Radar Digital

Mutualidad

Informe de Tendencias Digitales 2027

Noviembre 2027

Mutualidad

Copyright © 2026.
Mutualidad
Todos los derechos reservados.

Índice

01 Claves **3**

02 Introducción **4**

03 Control de la decisión y el escalado: cómo escalar la IA para generar una ventaja competitiva **6**

Dos preguntas, un mismo control 6

Adopción amplia, producción limitada y controlada, y autonomía acotada 6

La retroalimentación: cómo cada plano alimenta al otro 8

Dónde se encuentran decisión y escalado: ámbitos y mercado 9

Los modelos de Zurich y MAPFRE como casos de referencia..... **¡Error! Marcador no definido.**

Barreras para implantar y escalar la IA..... **¡Error! Marcador no definido.**

04 FinOps, de pagar la factura de la nube a gobernar el valor de la tecnología **14**

La IA, primera prioridad del gasto tecnológico 14

De la nube a toda la inversión tecnológica..... 14

El caso de referencia: Allianz Ayudhya 15

Barreras de FinOps 16

05 Infraestructura híbrida: saber dónde está cada dato se convierte en una exigencia de supervisión **17**

Una dependencia concentrada que el marco regulatorio ya no ignora..... 17

Dos marcos, dos tiempos. La obligación de DORA y la ambición de la propuesta CADA..... 18

De la norma a la arquitectura: el modelo de Helvetia 20

Barreras y desafíos ..... **¡Error! Marcador no definido.**

06 Ecosistemas digitales: quién responde ante el cliente **22**

El crecimiento ya se produce en red: promesa y realidad de los ecosistemas 22

Elegir socio: control antes que ahorro 22

MAPFRE y Tuio: una alianza de capacidades complementarias..... 24

Riesgos de crecer en red 25

07 Conclusión: de experimentar a escalar con control **26**

Sobre el Radar Digital **27**

Misión..... 27

Funciones 27

Objetivos 27

01 Claves

- **Tendencia central: de experimentar a industrializar con control.** El contexto asegurador está en proceso de cambio y de **paso de la mera experimentación y desarrollo de proyectos piloto a la industrialización con control.** Actualmente, la IA ya está muy extendida, pero su madurez sigue siendo baja, porque la mayor parte se queda en la experimentación y en el uso de herramientas. Además, los proyectos piloto ya no dan por sí solos una ventaja competitiva. **La ventaja está en industrializar lo que funciona y aporta valor, de forma medible, resiliente y generando confianza**.

- **IA agéntica supervisada: autonomía acotada.** Solo el **9% de los casos de uso que conoce EIOPA es agéntico**, frente al 83% que funciona en modo asistido o semiautónomo. Aun así, la mayoría de las entidades espera que la IA agéntica se generalice en un plazo de tres a cinco años.
- **FinOps: de pagar la factura de la nube a gobernar el valor de la tecnología.** La gestión financiera de la tecnología ya no se limita al gasto en la nube. Ahora abarca también la IA, el software como servicio, las licencias y los centros de datos propios. Su valor estratégico depende de su participación en las decisiones de inversión. La clave está en **vincular la inversión tecnológica a resultados de negocio y reinvertir los ahorros de la optimización en innovación.**
- **Infraestructura híbrida: saber dónde está cada dato.** Casi el 80% de las aseguradoras europeas confía el almacenamiento de sus datos en la nube a grandes tecnológicas. La Unión Europea ha comenzado a desarrollar marcos regulatorios con el fin de obtener y garantizar una mayor capacidad de gobernanza de los datos, resiliencia y trazabilidad. **DORA**, ya en vigor, **busca garantizar la resiliencia**: que las entidades financieras y sus proveedores tecnológicos puedan resistir ciberataques o fallos de sistemas, responder a ellos y recuperarse. Y la propuesta CADA apunta **hacia la soberanía, es decir, a quién controla en última instancia la infraestructura y el software**, y marca como objetivo triplicar la capacidad de centros de datos de la UE en los próximos cinco a siete años.
- **Escalar la IA: de la experimentación a la producción.** El 64% de los casos de uso de IA generativa sigue en prueba de concepto o en fase experimental; la ventaja se centrará, por tanto, en quienes consigan industrializar con criterio y objetivos claros, con proyectos repetibles (aplicables en otras ramas, procesos o mercados) y con resultados medibles.
- **Ecosistemas digitales: quién responde ante el cliente.** El crecimiento del seguro se desplaza hacia redes de socios, plataformas y canales digitales que ninguna aseguradora puede construir en solitario. En torno al **63% de las aseguradoras considera los ecosistemas un motor clave de su crecimiento**. Sin embargo, entrar en un ecosistema es una decisión de gobierno, no solo comercial: en ella se determina **qué aporta cada socio, quién controla el dato.**

02 Introducción

El sector asegurador está comenzando a pasar de la mera experimentación tecnológica hacia **modelos de innovación industrializados e integrados. La ventaja competitiva se encuentra en la capacidad de escalar los proyectos de IA con control,** pasando de la experimentación a conseguir que la innovación sea capaz de producir resultados con impacto medible, resiliencia operativa y confianza.

En la actualidad, la IA está ampliamente adoptada a nivel empresarial, pero cuenta con una madurez baja, limitada a experimentación y uso de herramientas. En 2025, **el 65% de aseguradoras europeas ya usaba IA generativa dentro de sus procesos operativos**, tanto orientada al cliente como en back office; pero **solo un 32% de los casos de uso se encontraba en fase de producción**, en comparación con el 64% que estaba en las primeras etapas de desarrollo y proyectos piloto[1].

En este sentido, **la tendencia central se vertebra a partir de la idea de escalar innovación con control, eficiencia e integración.** A partir de esto, se desprenden cinco tendencias concretas:

1. **Desarrollo de IA agéntica** supervisada para procesos *core*, con autonomía acotada.
2. **FinOps convierte el gobierno financiero en una ventaja estratégica** a través de la optimización de las inversiones en nube e IA.

[1] EIOPA. Generative AI Market Survey: Outlook, Use Cases and Risk Management. Febrero, 2025. [Consultado el 05/11/2026]. Disponible en: https://www.eiopa.europa.eu/document/download/bec886e2-dea0-4bbe-9624-d5f23f85700a_en?filename=EIOPA-BoS-25-679-GenAI-Report.pdf

3. **La infraestructura híbrida se convierte en una exigencia de supervisión** y obliga a la aseguradora a controlar dónde procesar los datos.
4. **Escalar la IA exige combinar adopción, gobernanza y pilotos controlados** para obtener ventajas sostenibles.
5. **Los ecosistemas digitales aceleran su crecimiento** y exigen que las aseguradoras definan su estrategia de integración.

Las tendencias 1 y 4, IA agéntica y escalado de la IA, se analizan en un único capítulo por su interdependencia.

Las cinco tendencias comparten un denominador común, el control. Control sobre las decisiones delegadas en la IA, sobre el coste de la tecnología, sobre la ubicación y trazabilidad de los datos, sobre el avance hacia la producción y sobre el reparto de las responsabilidades y alianzas. El análisis sitúa estas tendencias en el horizonte de 2027 y se centra en el sector asegurador en su conjunto; los casos de referencia proceden de grandes grupos y no incluyen ejemplos específicos de vida-ahorro, previsión social o modelo mutualista.

Hilo conductor: el control como denominador común

Cinco tendencias, una misma cuestión de fondo: quién mantiene el control y sobre qué

Cada tendencia, una dimensión del control

Tendencia · dimensión del control que pone en juego · pregunta a la que responde

Tendencia	Dimensión del control	Pregunta que responde
1. IA agéntica supervisada	Control de la decisión	¿Quién decide?
2. FinOps	Control del coste	¿Cuánto cuesta y qué devuelve?
3. Infraestructura híbrida	Control del dato	¿Dónde está el dato y quién lo controla?
4. Escalar la IA	Control del escalado	¿Qué llega a producción?
5. Ecosistemas digitales	Control de las alianzas	¿Quién responde ante el cliente?

Fuente: Vecdis.

Para su exposición, el informe se organiza en cuatro capítulos con una misma estructura analítica. Cada tendencia se abre con la pregunta estratégica que obliga a responder a las aseguradoras. Sigue un diagnóstico de la situación actual, apoyado en datos de supervisores, encuestas sectoriales y marcos regulatorios. Después se ilustra con uno o varios casos de referencia de entidades que ya la han llevado a la práctica, y se cierra con las barreras o riesgos que condicionan su desarrollo. Con esta lógica, cada tendencia se resume en una pregunta de control:

- **IA agéntica y escalado:** qué llega a producción y quién decide una vez allí
- **FinOps:** cuánto cuesta la tecnología y qué devuelve
- **Infraestructura híbrida:** dónde está cada dato y quién lo controla, a la luz de DORA y de la propuesta CADA

- **Ecosistemas digitales:** quién responde ante el cliente

03 Control de la decisión y el escalado: cómo escalar la IA para generar una ventaja competitiva

La IA ya está adoptada en el sector asegurador, pero **solo una parte reducida de sus casos de uso llega a producción y una parte todavía menor decide por sí misma.** Ambos límites responden a una misma lógica de control. **La ventaja competitiva no estará en tener más pilotos ni en conceder más autonomía, sino en gobernar conjuntamente qué llega a producción y quién decide en cada proceso,** de forma que cada caso escalado genere confianza y defina un perímetro claro de actuación, con un escalado controlado y una autonomía que se amplía de forma gradual, bajo supervisión humana constante.

