

Notas

Esta presentación explica el área de actuación Riesgo y regulación de SEVEN-G. SEVEN-G es un marco abierto y gratuito para que una compañía gobierne, mida y decida sobre la IA. Su autor es Fernando García Varela y se publica con licencia CC BY 4.0.

El área responde a una pregunta doble: qué riesgo asume la compañía con cada sistema de IA y qué norma le aplica. Para responderla, SEVEN-G pide cuatro cosas:

- Inventariar todos los sistemas de IA, también los de terceros y los que se usan sin autorización.
- Clasificar cada sistema según la regulación que le aplica, empezando por el Reglamento Europeo de IA.
- Valorar sus riesgos antes y después de los controles, y que acepte el riesgo que queda el órgano que corresponde a su nivel.
- Registrar los incidentes y las no conformidades y corregirlos con plazo.

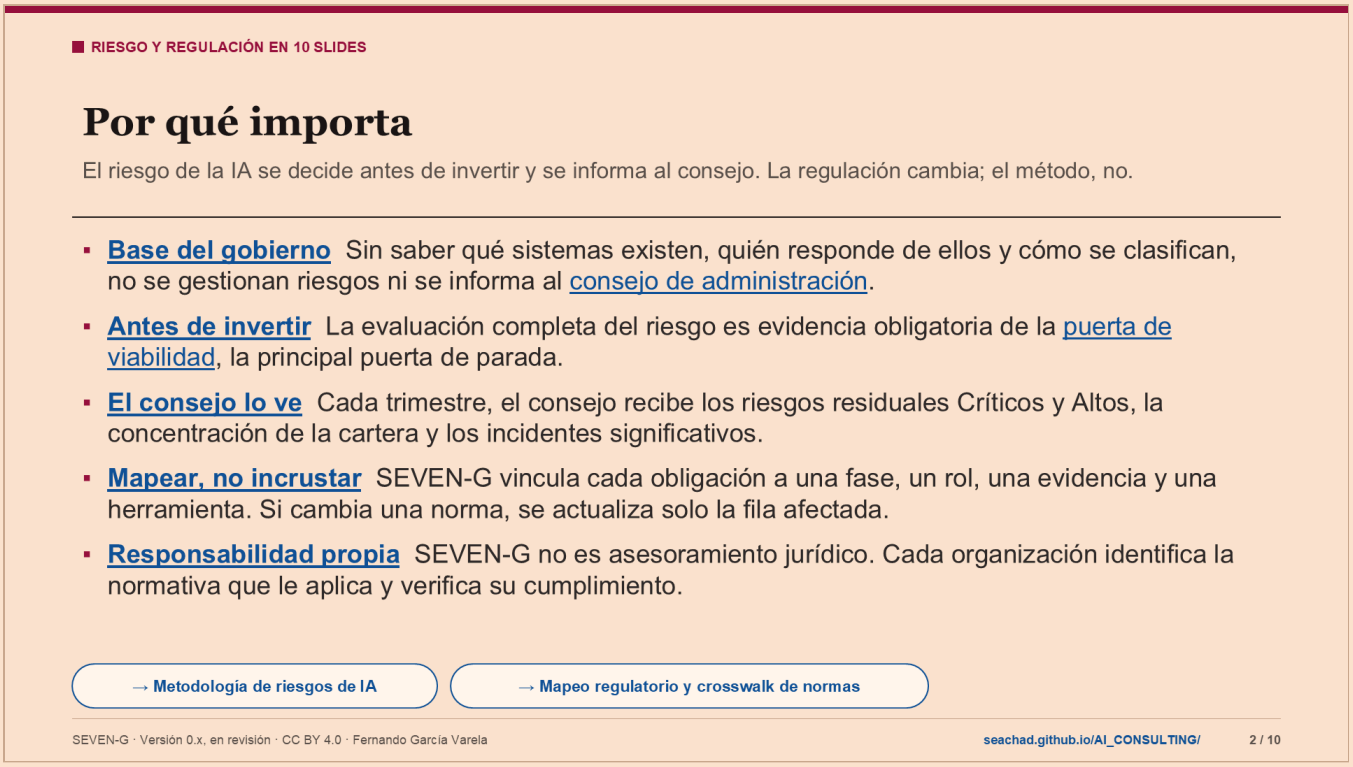
Las diez slides siguen este orden: por qué importa, los conceptos clave, cómo lo trata SEVEN-G a lo largo del ciclo de vida, las herramientas y plantillas, un ejemplo con datos ficticios, los errores frecuentes, preguntas para la dirección o el aula, la relación con otras áreas y con SPHERES, y cómo empezar.

Una advertencia que vale para toda la presentación: SEVEN-G no es asesoramiento jurídico y no garantiza el cumplimiento de ninguna norma. Cada organización identifica la normativa que le aplica, incluida la de su sector, y verifica su vigencia con asesoramiento cualificado.

Pregunta para abrir la sesión: si mañana un supervisor le pidiera la lista de sistemas de IA de su compañía con su clasificación, ¿cuánto tardaría en dársela?

FUENTES Y ENLACES

- **Página del área Riesgo y regulación** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/areas/riesgo.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
- **Qué es SEVEN-G** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/entrada/index.html



Notas

Esta slide da cinco razones para tomarse en serio el área.

- Base del gobierno. El documento 32 llama al inventario la base de todo el gobierno. Si la compañía no sabe qué sistemas de IA usa, tampoco sabe qué riesgos tiene ni qué obligaciones debe cumplir.
- Antes de invertir. El primer principio de la metodología de riesgos (documento 33) es que el riesgo se valora antes de invertir. La evaluación completa se exige en la puerta de viabilidad (G3). Es la principal puerta de parada: allí se decide si se sigue antes del gasto grande de diseño y construcción.
- El consejo lo ve. El consejo o su comisión delegada recibe cada trimestre los residuales Críticos y Altos por esfera, la concentración y los escenarios de cartera, el cumplimiento del apetito de riesgo y los incidentes significativos. El informe usa lenguaje de negocio: qué puede pasar, a quién afecta, qué se hace y qué decisión se pide.
- Mapear, no incrustar. SEVEN-G no copia la regulación dentro de sus fases. Vincula cada obligación a una fase o etapa, un rol responsable, una evidencia y una herramienta. Por qué importa: la regulación de la IA cambia con rapidez, y así un cambio normativo no obliga a rehacer el ciclo de vida, las puertas ni las plantillas.
- Responsabilidad propia. El mapeo regulatorio del documento 34 es orientativo y refleja el estado de las normas a una fecha de consulta. La organización usuaria es la única responsable de identificar la normativa que le aplica, clasificar cada sistema y verificar su cumplimiento con asesoramiento jurídico cualificado.

Pregunta para el aula: ¿qué es más caro para una compañía, parar un caso de IA antes de construirlo o descubrir después de ponerlo en producción que estaba mal clasificado?

