thinkia

GOBIERNO Y RIESGO · ERA DE LA INTELIGENCIA 2026

Shadow *AI*.

El riesgo invisible no es que tus empleados usen IA. Es que la usan sin que tú lo veas. No es un problema de prohibición: es de gobierno.

CARTA DEL AUTOR

La IA ya entró por la puerta de atrás. La pregunta es *quién la gobierna.*

Cuando un comité de dirección me pregunta cuándo empezará su empresa a usar inteligencia artificial, mi respuesta suele incomodar: ya la usa, todos los días, y casi nadie en la sala lo sabe con precisión. La adopción no esperó a la estrategia. Llegó de abajo arriba, en pestañas de navegador y conversaciones privadas con modelos que viven fuera del perímetro corporativo. A eso lo llamamos Shadow AI, y es la versión acelerada de un viejo conocido: la shadow IT.

La diferencia es de velocidad y de superficie. La shadow IT exigía instalar algo; la Shadow AI solo exige una cuenta gratuita y una idea de cómo ahorrar media hora. Por eso se extiende más rápido y deja menos rastro. Y por eso el reflejo de prohibirla, comprensible, es también el más contraproducente: lo prohibido no desaparece, se vuelve invisible.

Este documento no busca alarmar. Busca reencuadrar. La Shadow AI no es un fallo moral de los empleados ni una brecha que tapar con una circular. Es la señal de que el valor llegó antes que el control, y de que el trabajo del responsable ya no es impedir, sino gobernar: ver lo que ocurre, dar la herramienta buena y poner los límites correctos. De eso trata lo que sigue.

David Alejano

Chief Strategy Officer · Thinkia · Madrid, junio de 2026

linkedin.com/in/dalejano

RESUMEN EJECUTIVO

Shadow AI es el uso de inteligencia artificial por parte de empleados al margen de la supervisión de IT. No es una hipótesis de futuro: ya ocurre en la mayoría de las organizaciones. Aproximadamente tres de cada cuatro profesionales del conocimiento usan IA en su trabajo, con frecuencia con herramientas y datos que nadie ha aprobado.

La tesis de este documento es directa: el riesgo invisible no es que tus empleados usen IA, sino que la usan sin que tú lo veas, y eso no se resuelve prohibiendo. Lo que no se gobierna, no se controla; y lo que no se controla, expone.

Estas páginas diagnostican el fenómeno, inventarían sus riesgos reales, explican por qué prohibir lo agrava y proponen un marco de gobierno en tres movimientos: visibilizar, gobernar y habilitar. El objetivo no es frenar la adopción, sino convertirla de pasivo silencioso en capacidad gobernada.

75%

EMPLEADOS DEL CONOCIMIENTO

ya usan IA en el trabajo, a menudo sin supervisión de IT.

3

MOVIMIENTOS DE GOBIERNO

visibilizar, gobernar y habilitar, en ese orden.

0

INSTALACIONES NECESARIAS

basta una cuenta gratuita para que el dato salga del perímetro.

CONTENIDOS

En estas páginas.

Sección 01

Qué es Shadow AI y por qué ya está *dentro.*

No es una amenaza que viene. Es una realidad que ya está operando en tu organización, fuera del cuadro de mando de IT.

Shadow AI es el uso de herramientas de inteligencia artificial por parte de empleados sin aprobación, supervisión ni visibilidad de los equipos de tecnología y seguridad. Un analista que pega un contrato en un chatbot público para resumirlo, un comercial que genera una propuesta con datos de cliente, un desarrollador que completa código con un asistente no autorizado: ninguno actúa con mala intención, y todos amplían, sin saberlo, la superficie de riesgo de la empresa.

El fenómeno hereda el patrón de la **shadow IT** —las aplicaciones que los equipos adoptaban sin pasar por IT— pero lo acelera. La shadow IT exigía instalar, configurar, a veces pagar. La Shadow AI solo exige abrir una pestaña. Esa fricción casi nula explica por qué se extiende más deprisa de lo que cualquier política puede seguir, y por qué deja un rastro mucho más tenue.

> **La shadow IT exigía instalar algo. La Shadow AI solo exige *una pestaña*.**

La consecuencia es contraintuitiva: cuanto mejor es la herramienta, más se usa a la sombra. La utilidad inmediata vence a la política lejana cada vez que un empleado tiene una tarea delante y un plazo encima. Negar que esto ocurre no lo detiene; solo garantiza que ocurra sin testigos.

Sección 02

Anatomía del fenómeno: *por qué lo hacen.*

Entender la Shadow AI exige una concesión incómoda: los empleados que la usan suelen tener razón en lo inmediato. Resuelven una tarea real, ganan tiempo real y mejoran un resultado real. El problema no está en su juicio local, sino en la suma de muchos juicios locales sin un marco común. La motivación es productividad, no rebeldía.

