PLANTILLA P13 · PLAN DE MITIGACIÓN Y CONTINGENCIA

Plan de mitigación y contingencia

Convierte la respuesta a cada riesgo en acciones con responsable, plazo, coste y prueba de eficacia, y define qué se hace si el riesgo se materializa.

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 Resumen de riesgos que requieren tratamiento

04 Acciones de mitigación

05 Transferencia del riesgo

06 Planes de contingencia

07 Riesgos aceptados sin acciones

08 Seguimiento del plan (Enterprise)

09 Coste total del plan

10 Criterios de calidad

11 Aprobación y verificación

12 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 3, junto con la matriz y registro de riesgos (P12), antes de G3. Se sigue en las fases 4 y 5 (los controles deben estar diseñados en G4 y funcionando en G5) y se actualiza en la fase 6.
Quién la rellena	El responsable de riesgos de IA coordina. Cada acción la propone y ejecuta su responsable (habitualmente el responsable técnico o el de producto).

Aspecto	Indicación
Quién la verifica	Lite: responsable de riesgos en G3; si él ha elaborado el plan, verifica la oficina de IA o el auditor de IA. Enterprise: auditor de IA.
Quién decide	Se aprueba con G3: patrocinador con conformidad de riesgos (Lite) · comité de IA (Enterprise). La financiación de las acciones forma parte de la decisión.
Gate en que se revisa	Viabilidad; seguimiento en G4, G5 y R6. (G3)
Herramienta	T06 · Matriz y registro de riesgos: registra la respuesta, los controles y el plan de contingencia de cada riesgo; las acciones de tratamiento con responsable, plazo y estado se siguen en esta plantilla. El Excel del caso que genera T06 propone, para cada riesgo registrado, acciones de mitigación (sección 4) y un plan de contingencia (sección 6) a partir del catálogo del documento 33 §9, con las columnas de esta plantilla a completar: es el punto de partida, no el plan aprobado.
Lite frente a Enterprise	Lite puede omitir las columnas y bloques marcados **(Enterprise)**. Todo riesgo residual Medio, Alto o Crítico debe tener acciones y, si es Alto o Crítico, plan de contingencia, en ambas intensidades.

Reglas de cumplimentación:

- Cada acción se vincula a un riesgo de P12 y dice **qué reduce**: la probabilidad, el impacto o ambos.
- Una acción no reduce el riesgo residual hasta que existe **evidencia de eficacia**.
- Los controles críticos de seguridad, cumplimiento legal y supervisión humana no admiten "Continuar con condiciones" (01 §7.3).
- Los costes de las acciones se incorporan a la evaluación de viabilidad (P10) en su categoría.

02

Identificación

Campo	Contenido	Guía
Código del caso de uso		IA-AAAA-NNN.
Versión de P12 asociada		El plan corresponde a una versión concreta del registro.
Versión del documento		
Fecha		DD-MM-AAAA.
Autor		Nombre y rol.

Campo	Contenido	Guía
Intensidad		Lite · Enterprise.

03

Resumen de riesgos que requieren tratamiento

Nº (P12)	Riesgo	Nivel inherente	Respuesta	Nivel residual objetivo	Fecha objetivo
			Evitar · Mitigar · Transferir · Aceptar	Bajo · Medio · Alto · Crítico	
***(ejemplo ilustrativo)* R01**	Fuga de datos de otro cliente por inyección de instrucciones	16 Crítico	Mitigar	8 Medio	Antes de G5

04

Acciones de mitigación

Nº acción	Riesgo	Acción	Tipo de control	Reduce	Responsable	Fecha límite	Coste estimado (€) y categoría	Evidencia de eficacia
A01			Preventivo · Detectivo · Correctivo	Probabilidad · Impacto · Ambos				
***(ejemplo ilustrativo)* A01**	R01	Aislar el contexto de cada conversación y limitar la consulta a los pedidos del cliente autenticado.	Preventivo	Probabilidad	Responsable técnico	15-12-2026	8.000 · Personas de construcción	Prueba de 300 ataques de inyección sin fugas

Nº acción	Riesgo	Acción	Tipo de control	Reduce	Responsable	Fecha límite	Coste estimado (€) y categoría	Evidencia de eficacia
***(ejemplo ilustrativo)* A02**	R01	Filtro de salida que bloquea datos personales que no pertenecen al cliente.	Preventivo	Impacto	Responsable técnico	15-12-2026	4.000 · Licencias	Informe de pruebas del filtro
***(ejemplo ilustrativo)* A03**	R01	Alerta de operación cuando el filtro bloquea una respuesta.	Detectivo	Impacto	Responsable de operación	31-01-2027	1.500 · Control y cumplimiento	Alerta configurada y probada (P25)

Categorías de coste: licencias · consumo de modelos · cómputo e infraestructura · datos · personas de construcción · personas de operación · proveedores y servicios · control y cumplimiento · adopción y formación.

