Informe “El Reto” enerTIC

Comité de Expertos de Innovación para la eficiencia en Operaciones del Sector Energético

10 claves para digitalizar los activos energéticos con IA sin comprometer la seguridad, la eficiencia ni la continuidad operativa



Septiembre 2026

Sumario

Resumen ejecutivo..... 3

Reconocimientos..... 5

Identificación del reto por el Comité de Expertos..... 6

DECALOGO

1. Diseño estratégico resiliente y soberano..... 7

2. Modernización y digitalización de activos legacy..... 9

3. Virtualización de la infraestructura física crítica..... 13

4. IA para el mantenimiento predictivo y prescriptivo en el mundo físico..... 16

5. Simulación y optimización de escenarios para la toma de decisiones..... 20

6. Computación e inteligencia artificial on-edge..... 25

7. Explotación integral de smart meters..... 29

8. Seguridad y responsabilidad del Consejo (NIS2)..... 34

9. Protección del «eslabón más débil» de la cadena..... 38

10.Convergencia cultural IT-OT y rediseño operativo mediante business cases sólidos..43

Resultados esperados..... 48

Anexo: Marcos normativos, certificaciones y *frameworks* de referencia..... 52

Informes El Reto 2026..... 53

Acerca de enerTIC..... 56

Resumen ejecutivo

El informe plantea una prioridad central: **digitalizar los activos energéticos para mejorar la capacidad de anticipar y decidir, preservando la seguridad, la eficiencia y la continuidad operativa**. Esto exige conocer las funciones críticas, modernizar de forma proporcionada la infraestructura existente y definir qué decisiones pueden apoyarse o ejecutarse mediante tecnología, bajo qué límites y con qué responsabilidad humana.

El decálogo plantea cinco prioridades de actuación:

- **Diseñar para la resiliencia y modernizar con criterio**. Cada organización debe identificar qué funciones necesita preservar durante una incidencia, de qué activos y proveedores dependen y cómo operará en condiciones degradadas. El inventario y la clasificación del parque instalado permiten decidir qué conservar, proteger, instrumentar, virtualizar o sustituir. Las funciones digitales pueden evolucionar a un ritmo distinto del hardware físico siempre que se validen su comportamiento, disponibilidad y reversibilidad.
- **Convertir la información operativa en decisiones mejores**. El mantenimiento predictivo permite anticipar degradaciones; el prescriptivo compara intervenciones según riesgo, recursos y consecuencias para la operación. La simulación y la optimización ayudan a evaluar escenarios y asignar capacidad limitada entre objetivos que pueden entrar en conflicto. Los modelos deben utilizar datos contextualizados, representar la incertidumbre y ofrecer recomendaciones comprensibles dentro del tiempo disponible para actuar.
- **Distribuir la inteligencia y activar el potencial de la demanda**. La computación *on-edge* acerca determinadas capacidades al activo para reducir latencias y conservar autonomía cuando falla la conectividad. Los contadores inteligentes pueden aportar una visión más precisa del consumo y facilitar ahorro, autoconsumo y flexibilidad. Para generar valor, la medida debe conectarse con sistemas de actuación, preferencias del usuario y mecanismos que verifiquen y distribuyan el beneficio obtenido.
- **Gobernar el riesgo ciberfísico en toda la cadena**. La mayor conectividad exige proteger funciones operativas, contener incidentes y demostrar capacidad de recuperación. NIS2 refuerza el papel de los órganos de dirección en la supervisión del riesgo. Fabricantes, integradores, mantenedores, proveedores y pymes forman parte del perímetro real de la infraestructura; sus requisitos deben ajustarse a la criticidad de la función que desempeñan y comprobarse mediante evidencias y ejercicios conjuntos.
- **Rediseñar los procesos mediante la convergencia IT-OT**. Integrar sistemas aporta valor cuando reduce el tiempo necesario para comprender una situación, comparar alternativas, autorizar una actuación y verificar su resultado. IT y OT deben compartir objetivos, responsabilidades y criterios de cambio. Cada iniciativa necesita un business case construido alrededor de la decisión que mejora, con indicadores de adopción, resultados operativos y costes durante todo su ciclo de vida.

Estas prioridades deben aplicarse según la criticidad de los activos y la madurez de cada organización. En algunos casos, el primer avance será completar inventarios, documentar dependencias, controlar accesos o probar la recuperación. En otros, resultará viable desplegar modelos prescriptivos, virtualizar funciones seleccionadas, coordinar recursos distribuidos o incorporar mayor autonomía local. **La progresión debe apoyarse en capacidades verificadas antes de ampliar el alcance o la automatización**.

El criterio para iniciar cada proyecto es **identificar la función o decisión que se quiere mejorar, establecer una línea de base y determinar qué datos, personas, sistemas y controles necesita**. Después podrán elegirse la arquitectura y el grado de automati-

zación adecuados. El resultado deberá comprobarse en términos de tiempo de decisión, disponibilidad, utilización de activos, riesgo, coste y valor generado.

La finalidad del decálogo es que redes, plantas y cadenas de valor energéticas puedan evolucionar sin perder el control sobre su operación. Una digitalización guiada por decisiones y resultados permitirá aprovechar mejor los activos existentes, responder con mayor rapidez a las incidencias y avanzar en **eficiencia, competitividad, resiliencia, soberanía y sostenibilidad**.

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 Operaciones del Sector Energético

Presidente



Óscar García
Kyndryl

Miembros titulares



Luis Otero
Engie



Rafael Bolívar
Enagás



Caio Araujo
Capital Energy & Kynegos



Fco. Javier López
NTT Data



Almudena Nieto
GMV



Ignacio Moratalla
Ayesa Digital



Diogo Lopes
Inetum



Iñaki Echeverría
Palo Alto Networks



Daniel Ramos
FI Group

Otros expertos participantes

Beatriz Cid
Engie

Bruno Gerlic
Baobab AI

Celia Cuevas
VASS Company

Hugo Soto
N3uron

Jokin Alonso
Verbund

Kevin García
Capgemini

Marina Rodriguez
Fujitsu

Roberto Díaz
GFT Technologies

Santiago Trillo
DXC

Sergio Fernández
Aviva Voice

Manuel Ayllón
VASS Company

Identificación del Reto

Las infraestructuras energéticas deben responder a una demanda creciente, integrar generación renovable y almacenamiento, y operar en un entorno más distribuido e interdependiente. Al mismo tiempo, buena parte de las redes, plantas y sistemas de control que sostienen el suministro fueron diseñados para condiciones distintas y permanecerán en servicio durante décadas. Desde el Comité de Expertos identificamos una tensión creciente entre la necesidad de incorporar inteligencia digital y la obligación de preservar la seguridad, la eficiencia y la continuidad de los procesos físicos.

Esta tensión se aprecia en activos cuyo estado resulta difícil de observar, sistemas heredados que necesitan conectarse sin haber sido concebidos para ello y funciones críticas ligadas a equipos específicos. También aparece cuando se desconoce qué dependencias sostienen una operación, cuánto tiempo puede mantenerse durante una incidencia o cómo recuperar una configuración validada. Modernizar exige distinguir qué activos pueden seguir aportando valor, cuáles necesitan protección o mayor visibilidad y cuáles deben sustituirse.

La inteligencia artificial amplía las posibilidades de anticipar fallos, simular escenarios y recomendar actuaciones, pero eleva las exigencias sobre los datos y los modelos. Una alerta sin contexto puede distraer al operador; una predicción presentada sin incertidumbre puede inducir una intervención inadecuada; y una decisión automatizada fuera de los límites validados puede afectar al proceso físico. Acercar el procesamiento al activo reduce tiempos de respuesta y dependencia de las comunicaciones, siempre que exista control sobre las versiones, la autonomía local y el retorno a un modo seguro.

La mayor conectividad extiende además el riesgo más allá de cada instalación. Fabricantes, integradores, mantenedores, proveedores de software y empresas auxiliares pueden disponer de accesos, conocimiento o componentes esenciales para la continuidad. Una incidencia en cualquiera de ellos puede trasladarse a varios activos o instalaciones. La ciberseguridad requiere, por tanto, una visión que conecte dirección, IT, OT, operación y cadena de suministro, y que demuestre la capacidad de contener incidentes y recuperar el servicio.

El reto también es organizativo. Integrar datos y aplicaciones aporta poco si el personal sigue buscando información en varios sistemas, recibe alarmas sin priorizar o espera autorizaciones cuya responsabilidad no está clara. La convergencia IT-OT debe mejorar el proceso real de decisión: ofrecer contexto a tiempo, comparar alternativas, definir quién puede actuar y conservar el conocimiento de quienes operan los activos. El valor de cada inversión tendrá que comprobarse en resultados operativos y económicos, además de en capacidades tecnológicas desplegadas.

No existe una respuesta única para redes eléctricas, refinerías, instalaciones gasistas, plantas de hidrógeno, activos hidráulicos o consumidores flexibles. Tampoco todas las organizaciones parten del mismo nivel de madurez. El Comité sitúa aquí el reto central del informe: **digitalizar los activos energéticos y aplicar inteligencia a su operación de forma proporcionada, verificable y gobernada, para decidir mejor sin perder el control sobre las funciones críticas**. El decálogo desarrolla las decisiones técnicas y organizativas necesarias para avanzar hacia un sistema energético más eficiente, competitivo, resiliente y sostenible.

1. Diseño estratégico resiliente y soberano

Diseñar activos energéticos preparados para operar, adaptarse y preservar el control en un sistema cada vez más distribuido, tensionado e incierto

Las infraestructuras energéticas afrontan la electrificación de la economía, el crecimiento de grandes consumidores, la incorporación masiva de renovables, la bidireccionalidad de los flujos y una exposición creciente a riesgos físicos, tecnológicos y cibernéticos. La interdependencia entre redes, plantas, sistemas digitales, proveedores y operadores amplifica además las consecuencias de cualquier incidencia.

Esta transformación alcanza a redes eléctricas y plantas de generación, pero también a refinerías, instalaciones químicas, infraestructuras gasistas, electrolizadores, plantas de biocombustibles, terminales de almacenamiento y redes logísticas. La digitalización mejora su observación, automatización y optimización, aunque incorpora dependencias que deben evaluarse desde el diseño.

El reto consiste en determinar cómo funcionará la infraestructura si pierde conectividad, se degrada un sistema crítico, falla un proveedor o se compromete el entorno OT. Un activo resiliente debe **mantener las funciones esenciales, preservar el control y recuperar progresivamente sus capacidades**. Resiliencia, seguridad y soberanía deben convertirse, por tanto, en criterios arquitectónicos verificables.

Empezar por la función crítica

La arquitectura debe partir de las funciones que sostienen la continuidad, no de las posibilidades de una solución tecnológica. Esto exige una cartografía que conecte activos físicos, sistemas digitales, personas y procesos.

Para cada función crítica conviene determinar:

- Activos físicos y digitales implicados.
- Datos necesarios y tiempo máximo de indisponibilidad.
- Dependencias tecnológicas, energéticas y organizativas.
- Capacidad mínima que debe mantenerse durante una incidencia.
- Consecuencias económicas, operativas y de seguridad de su pérdida.
- Personas o equipos que conservan la autoridad.

La pregunta central es **qué funciones deben preservarse y bajo qué condiciones**. A partir de ella pueden definirse la arquitectura, la redundancia, el modelo de automatización y la distribución de capacidades, haciendo visibles los intercambios entre coste, eficiencia, autonomía y riesgo.

Diseñar para operar en estados degradados

Evitar el fallo continúa siendo prioritario, pero ya no resulta suficiente. La infraestructura debe poder **degradarse de forma controlada**, contener una incidencia y mantener sus funciones esenciales cuando existan datos incompletos, pérdida de conectividad o capacidades limitadas.

Esta operación puede requerir:

- Priorización dinámica de cargas, procesos y suministros críticos.
- Segmentación y aislamiento selectivo.
- Reconfiguración parcial de redes, plantas o procesos.

- Redundancia física, lógica y organizativa.
- Modos locales ante la pérdida de conectividad.
- Procedimientos seguros de recuperación.

Estas capacidades deben definirse, probarse y asignarse a responsables concretos. También debe establecerse qué acciones pueden automatizarse dentro de límites validados, cuáles requieren supervisión y cuándo el operador debe recuperar el control. **La resiliencia técnica necesita una arquitectura de decisión igualmente resiliente**.

Soberanía del dato e inteligencia operativa

La soberanía del dato es la capacidad efectiva de controlar la información, los modelos y las decisiones que sostienen una función crítica. Abarca la ubicación del dato, pero también la dependencia de proveedores, la portabilidad, la interoperabilidad y la posibilidad de operar si un servicio externo deja de estar disponible.

Desde el diseño debe decidirse:

- Qué datos son imprescindibles y cuáles deben permanecer próximos al activo.
- Qué capacidades deben funcionar sin conectividad externa.
- Qué latencia admite cada decisión.
- Cómo trasladar datos, configuraciones y modelos a otra plataforma.
- Cómo auditar y revertir una actuación automatizada.

La distribución entre activo, *edge*, centros de control y plataformas centralizadas dependerá de la criticidad, la latencia y la conectividad. **Ninguna función crítica debería depender de un sistema externo sin evaluar las consecuencias de su indisponibilidad**. Los contratos y la arquitectura deben contemplar además mecanismos de portabilidad, interoperabilidad y salida.

Integrar resiliencia, seguridad y evolución

Los activos físicos pueden permanecer en servicio durante décadas, mientras las capacidades digitales evolucionan con mucha mayor rapidez. Los principios *secure by design* y *resilience by design* deben traducirse en cuatro requisitos:

- Conocer activos, sistemas y dependencias.
- Limitar la propagación de incidencias.
- Mantener las capacidades esenciales ante fallos parciales.
- Actualizar, sustituir o revertir componentes sin desestabilizar el conjunto.

La modernización de activos *legacy* debe ser progresiva y evitar que sus limitaciones bloqueen la observación, la integración o la evolución. Cuando intervenga IA, la arquitectura tendrá que garantizar que cada modelo sea **validable**, **trazable**, **supervisable** y **reversible**, con un modo seguro de funcionamiento ante pérdida de fiabilidad.

Convertir los principios en decisiones de inversión

Cada proyecto debe explicar qué función crítica refuerza, qué dependencias incorpora y qué capacidad de respuesta conserva la organización. Antes de aprobarlo conviene evaluar:

- Problema operativo o de negocio que resuelve.
- Comportamiento previsto durante una incidencia.
- Nuevos riesgos y dependencias.

- Alternativas de recuperación y reversión.
- Capacitación necesaria.
- Indicadores con los que se medirá el resultado.

El *business* case debe integrar inversión, OPEX, TCO, retorno directo y **valor económico del riesgo evitado**: continuidad, indisponibilidad reducida, capacidad productiva preservada y adaptación futura. La financiación pública puede acelerar actuaciones prioritarias, pero no sustituir una justificación basada en criticidad, riesgo y valor operativo.

Medir la resiliencia

Los indicadores deben adaptarse a las responsabilidades de cada perfil:

PERFIL	INDICADORES PRINCIPALES
Dirección financiera y de negocio	Coste esperado de indisponibilidad; pérdidas evitadas; OPEX, CAPEX y TCO; impacto sobre producción, margen y compromisos.
Operación y mantenimiento	Disponibilidad de funciones críticas; capacidad de operar en modo degradado; tiempo de recuperación; producción o suministro preservado.
Tecnología y OT	Dependencias identificadas; puntos únicos de fallo; autonomía sin conectividad; portabilidad; recuperación y reversión validadas.

