EL SOFTWARE YA ES PRODUCTO. LONDRES YA ASEGURA LA IA. ¿Y NUESTRAS PÓLIZAS DE RC?



Lo que el mercado británico ya está cubriendo, lo que la Directiva (UE) 2024/2853 exigirá desde el 9 de diciembre de 2026 y los vacíos que quedarán entre ambos si no adaptamos a tiempo los wordings de Responsabilidad Civil.

Por qué escribo esto ahora.

El jueves 15 de octubre, Expansión dedicó dos páginas de su sección de Finanzas y Mercados al seguro ante los riesgos de la inteligencia artificial. La primera pieza explicaba cómo Londres aspira a convertirse en el gran centro mundial de los seguros de IA, con CFC, Chaucer, Armilla, Beazley y Testudo ofreciendo ya coberturas explícitas. La segunda cuantificaba el crecimiento del seguro de ciberriesgos hasta cerca de 28.000 millones de dólares en 2030 y cerraba con un aviso que me parece lo más importante de todo: la cobertura está fragmentada y existe un «riesgo de brecha» en el que ninguna póliza individual responde de forma integral.

Leí ambos artículos con la Directiva (UE) 2024/2853 sobre la mesa. Desde enero trabajamos en Grupo Galilea en su impacto sobre las pólizas de Responsabilidad Civil de nuestros clientes, y la conexión entre ambas realidades me parece evidente. Curiosamente, casi nadie la está haciendo en voz alta: **Londres está aprendiendo a asegurar el fallo del software y de la IA justo cuando Europa convierte ese mismo fallo en responsabilidad objetiva del fabricante.** Faltan menos de dos meses para el 9 de diciembre.

En estas páginas hago tres cosas. Primero, repaso lo que el mercado británico está ofreciendo realmente, separando el dato del titular. Segundo, explico qué dice la Directiva sobre el software, las actualizaciones y la ciberseguridad. Y tercero, doy mi opinión como corredor sobre dónde encajan ambas cosas, qué riesgos

se nos vienen encima y qué huecos de cobertura quedarán si los contratos no se adaptan a tiempo.

Lo que Londres ya está asegurando

Hay que reconocerlo: el mercado británico va por delante, y la cronología de este mismo año lo demuestra. En febrero, Chaucer y Armilla lanzaron Vanguard AI, que combina el Cyber y la Tech E&O de Chaucer con una capa autónoma de responsabilidad por IA de Armilla, con reglas de asignación predefinidas entre las tres coberturas. En marzo, HSB (Munich Re) presentó su seguro de responsabilidad por IA para pequeñas empresas. En junio, CFC incorporó cobertura afirmativa de IA en siete líneas: Tech E&O, RC Profesional, eHealth, Propiedad Intelectual, Management Liability, Media y Cyber, con mención expresa a la alucinación del modelo, al contenido generado por IA y al model drift. En septiembre, Beazley confirmó su cobertura afirmativa de IA dentro de Cyber y Tech E&O. Testudo, coverholder de Lloyd's con capacidad liderada por Apollo, ofrece límites de entre uno y diez millones de dólares frente a alucinaciones, difamación, propiedad intelectual o datos. Y Hiscox UK anuncia cobertura de IA «explícita y afirmativa» dentro de su oferta tecnológica.

Conviene, eso sí, leer con matices. Lo de Beazley es más una confirmación afirmativa de lo que el ciber ya cubría que una cobertura nueva. Testudo y HSB están pensados sobre todo para empresas norteamericanas, y nacen en buena parte para tapar las exclusiones de IA generativa que entraron en las pólizas de RC General estadounidenses el 1 de enero de 2026. Y el producto de HSB para pymes tiene un detalle relevante para nosotros: cubre expresamente lesiones corporales y daños materiales causados por el uso de IA, algo que algunas pólizas de RC General excluyen.

Las cifras de contexto apuntan en la misma dirección. Lloyd's cerró 2025 con 57.900 millones de libras en primas brutas y un ratio combinado del 87,6%. Deloitte prevé que las primas específicas de IA alcancen los 4.800 millones de dólares en 2032, con un crecimiento cercano al 80% anual. Munich Re estima que el ciberseguro global pasará de unos 15.000 millones de dólares en 2025 a unos 28.000 en 2030, aunque esa cifra incluye todo el ciber y no aísla cuánto corresponde a la IA. Y un dato que invita a la prudencia: en Estados Unidos, según el informe de la NAIC, casi tres de cada cuatro reclamaciones de ciberseguro se cerraron sin pago (28.555 frente a 9.941 con pago). «Sin pago» no equivale siempre a rechazo, porque incluye retiradas e importes por debajo de franquicia, pero ilustra lo difícil que es hoy cobrar un siniestro tecnológico.

