DOCUMENTO 36 · TERCEROS Y PROVEEDORES DE IA

Terceros y proveedores de IA

Decidir qué construir, comprar o aliar, y gestionar a los proveedores de IA con una exigencia proporcional a su criticidad

Fernando García Varela Versión 0.2 (borrador de trabajo) 19-10-2026 Borrador para revisión

3	4	6	16
niveles de exigencia	factores de clasificación	etapas del ciclo del proveedor	cláusulas contractuales clave

EN ESTE DOCUMENTO

01 Objeto y alcance

02 Principios

03 Construir, comprar o aliarse

04 Niveles de exigencia N1–N3

05 Ciclo de vida del proveedor

06 Cláusulas contractuales clave

07 Dependencia tecnológica y concentración

08 IA embebida en software ya contratado

09 Registro de proveedores

10 Seguimiento e indicadores

11 Roles

12 Herramientas y plantillas asociadas

13 Documentos relacionados

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.

LO ESENCIAL **Condicional: depende de un disparador**

Disparador: interviene un proveedor de IA (modelo, plataforma o software con funciones de IA), también la IA embebida en software ya contratado. El nivel de exigencia N1 a N3 decide cuánta diligencia debida, qué cláusulas y qué plan de salida.

Matriz de obligatoriedad y lectura por capas (documento 94)

01

Objeto y alcance

La mayor parte de la IA que usa una compañía depende de terceros: modelos de propósito general consumidos como servicio, plataformas en la nube, software con funciones de IA, integradores, proveedores de datos y componentes de código abierto. Este documento establece cómo se decide recurrir a un tercero, cómo se le exige en proporción a su criticidad, qué debe decir el contrato y cómo se vigilan la dependencia y la concentración.

1.1 Tipos de tercero

Tipo	Ejemplos	Particularidad
Proveedor de modelos	Modelos de propósito general accesibles por interfaz de programación; modelos especializados.	Cambios de versión frecuentes; uso de datos; concentración.
Plataforma	Nube, plataformas de datos, de agentes o de despliegue de modelos.	Dependencia arquitectónica; ubicación de datos.
Software con IA	Aplicaciones de negocio con funciones de IA, contratadas específicamente o ya existentes (sección 8).	La IA llega por actualización; control limitado.
Integrador o consultor	Construcción, integración u operación por cuenta de la compañía.	Conocimiento fuera de casa; propiedad de lo construido.
Proveedor de datos	Datos de entrenamiento, enriquecimiento o referencia.	Licencias, calidad, base legal.
Componentes abiertos	Modelos con pesos abiertos, bibliotecas, conectores, servidores de herramientas.	Sin contrato: la exigencia recae en la verificación propia (SEG-09, AG-13).
Socio o alianza	Desarrollo conjunto, explotación compartida, consorcios.	Reparto de propiedad intelectual, datos y responsabilidades.

1.2 Normas de referencia

Consultadas en septiembre de 2026; deben verificarse en su versión vigente:

- **Reglamento (UE) 2024/1689** (Reglamento Europeo de IA), en particular las responsabilidades a lo largo de la cadena de valor (art. 25), las obligaciones de los responsables del despliegue (art. 26) y las de los proveedores de modelos de propósito general (art. 53). Modificado por el Reglamento (UE) 2026/1744 (Ómnibus digital sobre IA), publicado en el Diario Oficial el 24 de julio de 2026, que

aplaza las obligaciones de los sistemas de alto riesgo del anexo III al 2 de diciembre de 2027 y las del anexo I al 2 de agosto de 2028.

- **Reglamento (UE) 2022/2554 (DORA)**, arts. 28 a 30 y su desarrollo: Reglamento Delegado (UE) 2024/1773 (política sobre acuerdos contractuales para funciones esenciales o importantes), Reglamento de Ejecución (UE) 2024/2956 (registro de información) y Reglamento Delegado (UE) 2025/532 (subcontratación).
- **Reglamento (UE) 2016/679 (RGPD)**, art. 28 (encargados del tratamiento) y capítulo V (transferencias internacionales).
- **ISO/IEC 42001**, control A.10 del anexo A (relaciones con terceros y clientes).
- **Directiva (UE) 2022/2555 (NIS2)** en lo relativo a la seguridad de la cadena de suministro, según su transposición nacional.

Este documento no constituye asesoramiento jurídico. El contenido contractual debe revisarse con asesoría jurídica cualificada. Los niveles de exigencia y las obligaciones descritas son orientativos: la responsabilidad de la clasificación regulatoria de los terceros y de los sistemas y del cumplimiento, incluida la regulación sectorial aplicable, es de la organización (documento 93, sección 11).