Cada organización debe seleccionar los KPIs relevantes, establecer una línea de base y fijar objetivos coherentes con su riesgo y madurez. Deben analizarse conjuntamente: reducir costes puede limitar la autonomía; aumentar redundancias eleva el TCO; y ampliar la automatización exige mayor validación y supervisión.

Resiliencia y soberanía como garantías de competitividad

El valor de una infraestructura energética depende de su rendimiento normal y de su capacidad para absorber incidencias, preservar funciones esenciales y recuperar el servicio. Conocer las dependencias, distribuir adecuadamente las capacidades y conservar el control del dato facilita incorporar nuevas tecnologías con menor riesgo.

Diseñar activos resilientes y soberanos significa anticipar las decisiones difíciles: **qué debe seguir funcionando, qué puede degradarse, qué dependencias son aceptables, quién conserva la autoridad y cuánto riesgo asume la organización**.

2. Modernización y digitalización de activos legacy

Integrar infraestructuras energéticas heredadas en el ecosistema digital sin comprometer la continuidad operativa

Buena parte del sistema energético continúa apoyándose en PLC, SCADA, RTU, relés, equipos electromecánicos y sistemas de control diseñados hace décadas. Esta realidad afecta a redes eléctricas y plantas de generación, pero también a refinerías, instalaciones químicas, infraestructuras gasistas, activos hidráulicos, plantas de biocombustibles y terminales logísticas.

Muchos de estos activos siguen cumpliendo correctamente su función física, aunque deben operar en un entorno de mayor conectividad, integración IT-OT, supervisión remota, exigencia regulatoria y exposición cibernética. El reto no consiste en sustituirlos masivamente, sino en **conocerlos, protegerlos y decidir cómo deben evolucionar**.

Modernizar exige determinar qué puede mantenerse, instrumentarse, encapsularse o integrarse; qué funciones conviene desacoplar del hardware; y cuándo la obsolescencia hace necesaria una sustitución. Esta base debe consolidarse antes de incorporar IA, virtualización u optimización avanzada.

Hacer visible y clasificar el legado

La modernización comienza con una cartografía operativa que conecte cada activo con su función, criticidad, dependencias y consecuencias de indisponibilidad. Un inventario limitado a enumerar equipos no permite tomar decisiones sobre continuidad o inversión.

Para cada activo relevante conviene registrar:

- Función y proceso al que da soporte.
- Fabricante, modelo, antigüedad, soporte, software y configuración.
- Protocolos, sistemas relacionados y accesos.
- Dependencias energéticas, digitales y de comunicaciones.
- Repuestos, documentación y conocimiento disponibles.
- Datos generados y posibilidades reales de extracción.
- Criticidad para seguridad, producción y continuidad.

En entornos OT, el descubrimiento debe evitar técnicas activas que puedan afectar a equipos sensibles. Documentación, entrevistas, inspección física y observación pasiva permiten ganar visibilidad sin introducir riesgos innecesarios.

La priorización debe combinar cuatro dimensiones:

DIMENSIÓN	PREGUNTA PRINCIPAL
Criticidad operativa	¿Qué consecuencias tendría el fallo sobre seguridad, suministro, producción o medioambiente?
Obsolescencia	¿Existen soporte, repuestos, conocimiento y capacidad de actualización?
Exposición y dependencia	¿Qué conectividad, accesos, propagación y puntos únicos de fallo presenta?
Potencial de valor	¿Sus datos pueden mejorar mantenimiento, eficiencia, planificación o capacidad productiva?

La edad no determina por sí sola la prioridad. Un equipo antiguo puede continuar siendo viable si está controlado y dispone de soporte; otro más reciente puede concentrar una función crítica o depender de un proveedor sin alternativa. También deben considerarse el riesgo de mantenerlo, el coste de intervenir, la vida útil restante y el tiempo necesario para implantar otra solución.

Elegir una estrategia proporcionada

La modernización no es una decisión binaria entre conservar y sustituir. Cada activo puede requerir una combinación de actuaciones:

ESTRATEGIA	CUÁNDO RESULTA ADECUADA	OBJETIVO
Mantener y documentar	Funciona, tiene baja exposición y conserva soporte o conocimiento	Preservar valor y controlar su evolución
Proteger o encapsular	Es crítico, difícil de actualizar y necesita limitar su exposición	Reducir riesgo sin alterar su función
Instrumentar	El núcleo físico sigue siendo válido, pero ofrece poca visibilidad	Obtener datos sin sustituirlo
Integrar	Existen datos accesibles, aunque aislados o sin contexto	Incorporarlos a supervisión y decisión
Desacoplar o virtualizar	El hardware puede mantenerse mientras las funciones digitales evolucionan	Separar los ciclos físicos y digitales
Sustituir	El riesgo, la obsolescencia o el coste superan el valor de conservarlo	Renovar la capacidad de forma controlada

Un PLC puede mantenerse y aislarse mientras una pasarela extrae sus datos; un SCADA puede conservar funciones críticas e integrarse con una capa moderna de supervisión. La sustitución debe reservarse para riesgos difíciles de mitigar y planificarse con ventanas de intervención, pruebas y reversión.

Modernizar sin detener la operación

La implantación debe avanzar mediante una secuencia controlada:

1. **Comprender**: inventariar y documentar activos y dependencias.
2. **Priorizar**: seleccionar riesgos críticos y oportunidades de valor.
3. **Diseñar**: elegir la estrategia adecuada.
4. **Probar**: validar sobre un entorno o alcance limitado.
5. **Desplegar**: intervenir con continuidad y reversión.
6. **Medir**: comprobar resultados y decidir si se escala.

Un piloto debe responder a una hipótesis operativa, no limitarse a demostrar una tecnología. Debe definir problema, alcance, datos, riesgos, resultado esperado, KPIs y criterios para escalar, modificar o detener la iniciativa. **Cada actuación validada debe reducir incertidumbre y crear una base reutilizable**.

Extraer inteligencia y preservar conocimiento

Pasarelas industriales, sensores externos, conversores de protocolo y capas de supervisión pueden aportar visibilidad sin modificar la lógica de control. Los datos deben ser fiables y relacionarse con el activo, la carga, el modo de operación y las condiciones en que se generaron; capturarlos sin contexto apenas produce valor.

La modernización debe abordar también la obsolescencia del conocimiento. Parte de la operación depende de técnicos que recuerdan modificaciones, interpretan señales y resuelven incidencias que no están documentadas. Conviene:

- Actualizar esquemas, configuraciones y procedimientos reales.
- Registrar incidencias, soluciones y excepciones conocidas.
- Entrevistar a operadores y mantenedores.
- Crear repositorios accesibles y actualizables.
- Impulsar formación cruzada y validar la documentación mediante ejercicios.

El objetivo es **convertir experiencia individual en capacidad organizativa**. Esta lógica debe aplicarse con perspectiva multienergía: una intervención sobre activos eléctricos, térmicos, gasistas, hidráulicos o logísticos puede modificar consumos, producción, almacenamiento y flexibilidad del conjunto.

Construir el *business* case sobre el coste de no modernizar

Cuando un activo continúa funcionando, el ahorro inmediato puede no justificar la intervención. El análisis debe incorporar OPEX, CAPEX y TCO, junto con:

- Coste esperado de indisponibilidad.
- Obsolescencia de componentes y repuestos.
- Dependencia de soporte o conocimiento escaso.
- Exposición regulatoria y cibernética.
- Pérdidas de eficiencia o capacidad productiva.
- Imposibilidad de integrar nuevas capacidades.
- Riesgo de una sustitución urgente y no planificada.

La pregunta es **qué retorno genera modernizar y qué coste o riesgo supone no hacerlo**. Los indicadores deben adaptarse a cada perfil:

PERFIL	INDICADORES PRINCIPALES
Dirección y negocio	OPEX frente a CAPEX; TCO; coste de indisponibilidad; pérdidas evitadas; retorno; valor de extender la vida útil.
Operación y mantenimiento	Disponibilidad; fallos; tiempo de reparación; paradas; coste de mantenimiento; repuestos críticos; cobertura de monitorización.
Tecnología y OT	Activos inventariados; sistemas sin soporte; dependencias; documentación; datos accesibles; interoperabilidad y tiempo de integración.

La financiación vinculada a modernización industrial, digitalización, eficiencia energética o ciberseguridad puede acelerar actuaciones, pero **no debe sustituir la priorización por criticidad y valor**.

Modernizar para seguir operando

Modernizar significa lograr que infraestructuras que han sostenido la operación durante décadas sigan aportando valor en un sistema más conectado y exigente. La decisión debe equilibrar criticidad, obsolescencia, exposición, valor del dato y capacidad de evolución.

Un activo conocido, documentado y correctamente integrado puede avanzar hacia supervisión avanzada, mantenimiento prescriptivo, IA *on-edge* o simulación. El objetivo final es extender su vida útil cuando resulte viable, reducir riesgos y crear una operación más eficiente, competitiva y resiliente.

3. Virtualización de la infraestructura física crítica

Evolucionar subestaciones, redes y activos energéticos hacia modelos más flexibles, observables y preparados para una demanda creciente

Una parte relevante de la infraestructura energética continúa operando sobre subestaciones, relés, sistemas de automatización y arquitecturas de telecontrol concebidos para flujos unidireccionales y demandas más estables. La electrificación industrial, los centros de datos, las renovables, el almacenamiento y el autoconsumo exigen ahora mayor flexibilidad y una observación más granular.

Esta diferencia entre el ciclo de vida del activo físico y la velocidad de evolución digital también afecta a refinerías, instalaciones químicas, plantas de hidrógeno, infraestructuras gasistas e hidráulicas y terminales logísticas. La virtualización permite **desacoplar progresivamente ambos ciclos**, de modo que determinadas funciones puedan actualizarse y escalar sin sustituir activos físicos todavía válidos.

Qué significa virtualizar

Digitalizar incorpora capacidades de captura e intercambio de información; sensorizar añade nuevas variables observables; y un gemelo digital representa el comportamiento de un activo. **Virtualizar significa desacoplar una función digital del hardware específico** sobre el que se ha ejecutado tradicionalmente.

Funciones de supervisión, automatización, registro o protección pueden trasladarse, cuando resulte adecuado, desde dispositivos propietarios a software ejecutado sobre plataformas estandarizadas. Esto puede facilitar:

- Actualizaciones sin sustituir todo el hardware.
- Consolidación de aplicaciones e infraestructura.
- Despliegue y escalado más rápidos.
- Mayor interoperabilidad.
- Menor dependencia tecnológica.
- Separación de los ciclos físico y digital.

La virtualización no elimina transformadores, interruptores, válvulas, bombas, sensores o actuadores. Modifica la forma de desplegar y evolucionar la inteligencia que los observa y coordina.

Diferentes funciones, diferentes exigencias

La conveniencia de virtualizar depende de la criticidad y los requisitos temporales de cada función:

TIPO DE FUNCIÓN	EJEMPLOS	CONSIDERACIONES
Supervisión e información	HMI, históricos, visualización y documentación	Elevado potencial si se garantizan disponibilidad y acceso
Analítica y apoyo	Anomalías, condición e indicadores	Permite avanzar sin actuar directamente sobre el proceso
Automatización y coordinación	Secuencias, control avanzado y consignas	Exige validar latencia, determinismo, aislamiento y fallos
Protección y control crítico	Actuación directa sobre activos y seguridad	Requiere máxima validación, redundancia, sincronización y garantía temporal

Una organización puede comenzar con ingeniería, supervisión o analítica y avanzar conforme demuestre disponibilidad y recuperación. Las arquitecturas híbridas permiten mantener funciones críticas en equipos especializados y virtualizar otras. **El objetivo no es virtualizar al máximo, sino alcanzar el nivel que aporte valor sin perder control**.

La subestación como caso de transformación

En una subestación convergen activos eléctricos longevos, relés, dispositivos electrónicos, comunicaciones y telecontrol. La dependencia de hardware específico dificulta actualizar funciones o integrar dispositivos heterogéneos.

La estandarización asociada a IEC 61850 y la evolución hacia modelos definidos por software permiten independizar progresivamente herramientas de ingeniería, HMI, registro de eventos, pasarelas, automatismos y, cuando existan garantías suficientes, determinadas protecciones. El estándar facilita el intercambio, pero **no garantiza por sí solo la interoperabilidad**: cada integración debe validarse.

Así, transformadores y aparellaje pueden permanecer en servicio durante décadas mientras la supervisión, el análisis y la coordinación evolucionan con mayor rapidez.

Decidir qué conviene virtualizar

La decisión debe responder a un problema operativo y evaluar:

- Criticidad para seguridad y continuidad.
- Latencia máxima, variabilidad y determinismo.
- Sincronización, disponibilidad y redundancia requeridas.
- Interoperabilidad y acoplamiento con el hardware.
- Posibilidad de probar sin afectar al proceso.
- Capacidad de recuperación y reversión.
- Madurez, soporte y ciclo de vida de la solución.
- Ahorro, flexibilidad y mejora operativa esperados.

La latencia media no basta para funciones críticas: importa el comportamiento bajo carga, durante fallos parciales y en estados degradados. También deben incluirse mantenimiento, licencias, validación, soporte y recursos computacionales. Consolidar hardware puede perder sentido si aumenta excesivamente la complejidad o crea una dependencia más difícil de controlar.

Conviene mantener hardware dedicado cuando no puedan garantizarse los tiempos, la redundancia o la recuperación; la función no pueda probarse con seguridad; la integración añada más complejidad que valor; falten profesionales capacitados; o los requisitos regulatorios y de certificación exijan otra solución. La virtualización tampoco corrige la degradación física ni debe prolongar activos cuya sustitución ya resulte necesaria.

Desplegar de forma progresiva y reversible

Una ruta prudente puede seguir seis fases:

1. **Seleccionar**: identificar una función con valor verificable.
2. **Caracterizar**: documentar criticidad, latencia, interfaces y disponibilidad.
3. **Probar**: reproducir cargas, comunicaciones y escenarios de fallo.
4. **Ejecutar en paralelo**: comparar resultados sin actuar sobre el proceso.
5. **Transferir**: asumir responsabilidades limitadas y supervisadas.
6. **Validar y escalar**: extender solo cuando se cumplan los criterios.

El *shadow mode* permite utilizar datos reales y comparar tiempos, estabilidad y respuesta ante incidencias. La aceptación debe exigir cumplimiento temporal, disponibilidad en condiciones normales y degradadas, recuperación correcta, ausencia de impactos imprevistos y **capacidad efectiva de reversión**. Volver a una configuración validada debe estar definido, asignado y probado.

Observabilidad, programabilidad y papel humano

La virtualización puede facilitar registros consistentes, correlación de eventos, análisis de capacidad y reconfiguración más rápida. Una función desacoplada puede actualizarse o replicarse con mayor agilidad, pero cada cambio necesita control de versiones, validación y trazabilidad.

Antes del despliegue deben establecerse responsables, autoridad para aprobar cambios, comunicación de degradaciones, activación de configuraciones alternativas y condiciones de reversión. El operador necesita ver el estado de cada función, sus dependencias y los recursos que utiliza. Los perfiles OT deben comprender la plataforma digital y los equipos tecnológicos, los requisitos físicos de disponibilidad, determinismo y seguridad.

