PLANTILLA P12 · MATRIZ Y REGISTRO DE RIESGOS

Matriz y registro de riesgos

Identifica, valora y sigue los riesgos del caso de uso con escalas comunes, nivel inherente y residual, respuesta y aceptación por el órgano que corresponde.

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 Escalas

04 Registro de riesgos

05 Matriz de calor del caso de uso

06 Aceptación del riesgo residual

07 Riesgos de cartera (Enterprise)

08 Historial de revisiones

09 Criterios de calidad

10 Aprobación y verificación

11 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	Se crea en la fase 3 y es un registro vivo: se actualiza en la fase 5 (registro de riesgos actualizado antes de G5), en la fase 6 y en cada R6, y siempre que se materialice un riesgo, cambie la clasificación o aparezca un riesgo nuevo.
Quién la rellena	El responsable de riesgos de IA coordina y valora; el responsable de producto y el responsable técnico identifican riesgos y proponen controles; cada riesgo tiene un responsable.

Aspecto	Indicación
Quién la verifica	Lite: responsable de riesgos en G3 y G5; si él ha elaborado el registro, verifica la oficina de IA o el auditor de IA. Enterprise: auditor de IA.
Quién decide	La aceptación del riesgo residual la decide el órgano de la sección 6 según el nivel. El *gate* lo decide el órgano de 01 §7.5.
Gate en que se revisa	Viabilidad, G5 · Puesta en producción y R6 · Revisión de continuidad. (G3)
Herramienta	T06 · Matriz y registro de riesgos: vista «Riesgos» y pestaña «Riesgos» de la ficha del registro T01, con los mismos campos, escalas, matriz de calor y reglas de aceptación que esta plantilla, exportación CSV y Excel del caso (matriz, registro, planes de mitigación y contingencia propuestos para P13 y riesgos tipo a considerar).
Lite frente a Enterprise	Lite puede omitir las columnas y bloques marcados **(Enterprise)**. Las escalas, los niveles inherente y residual, la respuesta y la aceptación son obligatorios en ambas.

Reglas de cumplimentación:

- Las escalas y los niveles son **los de la especificación común §5.1 y el documento 33**. No se modifican por caso de uso.
- El impacto se valora en **cinco ejes** y se toma el **mayor**.
- El nivel se calcula **inherente** (sin controles) y **residual** (con controles eficaces). Un control solo reduce el residual si existe y funciona; los controles previstos se indican aparte.
- Un riesgo residual **Crítico** sin aprobación del consejo o de su comisión delegada **bloquea G3 y G5**.
- Los riesgos tipo del catálogo del documento 33 (formato RT-<CAT>-NN) se usan como punto de partida para no omitir riesgos conocidos.

02

Identificación

Campo	Contenido	Guía
Código del caso de uso		IA-AAAA-NNN.
Sistemas de IA cubiertos		Códigos de P05.
Clasificación regulatoria		Taxonomía de 03 §3.3 (P11).
Intensidad y nivel de ambición		

Campo	Contenido	Guía
Versión del documento		
Fecha de la última revisión		DD-MM-AAAA.
Próxima revisión		Fecha de la siguiente R6 o del siguiente *gate*.
Umbrales económicos de impacto aplicables		Referencia a los aprobados en C2 (documento 13).

03

Escalas

3.1 Probabilidad

Valor	Nombre	Referencia orientativa
1	Rara	Menos de una vez en 5 años o < 5 % en el horizonte del caso de uso
2	Improbable	Una vez cada 2–5 años o 5–20 %
3	Posible	Una vez cada 1–2 años o 20–50 %
4	Probable	Varias veces al año o 50–80 %
5	Casi segura	Mensual o más, o > 80 %

3.2 Impacto

Valor	Nombre
1	Insignificante
2	Menor
3	Moderado
4	Grave
5	Crítico

Ejes de valoración (se toma el mayor):

Eje	Qué se valora	Guía
Económico	Pérdidas, sobrecostes, valor no materializado.	Umbrales en euros fijados por la compañía en C2, en proporción a su tamaño.
Personas y derechos	Perjuicio a clientes, empleados u otras personas; discriminación; seguridad física.	
Regulatorio	Incumplimientos, sanciones, requerimientos del supervisor.	
Operativo	Interrupción o degradación de procesos y servicios.	
Reputacional	Pérdida de confianza de clientes, mercado o sociedad.	

