Hitachi Digital

HITACHI

De copiloto a agente

¿Quién responde cuando la IA actúa sobre el activo?

Autonomía, evidencia y responsabilidad en la O&M eólica

Israel Matsuki · WIND OPS 26 · Valladolid, 14 de octubre de 2026

Ya no es sólo una cuestión de precisión. Es una cuestión de responsabilidad

HITACHI

IA CONSULTIVA

- El modelo propone
- La persona decide
- La persona responde

IA AGÉNTICA

- El agente decide y ejecuta
- Abre la orden, reparametriza, ordena el curtailment, moviliza cuadrilla
- **¿Quién le dio autoridad?**

El salto crítico no es sólo tecnológico. Es de autoridad y de responsabilidad.

Tres fronteras de responsabilidad

HITACHI

01

LA GARANTÍA

¿Qué ocurre con la garantía y la disponibilidad cuando una consigna la modifica un agente autorizado por el propietario, pero no por el tecnólogo?

02

LA PÓLIZA

Las exposiciones de IA empiezan a generar exclusiones y nuevas condiciones en algunos mercados. ¿Sabemos cómo respondería nuestra póliza ante un daño físico iniciado por una acción autónoma?

03

LA IDENTIDAD

Un agente con capacidad de escritura debe tratarse como una identidad no humana privilegiada en el entorno OT. El control deja de poder basarse sólo en el perímetro de red.

El problema aparece cuando garantía, cobertura e identidad no comparten la misma definición de la autoridad del agente.

La regulación ha ganado tiempo. Los contratos, no.

HITACHI

2027 — **AI Act · art. 6(2) y Anexo III**
IA como componente de seguridad en determinadas infraestructuras críticas, incluido el suministro eléctrico.

2028 — **AI Act · art. 6(1) y Anexo I**
IA como componente de seguridad de producto regulado sujeto a evaluación de conformidad por tercero.

Pendiente — **NIS2 · España**
Transposición completa aún pendiente; España fue llevada ante el TJUE en julio de 2026. La generación eléctrica, entre los sectores de alta criticidad.

Hoy — **Lo que ya está firmado**
Garantía, póliza, accesos a OT y contratos de O&M.

La norma dice cuándo empiezan a aplicar ciertas obligaciones.

No dice qué autoridad operacional concedemos hoy. Eso lo deciden los contratos que ya están firmados.

Reglamento (UE) 2026/1744, de 8 de julio de 2026 (DOUE de 24 de julio), que modifica el Reglamento (UE) 2024/1689. Estado de la transposición de NIS2 en España a septiembre de 2026.

El sobre de autoridad

HITACHI

Alcance · Condiciones · Revocación ex ante: ¿puede esta acción ocurrir ahora?

PERMISO ≠ AUTORIDAD OPERATIVA el permiso dice QUÉ puede hacer; la autoridad, CUÁNDO tiene derecho a hacerlo

Qué puede leer	Qué puede escribir	Sobre qué activos	En qué ventana	Quién define y quién asume
Fuentes y ámbito del dato	GMAO, consigna, mercado	Flota, familia o máquina	Horario, estado, umbral de escalado	Propietario · tecnólogo/O&M · riesgo

CUÁNDO PIERDE LA AUTORIDAD *el trip del agente*

Dato degradado · estado fuera del envelope · anomalía de ciberseguridad

La máquina tiene un envelope operativo y protecciones que la sacan de servicio. El agente necesita condiciones explícitas de revocación.

Sin evidencia, la autoridad no se sostiene

Identidad · entradas · decisión · acción · autoridad invocada ex post: ¿puedo demostrar después qué ocurrió y por qué?

- **Linaje del dato**
  De qué sensor, con qué calidad y con qué transformaciones llegó cada entrada.
- **Registro de decisión**
  Entrada, versión de modelo, acción ejecutada, autoridad invocada, marca de tiempo.
- **Recuperación y estado seguro**
  La acción física no siempre se deshace: hay que poder compensarla y volver a un estado seguro.
- **Expediente de incidente**
  Reconstruible por un tercero, sin depender de quien montó el sistema.

28 DE ABRIL DE 2025 ENTSO-E pudo reconstruir la secuencia y los factores sistémicos. Pero de un tramo de 928 MW desconectados en aproximadamente un segundo, no pudo determinar la causa individual de la mayoría de los disparos. Sin ninguna IA de por medio.

Si añadimos actores autónomos, la exigencia de evidencia no puede bajar.

Tiene que subir.

Tres preguntas para el lunes

HITACHI

1. Si mañana autorizas a un agente a actuar sobre el activo, ¿qué no le dejarías hacer nunca?
2. Si esa acción causa un daño, ¿está claro quién asume el riesgo?
3. Seis meses después, ¿podrías demostrar qué vio, qué decidió y por qué actuó?

La pregunta ya no es sólo si confiamos en el modelo.
Es cuánta autoridad estamos dispuestos a darle, y qué evidencia exigimos a cambio.



Israel Matsuki

Strategic Growth Leader | Energy, Mobility & Industrial Digital Transfor...