparece cuando una tecnología esencial se desconoce, carece de alternativas o impide mantener la actividad si el servicio desaparece.

La soberanía tecnológica tampoco equivale a autosuficiencia ni a elegir automáticamente una determinada procedencia. Representa la **capacidad para decidir, supervisar elementos críticos, conservar los datos y reaccionar ante escenarios adversos** sin quedar completamente condicionados por un tercero.

La dependencia como riesgo estructural

Un servicio puede apoyarse en *cloud*, *software*, identidades, comunicaciones y equipos de distintas empresas. Estas dependencias acumuladas pueden crear una elevada barrera de salida.

DEPENDENCIA	EJEMPLO	RIESGO PRINCIPAL	PREGUNTA DE CONTROL
Tecnológica	Plataforma o protocolo propietario	Difícil sustitución	¿Puede cambiarse sin rediseñar el proceso?
Operacional	Administración externalizada	Incapacidad para operar sin el proveedor	¿Qué funciones permanecen internamente?
De datos	Formatos o repositorios controlados	Pérdida de acceso o contexto	¿Puede recuperarse información utilizable?
Cloud	Servicios PaaS o APIs nativas	Complejidad de reversión	¿Qué componentes son portables?
Hardware	Repuestos o firmware específicos	Obsolescencia y escasez	¿Existen alternativa y soporte?
Conocimiento	Configuración conocida por terceros	Incapacidad para mantener o recuperar	¿Hay documentación y competencias?
Contractual	Licencias y condiciones variables	Incremento de costes o restricciones	¿Existe capacidad real de salida?
Concentración	Varias funciones en un proveedor	Fallo común	¿Qué operación depende del mismo actor?
Subcontratación	Proveedores indirectos desconocidos	Riesgo fuera de la visibilidad	¿Quién interviene realmente?

La evaluación debe reconstruir la cadena completa. Proveedores diferentes pueden depender de la misma nube, identidad o librería; la diversificación aparente no siempre aporta resiliencia.

Mapear desde el proceso hasta el componente

El análisis debe comenzar por el negocio y avanzar hacia la tecnología:

1. Identificar procesos y servicios esenciales.
2. Determinar qué aplicaciones y plataformas los soportan.
3. Mapear infraestructura, comunicaciones, identidades y datos.
4. Identificar proveedores y subproveedores relevantes.
5. Localizar componentes sin alternativa o con soporte limitado.
6. Evaluar las capacidades conservadas internamente.
7. Estimar impacto, coste y tiempo de sustitución.

El mapa debe incluir propietarios, función, datos, accesos, ubicaciones, licencias, fin de vida, alternativas y contingencias. Debe actualizarse cuando cambien la infraestructura o el servicio.

Criticidad, sustituibilidad y control

No todas las dependencias requieren el mismo tratamiento. La prioridad debe concentrarse en funciones esenciales con pocas alternativas o elevado impacto.

CRITERIO	RIESGO ELEVADO CUANDO…	RESPUESTA POSIBLE
Impacto	Se pierde observabilidad o capacidad operativa	Redundancia y operación degradada
Sustituibilidad	Migrar exige años o rediseño	Portabilidad, estándares y plan de salida
Tolerancia	La interrupción admisible es mínima	Respaldo y SLA reforzados
Control	La administración depende del proveedor	Accesos propios, auditoría y documentación
Concentración	Un fallo afecta a varios procesos	Diversificación selectiva y aislamiento
Conocimiento	Las competencias residen fuera	Formación y transferencia
Portabilidad	El dato solo sirve en la plataforma	Exportación y pruebas de reutilización
Ciclo de vida	El fin de soporte está próximo	Renovación, stock y transición

El tiempo de sustitución es decisivo. Puede haber alternativas en el mercado y persistir una dependencia crítica si migrar datos, interfaces y usuarios requiere un plazo incompatible con el negocio.

La respuesta tampoco consiste en duplicarlo todo. Varios proveedores aumentan costes, complejidad y superficie de exposición. La diversificación debe responder a un riesgo identificado y ser sostenible operativamente.

Control y portabilidad del dato

La ubicación geográfica de la información es relevante, pero no determina por sí sola el control. Este depende también de quién administra la plataforma y las claves, qué subproveedores intervienen, cómo se exportan los datos y qué sucede con las copias tras finalizar el contrato.

La portabilidad no consiste en descargar ficheros: debe preservar estructura, significado, trazabilidad, relaciones e históricos. Una exportación sin modelos ni configuración puede ser técnicamente completa y operacionalmente inútil.

Las pruebas de salida deben recuperar una muestra representativa, reconstruirla y utilizarla fuera de la plataforma. También deben comprobar qué funciones continuarían disponibles si fallan el portal, la API o el plano de administración del proveedor.

Cloud: escala con capacidad de reversión

Cloud aporta elasticidad, rapidez y capacidades avanzadas. El riesgo surge cuando la arquitectura ignora concentración, reversibilidad y dependencia de servicios propietarios.

Conviene distinguir infraestructura portable, servicios gestionados, funciones nativas y grandes volúmenes de datos. Multirregión protege frente a fallos localizados; *multicloud* puede reducir concentración, pero también duplicar costes y conocimientos.

El plan de reversibilidad debe definir:

- Datos, configuraciones e interfaces que deben extraerse.
- Componentes que necesitan reconstruirse.
- Aplicaciones vinculadas a servicios propietarios.
- Volumen, tiempo y coste de transferencia.
- Capacidades necesarias para ejecutar la transición.
- Mantenimiento del servicio durante la migración.

Un documento no probado ofrece confianza limitada. La organización debe ejecutar exportaciones, restauraciones o migraciones controladas y decidir conscientemente dónde acepta dependencia a cambio de valor.

Software, hardware y conocimiento

Las aplicaciones incorporan componentes de terceros. Su gestión requiere inventario —mediante SBOM cuando proceda—, procedencia, verificación, control de vulnerabilidades, soporte, pruebas y capacidad de retroceso.

En OT, una actualización legítima puede provocar indisponibilidad. Las versiones deben probarse en entornos controlados o activos menos críticos, con capacidad para detener el despliegue y recuperar una configuración conocida.

El hardware presenta otra escala temporal. Equipos energéticos operan durante décadas, mientras sus componentes digitales pueden quedar sin soporte antes. Las estrategias incluyen:

- Stock de repuestos basado en criticidad y plazo de suministro.
- Homologación de alternativas compatibles.
- Sustitución antes del fin de soporte.
- Conservación de firmware, herramientas y configuraciones.
- Verificación de procedencia y autenticidad.

El conocimiento puede constituir la dependencia menos visible. Ser propietario de equipos y datos no garantiza capacidad para operar sin el proveedor. La transferencia debe incluir configuración, código, interfaces, recuperación y decisiones arquitectónicas. La autonomía no exige internalizar todas las tareas, sino **conservar capacidad para gobernarlas, supervisarlas y recuperar funciones prioritarias**.

