Lista de preguntas para founders

Estas son las preguntas técnicas que hago a un founder en una primera reunión, y lo que escucho en las respuestas. No reemplazan una revisión, pero suelen mostrar dónde están los riesgos reales.

1. Arquitectura y cloud. ¿Cómo está alojado el producto, y qué se rompería primero si tuvieran tres veces más clientes?

Buena señal: Pueden nombrar el proveedor, la base de datos y un cuello de botella concreto, con un plan para crecer sin reescribir todo.
Señal de alerta: Un "estamos en la nube" vago, o ya plantean una reescritura como la única forma de crecer.

2. Cómo publican los cambios. ¿Cómo llega un cambio a producción, y puede hacerlo otra persona si no estás?

Buena señal: Las pruebas y el armado corren solos, alguien aprueba producción, y pueden volver atrás en un paso.
Señal de alerta: Los deploys salen de una sola computadora, y si esa persona no está, no hay releases.

3. Pruebas. ¿Qué partes del producto tienen pruebas automatizadas, y cuáles se revisan a mano?

Buena señal: Los flujos de pago e inicio de sesión tienen pruebas que bloquean un mal cambio, y saben dónde la cobertura es floja.
Señal de alerta: "Probamos a mano antes de cada salida," o no pueden decir qué está cubierto.

4. Accesos y bajas. ¿Quién tiene acceso de administrador a producción, al código y a la cuenta de cloud? ¿Qué pasa cuando alguien se va?

Buena señal: Personas con nombre y apellido, MFA obligatorio, y una lista corta que ya usaron para dar de baja a alguien.
Señal de alerta: Usuarios compartidos, MFA opcional, o ex contratistas que quizá siguen teniendo acceso.

5. Backups. ¿Cuándo fue la última vez que restauraron un backup de producción, y cuánto tardó?

Buena señal: Una prueba de restore con fecha, un tiempo de recuperación conocido, y backups en un lugar que una sola clave filtrada no pueda borrar.
Señal de alerta: "Los backups están activos," pero nadie restauró uno nunca. El tiempo de recuperación es una suposición.

6. Caídas. ¿Cómo se enteran de que el producto está caído, y quién responde fuera de horario?

Buena señal: Una alerta llega a una persona antes de que escriban los clientes, y hay alguien claramente de guardia.
Señal de alerta: Los clientes o el equipo de soporte se enteran primero, y no hay nadie de guardia.

7. Titularidad. ¿Quién es dueño de los repositorios, las cuentas de cloud y las cuentas de las tiendas de apps? ¿Alguna está a nombre de una agencia o un contratista?

Buena señal: La empresa es dueña de todas las cuentas, los contratos ceden la propiedad intelectual, y las agencias trabajan dentro de esas cuentas.
Señal de alerta: Una agencia tiene el código, la ficha en la tienda o las claves de firma, y el contrato no dice nada sobre la titularidad.

8. Riesgo de persona clave. Si la persona que armó esto no estuviera dos semanas, ¿qué se detendría?

Buena señal: Al menos otra persona puede hacer deploy y entrar a producción, y hay una descripción corta de cómo encaja el sistema.
Señal de alerta: Una sola persona concentra los deploys, el acceso a producción y el conocimiento de cómo funciona todo.

9. Uso de AI. ¿Qué parte del producto es realmente AI, a dónde van los datos de los clientes, y hay un tope de gasto?

Buena señal: Separan la AI real del software convencional, nombran al proveedor, dicen qué datos se envían, y pueden señalar un tope y términos básicos sobre esos datos.
Señal de alerta: El pitch habla de "AI," pero no pueden explicar qué hace el modelo, a dónde van los datos, ni cuánto cuesta.

10. Costos de cloud. ¿Cuánto gastan en cloud por mes, y qué parte de eso podrían recortar sin afectar a los clientes?

Buena señal: Conocen el número mensual, qué lo mueve, y un par de piezas sin uso o sobredimensionadas que podrían bajar.
Señal de alerta: No conocen la factura, o viene subiendo y nadie la mira.