Insight ON: AI

¿Quién gestiona tu IA?

Lo que realmente significa trabajar con un socio “de extremo a extremo” (End-to-End)

InsightAI

Hay un momento que muchos líderes tecnológicos reconocerán: el proyecto concluye, el nuevo sistema se pone en marcha y tu socio tecnológico pasa al siguiente proyecto. A partir de ese momento, la organización acaba siendo responsable de una solución que nunca se diseñó pensando en su operación a largo plazo: marcos de gobernanza que siempre se iban a "solucionar más adelante", equipos que trabajan con el sistema a diario pero que no participaron en su construcción, y documentación que describe cómo se hizo el sistema en lugar de cómo mantenerlo en funcionamiento.

Estas asociaciones centradas únicamente en la entrega siguen siendo comunes en los proyectos tecnológicos y, aunque dificultan especialmente la resolución de los problemas del "Día 2", para algunos tipos de software la brecha que dejan puede ser manejable. Para la IA, no suele serlo. Un sistema de IA en producción tiene un conjunto adicional de requisitos continuos en comparación con el software convencional, y estos requisitos no siempre se anuncian cuando las cosas empiezan a ir mal.

La mayoría de las organizaciones que construyen IA con un alcance que termina en la entrega no asumen plenamente lo que eso significa hasta que ya están inmersas en ello: el socio ha avanzado y el sistema que les queda por gestionar es más difícil de mantener, gobernar y mantener fiable de lo que habían previsto. Esta es la brecha de entrega: el espacio entre un sistema que se ha lanzado y una capacidad de IA que funciona de forma fiable y dentro de las normas. Las organizaciones que cierran esa brecha tienden a compartir un enfoque común: trabajan con socios que pensaban en el largo plazo desde el primer día.

En 2026, cerrar la brecha de entrega es más urgente que nunca. A partir del 2 de agosto, las obligaciones de alto riesgo de la Ley de IA de la UE pasarán a ser plenamente aplicables para las empresas que operen en la UE. La legislación exige a las organizaciones construir IA de forma responsable, pero también les exige operarla de forma responsable de manera continua. Esto significa evaluaciones de conformidad, procesos documentados, supervisión continua y una clara rendición de cuentas por las decisiones automatizadas. "Lanzado" ya no es la línea de meta, y para las organizaciones cuyas asociaciones de IA se construyeron en torno a un punto final de entrega, esa es una brecha real que cerrar.

El acuerdo provisional también introduce un calendario fijo para la aplicación diferida de las normas de alto riesgo: las nuevas fechas de aplicación serían el 2 de diciembre de 2027 para los sistemas de IA de alto riesgo independientes y el 2 de agosto de 2028 para los sistemas de IA de alto riesgo integrados en productos. Además, el acuerdo provisional restablece la obligación de los proveedores de registrar los sistemas de IA en la base de datos de la UE para sistemas de alto riesgo, cuando consideren que sus sistemas están exentos de la clasificación como de alto riesgo. También restablece el criterio de estricta necesidad para el tratamiento de categorías especiales de datos personales con el fin de garantizar la detección y corrección de sesgos.

El acuerdo provisional pospone la fecha límite para el establecimiento de entornos controlados de pruebas de IA (sandboxes) por parte de las autoridades competentes a nivel nacional hasta el 2 de agosto de 2027 y reduce el periodo de gracia para que los proveedores implementen soluciones de transparencia para el contenido generado artificialmente de 6 a 3 meses, con la nueva fecha límite fijada para el 2 de diciembre de 2026. El acuerdo entre los colegisladores también aclara las competencias de la Oficina de IA para la supervisión de sistemas de IA basados en modelos de IA de propósito general cuando el modelo y ese sistema son desarrollados por el mismo proveedor, enumerando las excepciones en las que las autoridades nacionales siguen siendo competentes, incluyendo la aplicación de la ley, el control de fronteras, las autoridades judiciales y las instituciones financieras.