Contratos orientados a continuidad y salida

Los contratos deben reflejar la criticidad real del servicio:

ÁMBITO	ELEMENTOS NECESARIOS	RIESGO REDUCIDO
Nivel de servicio	Disponibilidad, soporte y prioridades	Respuesta insuficiente
Incidentes	Plazos, evidencias y cooperación	Descoordinación
Subcontratación	Notificación y aprobación	Dependencias desconocidas
Datos	Propiedad, ubicación, formatos y eliminación	Pérdida de control
Cambios	Comunicación, pruebas y aprobación	Alteraciones unilaterales
Ciclo de vida	Soporte y fin de producto	Obsolescencia no planificada
Continuidad	RTO, RPO y pruebas	Recuperación insuficiente
Reversibilidad	Exportación, asistencia, plazos y costes	Bloqueo tecnológico
Transferencia	Documentación, código y formación	Dependencia del conocimiento externo

Los derechos deben ser ejercitables. La auditoría no debe limitarse a informes genéricos y la portabilidad necesita formatos y tiempos concretos. En desarrollos críticos puede custodiarse código o configuración.

Seguimiento de proveedores y operación degradada

NIS2 incorpora la cadena de suministro a la gestión del riesgo. La evaluación debe considerar gobierno, vulnerabilidades, continuidad, subcontratación, concentración e incidentes, con seguimiento durante todo el contrato.

La organización también debe prepararse para perder temporalmente un proveedor sin que exista un ciberataque. La operación degradada debe establecer:

- Funciones que pueden continuar y durante cuánto tiempo.
- Datos, credenciales y licencias disponibles localmente.
- Tareas que requieren conocimiento externo.
- Servicios prioritarios y riesgos adicionales.
- Criterios para regresar a la normalidad.

Estas capacidades deben probarse: una exportación puede ser demasiado lenta, una licencia de emergencia haber caducado o el procedimiento depender de alguien que ya no está disponible.

Estándares abiertos e IA externa

Los estándares abiertos facilitan interoperabilidad y alternativas, pero las extensiones propietarias o la falta de competencias pueden mantener barreras. El código abierto tampoco garantiza soberanía: puede depender de una comunidad pequeña o carecer de mantenimiento. El criterio es la capacidad efectiva para utilizar, mantener y sustituir la tecnología.

La IA introduce dependencias sobre modelos, APIs, plataformas de entrenamiento y procesamiento. Deben evaluarse la portabilidad de datos, variables, instrucciones y pruebas; los cambios de versión; la disponibilidad de alternativas; el acceso a registros; el coste de inferencia y el tratamiento de información confidencial.

Desacoplar la lógica empresarial del modelo, utilizar capas de abstracción y conservar conjuntos de evaluación reduce el coste de sustitución y evita que el conocimiento del proceso quede encerrado en un servicio externo.

KPIs de dependencia y reacción

El número de proveedores evaluados no refleja el nivel de riesgo. Los indicadores deben medir visibilidad, concentración, sustituibilidad y preparación.

DIMENSIÓN	KPI	SEÑAL DE ALERTA
Inventario	Servicios críticos con dependencias mapeadas	Procesos esenciales sin mapa
Concentración	Funciones críticas por proveedor	Un actor sostiene varias capacidades
Sustituibilidad	Tiempo estimado de migración	Alternativa no desplegable a tiempo
Reversibilidad	Planes de salida probados	Documentación sin pruebas
Portabilidad	Exportación y reutilización de datos	Información que no puede reconstruirse
Ciclo de vida	Activos próximos al fin de soporte	Ausencia de renovación o repuestos
Conocimiento	Perfiles capacitados por función	Competencia concentrada fuera
Continuidad	Tiempo de operación sin proveedor	Dependencia inmediata

Reducir el riesgo no siempre implica eliminar dependencias. Puede significar mejorar visibilidad, contratos, conocimiento y capacidad demostrada de reacción.

Gobierno durante todo el ciclo de vida

Negocio, IT, OT, ciberseguridad, compras, riesgos, asesoría jurídica y finanzas deben participar desde la adquisición hasta la retirada. El ciclo comprende requisitos de control, evaluación de dependencia, contratación, transferencia, monitorización, pruebas de salida y migración final.

El coste de transición debe incorporarse al coste total de propiedad. Una solución barata durante la operación puede resultar más cara si exige una migración compleja.

La soberanía tecnológica exige **control demostrable**: dependencias identificadas, datos recuperables, proveedores supervisados, conocimiento conservado, planes de salida viables y operación degradada probada. Así puede aprovecharse la innovación sin ceder irreversiblemente procesos esenciales, reforzando la resiliencia, la competitividad y la sostenibilidad.

9. Datos sintéticos y honestidad algorítmica

Garantizar la confiabilidad de los sistemas de inteligencia artificial en un contexto donde los datos pueden ser observados, inferidos, reconstruidos o generados

Los modelos actuales pueden completar valores, simular escenarios y producir datos no observados. Esto permite trabajar con activos nuevos o fallos raros, pero puede ocultar la frontera entre evidencia, estimación y generación.

La confianza exige conocer las transformaciones, qué parte fue inferida y qué incertidumbre acompaña al resultado. Una representación convincente puede contener detalles nunca capturados.

La **honestidad algorítmica** es la obligación de presentar cada resultado según su naturaleza real, haciendo visibles su procedencia, confianza, limitaciones y condiciones de validez.

Distinguir observación, transformación e inferencia

Si todas las clases de información se almacenan y presentan igual, una estimación puede interpretarse como medición o un dato sintético como evidencia.

TIPO	ORIGEN	EJEMPLO	IDENTIFICACIÓN NECESARIA
Observada	Captura directa	Temperatura medida	Fuente, fecha, calibración y calidad
Derivada	Cálculo determinista	Potencia calculada	Entradas, fórmula y versión
Agregada	Combinación temporal o espacial	Consumo horario	Ventana y tratamiento de ausencias
Imputada	Sustitución de un valor ausente	Lectura interpolada	Método y confianza
Inferida	Resultado probabilístico	Probabilidad de fallo	Modelo, variables y validación
Simulada	Modelo físico o digital	Respuesta ante un escenario	Parámetros y supuestos
Sintética	Generación estadística o mediante IA	Serie artificial de fallos	Generador, distribución y finalidad
Reconstruida	Estimación de información ausente	Imagen completada	Áreas reconstruidas y método
Generada	Creación de contenido nuevo	Configuración propuesta	Modelo, instrucciones, fuentes y revisión

La clasificación debe acompañar al dato durante todo su ciclo. Si una serie imputada entrena un modelo, esa condición debe conservarse. El linaje remontará el resultado hasta las observaciones, supuestos y modelos.

Por qué utilizar datos sintéticos

Los fallos críticos son poco frecuentes; los activos nuevos carecen de históricos; y algunos eventos extremos no pueden reproducirse sin comprometer la seguridad. Los datos sintéticos pueden apoyar:

- Entrenamiento inicial de activos nuevos.
- Representación de fallos raros y estados extremos.
- Evaluación de detectores de anomalías.
- Pruebas antes de acceder a producción.
- Ampliación de clases poco representadas.
- Simulación de degradaciones y ejercicios de formación.
- Generación de perfiles preservando determinadas características.

Estas muestras representan hipótesis, no evidencia. El modelo aprenderá aquello que el generador considera posible y heredará sus omisiones y sesgos.