3.3 Nivel de riesgo

Nivel = Probabilidad × Impacto: **Bajo** 1–4 · **Medio** 5–9 · **Alto** 10–15 · **Crítico** 16–25.

Probabilidad \ Impacto	1 Insignificante	2 Menor	3 Moderado	4 Grave	5 Crítico
5 Casi segura	5 Medio	10 Alto	15 Alto	20 Crítico	25 Crítico
4 Probable	4 Bajo	8 Medio	12 Alto	16 Crítico	20 Crítico
3 Posible	3 Bajo	6 Medio	9 Medio	12 Alto	15 Alto
2 Improbable	2 Bajo	4 Bajo	6 Medio	8 Medio	10 Alto
1 Rara	1 Bajo	2 Bajo	3 Bajo	4 Bajo	5 Medio

En una hoja de cálculo: `=SI(P*I>=16;"Crítico";SI(P*I>=10;"Alto";SI(P*I>=5;"Medio";"Bajo")))`.

04

Registro de riesgos

4.1 Identificación

Nº	Riesgo (causa, evento y consecuencia)	Categoría	Riesgo tipo de referencia	Sistema o fase	Responsable del riesgo	Fecha de alta
R01		EST · TEC · DAT · ECO · LEG · ORG · REP · GEN · SEG · TER	Código del catálogo del documento 33, si existe			
R02						
(ejemplo ilustrativo) **R01**	Por una inyección de instrucciones en el mensaje de un cliente, el asistente revela datos del pedido de otro cliente, con perjuicio para el afectado y posible incumplimiento del RGPD.	GEN	Catálogo GEN del documento 33	Asistente de consultas · fases 5–6	Responsable técnico	20-11-2026

Categorías: EST estratégico · TEC técnico · DAT datos · ECO económico · LEG legal y cumplimiento · ORG organizativo · REP reputacional · GEN IA generativa y agentes · SEG seguridad e IA ofensiva · TER terceros.

4.2 Valoración inherente y residual

Nº	P inh.	I inh.	Eje dominante	Nivel inherente	Controles existentes y eficaces	P res.	I res.	Nivel residual	Tendencia (Enterprise)
R01	1–5	1–5		Bajo · Medio · Alto · Crítico					Sube · Estable · Baja

Nº	P inh.	I inh.	Eje dominante	Nivel inherente	Controles existentes y eficaces	P res.	I res.	Nivel residual	Tendencia (Enterprise)
***(ejemplo ilustrativo)* R01**	4	4	Personas y derechos	16 Crítico	Aislamiento de sesión por cliente; filtro de salida de datos personales; pruebas de inyección con 0 fugas	2	4	8 Medio	Baja

4.3 Respuesta y seguimiento

Nº	Respuesta	Controles previstos (P13)	Aceptado por	Fecha de aceptación	Estado	Próxima revisión
R01	Evitar · Mitigar · Transferir · Aceptar				Identificado · En tratamiento · Aceptado · Materializado · Cerrado	
***(ejemplo ilustrativo)* R01**	Mitigar	Monitorización de salidas con alerta (P25)	Patrocinador, con conformidad del responsable de riesgos	15-01-2027	Aceptado	R6 del segundo trimestre de 2027

Respuestas: **Evitar** (se elimina la causa o la actividad) · **Mitigar** (controles que reducen probabilidad o impacto) · **Transferir** (seguro o contrato; el riesgo reputacional y regulatorio no se transfiere por completo) · **Aceptar** (se asume el residual con aprobación). La lista de estados es propuesta de esta plantilla, a confirmar en el documento 33.

05

Matriz de calor del caso de uso

Anote en cada celda los números de riesgo según su valoración **residual**.

