

ANÁLISIS II ENCUESTA: ADOPCIÓN Y GOBIERNO DE LA IA

Estudio Completo

Noviembre 2024

1. Introducción	2
2. Análisis de resultados	3
1.1. Cuestiones principales	3
1.1.1. ¿Su organización ha implementado sistemas basados en Inteligencia Artificial Generativa?	3
1.1.2. ¿Qué tipo de sistemas?	4
1.1.3. ¿Qué previsión de incremento de uso de la IA Generativa cree que va a pasar en su organización en los próximos 3 años?	6
1.1.4. ¿En su organización hay algún rol o equipo responsable de definir la estrategia a seguir con la adopción y despliegue de la IA?	7
1.1.5. ¿En su organización se ha definido un modelo de uso y despliegue de la IA (cómo se introduce en la organización, qué ámbitos se priorizan,...)?	8
1.1.6. ¿Se han establecido políticas y procedimientos específicos para garantizar la seguridad de los sistemas de IA en su organización?	9
1.1.7. ¿Qué grado de supervisión y control aplica sobre el uso de herramientas públicas de IA tipo ChatGPT con equipos corporativos?	11
1.1.8. ¿Cómo calificaría su nivel de conocimiento de esta tecnología?	12
1.1.9. ¿En qué medida cree que hay potencial riesgo en el uso de IA en su organización?	13
1.1.10. En caso de que así lo crea, ¿en qué áreas cree que habrá mayor riesgo en el uso de la IA?	14
2.1.11. ¿Se ha capacitado al personal en temas de seguridad relacionados con la IA y la detección de posibles amenazas?	15
2.1.12. ¿Está familiarizado con el Reglamento Europeo de Inteligencia Artificial (AI Act) de la UE y sus implicaciones para la seguridad y la protección de datos?	16

2.1. Cuestiones adicionales	17
2.1.1. Indique el sector de actividad de su organización	17
2.1.2. Seleccione cuál es su rol en la organización	18
2.1.3. ¿Se han identificado y evaluado los riesgos de seguridad asociados con la implementación de sistemas de IA?	19
2.1.4. ¿Se han realizado evaluaciones de impacto en la privacidad y se han implementado salvaguardias adecuadas para proteger los datos personales en sistemas de IA?	20
2.1.5. ¿Existe un proceso para auditar y revisar regularmente los sistemas de IA implementados para identificar posibles vulnerabilidades o debilidades de seguridad?	21
2.1.6. ¿Su organización tiene un plan de respuesta a incidentes de seguridad específico para sistemas de IA?	22
2.1.7. ¿Considera preciso implementar en su organización algún tipo de control sobre los posibles sesgos de estos sistemas?	23
2.1.8. ¿Ha realizado o tiene previsto hacer un inventario de modelos y sistemas IA en su organización?	24
2.1.9. ¿Ha realizado o tiene previsto hacer una evaluación de impacto según establece el Reglamento Europeo de Inteligencia Artificial?	25
2.1.10. ¿Qué otros aspectos considera que deberían tratarse con relación a riesgos en la adopción y gobierno de la IA?	26

1. Introducción

Por segundo año consecutivo el Grupo de Trabajo en Inteligencia Artificial del ISMS Forum ha desarrollado la encuesta de Adopción y Gobierno de la IA en las organizaciones.

Dicha encuesta se ha difundido por los canales habituales de la asociación, lo que implica que, mayoritariamente, ha sido respondida por profesionales de Seguridad de la Información en sus diversas disciplinas de actividad.

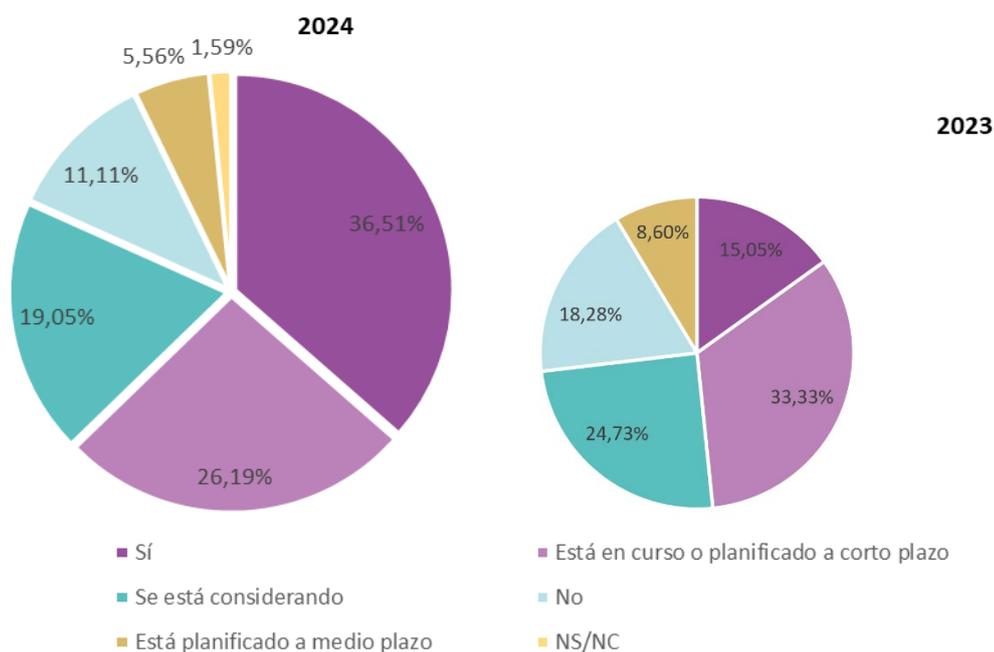
En este documento se muestran los resultados con un pequeño análisis asociado y comparado con los resultados de la primera encuesta similar realizada en 2023.