Los analistas jurídicos y del sector subrayan que el retraso no es un “botón de repetición” para el cumplimiento. Los requisitos fundamentales —como la gobernanza de datos, la documentación técnica y la supervisión humana— permanecen inalterados. La principal recomendación de la Oficina de IA de la UE y de las firmas jurídicas es tratar esta prórroga de 16 meses como un “periodo de construcción” en lugar de un periodo de espera, ya que la complejidad de lograr el cumplimiento (especialmente para los sistemas de alto riesgo) a menudo requiere revisiones operativas significativas que tardan más de un año en implementarse correctamente.

Estrategia, ingeniería, operaciones: por qué los socios de IA deben cubrirlas todas

La brecha de entrega aparece con tanta regularidad porque la mayoría de las asociaciones de IA se planifican en torno a una sola fase de un proceso de tres fases. Estos alcances parciales conducen a tres problemas recurrentes en el éxito a largo plazo de los proyectos de IA.

El primer problema recurrente se produce cuando la consultoría se detiene en la estrategia. Producen una hoja de ruta coherente, un caso de negocio bien argumentado y una visión genuinamente atractiva de lo que el producto podría hacer. Pero luego la realidad de la ingeniería se convierte en el problema de otro. Las preguntas que determinan si un sistema de IA funciona realmente en producción —como cómo se comporta el modelo con datos reales en lugar de conjuntos de prueba limpios, cómo son los costes de inferencia a escala y cómo se conecta con los sistemas que la empresa ya ejecuta— necesitan a alguien en la sala que las entienda desde el principio. Las brechas entre la estrategia y la realidad de la ingeniería pueden causar problemas en cualquier proyecto tecnológico, pero en la IA suelen aflorar más tarde y costar más de solucionar.

El segundo es el socio tecnológico que se detiene en el lanzamiento. El sistema se lanza, funciona el primer día y el programa se cierra. Pero un sistema de IA en producción no es un producto terminado. A diferencia del software convencional, puede degradarse de formas que no son visibles inmediatamente, incluyendo la deriva del modelo (model drift), salvaguardas que requieren un mantenimiento activo a medida que cambian los patrones de uso, y resultados que parecen plausibles pero que ya no son sólidos. Mantenerlo funcionando bien requiere una supervisión continua, una gobernanza activa y alguien que siga siendo responsable de que las decisiones que toma sigan siendo las correctas. Pero si nada de eso estaba en el alcance del proyecto, la empresa recibe algo que está funcionando y se le deja la tarea de averiguar cómo mantenerlo así.

El tercer problema recurrente es más difícil de ver por adelantado, pero a menudo representa un problema significativo en la práctica: hacer que la IA moderna funcione sin problemas con los sistemas heredados (legacy) sobre los que se construye el negocio. La investigación en The Digital Sovereignty Trilemma encontró que el 41% de los líderes de TI afirman que su incapacidad para mover las aplicaciones de negocio heredadas los está frenando activamente. Este es un desafío real y generalizado. Incluso las organizaciones que no están activamente restringidas por sistemas heredados es poco probable que tengan una infraestructura desde cero (greenfield). La mayoría ya tendrá décadas de sistemas, procesos y arquitecturas de datos que no fueron diseñados pensando en la IA. La integración con sistemas heredados es también donde las asociaciones de entrega dejan con mayor frecuencia trabajo inacabado. Las conexiones más difíciles —entre la capacidad de IA moderna y los sistemas más antiguos que ejecutan otras funciones— tienden a resolverse lo justo para el lanzamiento, posponiendo el trabajo más profundo. Una vez que el programa se cierra, ese trabajo diferido pasa a ser gestión de la organización.

La capacidad de extremo a extremo (end-to-end) debería incluir al mismo socio asumiendo todas estas etapas. La inteligencia operativa real significa un diseño de estrategia basado en la realidad de la ingeniería, una ingeniería diseñada para funcionar desde el primer día y una estrategia operativa integrada desde el principio para mantener los sistemas funcionando, conformes a la normativa y mejorando con el tiempo. Y, fundamentalmente, también significa un socio que ayude a identificar y diseñar casos de uso que creen un valor de negocio real, no solo aquellos que sean técnicamente viables.