02

Principios

#	Principio	Consecuencia
1	**La responsabilidad no se externaliza**	La compañía responde ante clientes, supervisores y consejo aunque el sistema sea de un tercero.
2	**Exigencia proporcional**	La diligencia, el contrato y el seguimiento dependen del nivel N1–N3, no del importe del contrato.
3	**Salir antes de entrar**	La estrategia de salida se diseña al seleccionar, no al terminar.
4	**Los datos de la compañía no entrenan a otros**	Salvo decisión expresa y documentada.
5	**Ningún cambio de modelo sin saberlo**	El proveedor informa de los cambios relevantes y la compañía los evalúa.
6	**La concentración se gestiona en cartera**	La dependencia de un proveedor se mide en todos los sistemas, no solo en uno.
7	**La IA que llega por actualización también se gobierna**	Las funciones de IA de software ya contratado entran en el inventario y se evalúan.

#	Principio	Consecuencia
8	**Probar también es usar**	Ninguna herramienta externa de IA se usa con datos de la compañía —tampoco para probarla, investigar o compararla— sin la evaluación de proveedor (P55) proporcionada a su nivel N1–N3. Una prueba con datos sintéticos o públicos no la necesita; con datos internos, personales o confidenciales, sí.

> **Por qué importa.** Muchas fugas no ocurren en producción sino en la prueba: alguien sube un documento real a una herramienta «solo para ver qué tal funciona». Tratar la prueba como uso hace que la evaluación del proveedor llegue antes que los datos.

03

Construir, comprar o aliarse

3.1 Opciones

Opción	Qué significa	Cuándo tiene sentido
Construir	Desarrollo propio, aunque use modelos o componentes de terceros.	Diferenciación competitiva, datos propios únicos, necesidad de control.
Comprar	Producto o servicio de mercado con configuración limitada.	Función no diferencial, solución madura, prioridad de plazo.
Adaptar	Producto o modelo de mercado con ajuste, integración o extensión significativos.	Base madura con necesidades propias relevantes.
Aliarse	Desarrollo o explotación conjunta con un tercero.	Capacidades o datos complementarios; reparto de riesgo en apuestas de Transformar.

3.2 Criterios de decisión

Criterio	Favorece construir	Favorece comprar	Favorece aliarse
Diferenciación	La capacidad es fuente de ventaja competitiva.	Función estándar del sector.	Ventaja que ninguno logra por separado.

Criterio	Favorece construir	Favorece comprar	Favorece aliarse
Datos	Datos propios únicos y sensibles.	Los datos necesarios son genéricos.	Datos complementarios de ambas partes.
Capacidad interna	Equipo capaz de construir y operar.	Sin capacidad ni intención de crearla.	Capacidad parcial.
Plazo	Plazo compatible con desarrollo.	Urgencia.	Plazo intermedio.
Control y cumplimiento	Necesidad de explicar, auditar y modificar a fondo.	El proveedor aporta cumplimiento verificable.	Reparto contractual claro de obligaciones.
Coste total	Menor coste recurrente a escala.	Menor inversión inicial.	Inversión y riesgo compartidos.
Dependencia	Evitar dependencia en una función crítica.	Dependencia aceptable y sustituible.	Dependencia mutua equilibrada.
Propiedad intelectual	Necesidad de poseer el resultado.	No relevante.	Reparto negociable.

Reglas:

1. La decisión se documenta en la evaluación de viabilidad (P10) de la fase 3 con los criterios de la tabla y el coste total a tres años según las categorías del documento 42, incluido el **coste de salida**.
2. En casos de uso de **Optimizar**, comprar debería ser la opción de partida salvo razón documentada. En **Transformar**, la dependencia de un tercero en la capacidad diferencial debe justificarse ante el órgano que aprueba la apuesta.
3. **Construir sobre modelos de terceros no elimina la dependencia**: se aplica este documento al proveedor del modelo.
4. Si la compañía modifica sustancialmente un sistema de alto riesgo de un tercero, cambia su finalidad o lo comercializa con su nombre, puede pasar a ser **proveedor** a efectos del Reglamento de IA (art. 25.1), con las obligaciones correspondientes. Esta consecuencia se analiza antes de decidir adaptar.

04

Niveles de exigencia N1–N3

4.1 Factores de clasificación

El nivel se determina para cada relación entre un proveedor y un servicio. Un mismo proveedor puede tener niveles distintos para servicios distintos. **El nivel es el más alto que resulte de cualquiera de los cuatro factores.**

Factor	N1 · Estándar	N2 · Reforzado	N3 · Crítico
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.
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). El nivel se determina en la fase 3, se revisa en cada R6 y ante cualquier cambio del servicio, y se registra en T09.