Esta II edición de la encuesta ha obtenido 131 participaciones.

2. Análisis de resultados

1.1. Cuestiones principales

1.1.1. ¿Su organización ha implementado sistemas basados en Inteligencia Artificial Generativa?

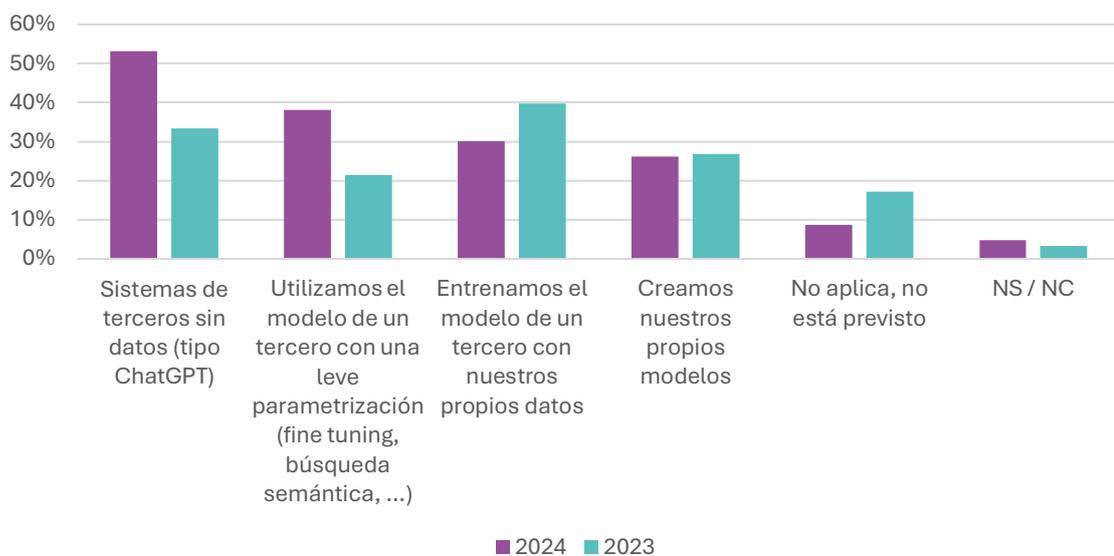


El gráfico de 2024 muestra una evolución en la implementación de sistemas basados en Inteligencia Artificial Generativa respecto a los datos de 2023.

- **Crecimiento en la implementación:** Claramente la IA Generativa ha penetrado en el tejido empresarial. Si ya en 2023 el 48,89% de las compañías estaban empleando esta tecnología en sus procesos o planificaban su uso a corto plazo, esta cifra ha incrementado significativamente durante 2024, extendiéndose su uso entre casi una de cada tres empresas. (62,7%).
- **Reducción de la incertidumbre:** El porcentaje de organizaciones que lo están considerando (**19,05%**) y las que no tienen planes (**11,11%**) se ha reducido en comparación con el 2023, lo que refleja que muchas organizaciones han pasado de la fase de evaluación a la adopción.

En resumen, los datos de 2024 reflejan un crecimiento natural de la adopción de IA Generativa, impulsado por una combinación de madurez tecnológica, reducción de costos, una mayor comprensión de los casos de uso y presión competitiva. Las empresas que en 2023 estaban en la fase de consideración o planificación ahora están adoptando estas tecnologías, mientras que el escepticismo y la incertidumbre han disminuido notablemente. Se espera que esta tendencia continúe, con más organizaciones planificando implementaciones a corto o medio plazo.

1.1.2. ¿Qué tipo de sistemas?



Si analizamos la evolución de las respuestas de los dos años vemos:

Sistemas de terceros sin datos (tipo ChatGPT)

El aumento de **33,33% a 53,17%** refleja una mayor adopción de herramientas de terceros sin integración de datos, impulsado por su **accesibilidad, rapidez y menores costos**. Las empresas prefieren soluciones listas para usar que no requieren entrenamiento complejo.

Utilizamos el modelo de un tercero con leve parametrización (fine tuning, búsqueda semántica, ...)

El crecimiento de **21,51% a 38,10%** muestra que más organizaciones optan por ajustar modelos de terceros para adaptarlos a sus necesidades, lo que **combina personalización y bajo costo**, ofreciendo mayor precisión sin una carga técnica significativa.

Creamos nuestros propios modelos

La estabilidad en torno al **26%** indica que sigue siendo una opción para empresas con necesidades muy específicas, aunque el coste y la complejidad limitan su adopción.