Estos principios pueden aplicarse a supervisión, historiadores, telecontrol y control avanzado en refino, química, hidrógeno, infraestructuras gasistas e hidráulicas, redes térmicas, microrredes y sistemas híbridos. Las funciones ligadas a seguridad de proceso o actuación inmediata requerirán siempre un nivel superior de garantía.

Construir un business case verificable

El análisis debe contemplar hardware, licencias, infraestructura computacional, redundancia, integración, migración, validación y soporte. Los beneficios pueden proceder de reducir equipamiento específico, acelerar actualizaciones, extender la vida del activo, mejorar disponibilidad y habilitar nuevas aplicaciones.

PERFIL	INDICADORES PRINCIPALES
Dirección y negocio	TCO frente a la arquitectura convencional; CAPEX evitado; OPEX; tiempo de despliegue; coste de indisponibilidad; retorno.
Operación y mantenimiento	Disponibilidad; recuperación y reversión; incidencias; cambios validados; intervenciones físicas evitadas; observabilidad.
Tecnología y OT	Funciones desacopladas; latencia y variabilidad; uso y reserva de recursos; compatibilidad; versiones; pruebas en degradado.

Los resultados deben compararse con una línea de base. La financiación para digitalización, resiliencia o modernización puede acelerar la inversión, pero la decisión debe sustentarse en el valor operativo y el riesgo.

Virtualizar para que la inteligencia evolucione

Las ampliaciones físicas seguirán siendo necesarias, pero resultarán insuficientes si las funciones digitales permanecen ligadas a arquitecturas rígidas. La virtualización permite conservar activos válidos y actualizar su supervisión, integración o automatización.

El valor reside en **seleccionar las funciones adecuadas, validarlas en condiciones representativas y escalar solo cuando los resultados lo justifiquen**. La infraestructura física permanece; su inteligencia adquiere capacidad para evolucionar y preparar el despliegue posterior de mantenimiento prescriptivo, simulación, optimización e inteligencia distribuida.

4. IA para el mantenimiento predictivo y prescriptivo en el mundo físico

Anticipar fallos, seleccionar la mejor actuación y optimizar la gestión de activos energéticos mediante inteligencia aplicada a la operación

Las infraestructuras energéticas afrontan mayores tensiones de demanda, activos envejecidos, generación distribuida y exigencias crecientes de continuidad. El mantenimiento correctivo asume las consecuencias de la avería; el preventivo reduce parte del riesgo, pero puede intervenir demasiado pronto o no detectar degradaciones entre revisiones. La monitorización basada en condición utiliza el estado real del activo y la IA permite identificar patrones y anticipar su evolución.

El salto decisivo consiste en transformar la predicción en una actuación. Conocer la probabilidad de fallo aporta valor, pero la organización necesita decidir cuándo intervenir, qué recursos utilizar y qué consecuencias tendría retrasar la acción. El mantenimiento prescriptivo integra condición, criticidad, producción, personal, repuestos, ventanas de intervención, seguridad y coste para **recomendar la alternativa que ofrece el mejor equilibrio operativo**.

Del calendario a la decisión prescriptiva

Cada nivel de mantenimiento responde a una pregunta y exige mayor madurez de datos e integración:

NIVEL	PREGUNTA	CAPACIDAD
Correctivo	¿Qué ha fallado?	Reparar después de la avería
Preventivo	¿Cuándo corresponde intervenir?	Actuar por calendario, uso o ciclos
Basado en condición	¿Cómo se encuentra el activo?	Intervenir según su estado observado
Predictivo	¿Qué puede fallar y cuándo?	Anticipar degradaciones y estimar riesgo
Prescriptivo	¿Qué conviene hacer?	Recomendar la mejor actuación disponible
Optimización de cartera	¿Cómo asignamos los recursos?	Priorizar activos, ventanas e intervenciones

Ante una degradación, el sistema puede comparar la intervención inmediata, la reducción de carga, una mayor supervisión, la espera hasta una parada planificada o la sustitución de un componente. Cada alternativa afecta de forma distinta a riesgo, disponibilidad, producción, coste y seguridad. **La mejor decisión para un activo puede no ser la mejor para el conjunto**, por lo que la prescripción debe incorporar la perspectiva de cartera.

Convertir señales físicas en riesgo operativo

Transformadores, interruptores, turbinas, compresores, bombas, hornos, reactores o electrolizadores generan señales térmicas, eléctricas, mecánicas, hidráulicas y ambientales. Una lectura aislada rara vez explica el estado del equipo. Debe relacionarse con históricos, carga, configuración, condiciones de proceso, órdenes de trabajo y fallos anteriores.

La detección de anomalías permite identificar desviaciones, pero una anomalía no equivale necesariamente a un fallo. Para que una alerta resulte accionable debe precisar:

- Variables que explican la desviación.
- Componente y modo de fallo compatibles.
- Probabilidad y horizonte de evolución.
- Consecuencias sobre el activo y el proceso.
- Margen disponible para intervenir.
- Comprobaciones que reducirían la incertidumbre.

Los modelos híbridos combinan datos y algoritmos con reglas de ingeniería, límites físicos, análisis de criticidad y conocimiento experto. Su explicación debe ser proporcional a la decisión: priorizar una inspección requiere menos evidencia que reducir carga o detener un proceso crítico.

La estimación de vida útil remanente o RUL tampoco debe interpretarse como una fecha exacta. Es una previsión sujeta a incertidumbre que debe incluir un intervalo de confianza y actualizarse con nuevos datos. La prioridad surge de combinar:

- Probabilidad y horizonte de fallo.
- Consecuencias sobre seguridad, medioambiente, producción y suministro.

- Redundancia y alternativas operativas.
- Disponibilidad de repuestos y duración de la intervención.
- Posibilidad de modificar el régimen operativo.
- Confianza de la predicción.

Esta jerarquía evita inundar a mantenimiento con alertas y distingue entre actuaciones inmediatas, mayor supervisión e intervenciones programables.

Prescribir e integrar la actuación

Una recomendación debe incorporar estado y criticidad del activo, personal disponible, repuestos, ventanas de parada, demanda prevista, coste energético, interdependencias y riesgo de aplazamiento. Así puede comparar si conviene intervenir, reducir carga, transferir operación o coordinar el trabajo con otras actuaciones.

Para transformar la analítica en mantenimiento real, el flujo debe cerrar el ciclo:

1. Capturar y contextualizar el dato.
2. Detectar la degradación.
3. Estimar riesgo y horizonte temporal.
4. Comparar alternativas.
5. Validar técnica y operativamente.
6. Crear o priorizar la orden de trabajo.
7. Ejecutar y registrar la intervención.
8. Verificar el resultado y realimentar el modelo.

La integración con EAM, GMAO o CMMS permite asociar la recomendación al activo, comprobar repuestos y competencias, y proponer una ventana de intervención. La información posterior —degradación confirmada, componente sustituido y evolución del equipo— permite medir la calidad del modelo. Sin este retorno, la organización acumula predicciones, pero no aprendizaje. **Observar, recomendar, actuar, verificar y mejorar debe funcionar como un circuito cerrado**.

Definir el papel humano y gobernar el modelo

Antes del despliegue deben asignarse el responsable del activo, el propietario del dato, el responsable técnico del modelo y las personas autorizadas para validar, aprobar y ejecutar la intervención. También debe definirse qué ocurrirá cuando el modelo pierda fiabilidad.

El grado de autonomía dependerá del impacto. El sistema puede priorizar automáticamente una inspección de bajo riesgo, mientras una parada o reducción de carga requerirá validación humana. La recomendación debe mostrar qué detecta, qué variables la sustentan, su nivel de confianza, las consecuencias de cada alternativa y las condiciones bajo las que dejaría de ser válida.

El experto debe poder aceptar, modificar o rechazar la propuesta y registrar el motivo. Estas discrepancias pueden revelar datos incompletos o conocimiento operativo todavía no incorporado. **La supervisión humana debe ser efectiva, no una aprobación formal**.

La gobernanza debe cubrir todo el ciclo de vida:

- Caso de uso, activos, datos y modos de fallo autorizados.
- Errores aceptables según sus consecuencias.
- Validación con datos y condiciones representativos.

- Versionado de modelos, datos y parámetros.
- Monitorización de precisión, falsos positivos, falsos negativos y deriva.
- Reentrenamiento y despliegue controlados.
- Reversión y retirada cuando el modelo deje de ser fiable o útil.

El equilibrio entre falsos positivos y negativos debe fijarse según el riesgo. Las actualizaciones deben dejar constancia de qué versión está operativa, cómo fue validada y cómo recuperar la anterior.

Escalar con validación local y perspectiva multienergía

Un modelo validado sobre un equipo no puede trasladarse automáticamente. Cargas, ambientes, configuraciones y políticas de mantenimiento varían incluso entre activos de la misma familia. El escalado puede avanzar desde un modo de fallo concreto hacia una familia de activos, una instalación y, finalmente, una cartera coordinada, reutilizando componentes y aprendizaje, pero manteniendo la validación local.

La estandarización de taxonomías, modos de fallo, datos y órdenes de trabajo facilita esta evolución. La perspectiva multienergía resulta esencial cuando la indisponibilidad de un electrolizador modifica demanda eléctrica y producción de hidrógeno, o el fallo de un compresor afecta a procesos industriales y flujos logísticos.

La aplicación alcanza redes eléctricas, renovables, refino y química, hidrógeno, infraestructuras gasistas e hidráulicas, biocombustibles, redes térmicas, microrredes y sistemas de almacenamiento. La prescripción debe considerar sus interdependencias para evitar que una decisión óptima para un equipo perjudique al conjunto.

Medir el valor generado

La precisión técnica solo tiene valor si mejora decisiones, disponibilidad, riesgo y utilización de recursos:

PERFIL	INDICADORES PRINCIPALES
Dirección y negocio	Coste de mantenimiento; OPEX evitado; pérdidas de producción o suministro; vida útil extendida; coste esperado de fallo; retorno.
Mantenimiento y operación	MTBF y MTTR; mantenimiento planificado; averías urgentes; antelación útil; disponibilidad; intervenciones innecesarias evitadas.
Tecnología y OT	Activos cubiertos; calidad y contexto del dato; falsos positivos y negativos; error de RUL; modelos monitorizados; trazabilidad y reversión.
Adopción	Recomendaciones aceptadas, modificadas o rechazadas; actuaciones completadas; resultado real frente al esperado; valor por caso de uso.

Los resultados deben compararse con una línea de base. Una alta tasa de aceptación no demuestra por sí sola calidad; puede ocultar una validación automática. Deben analizarse también las causas de rechazo y el resultado real de cada actuación.

Una ruta práctica hacia la prescripción

NIVEL	PRIORIDADES
1. Conocer el estado	Seleccionar activos y fallos críticos; contextualizar datos; integrar históricos; definir responsables y línea de base.
2. Anticipar el fallo	Detectar anomalías; estimar riesgo y RUL; validar con expertos; integrar alertas; medir precisión y antelación.
3. Recomendar y optimizar	Comparar alternativas; incorporar recursos, producción y riesgo; priorizar la cartera; generar órdenes; aprender de los resultados.

No todas las organizaciones deben alcanzar inmediatamente el nivel prescriptivo. Cuando los activos están poco documentados o los datos son insuficientes, mejorar la monitorización por condición ya puede generar valor. El avance debe apoyarse en resultados verificables, integración y confianza.

La financiación para digitalización, eficiencia energética y modernización puede facilitar el despliegue. Los modelos deberán alinearse además con los marcos aplicables de IA, seguridad industrial, ciberseguridad y protección de infraestructuras.

De anticipar la avería a decidir mejor

El mantenimiento con IA alcanza su valor cuando convierte señales físicas en decisiones operativas. Detectar una degradación es el comienzo; preservar la continuidad exige determinar qué hacer, cuándo actuar y cómo coordinar recursos.

Esta evolución requiere datos contextualizados, conocimiento físico, integración con mantenimiento, modelos gobernados y responsabilidades claras. La IA amplía la capacidad del experto para comparar alternativas y priorizar actuaciones, pero no elimina su autoridad. El objetivo es **decidir mejor cómo proteger la continuidad, la eficiencia y el valor de los activos energéticos**.

5. Simulación y optimización de escenarios para la toma de decisiones

Transformar el dato operativo en capacidad de anticipación y asignar recursos limitados para alcanzar los objetivos del sistema

La digitalización ha multiplicado la visibilidad sobre redes, plantas y activos críticos, pero conocer qué ocurre no determina por sí mismo qué decisión adoptar. Renovables variables, almacenamiento, generación distribuida, grandes consumos y demanda flexible crean múltiples escenarios, mientras las organizaciones deben equilibrar capacidad, coste, margen, seguridad, continuidad, emisiones y compromisos de suministro.

La simulación permite explorar cómo podría comportarse el sistema antes de intervenir. La optimización determina cómo utilizar los recursos disponibles para cumplir los objetivos respetando las restricciones. Conectarlas permite **construir escenarios,**

comparar consecuencias y recomendar actuaciones respaldadas por modelos físicos, datos operativos y criterios de negocio.

De observar a decidir

Las capacidades responden a preguntas distintas:

CAPACIDAD	PREGUNTA	RESULTADO
Monitorización	¿Qué está ocurriendo?	Estado actual
Analítica descriptiva	¿Qué ha ocurrido y por qué?	Interpretación de eventos e históricos
Predicción	¿Qué es probable que ocurra?	Comportamientos futuros
Simulación	¿Qué ocurriría si cambian las condiciones?	Consecuencias de distintos escenarios
Optimización	¿Qué combinación utiliza mejor los recursos?	Solución que maximiza o minimiza objetivos
Prescripción	¿Qué actuación conviene ejecutar?	Recomendación contextualizada

Una predicción puede anticipar demanda; la simulación analiza cómo respondería la infraestructura; la optimización combina generación, almacenamiento y flexibilidad; y la prescripción propone una actuación. Esta última debe mostrar supuestos, restricciones, impacto previsto y condiciones de validez. **El valor surge al convertir capacidades analíticas en alternativas comparables y accionables**.

Simular con la fidelidad necesaria

La simulación representa un activo, planta, red o sistema multienergía para evaluar su respuesta sin actuar directamente sobre él. Puede combinar ecuaciones físicas, datos históricos, reglas de control, IA, restricciones técnicas e información meteorológica, económica y de mercado.

Los modelos físicos ofrecen coherencia e interpretabilidad, pero pueden resultar costosos de construir. Los basados en datos capturan patrones complejos, aunque dependen de la representatividad de la información. Los modelos híbridos aprovechan ambas aproximaciones.

El nivel de detalle debe responder a la decisión. Evaluar capacidad de red exige representar restricciones eléctricas; planificar hidrógeno requiere relacionar precio, rendimiento del electrolizador, almacenamiento y demanda. **Una réplica exhaustiva puede elevar costes y retrasar el valor sin mejorar la decisión**.

El gemelo digital mantiene el modelo conectado con el activo mediante datos OT, topología, información GIS, parámetros de ingeniería, históricos, demanda, producción y restricciones. No es una visualización estática, sino un modelo vivo que permite:

- Evaluar nuevos consumos, generación o ampliaciones.
- Probar reconfiguraciones, arranques y paradas.
- Comparar estrategias de producción.
- Preparar respuestas ante incidencias.
- Formar operadores en escenarios poco frecuentes.