4.2 Requisitos por nivel

Requisito	N1 · Estándar	N2 · Reforzado	N3 · Crítico
Diligencia debida	Cuestionario básico; revisión de condiciones de servicio y de privacidad.	Cuestionario completo (4.3; P55); certificaciones e informes independientes; análisis de subencargados.	Todo lo de N2, más solvencia financiera, continuidad, subcontratación en cadena, referencias y verificación directa o por tercero.

Requisito	N1 · Estándar	N2 · Reforzado	N3 · Crítico
Seguridad	Configuración de datos verificada (no entrenamiento, retención).	Evaluación documental de seguridad de IA (SEG y AG aplicables).	Evaluación técnica, pruebas adversarias propias o informes independientes recientes; derecho a pruebas.
Contrato	Condiciones estándar revisadas con las cláusulas 1–4 de la sección 6.	Anexo de IA y encargo de tratamiento con las cláusulas marcadas para N2.	Contrato negociado con todas las cláusulas; DORA art. 30.3 si soporta funciones esenciales o importantes de una entidad financiera.
Aprobación	Responsable de producto con conformidad de compras.	Patrocinador con conformidad de riesgos y de protección de datos.	Comité de IA con conformidad de riesgos, seguridad de la información, protección de datos y jurídico.
Auditoría	No requerida.	Informes independientes anuales.	Derecho de auditoría y acceso, directo o por tercero designado.
Seguimiento	Revisión anual.	Revisión semestral e indicadores de servicio.	Revisión trimestral, indicadores mensuales, reunión de gobierno de la relación.
Salida	Exportación de datos garantizada.	Plan de salida documentado.	Plan de salida con alternativa identificada y ensayo o prueba documentada.
Incidentes	Según condiciones del proveedor, verificadas.	Notificación sin dilación indebida con plazo compatible con las obligaciones propias.	Notificación en un plazo máximo acordado (orientativamente 24 horas o menos desde la detección) y cooperación en la respuesta y en las notificaciones regulatorias.
Registro	T09.	T09.	T09 y, si aplica DORA, registro de información.

Un proveedor N3 implica normalmente intensidad **Enterprise** en los casos de uso que lo usan (01 §9.2).

4.3 Contenido del cuestionario de diligencia debida

1. **Identidad y solvencia:** grupo, país, antigüedad, situación financiera, seguros.
2. **Servicio y modelo:** modelos usados, propios o de terceros; versiones; política de cambios y retirada de versiones; documentación del modelo.
3. **Datos:** uso para entrenamiento o mejora; retención; ubicación; transferencias; cifrado; separación entre clientes; borrado.
4. **Subencargados y cadena de suministro:** lista, ubicación, funciones, política de cambios.

5. **Seguridad:** certificaciones, pruebas de intrusión, gestión de vulnerabilidades, protección frente a inyección de instrucciones, fuga y extracción, controles de agentes si los hay.
6. **Cumplimiento del Reglamento de IA:** rol del proveedor, clasificación, documentación técnica e instrucciones de uso, registros, supervisión humana, cooperación en incidentes, obligaciones como proveedor de modelos de propósito general si aplica.
7. **Protección de datos:** condición de encargado, medidas, apoyo a evaluaciones de impacto y a derechos de los interesados.
8. **Propiedad intelectual:** titularidad de resultados, licencias de datos de entrenamiento, indemnidad.
9. **Continuidad:** disponibilidad, planes de continuidad, pruebas, dependencia de terceros.
10. **Incidentes:** proceso, plazos de notificación, historial de incidentes relevantes.
11. **Salida:** formatos de exportación, asistencia, plazos, borrado certificado.
12. **Ética y uso responsable:** políticas de uso aceptable, gestión de sesgo, restricciones de uso.

El cuestionario completo está en P55. Un resultado **No conforme** en los bloques 3 (datos), 5 (seguridad) o 7 (protección de datos) impide usar el proveedor con datos de producción hasta resolverlo.

Criterios de compra de seguridad de la IA. En N2 y N3 la compañía pide además: certificación ISO/IEC 42001 del servicio, si existe, con su alcance; informes independientes recientes de pruebas adversarias del servicio de IA; derecho a hacer pruebas propias (N3); acceso a los registros de entradas, salidas y acciones que necesitan la monitorización y la investigación de incidentes (52 §11); y ubicación del tratamiento, incluidos los filtros y la monitorización del propio proveedor. Se recogen en el bloque 5 de P55.