Dos preguntas, un mismo control

La industrialización de la IA obliga a las aseguradoras a responder a dos preguntas que suelen tratarse por separado: **¿qué llega a producción?** y **¿quién decide una vez allí?** La primera es una cuestión de escalado: convertir pilotos aislados en capacidades repetibles, auditables y conectadas con resultados. La segunda es una cuestión de autonomía: delimitar qué parte de cada proceso ejecuta la IA y qué parte conserva el profesional. Este documento sostiene que ambas preguntas son inseparables.

Por eso este capítulo trata juntas la IA agéntica controlada y el escalado de la IA.

La razón es estructural. Un agente con autonomía que no está en producción no genera valor, y **un caso en producción cuya decisión nadie ha delimitado no puede auditarse ni medirse, ni por tanto escalarse**. Incluso EIOPA describe ambos fenómenos como parte de un mismo movimiento: las entidades están aplicando un escalado controlado de la IA generativa, centrado en la eficiencia interna y con una fuerte supervisión humana, y el sector espera pasar progresivamente de herramientas asistidas a sistemas más autónomos[2].

Desde esta lectura, el control no frena la innovación, sino que la hace acumulativa. **Cada caso que llega a producción con su perímetro de decisión bien definido aporta evidencia, trazabilidad y confianza**; esa evidencia es la que permite ampliar la autonomía del caso siguiente y, con ella, su valor.

Adopción amplia, producción limitada y controlada, y autonomía acotada

La IA generativa está ya ampliamente adoptada en el seguro europeo, pero la autonomía real de los sistemas sigue siendo minoritaria: **solo el 9% de los casos de uso reportados al supervisor europeo es agéntico, frente al 83% que opera en modo asistido o semiautónomo**[3].

Este diagnóstico se apoya igualmente en la situación actual respecto al uso de la **IA generativa**, que, según los datos de 2025, alcanzaba casi el 65% **de las entidades aseguradoras en Europa, a lo que se sumaba otro 23% con planes para incorporar IA generativa en los próximos tres años**. Sin embargo, la amplitud de la adopción no se traduce directamente en capacidad productiva, y así se muestra la situación de los 957 casos de uso reportados por todas las entidades, donde **el 64% se**

[2] Ibíd.
[3] Ibíd.

mantenía en fase de prueba de concepto o experimentación, y solo el 32% se encontraba en producción[4].

En definitiva, los datos disponibles muestran tres capas sucesivas: casi dos de cada tres aseguradoras europeas usan IA generativa, solo uno de cada tres casos de uso está en producción y menos de uno de cada diez es agéntico.

El mercado español muestra un mismo patrón de adopción elevada. En 2025, **8 de cada 10 aseguradoras habían implantado proyectos de IA**, a lo que se puede sumar un 10% más si se incluyen proyectos en desarrollo; y la tecnología se aplica de forma transversal a todas las ramas de negocio y procesos operativos, como suscripción, análisis de riesgos, atención al cliente o detección de fraude[5]. Además, el 74% de las que desarrollan proyectos disponía de un plan de adaptación al Reglamento europeo de IA[6].

En resumen, España combina una adopción amplia con una preparación regulatoria avanzada, aunque no hay un dato comparable sobre el paso a producción. Además, los datos proporcionados para el caso español hacen referencia a proyectos de IA en general, mientras que el europeo trata solo IA generativa, por lo que no se pueden comparar los datos en cuanto al nivel de implantación.

Aun así, se pueden extraer **conclusiones comunes, que muestran una amplia experimentación, pero bajos niveles de** industrialización, impacto y retorno tangible de los proyectos estructurados. Dos de cada tres casos de uso de la IA generativa siguen en prueba de concepto, y los casos orientados al cliente son los que permanecen en fases tempranas con mayor frecuencia. Sin embargo, EIOPA interpreta esta situación como un potencial de crecimiento estructurado en próximos años, no como un fracaso de la experimentación.

Es decir, el proceso de experimentación es necesario para establecer marcos de gobernanza y de medición del impacto que tiene cada proyecto en la empresa, y así poder decidir dónde escalar y qué proyectos eliminar. **Tras años en los que la experimentación era una ventaja en sí misma, esta empieza a ser la base general sobre la que construir proyectos de producción estructurales, con criterios de repetibilidad y resultados medibles, cuya consecución efectiva será la verdadera ventaja competitiva**.

En cuanto a la brecha de autonomía, EIOPA clasifica los casos en tres niveles: **asistido** (el sistema responde a las peticiones del profesional), **semiautónomo** (genera resultados completos que requieren validación humana antes de aplicarse) y **agéntico** (toma decisiones y ejecuta tareas complejas con intervención humana mínima o nula). El predominio de los dos primeros responde a una estrategia deliberada para mantener la precisión, la responsabilidad y el control, sobre todo en casos sensibles o de alto impacto. Las entidades prevén que este equilibrio cambie: el peso de los modelos asistidos y semiautónomos se reducirá considerablemente en tres años, y la mayoría espera que la IA agéntica se generalice en un horizonte de tres a cinco años[7].

[4] Ibíd.
[5] MINSAIT. Más del 70% de las aseguradoras que desarrollan proyectos con IA cuenta ya con planes específicos para adaptar sus sistemas a la nueva regulación europea. Octubre, 2025. [Consultado el 05/11/2026]. Disponible en: https://www.indragroup.com/cms-content/2025/12/251027-NP-Minsait-Informe-ICEA-IA-Seguros.pdf
[6] Ibíd.
[7] EIOPA (2025). Generative AI Market Survey, op. cit.



La retroalimentación: cómo cada plano alimenta al otro

La relación entre ambas tendencias no es de simple coexistencia, sino de retroalimentación: cada plano produce lo que el otro necesita para avanzar. El diagrama recoge este ciclo:



Del escalado a la decisión. Un caso en producción genera lo que un piloto no puede generar: volumen, registro y resultados. Las entidades europeas ya mantienen inventarios de casos de uso, registran las intervenciones humanas y documentan el ciclo de vida de sus sistemas.

De la decisión al escalado. A la inversa, un perímetro de decisión claro es lo que hace un caso auditable y replicable. Las alucinaciones y los comportamientos inesperados son, según las propias entidades, un límite a niveles más altos de automatización y dificultan probar los sistemas de forma robusta; acotar la decisión reduce ese riesgo y despeja el paso a producción.

- **El caso de Zurich lo ilustra:** al dejar la decisión en el suscriptor, según se desprende del despliegue, y aplicar un marco de riesgo común, ha convertido su despliegue en un modelo repetible para más de 20 mercados[8].

El gobierno, en el centro del ciclo. EIOPA describe cómo las entidades aplican un escalado controlado y por pasos, por ejemplo, evitando aplicaciones orientadas al cliente en las primeras fases o exigiendo validación humana de los resultados en lugar de sistemas totalmente autónomos, y cómo algunas despliegan la automatización por fases: pruebas en paralelo, supervisión humana activa y, finalmente, automatización[9]. Es decir, una misma decisión de gobierno fija a la vez qué pasa a producción y con qué autonomía.

Dónde se encuentran decisión y escalado: ámbitos y mercado

La IA generativa ha entrado en el sector por la atención al cliente, los siniestros y la venta y distribución, y el mapa de los próximos años apunta a una profundización en esos mismos terrenos, con el fraude incorporándose como el área de mayor crecimiento previsto. La IA agéntica sigue el mismo recorrido: las entidades que ya la contemplan esperan concentrarla en **siniestros, suscripción y atención al cliente,** y ven además un **potencial relevante en la detección del fraude y la automatización del back office**[10]**.**

[8] REINSURANCE NEWS. Zurich Insurance scales Cytora AI platform across global underwriting operations. Mayo, 2026. [Consultado el 05/11/2026]. Disponible en: https://www.reinsurancene.ws/zurich-insurance-scales-cytora-ai-platform-across-global-underwriting-operations/

[9] EIOPA (2025). Generative AI Market Survey, op. cit.

[10] Ibíd.

Dónde escalar la IA en seguros: qué hace, quién decide y por qué escala

Tres ámbitos con la decisión repartida entre el sistema y el profesional

Reparto de tareas y decisión por ámbito

Ámbito · papel de la IA · quién conserva la decisión · condición que permite escalarlo

Ámbito	Qué hace la IA	Quién decide	Qué lo hace escalable
Siniestros estándar	Recibe el parte, extrae datos, valida la cobertura y detecta excepciones.	El tramitador, en excepciones, casos complejos y pagos por encima de umbral.	Volumen elevado y reglas de cobertura explícitas.
Suscripción	Lee la solicitud, estructura los datos de riesgo y prepara una recomendación.	El suscriptor: aceptación, precio, condiciones y excepciones.	Marco de suscripción común que permite replicar el modelo entre mercados.
Mediación, servicio y renovaciones	Clasifica consultas, prioriza oportunidades y actualiza el CRM.	El mediador o gestor: la relación y el asesoramiento.	Base documental única y alto número de usuarios.