Pueden obtenerse mediante simuladores físicos, modelos estadísticos, modelos generativos o enfoques híbridos. La elección debe considerar el fenómeno, los datos reales disponibles, el conocimiento físico, la necesidad de interpretación, el coste de validación y las consecuencias de utilizar escenarios irreales. **No debe emplearse un generador complejo cuando una solución sencilla ofrece mayor control**.

Los datos sintéticos no sustituyen a los reales

La similitud visual o estadística no garantiza que una muestra reproduzca las relaciones relevantes. El *domain gap* puede aparecer porque el simulador simplifica el sistema, no representa extremos o queda desactualizado.

Entre los riesgos se encuentran:

- Combinaciones físicamente imposibles.
- Distribuciones demasiado suaves o sin extremos.
- Repetición de patrones y pérdida de diversidad.
- Correlaciones plausibles, pero inexistentes.
- Amplificación de sesgos originales.
- Etiquetas perfectas alejadas de la ambigüedad real.

Estos problemas se ocultan si entrenamiento y evaluación comparten generador. El rendimiento debe comprobarse sobre observaciones reales independientes y limitar la proporción sintética para evitar aprender sus particularidades.

Validar desde la plausibilidad hasta la utilidad

La validación necesita varios niveles complementarios:

NIVEL	PREGUNTA	MÉTODO	ACEPTACIÓN
Física	¿Respeta leyes y límites?	Reglas, balances y simulación	Sin estados imposibles
Estadística	¿Reproduce relaciones relevantes?	Distribuciones, correlaciones y extremos	Similitud suficiente
Diversidad	¿Cubre escenarios sin repetir?	Cobertura y análisis de modos	Variabilidad adecuada
Analítica	¿Mejora la tarea prevista?	Ablación y comparación	Mejora sin deteriorar otras clases
Generalización	¿Funciona sobre datos reales?	Validación externa y temporal	Rendimiento consistente
Operacional	¿Mejora una decisión?	Piloto frente al proceso anterior	Beneficio medible y riesgo aceptable
Robustez	¿Resiste cambios?	Ruido y escenarios extremos	Degradación conocida
Privacidad	¿Evita reproducir registros?	Similitud y reidentificación	Riesgo dentro de límites

Los expertos deben validar la plausibilidad física. Las pruebas compararán datos reales, reales más sintéticos y solo sintéticos, segmentando por clases, condiciones y activos. Así se distingue información útil de simple volumen.

La paradoja de los eventos raros

Los datos sintéticos son especialmente atractivos para representar fallos raros, precisamente aquellos con menor evidencia para validar el generador. El conocimiento experto y los modelos físicos pueden descartar estados imposibles, pero las muestras deben tratarse como hipótesis de trabajo.

En problemas desbalanceados, la exactitud global engaña. Deben evaluarse recall, precisión de alertas, falsos negativos y positivos, antelación y calibración. Perder un fallo crítico puede ser mucho más grave que investigar una falsa alarma, aunque demasiadas alertas saturan al equipo.

Reconstrucción algorítmica y artefactos

La superresolución generativa estima detalles a partir de patrones aprendidos. Puede producir bordes, texturas u objetos que el sensor no registró, sugerir una grieta inexistente o suavizar una anomalía real. **La calidad visual no equivale a veracidad**.

Los controles deben incluir:

- Conservación y presentación paralela del original.
- Identificación de las áreas reconstruidas.
- Registro del modelo y los parámetros.
- Prohibición de medir sobre píxeles generados cuando no exista validación.
- Confirmación mediante otra fuente y revisión humana.
- Limitación a los usos expresamente autorizados.

Los artefactos también aparecen en series, texto y redes: oscilaciones inexistentes, picos eliminados, explicaciones sin fuentes o topologías imposibles. Cada modalidad necesita controles y usos permitidos. Una serie imputada puede servir para análisis agregados, pero no para reconstruir una incidencia.

Incertidumbre y capacidad de abstención

Un sistema puede producir una respuesta aunque trabaje fuera de condiciones conocidas. Debe distinguirse entre **incertidumbre aleatoria**, inherente al fenómeno, e **incertidumbre epistémica**, derivada de información insuficiente o condiciones no representadas.

El sistema debe identificar valores fuera de rango, nuevos activos, escenarios ambientales desconocidos, pérdida de sensores y desacuerdo entre modelos. La salida debe incorporar confianza, intervalos o una advertencia de que el caso está fuera de distribución.

Si la incertidumbre supera los límites, el modelo debe abstenerse, solicitar datos o transferir la decisión. Reconocer que no existe evidencia suficiente puede ser más seguro que responder siempre con una elevada precisión media.

Un contrato de información con el usuario

Cada resultado relevante debería indicar:

- Naturaleza: observada, derivada, inferida o generada.
- Fuentes, fecha y condiciones de los datos.
- Modelo, versión y transformaciones.
- Confianza e incertidumbre.
- Ámbito validado y limitaciones.
- Necesidad de confirmación y responsable.

La información debe adaptarse al perfil: el operador necesita una explicación accionable; el auditor, trazabilidad; el científico de datos, versiones y métricas; y el directivo, riesgos y límites. La transparencia consiste en proporcionar el contexto necesario para decidir, no en mostrar todos los parámetros.

Las interfaces tampoco deben ocultar incertidumbre. Colores, puntuaciones e imágenes pueden transmitir más certeza de la existente. El usuario debe distinguir claramente **evidencia, estimación y recomendación**.

Supervisión proporcional al impacto

Revisar humanamente cada salida puede eliminar el beneficio de la automatización. La intervención debe ajustarse al impacto, la reversibilidad y la incertidumbre.

IMPACTO	USO DEL RESULTADO	SUPERVISIÓN
Bajo	Imputación para análisis exploratorio	Revisión por muestreo
Moderado	Priorización de inspecciones	Validación de casos relevantes
Alto	Propuesta de orden de mantenimiento	Confirmación responsable
Muy alto	Modificación acotada de un activo	Autorización y controles independientes
Crítico o irreversible	Información de apoyo	Decisión humana y fuentes adicionales

La persona necesita información, tiempo y autoridad reales. Deben evitarse el sesgo de automatización —aceptar por proceder de un sistema— y la aversión algorítmica —rechazar por un error aislado—. Formación y experiencia ayudan a construir una confianza calibrada.

Auditoría del dato, el modelo y la decisión

La auditoría debe reconstruir el objetivo, los datos, su validación, las versiones del modelo, la confianza comunicada, la decisión, la actuación y el resultado observado.

Los registros deben ser proporcionales al impacto. Fichas de datos, documentación del generador, tarjetas de modelo, informes de validación, historial de recomendaciones y motivos de rechazo proporcionan evidencia para explicar y revisar decisiones. Esta documentación debe actualizarse cuando cambien los datos, modelos o usos.

KPIs de confiabilidad y control

El volumen sintético o la sofisticación del modelo no son indicadores de éxito.