05

Ciclo de vida del proveedor

Etapa	Qué se hace	Evidencia	Responsable	Fase SEVEN-G
1. Selección	Decisión de construir, comprar o aliarse; requisitos; nivel N preliminar; alternativas comparadas.	P10; requisitos; comparativa.	Responsable de producto con compras.	3
2. Diligencia debida	Cuestionario y verificación según nivel; evaluación de seguridad y protección de datos; riesgos RT-TER.	P14; P55; riesgos en P12.	Compras, seguridad, protección de datos, riesgos.	3
3. Contrato	Negociación con las cláusulas del nivel; aprobación.	Contrato (P56); lista de cláusulas verificada en P14.	Jurídico y compras.	3–4

Etapa	Qué se hace	Evidencia	Responsable	Fase SEVEN-G
4. Integración	Configuración segura (retención, no entrenamiento, regiones); identidades y permisos; registro; pruebas; plan de salida.	P15, P18; plan de salida.	Responsable técnico.	4–5
5. Seguimiento	Indicadores de servicio, incidentes, cambios de modelo, subencargados, revisiones periódicas, reevaluación de nivel.	T09; actas de revisión (P57 §5); P27.	Gestor de la relación y responsable de operación.	6
6. Salida	Activación del plan: transición, portabilidad, borrado certificado, revocación de accesos, lecciones.	Certificado de borrado y acta de cierre (P57 §8–9); P30.	Responsable técnico y jurídico.	7

Disparadores de reevaluación: cambio de modelo o de versión principal; cambio de subencargados o de ubicación; incidente S1 o S2 imputable al proveedor; cambio de propiedad del proveedor; cambio de uso o de nivel de autonomía; nueva obligación regulatoria; deterioro de indicadores de servicio; aviso de retirada de un modelo.

06

Cláusulas contractuales clave

Sí = debe figurar · **Rec.** = recomendada · **—** = no requerida. En N1 muchas cláusulas no son negociables: se verifican en las condiciones estándar y, si faltan, se registra el riesgo y quién lo acepta. En todos los niveles, mientras una cláusula **Sí** falte sin ese riesgo registrado y aceptado por el órgano que corresponde a su nivel (33 §7), el proveedor no se usa con datos de producción.

#	Cláusula	Qué debe asegurar	N1	N2	N3
1	**Uso de datos para entrenamiento**	Las entradas, contextos, resultados y datos de la compañía no se usan para entrenar ni mejorar modelos ni para otros fines, salvo autorización expresa y específica.	Sí	Sí	Sí
2	**Confidencialidad y tratamiento de datos**	Confidencialidad; encargo de tratamiento conforme al art. 28 del RGPD cuando haya datos personales; retención limitada y borrado.	Sí	Sí	Sí
3	**Ubicación y transferencias**	Regiones de tratamiento y almacenamiento; garantías del capítulo V del RGPD para transferencias internacionales; aviso previo de cambios.	Sí	Sí	Sí

#	Cláusula	Qué debe asegurar	N1	N2	N3
4	**Seguridad**	Medidas mínimas, certificaciones mantenidas, gestión de vulnerabilidades, protección frente a amenazas específicas de IA.	Sí	Sí	Sí
5	**Subencargados**	Lista actualizada; autorización previa o derecho de oposición ante cambios; mismas obligaciones en cadena.	Rec.	Sí	Sí
6	**Propiedad intelectual y resultados**	Titularidad o derechos de uso de los resultados; indemnidad frente a reclamaciones por infracción derivadas del modelo o de sus datos de entrenamiento; propiedad de lo desarrollado a medida.	Rec.	Sí	Sí
7	**Notificación de incidentes**	Plazo máximo, contenido mínimo, cooperación en la investigación y en las notificaciones regulatorias de la compañía (documento 37).	Rec.	Sí	Sí
8	**Cambios de modelo**	Preaviso de cambios de versión, comportamiento o retirada de modelos; posibilidad de fijar versiones durante un periodo; información suficiente para evaluar el cambio antes de su efecto.	Rec.	Sí	Sí
9	**Niveles de servicio**	Disponibilidad, latencia, soporte, penalizaciones y medición.	—	Sí	Sí
Mapa de esferas y niveles de ambición (10)	**Registros y trazabilidad**	Acceso a los registros necesarios para supervisión, investigación y obligaciones regulatorias, con plazos de conservación.	—	Sí	Sí
Modelo de madurez (11)	**Auditoría y acceso**	Derecho de auditoría, inspección y acceso de la compañía, de auditores designados y de los supervisores competentes.	—	Rec.	Sí
Índice de transformación (12)	**Obligaciones del Reglamento de IA en la cadena de valor**	Reparto de roles; entrega de documentación técnica e instrucciones de uso; información sobre capacidades y limitaciones; cooperación en supervisión humana, registros, vigilancia posterior a la comercialización e incidentes graves; acuerdo escrito del art. 25.4 cuando el tercero suministra componentes a un sistema de alto riesgo.	Rec.	Sí	Sí
Tesis de IA, ambición y apetito de riesgo (13)	**Transparencia sobre funciones de IA**	Aviso previo de nuevas funciones de IA en el servicio; posibilidad de mantenerlas desactivadas hasta su evaluación.	Rec.	Sí	Sí
Gestión de cartera (14)	**Continuidad**	Planes de continuidad y recuperación probados, con información a la compañía de sus resultados.	—	Rec.	Sí

