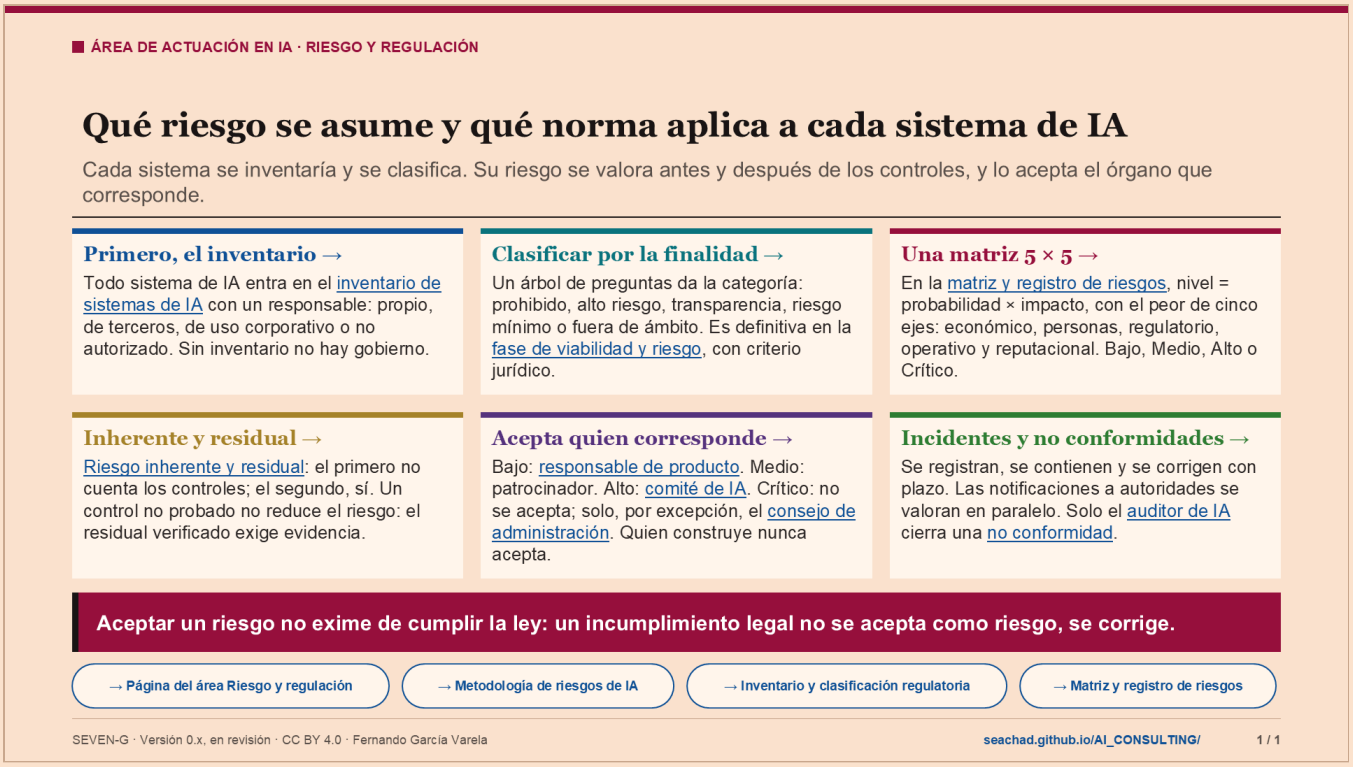

Notas

Esta slide resume el área de actuación Riesgo y regulación de SEVEN-G. Responde a dos preguntas que el consejo necesita contestar para cada sistema de IA: qué riesgo asume la compañía y qué norma le aplica. La respuesta tiene seis piezas, que se leen en orden.