NS/NC (No sabe/No contesta)

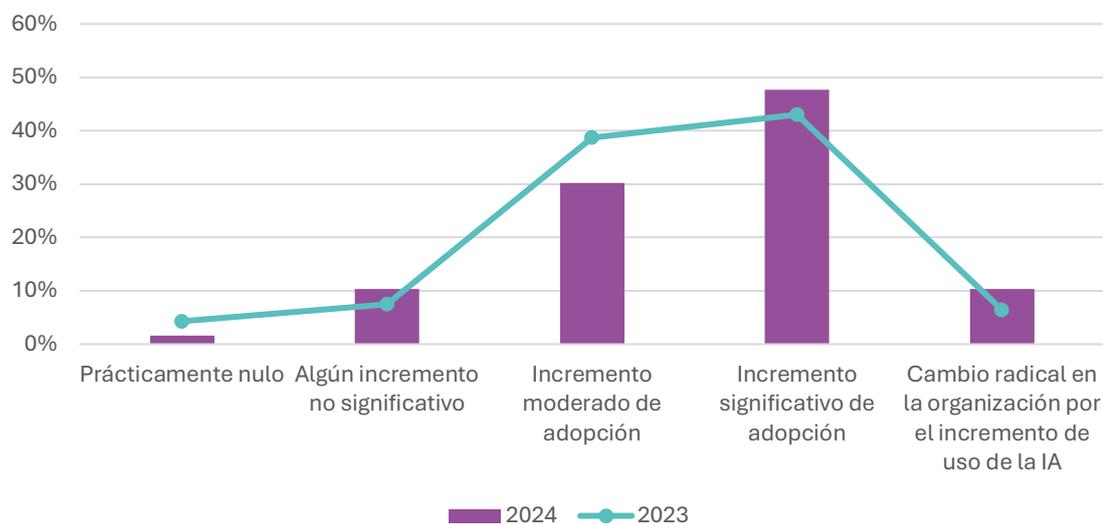
El leve aumento de **3,23% a 4,76%** refleja indecisión debido a la mayor **complejidad tecnológica, excusa formación** y falta de claridad en la estrategia de adopción.

No aplica, no está previsto

La caída de **17,20% a 8,73%** sugiere que menos empresas ven la IA generativa como irrelevante, probablemente debido a la **presión competitiva** y la expansión de los casos de uso.

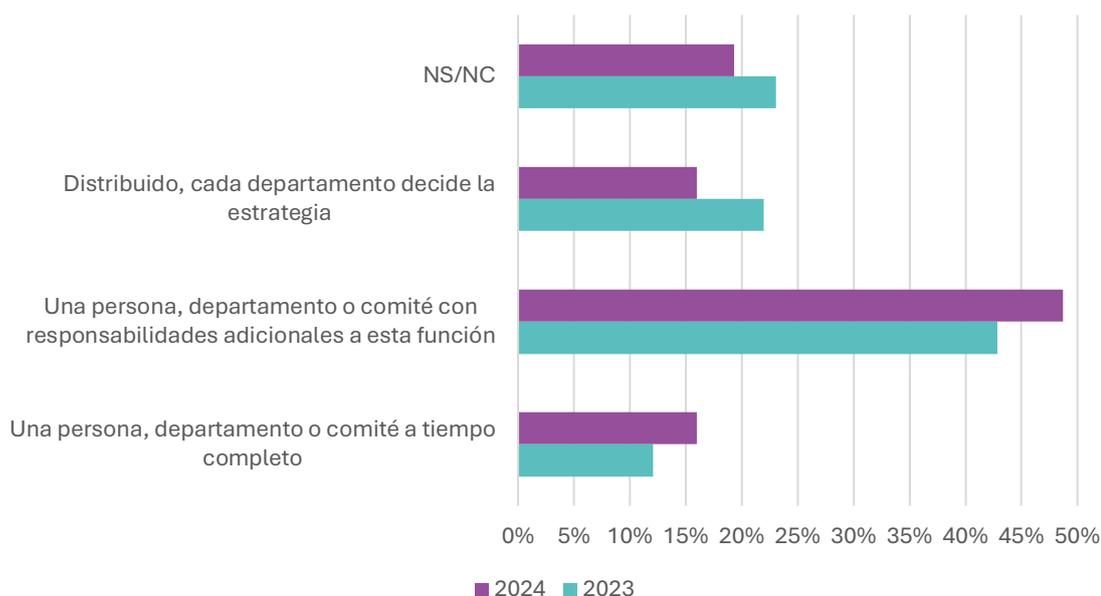
En resumen, el mercado de IA generativa está avanzando hacia el uso de sistemas preentrenados y parametrizados por su rapidez de implantación y menor costo, mientras que la creación y entrenamiento de modelos propios se mantiene estable, aunque en menor medida, debido a su complejidad y coste. Las empresas ahora pueden elegir soluciones que se adapten mejor a sus necesidades sin grandes inversiones en infraestructura.

1.1.3. ¿Qué previsión de incremento de uso de la IA Generativa cree que va a pasar en su organización en los próximos 3 años?