#	Cláusula	Qué debe asegurar	N1	N2	N3
15	**Salida y transición**	Periodo de transición, asistencia, exportación en formatos utilizables (datos, configuraciones, instrucciones, registros), borrado certificado, continuidad durante la transición.	Rec.	Sí	Sí
16	**Terminación**	Derecho a terminar por incumplimiento grave, cambio regulatorio, incumplimiento de seguridad, cambio de control o instrucción del supervisor.	Rec.	Sí	Sí

6.1 Obligaciones del Reglamento de IA en la cadena de valor

Situación	Qué implica para el contrato
La compañía despliega un sistema de alto riesgo de un proveedor	El proveedor debe entregar instrucciones de uso que permitan cumplir las obligaciones del responsable del despliegue (art. 26): uso conforme, supervisión humana, vigilancia, conservación de registros y comunicación de riesgos e incidentes graves al proveedor. El contrato asegura el acceso a esa información y la cooperación.
La compañía se convierte en proveedor (art. 25.1)	Por modificación sustancial, cambio de finalidad o comercialización con su nombre. El proveedor inicial debe cooperar y facilitar información (art. 25.2); el contrato lo recoge.
Un tercero suministra herramientas, servicios, componentes o procesos a un sistema de alto riesgo de la compañía	Acuerdo escrito que especifique la información, capacidades, acceso técnico y asistencia necesarios (art. 25.4). No se exige a componentes distintos de modelos de propósito general puestos a disposición del público con licencia libre y de código abierto.
La compañía integra un modelo de propósito general	El proveedor del modelo debe facilitar a los proveedores posteriores información y documentación para comprender sus capacidades y limitaciones (art. 53). El contrato asegura su obtención y actualización.

Las obligaciones de los sistemas de alto riesgo del anexo III son aplicables desde el 2 de diciembre de 2027, tras el Ómnibus digital sobre IA. Los contratos de larga duración firmados antes **deberían** incluir ya estas cláusulas.

6.2 DORA para terceros TIC

Aplica a las entidades financieras sujetas a DORA cuando el servicio de IA es un servicio TIC prestado por un tercero:

Requisito	Referencia	Encaje en SEVEN-G
Estrategia y política de riesgo de terceros TIC aprobada por el órgano de administración	Art. 28.2; Reglamento Delegado (UE) 2024/1773	Política corporativa (31) y C2.
Registro de información de todos los acuerdos con terceros TIC	Art. 28.3; Reglamento de Ejecución (UE) 2024/2956	T09 alimenta el registro.
Análisis previo a la contratación, diligencia debida y conflictos de interés	Art. 28.4	Etapas 1 y 2 del ciclo (sección 5).
Estrategias de salida para servicios que soportan funciones esenciales o importantes	Art. 28.8	Cláusula 15; salida probada en N3.
Evaluación del riesgo de concentración y de la subcontratación en cadena	Art. 29; Reglamento Delegado (UE) 2025/532	Sección 7; cláusula 5.
Cláusulas contractuales mínimas para todos los servicios TIC y reforzadas para funciones esenciales o importantes	Art. 30.2 y 30.3	Sección 6; todo servicio N3 de una entidad financiera se revisa contra el art. 30.3.
Proveedores terceros esenciales de servicios de TIC designados por las Autoridades Europeas de Supervisión	Arts. 31 y siguientes	La supervisión europea del proveedor no sustituye la gestión del riesgo por la entidad. Las AES publicaron la primera lista de designados en noviembre de 2025; debe consultarse la vigente.

Si la compañía no está sujeta a DORA, sus requisitos **pueden** usarse como referencia de buenas prácticas para servicios N3.

