Quién paga cuando falla la IA

El fabricante de Claude advirtió que su seguro podría no alcanzar, casi una de cada cuatro empresas que ya usan IA no sabe quién responde y un banco ya les cerró la puerta a los agentes, por lo que la respuesta está en el contrato que tu empresa firma hoy con quien le vende IA.

Por Oscar Obando Chaves · Chief AI Officer · Legal AI Engineer · Noviembre 2026 · Documento de distribución libre · Publicado originalmente en LinkedIn

El fabricante no está seguro de su seguro

El fabricante de Claude le advirtió a la SEC que su seguro podría no alcanzar si su IA causa un daño grande. Anthropic lo escribió entre los factores de riesgo del prospecto que hizo público el 26 de octubre de 2026 para salir a bolsa, donde reconoce que sus modelos pueden comportarse de formas que nadie buscó y que el mercado de seguros para la IA recién empieza.

Si el fabricante del modelo no está seguro de su seguro, tu empresa difícilmente puede contar con él, y tu propia póliza puede traer sus exclusiones. Todo esto ocurre cuando casi una de cada cuatro empresas que ya usan IA no tiene claro quién responde si la IA produce un mal resultado y un banco ya les cerró la puerta a los agentes.

Fuentes: Anthropic, PBC, formulario S-1 ante la SEC (26 de octubre de 2026), págs. 51 y 94.

Lo que dice el prospecto

En la página 51 del formulario S-1, Anthropic escribió que ninguna aseguradora, y quizá ni la industria de seguros en su conjunto, podría tener la capacidad para asegurar el daño de un incidente catastrófico de IA. Entre los mismos factores de riesgo advirtió que sus pólizas podrían no alcanzar y que el mercado de seguros para los riesgos propios de la IA recién empieza.

El mismo prospecto preliminar muestra, en sus páginas 51 y 94, que el proveedor que limita su responsabilidad en sus términos de servicio, con exclusiones de garantía y topes, acepta en ciertos contratos defender e indemnizar sin tope a la contraparte si lo que genera su modelo infringe la propiedad intelectual de otros. La diferencia está en lo que cada uno negoció con él.

Fuentes: Anthropic, PBC, formulario S-1 ante la SEC, prospecto preliminar (26 de octubre de 2026), págs. 51 y 94, en traducción propia.

Lo que hacen las empresas y lo que hizo un banco

El Deloitte AI Institute encuestó entre mayo y junio de 2026 a 3.500 líderes de empresas que ya usan IA en 25 países, y publicó el 29 de octubre su informe The State of AI in the Enterprise. Ahí encontró que el 40 % deja que la IA ejecute decisiones o acciones sin aprobación humana, al menos en grado moderado, y que el 23 % no tiene claro quién responde cuando la IA produce un mal resultado.

El 27 de octubre de 2026 el Royal Bank of Canada anunció que bloqueará el acceso directo de los agentes de IA personales a su banca en línea y que las conexiones que ya existen dejarán de funcionar. Su garantía de seguridad para la banca digital no cubre a quien comparte sus contraseñas o autoriza una operación, que es lo que hace quien le entrega su banca a un agente.

Fuentes: Deloitte AI Institute, The State of AI in the Enterprise (29 de octubre de 2026), con 3.500 líderes de 25 países encuestados entre mayo y junio de 2026; RBC, aviso sobre agentes de IA de terceros (27 de octubre de 2026), y RBC Digital Banking Security Guarantee.

La cadena, del proveedor del modelo a tu cliente

Puestas en fila, esas piezas forman una cadena en la que el proveedor del modelo advierte que su seguro podría no alcanzar y tu póliza puede traer exclusiones para los daños causados con IA, que conviene leer antes del incidente.

Tu banco puede negarse a devolver lo que se pierda si un agente usó tus claves, y al final de esa cadena está tu cliente, que le reclama a tu empresa, puesto que es la que lo atendió.

Fuentes: Anthropic, PBC, formulario S-1 (26 de octubre de 2026), y RBC Digital Banking Security Guarantee.

Lo que una empresa mediana puede pedir en su contrato

Quién paga cuando falla la IA se escribe en el contrato que tu empresa firma hoy con quien le vende IA, donde una empresa mediana puede pedir seis puntos, y hay un séptimo que se escribe dentro de casa.

1. Indemnidad, para que el proveedor responda si lo que genera su modelo infringe derechos de otros.

2. Topes, que digan hasta cuánto responde si falla y frente a qué daños.

3. Aviso de incidentes, con el plazo en horas para avisarte si sus sistemas o tus datos quedan expuestos.

4. Cambios de modelo, con aviso previo cuando cambie el modelo que usas, para probarlo antes de que atienda a tus clientes.

5. Tus datos, con lo que el contrato dice sobre si el proveedor los usa para entrenar, dónde quedan y cómo se borran.

6. Salida, con la forma en que te llevas tus datos y tus instrucciones si cambias de proveedor.

7. Dentro de tu empresa, quién autoriza a cada agente, con qué claves y hasta dónde.

Ninguna aseguradora, y quizá ni la industria de seguros en su conjunto, podría tener la capacidad para asegurar el daño de un incidente catastrófico de IA.

Anthropic, PBC, factores de riesgo del formulario S-1 ante la SEC, 26 de octubre de 2026, pág. 51 (traducción propia)

Oscar Obando Chaves es Chief AI Officer y Legal AI Engineer ecuatoriano, con formación en derecho. Ayuda a las empresas a decidir cómo usan la IA y construye con ella sistemas para el negocio y para lo legal. Chief AI Officer y Senior AI Counsel en HEKA Law, ISO 42001 AI Management Leader e ISO 38507 AI Governance Leader. Publica análisis semanal sobre el impacto real de la IA.