TÉRMINOS DE ESTA SLIDE

- **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

- **Puerta de viabilidad** (G3): La puerta más importante: decide, con la prueba de viabilidad, la clasificación regulatoria y el registro de riesgos, si el caso merece el gran gasto de construirlo. Se decide siempre por separado, nunca agrupada con otras. Es la principal puerta de parada: parar aquí cuesta poco; después, mucho. El enlace abre sus criterios en el documento 21. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/21_SEVEN-G_Criterios_de_gate_y_auditoria.html#6-4-g3-viabilidad

FUENTES Y ENLACES

- **Documento 33 §2 · Principios de la metodología de riesgos** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html#principios
- **Documento 33 §12 · Información de riesgos** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html#informacion-de-riesgos
- **Documento 34 §1.1 · SEVEN-G mapea, no incrusta** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/34_SEVEN-G_Mapeo_regulatorio.html#1-1-principio-seven-g-mapea-no-incrusta
- **Metodología de riesgos de IA** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html
- **Mapeo regulatorio y crosswalk de normas** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/34_SEVEN-G_Mapeo_regulatorio.html



Notas

Estos siete conceptos son el vocabulario mínimo del área. Todos salen del glosario de SEVEN-G (documento 02).

- Riesgo inherente. Es el riesgo antes de los controles propios del caso de uso. Los controles generales de la compañía solo cuentan si están probados y documentados.
- Riesgo residual. Es el riesgo con controles. Tiene dos momentos: el objetivo, que se espera tras aplicar los controles planificados y se usa en las puertas de viabilidad (G3) y diseño (G4); y el verificado, cuando hay evidencia de que los controles funcionan, que se exige en la puesta en producción (G5) y se sigue en la revisión de continuidad (R6). Por qué importa: separa lo que se promete de lo que se ha comprobado.
- Aceptación del riesgo. Es una decisión registrada, con vigencia y condiciones. La aceptación caduca si cambian el nivel, el sistema, el proveedor, el modelo, la clasificación regulatoria o la autonomía.
- Clasificación regulatoria. Determina, con criterio jurídico cualificado, la categoría del sistema (prohibido, alto riesgo, obligaciones de transparencia, riesgo mínimo, fuera de ámbito o pendiente de clasificar) y el rol de la compañía: por ejemplo, proveedor o responsable del despliegue.
- Sistema de IA de alto riesgo. Lo define el Reglamento Europeo de IA, no SEVEN-G. Es un criterio que lleva el caso de uso a la intensidad Enterprise, la más exigente. Las fechas de aplicación de sus obligaciones se tratan en el documento 34.
- No conformidad. Es un incumplimiento de un requisito obligatorio del marco. Se gestiona con contención, causa raíz, acción correctiva, verificación de eficacia, cierre y reauditoría.
- Incidente de IA. Es un suceso con daño real o posible, aunque el sistema siga disponible. Se clasifica por severidad: S1 crítica, S2 alta, S3 media y S4 baja.

El Reglamento Europeo de IA, el Reglamento (UE) 2024/1689 con sus modificaciones, es la referencia principal de la clasificación. Su texto oficial está en EUR-Lex.

Pregunta para el aula: ¿por qué cree que SEVEN-G distingue un incidente, que es un hecho con daño, de una no conformidad, que es un incumplimiento de una regla?

TÉRMINOS DE ESTA SLIDE

- **Glosario y convenciones** (documento 02): El glosario oficial de SEVEN-G: cada término con su definición, su equivalente en inglés y el documento que lo desarrolla, más las escalas y los códigos que se usan en todo el marco. Sirve para que todos llamen igual a lo mismo. El enlace abre el documento. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/02_SEVEN-G_Glosario_y_convenciones.html
- **Puerta de viabilidad** (G3): La puerta más importante: decide, con la prueba de viabilidad, la clasificación regulatoria y el registro de riesgos, si el caso merece el gran gasto de construirlo. Se decide siempre por separado, nunca agrupada con otras. Es la principal puerta de parada: parar aquí cuesta poco; después, mucho. El enlace abre sus criterios en el documento 21. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/21_SEVEN-G_Criterios_de_gate_y_auditoria.html#6-4-g3-viabilidad

FUENTES Y ENLACES

- **Documento 33 §5.1 · Riesgo inherente y residual** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html#5-1-definiciones
- **Documento 37 §1.1 · Definiciones de incidente y no conformidad** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/37_SEVEN-G_No_conformidades_e_incidentes.html#1-1-definiciones
- **Reglamento (UE) 2024/1689 (Reglamento Europeo de IA), EUR-Lex** https://eur-lex.europa.eu/eli/reg/2024/1689/oj/spa
- **Página del área Riesgo y regulación** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/areas/riesgo.html



Notas

SEVEN-G no trata el riesgo como un trámite de una sola vez. Lo trabaja en cada momento del ciclo de vida del caso de uso (fases 0 a 7) y en el ciclo corporativo (C1 a C5).

- Fase 0. El sistema se da de alta en el inventario y recibe una clasificación provisional. Se buscan los riesgos evidentes: práctica prohibida, datos protegidos o función crítica. Una práctica prohibida por el Reglamento Europeo de IA no se valora: se evita.
- Puerta de viabilidad (G3). Es la evaluación completa: riesgo inherente, controles planificados, residual objetivo y aceptación. La clasificación pasa a ser definitiva, con criterio jurídico cualificado.
- Puerta de diseño (G4). Cada riesgo Medio o superior tiene un control diseñado.
- Puerta de puesta en producción (G5). La eficacia de los controles se prueba y el residual pasa a verificado. La aceptación se ratifica.
- Revisión de continuidad (R6). Se revisan el registro, los indicadores de riesgo clave, los incidentes, los cambios y la clasificación.
- Puerta de escalado o retirada (G7). Se miran los riesgos acumulados y los de la retirada.

Quién decide. La aceptación del riesgo residual sigue una escala fija: Bajo, el responsable de producto de IA; Medio, el patrocinador de IA con la conformidad del responsable de riesgos de IA; Alto, el comité de IA, con plan de tratamiento y vigencia hasta la siguiente revisión de continuidad; Crítico, no se acepta: solo, por excepción, lo aprueba el consejo o su comisión delegada, dentro del apetito de riesgo aprobado. Nadie acepta un riesgo de un caso de uso que construye él mismo.

Una regla que conviene subrayar: la regla de impacto extremo. Un riesgo con impacto 5 en el eje de personas y derechos o en el regulatorio se trata como mínimo como Alto a efectos de aceptación, aunque su probabilidad sea 1. Así, un suceso raro pero inaceptable no lo acepta el responsable de producto.

