PLANTILLA P15 · REGISTRO DE ARQUITECTURA

Registro de arquitectura

Documenta la arquitectura de la solución, las decisiones de diseño con sus alternativas y la trazabilidad entre los riesgos y requisitos de la fase 3 y los controles diseñados.

Fernando García Varela Versión 0.1 (borrador de trabajo) 16-09-2026 Borrador para revisión

EN ESTE DOCUMENTO

01 Instrucciones de uso

02 Identificación

03 Visión general

04 Componentes

05 Modelos

06 Flujos de datos e integraciones

07 Decisiones de arquitectura

08 Trazabilidad de riesgos, obligaciones y controles

09 Requisitos no funcionales

10 Supervisión, seguridad, operación y reversibilidad

11 Coste de operación estimado (Enterprise)

12 Criterios de calidad

13 Aprobación y verificación

14 Control de versiones

Aviso legal y exención de responsabilidad. SEVEN-G es un marco metodológico de referencia que se ofrece «tal cual» y con fines exclusivamente informativos. No constituye asesoramiento jurídico, regulatorio, financiero ni profesional, ni garantiza el cumplimiento de ninguna norma. Las referencias a regulación general (como el Reglamento Europeo de IA, el RGPD, DORA o NIS2), a normas técnicas y a regulación específica de cada sector o jurisdicción pueden ser incompletas, no aplicar a un caso concreto o quedar desactualizadas por cambios normativos, interpretaciones o criterios de las autoridades posteriores a su fecha de consulta. **Cada organización que use SEVEN-G es la única responsable de identificar la normativa que le aplica, verificar su vigencia y certificar su propio cumplimiento regulatorio**, con el asesoramiento cualificado que corresponda. Esta metodología es una ayuda genérica y gratuita, compartida con la comunidad para que nadie tenga que empezar desde cero; cada persona u organización puede y debe adaptarla a su propio uso. No debe entenderse que sus partes jurídicamente sensibles hayan sido revisadas por una asesoría jurídica: esas revisiones, para cada empresa o sector, son responsabilidad última de la empresa, el consultor o la organización que la use. Aunque se procura mantenerla al día, alguna norma puede haber cambiado sin que se recoja aquí. En la máxima medida permitida por la ley, el autor no asume responsabilidad alguna por los efectos de su aplicación en ninguna organización ni por su aplicabilidad completa. La metodología no otorga certificación de ningún tipo. El autor no asume responsabilidad alguna por el uso que se haga de este contenido ni por las decisiones que se adopten con él. Los datos, cifras, compañías y casos de los ejemplos son ficticios o ilustrativos.

01

Instrucciones de uso

Aspecto	Indicación
Cuándo se usa	En la fase 4 (Diseño de la solución), antes de G4. Se mantiene vivo en las fases 5 y 6: todo cambio de arquitectura relevante añade una decisión y actualiza la versión.

Aspecto	Indicación
Quién la rellena	El responsable técnico de IA, que responde y realiza el trabajo en la fase 4. Consulta a seguridad de la información, al responsable de operación y al responsable de riesgos.
Quién la verifica	Lite: oficina de IA. Enterprise: auditor de IA.
Quién decide	Lite: responsable técnico con conformidad de riesgos (01 §7.5). Enterprise: comité de IA.
Gate en que se revisa	Diseño. Se comprueba de nuevo en G5 (lo construido coincide con lo diseñado) y en R6 (cambios). (G4)
Herramienta	No tiene herramienta propia; se enlaza como evidencia en T03.
Lite frente a Enterprise	Lite puede omitir los campos y bloques marcados **(Enterprise)**. La visión general, los componentes, las decisiones y la trazabilidad de controles son obligatorios en ambas.

Reglas de cumplimentación:

- La arquitectura debe cubrir los **controles exigidos por la clasificación de riesgo** y los riesgos de la fase 3 deben tener **control diseñado** (01 §6.6).
- Debe existir un **mecanismo de parada** y una vía de reversión (P19).
- Los diagramas se adjuntan como fichero enlazado o como bloque Mermaid; no se dibujan en texto.
- Este registro resume y enlaza: el linaje de datos y modelos va en P16, la supervisión humana en P17, la seguridad en P18, la reversión en P19 y la monitorización en P25.