La desviación entre resultado simulado y observado puede indicar cambios en el activo, errores de datos o necesidad de recalibración. El gemelo debe dimensionarse desde un

componente hasta una cartera según la decisión, y medirse por la incertidumbre o el riesgo que reduce, no por el volumen de datos integrado.

Optimizar recursos y objetivos

Todo problema de optimización debe definir:

- **Objetivo**: resultado que se desea maximizar o minimizar.
- **Variables de decisión**: elementos que pueden modificarse.
- **Restricciones**: límites físicos, operativos, económicos o regulatorios.
- **Horizonte temporal**: periodo sobre el que se calcula.

Una red puede minimizar pérdidas y congestiones mediante configuración, almacenamiento y flexibilidad. Una refinería puede maximizar margen ajustando cargas y secuencias dentro de límites productivos y de seguridad. Una planta de hidrógeno puede decidir cuándo producir y almacenar considerando precios, renovables, eficiencia y contratos.

La formulación del objetivo es una decisión estratégica. Minimizar costes puede reducir resiliencia; maximizar producción puede aumentar desgaste; y reducir emisiones puede afectar al margen. La optimización multiobjetivo permite comparar alternativas eficientes —menor coste, mayor disponibilidad, menores emisiones o mayor margen de capacidad— haciendo visibles sus compromisos.

Debe distinguirse entre:

- **Restricciones duras**: nunca pueden incumplirse, como seguridad e integridad física.
- **Restricciones blanda**s: pueden superarse bajo condiciones y penalizaciones.
- **Preferencias**: orientan la solución sin constituir un límite absoluto.

Esta separación explica por qué se descarta una alternativa y qué tendría que cambiar para hacerla viable.

Decidir dentro de la incertidumbre

Demanda, meteorología, precios y disponibilidad de activos no pueden conocerse con exactitud. Una simulación determinista resulta útil para condiciones concretas, pero puede crear una falsa certeza cuando existe alta variabilidad.

ENFOQUE	UTILIDAD
Análisis de sensibilidad	Identificar las variables que más influyen
Simulación probabilística	Evaluar distribuciones de resultados
Optimización estocástica	Incorporar escenarios y probabilidades
Optimización robusta	Mantener soluciones válidas bajo condiciones adversas
Pruebas de estrés	Analizar eventos extremos y fallos múltiples

El resultado debe incluir rangos, probabilidades y niveles de confianza. Si una mínima variación de precio, demanda o disponibilidad cambia por completo la solución, la decisión es frágil; si permanece válida bajo distintas condiciones, ofrece mayor robustez.

La técnica debe ajustarse al problema y al tiempo disponible. La optimización lineal resulta adecuada para relaciones proporcionales; la programación entera o mixta, para arranques y decisiones discretas; los métodos no lineales, para rendimientos varia-

bles; y los enfoques heurísticos, cuando una solución suficientemente buena resulta más útil que alcanzar el óptimo teórico. La IA puede aproximar simulaciones costosas, siempre que se conozcan y validen sus límites. **La sofisticación técnica importa menos que obtener una decisión útil dentro del tiempo operativo**.

Aplicaciones en un sistema multienergía

ÁMBITO	APLICACIONES PRINCIPALES
Redes eléctricas	Conexión de grandes consumidores, refuerzos, congestiones, almacenamiento, flexibilidad y reconfiguración
Industria, refino y química	Secuencias, cargas, consumos, vapor, combustibles, campañas, paradas y logística
Hidrógeno y almacenamiento	Operación del electrolizador, producción, carga, almacenamiento, demanda y contratos
Consumidores y recursos distribuidos	Procesos flexibles, climatización, bombeos, frío, vehículos eléctricos, baterías y autoconsumo

La simulación no sustituye las inversiones físicas, pero ayuda a priorizarlas y aprovechar mejor la capacidad existente. La perspectiva multienergía evita optimizaciones parciales: reducir electricidad puede elevar el uso de combustible o vapor; desplazar una carga puede trasladar la restricción a otra parte del proceso.

La demanda flexible debe respetar potencia disponible, duración, recuperación posterior, impacto productivo y preferencias del consumidor. Su activación necesita ofrecer un beneficio económico claro y conservar el control del usuario.

Estas capacidades apoyan decisiones estratégicas —dimensionamiento e inversión—, tácticas —producción, mantenimiento y aprovisionamiento— y operativas —reconfiguración, consignas y respuesta ante incidencias—. El detalle, la frecuencia de actualización y el tiempo de cálculo deben adaptarse a cada horizonte.

Gobernar modelos y mantener al experto

Los modelos no son neutrales: sus resultados dependen de objetivos, pesos, restricciones, datos y supuestos. La gobernanza debe establecer:

- Quién define objetivos, prioridades y límites.
- Qué datos, previsiones e hipótesis se utilizan.
- Quién valida el modelo y modifica sus parámetros.
- Quién autoriza la decisión.
- Cómo se registra el resultado ejecutado.

La validación debe comparar el modelo con datos reales, escenarios conocidos, condiciones extremas y conocimiento experto. La trazabilidad debe reconstruir el estado del sistema, versión, previsiones, restricciones, alternativas, recomendación, decisión adoptada y resultado observado.

Un modelo puede ser matemáticamente correcto y producir una decisión inadecuada si optimiza el objetivo equivocado. Por ello, el experto necesita comprender qué variables influyen, qué supuestos son inciertos, qué restricciones han limitado la solución y qué alternativas próximas existen. En decisiones críticas puede ser preferible presentar varias opciones eficientes.

La automatización dependerá de criticidad, confianza, reversibilidad e impacto. **El modelo debe ampliar la capacidad del experto sin ocultar los criterios que generan el resultado**.

Medir la calidad y el valor

La evaluación debe combinar fidelidad del modelo, oportunidad y efecto real de la decisión:

PERFIL	INDICADORES PRINCIPALES
Dirección y negocio	Margen; coste energético; CAPEX priorizado o evitado; capacidad liberada; pérdidas reducidas; retorno previsto y realizado.
Operación y planificación	Utilización de activos; producción por MW; congestiones; almacenamiento y flexibilidad; tiempo para evaluar alternativas; mejora frente a la referencia.
Tecnología y modelos	Desviación simulado-real; precisión de previsiones; tiempo de cálculo; recalibración; sensibilidad; trazabilidad y deriva.
Adopción y decisión	Recomendaciones aceptadas, modificadas o rechazadas; soluciones inviables; restricciones omitidas; tiempo hasta decidir; valor acumulado.

Un modelo preciso que responde fuera de la ventana de decisión aporta poco. Una solución óptima pero inviable tampoco mejora la operación.

Una ruta hacia la inteligencia de decisión

NIVEL	PRIORIDADES
1. Representar y comprender	Seleccionar una decisión; identificar variables y restricciones; integrar datos; construir y validar el modelo.
2. Simular y comparar	Crear escenarios; incorporar incertidumbre; evaluar consecuencias; identificar variables sensibles.
3. Optimizar y prescribir	Definir objetivos; comparar combinaciones; generar recomendaciones; integrarlas y medir resultados.

Los primeros casos deben centrarse en decisiones frecuentes, datos accesibles y resultados medibles. Una simulación acotada que mejora una inversión o programación puede aportar más valor que un gemelo digital de gran alcance sin una decisión asociada. La financiación vinculada a digitalización, eficiencia, flexibilidad y resiliencia puede acelerar estas capacidades, pero no sustituir un caso de uso claro.

Decidir mejor dentro de la incertidumbre

La simulación permite comprender qué podría ocurrir; la optimización determina cómo utilizar recursos limitados; y la prescripción convierte el resultado en una recomendación. Su valor depende de representar correctamente el sistema, hacer explícitos los objetivos, incorporar incertidumbre y mantener al experto dentro del proceso.

La inteligencia de decisión no elimina los conflictos entre coste, seguridad, resiliencia, margen y sostenibilidad. **Los hace visibles y permite compararlos de forma estructurada**, una capacidad esencial para operar infraestructuras y sistemas multienergía con mayor eficiencia, competitividad y resiliencia.

6. Computación e inteligencia artificial *on-edge*

Acercar la capacidad de procesamiento y decisión al activo para reducir latencias, reforzar la autonomía operativa y mantener la continuidad en infraestructuras críticas

Sensores, PLC, cámaras, dispositivos electrónicos y sistemas de control generan volúmenes crecientes de datos en redes, plantas e infraestructuras distribuidas. El reto consiste en procesarlos dentro del tiempo útil: una alteración eléctrica, térmica o de presión puede requerir una respuesta incompatible con enviar toda la información a una plataforma remota y esperar su retorno.

La computación *on-edge* acerca tratamiento, inferencia y decisión al origen del dato. Puede reducir latencia y comunicaciones, además de mantener determinadas funciones cuando se degrada la conectividad. Sin embargo, distribuir inteligencia entre cientos o miles de nodos introduce nuevas necesidades de gestión, actualización y gobierno.

El objetivo no es trasladar toda la computación al *edge*, sino ubicar cada capacidad donde aporte mayor valor. La arquitectura más robusta será normalmente híbrida: inteligencia local para contexto, rapidez y continuidad; capacidades centrales para entrenamiento, coordinación y visión global.

Diferenciar procesamiento, inferencia y aprendizaje

CAPACIDAD	FUNCIÓN
Computación edge	Filtrar, agregar, contextualizar y ejecutar reglas cerca de la fuente
Inferencia on-edge	Aplicar localmente un modelo entrenado para clasificar, predecir o recomendar
Entrenamiento centralizado	Crear modelos con mayor capacidad computacional e históricos agregados
Adaptación local	Ajustar el modelo al activo, controlando fragmentación y pérdida de rendimiento
Aprendizaje federado	Compartir parámetros entre nodos sin centralizar todos los datos

La combinación más habitual es entrenamiento centralizado e inferencia local. La adaptación y el aprendizaje federado pueden aportar valor cuando existen restricciones de datos o diferencias relevantes entre instalaciones, pero añaden complejidad. Tampoco garantizan por sí mismos privacidad, seguridad o calidad. **Entrenamiento, adaptación e inferencia deben distribuirse según criticidad, conectividad y necesidad operativa**.

Decidir dónde ejecutar cada función

NIVEL	CAPACIDADES ADECUADAS	CRITERIO DOMINANTE
Dispositivo o activo	Adquisición, preprocesamiento, reglas y respuesta inmediata	Latencia mínima y autonomía
Edge industrial	Inferencia, correlación local, imagen y coordinación próxima	Contexto local y reducción de tráfico
Centro de planta o control	Supervisión e integración de varios activos	Coordinación operativa
Centro de datos o *cloud*	Entrenamiento, simulación, analítica transversal y gestión de flotas	Escala y visión global

La ubicación debe valorar tiempo de respuesta, volumen de datos, comunicaciones, consecuencias de una desconexión, recursos computacionales, sensibilidad de la información y mantenimiento de los nodos. Una protección con requisitos estrictos no debería depender de una respuesta remota; una previsión agregada puede beneficiarse de datos procedentes de múltiples instalaciones.

Muchas funciones abarcan varios niveles: el activo filtra; el nodo ejecuta la inferencia; el centro coordina; y una plataforma central entrena nuevas versiones. **Distribuir la inteligencia no debe fragmentar su gobierno**.

Cuando la latencia condiciona la operación

La latencia debe medirse de extremo a extremo: captura, transmisión, preparación, inferencia, generación de la recomendación, comunicación y ejecución. También importa su variabilidad bajo carga, fallos de hardware, pérdida parcial de comunicaciones o competencia por recursos.

Conviene distinguir:

- **Tiempo real estricto**: incumplir el plazo puede comprometer seguridad o estabilidad.
- **Tiempo real operativo**: el resultado debe llegar en segundos o minutos.
- **Procesamiento diferido**: puede realizarse posteriormente sin afectar a la actuación.

La IA exige especial prudencia en bucles de tiempo real estricto. Protección, enclavamientos y seguridad necesitan determinismo, validación y respaldo independiente. En muchos casos, la IA aporta más valor en supervisión, diagnóstico o recomendación que sustituyendo lógicas críticas ya validadas.

Transformar datos en decisiones locales

Un flujo local debe incluir:

1. Captura y sincronización de señales.
2. Comprobación de calidad.
3. Filtrado, agregación y contextualización.
4. Ejecución de reglas y modelos.
5. Generación de alerta, recomendación o acción.
6. Almacenamiento temporal y sincronización posterior.

El contexto —carga, modo de operación, producto, meteorología o configuración— permite distinguir una anomalía de un comportamiento esperado. El nodo también debe saber cuándo no puede decidir: ante datos insuficientes o condiciones fuera del ámbito validado, debe reducir autonomía, solicitar comprobación o activar un modo alternativo.

Las actuaciones pueden ir desde descartar datos irrelevantes y priorizar alarmas hasta recomendar inspecciones o ajustar parámetros dentro de límites autorizados. Su alcance depende de criticidad, confianza y reversibilidad.

Mantener la operación sin conectividad

El *edge* puede sostener supervisión, detección de anomalías, reglas de seguridad, inferencia, almacenamiento temporal y ajustes limitados durante una interrupción. Esta autonomía debe definir:

- Tiempo máximo de operación independiente.
- Capacidades que permanecen disponibles.

- Funciones que se desactivan por falta de contexto.
- Límites aplicables y modo seguro.
- Datos que deben conservarse.
- Información proporcionada al personal.
- Recuperación de conexión y resolución de discrepancias.

La autonomía no equivale a aislamiento indefinido. El nodo debe sincronizar posteriormente datos, eventos y cambios, preservando la trazabilidad de lo ocurrido.

Diseñar y gestionar el *edge* industrial

Temperatura, polvo, vibraciones, humedad, interferencias, espacio y consumo condicionan el nodo industrial. Su diseño debe considerar capacidad de proceso, almacenamiento, aceleración, interfaces, protocolos, redundancia, soporte y observación remota.

Sobredimensionar eleva CAPEX y consumo; infradimensionar genera latencias y limita futuras versiones. La capacidad debe cubrir carga normal, picos, crecimiento y reserva para estados degradados. Modelos ligeros, cuantización o procesamiento selectivo pueden mejorar eficiencia, siempre que no deterioren la decisión.

Cada nodo necesita propietario, inventario, configuración, soporte y sustitución prevista. La gestión de flotas debe controlar:

- Nodo, aplicación, modelo y versión desplegados.
- Compatibilidad y rendimiento.
- Dispositivos desconectados o degradados.
- Distribución progresiva de actualizaciones.
- Reversión y retirada de versiones sin soporte.

El despliegue debe avanzar desde pruebas y *shadow mode* hacia un grupo limitado y una extensión progresiva. El versionado debe incluir modelo, parámetros, transformaciones y reglas; una diferencia de preprocesamiento puede alterar el resultado aunque el algoritmo sea idéntico.

También deben monitorizarse deriva de datos, cambios en la relación entre señales y resultado, nuevos regímenes operativos, degradación de sensores y particularidades locales. Adaptar cada nodo puede mejorar precisión, pero fragmentar la flota. Conviene mantener una base común validada y documentar los parámetros locales.

Mantener al humano dentro de la decisión

Para cada caso de uso debe establecerse:

- Qué decisión puede recomendar o ejecutar.
- Condiciones y límites de actuación.
- Confianza mínima.
- Situaciones que requieren validación humana.
- Procedimiento de escalado y retorno seguro.