Construyendo una capacidad de IA duradera en un proveedor de educación líder mundial

Lo que realmente significa cerrar la brecha de entrega en la práctica va más allá de acertar con la tecnología. Se nos acercó un proveedor de educación líder a nivel mundial que opera en casi 200 países y ofrece contenido digital, evaluaciones y soluciones de aprendizaje potenciadas por tecnología a escala global. La división de ingeniería de esta organización acudió a Insight AI planteando una pregunta en la que la mayoría de las organizaciones no piensan lo suficientemente pronto: no solo si la IA funcionaría, sino si sus propios equipos estarían equipados para ejecutarla de forma segura, gobernarla correctamente y seguir mejorándola por sí mismos.

Cuando Insight AI comenzó a trabajar con los equipos de ingeniería de esta organización, una encuesta inicial a los ingenieros participantes reveló algo que las cifras de adopción de IA de los titulares suelen ocultar. La mayor parte del equipo ya utilizaba herramientas de IA con regularidad, por lo que las cifras parecían saludables. Pero este es un patrón que se observa en muchas organizaciones: el uso regular de herramientas de IA no significa necesariamente un uso eficaz o seguro. Al profundizar en cómo se utilizaban realmente las herramientas, se reveló que la evaluación estructurada de los resultados de la IA era inconsistente, y que las técnicas más sofisticadas que suelen generar los beneficios más significativos estaban subutilizadas.

Aún más significativo fue lo que frenaba a la gente. La ansiedad por la seguridad y el cumplimiento normativo fue la barrera más citada, mencionada por ingenieros de distintos perfiles y responsabilidades. Las personas que no estaban seguras de qué datos era seguro compartir con la IA evitaban por completo ciertas herramientas o tomaban sus propias decisiones sin un marco coherente que las guiara. El problema no era el descuido; era la ausencia de normas, de orientación sobre las herramientas y de la confianza necesaria para trabajar de forma segura. Desplegar más tecnología no lo solucionaría.

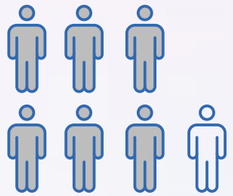
Qué cambió

El programa se propuso construir lo que los equipos habían echado en falta: la infraestructura para un uso seguro y eficaz de la IA. Esto se logró mediante una combinación de talleres basados en el trabajo real de ingeniería y control de calidad (QA), tutorías integradas en bases de código vivas y conjuntos de pruebas, y un conjunto de artefactos de gobernanza —guías de uso, marcos de decisión, bibliotecas de prompts, manuales de mejores prácticas— diseñados explícitamente para perdurar más allá del programa. En lugar de dejar que esas normas se desvanecieran una vez finalizado el proyecto, se creó una red de embajadores internos (champions), en la que los profesionales más experimentados asumieron un papel visible en la definición y adopción de las nuevas normas y un papel docente en la fase de tutoría. Los resultados fueron mucho más allá de los objetivos fijados al principio:

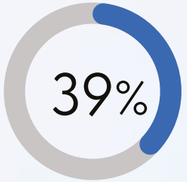
La cifra de gobernanza es la que más importa en el contexto de la fecha límite del 2 de agosto. Al final del programa, el personal directivo nombraba controles específicos: configuraciones confirmadas de licencias empresariales, fragmentos anonimizados para código sensible y la divulgación en Pull Requests (PR) como práctica estándar. Un equipo detectó que una herramienta con capacidad de escritura estaba sobrescribiendo el contenido de los tickets antes de que se convirtiera en un incidente real; el tipo de concienciación práctica sobre los riesgos que no proviene de un documento de política y que lleva meses construir.

