

12 señales de alerta tecnológicas antes de invertir

Lista de una página elaborada por Evgeny Goncharov (Alarifa, Madrid). Puede reenviarla libremente a sus clientes.

Para inversores, asesores de M&A y abogados que analizan una empresa cuyo valor depende de su tecnología. Una señal de alerta no es motivo para abandonar la operación. Es una pregunta que conviene responder antes de firmar y, a menudo, algo que reflejar en el precio o en el contrato.

N.º	SEÑAL DE ALERTA	QUÉ PREGUNTAR
01	Dependencia de una sola persona. Un ingeniero, un fundador o una agencia externa concentra el conocimiento, el código o los accesos de administración.	¿Quién mantendría el sistema en marcha si esa persona se fuera mañana? ¿Hay algo documentado?
02	Titularidad del código poco clara. Software desarrollado por autónomos o agencias sin cesión escrita de la propiedad intelectual; licencias de código abierto sin revisar.	¿Hay cesiones de propiedad intelectual firmadas por todos los que han escrito código? ¿Se han revisado las obligaciones de las licencias de código abierto?
03	Sin mapa de datos personales. Nadie sabe decir dónde están los datos de clientes, quién los trata ni con qué base jurídica.	¿Existe un registro de actividades de tratamiento conforme al RGPD? ¿Hay contratos de encargo del tratamiento con cada proveedor?
04	Promesas de IA que el producto no sostiene. «IA» que en realidad es un conjunto de reglas o trabajo manual, o modelos entrenados con datos que la empresa quizá no tenga derecho a usar.	¿Qué es exactamente el modelo, cómo se mide su rendimiento y de dónde salen los datos de entrenamiento? ¿Algún uso entra en las categorías de mayor riesgo del Reglamento Europeo de IA?
05	Uso descontrolado de herramientas de IA. La plantilla introduce datos de clientes o de la empresa en herramientas que nadie ha aprobado.	¿Hay una política de IA por escrito? ¿En qué herramientas han acabado datos de la empresa?
06	Costes tecnológicos que crecen más que los ingresos. El gasto en nube, licencias y subcontratación sube con cada cliente nuevo.	¿Cuánto cuesta la tecnología por cliente o por transacción, y cómo ha evolucionado?
07	Deuda técnica sin plan. Frameworks obsoletos, versiones sin soporte y miedo a tocar cualquier cosa.	¿Qué reconstruiría primero el equipo, y cuánto tiempo y dinero costaría?
08	Copias de seguridad nunca probadas. Existen, pero nunca se ha restaurado nada a partir de ellas.	¿Cuándo se hizo la última prueba de restauración completa y cuánto tardó?
09	Control de accesos débil. Contraseñas compartidas, ausencia de doble factor y antiguos empleados que siguen teniendo acceso.	¿Quién tiene hoy permisos de administrador y cuándo se revisaron los accesos por última vez?
10	Dependencia de un único proveedor. Una plataforma crítica sin condiciones de salida, o datos que no se pueden exportar.	Si el proveedor principal subiera los precios o cerrara, ¿cómo podría la empresa cambiar de proveedor y llevarse sus datos?
11	Sin historial de seguridad. Ni pruebas de penetración, ni registros de actividad (logs), ni constancia de incidentes pasados.	¿Se ha hecho una prueba de seguridad independiente? ¿Qué incidentes ha habido y se notificaron cuando era obligatorio?
12	Entregas que dependen de sobreesfuerzos y de apagar fuegos. Sin proceso de despliegue, sin pruebas automáticas, sin monitorización. Una hoja de ruta que promete mucho más de lo que se entrega.	¿Con qué frecuencia pone el equipo versiones en producción, cómo revierte un despliegue fallido y qué parte de lo planificado el año pasado se llegó a entregar?

Cómo usarla. Envíe la columna «Qué preguntar» a la dirección de la empresa objetivo antes de entrar en el data room. Las respuestas vagas ya son una señal. Para una due diligence tecnológica a precio cerrado sobre una empresa (señales de alerta, riesgo de IA y de datos, y un plan tecnológico de 100 días), escriba a eg@alarifa.com.