

## PREGUNTA CLAVE

**¿Tenemos una lista honesta de los 10 riesgos reales de cómo usamos IA hoy, con dueño y mitigación para los 5 mayores?**

## POR QUÉ IMPORTA

El riesgo real —el junior subiendo la base de clientes a una herramienta gratuita— no figura en las matrices heredadas de papers. Y el mapa debe incluir el riesgo de no adoptar.

## LOS CUATRO NIVELES

## N1

Sin mapa de riesgos de IA: los incidentes se descubren cuando ocurren.

## N2

Riesgos principales identificados y listados, sin dueños ni mitigación.

## N3

Riesgos gestionados: matriz viva con dueños, mitigaciones concretas (revisión humana en decisiones sensibles, cláusulas de PI, alternativas de proveedor) y plan de respuesta a incidentes.

## N4

Gestión integrada al negocio: apetito de riesgo definido por la dirección, revisión periódica, simulacros; marco alineable con ISO/IEC 42001.

## CÓMO SUBIR UN NIVEL

| Transición     | Acción                                                                                                                                                                                                                                       | Tiempo (est.) | Quién                       | Evidencia de hecho                                                  |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|-----------------------------|---------------------------------------------------------------------|
| <b>N1 → N2</b> | Taller de 2 horas con las cabezas técnicas y de negocio: listar los 10 riesgos reales de cómo se usa IA hoy.                                                                                                                                 | 1 taller      | Dirección + CTO + seguridad | Lista de 10 riesgos priorizada.                                     |
| <b>N2 → N3</b> | Para los 5 riesgos de mayor exposición: dueño, mitigación y disparador de escalamiento; definir qué es un 'incidente de IA' y qué se hace cuando ocurre; incluir la propiedad intelectual del conocimiento capturado (propio y del cliente). | 1 trimestre   | Dueños de riesgo + legales  | Matriz viva; plan de respuesta a incidentes publicado; PI incluida. |
| <b>N3 → N4</b> | Llevar el apetito de riesgo a la dirección (qué delegamos en IA y qué no) y revisarlo como el riesgo financiero; evaluar alinear el sistema con ISO/IEC 42001 (conocer, cumplir, después certificar).                                        | 2 trimestres  | Dirección                   | Apetito de riesgo aprobado; revisión semestral registrada.          |

## QUÉ MEDIR

Riesgos con dueño y mitigación sobre el total identificado · Incidentes de IA detectados y tiempo de respuesta · Antigüedad de la última revisión de la matriz

**Tablero:** Se lee con M5 y M8.

## VARIANTES POR PERFIL

**PyME (≈30).** La matriz de una página con 5 riesgos gestionados es N3 legítimo.

**Empresa grande (≈500).** Integrar al ERM existente en lugar de crear una burocracia paralela.

## ANTI-PATRÓN

*El riesgo teórico: sesgo algorítmico en un equipo que hace CRUD, mientras el riesgo real no figura.*

## EN QUÉ SE APOYA

Agrawal et al., Prediction Machines (el juicio incluye el costo de cada tipo de error: la matriz lo hace explícito) · Abbosh, Nunes & Downes (el riesgo mayor del incumbente es no liberar el valor atrapado a tiempo).

**Ver también:** G.2 · G.3 · 4.4