“Lee cada línea. La IA genera código de apariencia plausible que puede probar algo totalmente erróneo. Si no puedes hacer que la prueba falle con una entrada incorrecta, no está probando nada”.
QA Engineer

The results went well beyond what had been targeted at the outset:



6 de cada 7 desarrolladores afirman ahora que las herramientas de IA les ahorran tiempo real en el trabajo diario que entregan



39% de reducción en el tiempo de entrega para la primera confirmación de código (code commit), en comparación con un objetivo del 15-20%

2-8 horas ahorradas por cada prueba automatizada creada

10-30 minutos ahorrados por informe de errores (bug report)

De la adopción a la agencia

La prueba más sólida de que esta capacidad se transfirió genuinamente fue lo que ocurrió después de que terminara el programa. El equipo de QA, el grupo que se había calificado de forma más conservadora al principio, pasó a construir dos agentes orientados a problemas específicos en su propio proceso de entrega: uno que redujo el trabajo manual de cumplimiento de accesibilidad de hasta 38 horas por página a unos 30 minutos, y otro que recortó el tiempo de revisión de diseño por componente de hasta tres horas a menos de diez minutos. Ninguno de los dos fue construido por Insight AI. Fueron construidos por los propios ingenieros del equipo, utilizando una capacidad que ahora pertenece a esa organización.

¿Quieres crear este tipo de capacidad interna de IA en tus equipos?

Nuestros especialistas pueden mostrarte cómo se estructuró este programa: cómo se orquestó la transferencia de capacidades, la gobernanza y la aplicación en el mundo real para perdurar más allá de la entrega.

[Habla con un especialista en capacidad de IA]

Ingeniería pensando en el final

Este programa demuestra lo que significa construir una capacidad duradera a nivel organizativo, equipando a las personas que gestionan un sistema de IA para utilizarlo de forma segura y gobernarlo bien. La misma pregunta se aplica a nivel de ingeniería: si el sistema en sí fue construido para ser operado, adaptado y gobernado a lo largo del tiempo, o simplemente construido para ser lanzado.

Nosotros mismos pusimos en práctica esos principios cuando construimos AURA, una plataforma de conocimiento impulsada por IA diseñada para resolver un problema interno real: convertir el trabajo de proyectos finalizados en casos de estudio de cara al cliente era lento, manual y a menudo significaba que el contenido no estaba listo cuando surgía una oportunidad de venta. Con AURA, nuestros equipos comerciales tienen acceso inmediato a casos de éxito relevantes cuando están trabajando en un acuerdo, y pueden utilizarlo para crear narrativas en múltiples idiomas que muestren nuestra experiencia, lo que se traduce en un beneficio comercial directo.

Pero construirlo también nos dio la oportunidad de aplicar los mismos principios de ingeniería a nuestros propios sistemas que aplicaríamos en un proyecto con un cliente. El principio detrás de esas decisiones es sencillo: las elecciones que determinan si se puede confiar en un sistema a lo largo del tiempo rara vez son visibles en una demostración. Aparecen meses después, cuando los datos que maneja el sistema se vuelven más sensibles, cuando el uso escala, cuando el panorama regulatorio se endurece.

Por ello, en lugar de tratar la gobernanza y el cumplimiento como elementos que se añaden una vez que el sistema está en marcha, los integramos desde el principio. Nos aseguramos de que los datos se anonimizan por defecto y de que el acceso se rige por roles. Los cambios en la infraestructura son auditables y reproducibles, en lugar de aplicarse manualmente y ser difíciles de rastrear. Y la supervisión operativa está integrada, no añadida a posteriori.

Ninguna de estas elecciones cambia lo que hace el sistema el primer día, pero determinan si AURA puede operarse de forma responsable a escala, adaptarse a medida que cambian los requisitos y gobernarse bajo condiciones cada vez más exigentes, incluidas las obligaciones que la Ley de IA de la UE hace ahora continuas en lugar de puntuales. AURA sigue funcionando, ha seguido evolucionando y se gobierna por los mismos cimientos que pusimos en marcha al principio. La plataforma se ha desarrollado ahora para crear narrativas temáticas o sectoriales más amplias a partir de grupos de casos de estudio relevantes, algo que no habría sido posible construir sobre un sistema que no hubiera sido diseñado para crecer.