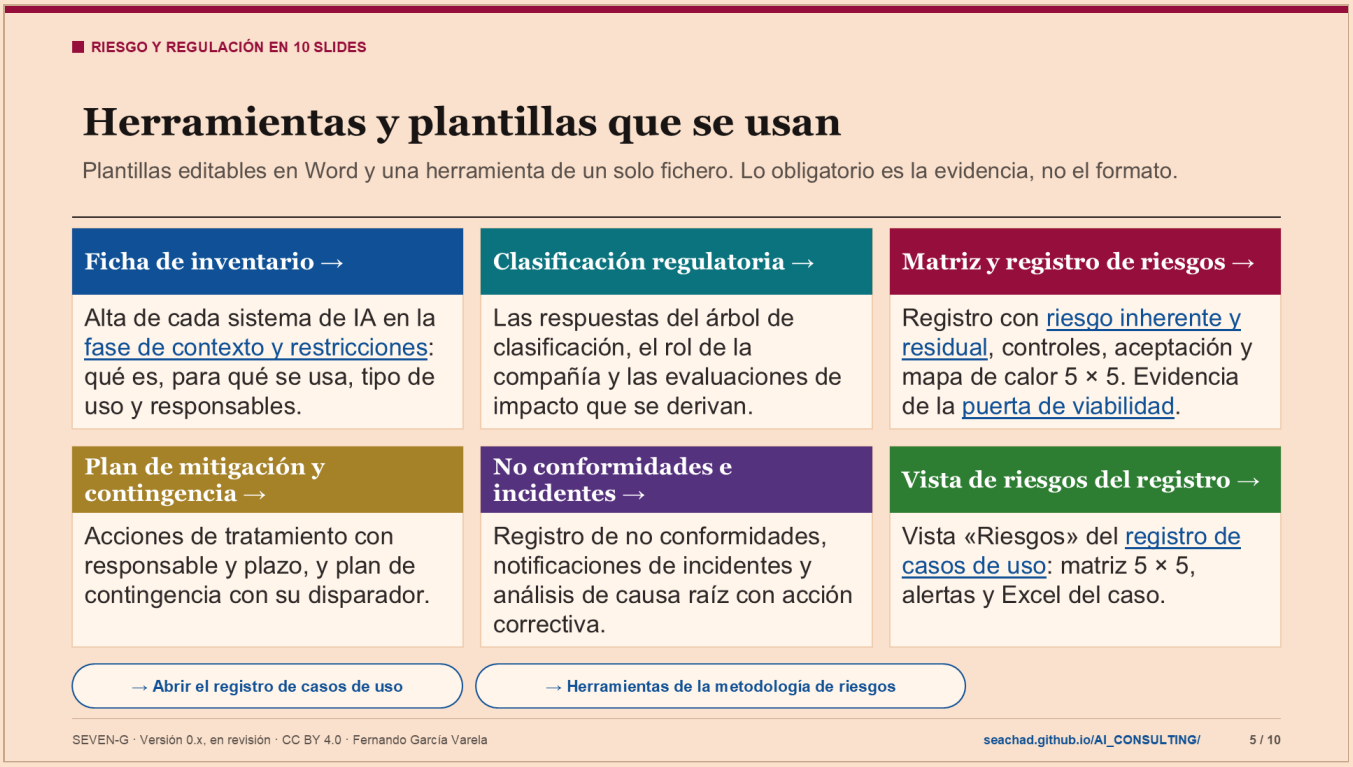
Pregunta para el aula: ¿por qué cree que SEVEN-G pide la clasificación definitiva en G3 y no al final, en G5?

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
- **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
- **Puerta de viabilidad** (G3): La puerta más importante: decide, con la prueba de viabilidad, la clasificación regulatoria y el registro de riesgos, si el caso merece el gran gasto de construirlo. Se decide siempre por separado, nunca agrupada con otras. Es la principal puerta de parada: parar aquí cuesta poco; después, mucho. El enlace abre sus criterios en el documento 21. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/21_SEVEN-G_Criterios_de_gate_y_auditoria.html#6-4-g3-viabilidad
- **Puesta en producción** (G5): Puerta que autoriza a usar el sistema de IA con usuarios, clientes o datos reales. Exige la validación y el piloto superados, el plan de reversión probado y la firma de varios niveles (negocio, tecnología, riesgos). Nada entra en producción sin esta firma. El enlace abre sus criterios en el documento 21. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/21_SEVEN-G_Criterios_de_gate_y_auditoria.html#6-6-g5-puesta-en-produccion

FUENTES Y ENLACES

- **Documento 33 §3.1 · El riesgo en el ciclo de vida del caso de uso** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html#3-1-en-el-ciclo-de-vida-del-caso-de-uso
- **Documento 33 §4.3 · Nivel de riesgo y matriz 5 × 5** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html#4-3-nivel-de-riesgo-y-matriz-5-5
- **Documento 33 §7.1 · Quién acepta el riesgo residual** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html#7-1-quien-acepta-el-riesgo-residual
- **Documento 32 §5.3 · Reglas de aplicación de la clasificación** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/32_SEVEN-G_Inventario_y_clasificacion_regulatoria.html#5-3-reglas-de-aplicacion
- **El riesgo en el ciclo de vida** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html#3-1-en-el-ciclo-de-vida-del-caso-de-uso
- **Quién acepta el riesgo** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html#7-1-quien-acepta-el-riesgo-residual
- **Reglas de clasificación** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/32_SEVEN-G_Inventario_y_clasificacion_regulatoria.html#5-3-reglas-de-aplicacion



Notas

Estas son las piezas de trabajo del área. Todas son abiertas y se pueden adaptar a la metodología propia de la compañía.

- Ficha de inventario del sistema de IA (P05). Es la evidencia del alta en la fase 0. Recoge una explicación comprensible del sistema, su tipo de uso y sus responsables con nombre.
- Clasificación regulatoria y evaluaciones de impacto (P11). Recoge, paso a paso, las respuestas al árbol de clasificación del documento 32, el rol de la compañía y qué evaluaciones se derivan. Cuando procede, se completan con la evaluación de impacto en protección de datos (P47) y la de derechos fundamentales (P48).
- Matriz y registro de riesgos (P12). Es el registro con los campos del documento 33: riesgo tipo del catálogo, probabilidad, impacto por eje, controles y su eficacia, residual objetivo y verificado, respuesta, aceptación y seguimiento. Es evidencia obligatoria de la puerta de viabilidad (G3).
- Plan de mitigación y contingencia (P13). Todo riesgo Alto o Crítico en tratamiento debe tener plan de contingencia: qué se hace si se materializa, quién lo activa y con qué disparador.
- No conformidades e incidentes (P50, P51 y P52). Registro de no conformidades, decisiones y notificaciones de incidentes, y hoja de análisis de causa raíz.
- Matriz y registro de riesgos (T06). Es la vista «Riesgos» del registro de casos de uso (T01). Calcula los niveles, dibuja la matriz 5 × 5 inherente y residual, avisa de aceptaciones caducadas o insuficientes y genera el Excel del caso con la matriz y propuestas de planes de mitigación y contingencia. Las propuestas son un punto de partida: no sustituyen la decisión del órgano competente.

Por qué importa: con una plantilla común, todos los casos de uso se valoran con la misma escala. Así el comité de IA y el consejo pueden comparar y sumar. SEVEN-G admite también una evidencia que la compañía ya tiene, si cubre lo que pide la plantilla.