DIMENSIÓN	KPI	SEÑAL DE ALERTA
Procedencia	Datos etiquetados por origen	Mezcla sin identificación
Composición	Proporción real y sintética	Predominio sintético sin validación
Fidelidad física	Violaciones de reglas	Muestras imposibles
Cobertura	Escenarios y clases representados	Más volumen sin más diversidad
Generalización	Diferencia entre sintético y real	Degradación en producción
Calibración	Confianza frente a frecuencia real	Seguridad elevada al equivocarse
Artefactos	Hallazgos atribuibles al procesamiento	Decisiones basadas en elementos generados
Abstención	Casos fuera de distribución escalados	Respuesta ante cualquier entrada
Supervisión	Correcciones y anulaciones humanas	Aceptación o rechazo sistemáticos
Impacto	Errores, fallos omitidos y costes	Mejora estadística sin valor operacional

Los indicadores deben segmentarse por clase, activo y condiciones. Las responsabilidades deben abarcar aprobación del uso sintético, validación del generador, usos permitidos, etiquetado, aceptación en producción, supervisión e investigación de errores.

La adopción responsable exige conservar la procedencia, validar sobre observaciones reales, incorporar restricciones físicas, comunicar incertidumbre, permitir la abstención y auditar las actuaciones. **La confianza no procede de asumir que el modelo siempre acierta, sino de saber cuándo sus resultados son sólidos, cuándo presentan límites y cómo comprobarlos**.

10. Infraestructuras digitales para un sistema energético más competitivo y escalable

Convertir los datos en una capacidad estructural para integrar nuevos consumos, acelerar inversiones y gestionar la creciente complejidad de la transición energética

La electrificación, los centros de datos, la movilidad, el almacenamiento y las renovables aumentan las exigencias sobre las redes. El crecimiento depende de la infraestructura física, pero también de la información, los modelos y la coordinación.

Puede existir margen técnico sin aprovechar por falta de visibilidad o datos compatibles. Las capacidades digitales permiten anticipar restricciones y comparar alternativas. **No crean capacidad física donde no existe**, pero ayudan a utilizarla mejor y orientar inversiones.

La escalabilidad como desafío conjunto

El crecimiento puede quedar limitado por cuellos de botella físicos, informacionales y organizativos.

CUELLO DE BOTELLA	MANIFESTACIÓN	CONTRIBUCIÓN DIGITAL	LÍMITE PERSISTENTE
Capacidad física	Líneas o subestaciones insuficientes	Mejor utilización y planificación	Puede exigir nuevos activos
Observabilidad	Margen real desconocido	Telemetría y modelos actualizados	Depende de la calidad del dato
Información	Fuentes dispersas o incompatibles	Integración y estándares	Requiere permisos y responsables
Análisis	Estudios lentos	Simulación y automatización	Las decisiones complejas exigen expertos
Coordinación	Múltiples agentes	Flujos compartidos y trazabilidad	Persisten intereses diferentes
Tramitación	Revisiones y documentos sucesivos	Expedientes y validaciones digitales	No elimina requisitos legales
Inversión	Incertidumbre sobre demanda y retorno	Escenarios y sensibilidad	El futuro continúa siendo incierto

Digitalizar reduce errores y tiempos, pero no sustituye evaluaciones, autorizaciones ni refuerzos. La escalabilidad exige que **activos físicos, procesos e información evolucionen coordinadamente**.

Esta convergencia articula la *Twin Transition*. Renovables, almacenamiento y demanda flexible requieren observabilidad, previsiones, simulación y trazabilidad. El reto es crecer sin multiplicar costes, complejidad y riesgos.

Nuevos consumos, perfiles diferentes

La electrificación añade perfiles con localizaciones, horarios y flexibilidad diferentes. Evaluar solo la potencia máxima puede distorsionar su impacto.

ACTIVIDAD	CARACTERÍSTICAS	INFORMACIÓN NECESARIA	POSIBLE APORTACIÓN
Centros de datos	Continuidad y crecimiento modular	Potencia, rampas, redundancia y carga prevista	Gestión controlada y baterías
Industria electrificada	Dependencia del proceso	Producción, horarios y calidad de suministro	Modulación compatible
Movilidad eléctrica	Demanda distribuida	Conexión, SoC, movilidad y potencia	Carga inteligente y agregación
Climatización	Inercia térmica	Temperatura, confort y demanda	Desplazamiento temporal
Electrolizadores	Consumo intensivo	Precio, renovables y compromisos	Modulación productiva
Almacenamiento	Consumo e inyección	SoC, SoH, potencia y duración	Picos y flexibilidad
Comunidades energéticas	Flujos locales	Generación, consumo y excedentes	Coordinación local

Dos proyectos con igual potencia pueden afectar de forma diferente. La planificación debe incorporar perfiles horarios, rampas, simultaneidad, crecimiento, almacenamiento y capacidad de respuesta.

Visibilidad sobre la capacidad disponible

La capacidad de conexión depende de topología, demanda, generación, indisponibilidades y criterios de seguridad. Una cifra agregada puede ocultar restricciones que aparecen únicamente durante ciertas horas.

Una visión dinámica combina modelos de red, históricos, proyectos comprometidos, escenarios y contingencias. Los mapas de capacidad deben indicar fecha, hipótesis, compromisos y limitaciones. **Una estimación no debe presentarse como garantía**.

La transparencia debe equilibrarse con la protección de información sensible. Es posible orientar decisiones sin exponer configuraciones críticas, siempre que los datos de activos, topología y estado mantengan suficiente calidad.

El dato como acelerador de proyectos

Los proyectos atraviesan evaluación, conexión, autorización y construcción. Parte de los retrasos es inevitable; otra procede de expedientes incompletos y versiones contradictorias.

FASE	CAPACIDAD DIGITAL	RESULTADO ESPERADO
Selección	Mapas y análisis geoespacial	Evitar ubicaciones poco viables
Solicitud	Formularios y validación automática	Menos errores y requerimientos
Estudio	Simulación y modelos comunes	Evaluaciones comparables
Coordinación	Expediente compartido y trazabilidad	Menos intercambios y versiones
Autorización	Integración documental	Visibilidad sobre el estado
Construcción	Monitorización de hitos	Anticipación de desviaciones
Puesta en servicio	Pruebas y actualización de activos	Incorporación coherente a operación
Explotación	Observabilidad e indicadores	Verificación del caso de negocio

La automatización debe centrarse en comprobaciones, consistencia y seguimiento. El juicio técnico permanece bajo profesionales autorizados. La métrica relevante es **el tiempo y la incertidumbre desde la propuesta hasta la operación**.

Compartir datos sin perder control

Los distintos agentes poseen partes de la realidad. Deben acordar qué compartir, con qué granularidad, quién accede, cuál es la fuente autorizada y qué responsabilidades asume cada participante.

APIs y espacios de datos facilitan el intercambio, pero no sustituyen semántica y gobierno. Debe compartirse lo necesario para el propósito autorizado, protegiendo la confidencialidad.

La interoperabilidad reduce el coste de incorporar agentes. Si cada relación requiere una integración específica, la complejidad crece con el número de participantes; los estándares y mecanismos reutilizables permiten escalar.

Planificar mediante escenarios

Demanda, costes y ritmos tecnológicos pueden desviarse de la previsión. La planificación debe explorar grados de electrificación, almacenamiento y flexibilidad, además de retrasos y condiciones extremas.