El análisis muestra una **reducción significativa en las previsiones de adopción nula o moderada**, lo que indica que las empresas son más conscientes de la relevancia de la IA generativa. La mayoría de las organizaciones ahora esperan **incrementos significativos de adopción de IA Generativa o incluso cambios radicales** en los próximos tres años. Esto sugiere una evolución hacia una **adopción más rápida y transformadora**, probablemente motivada por el potencial de la IA para mejorar la productividad y crear nuevas oportunidades de negocio.

1.1.4. ¿En su organización hay algún rol o equipo responsable de definir la estrategia a seguir con la adopción y despliegue de la IA?



Las tendencias que aumentan en 2024 muestran que cada vez más organizaciones están adoptando un enfoque estratégico para la gestión de la IA. Por un lado, el porcentaje de **personas, departamentos o comités a tiempo completo** dedicados exclusivamente a esta función crece del **12,09% en 2023 al 15,97% en 2024**, lo que indica una **mayor priorización** de la IA como un aspecto central para las empresas.

Por otro lado, el porcentaje de **personas, departamentos o comités con responsabilidades adicionales** en la gestión de IA también aumenta, pasando del **42,86% en 2023 al 48,74% en 2024**. Esto sugiere que, aunque muchas organizaciones aún no han creado roles exclusivos para la IA, la ven como una **función clave integrada en las tareas de gestión existentes**. Esto refleja que la IA está ganando importancia, pero en muchos casos se sigue gestionando junto con otras responsabilidades.

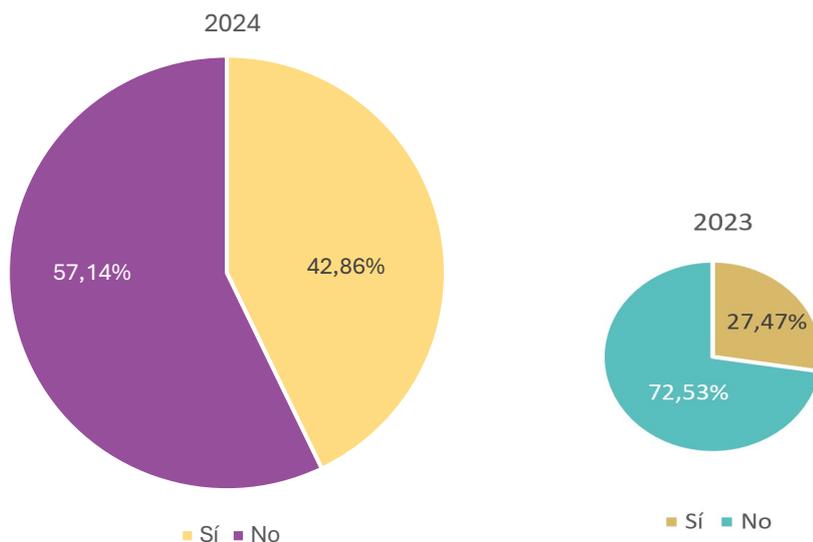
En 2024, se observan algunas tendencias a la baja en cuanto a la gestión de la IA dentro de las organizaciones. El porcentaje de empresas que **dejan la estrategia de IA en manos de cada departamento** disminuye del **21,98% en 2023 al 15,97% en 2024**.

Esta caída refleja una **menor preferencia por la descentralización**, lo que sugiere un **movimiento hacia la centralización y una mayor coordinación global** de la estrategia de IA en las empresas.

Asimismo, el porcentaje de **NS/NC (No sabe / No contesta)** también baja, del **23,08% en 2023 al 19,33% en 2024**, lo que indica que **más organizaciones han definido con mayor claridad su enfoque** hacia la adopción y gestión de la IA, reduciendo la incertidumbre sobre el tema.

El análisis muestra una clara **tendencia hacia la profesionalización** de la estrategia de IA dentro de las organizaciones, con más empresas creando roles o departamentos dedicados exclusivamente o en parte a esta tarea. La **distribución descentralizada** está perdiendo terreno, lo que sugiere que las empresas entienden la **necesidad de una estrategia de IA coherente y centralizada**. A medida que la IA se vuelve más crítica para la competitividad, más organizaciones reconocen la importancia de contar con **estructuras claras** y responsables asignados para gestionar su adopción y despliegue.

1.1.5. ¿En su organización se ha definido un modelo de uso y despliegue de la IA (cómo se introduce en la organización, qué ámbitos se priorizan,...)?

