Riesgo y regulación

Qué riesgo se asume y qué norma aplica a cada sistema.

> *«Un riesgo que nadie ha aceptado por escrito no está bajo control. Cada riesgo tiene dueño, se valora antes de invertir y quien construye nunca acepta su propio riesgo.»*

QUÉ ES

Inventario y clasificación

No se gobierna lo que no se conoce. El inventario recoge la IA propia, la contratada, la incluida en productos de terceros y el uso no autorizado. Cada sistema se clasifica según el Reglamento Europeo de IA, con criterio jurídico antes de la puerta de viabilidad. Ante la duda, la categoría más exigente.

Implicación: ¿Sabe su compañía qué IA llega dentro del software que ya compra?

Riesgo: Un sistema sin clasificar puede ser de alto riesgo, o estar prohibido, sin que nadie lo sepa.

QUÉ PROPONE

Riesgo con dueño y aceptación

Cada riesgo se valora por probabilidad e impacto, con el peor de cinco ejes de impacto, sin promediar. Lo acepta el órgano que corresponde a su nivel. Un riesgo crítico bloquea la viabilidad salvo que lo acepte el consejo dentro de su apetito. Un incumplimiento legal no se acepta: se corrige.

Implicación: ¿Quién aceptó por escrito los riesgos altos que hoy están en producción?

Riesgo: Sin órgano que acepte, el riesgo lo asume quien construye y nadie responde de él.

CÓMO SE COMPRUEBA

Controles probados e incidentes

Un control sin probar no reduce el riesgo: el residual se verifica antes de la puesta en uso. Las no conformidades las cierra el auditor de IA. En un incidente, primero se contiene; los plazos de notificación cuentan desde que la compañía lo conoce. Omitir una notificación es una no conformidad crítica.

Implicación: ¿Ha hecho su compañía un simulacro de incidente grave de IA en el último año?

Riesgo: Sin protocolo de incidentes, se pierden los plazos de notificación al regulador.

CUATRO PREGUNTAS PARA EL CONSEJO

1. **¿Tenemos inventariada toda la IA, también la de terceros?**
   Inventario completo, conciliado cada trimestre con compras y facturación de la nube. Un sistema en producción que no ha pasado las puertas es una no conformidad crítica.

2. **¿Qué sistemas son de alto riesgo según el Reglamento de IA?**
   Clasificación sistema a sistema, con criterio jurídico. Las fechas de aplicación de la norma no retrasan la clasificación.

3. **¿Qué riesgos altos o críticos hemos aceptado, y quién?**
   Registro de riesgos con dueño, residual verificado, órgano que aceptó y fecha de revisión. Un cambio en el sistema hace caducar la aceptación.

4. **¿Estamos preparados para un incidente grave?**
   Protocolo con severidades, plazos de notificación por norma, simulacro anual y aviso al consejo en 24 horas ante un incidente de la máxima gravedad.

QUÉ FALLA SI NO SE GOBIERNA

QUÉ FALLA	NIVEL	QUÉ HACER
IA de terceros en uso que nadie ha clasificado	ALTO	Conciliar el inventario con compras y nube
Riesgos críticos en producción sin aceptación	ALTO	Llevar cada riesgo crítico al órgano que corresponde
Controles que constan pero no se han probado	ALTO	Verificar el riesgo residual antes de la puesta en uso
Notificación al regulador fuera de plazo	ALTO	Fijar el protocolo de incidentes y sus plazos
Riesgo concentrado en un proveedor o un modelo	MEDIO	Revisar la concentración del riesgo en la cartera
Aceptaciones de riesgo caducadas tras un cambio	MEDIO	Revisar las aceptaciones tras cada cambio relevante

PARA SEGUIR LEYENDO

Metodología de riesgos de IA
Documento 33 · matriz, aceptación y riesgos tipo

Matriz y registro de riesgos
Plantilla editable

Inventario y clasificación regulatoria
Documento 32 · qué IA hay y qué norma aplica

ISO/IEC 23894 · Gestión del riesgo de la IA
ISO/IEC (JTC 1/SC 42) · 06-02-2023

Fernando García Varela · CC BY 4.0 · Versión 0.x, en revisión

Ayuda genérica y gratuita, sin revisión jurídica para ningún caso concreto: cada organización la adapta, identifica la normativa que le aplica y responde de su cumplimiento. No es asesoramiento ni certificación. En la máxima medida permitida por la ley, el autor no asume responsabilidad por los efectos de su aplicación.