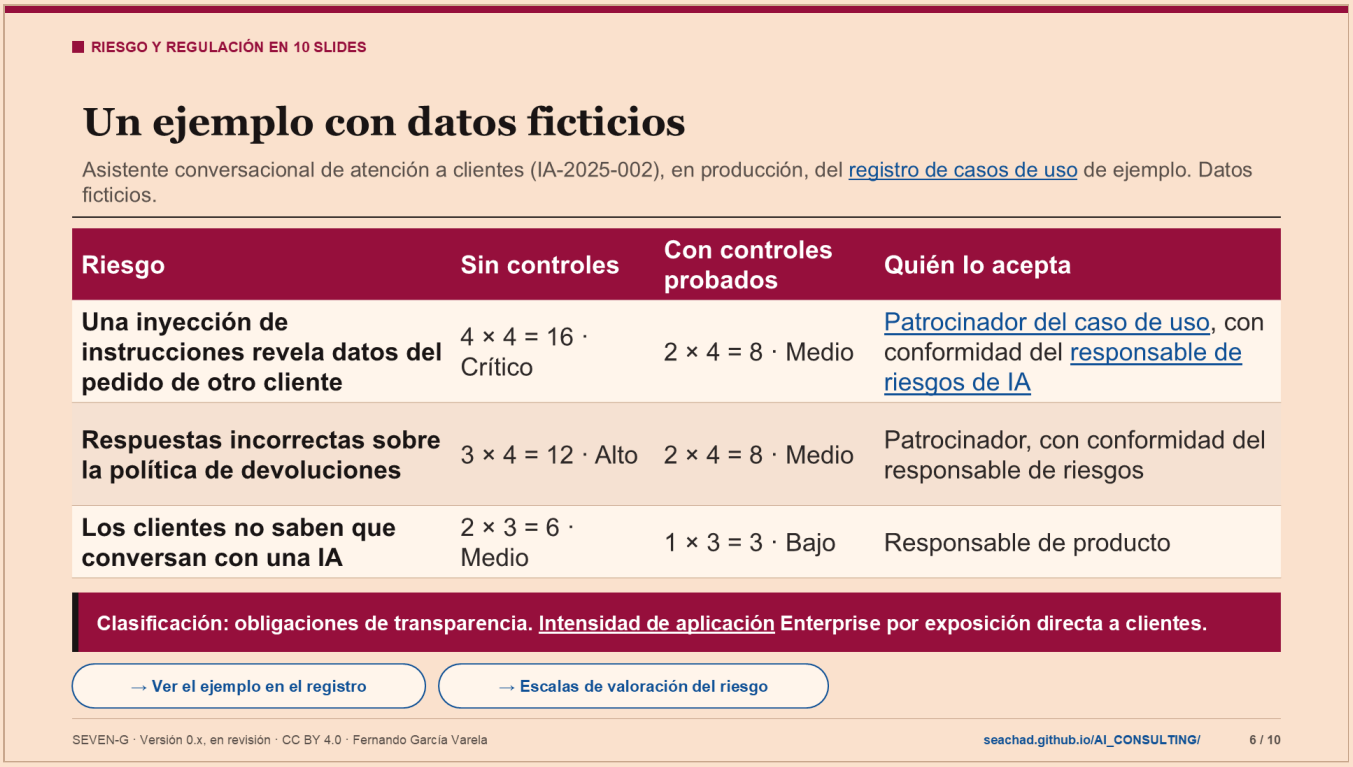
Pregunta para el aula: ¿qué ventaja tiene usar la misma escala de riesgos para la IA que el resto del marco corporativo de riesgos de la compañía?

TÉRMINOS DE ESTA SLIDE

- **Contexto y restricciones** (fase 0): Fase habilitante del ciclo de vida. Antes de hablar de valor, el caso de uso fija su contexto: patrocinador, roles, intensidad de gobierno, alta en el inventario y límites (datos, normas, presupuesto). La cierra la puerta de autorización (G0). Evita empezar un caso sin dueño ni reglas. 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_Manual es_de_fase.html#fase-0-contexto-y-restricciones
- **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
- **Puerta de viabilidad** (G3): La puerta más importante: decide, con la prueba de viabilidad, la clasificación regulatoria y el registro de riesgos, si el caso merece el gran gasto de construirlo. Se decide siempre por separado, nunca agrupada con otras. Es la principal puerta de parada: parar aquí cuesta poco; después, mucho. El enlace abre sus criterios en el documento 21. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/21_SEVEN-G_Criterios_de_gate_y_auditoria.html#6-4-g3-viabilidad
- **Registro de casos de uso** (T01): Es la herramienta central de SEVEN-G y la única fuente de datos del resto. Registra cada caso de uso de IA como una oportunidad en un CRM: fase, estado, fechas, criterios de cada puerta, riesgos, valor y motivo de parada. La usan la oficina de IA y los equipos; el comité y el consejo ven lo que sale de ella. Al abrir el enlace verá un registro de ejemplo con casos ficticios; lo que usted cambie se guarda solo en su navegador. https://seachad.github.io/AI_CONSULTING/SEVEN-G/herramientas/T01_registro_iniciativas/registro.html

FUENTES Y ENLACES

- **Documento 33 §13 · Herramientas y plantillas asociadas** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html#herramientas-y-plantillas-asociadas
- **Documento 32 §10 · Herramientas y plantillas asociadas** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/32_SEVEN-G_Inventario_y_clasificacion_regulatoria.html#herramientas-y-plantillas-asociadas
- **Plantilla P12 · Matriz y registro de riesgos** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/plantillas/P12_SEVEN-G_Matriz_y_registro_de_riesgos.html
- **Documento 37 §10 · Herramientas y plantillas asociadas** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/37_SEVEN-G_No_conformidades_e_incidentes.html#herramientas-y-plantillas-asociadas
- **Herramientas de la metodología de riesgos** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html#herramientas-y-plantillas-asociadas



RIESGO Y REGULACIÓN EN 10 SLIDES

Un ejemplo con datos ficticios

Asistente conversacional de atención a clientes (IA-2025-002), en producción, del registro de casos de uso de ejemplo. Datos ficticios.

Riesgo	Sin controles	Con controles probados	Quién lo acepta
Una inyección de instrucciones revela datos del pedido de otro cliente	4 × 4 = 16 · Crítico	2 × 4 = 8 · Medio	Patrocinador del caso de uso, con conformidad del responsable de riesgos de IA
Respuestas incorrectas sobre la política de devoluciones	3 × 4 = 12 · Alto	2 × 4 = 8 · Medio	Patrocinador, con conformidad del responsable de riesgos
Los clientes no saben que conversan con una IA	2 × 3 = 6 · Medio	1 × 3 = 3 · Bajo	Responsable de producto

Clasificación: obligaciones de transparencia. Intensidad de aplicación Enterprise por exposición directa a clientes.

→ Ver el ejemplo en el registro → Escalas de valoración del riesgo

SEVEN-G · Versión 0.x, en revisión · CC BY 4.0 · Fernando García Varela seachad.github.io/AI_CONSULTING/ 6 / 10

Notas

Este ejemplo sale del registro de casos de uso de ejemplo del sitio (T01). La compañía y todos los datos son ficticios.

El sistema es un asistente de IA generativa en la web y la aplicación que responde dudas de clientes sobre pedidos y devoluciones y deriva a una persona cuando no puede resolver. Está en producción (fase 6).

Su clasificación regulatoria es «obligaciones de transparencia»: las personas conversan con un sistema de IA y deben saberlo. No es de alto riesgo. Aun así, va con intensidad Enterprise, porque tiene exposición directa a clientes, que es uno de los criterios Enterprise. La evaluación de impacto en protección de datos está hecha; la de derechos fundamentales no aplica.