El objetivo no es adivinar un futuro exacto, sino identificar:

- Refuerzos necesarios en la mayoría de los escenarios.
- Inversiones desplegables por fases.
- Soluciones flexibles durante transiciones.
- Nodos expuestos a congestión recurrente.
- Riesgos de activos infrautilizados.
- Decisiones robustas frente a hipótesis diferentes.

La infraestructura digital permite actualizar escenarios con nuevos datos y conectar planificación y operación mediante aprendizaje continuo.

Extraer valor de los activos existentes

Parte del crecimiento puede absorberse utilizando mejor la infraestructura, sin operar siempre cerca de sus límites. Los datos ayudan a detectar pérdidas, ajustar mantenimiento, anticipar congestiones y priorizar refuerzos.

La utilización debe evaluarse junto al riesgo y la vida útil. Aumentarla puede generar valor y acelerar la degradación. La flexibilidad puede aplazar inversiones o actuar como solución transitoria, pero no sustituye un refuerzo cuando la restricción es estructural.

Infraestructuras digitales diseñadas para escalar

El ecosistema digital no debe convertirse en un nuevo cuello de botella. Una arquitectura escalable aplica:

- Modularidad y desacoplamiento.
- Interoperabilidad técnica y semántica.
- Procesamiento distribuido entre *edge*, centros de datos y *cloud*.
- Observabilidad y automatización de plataformas.
- Seguridad y resiliencia desde el diseño.
- Portabilidad y reversibilidad.
- Gestión eficiente del ciclo de vida del dato.

Cada plataforma añade licencias, integraciones y dependencias. Conviene reutilizar capacidades y retirar soluciones sin valor.

Caso de negocio, regulación y organización

Las inversiones digitales reducen tareas, mejoran mantenimiento y aceleran estudios. Su caso de negocio debe incluir tecnología, datos, formación y dependencia, junto con ahorros, ingresos, CAPEX mejor dimensionado y tiempo de puesta en servicio.

El **valor de opción** resulta especialmente relevante: mejores datos permiten posponer una decisión irreversible, invertir por fases o cambiar de estrategia con menor coste. La financiación y la regulación deben reconocer que estas capacidades sostienen activos físicos y producen valor en varias áreas.

La regulación debe aportar seguridad jurídica, transparencia, interoperabilidad y supervisión. La colaboración público-privada permite desarrollar estándares y probar soluciones antes de escalarlas.

La organización debe conectar planificación, operación, mercados, tecnología y finanzas. Indicadores compartidos evitan acelerar conexiones sin capacidad o maximizar utilización reduciendo resiliencia.

KPIs de competitividad y escalabilidad

El volumen de datos, APIs o modelos desplegados no demuestra impacto.

DIMENSIÓN	KPI	PRECAUCIÓN
Conexión	Plazos de conexión	Segmentar por complejidad y causa
Desarrollo	Tiempo hasta puesta en servicio	Incluye factores externos
Capacidad	MW de demanda y generación integrados	Considerar seguridad y calidad
Utilización	Factor de uso y margen disponible	Mayor uso puede reducir resiliencia
Congestión	Horas, energía y coste de restricciones	Analizar por ubicación
Renovables	MWh de *curtailment*	Depende también del mercado
Flexibilidad	MW disponibles y entregados	Incorporar duración
Inversión	CAPEX evitado o dimensionado	Aplazar no siempre ahorra
Información	Tiempo para evaluar escenarios	La rapidez no debe reducir calidad
Plataformas	Disponibilidad y coste por activo	Incluir operación y dependencia
Sostenibilidad	Consumo de la infraestructura digital	Relacionarlo con el valor generado

Los indicadores necesitan línea base y atribución prudente. Deben servir para identificar cuellos de botella, priorizar inversiones, revisar procesos y retirar iniciativas ineficaces.

Escalar con eficiencia y una hoja de ruta

Sensores e IA aumentan el procesamiento. La sostenibilidad digital exige capturar con la frecuencia necesaria, aplicar retención según valor, evitar duplicidades, medir el consumo y retirar servicios obsoletos.

Una hoja de ruta integrada comprende:

1. Priorizar procesos, activos y decisiones.
2. Evaluar datos, integración, seguridad y dependencias.
3. Seleccionar casos con impacto y línea base.
4. Construir componentes reutilizables.
5. Integrarlos en los procesos reales.
6. Medir resultados técnicos y empresariales.
7. Desarrollar competencias e incentivos.
8. Escalar y revisar arquitectura, costes y sostenibilidad.

Los casos de uso demuestran valor; las plataformas comunes permiten escalarlo; y la gobernanza evita multiplicar riesgos.

De la infraestructura digital al desarrollo económico

Un sistema energético competitivo necesita energía disponible, asequible, fiable y sostenible, además de información para conocer dónde existe capacidad, anticipar inversiones y coordinar nuevos recursos.

La infraestructura digital es parte estructural del sistema energético y debe avanzar junto a redes, generación, almacenamiento y demanda, integrando tecnología, regulación y capacidades humanas.

El reto es convertirla en **más proyectos integrados, mejores decisiones, mayor utilización de los activos y menor incertidumbre**. Cuando los datos reducen tiempos, costes y riesgos, dejan de ser un recurso interno y se convierten en un habilitador de eficiencia, competitividad y sostenibilidad para el conjunto del sistema energético.

Resultados esperados

La aplicación del decálogo debe traducirse en cambios observables: datos más confiables, mayor coordinación entre IT y OT, operaciones digitales más resilientes, inteligencia artificial aplicada con garantías y una mejor capacidad para anticipar restricciones y responder a las necesidades del sistema energético. El resultado buscado es una organización capaz de **gobernar y utilizar el dato como una infraestructura crítica sin comprometer la seguridad, la continuidad ni el control sobre sus decisiones**.

El avance dependerá del punto de partida, la criticidad de los activos y el grado de digitalización de cada organización. Aun así, pueden identificarse resultados comunes que deberían hacerse visibles cuando las recomendaciones se incorporen a la estrategia, la arquitectura, la contratación, la operación y la planificación energética.

Datos gobernados, confiables y preparados para su reutilización

La organización deberá conocer qué datos resultan críticos, dónde se originan, cómo se transforman y qué decisiones dependen de ellos. Esta visibilidad permitirá superar la fragmentación entre sistemas y proyectos, reducir discrepancias y conservar el significado de la información durante todo su ciclo de vida.

Esto deberá reflejarse en:

- **Clasificación de los datos según su criticidad, sensibilidad, temporalidad y uso previsto**, evitando aplicar los mismos controles a toda la información.
- Responsables definidos para dominios, conjuntos de datos, modelos e interfaces relevantes.
- Catálogos que documenten origen, linaje, transformaciones, calidad, permisos y consumidores.
- Identificadores y modelos comunes para relacionar activos físicos, ubicaciones, eventos y variables operativas.

- Reglas de calidad adaptadas a cada uso, con umbrales, alertas y procedimientos de corrección.
- Control de versiones y conservación de la información necesaria para reconstruir decisiones e incidencias.
- Políticas de retención, archivo y retirada basadas en valor, riesgo y obligaciones aplicables.
- Indicadores que permitan medir disponibilidad, completitud, puntualidad, consistencia y adecuación al propósito.