Si se mira con detalle, el patrón es claro:

- **La cobertura afirmativa de IA en Londres se está construyendo sobre las líneas financieras**: Tech E&O, RC Profesional, Cyber, Media y D&O. Es lógico, porque es donde hoy se concentran las reclamaciones.

- **La RC General y de Productos va en dirección contraria, al menos en EE. UU.** Desde el 1 de enero de 2026, Verisk/ISO ofrece endosos opcionales de exclusión de IA generativa para la póliza de RC General (CG 40 47, CG 40 48 y CG 35 08).

- **Los propios suscriptores de Lloyd's no ven aún la IA como un riesgo de producto.** En la encuesta de la Lloyd's Market Association de enero, el escenario de retirada de productos (product recall) por IA se calificó como muy improbable, por el uso todavía limitado de la IA en diseño y fabricación.

- **El Reino Unido reconoce que su propia ley tiene el mismo problema.** El 8 de octubre, la Law Commission abrió una consulta para reformar la Consumer Protection Act de 1987, que considera «ya no adecuada», entre otras cosas por su incertidumbre ante el software y la IA, y advierte de que el régimen actual puede exponer a las aseguradoras a riesgos imprevistos. La consulta cierra el 14 de enero de 2027.

Mi lectura: Londres está resolviendo muy bien la pregunta «¿qué pasa si la IA de mi cliente hace perder dinero a otro?». Pero casi todo lo que se ha lanzado se mueve en las líneas de pérdida financiera. Y la Directiva europea no actúa ahí. Actúa en la RC de Productos.

Lo que dice exactamente la Directiva

Conviene ir al texto, porque en estas semanas se está diciendo de todo. Estos son los artículos que, en mi opinión, cambian el riesgo asegurable de un fabricante, un importador o un integrador de software:

Artículo	Qué establece	Por qué importa al seguro
Art. 4.1, 4.3 y 4.4	El «producto» incluye expresamente el software y los archivos de fabricación digital. Los «servicios conexos» digitales y los componentes intangibles son componentes del producto.	Muchas pólizas definen «producto» como bien material. El software queda fuera de la definición o dentro de una exclusión.
Art. 4.5	El fabricante mantiene el «control» del producto mientras suministra, o puede suministrar, actualizaciones o mejoras de software.	El producto ya no «sale» del fabricante el día de la entrega: sigue vivo. El hecho generador de muchas pólizas se ancla a la fabricación o a la entrega.
Art. 7.2 c), e) y f)	Para valorar si un producto es defectuoso se tiene en cuenta su capacidad de seguir aprendiendo, el momento en que sale del control del fabricante y los requisitos de ciberseguridad.	El aprendizaje automático y la ciberseguridad pasan a ser criterios de defecto. Una vulnerabilidad puede ser un defecto.
Art. 11.2	No hay exoneración cuando el defecto se debe al software, a sus actualizaciones, a la falta de actualizaciones necesarias para mantener la seguridad o a una modificación sustancial.	No parchear se convierte en fuente de responsabilidad objetiva.
Art. 13.1	La responsabilidad no se reduce cuando el daño lo causan a la vez el defecto y un tercero.	Si un hacker explota una vulnerabilidad, el fabricante sigue respondiendo frente a la víctima.
Art. 15	La responsabilidad no puede limitarse ni excluirse por contrato frente al perjudicado.	Las limitaciones contractuales solo servirán, en su caso, para el recobro entre operadores.
Art. 8	Responden el fabricante, el fabricante del componente y, si el fabricante está fuera de la UE, el importador, el representante autorizado o el prestador de servicios logísticos. Quien modifica sustancialmente un producto se convierte en fabricante.	Un importador español de equipos británicos o americanos con software pasa a ser el responsable directo en Europa.
Arts. 9 y 10	Exhibición de pruebas y presunciones de defecto y de causalidad, también por complejidad técnica o científica excesiva.	Más condenas y más coste de defensa: peritos, documentación técnica, código y registros.
Art. 6.1	Daños indemnizables: muerte, lesiones (incluidas las psicológicas reconocidas médicamente), daños a bienes y destrucción o corrupción de datos no usados con fines profesionales.	El daño a datos aparece como daño de RC de Productos, algo que la mayoría de pólizas excluye.
Art. 17	Plazo de diez años, ampliable a veinticinco en lesiones de manifestación tardía.	Cola muy larga. Las pólizas claims made sin periodos de descubrimiento adecuados se quedan cortas.
Arts. 2.1 y 21	Se aplica a los productos introducidos en el mercado o puestos en servicio después del 9 de diciembre de 2026. La Directiva de 1985 sigue rigiendo para los anteriores.	Durante años convivirán dos regímenes en la misma cartera y, a veces, en la misma póliza.