- Primero, el inventario. Se inventarían todos los sistemas de IA de cuatro tipos de uso: casos de uso propios, IA de terceros integrada en procesos, uso corporativo de herramientas de propósito general y uso no autorizado. Cada sistema tiene un responsable con nombre, no un área genérica. Por qué importa: sin saber qué sistemas existen, no se pueden gestionar riesgos, cumplir obligaciones ni informar al consejo (documento 32).
- Clasificar por la finalidad. Un árbol de preguntas, basado en el Reglamento Europeo de IA, da la categoría del sistema: prohibido, alto riesgo, obligaciones de transparencia, riesgo mínimo o fuera de ámbito. Se clasifica por la finalidad prevista, no por la tecnología. La clasificación es provisional en la fase 0 y definitiva en la fase 3, con criterio jurídico cualificado. Ante la duda, se aplica la categoría más exigente.
- Una matriz 5 × 5. El nivel de riesgo es probabilidad por impacto, cada uno de 1 a 5. El impacto es el peor de cinco ejes: económico, personas y derechos, regulatorio, operativo y reputacional. No se promedia. Hay cuatro niveles: Bajo (1 a 4), Medio (5 a 9), Alto (10 a 15) y Crítico (16 a 25).
- Inherente y residual. El riesgo inherente es el nivel sin los controles específicos del caso de uso. El residual es el nivel con controles: objetivo en el diseño y verificado cuando hay evidencia de que los controles funcionan. Un control no probado no reduce el riesgo verificado.
- Acepta quien corresponde. Cada nivel residual lo acepta un órgano distinto. El residual Crítico no se acepta: solo, por excepción, lo aprueba el consejo o su comisión delegada. Un residual Crítico sin esa aprobación bloquea la puerta de viabilidad (G3) y la de puesta en producción (G5).
- Incidentes y no conformidades. Un incidente de IA es un suceso en el que un sistema causa o puede causar daño. Una no conformidad es el incumplimiento de un requisito obligatorio del marco. Los dos

se registran, se contienen y se corrigen con plazo.

Un ejemplo con datos ficticios del registro de ejemplo del sitio: el asistente conversacional de atención a clientes (IA-2025-002) se clasifica con obligaciones de transparencia, porque las personas conversan con una IA. Su riesgo de que una inyección de instrucciones revele datos de otro cliente es Crítico sin controles (4 × 4 = 16) y Medio con controles probados (2 × 4 = 8). Por eso lo acepta el patrocinador, con la conformidad del responsable de riesgos de IA.

Aviso importante: SEVEN-G no es asesoramiento jurídico ni garantiza el cumplimiento de ninguna norma. Cada organización identifica la normativa que le aplica, también la de su sector, y verifica su vigencia con asesoramiento cualificado (documento 34).

Pregunta para el aula: en su organización, ¿quién firma hoy la aceptación de un riesgo alto de un sistema de IA? ¿Es la misma persona que lo construye?

TÉRMINOS DE ESTA SLIDE

- **Inventario de sistemas de IA** (T02): Lista de todos los sistemas de IA de la compañía: los propios, la IA de terceros integrada en procesos, los asistentes que usan los empleados y el uso no autorizado detectado. Cada sistema tiene responsable, clasificación regulatoria, intensidad y autonomía. Es lo primero que se pide, porque no se puede gobernar lo que no se conoce. Es una vista del registro de casos de uso: al abrir el enlace, elija «Inventario» (datos ficticios). https://seachad.github.io/AI_CONSULTING/SEVEN-G/herramientas/T01_registro_iniciativas/registro.html
- **Viabilidad y riesgo** (fase 3): Fase en la que se comprueba con una prueba acotada si el caso es viable técnica y económicamente, se clasifica según la regulación y se registran sus riesgos. Termina en la puerta de viabilidad (G3), la principal puerta de parada antes del gran gasto. Es donde más dinero se ahorra parando a tiempo. El enlace abre el manual de la fase en el documento 20. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/20_SEVEN-G_Manuales_de_fase.html#fase-3-viabilidad-y-riesgo
- **Matriz y registro de riesgos** (T06): Matriz de probabilidad por impacto (5 × 5) y registro de los riesgos de cada caso de uso: riesgo inherente y residual, controles y su eficacia, respuesta, contingencia y quién acepta el riesgo. Es obligatoria desde la fase 3. Se rellena con la plantilla P12 o en la vista «Riesgos» del registro de casos de uso, que además descarga un Excel del caso con planes de mitigación propuestos. Datos ficticios. https://seachad.github.io/AI_CONSULTING/SEVEN-G/herramientas/T01_registro_iniciativas/registro.html
- **Riesgo inherente y residual**: El riesgo inherente es el que tiene un caso de uso sin controles; el residual, el que queda tras aplicarlos. Ambos se miden con probabilidad por impacto en una matriz de 5 × 5. El residual decide quién debe aceptar el riesgo: un Crítico solo lo acepta el consejo. El enlace abre la explicación en el documento 33. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html#riesgo-inherente-controles-y-riesgo-residual
- **Responsable de producto de IA**: Rol que construye el caso de uso: responde de la hipótesis de valor, del uso real y de la adopción. Por la separación de funciones, no puede verificar evidencias ni decidir las puertas de su propio caso. Es el interlocutor diario del equipo con el patrocinador. El enlace abre los roles en el documento 01. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/01_SEVEN-G_Metodologia_fundacional.html#8-1-roles-del-caso-de-uso
- **Comité de IA**: Órgano de dirección que decide la cartera y las puertas de su nivel, asigna presupuesto y eleva al consejo lo que le corresponde. Reúne a negocio, tecnología, finanzas y riesgos, y se rige por un reglamento (P38). Importa porque convierte decisiones dispersas en una sola cartera. El enlace abre su papel en el modelo de gobierno (documento 30). https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/30_SEVEN-G_Modelo_de_gobierno.html#3-3-comite-de-ia
- **Consejo de administración**: Máximo órgano de la compañía. En SEVEN-G aprueba la tesis de IA y el apetito de riesgo (C2), las apuestas de Transformar y su escalado, y supervisa la IA cada trimestre. La IA es un activo estratégico: sus grandes decisiones no son solo de tecnología. El enlace abre su papel en el modelo de gobierno (documento 30). https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/30_SEVEN-G_Modelo_de_gobierno.html#3-1-consejo-de-administracion