La gobernanza no deberá convertirse en una capa burocrática separada de la operación. Su valor será visible cuando reduzca reconciliaciones manuales, acelere la incorporación de nuevas fuentes y permita reutilizar información con menor coste y mayor confianza.

El dato confiable no será necesariamente perfecto. La organización deberá conocer sus límites y determinar para qué decisiones resulta suficiente, qué controles adicionales necesita y cuándo debe recurrirse a una fuente alternativa o a una validación humana.

Convergencia IT/OT más segura, resiliente y soberana

La integración entre sistemas corporativos y operacionales deberá facilitar el intercambio de información sin eliminar las diferencias de criticidad, disponibilidad y tiempos de respuesta propias de cada entorno. La organización contará con una visión común de activos, flujos y dependencias, manteniendo límites técnicos y responsabilidades claramente definidos.

Los resultados esperados incluyen:

- **Inventarios relacionados de activos IT, OT, aplicaciones, datos, comunicaciones y proveedores**, actualizados conforme evoluciona la infraestructura.
- Arquitecturas de integración controladas, con interfaces documentadas y reducción progresiva de conexiones punto a punto.
- Segmentación de redes y separación de funciones según criticidad y necesidad operacional.
- Identidades diferenciadas, privilegios mínimos y control reforzado de accesos remotos y cuentas técnicas.
- Detección temprana de anomalías mediante información contextual procedente de los entornos IT y OT.
- Procedimientos coordinados de respuesta ante incidentes, con funciones y escalados previamente definidos.
- Copias, redundancias, modos degradados y mecanismos de recuperación probados en condiciones realistas.
- Contratos que contemplen seguridad, soporte, actualización, notificación de incidentes, portabilidad y salida.
- Identificación de dependencias concentradas en tecnologías, servicios, componentes o especialistas difícilmente sustituibles.

El cumplimiento de NIS2 y de otras obligaciones constituirá una referencia mínima, no el resultado final. La mejora será efectiva cuando la organización pueda mantener los servicios esenciales, recuperar capacidades dentro de los tiempos previstos y tomar decisiones informadas ante una interrupción tecnológica o de suministro.

La soberanía no requerirá desarrollar internamente todos los componentes. Se traducirá en **capacidad para conocer, elegir y sustituir dependencias**, conservar acceso a los datos y mantener alternativas proporcionadas a la criticidad de cada servicio.

Inteligencia operacional confiable, explicable y centrada en las personas

La analítica y la inteligencia artificial deberán mejorar decisiones concretas sobre operación, mantenimiento, planificación y gestión energética. Cada modelo tendrá un propósito definido, una línea de base y criterios que permitan comprobar si su utilización produce un resultado mejor que el procedimiento anterior.

La evolución deberá observarse en:

- **Casos de uso vinculados a decisiones y resultados operativos verificables**, evitando desarrollar modelos sin integración en los procesos reales.
- Previsiones de demanda, generación, capacidad o degradación evaluadas por escenarios y segmentos relevantes.
- Reducción de tiempos de detección y diagnóstico mediante correlación de eventos y análisis contextual.
- Mantenimiento predictivo orientado a anticipar fallos sin generar un volumen inasumible de falsas alarmas.
- Modelos contrastados con restricciones físicas, conocimiento experto y observaciones reales no utilizadas durante su desarrollo.
- Detección de entradas fuera de distribución, degradación del rendimiento y cambios en las condiciones operativas.
- Resultados acompañados de niveles de confianza, limitaciones y mecanismos de abstención.
- Registro de datos, versiones, recomendaciones, decisiones, actuaciones y resultados posteriores.
- Supervisión humana proporcional al impacto, la incertidumbre y la reversibilidad de cada actuación.

La organización deberá distinguir con claridad entre información observada, derivada, inferida, reconstruida y sintética. Las interfaces y los informes no presentarán como evidencia directa aquello que haya sido generado o completado por un algoritmo. Las reconstrucciones conservarán acceso a la fuente original y los datos sintéticos se validarán sobre observaciones reales antes de utilizarse en decisiones relevantes.

Los equipos de operación y los expertos de dominio participarán en la definición, validación y seguimiento de los modelos. Su función evolucionará hacia la interpretación de excepciones, la revisión de hipótesis y el control de automatizaciones. La responsabilidad permanecerá identificada incluso cuando una parte del proceso se ejecute de forma automática.

La automatización avanzará gradualmente desde la recomendación y el modo sombra hasta actuaciones acotadas y reversibles. Las decisiones de mayor impacto mantendrán confirmación humana, protecciones independientes y capacidad efectiva de detener o revertir la actuación.

Mayor observabilidad y capacidad para gestionar la flexibilidad

La combinación de telemetría convencional con información meteorológica, geoespacial, de mercado, movilidad, satélites, drones y otros sistemas permitirá construir una visión más completa del estado de activos, redes y territorios. Cada fuente deberá evaluarse por su precisión, frecuencia, cobertura, disponibilidad y adecuación al uso.

Entre los resultados esperados se encuentran:

- **Mayor visibilidad sobre el estado, la capacidad y las restricciones del sistema**, reduciendo zonas o periodos con información insuficiente.
- Integración de fuentes heterogéneas mediante referencias temporales, espaciales y semánticas compatibles.

- Previsiones más precisas de demanda, generación renovable, congestión y disponibilidad de recursos.
- Detección anticipada de anomalías, cambios ambientales, degradaciones e impactos sobre infraestructuras.
- Estimaciones de capacidad que indiquen fecha, hipótesis, condiciones y márgenes de incertidumbre.
- Caracterización realista de la flexibilidad disponible, incluyendo potencia, duración, tiempo de respuesta, recuperación y efecto rebote.
- Coordinación de almacenamiento, demanda flexible y generación distribuida dentro de límites técnicos y comerciales.
- Evaluación de alternativas operativas y de inversión mediante escenarios, sensibilidades y contingencias.
- Confirmación mediante fuentes independientes cuando una decisión presente consecuencias elevadas o irreversibles.

La flexibilidad dejará de medirse únicamente por la potencia teórica de los recursos. La organización conocerá qué capacidad puede activarse realmente, durante cuánto tiempo, bajo qué condiciones y con qué efecto sobre la operación posterior.

Las nuevas fuentes no sustituirán de forma automática a la instrumentación existente. El resultado será una **observabilidad ampliada y verificable**, en la que cada fuente aporte valor conocido y mantenga mecanismos de contraste, continuidad y actualización.

Infraestructuras digitales escalables y orientadas al valor del sistema

Las plataformas deberán permitir incorporar activos, fuentes, usuarios y casos de uso sin multiplicar proporcionalmente las integraciones, los costes y los riesgos. La organización evolucionará desde soluciones aisladas hacia componentes comunes, interoperables y reutilizables, manteniendo capacidad para sustituirlos cuando dejen de responder a sus necesidades.