Fuente: Vecdis.

Dos casos, un mismo modelo: Zurich y MAPFRE

Delimitar la decisión para escalar, o escalar con una estructura que delimita la decisión

Leídos juntos, muestran el mismo modelo desde dos ángulos: **Zurich escala un caso porque ha delimitado con precisión la decisión**, y **MAPFRE delimita la decisión en cada caso porque ha construido una estructura para escalar**.

Dimensión	ZURICH · con Cytora	MAPFRE
Punto de entrada	Un proceso core (suscripción comercial).	Un modelo de gobierno y un Centro de IA para todo el grupo.
Qué hace la IA	Convierte solicitudes no estructuradas y multilingües en datos de riesgo listos para decidir.	Desde asistentes para la red comercial hasta verificación automática de daños.
Quién decide	El suscriptor (análisis de Vecdis).	Personas en los casos complejos; modelo «personas + IA».
Cómo escala	Modelo de despliegue replicable: **5 países en 90 días**, más de 20 mercados previstos.	Centro de IA con el objetivo explícito de escalar y reutilizar casos de uso.
Resultado principal	Triaje manual de 75 a 15 minutos **(–80 %)**.	**Más de 115 casos** aplicados (marzo de 2025); más de 150 desarrollados en 2025.
Tipo de dato	Declarado por la empresa.	Declarado por la empresa.

Fuente: Vecdis, con datos de Reinsurance News y MAPFRE.

Zurich y Cytora: delimitar la decisión para poder escalar

Zurich Insurance completó en 90 días el despliegue en cinco países de la plataforma de digitalización de riesgos de Cytora, habilitada con IA agéntica, y prevé extenderla a más de 20 mercados en los 16 meses siguientes[11]. Antes del despliegue, los suscriptores revisaban e interpretaban manualmente

[11] REINSURANCE NEWS (2026), op. cit.

cada solicitud, lo que limitaba la capacidad y generaba priorizaciones heterogéneas, agravadas por varios sistemas no conectados. Hoy, Cytora opera como capa de inteligencia previa dentro del flujo de suscripción: transforma solicitudes no estructuradas y multilingües en datos de riesgo estructurados, alineados con el marco global de suscripción del grupo y entregados en el idioma de cada mercado.



La clave del caso para este análisis no es la eficiencia, sino la relación entre decisión y escalado. De la descripción del despliegue se desprende que la IA prepara el expediente y que la decisión sobre aceptación, precio y excepciones permanece en el suscriptor; esa delimitación es la que permite replicar el modelo **de un país a otro con un marco de riesgo común**; Zurich ha establecido, de hecho, un enfoque de despliegue repetible pensado para acelerar la expansión internacional.

MAPFRE: construir la estructura para escalar con control

MAPFRE ha articulado su estrategia de IA en torno a un Centro de IA global, presentado en marzo de 2025 como **estructura clave para el gobierno y la gestión de estas capacidades en todo el grupo**, con dos objetivos explícitos: aplicar de forma coordinada casos de uso con resultados tangibles y garantizar su escalado y reutilización[12]. Esto ha ido acompañado de la publicación de un manifiesto por la IA humanista, cuyo primer principio es operar bajo un modelo de IA híbrida, que amplíe las capacidades de las personas.

La escala alcanzada. En marzo de 2025, MAPFRE contabilizaba más de 115 casos de uso aplicados en todo el mundo, más del 40% de las operaciones atendidas por asistentes virtuales y la gestión documental automatizada de más de 1,2 millones de clientes; en España, más de 60 casos de IA en producción y unos 5,4 millones de clientes, aproximadamente el 70% del total, que habían

[12] MAPFRE. Mapfre presenta su Manifiesto por una IA humanista, ética y responsable. Marzo, 2025. [Consultado el 05/11/2026]. Disponible en: https://www.mapfre.com/comunicacion/innovacion-comunicacion/mapfre-manifiesto-ia-humanista/

interactuado con soluciones de IA[13]. Más adelante, en la Junta General de 2026, declaró que 2025 cerró con el desarrollo de más de 150 casos de uso en el Centro de IA, un tercio de ellos de IA generativa[14].

Tres casos que muestran la relación entre decisión y escalado:

- **Asistentes virtuales con salida humana.** El 40% de las operaciones las atienden asistentes virtuales, con una condición expresa: los clientes pueden acudir a un agente humano cuando lo consideren necesario[15]. La autonomía se amplía a gran escala porque la decisión de escalar a una persona queda abierta.
- **MIA GPT, escalado sobre la red comercial.** Asistente para mediadores y centro de atención que consulta más de 1.500 documentos, con más de 3.000 usuarios y una satisfacción superior al 80%[16], además de un total de más de 90.000 consultas anuales[17].
- **IRIS, autonomía alta en un tramo acotado.** Desarrollado con ControlExpert y entrenado con más de 60.000 imágenes, verifica automáticamente los daños de un vehículo usado a partir de fotografías del cliente, sin intervención humana en el análisis y con una precisión superior al 98%, lo que permite activar la póliza al instante; la propia MAPFRE precisa que la IA complementa a los peritos, que se concentran en los casos de mayor complejidad. Según datos de 2022, en España y Colombia la solución debía beneficiar a más de 500.000 clientes al año, con despliegue previsto en Chile y Perú[18].

[13] Ibíd.
[14] MAPFRE. Mapfre raises the ambition of its Strategic Plan for 2026. Marzo, 2026. [Consultado el 05/11/2026]. Disponible en: https://www.mapfre.com/en/communicate/corporate-communicate/annual-general-meeting-2026/
[15] MAPFRE (2025). Manifiesto por una IA humanista, ética y responsable, op. cit.
[16] MAPFRE. La IA y su impacto en los servicios aseguradores. Abril, 2025. [Consultado el 05/11/2026]. Disponible en: https://www.mapfre.com/actualidad/innovacion/ia-digitalizacion-ciberseguridad/
[17] MAPFRE (2025). Manifiesto por una IA humanista, ética y responsable, op. cit.
[18] MAPFRE. Mapfre, galardonada en los premios Cionet Vocento por la verificación automática de daños en vehículos mediante IA. Noviembre, 2022. [Consultado el 05/11/2026]. Disponible en: https://www.mapfre.com/comunicacion/innovacion-comunicacion/premio-cionet-vocento-verificacion-automatica-inteligencia-artificial/

Barreras para implantar y escalar la IA

Dos frentes de control: quién decide con la IA y qué llega a producción

IA agéntica supervisada

Control de la decisión

Barrera	Respaldo en las fuentes
Agentes que operan sobre datos sensibles de póliza, siniestro y salud	La privacidad y la seguridad del dato, junto con el cumplimiento normativo y la escasez de perfiles cualificados, figuran entre las principales barreras de implantación. EIOPA menciona expresamente los datos de salud.
Alucinaciones y responsabilidad: ¿quién valida, aprueba y responde?	Las alucinaciones son el riesgo más citado, por delante de la ciberseguridad, la protección de datos y la explicabilidad. Las entidades piden marcos de responsabilidad para decisiones (semi)automatizadas.
Integrar agentes con el core legacy y estimar el coste por uso	Las entidades señalan costes elevados e impredecibles en los modelos de pago por uso. Integrar nuevas tecnologías con los sistemas heredados figura entre las principales barreras a la digitalización y como freno del mercado de la IA agéntica.

Escalado de la IA

Control del paso a producción

Barrera	Respaldo en las fuentes
Limitaciones en la conversión del piloto hacia una aplicación productiva, rentable y controlada	El **64 %** de los casos de uso permanece en prueba de concepto y solo el **32 %** ha llegado a producción. El informe describe un escalado controlado y por fases.
Baja madurez en el desarrollo de una gobernanza específica interna	Solo el **49 %** de las entidades europeas tiene una política de IA específica (**25 %** en 2023). En España, sin embargo, el **74 %** de las que desarrollan proyectos de IA dispone de un plan de adaptación al Reglamento de IA.
Baja integración del conocimiento actuarial y asegurador con la arquitectura de los modelos generativos	**Sin respaldo directo en las fuentes consultadas.** Responde a **criterio de Vecdis**. Como contexto, EIOPA señala que las entidades pueden apoyarse en su experiencia con modelos matemáticos, pero gran parte de las técnicas de gobierno de la IA tradicional no es aplicable a la IA generativa.

Fuente: Vecdis, con datos de EIOPA, MarketsandMarkets e ICEA-Minsait.