La interfaz debe mostrar el estado del nodo y del modelo, calidad de los datos, nivel de confianza, variables determinantes, acción propuesta o ejecutada y posibilidad de detenerla o revertirla. Durante una desconexión, el personal local necesita conocer qué capacidades siguen activas y qué decisiones ha tomado el sistema. **La autonomía tecnológica no puede reducir la visibilidad humana**.

Aplicaciones en infraestructuras y consumo

ÁMBITO	APLICACIONES
Redes y subestaciones	Calidad eléctrica, correlación de eventos, anomalías, alarmas, condición de activos y supervisión local
Renovables y almacenamiento	Vibraciones, imagen térmica, rendimiento, inversores, baterías y filtrado de eventos
Industria, refino y química	Equipos rotativos, consumos, variables de proceso, visión, alarmas y ajustes limitados
Hidrógeno y logística	Electrolizadores, compresores, almacenamiento, bombeos y movimientos
Edificios y demanda flexible	Autoconsumo, baterías, climatización, cargas críticas y respuesta a señales energéticas

El *edge* aporta conocimiento y respuesta local; los entornos centrales coordinan parques, plantas, mercados y carteras. Las funciones de seguridad deben seguir apoyándose en capas específicamente diseñadas y validadas. En el consumo, el procesamiento local permite conservar preferencias y reducir la transferencia de datos detallados.

Construir el *business case*

El análisis debe considerar dispositivos, plataformas, instalación, integración, mantenimiento, consumo energético y gestión de flotas. Los beneficios pueden proceder de reducir comunicaciones y procesamiento central, disminuir latencia, evitar indisponibilidades, mantener operación local y habilitar nuevos casos.

PERFIL	INDICADORES PRINCIPALES
Dirección y negocio	TCO; CAPEX y OPEX por nodo; comunicaciones evitadas; pérdidas evitadas; valor de continuidad; retorno; consumo computacional.
Operación y mantenimiento	Tiempo señal-acción; disponibilidad local; horas sin conectividad; eventos gestionados; alarmas priorizadas; recuperación.
Tecnología y OT	Latencia y variabilidad; datos locales; tráfico reducido; uso de recursos; inventario; despliegue y reversión.
Gobierno de modelos	Precisión por activo; deriva; inferencias fuera de ámbito; versiones obsoletas; actualizaciones revertidas; trazabilidad.

Reducir latencia o tráfico solo genera valor cuando mejora una decisión, preserva continuidad o reduce costes. La financiación para digitalización, redes inteligentes, eficiencia energética e IA puede acelerar el despliegue, que deberá alinearse con ciberseguridad, protección de datos, seguridad industrial y continuidad.

Una ruta práctica para la inteligencia *on-edge*

NIVEL	PRIORIDADES
1. Procesar y observar	Identificar necesidades de latencia; filtrar y contextualizar datos; almacenar localmente; inventariar nodos.
2. Inferir y recomendar	Desplegar modelos validados; utilizar shadow mode; generar recomendaciones; monitorizar e integrar resultados.
3. Actuar y aprender	Autorizar acciones limitadas; coordinar nodos; controlar adaptación, versiones, deriva y reversión.

Los primeros proyectos deben partir de una necesidad clara de baja latencia, menor tráfico o continuidad local. Implantar *edge* cuando una plataforma central ya cumple los requisitos puede añadir complejidad sin aportar valor.

Infraestructuras capaces de pensar localmente

El crecimiento de activos distribuidos hará difícil mantener arquitecturas completamente centralizadas. La computación *on-edge* acerca respuesta y contexto al activo, pero exige gobernar la flota, controlar versiones y definir límites de autonomía.

El futuro combinará procesamiento central y local. **La inteligencia central aportará escala, entrenamiento y coordinación; la inteligencia local, rapidez, autonomía y continuidad**. El resultado serán infraestructuras capaces de responder cerca del activo sin perder control ni visión integral.

7. Explotación integral de *smart meters*

Convertir los contadores inteligentes en una infraestructura distribuida de información, participación y flexibilidad para un sistema energético más eficiente

Electrificación, renovables, autoconsumo, almacenamiento, movilidad eléctrica y nuevos consumos están transformando la relación entre generación, red y demanda. Comprender cómo, cuándo y dónde se consume resulta esencial para anticipar picos, detectar restricciones, aprovechar excedentes y movilizar cargas adaptables.

Los contadores inteligentes conforman una extensa red de captura de información, pero su uso se ha concentrado en telemedida, facturación y gestión administrativa. El reto es evolucionar desde la infraestructura de medición avanzada o AMI hacia un ecosistema que convierta lecturas en **información comprensible, actuaciones verificables y valor compartido**.

El consumidor debe ocupar una posición central: necesita conocer qué beneficio obtendrá, qué consumos se modificarán, qué límites conservará y cómo se calculará el resultado.

Del contador a una cadena de valor

Una arquitectura AMI integra contadores, comunicaciones, sistemas de recogida, plataformas de gestión de datos de medida, validación, facturación, analítica e interfaces

para consumidores y agregadores. El contador mide, pero normalmente no controla una cámara frigorífica, la climatización o la recarga de un vehículo. Para activar flexibilidad debe conectarse con sistemas de gestión energética, BMS, controladores o plataformas capaces de actuar.

La cadena completa debe:

1. Medir con frecuencia y calidad suficientes.
2. Validar y contextualizar la lectura.
3. Comprender el comportamiento.
4. Identificar ahorro o flexibilidad.
5. Comunicar una recomendación.
6. Actuar sobre el consumo.
7. Verificar el resultado.
8. Calcular y distribuir el beneficio.

Si una etapa falla, la infraestructura puede generar datos sin producir decisiones. **El éxito debe medirse por el valor capturado, no por el número de contadores desplegados**.

Comprender el comportamiento con la granularidad adecuada

Los perfiles temporales permiten identificar cargas base, consumos fuera de horario, picos, anomalías y margen de adaptación.

La frecuencia debe responder a la decisión. Datos horarios o cuartohorarios pueden bastar para facturación, previsión y algunos servicios de flexibilidad; diagnosticar transitorios o equipos concretos exige mayor frecuencia y submedida. Para una pyme, combinar el contador general con *submetering*, sensórica o gestión energética puede convertir una señal agregada en una actuación concreta.

Capturar más detalle del necesario eleva comunicaciones, almacenamiento y gobierno. **La granularidad óptima es la mínima que permite mejorar la decisión prevista**.

Garantizar la calidad y el contexto del dato

Previsiones, recomendaciones y liquidaciones dependen de lecturas fiables. La gestión debe contemplar:

- Sincronización temporal e identificación del punto.
- Datos ausentes, duplicados o fuera de rango.
- Estimación controlada y registro de correcciones.
- Relación con contratos, tarifas, instalaciones y activos.
- Trazabilidad desde la lectura original hasta el indicador.

Los procesos de validación, estimación y edición deben distinguir datos reales y calculados, especialmente cuando intervienen facturación o remuneración. También deben reconocer cambios estructurales —autoconsumo, baterías, vehículos o ampliaciones productivas— para no interpretarlos como anomalías. La calidad es una capacidad continua con indicadores y responsables.

Identificar la flexibilidad real

No todo consumo puede desplazarse. Para cada carga debe determinarse:

- Potencia modificable, duración y tiempo de activación.
- Frecuencia de uso y recuperación posterior.

- Impacto sobre producción, confort, calidad o servicio.
- Capacidad de automatización.
- Compensación mínima esperada.

Debe considerarse el **efecto rebote**: reducir una carga puede exigir un consumo posterior para recuperar temperatura, presión, producción o almacenamiento.

También conviene diferenciar potencia interrumpida y energía evitada. Una reducción breve puede aliviar una congestión aunque el consumo total apenas cambie; otras actuaciones buscan disminuir energía, coste o emisiones.

Convertir al consumidor en participante activo

La medida inteligente debe traducirse en recomendaciones accionables. Una curva de consumo no siempre facilita actuar: es necesario indicar qué carga modificar, cuándo hacerlo, qué impacto tendrá y qué beneficio se espera.

La actuación puede ser manual, recomendada o automatizada. El usuario debe conservar preferencias y límites sobre temperatura, disponibilidad del vehículo, producción, cargas críticas o reserva de batería. **La automatización será aceptada si resulta comprensible, reversible y económicamente visible**.

Cuantificar y verificar el beneficio

No existe un porcentaje universal de ahorro. El valor depende del perfil, la tarifa, el equipamiento y la capacidad de actuación:

FUENTE	CÁLCULO ORIENTATIVO	VARIABLES
Desplazamiento	Energía trasladada × diferencia de precio	Periodos, pérdidas y rebote
Reducción de picos	Potencia evitada × coste aplicable	Duración y tarifa
Autoconsumo	Energía propia adicional × valor neto	Producción, consumo y almacenamiento
Eficiencia	Energía evitada × coste marginal	Actividad y condiciones equivalentes
Flexibilidad	Remuneración menos costes asociados	Potencia, duración, frecuencia e impacto
Anomalías evitadas	Coste esperado evitado	Probabilidad, consecuencia y detección
Almacenamiento	Valor carga-descarga menos pérdidas	Precio, eficiencia, ciclos y degradación

El beneficio neto debe descontar medida, automatización, integración, mantenimiento, pérdidas, degradación e impacto productivo o sobre el confort. Conviene mostrar escenarios conservador, esperado y de alta utilización, junto con sensibilidad a precios, activaciones y rebote.

Una línea de base verificable estima qué habría consumido el usuario sin actuación mediante históricos comparables, meteorología, horarios, producción, ocupación, autoconsumo y cambios estructurales. Después deben medirse potencia modificada, energía desplazada, recuperación, límites respetados y beneficio bruto y neto. **Medición y verificación permiten liquidar correctamente y demostrar el valor real al consumidor**.

IA, automatización y agregación

La IA puede facilitar previsión hiperlocal, segmentación de perfiles, detección de anomalías, estimación de líneas de base, identificación de flexibilidad y recomendaciones personalizadas. Los modelos deben diferenciar anomalías de cambios legítimos y explicar qué datos utilizan y cómo calculan referencias y compensaciones.

La flexibilidad coordina tres capas:

- **Medición**: confirma qué ha ocurrido.
- **Control**: modifica el comportamiento de la carga.
- **Agregación**: combina recursos hasta construir una capacidad utilizable.

El agregador necesita conocer capacidad, restricciones, tiempo de activación, fiabilidad, localización, compensación y efecto rebote. La ubicación es relevante: dos recursos idénticos pueden aportar distinto valor según las restricciones locales de red. La inteligencia local puede respetar preferencias del usuario, mientras una plataforma central coordina el conjunto.

Incorporar una visión multienergía

Industrias, edificios y territorios consumen electricidad, gas, agua, calor, frío y nuevos vectores como hidrógeno o biometano. Relacionar estas medidas permite identificar sustituciones, optimizar electricidad y calor, gestionar almacenamiento y planificar electrificación.

Cada vector mantiene unidades, frecuencias, calidad y posibilidades de actuación diferentes. Un modelo común de activos, puntos de medida, ubicación y tiempo debe relacionarlos sin borrar su significado físico. Reducir electricidad puede aumentar calor o combustible en otro proceso; la optimización debe considerar el balance completo.

Gobernar acceso, privacidad y confianza

Los datos pueden revelar horarios, procesos, ocupación o hábitos. El consumidor debe conocer:

- Datos recogidos, granularidad y finalidad.
- Actores autorizados y periodo de conservación.
- Beneficio esperado y cálculo de compensaciones.
- Preferencias, revisión y reclamación disponibles.

Medida, cálculo, activación y liquidación necesitan responsabilidades claras cuando participan distribuidores, comercializadores, agregadores y proveedores tecnológicos. La arquitectura debe alinearse con protección de datos, medida, mercados y derechos del consumidor. **Sin transparencia, beneficio comprensible y control, disminuirá la participación y la flexibilidad disponible**.

Medir el valor para cada participante

PERFIL	INDICADORES PRINCIPALES
Consumidores y pymes	Ahorro por actividad; energía y picos reducidos; autoconsumo; compensaciones; retorno; impacto operativo o sobre confort.
Operadores y distribuidores	Precisión de demanda; flexibilidad disponible; congestiones; capacidad liberada; activaciones verificadas; refuerzos aplazados.
Agregadores y comercializadores	Recursos activos; potencia prevista y entregada; fiabilidad; coste de adquisición; retención; valor distribuido.
Tecnología y datos	Cobertura; lecturas ausentes o estimadas; latencia; contexto; integraciones; trazabilidad; coste por punto.

Los indicadores deben mostrar el valor agregado y su distribución. Un programa puede beneficiar al sistema y fracasar si el consumidor recibe una compensación insuficiente o soporta un impacto mayor del previsto.

Una ruta práctica para capturar valor

NIVEL	PRIORIDADES
1. Medir y comprender	Validar datos; relacionar consumo y actividad; identificar cargas, picos y anomalías; recomendar.
2. Actuar y ahorrar	Incorporar submedida y control; desplazar consumos; reducir picos; optimizar autoconsumo y almacenamiento.
3. Agregar y aportar flexibilidad	Caracterizar recursos; definir límites; automatizar activaciones; verificar, liquidar y coordinar vectores.

Las pymes pueden comenzar por consumos fuera de horario, picos evitables, climatización, recarga y autoconsumo. Los resultados iniciales permiten justificar automatización, almacenamiento o participación avanzada. La financiación para eficiencia, autoconsumo, movilidad y gestión de demanda puede reducir barreras, siempre según programas vigentes.

Del dato distribuido a la flexibilidad compartida

Los contadores inteligentes pueden convertir millones de puntos de consumo en una infraestructura para observar demanda, anticipar restricciones y coordinar recursos. Su valor reside en las decisiones que habilitan.

La cadena debe conectar medida, contexto, inteligencia, automatización y verificación, con el consumidor en el centro. Cuando se completa, el contador deja de ser una herramienta administrativa y se convierte en **un punto distribuido de inteligencia que informa, facilita actuaciones y demuestra el valor de una demanda más flexible y eficiente.**

.

8. Seguridad y responsabilidad del Consejo (NIS2)

Convertir la ciberseguridad de las infraestructuras energéticas en una prioridad de continuidad operativa, resiliencia y gobernanza empresarial

La integración IT-OT, el mantenimiento prescriptivo, la virtualización, la inteligencia *on-edge* y la explotación del dato amplían la superficie digital de infraestructuras diseñadas originalmente para operar aisladas. Una vulnerabilidad puede provocar pérdida de visibilidad, alteración de consignas, indisponibilidad del control y consecuencias sobre producción, suministro, personas o medioambiente.

La seguridad debe evolucionar desde la protección de sistemas hacia la **gestión del riesgo ciberfísico**: detectar, contener, operar temporalmente en condiciones degradadas y recuperar el servicio con seguridad.

NIS2 sitúa este riesgo dentro de la gobernanza empresarial. Su artículo 20 establece que los órganos de dirección de las entidades esenciales e importantes deben aprobar las medidas de gestión del riesgo, supervisar su aplicación y recibir formación suficiente para comprender su impacto. Los equipos técnicos implantan las medidas; el Consejo debe conocer la exposición, priorizar inversiones y aceptar conscientemente el riesgo residual.