Cómo se leen las tres filas:

- Inyección de instrucciones. Un cliente escribe un mensaje que manipula al asistente para que revele datos de otro cliente. El eje determinante es personas y derechos. Sin controles es probable (4) y grave (4): 16, Crítico. Los controles son el aislamiento de la sesión por cliente, un filtro de salida de datos personales y pruebas adversarias antes de G5 sin fugas. Como son eficaces y están probados, bajan la probabilidad dos niveles: 2 × 4 = 8, Medio.
- Respuestas incorrectas. El eje determinante es el reputacional. Los controles son respuestas basadas en una base documental y la derivación a una persona. Pasa de Alto a Medio.
- Transparencia. El eje determinante es el regulatorio. El control es un aviso al inicio de cada conversación y en la interfaz. Pasa de Medio a Bajo.

Fíjese en dos cosas. Primero, el impacto no baja en las dos primeras filas: los controles reducen sobre todo la probabilidad. Segundo, quién acepta depende del nivel residual: Medio lo acepta el patrocinador de IA con la conformidad del responsable de riesgos de IA; Bajo, el responsable de producto.

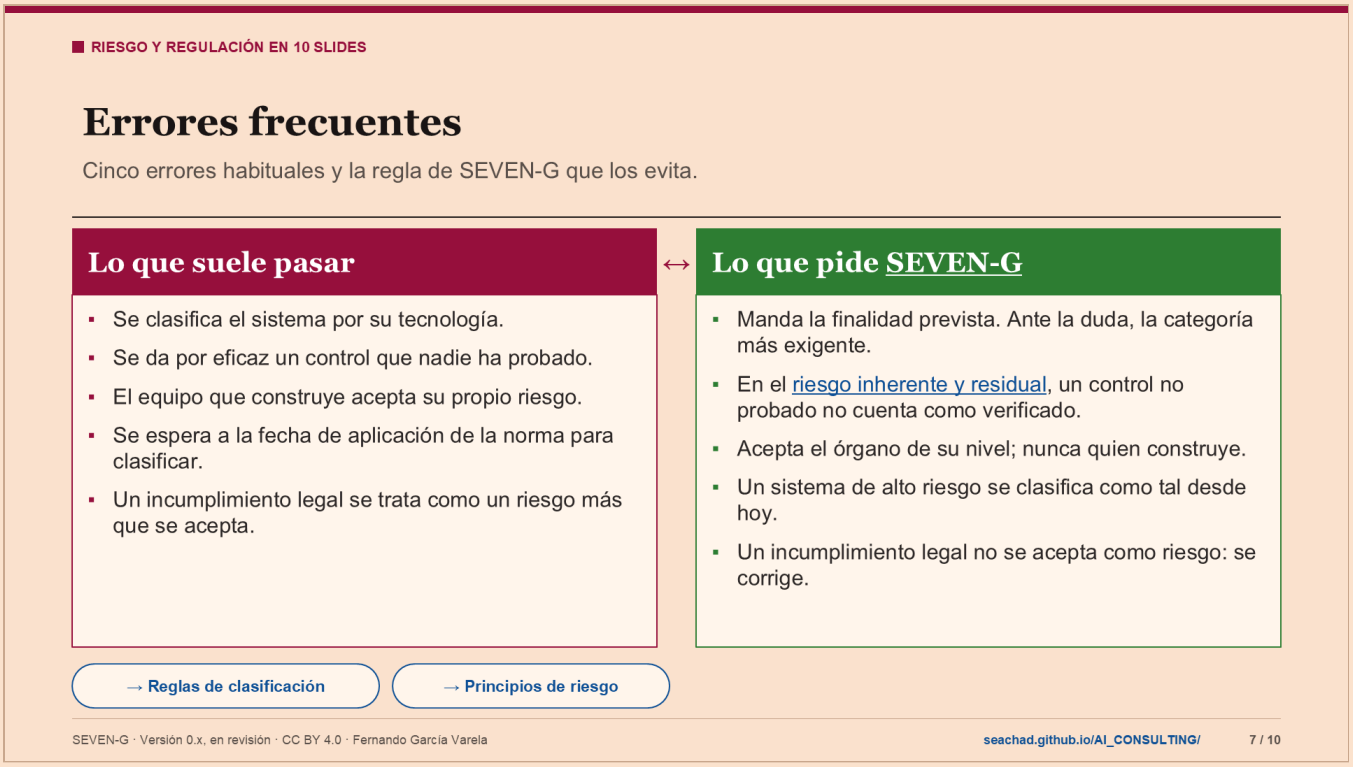
Pregunta para el aula: si mañana una prueba adversaria lograra una fuga, ¿qué pasaría con la eficacia del control, con el residual verificado y con la aceptación?

TÉRMINOS DE ESTA SLIDE

- **Registro de casos de uso** (T01): Es la herramienta central de SEVEN-G y la única fuente de datos del resto. Registra cada caso de uso de IA como una oportunidad en un CRM: fase, estado, fechas, criterios de cada puerta, riesgos, valor y motivo de parada. La usan la oficina de IA y los equipos; el comité y el consejo ven lo que sale de ella. Al abrir el enlace verá un registro de ejemplo con casos ficticios; lo que usted cambie se guarda solo en su navegador. https://seachad.github.io/AI_CONSULTING/SEVEN-G/herramientas/T01_registro_iniciativas/registro.html
- **Patrocinador del caso de uso**: La persona de negocio que pide el caso de uso, responde de su valor y defiende su presupuesto. Sin patrocinador, el caso no pasa la puerta de autorización. No puede verificar ni auditar su propio caso. Importa porque la IA sin dueño de negocio se queda en piloto. 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
- **Responsable de riesgos de IA**: Función de segunda línea que revisa los riesgos, la clasificación regulatoria y los proveedores de cada caso de uso, y confirma la intensidad. Es independiente de quien construye: no puede verificar lo que ha elaborado. Su papel evita que el equipo que quiere lanzar el caso valore solo sus riesgos. El enlace abre las incompatibilidades entre roles en el documento 01. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/01_SEVEN-G_Metodologia_fundacional.html#8-2-incompatibilidades
- **Intensidad de aplicación**: Cuánto gobierno necesita cada caso de uso: Express, Lite o Enterprise. Se decide por caso, no por compañía. Las puertas son siempre las mismas; cambian cuántos criterios se evalúan, qué sesiones se agrupan y quién verifica. Hace el marco proporcionado: un asistente interno no carga lo mismo que un agente que decide sobre clientes. El enlace abre la definición en el documento 01. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/01_SEVEN-G_Metodologia_fundacional.html#intensidad-de-aplicacion-express-lite-y-enterprise

FUENTES Y ENLACES

- **Documento 33 §4.3 · Nivel de riesgo y matriz 5 × 5** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html#4-3-nivel-de-riesgo-y-matriz-5-5
- **Documento 33 §5.3 · Eficacia de los controles** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html#5-3-eficacia-de-los-controles
- **Documento 32 §5.4 · Ejemplos ilustrativos de clasificación** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/32_SEVEN-G_Inventario_y_clasificacion_regulatoria.html#5-4-ejemplos-ilustrativos
- **Escalas de valoración del riesgo** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html#escalas-de-valoracion



Notas

Cada error de la izquierda tiene una regla escrita en los documentos 32 y 33 que lo evita.