Hay dos límites que conviene no olvidar, porque he visto artículos que los pasan por alto.
El derecho a indemnización bajo la Directiva corresponde a **personas físicas** (art. 5.1), y quedan fuera los bienes y los datos usados exclusivamente con fines profesionales (art. 6.1).
Es decir, la Directiva protege sobre todo al consumidor y al tercero persona física.
Las reclamaciones entre empresas seguirán discurriendo por el derecho contractual y extracontractual nacional. Eso no reduce el problema: lo desplaza, porque al final de cada cadena B2B suele haber un consumidor.

Dos datos de contexto más. La Comisión retiró formalmente en octubre de 2025 la propuesta de Directiva sobre responsabilidad por IA, de modo que **la Directiva de productos defectuosos se convierte en la vía principal de reclamación en Europa por daños causados por sistemas de IA.** Y, en la fecha en que escribo, EUR-Lex no recoge ninguna medida nacional de transposición comunicada por España. Como es sabido, las directivas no despliegan, como regla general, eficacia directa entre particulares, pero los jueces españoles sí están obligados a interpretar el derecho interno de conformidad con ellas. Esperar a la ley española para mover ficha me parece un error.

Dónde se tocan ambas realidades

El denominador común de lo que ocurre en Londres y de lo que dice la Directiva es el mismo: **la mala gestión del software.** No solo el ataque malicioso, sino algo mucho más cotidiano: una actualización que se envía sin pruebas suficientes, un parche de seguridad que no se publica, un modelo que «deriva» y empieza a tomar decisiones distintas de las previstas, un integrador que modifica el firmware de un equipo o un fabricante que deja de dar soporte a una gama antigua que sigue conectada a internet.

Londres está poniendo nombre y precio a esos eventos. CFC habla expresamente de alucinaciones y de model drift. Chaucer y Armilla describen fallos de decisión automatizada que generan daño incluso cuando no ha habido intrusión ni negligencia. Esa última idea es, casi literalmente, la definición de responsabilidad objetiva. La Directiva dice lo mismo desde el lado jurídico: no hace falta culpa, basta con defecto, daño y nexo causal, este último a menudo presunto.

Un caso real de hace pocas semanas

El ciberataque a los supermercados franceses del 12 de octubre es el mejor ejemplo que podía imaginar. Los atacantes tomaron el control del software de control remoto de Danfoss que regula las cámaras de frío y las mantuvieron en ciclo de descongelación, con temperaturas de hasta 50 grados. El ministro de Finanzas francés habló de unos 700 supermercados afectados. Según informó AFP, el fabricante explicó que la mayoría de los equipos eran modelos antiguos que ya no recibían actualizaciones de software ni de seguridad. Y la fiscalía de París investiga además varios incendios.

Ese caso concreto se rige por el régimen anterior, porque los equipos se pusieron en el mercado antes del 9 de diciembre de 2026. Pero hagamos el ejercicio de imaginar el mismo ataque sobre equipos vendidos en 2027:

• Las pérdidas de los supermercados (mercancía, instalaciones) son daños a bienes de uso profesional. Quedan **fuera** de la Directiva y se reclamarán por la vía contractual, donde jugarán las limitaciones de responsabilidad del contrato de suministro.

• Pero si un cliente enferma por consumir producto cuya cadena de frío se rompió, o si un incendio daña la vivienda o el vehículo de un tercero, eso **sí** es daño de la Directiva. El fabricante responde, aunque el causante material sea un hacker (art. 13.1) y no podrá exonerarse alegando que el defecto surgió después de la venta si el origen es la falta de actualizaciones de seguridad bajo su control (art. 11.2).

• Si el fabricante es de fuera de la UE, la reclamación se dirigirá al importador o al representante autorizado (art. 8.1 c). Y si un instalador local modificó sustancialmente el sistema, puede ser tratado como fabricante (art. 8.2).