07

Dependencia tecnológica y concentración

7.1 Dependencia de un proveedor

Señal de dependencia	Medida
Instrucciones, flujos o agentes diseñados sobre funciones propietarias.	Capa de abstracción de modelos; instrucciones y evaluaciones versionadas en repositorios propios.

Señal de dependencia	Medida
Datos, índices o memorias solo exportables en formatos cerrados.	Cláusula de exportación; copias periódicas en formato abierto.
Evaluaciones de calidad hechas solo por el proveedor.	Conjunto de evaluación propio que permite comparar modelos alternativos.
Conocimiento de la solución solo en el integrador.	Documentación, transferencia de conocimiento y propiedad de lo construido.
Precio por uso sin límites ni previsión.	Presupuestos de consumo, alertas y cláusulas de revisión de precios.
Sin alternativa probada.	Evaluación periódica de al menos una alternativa para servicios N3.

La **prueba de portabilidad** (P57 §7) para servicios N3 consiste en ejecutar el conjunto de evaluación propio con un modelo o proveedor alternativo y documentar la diferencia de resultados, coste y esfuerzo de migración. Se realiza al menos una vez al año o antes de renovar el contrato.

7.2 Concentración

La concentración se mide en cartera (documento 33 §10) con estos indicadores:

Indicador	Definición
Sistemas por proveedor	Número de sistemas en producción que dependen de cada proveedor de modelos y de plataforma.
Valor dependiente	Proporción del valor validado de la cartera que depende de cada proveedor.
Funciones críticas dependientes	Funciones críticas o importantes soportadas por cada proveedor.
Proveedores N3 sin salida probada	Número y antigüedad.
Subencargados comunes	Subencargados que aparecen en la cadena de varios proveedores N2 o N3.

Los límites de concentración forman parte del apetito de riesgo (documento 13). Cuando se superan, el comité de IA decide entre diversificar, reforzar la salida o aceptar el riesgo según 33 §7.

08

IA embebida en software ya contratado

Muchas aplicaciones de negocio incorporan funciones de IA mediante actualizaciones, a veces activadas por defecto. Son sistemas de IA de terceros integrados en procesos (01 §1.2) y deben gobernarse.

8.1 Proceso

Paso	Qué se hace	Responsable
1. Identificar	Cuestionario (P55, anexo A) a los proveedores de software vigentes sobre funciones de IA existentes y previstas; revisión de notas de versión; revisión de configuraciones. Se prioriza el software que trata datos personales o confidenciales o que interviene en decisiones.	Oficina de IA con compras y tecnología
2. Inventariar	Alta de cada función de IA relevante en el inventario (T02), vinculada al proveedor en T09, con etiqueta de tecnología "IA de terceros embebida".	Oficina de IA
3. Clasificar	Determinar si es uso corporativo de propósito general o IA que interviene en decisiones, operaciones o relación con clientes; nivel N; criterios Enterprise; clasificación regulatoria.	Responsable de riesgos de IA
4. Decidir	Mantener desactivada, activar con controles o activar como caso de uso con ciclo completo.	Según 4.2 y 01 §1.2
5. Contratar	Adenda (P56 §8) con las cláusulas 1, 3, 8 y 13 como mínimo y las que correspondan al nivel.	Jurídico y compras
6. Vigilar	Revisión de actualizaciones y cambios de configuración en cada R6 o, en su defecto, semestral.	Gestor de la relación

8.2 Reglas

- Las funciones de IA de software contratado que traten datos personales o confidenciales **deben** permanecer desactivadas hasta su evaluación, cuando la configuración lo permita.
- Si no pueden desactivarse, se registra el riesgo RT-TER-06, se evalúa con prioridad y se decide en el siguiente comité de IA.
- Una función embebida que interviene en decisiones sobre personas o actúa con nivel A2 o A3 recorre el ciclo de vida completo, centrado en selección, integración, contrato y controles.

09

Registro de proveedores

El registro de proveedores es la herramienta **T09**, sobre la entidad *Proveedor* del modelo de datos común (03 §4). Cada relación proveedor–servicio es un registro.