Tres fuerzas alimentan el fenómeno. La primera es la brecha de provisión: la herramienta corporativa, cuando existe, llega tarde, pide permisos o rinde peor que la pública, y el empleado no espera. La segunda es la asimetría de incentivos: a la persona se le mide por entregar, no por cumplir una política que percibe como freno. La tercera es la invisibilidad del coste: el riesgo de filtrar un dato es difuso y futuro, mientras que el beneficio de terminar antes es concreto y presente.

Leído así, el Shadow AI deja de ser un problema de disciplina y pasa a ser un problema de diseño. Donde la organización no ofrece una vía buena, gobernada y rápida, la sombra ocupa el hueco. Cerrar ese hueco —no castigar a quien cae en él— es la única intervención que escala.

LAS TRES FUERZAS

Por qué crece

- **Brecha de provisión.** La opción corporativa llega tarde o rinde peor que la pública.
- **Asimetría de incentivos.** Se premia entregar, no cumplir la política.
- **Coste invisible.** El beneficio es presente y concreto; el riesgo, futuro y difuso.

Ninguna se corrige con una circular. Las tres se corrigen con gobierno y buena provisión.

La adopción ya ocurrió. No es una decisión pendiente del comité, sino una realidad distribuida por toda la plantilla, casi siempre fuera del cuadro de mando de tecnología y seguridad.

75%

de los profesionales del conocimiento ya usan IA en el trabajo, a menudo sin supervisión de IT.

Fuente pendiente de verificación independiente.

SECCIÓN 03 · EL INVENTARIO DE RIESGOS

Qué se pone en juego cuando la IA opera fuera del perímetro.

RIESGO	CÓMO APARECE	IMPLICACIÓN
Fuga de datos	*Información sensible pegada en herramientas públicas que la retienen o la usan para entrenar.*	El dato corporativo abandona el perímetro sin registro ni posibilidad de recuperación.
Exposición de IP	*Código, contratos o estrategia procesados en modelos de terceros.*	Pérdida de control sobre la propiedad intelectual y posibles incumplimientos contractuales.
Incumplimiento	*Tratamiento de datos personales sin base legal ni evaluación de impacto.*	Riesgo regulatorio bajo GDPR y EU AI Act; sanciones y daño reputacional.
Seguridad	*Claves API dispersas, prompt injection, salidas no saneadas que entran en sistemas internos.*	Nueva superficie de ataque difícil de monitorizar y auditar.
Coste oculto	*Suscripciones individuales y consumo de tokens sin visibilidad financiera.*	Gasto fragmentado, sin economías de escala ni control de FinOps.
Decisión no auditada	*Resultados de IA que influyen en decisiones sin trazabilidad de su origen.*	Imposibilidad de explicar o defender una decisión ante un auditor o un cliente.

Sección 04

Por qué prohibir *agrava* el problema.

El instinto del responsable de seguridad ante un riesgo nuevo es legítimo: cerrar la puerta. Pero la Shadow AI no tiene una puerta. Tiene mil, todas del tamaño de una pestaña de navegador, y ninguna requiere permiso para abrirse. Una prohibición frontal no elimina el uso; lo empuja a canales aún menos visibles: dispositivos personales, cuentas privadas, conversaciones que ya no dejan rastro alguno en la red corporativa.

El resultado es la peor combinación posible: el mismo riesgo de antes, ahora sin observabilidad. La prohibición convierte un problema gobernable en uno clandestino. Y además impone un coste silencioso: la organización renuncia a una ganancia de productividad que sus competidores no están dejando sobre la mesa.

> **Prohibir no elimina el uso. Solo elimina los *testigos*.**

Esto no significa que todo valga. Hay usos que deben vetarse y datos que no pueden salir bajo ninguna circunstancia. La diferencia entre una política útil y una contraproducente está en su forma: una veta categorías concretas con una alternativa a mano; la otra veta la herramienta entera y deja al empleado sin salida buena. La primera se cumple. La segunda se evade.

Sección 05

El marco de gobierno en tres *movimientos.*

Gobernar la Shadow AI no es una elección entre permitir y prohibir. Es una secuencia de tres pasos, y el orden importa.

Vis

Visibilizar, primero ver, antes de decidir

No se gobierna lo que no se ve. El primer movimiento es un inventario honesto del uso real: qué herramientas, para qué tareas, con qué datos. Sin amnistía no hay inventario fiable; el objetivo es entender, no sancionar.

Gob

Gobernar, un único punto de control

Sobre la visibilidad se construye el control: un gateway corporativo que aplica autenticación, políticas de datos, cuotas y trazabilidad antes de que la petición llegue a un modelo. El control vive en la arquitectura, no en la buena voluntad del usuario.

Hab

Habilitar, dar la herramienta buena

El gobierno se sostiene si la vía oficial es la más cómoda. Ofrecer una herramienta corporativa rápida, capaz y segura elimina la razón para usar la sombra. La adopción gobernada no se impone: se hace irresistible.

Sección 06

La paradoja del *CISO.*

El responsable de seguridad vive una tensión que parece sin salida. Si frena, mata la productividad que la dirección le pide preservar y empuja el uso a la clandestinidad. Si permite sin control, asume un riesgo que su función existe para contener. Cualquiera de los dos extremos lo deja mal: esa es la paradoja.