04 FinOps, de pagar la factura de la nube a gobernar el valor de la tecnología

La gestión financiera de la tecnología ha dejado de limitarse a la factura de la nube. La práctica totalidad de los equipos FinOps gestiona ya el gasto en IA, y su alcance se extiende al software como servicio, las licencias y los centros de datos propios. La pregunta que responde esta tendencia es **cuánto cuesta la tecnología y qué devuelve**: cada inversión debe poder vincularse a un resultado de negocio.

La IA, primera prioridad del gasto tecnológico

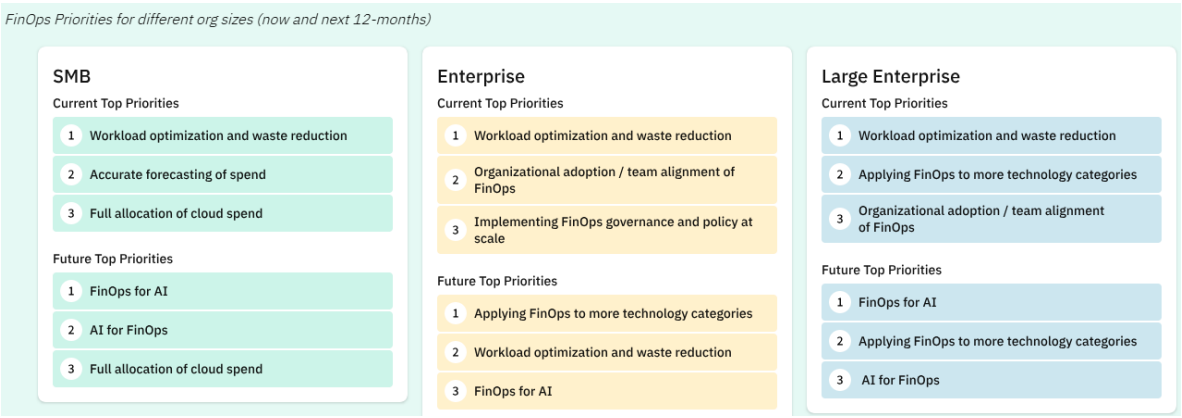
State of FinOps 2026, la sexta encuesta anual de la FinOps Foundation, recoge la visión de 1.192 profesionales que gestionan más de 83.000 millones de dólares de gasto cloud anual[19]. Su hallazgo central es la velocidad con que la IA ha entrado en el perímetro de gestión: **el 98% de los equipos gestiona ya este gasto, frente al 63% en 2025 y el 31% en 2024**, y "FinOps para IA" es su primera prioridad para los próximos doce meses[20].

Es decir, la IA ya no es un experimento que se financia al margen del presupuesto, sino una partida que exige la misma disciplina que cualquier otra inversión tecnológica.

Una función que sube de nivel, pero no siempre hasta la dirección. El 78% de las prácticas FinOps reporta ya a la organización del CTO o del CIO, y solo un 8% al CFO[21]. La ubicación importa menos que el alcance de la interlocución: los equipos que despachan con vicepresidencia o comité de dirección tienen entre dos y cuatro veces más influencia en la selección tecnológica que los que se quedan en el nivel de director, y participan cada vez más en negociaciones con proveedores y en decisiones de inversión plurianuales. Dicho de otro modo, FinOps solo genera ventaja estratégica cuando tiene voz en las decisiones que comprometen el gasto.

De la nube a toda la inversión tecnológica

FinOps ha dejado de ser una disciplina de optimización cloud para convertirse en un modelo de gobierno de todo el gasto tecnológico. La propia FinOps Foundation ha redefinido su misión en esta línea, pasando de gestionar el valor del cloud a gestionar el valor de la tecnología.



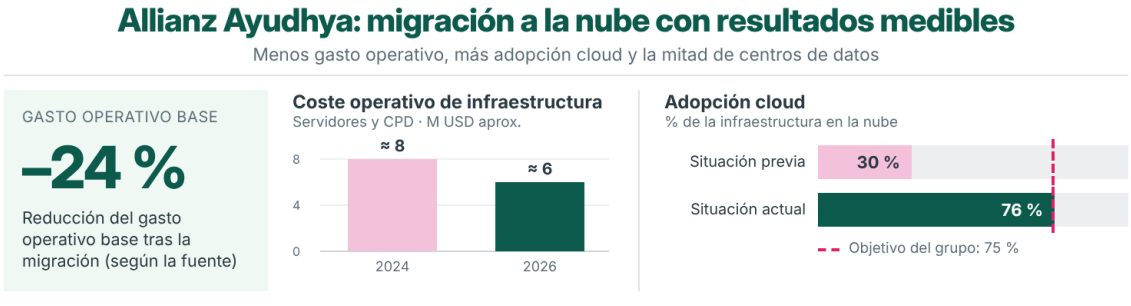
Fuente: FinOps

[19] FINOPS FOUNDATION. State of FinOps 2026 Report. 2026. [Consultado el 05/11/2026]. Disponible en: https://data.finops.org/
[20] Ibíd.
[21] Ibíd.

Dos hallazgos refuerzan la lectura estratégica. Por un lado, **muchas organizaciones deben autofinanciar su inversión en IA con los ahorros obtenidos en la optimización del resto de la infraestructura,** lo que conecta directamente la disciplina financiera con la capacidad de innovar. Por otro, **la optimización tradicional muestra rendimientos decrecientes:** los profesionales describen que los grandes focos de despilfarro ya se han resuelto, y que el valor se desplaza hacia la economía unitaria, la cuantificación del valor de la IA y la influencia en la selección tecnológica antes de comprometer el gasto.

El caso de referencia: Allianz Ayudhya

Allianz Ayudhya ilustra el punto de partida de esta evolución: la migración que fija la base de costes sobre la que después se puede innovar. Según el caso publicado por SoftwareOne, proveedor del proyecto, la filial de Allianz en Tailandia operaba con más de 500 servidores próximos al final de su vida útil y de su soporte, distribuidos en cuatro centros de datos, dos principales y dos de recuperación ante desastres. La compañía se enfrentaba a una disyuntiva: **reinvertir en hardware propio que se deprecia o dar el salto a la nube.** El proyecto solo podía avanzar con un caso de negocio sólido ante la dirección, y la migración a AWS se ejecutó finalmente en dos fases: primero el negocio de No Vida (2023) y después el de Vida y Salud (2025)[22].



Resumen de indicadores

Indicador	Situación previa	Situación actual
Coste operativo de servidores y centros de datos	≈ 8 M USD (2024)	**≈ 6 M USD (2026)**
Reducción del gasto operativo base	—	**–24 % (según la fuente)**
Adopción cloud	30 %	**76 % (objetivo del grupo: 75 %)**
Centros de datos	4	**2**

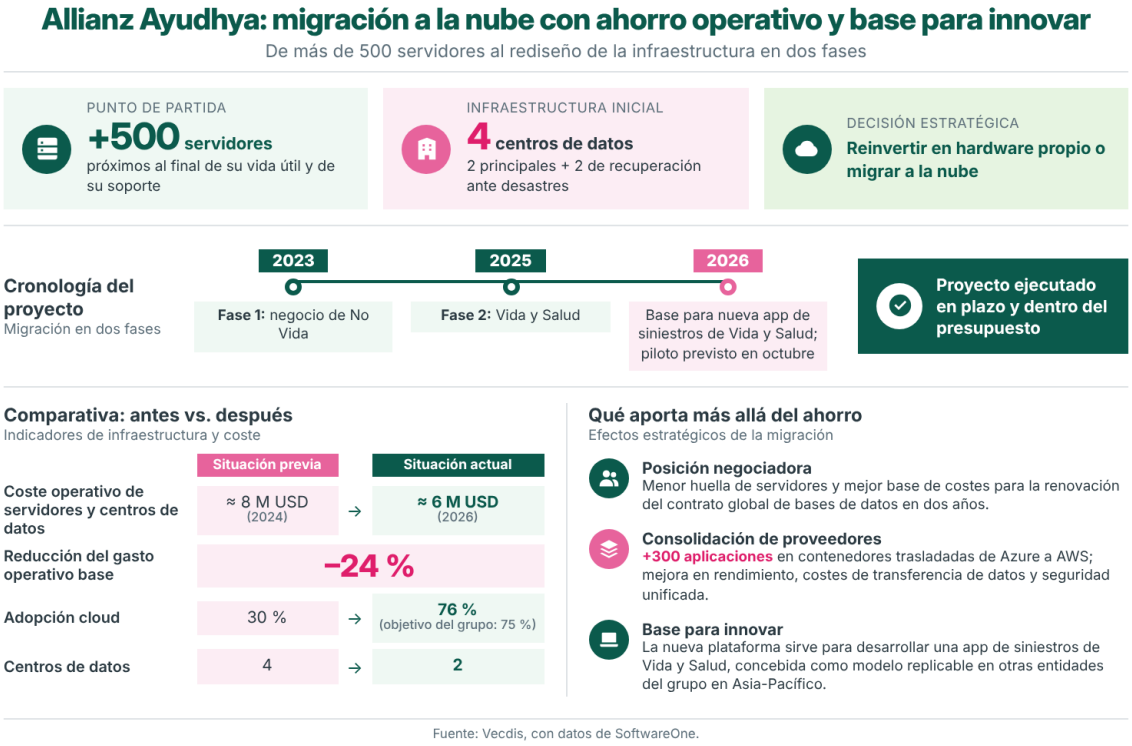
Fuente: Vecdis, con datos de SoftwareOne.