Lo que realmente exige agosto de 2026

Las obligaciones de alto riesgo de la Ley de IA de la UE no pueden satisfacerse con una aprobación única. Requieren una conformidad continua: documentación constante, supervisión, control humano de las decisiones automatizadas y estructuras claras de rendición de cuentas que puedan demostrarse en lugar de limitarse a describirse. Para las organizaciones cuyas asociaciones de IA terminan en la entrega, cumplir con ese estándar será un desafío operativo para el que no estarán preparadas.

Lo que ilustra el programa de capacidad de IA del proveedor de educación es cómo es la preparación regulatoria en la práctica: el 90% del personal directivo que puede nombrar controles específicos y aplicarlos en su contexto, el equipo que detectó un riesgo de gobernanza antes de que se convirtiera en un incidente de producción, las normas, los materiales de gobernanza y la red de defensores que continúan rigiendo el uso de la IA en la organización a medida que la tecnología sigue evolucionando.

Ese tipo de base operativa es también, cada vez más, una ventaja comercial. La investigación de **The Digital Sovereignty Trilemma** reveló que el 55% de las organizaciones señalan la complejidad regulatoria —GDPR, DORA, la Ley de IA— como uno de sus mayores desafíos estratégicos. Allí donde la mayoría encuentra dificultades, los que lo gestionan bien obtienen una ventaja: el 60% de los clientes exigen ahora pruebas de cumplimiento como parte de la contratación, y el 43% de las organizaciones han utilizado credenciales de soberanía para ganar o retener negocios. Las organizaciones que pueden demostrar un cumplimiento continuo, y no solo apuntar a una aprobación de entrega, son las que mantendrán una ventaja a medida que las obligaciones sigan creciendo.

De principio a fin

El programa de capacidad de IA de nuestro proveedor de educación y nuestro proyecto AURA muestran, ambos, lo que significa construir a largo plazo en la práctica, pero llegando desde direcciones diferentes. El programa de capacidad de IA construyó una capacidad interna —las normas, la gobernanza y la confianza para seguir mejorando— de modo que cuando Insight AI se marchara, la organización pudiera llevarla adelante. AURA se construyó para durar desde el principio, con las decisiones que determinan la operabilidad a largo plazo tomadas durante la construcción en lugar de posponerse para más adelante.

Para la mayoría de las organizaciones, esa pregunta se responde mucho antes de que el sistema se ponga en marcha. Depende de si el socio que lo construyó estuvo pensando en las operaciones desde el principio: si la estrategia tuvo en cuenta la realidad de la ingeniería, si la ingeniería se diseñó para lo que habría que operar y si la responsabilidad continua formaba parte del programa en lugar de ser una conversación para más adelante.

Esa continuidad en la responsabilidad —a través de la estrategia, la ingeniería y el trabajo continuo de mantener un sistema en funcionamiento— es lo que realmente significa “de extremo a extremo” (end-to-end).

Ambos se reducían a lo mismo: ¿quién está pensando más allá del lanzamiento antes de que el proyecto siquiera comience?

¿Quieres ver cómo se traducen estos principios de gobernanza e ingeniería en un sistema en producción? Podemos mostrarte cómo se diseñó AURA para la operabilidad a largo plazo, incluyendo el cumplimiento por diseño, la supervisión y las elecciones de arquitectura escalable.
[Solicita una demostración guiada de AURA]

Lee: **¿Atrapado en la fase piloto? Cómo llevar la IA a producción más rápido**, para conocer la otra cara de este desafío: pasar la IA de la fase piloto a la de producción y lo que se necesita para conseguirlo.

es.insight.com/ai