Del riesgo digital al riesgo ciberfísico

La superficie incluye SCADA, PLC, RTU, relés, sensores, nodos *edge*, historiadores, aplicaciones virtualizadas, accesos remotos e integraciones IT-OT. Una credencial comprometida o una configuración incorrecta pueden afectar a una función crítica, aunque el incidente no utilice técnicas sofisticadas.

El riesgo debe expresarse mediante consecuencias sobre:

- Visibilidad y control de los activos.
- Continuidad de producción y suministro.
- Seguridad de personas y medioambiente.
- Integridad, calidad y trazabilidad.
- Coste y tiempo de recuperación.

El anexo I de NIS2 incluye actividades de electricidad, calefacción y refrigeración urbanas, petróleo, gas e hidrógeno. La aplicación concreta depende de los criterios regulatorios y de la transposición nacional, pero confirma que la ciberresiliencia requiere una visión multienergía. Las interdependencias con electricidad, agua, comunicaciones, transporte y proveedores digitales deben formar parte de la evaluación.

El Consejo gobierna el riesgo

El Consejo no necesita seleccionar herramientas ni gestionar incidentes técnicos. Debe asegurar que la organización conoce sus funciones críticas, adopta medidas proporcionadas, asigna recursos y comprueba su eficacia.

Debería poder responder:

- Qué servicios son esenciales y qué activos los sostienen.
- Qué escenarios pueden interrumpirlos y cuál sería su impacto.
- Qué capacidad existe para detectar, contener y recuperar.
- Qué funciones pueden operar en modo degradado.

- Qué riesgos y terceros críticos permanecen sin tratar.
- Quién tiene autoridad durante una crisis.
- Qué pruebas demuestran que las medidas funcionan.

El cuadro de mando debe traducir controles técnicos a evidencia de negocio:

DIMENSIÓN	PREGUNTA DE GOBIERNO	EVIDENCIA
Exposición	¿Qué funciones pueden verse afectadas?	Activos, dependencias y escenarios
Protección	¿Qué reduce la probabilidad?	Cobertura y eficacia de medidas
Detección	¿Cuánto tardaríamos en identificarlo?	Visibilidad, tiempos y pruebas
Contención	¿Podemos limitar la propagación?	Segmentación y procedimientos
Continuidad	¿Qué seguiría funcionando?	Modos degradados y alternativas
Recuperación	¿Cómo volveríamos a operar?	RTO, RPO, copias y ejercicios
Riesgo residual	¿Qué aceptamos conscientemente?	Impacto, probabilidad y aprobación

La información debe actualizarse cuando cambia la arquitectura, aparece una vulnerabilidad crítica o se incorpora un proveedor relevante.

Traducir el riesgo a impacto y business case

La evaluación debe partir de escenarios como pérdida de supervisión, indisponibilidad de telecontrol, alteración de datos, bloqueo de mantenimiento, compromiso de un proveedor o propagación desde IT hacia OT.

Para cada escenario conviene estimar activos afectados, duración, producción o suministro perdido, recuperación, daños, consecuencias regulatorias y contractuales e impacto sobre personas y clientes. Los eventos extremos deben analizarse mediante pruebas de estrés, aunque su probabilidad sea baja.

La inversión puede compararse con pérdidas evitadas, menor alcance del incidente, reducción del tiempo de recuperación, capacidad preservada y exposición regulatoria mitigada. **El *business case* debe construirse sobre continuidad y riesgo, no únicamente sobre ahorro tecnológico**.

Utilizar NIS2 como palanca de modernización

El artículo 21 de NIS2 contempla medidas técnicas, operativas y organizativas relacionadas con incidentes, continuidad, recuperación, cadena de suministro, desarrollo seguro, evaluación de eficacia, formación, control de acceso y gestión de activos.

Estas exigencias pueden acelerar la identificación de activos sin soporte, la reducción de conectividad innecesaria, la integración controlada IT-OT, la recuperación de configuraciones y la trazabilidad de cambios. El cumplimiento debe evolucionar por cuatro niveles:

- **Cumplimiento formal**: existe una política.
- **Capacidad implantada**: la medida funciona técnicamente.
- **Capacidad operativa**: las personas saben utilizarla.
- **Resiliencia demostrada**: se ha probado en un escenario representativo.

El objetivo es alcanzar el último nivel y relacionar cada medida con una función crítica.

Conocer, segmentar y controlar accesos

El inventario debe incluir activos *IT*, *OT*, *IoT* y *edge*; *software* y configuraciones; comunicaciones; accesos; servicios externos; identidades; certificados; modelos de IA y proveedores. Debe relacionar cada elemento con su propietario, criticidad, soporte y recuperación. En OT, la observación pasiva puede resultar preferible a técnicas activas.

La segmentación limita la propagación y debe diferenciar entornos corporativos y operativos, zonas de criticidad, funciones de supervisión y control, activos de terceros, sistemas heredados y entornos de prueba. Cada flujo autorizado necesita origen, destino, justificación, responsable, registro y revisión. **La segmentación debe reflejar el proceso físico, no solo la topología informática**.

Los accesos internos y de terceros deben utilizar identidades individuales, privilegios mínimos, autorización temporal, canales controlados, registro y revocación. Las cuentas compartidas y accesos permanentes dificultan atribuir acciones y retirar permisos. El principio Zero Trust debe adaptarse a disponibilidad y latencia OT, evitando confianza permanente por ubicación en la red.

Detectar, contener y operar en degradado

La detección debe combinar comunicaciones, registros, identidades, configuraciones, variables físicas y contexto operativo. Correlacionar una orden inesperada con un cambio de configuración y una alteración del proceso aporta más valor que observar cada señal aisladamente. El SOC necesita conocimiento OT y colaboración con operadores e ingenieros.

La automatización y la IA pueden reducir ruido y acelerar la detección, pero las respuestas capaces de afectar al proceso requieren validación proporcional al riesgo.

Ante un incidente puede ser necesario:

- Aislar activos o zonas.
- Deshabilitar accesos.
- Transferir funciones.
- Reducir capacidad y priorizar servicios.
- Operar localmente o mediante procedimientos manuales.
- Detener un proceso de forma segura.

Estas decisiones deben estar ensayadas. Los procedimientos necesitan criterios de declaración, autoridad técnica y operativa, funciones que preservar, coordinación IT-OT, comunicación, notificación y condiciones de recuperación.

Recuperar el proceso completo

Una copia de seguridad no garantiza la recuperación. En OT debe reconstruirse hardware o plataforma, aplicaciones, configuración, lógica de control, datos, comunicaciones, identidades, certificados y dependencias, verificando la seguridad antes de reconectar.

La estrategia debe definir RTO, RPO, copias protegidas, configuraciones críticas, repuestos, plataformas alternativas y secuencia de restauración. Los simulacros de mesa revisan decisiones; las pruebas técnicas demuestran restauración; y los ejercicios integrales verifican la recuperación del servicio.

La crisis requiere responsabilidades previas sobre dirección, investigación, operación, continuidad, coordinación jurídica, comunicación y proveedores. El Consejo supervisa impacto, prioridades y recursos, sin interferir en decisiones técnicas ya asignadas. La formación debe adaptarse a dirección, operadores, equipos técnicos y personal general.

Evaluar eficacia, no existencia

La madurez debe comprobarse mediante restauraciones, simulacros, ejercicios, revisión de accesos, validación de segmentación y auditorías. Cada prueba debe identificar qué se esperaba, qué ocurrió, qué decisiones se retrasaron y qué dependencias o información faltaron.

Los hallazgos necesitan responsable, plazo y seguimiento. Repetir ejercicios sin cerrar acciones crea una falsa percepción de preparación. La eficacia también debe revisarse al virtualizar funciones, desplegar IA, incorporar *edge* o cambiar proveedores.

Medir la ciberresiliencia

PERFIL	INDICADORES PRINCIPALES
Consejo y alta dirección	Riesgo económico; escenarios fuera de apetito; riesgos sin tratamiento; inversiones; incidentes operativos; terceros críticos; riesgo residual.
Dirección y negocio	Coste de interrupción y recuperación; producción expuesta; CAPEX y OPEX; pérdidas evitadas; exposición contractual y regulatoria.
Operación y mantenimiento	Funciones en modo degradado; tiempo de aislamiento y recuperación; capacidad preservada; procedimientos manuales; accesos remotos.
Ciberseguridad, IT y OT	Inventario y monitorización; detección, contención y recuperación; segmentación; activos sin soporte; copias verificadas; RTO y RPO.

Los indicadores deben mostrar tendencia, objetivo y contexto. Reducir el número total de vulnerabilidades aporta poco si permanecen abiertas las que afectan a funciones críticas.

Una ruta práctica hacia la ciberresiliencia

NIVEL	PRIORIDADES
1. Conocer y proteger	Identificar funciones y dependencias; gobernar accesos; reducir conectividad; proteger configuraciones; asignar responsables.
2. Detectar, contener y recuperar	Mejorar visibilidad IT-OT; segmentar; correlacionar eventos; definir degradados, RTO y RPO; probar la respuesta.
3. Gobernar y mejorar	Cuantificar riesgo; integrar terceros; evaluar eficacia; cerrar acciones; actualizar exposición; supervisar desde el Consejo.

La financiación para ciberseguridad, resiliencia y modernización puede acelerar medidas, pero no sustituye la responsabilidad de adoptarlas. Las referencias deberán

revisarse antes de la publicación para reflejar la normativa nacional, autoridades y requisitos aplicables vigentes.

De proteger sistemas a preservar la operación

Una organización ciberresiliente conoce qué funciones sostienen el servicio, limita vías de propagación, detecta comportamientos anómalos, prepara estados degradados y demuestra que puede recuperarse.

NIS2 refuerza la responsabilidad del Consejo de aprobar y supervisar las medidas y comprender el riesgo. **El objetivo no es prometer que nunca habrá un incidente, sino contenerlo, preservar las funciones esenciales y recuperar la operación dentro de límites aceptables**. Proteger el dato importa; mantener la capacidad de producir, distribuir y decidir resulta esencial.

9. Protección del «eslabón más débil» de la cadena

Reforzar la resiliencia del sistema energético mediante capacidades mínimas, proporcionadas y verificables en proveedores, pymes e industria auxiliar

Una organización puede disponer de sistemas OT monitorizados y procedimientos sólidos de continuidad, pero seguir expuesta a través de un proveedor remoto, un integrador que conserva configuraciones críticas, un fabricante sin capacidad de actualización o una empresa auxiliar cuya indisponibilidad paraliza la operación.

El perímetro efectivo ya no coincide con los límites de la organización: incluye a todos los actores, productos y servicios capaces de afectar a una función crítica. La expresión «eslabón más débil» no identifica automáticamente a pymes o proveedores pequeños. El riesgo aparece cuando **las capacidades de protección y recuperación no se corresponden con la criticidad de la función**.

El objetivo es construir un mínimo común de resiliencia. Los operadores deben exigir capacidades proporcionadas y verificables, pero también facilitar criterios, herramientas y acompañamiento. La resiliencia de la cadena es una responsabilidad compartida.

Extender el perímetro a toda la cadena

Fabricantes, integradores OT, mantenedores, plataformas, servicios *cloud*, comunicaciones, ingenierías, logística y contratistas introducen dependencias diferentes. Para evaluar su riesgo deben analizarse cuatro dimensiones:

- **Acceso**: sistemas, datos o instalaciones que pueden alcanzar.
- **Impacto**: consecuencias de un error, compromiso o indisponibilidad.
- **Sustituibilidad**: tiempo y esfuerzo necesarios para reemplazarlos.
- **Concentración**: funciones o entidades dependientes del mismo actor o producto.

Un proveedor sin acceso técnico puede resultar crítico si suministra un componente difícil de sustituir; otro con acceso limitado puede representar un riesgo elevado si puede modificar una función de control.

El análisis debe alcanzar software, bibliotecas, componentes, subcontratistas, soporte, plataformas, herramientas remotas, identidades y mecanismos de actualización. NIS2

incorpora la seguridad de la cadena de suministro entre las medidas de gestión del riesgo y exige considerar las prácticas y vulnerabilidades de proveedores directos.

Clasificar según el riesgo real

Aplicar los mismos requisitos a todos genera costes y desvía atención. El seguimiento debe adaptarse a criticidad, acceso e impacto:

NIVEL	CARACTERÍSTICAS	SEGUIMIENTO
Bajo	Sin acceso crítico y fácilmente sustituible	Requisitos básicos y revisión contractual
Medio	Acceso limitado o dependencia moderada	Evaluación periódica y controles específicos
Alto	Acceso privilegiado, soporte OT o impacto relevante	Validación técnica, supervisión y pruebas
Crítico	Puede afectar a seguridad, continuidad o varias instalaciones	Gobierno conjunto, contingencia y seguimiento ejecutivo

La evaluación debe incorporar privilegios, datos tratados, duración de la conexión, soporte, actualizaciones, sustitución, subcontratistas y concentración. Debe revisarse cuando cambia el alcance del servicio, no únicamente al contratar.

Definir responsabilidades compartidas

ACTOR	RESPONSABILIDADES PRINCIPALES
Operador o contratante	Clasificar la función, limitar accesos, definir requisitos y supervisar el riesgo
Proveedor	Proteger sistemas, personas y credenciales; comunicar incidentes y cambios
Fabricante	Mantener soporte, gestionar vulnerabilidades y ofrecer actualizaciones fiables
Integrador	Documentar configuraciones, dependencias, cambios y reversión
Mantenedor	Utilizar accesos autorizados y preservar la trazabilidad
Subcontratista	Cumplir los requisitos trasladados por el proveedor principal
Dirección	Aceptar el riesgo residual y asignar recursos

Contratar un servicio no transfiere completamente el riesgo. Antes de una crisis debe estar claro quién detecta, comunica y contiene; quién revoca accesos; qué registros estarán disponibles; y cómo se recuperará el servicio.

Un mínimo viable de resiliencia para pymes

Una pyme no necesita reproducir la arquitectura de una gran *utility*, pero sí disponer de capacidades básicas:

CAPACIDAD	ACTUACIONES MÍNIMAS
Conocer	Inventariar equipos, aplicaciones, versiones, accesos, responsables y dependencias
Controlar accesos	Utilizar identidades individuales, privilegios mínimos, autenticación reforzada y revisiones
Separar lo esencial	Diferenciar IT y OT, limitar conexiones, aislar legado y controlar dispositivos externos
Recuperar	Proteger datos y configuraciones, probar restauraciones e identificar repuestos críticos
Mantener	Conocer soporte, vulnerabilidades, actualizaciones y fin de vida
Responder	Definir contactos, escalado, revocación, registro, comunicación y prioridades
Formar	Proteger credenciales, reconocer fraude, gestionar accesos y comunicar anomalías

La prioridad debe comenzar por los activos y conexiones que relacionan a la pyme con operaciones críticas de sus clientes.

Hacer seguro el mantenimiento remoto

El acceso remoto debe responder a una intervención concreta:

1. Solicitar y autorizar el trabajo.
2. Identificar al técnico y el alcance.
3. Habilitar acceso temporal.
4. Supervisar o registrar la actividad.
5. Cerrar la sesión y revocar privilegios.
6. Documentar los cambios.

Las conexiones permanentes necesitan justificación expresa. Cuando sean imprescindibles, conviene separar observación y modificación y detectar comportamientos anómalos. La organización debe conocer identidad, dispositivo de origen, activos accesibles, acciones permitidas y forma de revocar el acceso durante una emergencia.