Probabilidad \ Impacto	1 Insignificante	2 Menor	3 Moderado	4 Grave	5 Crítico
5 Casi segura					
4 Probable					

Probabilidad \ Impacto	1 Insignificante	2 Menor	3 Moderado	4 Grave	5 Crítico
3 Posible					
2 Improbable				R01 *(ejemplo ilustrativo)*	
1 Rara					

Resumen	Inherente	Residual
Crítico		
Alto		
Medio		
Bajo		

06

Aceptación del riesgo residual

Nivel residual	Quién puede aceptarlo	Requisito
Bajo (1–4)	Responsable de producto de IA	Con registro.
Medio (5–9)	Patrocinador de IA	Con conformidad del responsable de riesgos.
Alto (10–15)	Comité de IA	Con conformidad del responsable de riesgos y plan de mitigación (P13). Aplica también en intensidad Lite.
Crítico (16–25)	No se acepta	Excepcionalmente, solo el consejo o su comisión delegada, dentro del apetito de riesgo aprobado en C2. Sin esa aprobación bloquea G3 y G5.

Nº	Nivel residual	Órgano que acepta	Fecha	Referencia del acta o registro	Vigencia de la aceptación
					Hasta la próxima R6 o hasta el cambio que la invalide

07

Riesgos de cartera (**Enterprise**)

Campo	Contenido	Guía
Riesgos compartidos con otros casos de uso		Mismo proveedor, mismo modelo, mismos datos o misma función crítica.
Concentración		Si la suma de exposiciones supera el apetito de riesgo, se informa al comité de IA.
Riesgos que deben elevarse		Riesgos Altos o Críticos y riesgos concentrados.

08

Historial de revisiones

Fecha	Momento	Cambios principales	Riesgos nuevos	Riesgos cerrados	Revisado por
	G5 · R6 · Evento `(fase 3)`				

09

Criterios de calidad

Los criterios formales están en el documento 21 (ver criterios G3.xx, G5.xx y R6.xx) y la metodología en el documento 33.

#	Comprobación	Estado
1	Se ha contrastado el registro con el catálogo de riesgos tipo, incluidos GEN, SEG y TER cuando apliquen.	Cumple · No cumple · No aplica · Pendiente
2	Cada riesgo describe causa, evento y consecuencia, y tiene responsable.	
3	Las escalas usadas son las comunes y el impacto toma el mayor de los cinco ejes.	
4	Se calculan nivel inherente y residual; el residual solo considera controles existentes y eficaces.	

#	Comprobación	Estado
5	Cada riesgo tiene respuesta; los de Mitigar tienen controles en P13.	
6	La aceptación la firma el órgano que corresponde al nivel residual.	
7	No hay riesgos residuales Críticos sin aprobación del consejo o de su comisión delegada.	
8	El registro está actualizado en el momento del *gate* o de la revisión.	

10

Aprobación y verificación

Función	Rol en SEVEN-G	Nombre y cargo	Fecha	Firma o referencia
Coordina y valora	Responsable de riesgos de IA			
Identifica y propone controles	Responsable de producto y responsable técnico de IA			
Verifica	Oficina de IA o auditor de IA (Lite, si elabora riesgos) · Auditor de IA (Enterprise)			
Acepta el residual	Según la sección 6			
Decide el *gate*	Órgano de 01 §7.5			

Separación de funciones: quien acepta un riesgo no lo ha valorado; el responsable de riesgos emite conformidad, pero no acepta riesgos de nivel Medio o superior.

11

Control de versiones

Documento cumplimentado

Versión	Fecha	Autor	Cambios

Plantilla

Versión	Fecha	Cambios
0.1	16-09-2026	Primera versión. Aplica las escalas, niveles, respuestas, aceptación y categorías de la especificación común §5.1.

Fuentes externas citadas

Enlaces a la fuente oficial o primaria, comprobados antes de publicar. Verifique siempre la versión vigente en la fecha de uso.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/spa · Parlamento Europeo y Consejo de la UE · 27-04-2016