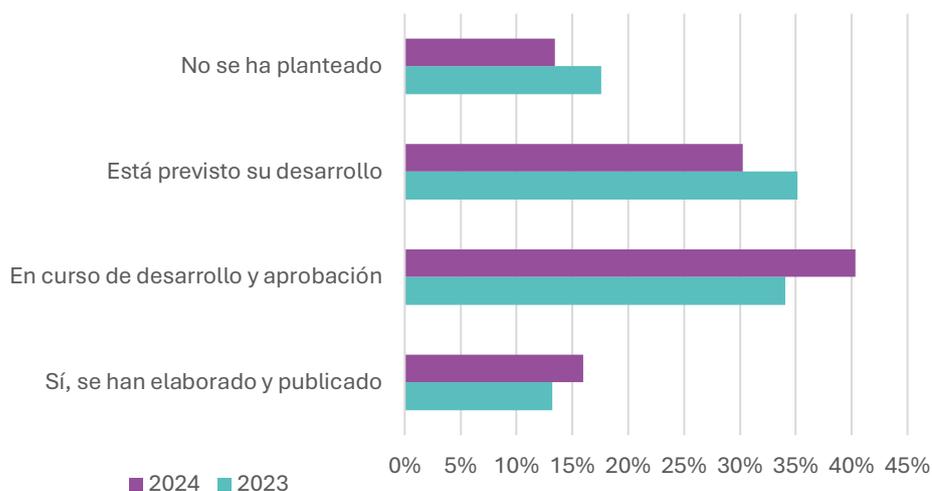


En 2024, el **42,86%** de las organizaciones ha definido un modelo para el uso y despliegue de la IA, un notable incremento con respecto al **27,47%** de 2023. Este aumento sugiere que las empresas están comenzando a reconocer la importancia de establecer un marco estructurado para integrar la inteligencia artificial en sus operaciones. La evolución en estas cifras indica un cambio en la mentalidad organizacional, donde se prioriza no solo la adopción de la tecnología, sino también la planificación estratégica de su implementación.

Por otro lado, el porcentaje de organizaciones que **no han definido un modelo** ha disminuido del **72,53%** en 2023 al **57,14%** en 2024. Este descenso es significativo, ya que refleja un movimiento hacia una mayor claridad en las estrategias de IA, lo que podría facilitar su adopción efectiva. Las empresas que aún no han establecido un modelo podrían estar perdiendo oportunidades para optimizar procesos y mejorar la toma de decisiones.

En resumen, el aumento en la definición de modelos para el uso y despliegue de la IA señala una creciente madurez en la adopción de esta tecnología, mientras que la disminución de las organizaciones sin un modelo indica un progreso hacia una gestión más estratégica y efectiva de la inteligencia artificial.

1.1.6. ¿Se han establecido políticas y procedimientos específicos para garantizar la seguridad de los sistemas de IA en su organización?

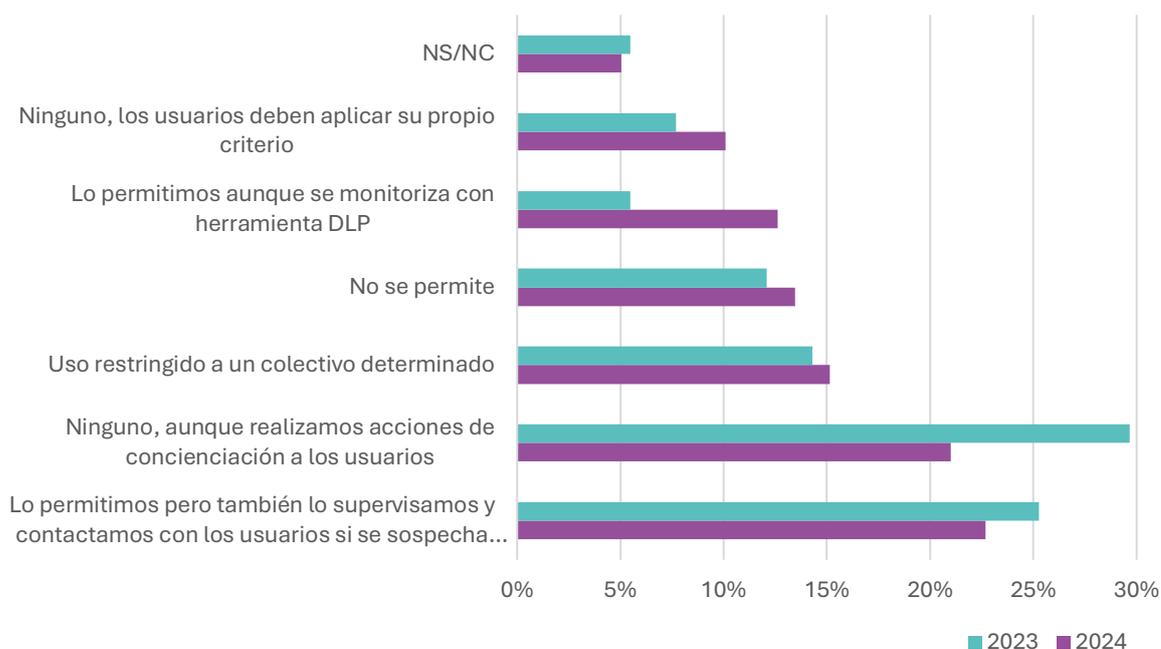


Las respuestas a la pregunta sobre políticas de seguridad para los sistemas de IA muestran cambios significativos entre 2023 y 2024:

1. **Políticas Elaboradas y Publicadas:** Aumentó del **13,19% en 2023 al 15,97% en 2024**, reflejando un creciente compromiso por establecer marcos claros de seguridad en IA.
2. **Desarrollo en Curso:** Creció del **34,07% al 40,34%**, indicando que más organizaciones están activamente trabajando en la creación de políticas de seguridad.
3. **Previsto Su Desarrollo:** Disminuyó del **35,16% al 30,25%**, sugiriendo una necesidad de acción más decidida en lugar de solo planificación.
4. **No Se Ha Planteado:** Redujo del **17,58% al 13,45%**, lo que indica que menos organizaciones ignoran la importancia de establecer políticas de seguridad.