Bloque	Campos
Identificación	Identificador interno; razón social; grupo; país; tipo de tercero (1.1); gestor interno de la relación.
Servicio	Descripción comprensible; modelos y versiones; tipo de contratación (construir sobre, comprar, adaptar, aliarse); sistemas e casos de uso vinculados (IA-AAAA-NNN).
Clasificación	Nivel N1–N3 con el valor de cada factor y justificación; función crítica o importante (sí o no); nivel de autonomía máximo; rol regulatorio del proveedor y de la compañía.
Datos	Categorías de datos; datos personales (sí o no); ubicación; transferencias y garantía; retención; uso para entrenamiento (excluido, autorizado o sin verificar).
Cadena	Subencargados con ubicación y función; subcontratación de funciones críticas.
Contrato	Referencia; fechas de inicio, renovación y fin; preaviso; estado de las 16 cláusulas (presente, parcial, ausente, no aplica).
Evaluación	Fecha y resultado de la diligencia debida (P14); certificaciones e informes con vigencia; evaluación de seguridad; condiciones impuestas.
Riesgo	Riesgos RT-TER y otros vinculados (T06); nivel residual principal.
Seguimiento	Indicadores de servicio; incidentes imputables (INC-AAAA-NNN); cambios de modelo notificados; fecha de última y próxima revisión.
Dependencia y salida	Sustituibilidad estimada; alternativa identificada; plan de salida (sí o no, fecha de prueba); valor de cartera dependiente.
Estado	En evaluación · Aprobado · Aprobado con condiciones · Rechazado · En salida · Finalizado.
Historial	Eventos con fecha, autor y motivo.

10

Seguimiento e indicadores

Indicador	Para qué	Destinatario
Proveedores por nivel N1–N3 y por tipo	Visión de la exposición a terceros.	Comité de IA
Revisiones periódicas vencidas	Detectar relaciones sin seguimiento.	Oficina de IA
Proveedores N2 y N3 con cláusulas clave ausentes	Priorizar renegociación.	Comité de IA
Configuración de no entrenamiento sin verificar	Controlar RT-TER-02.	Protección de datos
Cambios de modelo notificados y evaluados antes de su efecto	Controlar RT-TER-03.	Responsables técnicos
Incidentes imputables a proveedores por severidad	Calidad del servicio y cumplimiento.	Comité de IA; consejo si S1
Proveedores N3 sin salida probada	Controlar RT-TER-01 y RT-TER-05.	Comité de IA; consejo
Concentración de valor en el principal proveedor	Riesgo de cartera.	Consejo
Funciones de IA embebida identificadas y evaluadas	Controlar RT-TER-06.	Oficina de IA

Al consejo o su comisión delegada se informa trimestralmente de la concentración, de los proveedores N3 sin salida probada, de los incidentes S1 y S2 imputables a terceros y de las decisiones de aceptación de riesgos de terceros de nivel Alto.

11

Roles

Rol	Responsabilidad en la gestión de terceros
Responsable de producto de IA	Necesidad, requisitos, decisión propuesta de construir, comprar o aliarse.
Responsable técnico de IA	Evaluación técnica, integración segura, portabilidad, plan de salida técnico.
Responsable de operación de IA	Indicadores de servicio, incidentes y cambios de modelo en producción.

Rol	Responsabilidad en la gestión de terceros
Responsable de riesgos de IA	Nivel N, riesgos RT-TER, conformidad.
Compras	Proceso de selección, cuestionario, registro y gestión contractual.
Jurídico	Cláusulas, roles regulatorios, propiedad intelectual.
Seguridad de la información	Evaluación de seguridad y conformidad en N2 y N3.
Protección de datos	Encargo de tratamiento, transferencias, evaluaciones de impacto.
Comité de IA	Aprobación de N3, límites de concentración, aceptación de riesgos Altos.
Auditor de IA	Verifica en G3 y G5 que la evaluación y el contrato corresponden al nivel.

12

Herramientas y plantillas asociadas

Nombre	Uso
Evaluación de proveedor de IA (P14)	Nivel N con factores; decisión de construir, comprar o aliarse; cuestionario de diligencia debida; evaluación de seguridad y protección de datos; verificación de las 16 cláusulas; riesgos; plan de salida; conformidades y aprobación. Fase 3; se actualiza en R6 y ante disparadores.
Registro de proveedores de IA (T09)	Campos de la sección 9, alertas de revisión y renovación, indicadores de la sección 10 y vista de concentración. Módulo de T01; su formato de trabajo es P57.
Cuestionario de diligencia debida a proveedores de IA (P55)	Cuestionario de la sección 4.3 por nivel, con valoración y traslado a P14; anexo A para la IA embebida (sección 8). Fase 3.
Cláusulas contractuales tipo de IA (P56)	Redacción modelo de las 16 cláusulas de la sección 6, anexo de IA para contratos existentes y adenda de IA embebida. Fases 3–4.
Registro de proveedores y plan de salida (P57)	Registro de la sección 9, concentración, actas de revisión, plan de salida, prueba de portabilidad, certificado de borrado y acta de cierre (secciones 5, 7 y 9). Fases 3 a 7.
Evaluación de viabilidad · Matriz y registro de riesgos · Decisión de escalado o retirada (P10 · P12 · P30)	Decisión de contratación, riesgos RT-TER y salida.