Y llega la pregunta clave: **¿qué póliza responde?** La RC de Productos del fabricante, en muchos casos, excluirá el ciberriesgo, el software o los datos. Su póliza de Cyber cubre sus propios daños y su responsabilidad por privacidad, pero normalmente excluye las lesiones corporales y los daños materiales.

Su Tech E&O, si la tiene, está pensada para la pérdida
financiera de su cliente, no para lesiones de terceros. Ese espacio que queda entre las tres pólizas es exactamente lo que el despacho Fenwick ha bautizado como «riesgo de brecha» o gap risk: una fragmentación entre Cyber, Tech E&O, D&O y EPLI, con exclusiones que se van apilando.

Hay además un efecto de frontera que me preocupa especialmente. Desde el Brexit, un fabricante británico es un fabricante de fuera de la UE. Puede tener una excelente póliza de Tech E&O con cobertura afirmativa de IA en Londres. Pero cuando su equipo con software cause un daño a un consumidor español, la Directiva permitirá reclamar **al importador o al representante autorizado en Europa**. Y ese importador, con mucha probabilidad, tiene una RC General de pyme con una garantía de productos pensada para bienes tangibles.

Dónde están los gaps de cobertura

El siguiente cuadro resume mi lectura profesional de dónde chocan los riesgos de la Directiva con los clausulados habituales del mercado. No describe una póliza concreta, sino los patrones que encontramos con frecuencia al revisar wordings de RC General, RC de Productos y multirriesgos con garantía de RC.

Escenario bajo la Directiva	Respuesta habitual hoy	Gap que veo
Lesión o daño material causado por un fallo del software integrado en un equipo.	La RC de Productos define «producto» como bien material o excluye software, datos o «errores de programación». La Tech E&O suele excluir lesiones y daños materiales.	Alto. El siniestro cae entre dos pólizas y ninguna lo acoge con claridad.
Actualización remota defectuosa meses después de la venta.	El hecho generador se ancla a la fabricación, la entrega o la puesta en circulación.	Alto. Discusión sobre la fecha del siniestro y sobre si la actualización es «producto».
Falta de parche de seguridad y ataque de un tercero.	Exclusiones de ciberriesgo en la RC y exclusión de lesiones y daños materiales en el Cyber.	Muy alto. El art. 13.1 impide trasladar la culpa al hacker frente a la víctima.
Destrucción o corrupción de datos personales del consumidor.	Exclusión general de datos o de «daños inmateriales» en la RC.	Alto. Es un daño nuevo en la RC de Productos y suele estar excluido.
Sistema de IA que aprende y cambia su comportamiento (model drift).	No previsto. En algunas líneas aparecen ya exclusiones absolutas de IA.	Alto y creciente. Riesgo de exclusiones silenciosas por cambios en las definiciones.
Importador o representante de un fabricante británico o americano.	Actividad declarada como «distribuidor»; límites territoriales; sin RC de Productos estructurada.	Alto. El asegurado cree estar cubierto y no lo está.
Reacondicionador o integrador que modifica sustancialmente un equipo.	No figura como fabricante en la actividad declarada.	Medio a alto. Problema de declaración del riesgo.
Exhibición de pruebas y presunciones.	Sublímites de defensa pensados para un litigio clásico.	Medio. El coste pericial e informático puede agotar el sublímite.
Lesiones de aparición tardía (hasta 25 años).	Claims made con retroactividad y periodo de descubrimiento cortos.	Medio a largo plazo. Riesgo de cola sin respaldo.
Siniestro en serie por una misma actualización enviada a miles de equipos.	Cláusulas de unidad de siniestro y agregados no pensados para eventos digitales.	Alto. La IA y las actualizaciones replican el error a escala.

Los riesgos que vienen

Quiero ser claro, porque creo que el sector necesita esta conversación sin eufemismos.

• **Vamos a reproducir el error del silent cyber.** Durante años, las pólizas de daños y RC cubrieron, o no, el riesgo cibernético sin decirlo, hasta que el mercado tuvo que aclararlo póliza por

póliza. Con el software y la IA en la RC de Productos estamos exactamente en el mismo

punto, con una diferencia: esta vez la ley nos ha avisado de la fecha.

• **El riesgo de frecuencia es nuevo.** Un error mecánico afecta a un lote. Una actualización defectuosa o un modelo que falla puede afectar a todos los equipos conectados a la vez. La aseguradora de agentes de IA Harbor lo describe de forma muy gráfica: el error de un agente se repite, quizá miles de veces, hasta que alguien lo detecta. Eso tensiona límites, agregados y cláusulas de serie.