- Clasificar por la tecnología. Un mismo modelo de lenguaje puede servir para resumir documentos internos o para filtrar candidaturas en un proceso de selección. Lo primero suele ser riesgo mínimo; lo segundo, alto riesgo. Por eso manda la finalidad prevista y el uso razonablemente previsible. Ante la duda, se aplica la categoría más exigente mientras se resuelve, con fecha límite.
- Dar por eficaz un control no probado. Una política escrita o una instrucción al modelo no es por sí sola un control eficaz frente a la inyección de instrucciones: hay que probarla con pruebas adversarias. Un control no probado puede usarse en el residual objetivo, pero no en el verificado.
- Que el equipo acepte su propio riesgo. Es un conflicto de interés. SEVEN-G separa funciones: nadie acepta un riesgo de un caso de uso que construye él mismo.
- Esperar a la fecha de aplicación. Según el documento 34, a la fecha de consulta, las obligaciones de los sistemas de alto riesgo del anexo III se aplican desde el 2-12-2027. SEVEN-G pide clasificarlos como tales desde hoy, para que el diseño incorpore los requisitos a tiempo y no haya que rehacer sistemas con prisa.
- Aceptar un incumplimiento legal. La aceptación sirve para riesgos dentro del apetito. Un incumplimiento de la ley no es un riesgo que se acepta: se corrige.

Hay un sexto error que conviene comentar en el aula: no buscar los sistemas que nadie ha declarado. El documento 32 pide conciliar el inventario, al menos cada trimestre, con fuentes independientes: compras, facturas de nube, repositorios de código y notas de gasto.

Pregunta para el aula: ¿cuál de estos errores ha visto en su organización, y qué lo hizo posible?

TÉRMINOS DE ESTA SLIDE

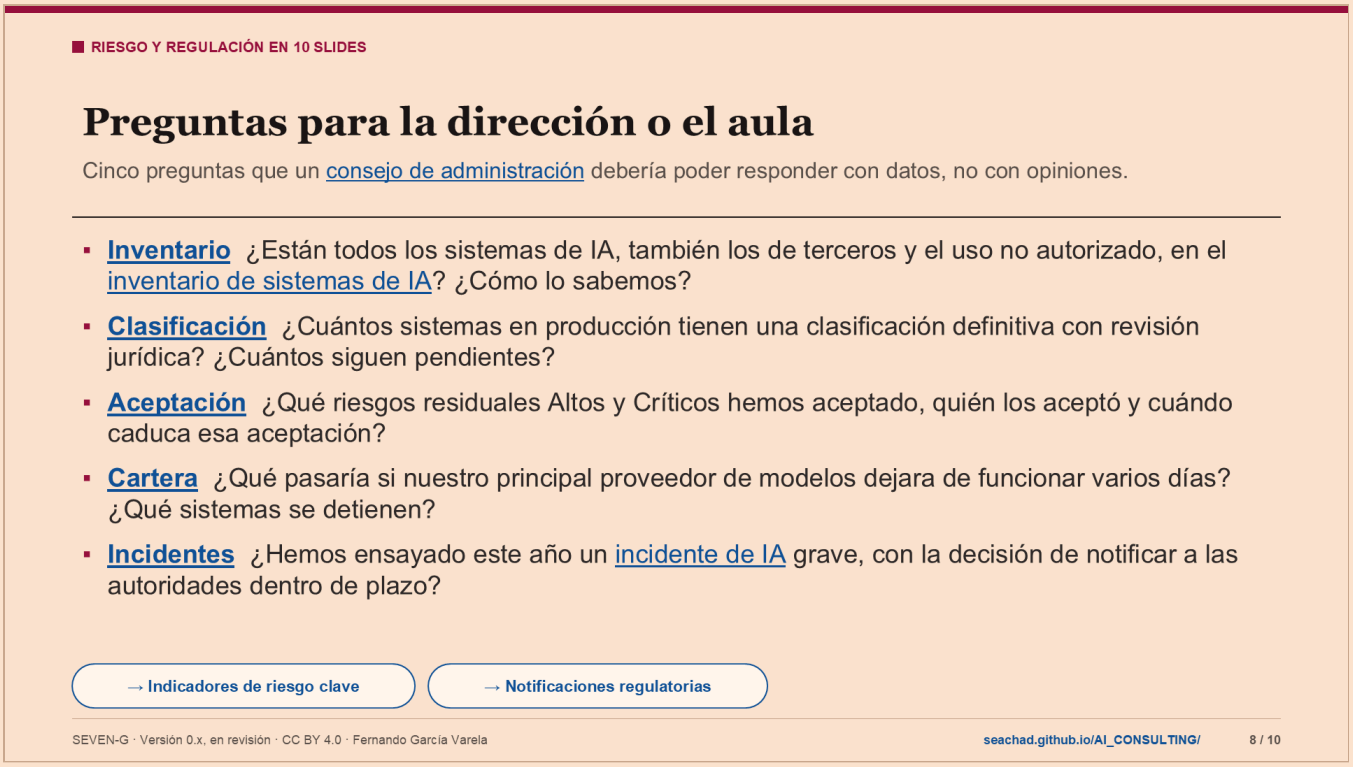
- **SEVEN-G**: SEVEN-G (Seven-phase Enterprise Value & Governance) es un marco abierto para que una compañía implante, gobierne y mida la IA, y sepa si se transforma o solo gana eficiencia. Trata cada caso de uso como una

inversión con puertas de decisión y da al consejo cifras que puede creerse. Lo usan la dirección, la oficina de IA, riesgos y el consejo. El enlace abre su página de entrada, con la historia, las preguntas y los ejemplos. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/entrada/index.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

FUENTES Y ENLACES

- **Documento 32 §5.3 · Reglas de aplicación de la clasificación** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/32_SEVEN-G_Inventario_y_clasificacion_regulatoria.html#5-3-reglas-de-aplicacion
- **Documento 32 §9 · Detección de sistemas no inventariados** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/32_SEVEN-G_Inventario_y_clasificacion_regulatoria.html#deteccion-de-sistemas-no-inventariados
- **Documento 33 §5.3 · Eficacia de los controles** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html#5-3-eficacia-de-los-controles
- **Documento 34 §3.1 · Calendario de aplicación verificado** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/34_SEVEN-G_Mapeo_regulatorio.html#3-1-calendario-de-aplicacion-verificado
- **Reglamento (UE) 2026/1744 (ómnibus digital sobre IA), EUR-Lex** https://eur-lex.europa.eu/eli/reg/2026/1744/oj/spa
- **Reglas de clasificación** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/32_SEVEN-G_Inventario_y_clasificacion_regulatoria.html#5-3-reglas-de-aplicacion
- **Principios de riesgo** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html#principios



Notas

Estas preguntas sirven para una sesión de consejo o de comité, y también para un debate en el aula con un caso real o ficticio. Cada una tiene detrás un indicador o una regla del marco.