Nombre	Uso
Inventario · Riesgos · Incidentes (T02 · T06 · T08)	Sistemas vinculados, riesgos e incidentes de terceros.

13

Documentos relacionados

Documento	Relación
01 · Metodología fundacional	IA de terceros integrada en procesos (§1.2), criterios Enterprise (§9.2) y encaje de DORA (§13).
13 · Tesis de IA, ambición y apetito de riesgo	Plazos de sustituibilidad, umbral M y límites de concentración.
31 · Política corporativa y uso aceptable	Uso corporativo de IA de propósito general y política de terceros.
33 · Metodología de riesgos de IA	Riesgos RT-TER y riesgo de cartera.
34 · Mapeo regulatorio	Obligaciones de la cadena de valor del Reglamento de IA , RGPD y DORA.
35 · Seguridad de IA y agentes	Controles SEG y AG exigibles a proveedores y componentes.
37 · No conformidades e incidentes	Incidentes de proveedores y notificaciones.
42 · Costes de IA	Coste total y coste de salida.

14

Control de versiones

Versión	Fecha	Cambios
0.1	16-09-2026	Primera versión. Define los criterios para construir, comprar, adaptar o aliarse; los niveles de exigencia N1–N3 con cuatro factores y requisitos por nivel; el ciclo de vida del proveedor; dieciséis cláusulas contractuales clave, con las obligaciones del Reglamento de IA en la cadena de valor y DORA ; la gestión de la dependencia y la concentración; el tratamiento de la IA embebida y los campos del registro de proveedores.

Versión	Fecha	Cambios
0.2	19-10-2026	Principio 8 «Probar también es usar» y criterios de compra de seguridad de la IA (4.3) (D159).

Fuentes externas citadas

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

Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva SRI 2 / NIS2) · https://eur-lex.europa.eu/eli/dir/2022/2555/oj/spa · Parlamento Europeo y Consejo de la UE · 14-12-2022

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

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

Reglamento (UE) 2026/1744 del Parlamento Europeo y del Consejo, de 8 de julio de 2026, por el que se modifican los Reglamentos (UE) 2024/1689, (UE) 2018/1139 y (UE) 2023/1230 en lo que respecta a la simplificación de la aplicación de normas armonizadas en materia de inteligencia artificial (Ómnibus digital sobre IA) · https://eur-lex.europa.eu/eli/reg/2026/1744/oj/spa · Parlamento Europeo y Consejo de la UE · 08-07-2026

Reglamento de Ejecución (UE) 2024/2956 de la Comisión, de 29 de noviembre de 2024, por el que se establecen normas técnicas de ejecución para la aplicación del Reglamento (UE) 2022/2554 en lo que respecta a las plantillas normalizadas para el registro de información · https://eur-lex.europa.eu/eli/reg_impl/2024/2956/oj/spa · Comisión Europea · 29-11-2024

Reglamento Delegado (UE) 2024/1773 de la Comisión, de 13 de marzo de 2024, por el que se completa el Reglamento (UE) 2022/2554 mediante normas técnicas de regulación que especifican el contenido detallado de la política relativa a los acuerdos contractuales sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes prestados por proveedores terceros de servicios de TIC · https://eur-lex.europa.eu/eli/reg_del/2024/1773/oj/spa · Comisión Europea · 13-03-2024

Reglamento Delegado (UE) 2025/532 de la Comisión, de 24 de marzo de 2025, por el que se completa el Reglamento (UE) 2022/2554 en lo que respecta a las normas técnicas de regulación que especifican los elementos que debe determinar y evaluar una entidad financiera cuando subcontrata servicios de TIC que sustentan funciones esenciales o importantes · https://eur-lex.europa.eu/eli/reg_del/2025/532/oj/spa · Comisión Europea · 24-03-2025

Autoridades Europeas de Supervisión (ABE/EBA, AESPJ/EIOPA y AEVM/ESMA): designación de proveedores terceros esenciales de servicios de TIC con arreglo a DORA (18 de noviembre de 2025) · https://www.eba.europa.eu/publications-and-media/press-releases/european-supervisory-authorities-designate-critical-ict-third-party-providers-under-digital · Autoridades Europeas de Supervisión (EBA, EIOPA, ESMA) · 18-11-2025

ISO/IEC 42001:2023 Tecnología de la información — Inteligencia artificial — Sistema de gestión · https://www.iso.org/standard/42001 · ISO/IEC (JTC 1/SC 42) · 18-12-2023