• **El mercado se va a endurecer antes de abrirse.** El precedente americano es elocuente: primero llegaron las exclusiones en la RC General y después los productos especializados para tapar el hueco. Si en Europa ocurre lo mismo, muchas empresas recibirán en 2027 un suplemento que, en vez de ampliar, aclarará lo que no cubre. Prefiero que eso lo descubran ahora, en una revisión, y no en un siniestro.

• **La pyme industrial española es la más expuesta.** Las grandes cuentas tienen programas internacionales, a menudo colocados en Londres. La pyme fabricante, importadora o instaladora de equipos conectados tiene, con frecuencia, una RC incluida en un multirriesgo, con un condicionado general pensado para otra realidad. Y es precisamente quien más productos con software está poniendo en el mercado.

• **El corredor también está en el perímetro.** Cuando cambia el marco legal en el que opera el cliente, aunque no cambie su actividad, el deber de asesoramiento no se suspende. Si nadie le avisa, no es un fallo del cliente. Es nuestro.

Qué propongo hacer antes del 9 de diciembre

Para las empresas

• Inventariar qué productos llevan software, conectividad, actualizaciones remotas o IA, y cuáles se venderán después del 9 de diciembre.

• Revisar juntas la RC de Productos, la Cyber y la Tech E&O, si existe. No basta con leer cada una por separado: hay que comprobar qué póliza responde a cada escenario del cuadro anterior.

• Revisar los contratos con proveedores de software y componentes: limitaciones de responsabilidad, obligaciones de actualización y derechos de repetición.

• Documentar la política de actualizaciones y de fin de soporte. Bajo la Directiva, esa documentación será prueba.

Para las aseguradoras

• Redefinir de forma expresa «producto», «componente» y «servicio conexo», en línea con el art. 4 de la Directiva.

• Decidir y escribir qué se cubre en actualizaciones, falta de actualizaciones, aprendizaje automático y vulnerabilidades. Cubrir o excluir, pero no callar.

• Coordinar la RC de Productos con Cyber y Tech E&O, como ha hecho Vanguard AI en Londres con sus reglas de asignación entre coberturas.

• Emitir suplementos de adaptación para las pólizas en vigor que crucen el 9 de diciembre.

Para los corredores

• Identificar la cartera expuesta: fabricantes, importadores, integradores, reacondicionadores, plataformas y cualquier cliente con productos conectados.

• Exigir por escrito a cada aseguradora su posición sobre la Directiva. Si no adapta el condicionado, que lo diga expresamente.

• Proponer un endoso de adaptación. En Grupo Galilea hemos redactado una cláusula tipo que redefine «producto», amplía el perímetro de asegurados, incorpora el daño a datos y regula el ciclo de vida del producto y las actualizaciones.

• Cuando el mercado local no dé respuesta, explorar capacidad especializada, incluida la de Londres, entendiendo bien que su cobertura afirmativa de IA está hoy en las líneas financieras y que habrá que trasladarla a la RC de Productos.

• Documentar el asesoramiento. Si el cliente decide no actuar, que conste que fue informado.

Conclusión

El mercado de Londres se está organizando para asegurar la inteligencia artificial, y lo hace bien. La Directiva europea va a convertir el fallo del software, incluida la falta de actualizaciones, en responsabilidad objetiva del fabricante y de toda su cadena. **Las dos realidades llegan a la vez, pero todavía no se han encontrado.** Londres asegura la IA en las líneas financieras; Europa la va a reclamar en la RC de Productos.

El 9 de diciembre no cambia el riesgo de un día para otro: cambia quién lo paga. Si nuestros contratos no se adaptan a tiempo, ese coste recaerá sobre empresas que creen estar cubiertas y no lo están. Evitarlo es, hoy, nuestro trabajo.

La pregunta ya no es si su empresa usa software o IA. Es si su póliza de Responsabilidad Civil sabe que lo hace.

Casimiro Rey

Director de Empresas y Negocio Internacional
Miembro del Comité de Dirección
Grupo Galilea S.L. (Söderberg & Partners)

Este artículo expresa la opinión profesional de su autor y tiene carácter divulgativo. No constituye asesoramiento jurídico ni análisis de una póliza concreta. Las valoraciones sobre clausulados reflejan patrones habituales del mercado, no el condicionado de ninguna aseguradora en particular.