Más allá del ahorro, el caso aporta tres elementos de valor estratégico.

- **Posición negociadora:** al reducir su huella de servidores, la filial ha ajustado sus necesidades de licencias de bases de datos y afrontará la renovación del contrato global, prevista en dos años, desde una base de costes significativamente menor.

[22] SOFTWAREONE. How Allianz Ayudhya accelerated cloud transformation and cut operating costs with SoftwareOne. [Consultado el 05/11/2026]. Disponible en: https://www.softwareone.com/en/case-studies/global/finance/allianz-aws-migration

- **Consolidación de proveedores**: más de 300 aplicaciones en contenedores se trasladaron de Azure a AWS; el ahorro directo fue reducido, pero la compañía gana en rendimiento, en costes de transferencia de datos y en seguridad unificada.
- **Base para innovar:** sobre la nueva plataforma se desarrolla una aplicación de siniestros de Vida y Salud, con piloto previsto en octubre de 2026, concebida como modelo replicable en otras entidades del grupo en Asia-Pacífico.



Barreras de FinOps

Barreras de FinOps

Por qué cuesta prever, medir y gobernar el gasto de la IA

Tres barreras y su grado de respaldo en las fuentes — Control del coste

Barrera · evidencia que la respalda · grado de respaldo (alto o parcial)

Barrera	Respaldo en las fuentes	Grado de respaldo
Coste variable de consultas, modelos y capacidad de cálculo, que dificulta prever y controlar el gasto de IA	Los costes de la IA tienen una tarificación menos transparente o más variable que los servicios cloud tradicionales, y los modelos de precios difieren mucho entre proveedores.	Alto
Dificultad para comprobar si cada uso de IA genera más valor del que cuesta	Determinar el valor y el retorno de la IA figura entre los principales retos. Las inversiones suelen ser exploratorias y su retorno es difícil de definir en fases tempranas.	Alto
Datos dispersos entre cloud, IA y APIs, que complican el control y el gobierno	El informe no habla de datos dispersos ni de APIs, pero recoge la demanda de una visión unificada del gasto de distintas tecnologías y la adopción creciente de un estándar común de datos de coste (FOCUS). La formulación es un **análisis de Vecdis**.	Parcial

Fuente: Vecdis, con datos de FinOps.

05 Infraestructura híbrida: saber dónde está cada dato se convierte en una exigencia de supervisión

La nube ha dejado de ser solo una decisión de eficiencia para convertirse en una cuestión de supervisión. Por infraestructura híbrida se entiende la combinación de centros de datos propios con una o varias nubes públicas, gestionadas bajo un mismo modelo de gobierno. La actualidad presenta una alta concentración del almacenamiento cloud en un número reducido de grandes proveedores externos, lo que limita el control y la trazabilidad de los datos. Dentro de este panorama, la Unión Europea ha desarrollado un marco regulatorio con dos objetivos distintos: reforzar la resiliencia operativa de las entidades y, como horizonte, la soberanía del dato. DORA (*Digital Operational Resilience Act*), aplicable desde enero de 2025, ya obliga a cada entidad a demostrar su resiliencia tecnológica y a responder plenamente de sus proveedores; la propuesta de CADA (*Cloud and AI Development Act*) anticipa, por su parte, un marco europeo de soberanía del dato. La pregunta deja de ser qué nube utilizar y pasa a ser **dónde está cada dato y quién lo controla**.

Una dependencia concentrada que el marco regulatorio ya no ignora

El sector asegurador europeo ha confiado buena parte de su infraestructura a un puñado de grandes proveedores tecnológicos. Esa decisión tiene una lógica de eficiencia, pero ha creado una dependencia que crece en volumen y en profundidad, y que el regulador ya trata como un riesgo sistémico. El problema no es usar la nube, sino depender de ella sin alternativas ni capacidad de salida.

La situación: una dependencia concentrada en pocos proveedores. Según el informe de EIOPA sobre la digitalización del seguro europeo, basado en una encuesta a 209 entidades de 22 Estados miembros, casi el 80% de las aseguradoras externaliza el almacenamiento de datos en la nube a

grandes tecnológicas, y esta es su principal relación comercial con ellas[23]. Y la relación rara vez se limita al almacenamiento: el software como servicio es la modalidad cloud más contratada, y los proveedores suelen sumar seguridad, analítica de datos e IA, chatbots o gestión de clientes. Es decir, cuantos más servicios se apoyan en un mismo proveedor, más difícil y costoso resulta sustituirlo.

Lejos de moderarse, se prevé que la dependencia aumente. La mayoría de las entidades espera incrementar de forma significativa o moderada la externalización de servicios a las grandes tecnológicas en los tres años siguientes. La IA generativa acelera el proceso, porque sus herramientas suelen proceder de los mismos proveedores que prestan los servicios cloud; las propias aseguradoras advierten de que un ciberataque o incidente en esos proveedores podría generar vulnerabilidades en toda su cadena de valor[24].

Por qué importa: de riesgo operativo a riesgo sistémico. Cuando muchas entidades dependen de los mismos pocos proveedores, un fallo en uno de ellos deja de ser un problema individual y se convierte en un riesgo para todo el sistema financiero. Esa es la lógica del marco europeo de supervisión de proveedores tecnológicos críticos que establece **DORA, concebido para abordar los riesgos sistémicos y de concentración derivados de esa dependencia[25].**

En paralelo al riesgo financiero, la Comisión Europea añade la dimensión geopolítica, al calificar la dependencia excesiva de proveedores no europeos como un riesgo significativo para la autonomía y la resiliencia digital de Europa[26]. A partir de esta concepción se diseña la propuesta CADA.

Algunas aseguradoras ya han empezado a reaccionar diversificando proveedores, diseñando arquitecturas capaces de conectarse a varios de ellos o alojando modelos de menor tamaño en sus propias instalaciones[27].

Dos marcos, dos tiempos. La obligación de DORA y la ambición de la propuesta CADA

La respuesta europea a esta dependencia avanza por dos vías complementarias. DORA, ya aplicable, se ocupa de la **resiliencia**: que cada entidad pueda soportar un fallo tecnológico y, si es necesario, cambiar de proveedor sin interrumpir el servicio. CADA, todavía en tramitación, se ocupa de la **soberanía**: quién controla en última instancia la infraestructura y el software. Ambas desplazan la pregunta relevante: **ya no basta con elegir una nube, sino que hay que demostrar en qué condiciones de control se utiliza**.

DORA: resiliencia como obligación vigente

El Reglamento de Resiliencia Operativa Digital es aplicable desde el 17 de enero de 2025 y armoniza las normas de resiliencia para veinte tipos de entidades financieras, entre ellas las aseguradoras, y para sus proveedores tecnológicos. Su finalidad es que puedan resistir, responder y recuperarse de disrupciones tecnológicas como ciberataques o fallos de sistemas[28].

[23] EIOPA. Report on the digitalisation of the European insurance sector. Abril, 2024. [Consultado el 05/11/2026]. Disponible en: https://www.eiopa.europa.eu/document/download/6ca9e171-42b9-44d7-a2e6-beaf0134ecb8_en?filename=Report%20on%20the%20digitalisation%20of%20the%20European%20insurance%20sector.pdf

[24] EIOPA (2025). Generative AI Market Survey, op. cit.

[25] EIOPA. Digital Operational Resilience Act (DORA). [Consultado el 05/11/2026]. Disponible en: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

[26] EUROPEAN COMMISSION. Cloud and AI Development Act. [Consultado el 05/11/2026]. Disponible en: https://digital-strategy.ec.europa.eu/en/policies/cloud-and-ai-development-act

[27] EIOPA (2025). Generative AI Market Survey, op. cit.

[28] EIOPA. Digital Operational Resilience Act (DORA), op. cit.

El reglamento dedica además un artículo específico a la protección y la prevención, que obliga a minimizar el riesgo de corrupción o pérdida de datos y a protegerlos tanto en reposo como en uso o en tránsito.

Marco DORA

Qué exige el Reglamento DORA y qué implica para la arquitectura de una aseguradora

Bloque	Qué exige	Qué implica para la arquitectura
Gestión del riesgo TIC	Un marco de gestión del riesgo tecnológico; en materia de protección, limitar el acceso a lo estrictamente necesario, autenticación robusta, cifrado según la clasificación del dato y redes que puedan aislarse ante un ataque.	Controles de acceso, cifrado y segmentación integrados en cada entorno, no añadidos después.
Gestión del riesgo de terceros	La entidad sigue siendo plenamente responsable aunque externalice; registro de información de todos los contratos con proveedores tecnológicos, con informe al menos anual al supervisor; estrategias de salida probadas para los servicios que soportan funciones críticas o importantes.	Saber qué dato reside en qué proveedor y poder trasladarlo de forma segura e íntegra a otro proveedor o a la propia entidad.
Pruebas de resiliencia	Pruebas básicas y avanzadas.	Entornos que puedan probarse sin afectar a la operación.
Incidentes TIC	Requisitos generales y notificación de los incidentes graves a la autoridad competente.	Registros centralizados que permitan reconstruir qué ocurrió, dónde y cuándo.
Intercambio de información	Intercambio de información e inteligencia sobre ciberamenazas.	Capacidad de compartir indicadores sin exponer datos de clientes.
Supervisión de proveedores críticos	Marco europeo de supervisión directa de los proveedores TIC críticos, para abordar los riesgos sistémicos y de concentración.	Los grandes proveedores pasan a estar supervisados, pero la responsabilidad frente al supervisor sigue siendo de la aseguradora.