- Inventario. El documento 32 mide la cobertura del inventario: los sistemas que aparecen en fuentes externas al inventario y no estaban registrados. Su objetivo orientativo es quedar por debajo del 5 %, con tendencia decreciente.
- Clasificación. El indicador «clasificación definitiva con revisión jurídica» tiene un objetivo del 100 % de los sistemas en producción. Un sistema en producción sin ficha completa y clasificación definitiva es una no conformidad mayor; si además es de alto riesgo o prohibido, crítica.
- Aceptación. Los indicadores de riesgo clave del documento 33 incluyen los residuales Críticos (cero sin aprobación del consejo), los residuales Altos y las aceptaciones caducadas (cero).
- Cartera. Los riesgos de los casos de uso no se suman: interactúan. El documento 33 recomienda escenarios de cartera, como la indisponibilidad del principal proveedor de modelos durante varios días o un cambio de comportamiento de un modelo base que usan varios sistemas.
- Incidentes. Un mismo incidente puede activar varios regímenes de notificación a la vez. El documento 37 los resume, por ejemplo el del Reglamento Europeo de IA para incidentes graves o el del RGPD para brechas de datos personales, y pide ensayar las notificaciones al menos una vez al año en un simulacro de incidente S1. Antes de aplicarlos, cada organización verifica los plazos vigentes con su asesoría jurídica.

Los umbrales de los indicadores son orientativos. Cada compañía los aprueba en la etapa de dirección (C2) y los recalibra en la revisión anual (C5).

Ejercicio para el aula: elija una de las cinco preguntas y diga qué dato necesitaría para responderla, quién lo tiene y con qué frecuencia debería llegar al consejo.

TÉRMINOS DE ESTA SLIDE

- **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
- **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
- **Incidente de IA y su severidad** (S1–S4): Un hecho en que un sistema de IA causa o puede causar daño: error grave, sesgo, fuga de datos, acción indebida de un agente. Se clasifica de S1 (el más grave) a S4. Los S1 y S2 llegan al consejo por la vía rápida y pueden exigir notificar a autoridades (P51). El enlace abre la escala de severidad en el documento 37. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/37_SEVEN-G_No_conformidades_e_incidentes.html#4-2-severidad

FUENTES Y ENLACES

- **Documento 32 §8.1 · Indicadores de calidad del inventario** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/32_SEVEN-G_Inventario_y_clasificacion_regulatoria.html#8-1-indicadores
- **Documento 33 §10 · Riesgo de cartera** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html#riesgo-de-cartera
- **Documento 33 §11.2 · Indicadores de riesgo clave** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html#11-2-indicadores-de-riesgo-clave
- **Documento 37 §5 · Notificaciones regulatorias** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/37_SEVEN-G_No_conformidades_e_incidentes.html#notificaciones-regulatorias
- **Reglamento (UE) 2016/679 (RGPD), EUR-Lex** https://eur-lex.europa.eu/eli/reg/2016/679/oj/spa
- **Indicadores de riesgo clave** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html#11-2-indicadores-de-riesgo-clave
- **Notificaciones regulatorias** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/37_SEVEN-G_No_conformidades_e_incidentes.html#notificaciones-regulatorias



Notas

El área de riesgo y regulación se conecta con otras áreas de SEVEN-G y con SPHERES.

- Riesgo, seguridad y agentes. El documento 35 define los controles de seguridad y de agentes, con código. En la puerta de diseño (G4), cada riesgo Medio o superior tiene un control diseñado, con su código cuando existe. En IA generativa y agentes, la eficacia frente a la inyección de instrucciones debe probarse con pruebas adversarias.
- Gobierno y decisiones. La escala de aceptación usa los órganos del marco: responsable de producto, patrocinador, comité de IA y consejo. La regla de que quien construye no acepta su propio riesgo viene de la separación de funciones.
- Normas y estándares. La metodología de riesgos es coherente con ISO/IEC 23894, con los requisitos de riesgo de ISO/IEC 42001 y con las funciones Map, Measure y Manage del NIST AI RMF. No sustituye el marco corporativo de riesgos de la compañía: lo especializa para la IA y se integra en él.
- SPHERES, esfera 08. SPHERES es la capa explicativa de las nueve esferas. La esfera 08, Regulación, ética y responsabilidad, mira tres dimensiones: cumplimiento (hoy), anticipación (mañana) y liderazgo ético (más allá de la ley). Regla de uso en el mapa: la esfera 08 nunca se usa para señalar que un caso de uso de otra esfera tiene riesgo regulatorio; eso va en su clasificación y en su registro de riesgos.
- Construcción de la solución, seguridad. El documento 53 de SEVEN-G pide análisis de seguridad, de secretos y de dependencias sobre el código generado con IA antes de la puerta de puesta en producción (G5). Un hallazgo crítico o alto bloquea G5, salvo aceptación formal del riesgo con la escala del documento 33. En los controles críticos de seguridad no se admite continuar con condiciones.

Por qué importa: un mismo riesgo se mira desde el negocio (SPHERES), desde el gobierno y la medición (SEVEN-G) y desde la construcción de la solución (documento 53), con el mismo lenguaje.

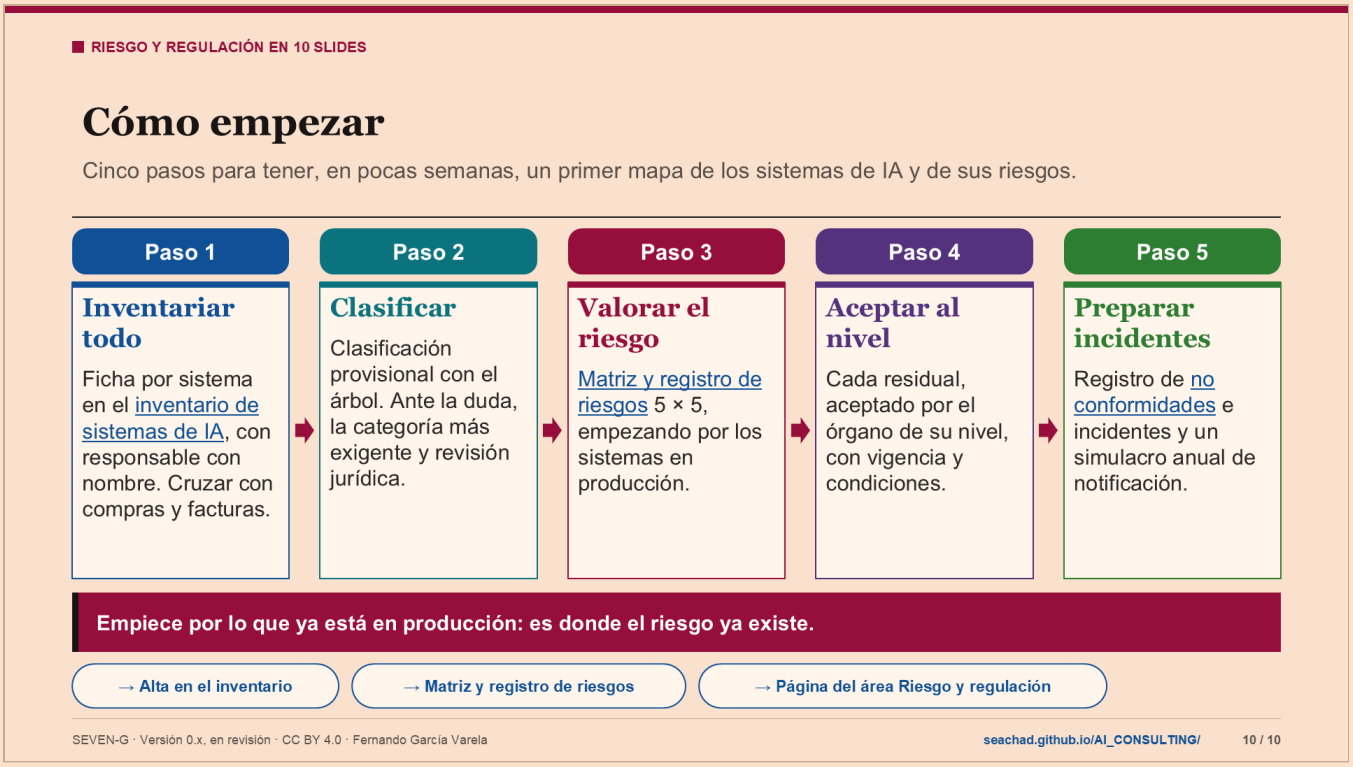
Pregunta para el aula: ¿quién debería poder vetar un uso legal de la IA que la compañía considera inaceptable?