En resumen, hay una tendencia positiva hacia la **implementación de políticas de seguridad para IA**, con más organizaciones tomando medidas activas y reconociendo la necesidad de proteger sus sistemas de IA ante riesgos potenciales.

1.1.7. ¿Qué grado de supervisión y control aplica sobre el uso de herramientas públicas de IA tipo ChatGPT con equipos corporativos?

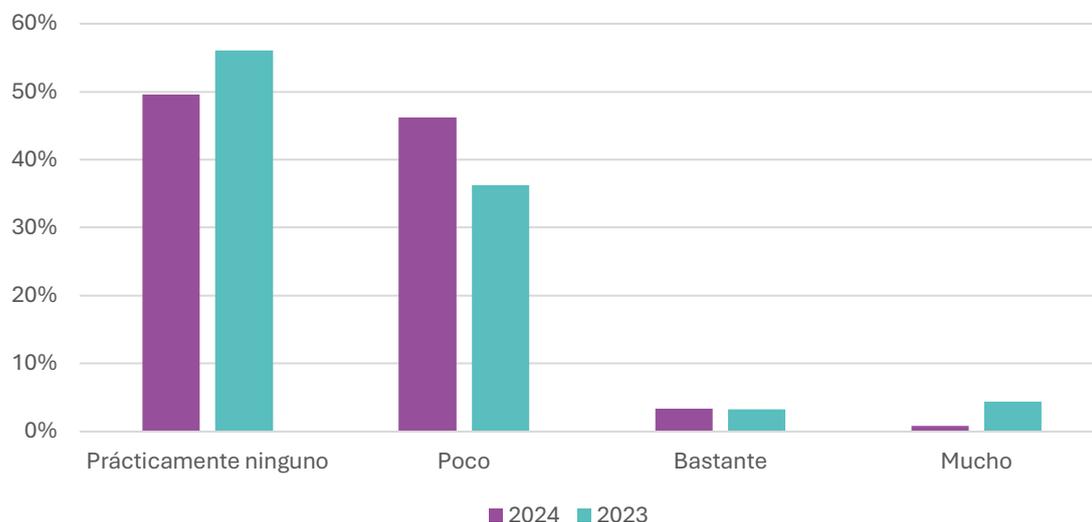


Desde la perspectiva de control cabe destacar:

- Aumenta significativamente el **control de acceso con herramienta DLP** (de 5,49% en 2023 a 12,61%),
- Leve aumento del **uso restringido a colectivos** (de 14,29% a 15,13%) y
- Ligero incremento de **prohibición de acceso** (de 12,09% a 13,45%).

En el lado opuesto al control sorprende ver la evolución a más del **uso libre por usuarios sin criterios generales**, es un punto que merece especial atención por los riesgos que ello conlleva de cara a pérdida del control de información clasificada desde un punto de vista de seguridad, así como posibles riesgos de compliance por el uso sin control de los resultados de estas herramientas.

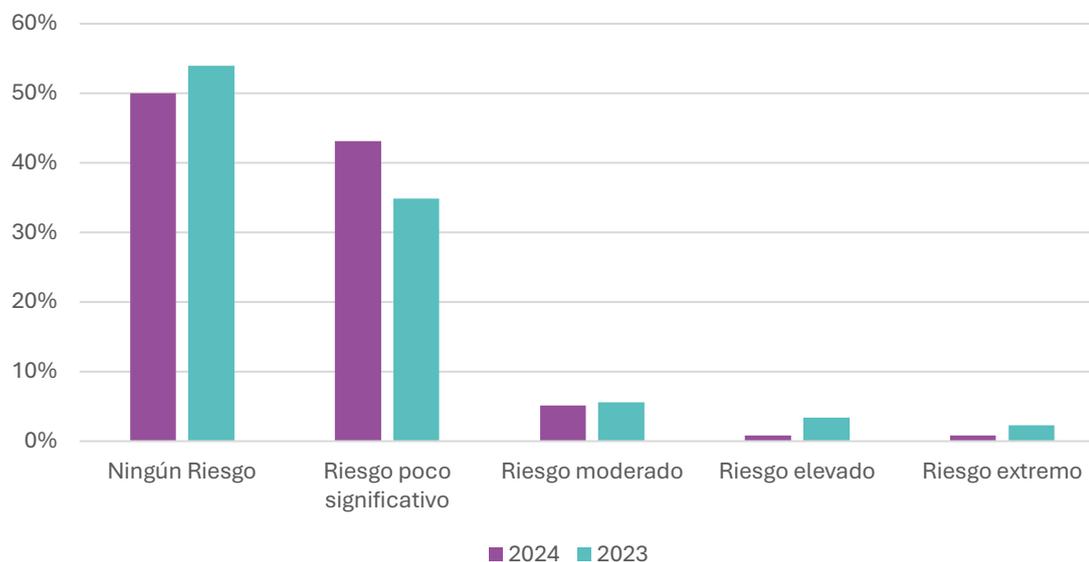
1.1.8. ¿Cómo calificaría su nivel de conocimiento de esta tecnología?