02

Identificación

Campo	Contenido	Guía
Código del caso de uso		IA-AAAA-NNN.
Sistemas de IA cubiertos		Códigos de P05.
Clasificación regulatoria e intensidad		De P11 y P04.
Nivel de autonomía		A0 · A1 · A2 · A3.
Versión del documento		
Fecha		DD-MM-AAAA.

Campo	Contenido	Guía
Autor		Nombre y rol.

03

Visión general

Campo	Contenido	Guía
Descripción de la solución		Qué hace, para quién y cómo se integra en el proceso, en lenguaje comprensible.
Diagrama de contexto		Enlace al diagrama: usuarios, sistemas externos, proveedores y límites de la solución.
Diagrama de componentes		Enlace al diagrama de componentes y flujos principales.
Alcance de esta versión		Qué incluye el diseño y qué se deja para versiones posteriores.
Restricciones de P02 aplicadas		Plataformas obligatorias, ubicación de datos, autonomía máxima, líneas rojas.

04

Componentes

Componente	Función	Tipo	Proveedor o equipo	Versión	Entorno de alojamiento	Datos que trata	Criticidad
		Modelo · Orquestación · Datos · Integración · Interfaz · Control · Monitorización					Baja · Media · Alta
(ejemplo ilustrativo) **Modelo de lenguaje**	Redactar respuestas a partir de la información del pedido	Modelo	Proveedor X (P14, N2)	Versión fijada por contrato	Nube del proveedor, región de la UE	Texto de la consulta y datos del pedido	Alta

Componente	Función	Tipo	Proveedor o equipo	Versión	Entorno de alojamiento	Datos que trata	Criticidad
(ejemplo ilustrativo) **Servicio de consulta de pedidos**	Devolver solo los pedidos del cliente autenticado	Integración	Equipo interno	1.0	Nube corporativa	Datos del pedido	Alta
(ejemplo ilustrativo) **Filtro de salida**	Bloquear datos personales ajenos al cliente	Control	Equipo interno	1.0	Nube corporativa	Respuesta generada	Alta

05

Modelos

Resumen; el detalle de versiones, datos de entrenamiento y evaluaciones va en P16.

Modelo	Tipo	Origen	Uso	Criterio de selección	Evaluación realizada	Sustituto previsto
	ML predictivo · IA generativa · Agente · Otro	Propio · Terceros · Código abierto			Métricas y fecha	

06

Flujos de datos e integraciones

Flujo	Origen	Destino	Datos	Frecuencia	Protección en tránsito	Transferencia fuera del EEE
				Tiempo real · Por lotes		Sí · No

Detalle de fuentes, transformaciones y versiones en P16.

07

Decisiones de arquitectura

Una fila por decisión relevante. Las decisiones no se borran: si se sustituyen, se marca la anterior como sustituida.

Nº	Decisión	Contexto	Alternativas consideradas	Motivo de la elección	Consecuencias y riesgos	Fecha	Estado
DA-01							Propuesta · Aprobada · Sustituida por DA-NN
(ejemplo ilustrativo) **DA-01**	El modelo no accede directamente al sistema de pedidos; recibe solo los datos devueltos por un servicio intermedio.	Riesgo de fuga de datos de otros clientes (P12, R01).	Acceso directo del modelo mediante herramienta; recuperación sobre un índice con todos los pedidos.	Limita por diseño los datos disponibles a los del cliente autenticado.	Mayor latencia; mantenimiento del servicio intermedio.	20-01-2027	Aprobada

08

Trazabilidad de riesgos, obligaciones y controles

Cada riesgo de P12 que requiera tratamiento y cada obligación de P11 debe tener al menos un control diseñado.