Fuente: Vecdis, con datos de EIOPA (Reglamento DORA).

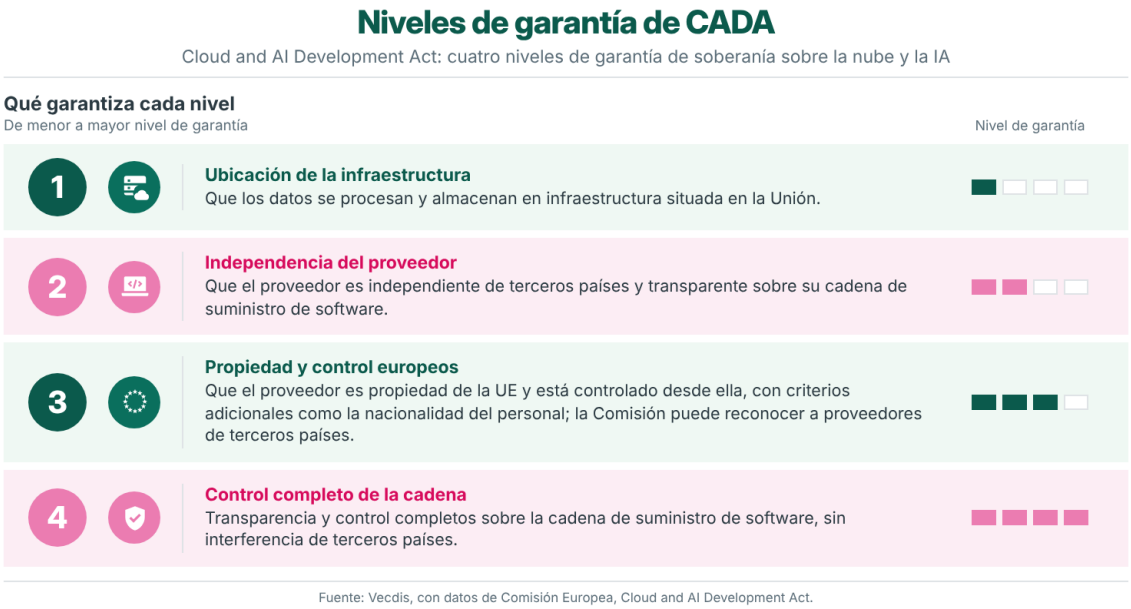
CADA: la soberanía del dato como horizonte

La Comisión Europea adoptó el 3 de junio de 2026 la propuesta de Cloud and AI Development Act, como parte del Plan de Acción Continente de IA, y articulada en torno a **tres objetivos: investigación e innovación, capacidad y autonomía.** Asimismo, **fija como meta al menos triplicar la capacidad de centros de datos de la UE en los próximos cinco a siete años,** simplificando los permisos y mejorando el acceso a energía, suelo, agua y financiación[29].

Este marco regulatorio marca la primera vez que se define oficialmente qué significa la soberanía cloud y de IA, a través de cuatro niveles de garantía que los organismos públicos deberán posteriormente aplicar según su evaluación de riesgos y frente a los cuales, los Estados miembros podrán reconocer a los proveedores en auditoría.

CADA se dirige en principio a los organismos públicos, aunque se espera un efecto de arrastre sobre el sector privado.

[29] EUROPEAN COMMISSION. Cloud and AI Development Act, op. cit.



De la norma a la arquitectura: el modelo de Helvetia

Helvetia ilustra cómo una aseguradora regulada puede anticiparse a las exigencias de supervisión en el diseño de su infraestructura sin renunciar a la velocidad. El caso es anterior a la aplicación de DORA y a la propuesta CADA, por lo que no responde directamente a ninguno de los dos marcos. Su enfoque, conocido como **gobierno como código**, consiste en que cada nuevo entorno en la nube nazca ya con los controles incorporados, en lugar de revisarlos después.

El punto de partida: una nube sin gobierno. Helvetia, aseguradora suiza fundada en 1858 e integrada desde diciembre de 2025 en Helvetia Baloise, con filiales en Francia, España, Alemania, Austria e Italia, describe cómo los primeros usos de la nube en una entidad regulada suelen nacer de pruebas aisladas de equipos técnicos, con credenciales compartidas y sin control del gasto. Ese modelo no resiste el paso a producción: el regulador exige saber quién hizo qué y dónde, la seguridad no puede abrir la red a cualquier proveedor y alguien debe responder del coste[30].

A partir de ahí, la compañía abordó la migración de sus centros de datos propios a la nube pública con un objetivo exigente, trasladar 200 aplicaciones a AWS y Microsoft Azure en un año, que cumplió[31].

Los requisitos: regulatorios antes que técnicos. Por razones regulatorias, Helvetia se impuso operar en al menos dos nubes, integrar sus sistemas propios y sus servicios SaaS, hacer a cada equipo responsable de su propio entorno y ofrecerlo en autoservicio. En gobierno, fijó cinco reglas: acceso con credenciales corporativas únicas y mínimo privilegio, registros de auditoría centralizados, uso exclusivo de regiones autorizadas, cifrado de todos los discos sin excepción y prohibición de servicios excesivamente caros[32].

El modelo: del formulario al entorno controlado. Toda petición entra por ServiceNow, donde el solicitante identifica el proyecto, a su responsable, a quien asume el coste y la red que necesita. Esa

[30] HASHICORP. Automatic multi-cloud landing zones via HCP Terraform at Helvetia Insurance. Septiembre, 2024. [Consultado el 05/11/2026]. Disponible en: https://www.hashicorp.com/en/resources/automatic-multi-cloud-landing-zones-via-hcp-terraform-at-helvetia-insurance

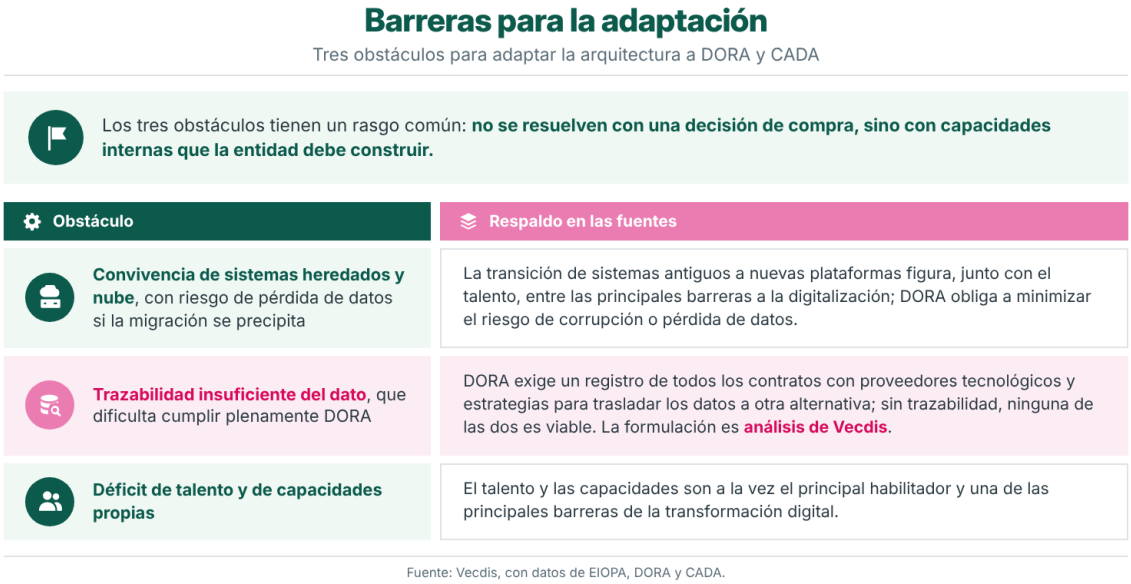
[31] IBM. The Great Migration. [Consultado el 05/11/2026]. Disponible en: https://www.ibm.com/case-studies/helvetia-insurance

[32] HASHICORP (2024), op. cit.

información se convierte en un fichero de configuración único, que actúa como fuente de verdad, y Terraform despliega a partir de él la cuenta y su *landing zone*: un entorno que nace conectado a los centros de datos propios mediante conexiones privadas y con las políticas aplicadas de serie. Una herramienta de seguridad alerta además si algún equipo se desvía de ellas, por ejemplo con un disco sin cifrar[33].