Como era previsible los resultados demuestran un aumento de conocimiento de la herramienta, sin embargo, cabe destacar:

- Un 49,58% declara tener **poco conocimiento** frente al 56,04% de 2023
- Un 46,22% dice tener **bastante conocimiento** frente al 36,26% de 2023
- Hay un muy leve aumento de personas que indiquen tener **mucho conocimiento** (un 3,36% frente al 3,3% de 2023)

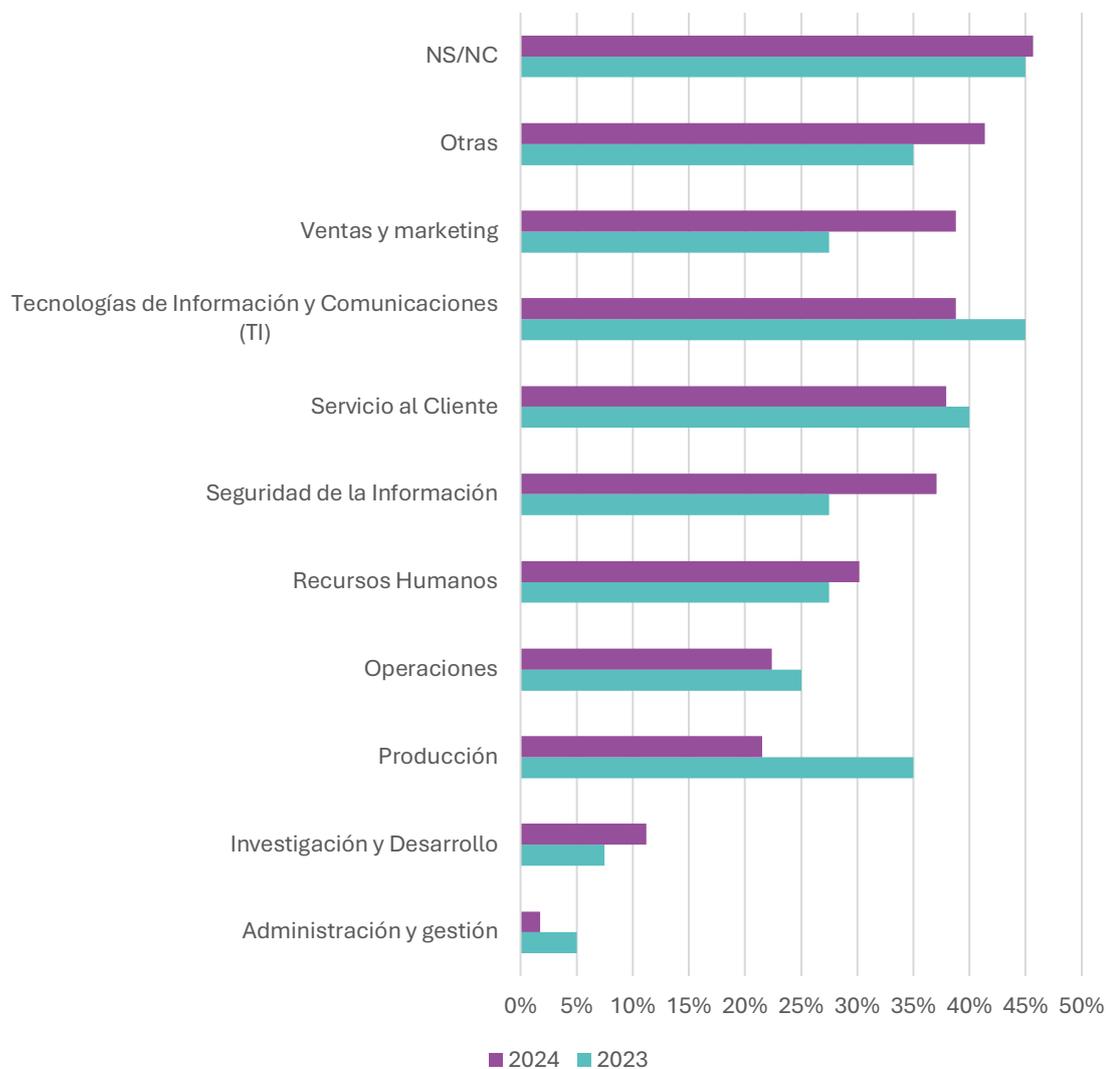
1.1.9. ¿En qué medida cree que hay potencial riesgo en el uso de IA en su organización?