Riesgo u obligación	Origen	Control diseñado	Componente	Plantilla de detalle	Cómo se probará en la fase 5
	P12 R.. · P11			P16 · P17 · P18 · P19 · P25	
(ejemplo ilustrativo) **Fuga de datos de otro cliente**	P12 R01	Servicio intermedio con filtrado por cliente autenticado y filtro de salida	Servicio de consulta de pedidos; filtro de salida	P18	300 ataques de inyección sin fugas

Riesgo u obligación	Origen	Control diseñado	Componente	Plantilla de detalle	Cómo se probará en la fase 5
(ejemplo ilustrativo) **Informar de que se conversa con un sistema de IA**	P11 §10	Aviso al inicio de cada conversación	Interfaz	P17	Revisión funcional

09

Requisitos no funcionales

Requisito	Objetivo	Cómo se mide	Componente responsable
Disponibilidad			
Tiempo de respuesta			
Capacidad y volumen			
Coste por transacción			
Registro de actividad y trazabilidad		Qué se registra, dónde y cuánto tiempo se conserva	
Accesibilidad (Enterprise)			

10

Supervisión, seguridad, operación y reversibilidad

Campo	Contenido	Guía
Puntos de supervisión humana		Dónde interviene una persona y qué no se delega nunca. Detalle en P17.
Identidad y permisos del sistema o del agente		Cuentas, permisos mínimos, límites de actuación. Detalle en P18.
Mecanismo de parada		Cómo se detiene el sistema, quién puede hacerlo y en cuánto tiempo.

Campo	Contenido	Guía
Reversión		Cómo se vuelve a la versión anterior o al proceso sin IA. Detalle en P19.
Monitorización		Métricas técnicas, de calidad, de coste y de seguridad. Detalle en P25.
Entornos		Desarrollo, pruebas, preproducción y producción; separación de datos.
Gestión de cambios (Enterprise)		Cómo se aprueban cambios de modelo, instrucciones o configuración.

11

Coste de operación estimado (Enterprise)

Categoría	Coste recurrente anual (€)	Supuestos	Cambio respecto de P10
Licencias			
Consumo de modelos			
Cómputo e infraestructura			
Personas de operación			
Proveedores y servicios			
Control y cumplimiento			

Si el coste recurrente supera el de P10 de forma relevante, se actualiza P08 y se informa en G4.

12

Criterios de calidad

Los criterios formales de G4 están en el documento 21 (ver criterios G4.xx).

#	Comprobación	Estado
1	La visión general y los diagramas enlazados reflejan la solución completa, incluidos proveedores.	Cumple · No cumple · No aplica · Pendiente
2	Cada componente tiene responsable, versión, alojamiento y datos que trata.	
3	Las decisiones relevantes tienen alternativas y motivo.	
4	Todo riesgo de P12 que requiere tratamiento y toda obligación de P11 tiene control diseñado y forma de prueba.	
5	Existe mecanismo de parada y vía de reversión.	
6	Los permisos del sistema o del agente se limitan a lo necesario y no superan la autonomía máxima de P02.	
7	Las restricciones de P02 (ubicación, plataformas, líneas rojas) se respetan.	
8	P16, P17, P18, P19 y P25 existen y son coherentes con este registro.	

13

Aprobación y verificación

Función	Rol en SEVEN-G	Nombre y cargo	Fecha	Firma o referencia
Elabora y responde	Responsable técnico de IA			
Consultado	Seguridad de la información · responsable de operación de IA · responsable de riesgos de IA			
Emite conformidad	Responsable de riesgos de IA			
Verifica	Oficina de IA (Lite) · Auditor de IA (Enterprise)			
Decide	Responsable técnico con conformidad de riesgos (Lite) · Comité de IA (Enterprise)			

Separación de funciones: en Lite, el responsable técnico decide G4 sobre su propio diseño solo porque 01 §7.5 lo permite con conformidad de riesgos y verificación independiente de la oficina de IA; ambas deben constar antes de la decisión.

14

Control de versiones

Documento cumplimentado

Versión	Fecha	Autor	Cambios

Plantilla

Versión	Fecha	Cambios
0.1	16-09-2026	Primera versión. Registro de componentes, decisiones de arquitectura y trazabilidad de riesgos y obligaciones a controles, alineado con 01 §6.6.