Incorporar seguridad desde la contratación

Antes de contratar deben evaluarse función, criticidad, acceso, arquitectura, soporte, vulnerabilidades, actualizaciones, subcontratistas, recuperación, portabilidad y salida. El contrato debe establecer de manera proporcionada:

- Requisitos mínimos y accesos permitidos.
- Comunicación de incidentes.
- Gestión de vulnerabilidades y actualizaciones.
- Registros y evidencias.
- Continuidad y recuperación.

- Uso de subcontratistas.
- Finalización, transferencia y revocación.

Las cláusulas deben ser ejecutables. Exigir notificaciones sin contactos operativos o auditorías ilimitadas a una pyme crea obligaciones formales sin reducir riesgo. Al finalizar el contrato deben recuperarse datos y activos, transferir conocimiento y eliminar dependencias ocultas.

La seguridad también abarca el ciclo de vida del producto. Deben conocerse soporte, comunicación de vulnerabilidades, origen de actualizaciones, componentes, exportación de configuraciones y migración. Una SBOM puede aportar visibilidad sobre dependencias, pero no sustituye la gestión del riesgo.

En OT, parchear sin validar puede comprometer disponibilidad; no hacerlo mantiene exposición. Se necesitan pruebas, ventanas, medidas compensatorias y reversión. La imposibilidad de mantener un producto genera una **deuda tecnológica que debe incorporarse al *business case***.

Acompañar y financiar la mejora

Imponer requisitos complejos sin apoyo puede producir respuestas documentales alejadas de la capacidad real. Las grandes empresas pueden ofrecer guías, arquitecturas de referencia, modelos de acceso, formación, plantillas de respuesta y evaluaciones orientadas a la mejora.

También pueden facilitar servicios compartidos de monitorización, identidades, copias, recuperación, intercambio de información o laboratorios de actualización.

Para una pyme, el *business* case debe relacionar la inversión con continuidad, conservación de clientes, acceso a cadenas exigentes, recuperación y digitalización segura. Las ayudas, programas sectoriales, cofinanciación, servicios comunes o contratos plurianuales pueden reducir barreras. **El coste no debe excluir a proveedores especializados ni justificar exposiciones incompatibles con la criticidad**.

Una cadena multienergía y una respuesta conjunta

Electricidad, refino, química, gas, hidrógeno, biocombustibles, agua y logística comparten fabricantes, integradores, plataformas y mantenedores. Evaluar cada vector de forma aislada puede ocultar concentraciones y puntos únicos de dependencia.

Cuando un incidente afecta a proveedor y clientes, los planes conjuntos deben definir:

- Contactos y canales alternativos.
- Información mínima que compartir.
- Autoridad para revocar accesos.
- Preservación de registros.
- Recuperación y validación del servicio.
- Coordinación con otros clientes y autoridades.

Los resultados de ejercicios e incidentes deben traducirse en causas, acciones correctoras, responsables y seguimiento.

Medir el progreso

PERFIL	INDICADORES PRINCIPALES
Pymes y proveedores	Activos inventariados; accesos autorizados; autenticación; copias probadas; sistemas sin soporte; formación; comunicación de incidentes.
Operadores	Proveedores clasificados y evaluados; accesos externos; dependencias sin alternativa; riesgos pendientes; revocación; ejercicios conjuntos.
Dirección financiera y compras	Exposición por proveedor; concentración; coste de sustitución; inversión; pérdidas evitadas; contratos con responsabilidades definidas.

Los indicadores deben impulsar mejoras, no limitarse a excluir. Un proveedor que reconoce carencias y ejecuta un plan puede representar menos riesgo que otro con certificaciones, pero sin visibilidad sobre accesos y dependencias.

Una ruta hacia la resiliencia compartida

NIVEL	PRIORIDADES
1. Conocer y controlar	Identificar proveedores críticos; inventariar accesos y dependencias; clasificar; fijar mínimos; definir contactos.
2. Verificar y acompañar	Solicitar evidencias; construir planes; probar accesos, copias y respuesta; formar; incorporar requisitos contractuales.
3. Fortalecer el ecosistema	Realizar ejercicios conjuntos; compartir información; crear servicios comunes; identificar concentraciones; cofinanciar mejoras.

El primer objetivo es que ningún actor conectado a una función crítica carezca de capacidades básicas para conocer, controlar y recuperar su entorno.

La resiliencia se construye desde el conjunto

La continuidad energética depende de grandes infraestructuras y de miles de empresas que las diseñan, fabrican, mantienen y conectan. Proteger únicamente al actor de mayor tamaño deja abiertas dependencias capaces de afectar al sistema.

Las pymes y la industria auxiliar son parte de la solución. Necesitan requisitos proporcionados, rutas prácticas y acompañamiento. **El sistema no será resiliente por el nivel del actor más avanzado, sino por la capacidad colectiva para impedir que una debilidad local se convierta en una interrupción sistémica**.

10. Convergencia cultural IT-OT y rediseño operativo mediante business cases sólidos

Transformar procesos, responsabilidades y flujos de decisión para que la digitalización permita operar con mayor agilidad, conocimiento y control

La modernización energética exige que IT y OT coordinen IA, analítica, virtualización, computación *edge*, sensórica y plataformas de datos. Sin embargo, conectar sistemas no garantiza mejores decisiones. Una plataforma puede integrar información y continuar generando poco valor si el operador debe reconstruir el contexto, resolver contradicciones o esperar autorizaciones imprecisas.

El reto es rediseñar cómo se detecta e interpreta una situación, qué alternativas se consideran, quién decide y cómo se actúa. La tecnología debe reducir el esfuerzo previo a la decisión sin trasladar la velocidad del entorno digital a funciones críticas sin garantías.

La convergencia requiere un modelo común donde disponibilidad, seguridad física, dato, ciberseguridad, eficiencia e innovación formen parte de la misma decisión. El business case debe medir tiempos, errores, utilización de activos, conocimiento preservado y riesgo evitado, no únicamente plataformas instaladas.

Comenzar por el proceso, no por la arquitectura

Un proceso puede contener datos dispersos, alarmas sin priorizar, comprobaciones manuales, hojas de cálculo, autorizaciones informales, conocimiento individual y órdenes de trabajo desconectadas. Digitalizarlo sin revisarlo traslada la fragmentación a herramientas nuevas.

La pregunta inicial debe ser:

¿Qué decisión necesita mejorar la organización y qué impide tomarla con mayor rapidez y calidad?

A partir de ella se identifican datos, sistemas, personas y autorizaciones. La arquitectura se convierte así en habilitadora del proceso objetivo.

Comprender las diferencias entre IT y OT

DIMENSIÓN	PRIORIDAD HABITUAL EN IT	PRIORIDAD HABITUAL EN OT
Cambio	Evolución y actualización frecuente	Estabilidad y cambios controlados
Disponibilidad	Recuperación de aplicaciones	Continuidad del proceso físico
Seguridad	Confidencialidad, integridad y disponibilidad	Seguridad física, disponibilidad e integridad
Vida útil	Años	Décadas
Pruebas	Entornos más fáciles de replicar	Condiciones difíciles de reproducir
Impacto del fallo	Pérdida de información o servicio	Parada, daño físico o riesgo para personas
Datos	Explotación transversal	Contexto específico del proceso
Automatización	Eficiencia y reducción de tareas	Comportamiento determinista y seguro

Estas diferencias responden a las funciones de cada entorno. El conflicto aparece cuando IT interpreta la prudencia como resistencia y OT percibe que se subestima el riesgo. La convergencia debe construir objetivos compartidos: continuidad, menor riesgo, visibilidad, eficiencia, evolución y control.

Mapear y rediseñar la decisión

El flujo real puede diferir del procedimiento documentado. Conviene seguir la decisión completa:

1. Detección del evento.
2. Contextualización de la información.
3. Diagnóstico.
4. Comparación de alternativas.
5. Autorización.
6. Ejecución.
7. Verificación.
8. Aprendizaje.

En cada fase deben medirse personas, sistemas, tiempos, traspasos, datos manuales, excepciones, errores y dependencia de conocimiento individual. Así se obtiene la **latencia de decisión**: una anomalía puede detectarse en segundos y tardar horas en resolverse por falta de contexto o autoridad.

El proceso rediseñado debe:

1. Identificar activo, contexto y criticidad.
2. Relacionar históricos, estado y dependencias.
3. Priorizar mediante reglas o IA.
4. Generar alternativas y consecuencias.
5. Facilitar validación y autorización.
6. Ejecutar dentro de límites definidos.
7. Registrar el resultado y realimentar el sistema.

La automatización no debe replicar cada paso. Una autorización sin valor sigue retrasando aunque sea digital; una comprobación duplicada debe eliminarse. **El objetivo es reducir complejidad sin retirar controles necesarios**.

Establecer la interacción entre persona y tecnología

NIVEL	PAPEL DE LA TECNOLOGÍA	PAPEL HUMANO
Información	Reúne y contextualiza datos	Interpreta y decide
Priorización	Clasifica eventos y urgencias	Revisa y asigna atención
Recomendación	Propone alternativas	Acepta, modifica o rechaza
Ejecución supervisada	Prepara o inicia la acción	Autoriza su ejecución
Automatización condicionada	Actúa dentro de límites	Supervisa excepciones
Retorno seguro	Reduce autonomía ante incertidumbre	Recupera el control

El nivel debe responder a criticidad, frecuencia, confianza, reversibilidad y consecuencias, no solo a capacidad técnica. Para cada proceso se definirán acciones recomendables, preparables y ejecutables; límites; confianza mínima; escalado; autoridad final y reversión.

La supervisión debe ser real. Si el operador recibe cientos de recomendaciones y segundos para aprobarlas, su intervención es únicamente formal.

Diseñar para el operador y preservar conocimiento

La interfaz debe presentar situación, activo, criticidad, variables explicativas, calidad del dato, alternativas, impacto, confianza, recomendación y tiempo para decidir. La información se adaptará al perfil: mantenimiento necesita señales y modos de fallo; operación, restricciones y reconfiguración; dirección, coste, riesgo y continuidad.

La explicabilidad debe ser operativa: variables modificadas, condición detectada, precedentes y supuestos. La priorización debe evitar fatiga de alarmas y considerar probabilidad, consecuencia, criticidad y tiempo disponible. Los usuarios deben participar desde el diseño.

La digitalización también debe convertir experiencia individual en capacidad organizativa:

- Documentar criterios y excepciones.
- Registrar decisiones y justificaciones.
- Relacionar incidencias, actuaciones y resultados.
- Incorporar conocimiento a reglas y modelos.
- Crear escenarios para formación.
- Conservar procedimientos manuales.

Cuando un experto modifica una recomendación, el motivo puede revelar datos ausentes o límites incorrectos. El aprendizaje debe ser bidireccional y mantener la capacidad de operar si falla la plataforma.

Definir gobernanza y gestionar capacidades como productos

Cada caso de uso debe asignar propietario del proceso, activo y dato; responsable del modelo y la tecnología; validador operativo; ciberseguridad; usuario autorizado y dirección. Una matriz RACI puede evitar que la responsabilidad quede diluida.

Comités de arquitectura IT-OT, gobierno del dato, revisión de modelos o equipos de producto pueden resolver decisiones recurrentes, siempre que dispongan de autoridad. Crear órganos sin capacidad para priorizar añade demora.

Las capacidades digitales deben gestionarse como productos operativos con responsable, usuarios, hoja de ruta, presupuesto, indicadores, soporte, versiones y mejora continua. El despliegue necesita formación, monitorización, recogida de observaciones, actualización controlada y retirada cuando deje de aportar valor.

La resistencia en OT suele ser racional: una intervención deficiente puede provocar indisponibilidad o riesgo físico. Los primeros despliegues deben abordar problemas concretos, con usuarios implicados, línea de base, criterios de éxito y reversión. El *shadow mode* permite comparar recomendaciones sin actuar y construir confianza.

Al escalar deben separarse componentes comunes —modelos de datos, gobierno, interfaces y validación— de configuraciones y decisiones locales. Una centralización excesiva ignora particularidades; un enfoque completamente local duplica costes y fragmenta el aprendizaje.

Aplicaciones operativas

ÁMBITO	REDISEÑO DE LA DECISIÓN
Redes eléctricas	Correlacionar alarmas, reconstruir topología, estimar suministro afectado, comparar aislamientos y preparar reconfiguraciones
Refino y química	Relacionar desviaciones con equipos, históricos y límites; evaluar impacto energético, productivo y de seguridad
Hidrógeno y multienergía	Integrar precio, renovables, electrolizador, compresión, almacenamiento, demanda, contratos y mantenimiento
Gestión de activos	Conectar condición, criticidad, producción, repuestos, personal, orden de trabajo, autorización y resultado

La autoridad sobre decisiones críticas permanece en el operador salvo escenarios previamente validados para automatización condicionada. El valor procede de reducir diagnóstico, traspasos y decisiones parciales.

Construir el business case alrededor de la decisión

El análisis debe comenzar por frecuencia, tiempo, personas, errores, impacto del retraso y parte mejorable mediante tecnología. Los beneficios pueden incluir:

- Menor tiempo de decisión e indisponibilidad.
- Reducción de errores, reprocesos y tareas manuales.
- Mejor utilización de activos y ahorro energético.
- Producción o margen adicional.
- Riesgo evitado y conocimiento preservado.

Los costes deben incorporar tecnología, integración, calidad de datos, validación, formación, mantenimiento de modelos, soporte, ciberseguridad y cambios organizativos.

Debe compararse la situación actual, la solución y el coste de no actuar. Un proceso manual puede ocultar horas de búsqueda, pérdida de capacidad y dependencia de especialistas. Tras el despliegue, si el tiempo no disminuye, la recomendación no se utiliza o el resultado no mejora, habrá que revisar el proceso o detener la inversión.

Medir el resultado

PERFIL	INDICADORES PRINCIPALES
Dirección y negocio	Coste por decisión; OPEX y CAPEX; ahorro; producción o margen; indisponibilidad y riesgo evitados; retorno; escalabilidad.
Operación y mantenimiento	Tiempos de diagnóstico, decisión y actuación; traspasos; horas de búsqueda; reprocesos; disponibilidad; productividad.
Tecnología y datos	Fuentes integradas; calidad y latencia; trazabilidad; cambios; incidencias; modelos monitorizados; coste de plataforma.
Adopción y gobierno	Usuarios; recomendaciones consultadas, modificadas o rechazadas; decisiones a tiempo; resultados; formación y responsabilidades.

Los indicadores de adopción necesitan contexto. Una aceptación elevada puede mostrar confianza o aprobación automática; una baja puede revelar datos insuficientes o una recomendación mal integrada. **La calidad se demuestra cuando mejora la decisión y el resultado, no cuando desaparece la discrepancia humana**.

Formación, liderazgo y marcos habilitadores

La formación debe ser bidireccional: proceso y activos para IT; datos, arquitectura e IA para OT; y ciberseguridad industrial, interpretación de modelos, cambios, reversión y operación degradada para ambos.

Los perfiles híbridos traducen necesidades operativas en requisitos tecnológicos, sin sustituir a los especialistas. La dirección debe priorizar procesos, resolver conflictos, asignar propietarios y financiar adopción y evolución.