La salida no está en elegir un extremo, sino en cambiar el eje de la decisión. La pregunta no es «¿permito o prohíbo?», sino «¿cómo hago que el uso ocurra dentro de un marco que veo y controlo?». Planteada así, la seguridad deja de ser un muro y pasa a ser un cauce: no detiene el agua, la conduce. El CISO que gobierna en lugar de bloquear convierte un pasivo de riesgo en un activo de confianza, y deja de ser percibido como el departamento del «no».

Ese cambio de papel tiene un dividendo político además de técnico. Un equipo de seguridad que habilita con criterio gana la autoridad que pierde el que solo prohíbe. Y esa autoridad es, a la larga, la que permite imponer los pocos vetos que de verdad importan.

CAMBIO DE EJE

De muro a cauce

La pregunta deja de ser binaria. No «permitir o prohibir», sino cómo hacer que el uso ocurra dentro de un marco gobernado.

- El muro detiene el agua y la desborda por otro lado.
- El cauce no la detiene: la conduce y la mide.
- Quien habilita con criterio gana autoridad para los vetos que importan.

Lo que no gobiernas, *no lo controlas*.

Sección 07

Cómo se mide el *éxito.*

Gobernar sin medir es volver a quedarse a ciegas. Cuatro indicadores dicen si el marco funciona.

01 **Proporción de uso gobernado**
Qué fracción del uso real de IA pasa por la vía corporativa frente a la sombra. Es la métrica madre: si sube, el resto mejora con ella.

02 **Incidentes evitados y detectados**
Intentos de fuga de datos bloqueados, usos de riesgo interceptados, credenciales rotadas. Mide la observabilidad que la prohibición destruía.

03 **Coste de IA visibilizado**
Gasto que pasa de suscripciones dispersas e invisibles a consumo medido y presupuestado. Lo que se ve, se optimiza.

04 **Adopción de la herramienta corporativa**
Uso real de la vía oficial. Si la herramienta buena se usa, la sombra se vacía sola: es la prueba de que habilitar funcionó.

PARA RECORDAR

Cuatro ideas que conviene llevarse.

01

La Shadow AI ya está dentro.

No es un riesgo futuro: la adopción llegó de abajo arriba antes que la estrategia de arriba abajo.

02

No es indisciplina, es diseño.

Donde no hay vía buena, gobernada y rápida, la sombra ocupa el hueco. Se cierra el hueco, no se castiga a quien cae en él.

03

Prohibir empeora la posición.

Mantiene el riesgo y elimina la observabilidad. Veta categorías concretas con alternativa, no la herramienta entera.

04

Visibilizar, gobernar, habilitar.

El orden importa: ver primero, controlar en la arquitectura, y hacer irresistible la vía oficial.

Conclusión

De pasivo silencioso a *capacidad gobernada.*

La Shadow AI es, antes que nada, una buena noticia mal gestionada. Significa que tu gente ya encontró valor en la inteligencia artificial sin que nadie se lo ordenara. El problema no es el apetito; es que ese apetito se está satisfaciendo fuera de tu vista, con tus datos y sin tus límites.

Por eso conviene repetir la tesis sin rodeos: **el riesgo invisible no es que tus empleados usen IA, sino que la usan sin que tú lo veas, y eso no se resuelve prohibiendo. Lo que no se gobierna, no se controla; y lo que no se controla, expone.**

El camino no es frenar la adopción, sino encauzarla: visibilizar lo que ya ocurre, gobernarlo desde la arquitectura y habilitar una vía oficial tan buena que la sombra se quede sin razón de ser. Hecho así, lo que hoy es un pasivo silencioso se convierte en una capacidad gobernada, y la seguridad deja de ser el departamento del «no» para volverse el que hace posible decir «sí, con criterio».

> “
>
> **La seguridad madura no construye muros. Construye *cauces*.**

Thinkia

UN WHITEPAPER EJECUTIVO · 2026

FUENTES Y NOTA METODOLÓGICA

Fuentes.

01 Dato de adopción de IA por empleados del conocimiento (≈75 %, uso frecuente sin supervisión de IT). Pendiente de verificación independiente contra la fuente primaria antes de publicar.

02 Marco regulatorio de referencia: Reglamento de IA de la UE (EU AI Act) y Reglamento General de Protección de Datos (GDPR). Verificar versiones y plazos vigentes en el momento de publicación.

03 Patrón de shadow IT como antecedente conceptual de la Shadow AI. Referencia general de gobierno de tecnología, sin atribución a un autor único.

Nota: las cifras cuantitativas de este documento deben verificarse de forma independiente contra su fuente primaria antes de la publicación. Los marcos regulatorios citados pueden haber cambiado; confírmense las versiones vigentes.

CÓMO CITAR ESTE DOCUMENTO

Alejano, D. (2026). *Shadow AI*. Thinkia, serie de liderazgo de pensamiento. thinkia.com

thinkia

thinkia.com