05

Transferencia del riesgo

Rellenar si alguna respuesta es "Transferir".

Riesgo	Mecanismo	Contraparte	Cobertura y límites	Coste anual (€)	Parte del riesgo que no se transfiere
	Seguro · Cláusula contractual · Garantía del proveedor				Reputacional, regulatorio o de personas que permanece en la compañía

06

Planes de contingencia

Uno por cada riesgo residual Alto o Crítico y por cada riesgo con impacto 5 aunque su nivel sea menor.

Campo	Contenido	Guía
Riesgo		Nº de P12.
Escenario		Qué ocurre cuando el riesgo se materializa.
Disparador		Indicador y umbral que activan el plan. Debe poder observarse en la monitorización (P25).
Acciones inmediatas		Contención en las primeras horas, incluida la parada del sistema si procede.
Uso del plan de reversión		Si se activa P19 y cómo se vuelve al proceso anterior.
Responsable de activar el plan		Persona con autoridad para detener el sistema.
Tiempo máximo de reacción		Horas desde el disparo hasta la contención.
Comunicación		A quién se informa: comité de IA, protección de datos, clientes, supervisores.
Notificaciones regulatorias		Si puede ser un incidente grave o una violación de seguridad de datos personales, se sigue el plan de respuesta a incidentes (P26) con sus plazos.
Recuperación		Condiciones para volver a operar.

(ejemplo ilustrativo) Riesgo R01. Disparador: una sola respuesta con datos de otro cliente confirmada. Acciones: desactivar el asistente en el canal web y derivar las consultas a agentes; conservar registros; abrir incidente S1 o S2 según alcance. Responsable: responsable de operación de IA. Tiempo máximo de reacción: 1 hora. Comunicación: comité de IA y delegado de protección de datos de inmediato.

07

Riesgos aceptados sin acciones

Riesgo	Nivel residual	Motivo de la aceptación	Aceptado por (P12 §6)	Condición que obligaría a revisarla

08

Seguimiento del plan (**Enterprise**)

Fecha de revisión	Acciones implantadas	Acciones con eficacia verificada	Acciones vencidas	Riesgos que cambian de nivel	Decisión

Las acciones vencidas en controles relevantes se tratan como condición vencida y pueden constituir no conformidad (01 §12).

09

Coste total del plan

Categoría	Inversión única (€)	Coste recurrente anual (€)
Control y cumplimiento		
Personas de construcción		
Personas de operación		
Licencias		
Proveedores y servicios		
Otras categorías		
Total		

El total debe figurar en P10 §6.1.

10

Criterios de calidad

Los criterios formales están en el documento 21 (ver criterios G3.xx, G4.xx y G5.xx).

#	Comprobación	Estado
1	Todo riesgo residual Medio, Alto o Crítico de P12 tiene acciones o aceptación documentada.	Cumple · No cumple · No aplica · Pendiente
2	Cada acción tiene responsable, fecha, coste y evidencia de eficacia prevista.	
3	Los riesgos residuales Altos y Críticos, y los de impacto 5, tienen plan de contingencia con disparador observable.	
4	Los planes de contingencia enlazan con P19 (reversión) y P26 (incidentes).	
5	Las transferencias indican lo que no se transfiere.	
6	El coste del plan está incorporado en P10.	
7	No se proponen condiciones sobre controles críticos de seguridad, cumplimiento legal o supervisión humana.	

11

Aprobación y verificación

Función	Rol en SEVEN-G	Nombre y cargo	Fecha	Firma o referencia
Coordina	Responsable de riesgos de IA			
Responde de las acciones	Responsables de cada acción			
Verifica	Oficina de IA o auditor de IA (Lite, si elabora riesgos) · Auditor de IA (Enterprise)			
Decide y financia	Patrocinador con conformidad de riesgos (Lite) · Comité de IA (Enterprise)			

Separación de funciones: quien ejecuta una acción no verifica su eficacia.

12

Control de versiones

Documento cumplimentado

Versión	Fecha	Autor	Cambios

Plantilla

Versión	Fecha	Cambios
0.1	16-09-2026	Primera versión. Acciones de mitigación vinculadas a P12, transferencia, contingencia y coste por categoría de la especificación común §5.1 y §5.7.