TÉRMINOS DE ESTA SLIDE

- **Pruebas adversarias** (P53): Pruebas en que un equipo intenta engañar o romper un sistema de IA como lo haría un atacante: inyección de instrucciones, fuga de datos, abuso de herramientas de un agente. Un escenario crítico superado por el atacante impide desplegar. Se planifican e informan con la plantilla P53. El enlace abre la plantilla. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/plantillas/P53_SEVEN-G_Plan_e_informe_de_pruebas_adversarias.html
- **Separación de funciones**: Principio por el que quien construye no controla y nadie se aprueba a sí mismo: quien aporta las evidencias no las verifica ni decide, y los roles incompatibles no recaen en la misma persona. Es una de las reglas del núcleo que nunca se rebajan. Da al consejo la seguridad de que una cifra o un control no los firma solo quien los defiende. El enlace abre los roles y las incompatibilidades en el documento 01. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/01_SEVEN-G_Metodologia_fundacional.html#roles-organos-y-separacion-de-funciones
- **SPHERES**: Metodología que explica dónde puede crear valor la IA en una compañía y con qué ambición, con tres preguntas: ¿dónde jugamos?, ¿con qué ambición? y ¿qué preguntamos? Es la capa explicativa de las esferas y los niveles de ambición; las reglas operativas están en SEVEN-G. Sirve para conversar con la dirección y el consejo. El enlace abre su documento de presentación. https://seachad.github.io/AI_CONSULTING/SPHERES/html/es/00_SPHERES_Que_es_y_para_que_sirve.html#que-es-spheres
- **Puesta en producción** (G5): Puerta que autoriza a usar el sistema de IA con usuarios, clientes o datos reales. Exige la validación y el piloto superados, el plan de reversión probado y la firma de varios niveles (negocio, tecnología, riesgos). Nada entra en producción sin esta firma. El enlace abre sus criterios en el documento 21. https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/21_SEVEN-G_Criterios_de_gate_y_auditoria.html#6-6-g5-puesta-en-produccion

FUENTES Y ENLACES

- **SPHERES 04 · Esfera 08, Regulación, ética y responsabilidad** https://seachad.github.io/AI_CONSULTING/SPHERES/html/es/04_SPHERES_Regulacion_y_gobierno_de_la_IA.html#esfera-08-regulacion-etica-y-responsabilidad
- **Documento 53, sección 7.4 · Seguridad** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/53_SEVEN-G_Construccion_de_soluciones_con_IA.html#7-4-seguridad
- **Documento 33 §1.3 · Normas de referencia** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html#1-3-normas-de-referencia
- **ISO/IEC 23894:2023 · Orientación sobre la gestión del riesgo de la IA** https://www.iso.org/standard/77304.html
- **NIST AI RMF 1.0 · Marco de gestión de riesgos de IA** https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-ai-rmf-10
- **Qué es SPHERES** https://seachad.github.io/AI_CONSULTING/SPHERES/html/es/00_SPHERES_Que_es_y_para_que_sirve.html
- **Construcción de soluciones con IA** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/53_SEVEN-G_Construccion_de_soluciones_con_IA.html
- **Página del área Riesgo y regulación** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/areas/riesgo.html



Notas

Estos cinco pasos ordenan lo que piden los documentos 32, 33 y 37 para una compañía que empieza.

- Paso 1. Inventariar todo. El documento 32 da plazos de referencia: el alta, en 5 días hábiles desde que se identifica el sistema; la clasificación provisional, en 10 días hábiles desde el alta. Cada sistema lleva un responsable con nombre, no un área. Para encontrar lo que nadie ha declarado, se concilia el inventario con compras y contratos, facturas de nube, repositorios de código y notas de gasto. Plantilla: ficha de inventario (P05).
- Paso 2. Clasificar. El árbol de clasificación recorre siete preguntas: si es un sistema de IA, si hay una exclusión, si es una práctica prohibida, si es de alto riesgo por el anexo I o por el anexo III, si aplica la excepción del artículo 6.3 y si hay obligaciones de transparencia. Después se fija el rol de la compañía y las evaluaciones que se derivan. Plantilla: P11. La clasificación definitiva requiere criterio jurídico cualificado.
- Paso 3. Valorar el riesgo. Se empieza por los sistemas en producción, que son los que ya pueden causar daño. Cada riesgo se describe como causa, evento y consecuencia, se valora con la matriz 5 × 5 y tiene un responsable con nombre. Plantilla: P12; herramienta: la vista de riesgos del registro (T06).
- Paso 4. Aceptar al nivel. Cada riesgo residual lo acepta el órgano de su nivel, con vigencia y condiciones. Un incumplimiento legal no se acepta: se corrige.
- Paso 5. Preparar incidentes. Se abre el registro de no conformidades e incidentes (P50) y se ensayan las notificaciones al menos una vez al año en un simulacro de incidente S1 (P51).

Los plazos y umbrales son de referencia: cada compañía los fija en la etapa de dirección (C2). Y, de nuevo, SEVEN-G es una ayuda, no asesoramiento jurídico: cada organización verifica la normativa que le aplica.

Para seguir, abra la página del área. Desde ella se llega a los documentos 32, 33, 34 y 37 y a la plantilla P12.

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
- **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
- **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

- **Documento 32 §7.1 · Procedimiento de alta en el inventario** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/32_SEVEN-G_Inventario_y_clasificacion_regulatoria.html#7-1-alta
- **Documento 32 §5 · Árbol de clasificación regulatoria** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/32_SEVEN-G_Inventario_y_clasificacion_regulatoria.html#arbol-de-clasificacion-regulatoria
- **Documento 33 §8 · Registro de riesgos** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/33_SEVEN-G_Metodologia_de_riesgos_de_IA.html#registro-de-riesgos
- **Documento 37 §3.10 · Plazos de las no conformidades** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/37_SEVEN-G_No_conformidades_e_incidentes.html#3-10-plazos
- **Página del área Riesgo y regulación** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/areas/riesgo.html
- **Alta en el inventario** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/32_SEVEN-G_Inventario_y_clasificacion_regulatoria.html#7-1-alta
- **Matriz y registro de riesgos** https://seachad.github.io/AI_CONSULTING/SEVEN-G/html/es/plantillas/P12_SEVEN-G_Matriz_y_registro_de_riesgos.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/