CURSO · MÓDULO 05

Módulo 05 · Gobierno y riesgo

Quién construye, quién verifica, quién decide y quién puede aceptar un riesgo

Fernando García Varela Versión 0.1 (borrador de trabajo) 19-09-2026 Borrador para revisión

20	3	25	4
minutos	garantías que nunca se reducen	celdas de la matriz de riesgos	niveles de riesgo

EN ESTE DOCUMENTO

01 Objetivo
02 Ideas clave
03 Recorrido guiado
04 Ejercicio
05 Autocomprobación
06 Siguiente paso

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

Objetivo

Al terminar sabrá explicar la separación de funciones del marco, asignar los roles de un caso de uso sin incompatibilidades y leer un registro de riesgos: nivel inherente, residual y órgano que puede aceptarlo.

02

Ideas clave

1. **Nadie se aprueba a sí mismo.** Quien construye no verifica ni decide su propio trabajo; la conformidad de riesgos es independiente del equipo; el consejo aprueba la dirección y el apetito de riesgo.
2. **No hace falta crear órganos nuevos.** En una compañía mediana bastan el comité de dirección con un punto mensual de IA, una oficina de IA de una persona y un auditor independiente para los casos de uso Enterprise.

3. **Riesgo = probabilidad × impacto**, de 1 a 25, en cuatro niveles. Se valora antes de los controles (inherente) y después (residual).
4. **Cada nivel tiene su órgano de aceptación.** Un riesgo residual Crítico solo lo acepta el consejo; sin esa aprobación, bloquea G3 y G5.

03

Recorrido guiado

Paso	Qué abrir	Qué mirar
1	documento 01, sección 8	Roles del caso de uso, incompatibilidades y órganos de la compañía.
2	documento 30, sección 11	La adaptación a organizaciones pequeñas.
3	documento 33, secciones 4 a 7	Escalas, riesgo inherente y residual, respuestas y aceptación.
4	documento 32, sección 5	El árbol de clasificación regulatoria: se hace antes de diseñar.
5	T06 (vista de riesgos del registro)	La matriz 5 × 5 de la cartera de ejemplo y las observaciones que genera.

04

Ejercicio

En la vista de riesgos del registro de ejemplo, pulse la celda con el riesgo residual más alto. ¿Qué caso de uso es, quién lo ha aceptado y tiene plan de contingencia? Después cambie a riesgo inherente y observe cuánto reducen el riesgo los controles: ¿es creíble esa reducción?

05

Autocomprobación

1. ¿Puede el patrocinador ser también el responsable de riesgos de su caso de uso?
2. ¿Quién acepta un riesgo residual Alto?
3. ¿En qué fase debe existir ya el registro de riesgos?
4. ¿Qué pasa con un caso de uso Lite que empieza a tratar datos especialmente protegidos?

06

Siguiente paso

Módulo 06 · Medir el valor · Guía del curso

Respuestas. 1) No: son roles incompatibles. 2) El comité de IA. 3) En la fase 3; es criterio de G3. 4) Pasa a intensidad Enterprise: la intensidad se revisa en G3 y en cada R6, y basta un criterio.