PLANTILLA P14 · EVALUACIÓN DE PROVEEDOR DE IA

Evaluación de proveedor de IA

Determina el nivel de exigencia de un proveedor de IA, resume su evaluación de diligencia debida, la dependencia que genera y su plan de salida, y comprueba que el contrato incluye las cláusulas clave.

Fernando García Varela Versión 0.2 (borrador de trabajo) 19-09-2026 Borrador para revisión

EN ESTE DOCUMENTO

01 Instrucciones de uso

02 Identificación

03 Nivel de exigencia

04 Evaluación del proveedor

05 Cláusulas contractuales clave

06 Conclusión

07 Criterios de calidad

08 Aprobación y verificación

09 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, antes de G3, para cada proveedor que aporte modelos, plataformas, datos o servicios de IA al caso de uso. Se revisa antes de firmar o renovar el contrato, ante cualquier disparador de reevaluación (36 §5) y con la periodicidad del nivel de exigencia.
Quién la rellena	El responsable técnico de IA, con compras y el responsable de riesgos de IA. Consulta a seguridad de la información, protección de datos y asesoría jurídica.
Quién la verifica	Lite: responsable de riesgos de IA; si ha elaborado la evaluación, verifica la oficina de IA o el auditor de IA. Enterprise: auditor de IA.

Aspecto	Indicación
Quién decide	Se aprueba con G3, según el nivel de exigencia (36 §4.2): N1, responsable de producto con conformidad de compras · N2, patrocinador con conformidad de riesgos y de protección de datos · N3, comité de IA con conformidad de riesgos, seguridad de la información, protección de datos y jurídico.
Gate en que se revisa	Viabilidad; comprobación de cláusulas firmadas en G5. (G3)
Herramienta	T09 · Registro de proveedores de IA (formato de trabajo en P57).
Documentos de apoyo	P55 · Cuestionario de diligencia debida (detalle de los doce bloques que se resumen en la sección 4) · P56 · Cláusulas contractuales tipo (texto modelo de las cláusulas de la sección 5) · P57 · Registro de proveedores y plan de salida.
Lite frente a Enterprise	La profundidad depende del nivel de exigencia (N1, N2, N3), no de la intensidad (36 §2, principio 2). Un proveedor N3 implica normalmente intensidad Enterprise (01 §9.2).

Reglas de cumplimentación:

- El nivel de exigencia se determina por el **factor más exigente** (36 §4.1).
- Los requisitos por nivel son los del documento 36 §4.2: diligencia debida, seguridad, contrato, aprobación, auditoría, seguimiento, salida, incidentes y registro.
- Esta plantilla **resume** la evaluación: el detalle de las preguntas, las respuestas y las evidencias está en P55.
- *Este documento no constituye asesoramiento jurídico.* Referencias consultadas en septiembre de 2026; debe verificarse su vigencia.

02

Identificación

Campo	Contenido	Guía
Código del caso de uso		IA-AAAA-NNN.
Sistemas de IA afectados		Códigos de P05.
Código de la relación proveedor–servicio		PRV-AAAA-NNN del registro T09 (P57).
Proveedor		Razón social y país de establecimiento.

Campo	Contenido	Guía
Servicio o componente evaluado		Modelo por API, plataforma, software con IA embebida, datos, servicios profesionales.
Opción de abastecimiento		Construir · Comprar · Adaptar · Aliarse (36 §3.1).
Versión del documento		
Fecha		DD-MM-AAAA.
Autor		Nombre y rol.

03

Nivel de exigencia

Factor	N1 · Estándar	N2 · Reforzado	N3 · Crítico	Valoración
Criticidad del servicio	Proceso interno cuya interrupción tendría impacto 1–2 (documento 33).	Proceso relevante con impacto 3; exposición directa a clientes; decisiones sobre personas.	Función crítica o importante (incluida la definición de DORA cuando aplique); impacto 4–5; sistema de alto riesgo según el Reglamento de IA .	N1 · N2 · N3
Datos tratados	Públicos o internos no sensibles.	Datos personales o información confidencial.	Categorías especiales de datos, datos personales a gran escala, secretos empresariales o información confidencial crítica.	
Autonomía	A0: el sistema del proveedor asiste.	A1, o A2 sin efectos sobre terceros, dinero, datos personales ni producción.	A2 o A3 con efectos sobre terceros, dinero, datos personales o sistemas de producción.	
Sustituibilidad	Sustituible en menos de 3 meses sin coste relevante.	Sustituible en 3 a 12 meses o con coste relevante.	Más de 12 meses, coste superior al umbral de materialidad M o sin alternativa.	