Ciberseguridad, seguridad industrial, IA, protección de datos y continuidad deben integrarse desde el diseño. La financiación vinculada a digitalización, eficiencia energética, modernización, ciberseguridad e IA puede acelerar proyectos cuyo valor operativo ya esté justificado.

Una ruta práctica de convergencia

NIVEL	PRIORIDADES
1. Comprender el proceso	Seleccionar una decisión; mapear personas, datos, sistemas y tiempos; identificar puntos ciegos; definir propietario y línea de base.
2. Integrar y asistir	Reunir información; contextualizar eventos; digitalizar autorizaciones útiles; recomendar; registrar resultados; formar.
3. Rediseñar y automatizar	Eliminar pasos; paralelizar tareas; autorizar automatización condicionada; integrar órdenes y actuación; medir y escalar.

La transformación debe avanzar proceso a proceso. Intentar modificar simultáneamente toda la operación aumenta complejidad y dificulta atribuir resultados.

De integrar sistemas a transformar la operación

La convergencia IT-OT genera valor cuando cambia la forma de trabajar. La tecnología debe ofrecer contexto, alternativas y consecuencias antes de decidir; reducir tareas manuales; ampliar la capacidad de análisis; y preservar la autoridad sobre actuaciones críticas.

La inversión se justifica por su efecto sobre tiempo, disponibilidad, coste, riesgo y productividad, no por la sofisticación de la herramienta. **El éxito no se medirá por los sistemas conectados, sino por la capacidad de detectar antes, comprender mejor, decidir con mayor rapidez y actuar sin perder el control**.

Resultados esperados

La aplicación del decálogo debe traducirse en cambios observables: activos mejor conocidos y preparados para operar ante incidencias, decisiones de mantenimiento y operación mejor fundamentadas, mayor autonomía de las capacidades locales, demanda flexible con beneficios verificables y una ciberresiliencia que alcance a toda la cadena de valor. El resultado buscado es una organización capaz de **digitalizar sus activos energéticos sin perder seguridad, eficiencia ni control sobre las funciones críticas**.

El avance dependerá del estado del parque instalado, la criticidad de cada proceso y la madurez digital de la organización. Aun así, pueden identificarse resultados comunes que deberían hacerse visibles en el diseño de infraestructuras, la gestión de activos, la operación diaria, la contratación y las decisiones de inversión.

Activos más visibles, resilientes y preparados para evolucionar

Las organizaciones deberán conocer qué funciones sostienen la continuidad, qué activos físicos y digitales intervienen en ellas y qué dependencias podrían impedir su operación o recuperación. Esta visión permitirá modernizar con prioridades claras y conservar los equipos que siguen aportando valor sin mantener riesgos ocultos.

El progreso deberá reflejarse en:

- **Inventarios que relacionen activos, funciones críticas, responsables, comunicaciones, proveedores y consecuencias de indisponibilidad**.
- Clasificación de los activos según criticidad, obsolescencia, exposición y potencial de mejora operativa.
- Decisiones justificadas sobre qué mantener, proteger, instrumentar, integrar, virtualizar o sustituir.
- Mayor disponibilidad de datos contextualizados sobre el estado y rendimiento de los equipos.
- Modos degradados definidos y probados, con funciones esenciales y autoridad operativa identificadas.
- Menos puntos únicos de fallo y mayor capacidad de recuperación tras incidencias físicas o digitales.
- Funciones virtualizadas únicamente cuando cumplan los requisitos de disponibilidad, comportamiento temporal y reversión.
- Procedimientos y configuraciones documentados para conservar el conocimiento necesario durante todo el ciclo de vida.

La mejora no se medirá por el número de equipos conectados o sustituidos. Deberá apreciarse en la reducción de dependencias desconocidas, la extensión segura de la vida útil y la capacidad de mantener o recuperar funciones críticas dentro de los límites establecidos.

Mantenimiento y operación basados en decisiones mejor fundamentadas

La inteligencia artificial deberá ayudar a transformar señales físicas en actuaciones útiles. Las alertas se relacionarán con el activo, su modo de operación, el fallo probable y las consecuencias para el conjunto del proceso. La predicción aportará margen para actuar; la prescripción permitirá comparar alternativas reales de intervención.

Entre los resultados esperados se encuentran:

- **Detección de degradaciones con antelación suficiente para planificar una respuesta**, sin trasladar a los operadores un volumen inasumible de alertas.

- Estimaciones de riesgo y vida útil remanente acompañadas de incertidumbre y condiciones de validez.
- Recomendaciones que consideren criticidad, producción, repuestos, personal, ventanas de intervención y seguridad.
- Integración de las propuestas con órdenes de trabajo, autorizaciones y registro de resultados.
- Modelos de simulación contrastados con el comportamiento observado de activos, plantas y redes.
- Escenarios que hagan visibles los compromisos entre coste, margen, disponibilidad, emisiones y utilización de recursos.
- Restricciones físicas y de seguridad incorporadas antes de optimizar una actuación.
- Versiones, datos, recomendaciones y decisiones trazables, con seguimiento del rendimiento y capacidad de reversión.
- Validación humana proporcional al impacto y a la posibilidad de deshacer cada actuación.

La organización deberá comprobar si disminuyen las averías imprevistas, las intervenciones innecesarias y el tiempo necesario para diagnosticar y decidir. Un modelo más preciso solo supondrá un avance si mejora el resultado operativo frente a la práctica anterior.

Procesamiento distribuido con autonomía y control

La capacidad de procesamiento deberá situarse donde resulte útil para cada función. Acercarla al activo permitirá analizar señales de alta frecuencia, responder dentro de la ventana operativa y conservar determinadas capacidades durante una interrupción de las comunicaciones. Los sistemas centrales mantendrán la visión conjunta, la coordinación y el entrenamiento de modelos cuando corresponda.

Esto deberá hacerse visible mediante:

- **Tiempos de respuesta medidos desde la captura de la señal hasta la recomendación o actuación**, incluida su variabilidad en condiciones exigentes.
- Datos filtrados y contextualizados localmente, con una reducción justificada de comunicaciones.
- Funciones esenciales que puedan mantenerse durante periodos de desconexión previamente definidos.
- Límites claros sobre qué puede decidir cada nodo y cuándo debe reducir su autonomía.
- Información accesible para el operador sobre estado del nodo, calidad de los datos, confianza del modelo y acciones realizadas.
- Inventario de nodos, aplicaciones, configuraciones y versiones desplegadas.
- Actualizaciones progresivas, pruebas en modo sombra y procedimientos de retorno ensayados.
- Detección de deriva, diferencias entre instalaciones y fallos de sensores antes de que degraden las decisiones.

El despliegue deberá valorar también el consumo energético, el mantenimiento y la sustitución de los nodos. La autonomía local habrá generado valor cuando preserve continuidad o mejore una decisión sin crear una nueva infraestructura difícil de supervisar.

Demanda más flexible y beneficios verificables para el consumidor

Los contadores inteligentes deberán pasar de proporcionar lecturas para facturación a facilitar información útil sobre consumos, picos, autoconsumo y capacidad de adaptación. Para que esa información produzca resultados, deberá conectarse con sistemas de gestión y actuación y respetar las necesidades de hogares, pymes e industrias.

Los avances esperados incluyen:

- **Lecturas validadas, contextualizadas y trazables**, diferenciando datos reales, estimados y corregidos.
- Granularidad y submedida ajustadas a las decisiones que se pretenden mejorar.
- Identificación de consumos fuera de horario, picos evitables y cargas con capacidad real de adaptación.
- Recomendaciones que indiquen qué actuación realizar, cuándo y con qué beneficio esperado.
- Preferencias y restricciones definidas por el usuario antes de cualquier automatización.
- Recursos flexibles caracterizados por potencia, duración, tiempo de activación, frecuencia y efecto rebote.
- Líneas de base verificables para comparar el consumo real con el que habría existido sin la actuación.
- Cálculo del beneficio neto, incluyendo inversión, pérdidas, degradación e impacto sobre confort o producción.
- Agregación de recursos teniendo en cuenta su localización y las restricciones de la red.

El resultado deberá apreciarse tanto en el valor aportado al sistema como en el recibido por cada participante. La capacidad flexible anunciada tendrá que corresponderse con la efectivamente entregada, y el consumidor deberá poder entender cómo se ha medido y compensado su contribución.

Ciberresiliencia extendida a toda la cadena de valor

La protección deberá centrarse en preservar la operación física. El Consejo y la dirección contarán con una visión del riesgo vinculada a funciones esenciales, escenarios de interrupción, capacidad de respuesta e impacto económico. Los equipos técnicos dispondrán de responsabilidades y procedimientos coordinados para prevenir, detectar, contener y recuperar.

La mejora deberá reflejarse en:

- **Escenarios de riesgo ciberfísico evaluados según su efecto sobre personas, activos, producción y suministro**.
- Inventarios y mapas de dependencias utilizados para decidir qué proteger y recuperar primero.
- Segmentación y accesos remotos ajustados a la criticidad de cada función.
- Correlación de señales digitales y físicas para detectar incidencias con contexto operativo.
- Copias de datos, lógicas y configuraciones cuya restauración haya sido probada.
- Modos degradados, tiempos objetivo de recuperación y autoridad de actuación definidos antes de la crisis.
- Proveedores clasificados según acceso, impacto, sustituibilidad y concentración de dependencias.

- Capacidades mínimas proporcionadas y verificables en pymes, mantenedores, integradores y fabricantes.
- Contratos y ejercicios conjuntos que aclaren notificación, revocación de accesos, continuidad y recuperación.
- Hallazgos de pruebas y simulacros convertidos en acciones con responsable y seguimiento.

La eficacia deberá demostrarse en ejercicios representativos. Disponer de políticas o herramientas será insuficiente si la organización no puede contener una incidencia, sostener las funciones esenciales y restablecer el proceso completo con seguridad.

Procesos IT-OT integrados y decisiones con retorno demostrable

La convergencia IT-OT deberá modificar la forma de trabajar. El personal recibirá el contexto necesario antes de decidir, conocerá las alternativas y sus consecuencias y dispondrá de responsabilidades claras para autorizar, ejecutar y verificar cada actuación. Las capacidades digitales se gestionarán durante toda su vida útil, con presupuesto, soporte y evolución.

Esto deberá observarse en:

- **Procesos prioritarios mapeados desde la detección hasta la verificación del resultado**, con tiempos, traspasos y puntos de espera identificados.
- Menor esfuerzo manual para reunir información, interpretar alarmas y reconstruir el estado operativo.
- Autorizaciones útiles y límites de automatización definidos según criticidad y reversibilidad.
- Interfaces diseñadas con los operadores y adaptadas a las decisiones de cada perfil.
- Conocimiento de planta documentado y utilizado para validar recomendaciones y formar a nuevos equipos.
- Responsables del proceso, activo, dato, modelo y actuación identificados para cada caso de uso.
- Adopción medida mediante uso real, recomendaciones aceptadas o modificadas y causas de rechazo.
- Business cases que comparen situación actual, inversión, coste de no actuar y resultado obtenido.
- Formación bidireccional para que IT comprenda las restricciones físicas y OT pueda utilizar y cuestionar las nuevas capacidades.

Los primeros despliegues deberán ofrecer evidencia suficiente para decidir si conviene ampliar, modificar o detener una iniciativa. El ahorro de tiempo, la disponibilidad preservada, la reducción de errores, la utilización de activos y el riesgo evitado permitirán valorar el retorno más allá del rendimiento de la herramienta.

En conjunto, el decálogo habrá producido resultados cuando las organizaciones puedan demostrar que conocen mejor sus activos, preservan sus funciones críticas, intervienen antes sobre las degradaciones, utilizan la inteligencia dentro de límites seguros, aprovechan la flexibilidad de la demanda y responden de forma coordinada ante incidencias. El resultado esperado es una operación energética más eficiente, **competitiva, resiliente y sostenible**, capaz de evolucionar tecnológicamente sin perder el control sobre sus decisiones.

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

La selección reúne referencias legales, normas técnicas, sistemas de gestión certificables y un marco voluntario de ciberseguridad. Su aplicación concreta depende de la actividad y los activos de cada organización.

- **Directiva NIS2 — Directiva (UE) 2022/2555**. Establece requisitos de gestión del riesgo de ciberseguridad, seguridad de la cadena de suministro, notificación de incidentes y responsabilidad de la dirección para las entidades comprendidas en su ámbito, incluidas las energéticas. Texto oficial.
- **Directiva CER — Directiva (UE) 2022/2557**. Establece un marco para evaluar riesgos y reforzar la resiliencia de las entidades críticas que prestan servicios esenciales, entre ellas las del sector energético. Texto oficial.
- **Reglamento de Inteligencia Artificial — Reglamento (UE) 2024/1689**. Introduce obligaciones basadas en el riesgo y requisitos específicos para determinados sistemas de IA de alto riesgo vinculados a infraestructuras críticas. Texto oficial.
- **Reglamento de Ciberresiliencia — Reglamento (UE) 2024/2847**. Fija requisitos de ciberseguridad para productos con elementos digitales, desde su diseño hasta la gestión de vulnerabilidades y actualizaciones. Texto oficial.
- **Directiva sobre el mercado interior de la electricidad — Directiva (UE) 2019/944**. Incluye disposiciones sobre sistemas de medición inteligentes, sus funcionalidades y el acceso de los consumidores a sus datos de consumo. Texto oficial.
- **Reglamento General de Protección de Datos — Reglamento (UE) 2016/679**. Regula el tratamiento de datos personales, incluidos los procedentes de contadores inteligentes cuando permiten identificar a una persona. Texto oficial.
- **Serie ISA/IEC 62443 — Ciberseguridad industrial**. Proporciona requisitos y métodos para proteger sistemas de automatización y control, gestionar riesgos y asignar responsabilidades a operadores, integradores y fabricantes. Descripción oficial.
- **Serie IEC 61850 — Automatización eléctrica**. Define modelos de información y comunicaciones para integrar equipos y funciones de automatización en redes e instalaciones eléctricas. Introducción oficial a la serie.
- **Serie IEC 61511 — Seguridad funcional en plantas de proceso**. Establece requisitos para diseñar, operar y mantener sistemas instrumentados de seguridad durante su ciclo de vida. Serie oficial.
- **ISO/IEC 27001:2022 — Gestión de la seguridad de la información**. Define los requisitos de un sistema de gestión certificable para identificar y tratar riesgos sobre la información. Ficha oficial.
- **ISO 22301:2019 — Gestión de la continuidad de negocio**. Define los requisitos de un sistema de gestión certificable para prepararse ante interrupciones, responder y recuperar las actividades prioritarias. Ficha oficial.
- **ISO 55001:2024 — Gestión de activos**. Establece requisitos para gestionar activos de forma sistemática y relacionar su desempeño, riesgos y costes con los objetivos de la organización. Ficha oficial.
- **ISO 50001:2018 — Gestión de la energía**. Establece requisitos para medir y mejorar de forma continua el desempeño energético mediante un sistema de gestión certificable. Ficha oficial.
- **ISO/IEC 42001:2023 — Gestión de la inteligencia artificial**. Define los requisitos de un sistema de gestión para gobernar el desarrollo y uso de la IA y mejorar el tratamiento de sus riesgos. Ficha oficial.
- **NIST *Cybersecurity Framework* 2.0**. Ofrece un marco voluntario para gobernar el riesgo de ciberseguridad, evaluar capacidades y priorizar mejoras. Marco oficial

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