Fuente: Vecdis.



Fuente: Vecdis, con datos de EIOPA, DORA y CADA.

[33] Ibíd.

06 Ecosistemas digitales: quién responde ante el cliente

El crecimiento del seguro se desplaza hacia redes de socios, plataformas y canales digitales que ninguna aseguradora puede construir en solitario, y la IA ya ha abierto canales de venta que hace dos años no existían. Pero entrar en un ecosistema no es una decisión comercial, sino de gobierno: quien no define con precisión qué aporta cada socio, quién controla el dato y cómo se reparten responsabilidades, costes y riesgos corre el riesgo de ceder lo más valioso que tiene, la relación con el cliente. La pregunta que plantea esta tendencia es **quién responde ante el cliente**.

El crecimiento ya se produce en red: promesa y realidad de los ecosistemas

Los ecosistemas se han instalado en la agenda estratégica del sector por dos fuerzas que actúan a la vez: la convicción de las aseguradoras de que el crecimiento futuro pasa por las alianzas y la exigencia de un cliente que espera una experiencia digital sin fricciones. Sin embargo, los datos de distribución muestran que esa transformación está todavía en sus primeras fases.

Según el *Insurtech Global Outlook 2026* de NTT Data, **en torno al 63% de las aseguradoras considera los ecosistemas un motor clave de su crecimiento e innovación futuros[34].** Este informe describe esos ecosistemas como redes de plataformas, corredores, agencias de suscripción, reaseguradoras y proveedores de datos, y sostiene que las entidades que ganarán en este entorno serán las que dispongan de interfaces estándar preparadas para conectar socios, sean capaces de lanzar nuevas propuestas en semanas y no en meses, y conviertan la colaboración en una capacidad repetible que proteja de forma duradera la relación con el cliente.

Además, el capital acompaña a esta perspectiva. **La inversión global en insurtech superó los 4.000 millones de dólares en 2025**, una de cada cuatro insurtech financiadas ha incorporado ya la IA a sus productos u operaciones, y se espera que el seguro embebido (embedded), que se contrata junto con la compra de otro producto o servicio, supere los 700.000 millones de dólares a escala global[35].

La exigencia de la demanda. El 73% de los clientes espera experiencias digitales fluidas en cada interacción con su seguro, y más de la mitad de los adultos utiliza ya IA generativa, lo que está elevando sus expectativas de inmediatez y personalización[36]. Sin embargo, ninguna aseguradora tiene la capacidad por sí sola para ofrecer esa experiencia en todos los momentos de la vida del cliente. Ahí es donde el desarrollo de ecosistemas genera una vía para garantizar esa oferta.

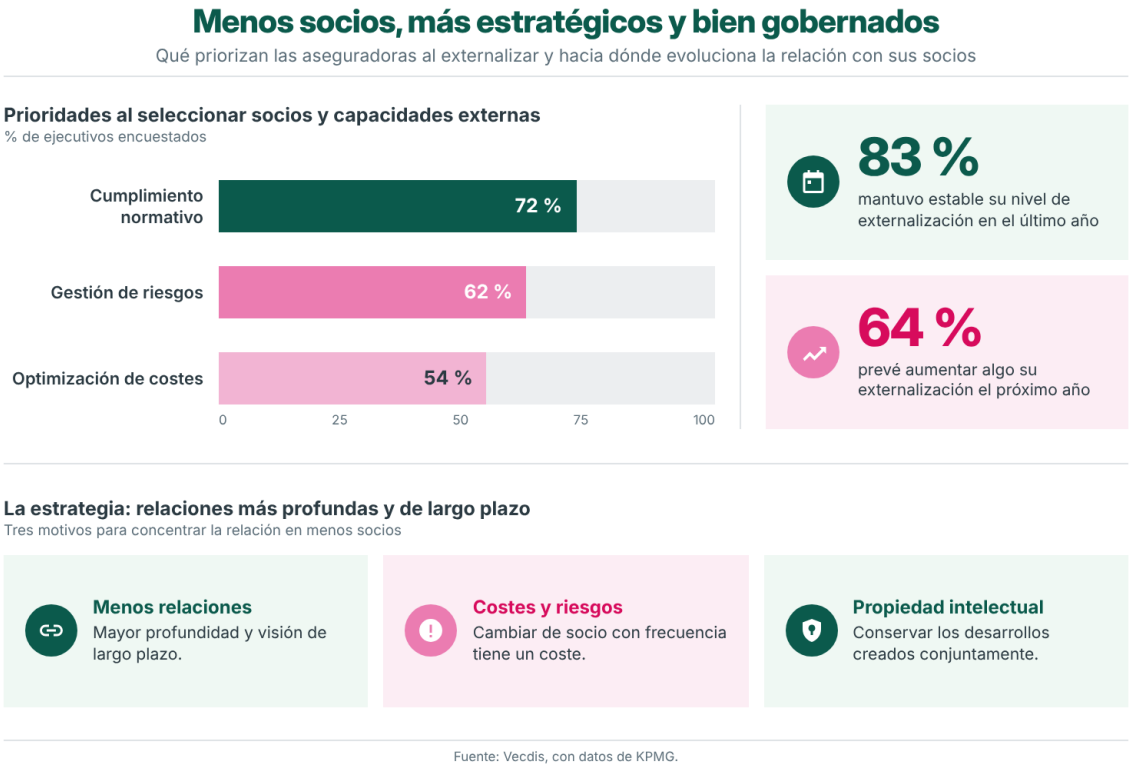
La realidad del canal: una transformación que apenas empieza. Los datos del supervisor europeo sitúan esa ambición en su punto de partida. **En 2024, las ventas puramente digitales representaban de media solo el 9% de las primas en Vida y el 19% en No Vida**, aunque las entidades esperan que crezcan progresivamente[37]. Al mismo tiempo, las alianzas con insurtech eran todavía más comerciales que estratégicas, pues cerca del 40% de las aseguradoras mantenía relaciones con startups, pero no invertían en ellas ni planeaban hacerlo.

Elegir socio: control antes que ahorro

La forma en que las aseguradoras seleccionan a sus socios ha cambiado de naturaleza. KPMG describe un desplazamiento desde el arbitraje de costes, lógica tradicional de la externalización, hacia

[34] NTT DATA. Insurtech Global Outlook 2026. 2026. [Consultado el 05/11/2026]. Disponible en: https://insurance.nttdata.com/insurtech-global-outlook-2026/
[35] Ibíd.
[36] Ibíd.
[37] EIOPA (2024). Report on the digitalisation of the European insurance sector, op. cit.

la búsqueda de socios que aporten capacidades difíciles o imposibles de desarrollar internamente y que ayuden a innovar más rápido[38].



Los resultados de la encuesta a directivos respecto a los factores que determinan dónde ubicar a los socios de externalización muestran una tendencia clara: una alianza que ahorra dinero pero genera exposición regulatoria o riesgo operativo acaba destruyendo valor en lugar de crearlo. Así, se retoma la idea central de tener control sobre todo el proceso y confianza en el sistema de alianzas.

Asimismo, de la encuesta se desprende la **tendencia hacia una mayor externalización, aunque gradual y con menor cantidad de socios**. Las aseguradoras parecen más dispuestas a confiar actividad a terceros, aunque sin precipitarse: **el 83% de los ejecutivos mantuvo estable su nivel de externalización en el último año y el 64% prevé aumentarlo ligeramente** en el próximo. KPMG interpreta este avance mesurado como un signo de madurez, entendido como externalización no solo para reducir costes, sino para incorporar capacidades estratégicas, hasta el punto de confiar a sus socios funciones que antes se consideraban críticas, como la conciliación, la información financiera o la fiscalidad[39].

Ese cambio de propósito modifica también la forma de relacionarse con los socios. Las aseguradoras prefieren menos relaciones, más profundas y a largo plazo, porque cambiar de socio con frecuencia genera sus propios costes y riesgos, y les preocupa conservar la propiedad intelectual de lo que se construye en común. Para que la alianza funcione, se necesitan cumplir dos condiciones:

- Definir qué se pretende conseguir antes de elegir socio

[38] KPMG. Building partnerships that transform insurance operations. 2025. [Consultado el 05/11/2026]. Disponible en: https://kpmg.com/us/en/articles/2026/building-partnerships-transform-insurance-operations.html
[39] Ibíd.

- Gobernar la relación con algo más que acuerdos de nivel de servicio, mediante revisiones estratégicas periódicas que comprueben si sigue cumpliendo sus objetivos

Trasladado a los ecosistemas, los resultados apuntan a que el criterio de selección se desplaza del precio y la innovación hacia la capacidad del socio para preservar el control regulatorio, operativo y sobre el dato.

MAPFRE y Tuio: una alianza de capacidades complementarias

La operación entre MAPFRE y Tuio ilustra cómo una aseguradora tradicional puede incorporarse a la distribución digital sin renunciar a su modelo: en lugar de construir internamente un canal nuevo, se asocia con quien ya lo ha desarrollado y le aporta lo que a este le falta.