Esto permitirá:

- **Reducir el tiempo y el coste necesarios para integrar nuevas fuentes, activos y aplicaciones**.
- Reutilizar servicios de identidad, calidad, catálogo, intercambio, observabilidad y seguridad.
- Sustituir progresivamente integraciones específicas por interfaces y modelos de información comunes.
- Distribuir el procesamiento entre OT, edge, centros de datos y nube según latencia, criticidad, coste y soberanía.
- Conocer el rendimiento, la disponibilidad, el consumo y el coste de las plataformas por activo o servicio integrado.
- Retirar repositorios, interfaces, licencias y modelos que hayan dejado de aportar valor.
- Evaluar inversiones digitales mediante coste total, riesgo, dependencia y beneficio operacional.
- Priorizar refuerzos físicos y digitales mediante escenarios actualizados de demanda, generación y capacidad.
- Acelerar estudios, conexiones y proyectos mediante información estructurada, trazable y reutilizable.
- Medir la contribución digital a la utilización de activos, la reducción de restricciones y el tiempo de puesta en servicio.

La infraestructura digital deberá gestionarse también con criterios de eficiencia. La captura, conservación y procesamiento de información responderán a una necesidad conocida, evitando frecuencias innecesarias, duplicidades y cargas analíticas sin consumidores. El consumo digital se relacionará con el valor generado para la operación y el sistema energético.

La modernización seguirá una hoja de ruta por capacidades y resultados. Las actuaciones de bajo arrepentimiento —inventariar, documentar dependencias, mejorar la calidad, reforzar recuperación o preparar interfaces— permitirán avanzar con independencia de la evolución futura. Las inversiones de mayor alcance se desplegarán por fases y con criterios definidos de validación, ampliación o retirada.

En conjunto, el avance será visible cuando la organización pueda demostrar que conoce y protege mejor sus datos, integra IT y OT con mayor seguridad, recupera sus capacidades ante incidentes, utiliza la inteligencia artificial con honestidad y aprovecha nuevas fuentes para anticipar restricciones y coordinar recursos. El resultado esperado es una infraestructura del dato **gobernada, confiable, resiliente y escalable**, capaz de transformar la información en eficiencia, competitividad, seguridad y sostenibilidad para el sistema energético.

Anexo: Marcos normativos, certificaciones y *frameworks* de referencia

- **Directiva NIS2 – Directiva (UE) 2022/2555**. Establece obligaciones de gestión del riesgo cibernético, responsabilidad directiva, seguridad de la cadena de suministro y notificación de incidentes para entidades esenciales e importantes, incluidas las del sector energético.
- **Directiva CER – Directiva (UE) 2022/2557**. Define un marco para reforzar la resiliencia física y organizativa de las entidades críticas mediante evaluaciones de riesgo, medidas preventivas, continuidad y comunicación de incidentes.
- **Código de red europeo sobre ciberseguridad – Reglamento Delegado (UE) 2024/1366**. Introduce reglas sectoriales para la ciberseguridad de los flujos eléctricos transfronterizos, incluyendo requisitos mínimos, evaluación de riesgos, monitorización, notificación y gestión de crisis.
- **Cyber Resilience Act – Reglamento (UE) 2024/2847**. Establece requisitos de ciberseguridad durante todo el ciclo de vida de los productos con elementos digitales, desde su diseño y comercialización hasta la gestión de vulnerabilidades y actualizaciones.
- **Data Act – Reglamento (UE) 2023/2854**. Regula el acceso y uso de los datos generados por productos conectados y servicios relacionados, además de impulsar la interoperabilidad y el cambio entre proveedores de procesamiento de datos.
- **Reglamento Europeo de Inteligencia Artificial – Reglamento (UE) 2024/1689**. Aplica un enfoque basado en riesgo e impone requisitos de gobierno, calidad del dato, documentación, supervisión humana y seguimiento para determinados sistemas de IA vinculados a infraestructuras críticas.
- **Reglamento General de Protección de Datos – Reglamento (UE) 2016/679**. Establece los principios y obligaciones aplicables al tratamiento de datos personales, relevantes para información de clientes, medición inteligente, movilidad, empleados y otros conjuntos utilizados por el sector energético.
- **ISO/IEC 27001:2022 e ISO/IEC 27019:2024**. La primera permite implantar y certificar un sistema de gestión de seguridad de la información, mientras que la segunda adapta los controles a la generación, transporte, almacenamiento y distribución de energía.
- **Serie ISA/IEC 62443**. Proporciona requisitos y modelos para proteger los sistemas de automatización y control industrial durante su ciclo de vida, asignando responsabilidades a operadores, integradores, proveedores y fabricantes.
- **ISO 22301:2019**. Norma certificable para establecer un sistema de gestión de continuidad de negocio que permita prepararse, responder y recuperar servicios ante interrupciones.
- **ISO/IEC 42001:2023**. Norma certificable para gobernar el desarrollo y uso responsable de sistemas de inteligencia artificial mediante políticas, responsabilidades, evaluación de impactos, gestión de riesgos y mejora continua.
- **ISO 8000-61:2016**. Define un modelo de referencia de procesos para gestionar la calidad del dato y evaluar la capacidad y madurez de la organización en esta materia.
- **IEC 61850 e IEC 62351**. Estas familias proporcionan modelos de información y comunicaciones interoperables para la automatización eléctrica, junto con mecanismos de seguridad para los protocolos e intercambios utilizados por los sistemas energéticos.
- **NIST Cybersecurity Framework 2.0**. Ofrece una estructura flexible para gobernar, identificar, proteger, detectar, responder y recuperar frente al riesgo cibernético, adaptable al tamaño, madurez y criticidad de cada organización.
- **DAMA-DMBOK**. Marco de referencia para organizar la gestión del dato mediante disciplinas como gobierno, arquitectura, modelado, calidad, metadatos, datos maestros, integración y ciclo de vida.

Informes El Reto 2026

Cinco perspectivas sobre energía, inteligencia y decisiones

En 2026, la expansión de la IA y de la capacidad de cómputo coincide con la electrificación de la industria y la movilidad, la integración de renovables y almacenamiento y la llegada de grandes consumidores a redes que también deben atender la demanda existente. La potencia disponible y los plazos de conexión condicionan proyectos digitales e industriales. La crisis de suministro vinculada al estrecho de Ormuz vuelve a situar la seguridad energética y la exposición geopolítica en primer plano; los riesgos ciberfísicos amplían las exigencias de continuidad en servicios cada vez más digitalizados.

Para enerTIC.org, que cumple quince años, esta coyuntura confirma la necesidad de analizar conjuntamente la transición energética y digital. Una nueva carga de IA exige decisiones sobre arquitectura, potencia, refrigeración y gobierno del dato; su suministro requiere previsiones y capacidad de red; su valor depende después de cómo se utilice para operar activos, mejorar procesos industriales o prestar servicios urbanos. Las compañías energéticas y *utilities* están en el centro de esta relación, junto con los grandes consumidores y los territorios que intervienen en la demanda.

Una relación de doble sentido

La infraestructura digital necesita electricidad y una gestión responsable de su energía y refrigeración. Al mismo tiempo, el sistema energético necesita infraestructura digital para observar activos dispersos, anticipar congestiones y coordinar generación, almacenamiento y demanda. Los informes de CPDs y Energía IT abordan ambos lados de este vínculo; el de Energía OT lo traslada a funciones físicas que deben mantenerse incluso cuando falla una conexión o un proveedor.