Los plazos de sustituibilidad son orientativos y se aprueban en C2 (documento 13).

Campo	Contenido	Guía
Nivel de exigencia		N1 Estándar · N2 Reforzado · N3 Crítico. El más alto de los cuatro factores.

Campo	Contenido	Guía
Justificación		
Tercero TIC que presta servicios en funciones esenciales o importantes (DORA)		Sí · No · No aplica. Solo entidades sujetas a DORA.

(ejemplo ilustrativo) Proveedor de modelo de lenguaje por API para el asistente de consultas: criticidad N2 (exposición directa a clientes), datos N2 (datos personales de pedidos), autonomía N1 (A0), sustituibilidad N2 (sustituible en unos seis meses). Nivel: **N2 Reforzado**.

04

Evaluación del proveedor

4.1 Resultado por bloque de diligencia debida

Se rellena desde el resumen de P55 §5, con los doce bloques del documento 36 §4.3. Resultado: **Conforme · Conforme con observaciones · No conforme · No evaluado**.

Bloque	Resultado	Observaciones
1 · Identidad y solvencia		
2 · Servicio y modelo		
3 · Datos		
4 · Subencargados y cadena de suministro		
5 · Seguridad		
6 · Cumplimiento del Reglamento de IA		
7 · Protección de datos		
8 · Propiedad intelectual		
9 · Continuidad		
10 · Incidentes		

Bloque	Resultado	Observaciones
11 · Salida		
12 · Ética y uso responsable		
Rendimiento con pruebas propias (P10)		Resultados de pruebas propias con datos representativos, no solo cifras del proveedor.

4.2 Dependencia y plan de salida

Campo	Contenido	Guía
Concentración		Otros sistemas de la compañía que dependen del mismo proveedor (T09; 36 §7.2).
Alternativas		Proveedores o soluciones alternativos identificados.
Salida exigida por el nivel		N1: exportación de datos garantizada · N2: plan de salida documentado · N3: plan de salida con alternativa identificada y ensayo o prueba documentada (36 §4.2).
Plan de salida		Referencia al plan de salida y, en N3, a la prueba de portabilidad de P57 §6 y §7.

05

Cláusulas contractuales clave

Las dieciséis cláusulas del documento 36 §6. **Sí** = debe figurar · **Rec.** = recomendada · **—** = no requerida. Estado: **Presente · Parcial · Ausente · No aplica** (36 §9). El texto modelo de cada cláusula está en P56.

#	Cláusula	N1	N2	N3	Estado
1	Uso de datos para entrenamiento	Sí	Sí	Sí	
2	Confidencialidad y tratamiento de datos	Sí	Sí	Sí	
3	Ubicación y transferencias	Sí	Sí	Sí	
4	Seguridad	Sí	Sí	Sí	
5	Subencargados	Rec.	Sí	Sí	
6	Propiedad intelectual y resultados	Rec.	Sí	Sí	

#	Cláusula	N1	N2	N3	Estado
7	Notificación de incidentes	Rec.	Sí	Sí	
8	Cambios de modelo	Rec.	Sí	Sí	
9	Niveles de servicio	—	Sí	Sí	
Mapa de esferas y niveles de ambición (10)	Registros y trazabilidad	—	Sí	Sí	
Modelo de madurez (11)	Auditoría y acceso	—	Rec.	Sí	
Índice de transformación (12)	Obligaciones del Reglamento de IA en la cadena de valor	Rec.	Sí	Sí	
Tesis de IA, ambición y apetito de riesgo (13)	Transparencia sobre funciones de IA	Rec.	Sí	Sí	
Gestión de cartera (14)	Continuidad	—	Rec.	Sí	
15	Salida y transición	Rec.	Sí	Sí	
16	Terminación	Rec.	Sí	Sí	

En N1 muchas cláusulas no son negociables: se verifican en las condiciones estándar y, si faltan, se registra el riesgo y quién lo acepta (36 §6; P56 §9). Para entidades sujetas a DORA, todo servicio N3 se revisa contra el art. 30.3 de ese reglamento (36 §6.2).