- **Auditor de IA**: Persona independiente que verifica la evidencia de las puertas en los casos de uso de intensidad Enterprise (en Lite lo hace la oficina de IA). No construye, no patrocina y no decide el caso que verifica. Da al consejo la seguridad de que las cifras y controles no los firma solo quien los defiende. El enlace abre su independencia y competencias en el documento 38. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/38_SEVEN-G_Marco_de_auditoria_de_IA.html#independencia-y-competencias-del-auditor-de-ia
- **No conformidad** (P50): Incumplimiento de una regla del marco o de un control, aunque no haya causado daño (por ejemplo, un caso en producción sin firma). Se clasifica en menor, mayor o crítica, se registra (P50), se analiza su causa (P52) y se corrige en plazo. Sirve para que el gobierno aprenda de sus fallos. El enlace abre el proceso en el documento 37. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/37_SEVEN-G_No_conformidades_e_incidentes.html#proceso-de-no-conformidades

FUENTES Y ENLACES

- **Página del área Riesgo y regulación** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/areas/riesgo.html
- **Documento 33 · Metodología de riesgos de IA** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html
- **Documento 32 · Inventario y clasificación regulatoria** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/32_SEVEN-G_Inventario_y_clasificacion_regulatoria.html
- **Documento 34 §1 · Alcance y responsabilidad del mapeo regulatorio** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/34_SEVEN-G_Mapeo_regulatorio.html#objeto-y-alcance
- **Documento 37 · No conformidades e incidentes** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/37_SEVEN-G_No_conformidades_e_incidentes.html
- **Reglamento (UE) 2024/1689 (Reglamento Europeo de IA), EUR-Lex** https://eur-lex.europa.eu/eli/reg/2024/1689/oj/spa
- **Metodología de riesgos de IA** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html
- **Inventario y clasificación regulatoria** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/32_SEVEN-G_Inventario_y_clasificacion_regulatoria.html

AVISO LEGAL

Aviso legal: ayuda metodológica genérica y gratuita, «tal cual» y con fines informativos; no es asesoramiento jurídico ni está revisada jurídicamente para ningún caso. Cada organización la adapta y es responsable de su revisión legal y de su cumplimiento regulatorio; puede no recoger cambios normativos recientes. En la máxima medida permitida por la ley, el autor no asume responsabilidad alguna por los efectos de su aplicación. No otorga certificación de ningún tipo. Detalle en el documento 93.

CC BY 4.0 (contenidos) · MIT (código) · Fernando García Varela · seachad.github.io/AI_CONSULTING/