El resultado se comprueba fuera de la plataforma

Un caso de IA industrial necesita datos de energía y producción con significado común, acceso seguro a OT y una decisión sobre cuándo consumir electricidad. Una plataforma urbana requiere capacidades semejantes a otra escala, además de responsables, mantenimiento y presupuesto para prestar el servicio. Por eso la colección relaciona consumo por tarea útil, capacidad de red, energía por unidad producida, continuidad de los activos y calidad de los servicios urbanos.

La pregunta que comparten los cinco informes es qué información, capacidades y decisiones permiten mejorar un resultado sin trasladar costes o riesgos a otra parte del sistema.

Infraestructuras IT · El regreso del CPD corporativo

El primer informe parte de una decisión que ya no es puramente tecnológica: dónde procesar cada carga y qué control conservar sobre datos, modelos y conocimiento generado. Propone elegir entre CPD propio, *colocation*, *edge* y nube híbrida según sensibilidad, latencia, coste y continuidad. La IA privada y las factorías de conocimiento pueden aprovechar información corporativa si existe gobierno de sus usos, trazabilidad y capacidad de trasladar el servicio o cambiar de proveedor.

Las nuevas cargas elevan la densidad de potencia, el tráfico interno y las necesidades térmicas. El decálogo plantea diseñar conjuntamente computación, red, almacenamiento y refrigeración híbrida; medir también el consumo por trabajo útil; y modernizar el parque instalado por fases. Examina además cuándo un CPD puede desplazar cargas, utilizar almacenamiento o participar en la flexibilidad del sistema eléctrico sin poner en riesgo la continuidad.

Energía IT · El dato como infraestructura crítica

El segundo informe estudia la dependencia inversa: generación, redes, almacenamiento y nuevos consumos precisan información para planificar, operar y coordinarse. Plantea identificar los datos esenciales, conocer su origen y sus transformaciones, asignar responsables y preservar la calidad con criterios ajustados a cada decisión. La interoperabilidad IT/OT debe conservar el significado de cada activo y señal, además de proteger los límites de seguridad de la operación.

Sobre esa base, la analítica y la IA pueden anticipar demanda, congestiones e incidencias, evaluar capacidad de conexión y estimar flexibilidad realmente disponible. El informe incorpora observabilidad ampliada, ciberresiliencia, soberanía tecnológica y una distinción necesaria entre datos observados, inferidos y sintéticos para no presentar incertidumbre como certeza operacional.

La conexión es concreta: el operador del CPD necesita potencia y condiciones de red verificables; la *utility* necesita previsiones fiables de la nueva demanda digital y conocer qué cargas pueden ser flexibles, dónde y durante cuánto tiempo.

Energía OT · Inteligencia sobre activos físicos

Este decálogo parte de redes, plantas, refinerías, instalaciones gasistas y otros activos de larga vida donde una recomendación puede afectar a personas, equipos y continuidad. Propone mapear funciones críticas y modernizar sistemas heredados mediante instrumentación, virtualización y cambios reversibles. El mantenimiento predictivo y prescriptivo, la simulación y el *edge* aportan contexto y respuesta cerca del activo; su autonomía debe ajustarse a límites físicos, calidad del dato y capacidad humana para intervenir. Los *smart meters* abren nuevas opciones de gestión de la demanda con beneficios que han de verificarse.

Industria · Energía, productividad y retorno

El informe industrial vincula la IA a casos con retorno y al rediseño de procesos. Un consumo aislado dice poco: debe relacionarse con producto, receta, estado de la línea y unidades válidas para conocer su efecto sobre coste, calidad y EBITDA. La integración IT/OT y la modernización selectiva de planta permiten actuar sin comprometer producción. Autoconsumo, almacenamiento y flexibilidad se dimensionan según perfiles y restricciones reales; la ciberseguridad y el control del know-how protegen el conocimiento que diferencia a la empresa.

Smart Cities · Datos útiles y capacidad de sostener servicios

El informe urbano identifica una brecha entre sensores y plataformas desplegados y decisiones que mejoran la ciudad. Exige calidad y contexto del dato, una Oficina del Dato con responsabilidades, interoperabilidad y espacios de confianza para coordinar energía, agua, movilidad, edificios y otros servicios. La ciudad de energía Net Zero incorpora generación local y flexibilidad; cada proyecto necesita además mantenimiento, presupuesto operativo y una hoja de ruta proporcionada a la madurez municipal.

Industria y territorios forman parte de la demanda que Energía IT debe prever y Energía OT debe poder gestionar. Su flexibilidad solo es útil cuando se conoce su localización, sus límites de proceso y su disponibilidad real; la infraestructura digital debe aportar esos datos sin añadir dependencias difíciles de sostener.

La colección completa

Cinco decálogos independientes y complementarios, elaborados desde los Comités de Expertos de enerTIC.org.



Infraestructuras IT:
Cargas IA · potencia · soberanía



Energía IT:
Dato crítico · red · flexibilidad



Energía OT:
Activos · edge · continuidad



Industria:
Proceso · energía · retorno



Smart Cities:
Dato fiable · servicios · territorio

Acerca de enerTIC

2011–2026 · 15 años impulsando la eficiencia energética desde la tecnología

La Plataforma enerTIC.org reúne a empresas, profesionales e instituciones para desarrollar el potencial de las tecnologías digitales en la mejora de la eficiencia energética. Su misión relaciona esa mejora con la sostenibilidad, la resiliencia y la competitividad: tres objetivos que hoy deben abordarse de forma conjunta en las decisiones sobre infraestructuras, operaciones e inversión.

En 2026, esa misión adquiere una dimensión concreta. La electrificación incrementa las exigencias sobre las redes; la expansión de la inteligencia artificial y los centros de datos añade nuevas demandas de energía y capacidad; y la incertidumbre geopolítica obliga a prestar más atención a la seguridad de suministro y a la continuidad de los servicios. Sensores, analítica, automatización o gemelos digitales pueden ayudar a responder, pero su utilidad depende de la calidad de los datos, de su integración con los sistemas existentes y de resultados que puedan medirse.

enerTIC trabaja en el punto de encuentro entre esas necesidades y las soluciones disponibles. El Consejo Consultivo aporta una visión estratégica; la Red de Colaboración Institucional amplía el diálogo; y cinco Comités de Expertos examinan los retos de los centros de datos, las infraestructuras IT y las operaciones del sector energético, la industria y los territorios inteligentes. Ese trabajo toma forma en informes, casos de uso y encuentros donde se contrastan experiencias y se identifican oportunidades de colaboración. El Smart Energy Congress reúne cada año esas perspectivas en una conversación común.

El 15° aniversario invita a mirar hacia la siguiente etapa. La eficiencia de un centro de datos depende también de su acceso a la energía; una red más inteligente necesita coordinar IT y OT; y una industria o una ciudad capaces de gestionar mejor su demanda pueden contribuir a un sistema más flexible. enerTIC impulsa esa visión conectada para que la digitalización se traduzca en decisiones verificables sobre consumo, emisiones, seguridad operativa y retorno de la inversión.

Empresa asociadas