La operación. El 30 de julio de 2026, MAPFRE anunció un acuerdo para adquirir el 38,9% del capital de Tuio, mediante la compra directa de participaciones a determinados socios y una ampliación de capital posterior[40].

El reparto de capacidades. El valor de la alianza reside en que cada parte aporta lo que a la otra le resultaría costoso construir:



Fuente: Vecdis, con datos de MAPFRE.

Un canal que no existía. El elemento más significativo del caso es la venta a través de asistentes conversacionales. Según MAPFRE, Tuio fue la primera aseguradora del mundo integrada con ChatGPT para la venta de seguros y, desde esa integración a comienzos de febrero, capta por esta vía más del 20% de sus nuevos clientes[41].

La lectura estratégica es doble. Por un lado, el asistente de IA se convierte en un nuevo punto de entrada del cliente: la aseguradora que no esté integrada en él corre el riesgo de quedar fuera de la conversación en el momento en que se genera la necesidad. Y por otro, ese punto de entrada

[40] MAPFRE. Mapfre refuerza su apuesta por la innovación y desarrollo del negocio digital adquiriendo una participación en Tuio. Julio, 2026. [Consultado el 05/11/2026]. Disponible en: https://www.mapfre.com/comunicacion/corporativo-comunicacion/innovacion-desarrollo-negocio-digital-tuio/
[41] Ibíd.

pertenece a un tercero, lo que reabre la pregunta central de esta tendencia: quién es titular de la relación con el cliente.

La lógica estratégica. MAPFRE justifica la inversión en su convicción de que la IA, y en particular la agéntica, supone un cambio tecnológico de gran alcance para el sector, y en su apuesta por modelos de distribución más ágiles que combinen la tecnología con el asesoramiento humano; añade además que la IA puede contribuir a reducir la brecha de protección al facilitar el acceso al seguro a colectivos menos protegidos[42].

El caso apunta a un modelo en el que **la aseguradora tradicional no sustituye su red para acceder al nuevo canal, sino que lo incorpora como complemento, conserva su propuesta de asesoramiento y gana un laboratorio de distribución** digital con el que aprender. Los resultados de la integración están aún pendientes: la operación se anunció en julio de 2026 y el dato del 20% corresponde al canal de Tuio, no a la alianza.

Riesgos de crecer en red

Los tres riesgos identificados comparten un origen: en un ecosistema, la aseguradora deja de controlar en solitario partes del proceso que hasta ahora gobernaba de principio a fin.

Barreras y desafíos

Tres riesgos de colaborar en ecosistemas: el dato, la responsabilidad y el cliente

Riesgo	Apoyo en las fuentes	Lectura estratégica
Pérdida de control Sobre la suscripción, la tarificación y el fraude al compartir datos sensibles con los socios.	Las aseguradoras citan la posible **fuga de información sensible** de clientes entre los factores que frenan la adopción tecnológica. KPMG recoge su preocupación por conservar la **propiedad intelectual** de lo que se construye con los socios.	**El dato, el activo que se comparte** Compartir la información acumulada (suscripción, tarificación y fraude) multiplica el valor y también el riesgo de fuga de datos, accesos no autorizados y ciberataques, según EIOPA. Además, exige preservar la propiedad intelectual (KPMG).
Responsabilidad difusa En la venta, los siniestros y el cumplimiento normativo.	KPMG advierte de que las alianzas que generan **exposición regulatoria o riesgo operativo** destruyen valor. NTT Data indica que cerca del **68 %** de las aseguradoras ve la **gobernanza y el cumplimiento** como barreras para escalar la IA.	**La aseguradora conserva la responsabilidad** Aunque se repartan tareas, la aseguradora sigue siendo plenamente responsable ante el cliente y el supervisor (DORA). Por ello, la gobernanza y el cumplimiento (**68 %** de las aseguradoras) son clave para escalar la IA.
Desplazamiento de la red comercial Pérdida de la relación con el cliente frente a quien orquesta el ecosistema.	La distribución a través de **canales de IA conversacional** ya está alterando la economía de la intermediación. NTT Data subraya que la colaboración debe **proteger la relación con el cliente**.	**La relación con el cliente, en disputa** Quien orquesta el ecosistema (plataforma, asistente de IA o distribuidor digital) tiende a quedarse con el contacto y el conocimiento del cliente. Esto ya afecta a la intermediación y obliga a revisar los costes de captación y la estrategia de distribución.

Fuente: Vecdis, con datos de EIOPA, KPMG, NTT Data y MarketsandMarkets.

[42] Ibíd.

07 Conclusión: de experimentar a escalar con control

Cada tendencia responde a una dimensión distinta del control, pero todas conducen a la misma conclusión: la ventaja competitiva no estará en experimentar más, sino en escalar lo que funciona sin perder el gobierno de la decisión, el coste, el dato, la producción y las alianzas.

Las cinco tendencias no avanzan de forma aislada. El control de la decisión condiciona qué casos de IA llegan a producción; FinOps determina si esos casos son sostenibles en coste; la infraestructura fija dónde se procesan sus datos y con qué resiliencia, y los ecosistemas trasladan esas mismas preguntas a la relación con terceros.

Entre ellas aparecen también tensiones. Ampliar la autonomía de la IA exige delimitar con más precisión la responsabilidad humana; crecer en red abre canales nuevos, pero reparte el control del dato y de la relación con el cliente, y concentrar servicios en pocos proveedores gana eficiencia a costa de capacidad de salida.

De cara a 2027 quedan cuestiones abiertas: el ritmo al que la IA agéntica pasará de los pilotos a los procesos core, el alcance final de la propuesta CADA sobre el sector privado y los resultados de alianzas aún recientes, como la de MAPFRE y Tuio.

Las cinco tendencias de un vistazo

Qué dice el dato y qué debe hacer Mutualidad

La ventaja está en escalar con control

Tendencia y pregunta	Dato clave	Claves de la tendencia	Caso de referencia	Clave para Mutualidad
1 IA agéntica supervisada *¿Quién decide?*	**9 %** de los casos de IA generativa son agénticos	La IA prepara. El profesional decide. La autonomía se amplía por fases y se generaliza en 3–5 años.	**Zurich–Cytora** Triaje de 75 a 15 min. El suscriptor decide.	**Ampliar la autonomía de forma gradual, con un responsable por decisión.**
2 FinOps *¿Cuánto cuesta la tecnología y qué devuelve?*	**98 %** de los equipos FinOps ya gestionan gasto en IA (31 % en 2024)	FinOps gobierna todo el gasto tecnológico. Los ahorros de optimización financian la IA.	**Allianz Ayudhya** –24 % de coste operativo tras migrar a la nube.	**Llevar FinOps al comité de dirección y medir el coste por caso de uso de IA.**
3 Infraestructura híbrida *¿Dónde está el dato y quién lo controla?*	Casi el **80 %** confía su almacenamiento cloud a BigTech	DORA obliga hoy. CADA anticipa la soberanía del dato. El riesgo es depender sin poder salir.	**Helvetia** 200 apps en un año, con controles desde el diseño.	**Mapear los proveedores y controlar el dato conforme a DORA.**
4 Escalar la IA *¿Qué llega a producción?*	Solo el **32 %** de los casos de IA generativa está en producción	Industrializar lo que funciona con criterios repetibles y resultados medibles.	**MAPFRE** Centro de IA con más de 150 casos desarrollados en 2025.	**Fijar criterios comunes para pasar de piloto a producción.**
5 Ecosistemas digitales *¿Quién responde ante el cliente?*	En torno al **63 %** ve los ecosistemas como motor de crecimiento	Decisión de gobierno. El control prima sobre el ahorro. Hay margen en un canal digital aún incipiente.	**MAPFRE–Tuio** Más del 20 % de nuevos clientes vía asistentes de IA.	**Ser titular de la relación con el mutualista y del dato.**

Condición común | Escalar sin comprometer la confianza de los mutualistas

Fuente: Vecdis.

Mutualidad

Sobre el Radar Digital

Misión

Constituimos el radar **#MutualidadDigital** como un lugar de encuentro para compartir intereses relacionados con la estrategia digital del sector asegurador y Mutualidad, basado en tres ejes:

- **Centro de análisis de datos**. Consideramos el radar como una herramienta de ayuda en la toma de decisiones. La misión principal será recoger, procesar y proporcionar información que sirva para conocer y comprender la digitalización del sector asegurador y concretamente de la Mutualidad mediante estudios con la participación de expertos (tanto internos como externos).
- **Espacio de información, intercambio y colaboración** (difundir la información además de promover la reflexión y el intercambio del co-

RADAR DIGITAL Mutualidad

- Informar de los hallazgos y evaluar la evolución digital de la Mutualidad dentro de su PE 27.
- Acelerar la toma de decisiones y su paso a la acción.

Objetivos

- Detectar tendencias digitales, explorar oportunidades, diseñar estrategias y lanzar proyectos.
- Research & Advisory para convertir la información en conocimiento.
  - Interpretar las dinámicas del mercado.
  - Confirmar las líneas digitales marcadas en la Mutualidad.

Funciones