06

Conclusión

Campo	Contenido	Guía
Resultado global		Conforme · Conforme con observaciones · No conforme.
Observaciones y condiciones		Qué debe resolverse, responsable y plazo (antes de firma o antes de G5).
Riesgos para P12		Riesgos de categoría TER u otros identificados en la evaluación.
Periodicidad de revisión		Según el nivel (36 §4.2): N1 revisión anual · N2 revisión semestral e indicadores de servicio · N3 revisión trimestral, indicadores mensuales y reunión de gobierno de la relación.

Campo	Contenido	Guía
Próxima revisión		Fecha.

Un resultado **No conforme** en los bloques 3 (datos), 5 (seguridad) o 7 (protección de datos) de P55 impide usar el proveedor con datos de producción hasta resolverlo (P55 §5). Tampoco se usa con datos de producción mientras una cláusula exigible (**Sí**) esté ausente sin el riesgo registrado y aceptado por el órgano que corresponde.

07

Criterios de calidad

Los criterios formales de G3 están en el documento 21 (ver criterios G3.xx) y los requisitos de terceros en el documento 36.

#	Comprobación	Estado
1	El nivel de exigencia está justificado con los cuatro factores.	Cumple · No cumple · No aplica · Pendiente
2	Los doce bloques tienen resultado trasladado desde P55 y el rendimiento se ha comprobado con pruebas propias.	
3	El uso de datos por el proveedor está resuelto por contrato.	
4	Las cláusulas exigibles del nivel están presentes o en negociación con fecha anterior a G5; las ausentes tienen riesgo registrado y aceptado.	
5	La dependencia y la salida están evaluadas según el nivel: en N2 existe plan de salida documentado y en N3 alternativa identificada y prueba documentada.	
6	Los riesgos identificados se han trasladado a P12.	
7	El proveedor está registrado en T09 y en la ficha P05.	

08

Aprobación y verificación

Función	Rol en SEVEN-G	Nombre y cargo	Fecha	Firma o referencia
Elabora	Responsable técnico de IA			
Consultado	Compras · seguridad · protección de datos · asesoría jurídica			
Emite conformidad	Las funciones que exige el nivel (fila «Decide»)			
Verifica	Responsable de riesgos (Lite) · Auditor de IA (Enterprise)			
Decide	N1: responsable de producto con conformidad de compras · N2: patrocinador con conformidad de riesgos y de protección de datos · N3: comité de IA con conformidad de riesgos, seguridad de la información, protección de datos y jurídico (36 §4.2)			

Separación de funciones: quien negoció el contrato no verifica la evaluación; quien tenga conflicto de interés con el proveedor lo declara en P03.

09

Control de versiones

Documento cumplimentado

Versión	Fecha	Autor	Cambios

Plantilla

Versión	Fecha	Cambios
0.1	16-09-2026	Primera versión. Niveles de exigencia N1–N3 de la especificación común §5.6, evaluación por bloques y cláusulas contractuales clave.
0.2	19-09-2026	Alineada con el documento 36: decisión y revisión por nivel N1–N3, factores, 12 bloques de diligencia (P55), 16 cláusulas (P56) y plan de salida (P57).

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) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero (DORA) · https://eur-lex.europa.eu/eli/reg/2022/2554/oj/spa · Parlamento Europeo y Consejo de la UE · 14-12-2022

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial) · https://eur-lex.europa.eu/eli/reg/2024/1689/oj/spa · Parlamento Europeo y Consejo de la UE · 13-06-2024