En general **aumenta la percepción de riesgo**, aunque de forma distribuida:

- Sólo el 0,86% considera que no hay **ningún riesgo** en el uso frente al 3,37%
- El 5,17% considera que hay **riesgo poco significativo** vs el 5,62% de 2023
- También disminuye ligeramente la percepción de **riesgo moderado**, pasando de un 53,93% en 2023 al 50% en 2024.
- El cambio más significativo está en el aumento de percepción de **riesgo elevado**, siendo en 2024 un 43,10% frente al 34,83% de 2023
- El **riesgo extremo** disminuye, pasando del 2,25% del ejercicio anterior al 0,86% en 2024

1.1.10. En caso de que así lo crea, ¿en qué áreas cree que habrá mayor riesgo en el uso de la IA?



El área que se considera con mayor riesgo en 2024 es **Seguridad de la Información** con un 45,69%, valor muy similar al 2023 que fue del 45%.

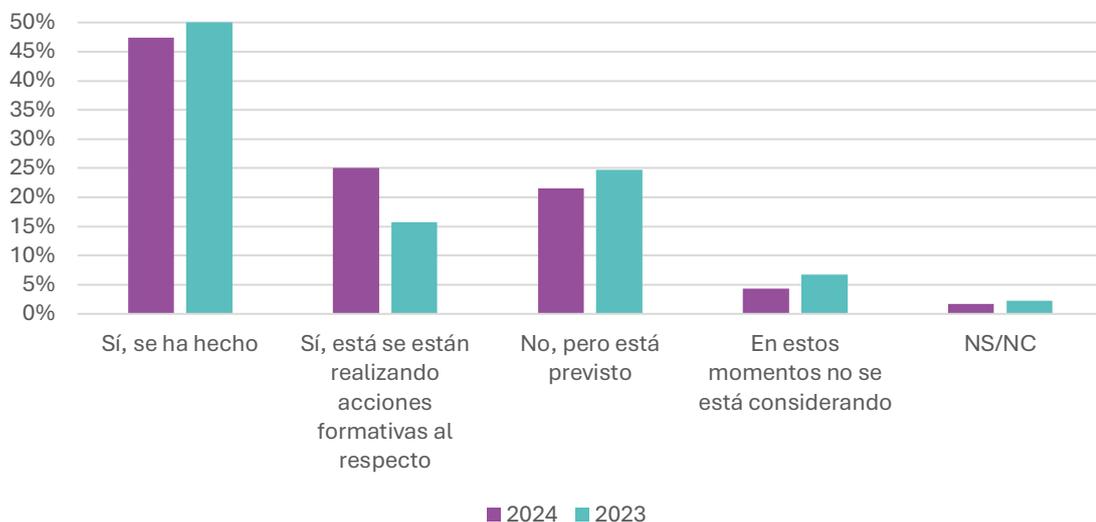
El descenso de riesgo es especialmente destacable en dos áreas:

- **Producción**, del 35% al 21,55%
- **Operaciones**, que en 2023 estaba en el top pasa del 45% al 38,79%

En el lado opuesto es destacable el incremento de riesgo en las áreas de:

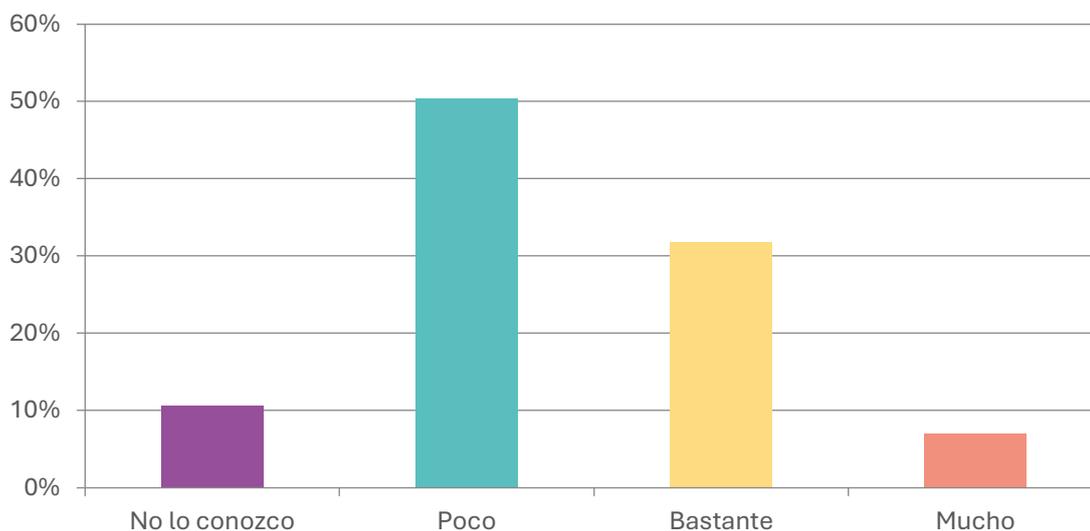
- **Recursos Humanos**, del 35% al 41,38%
- **Tecnologías de Información y Comunicaciones**, que pasa del 27,5% al 38,79%
- **Ventas y Marketing** que también sube del 27,5% al 37,07%

2.1.11. ¿Se ha capacitado al personal en temas de seguridad relacionados con la IA y la detección de posibles amenazas?



En el ámbito de la capacitación del personal en temas de seguridad relacionados con la IA y detección de posibles amenazas los resultados son muy similares, siendo destacable el incremento de las **organizaciones que están realizando acciones formativas**, que pasa del 15,73% en 2023 al 25% en este ejercicio.

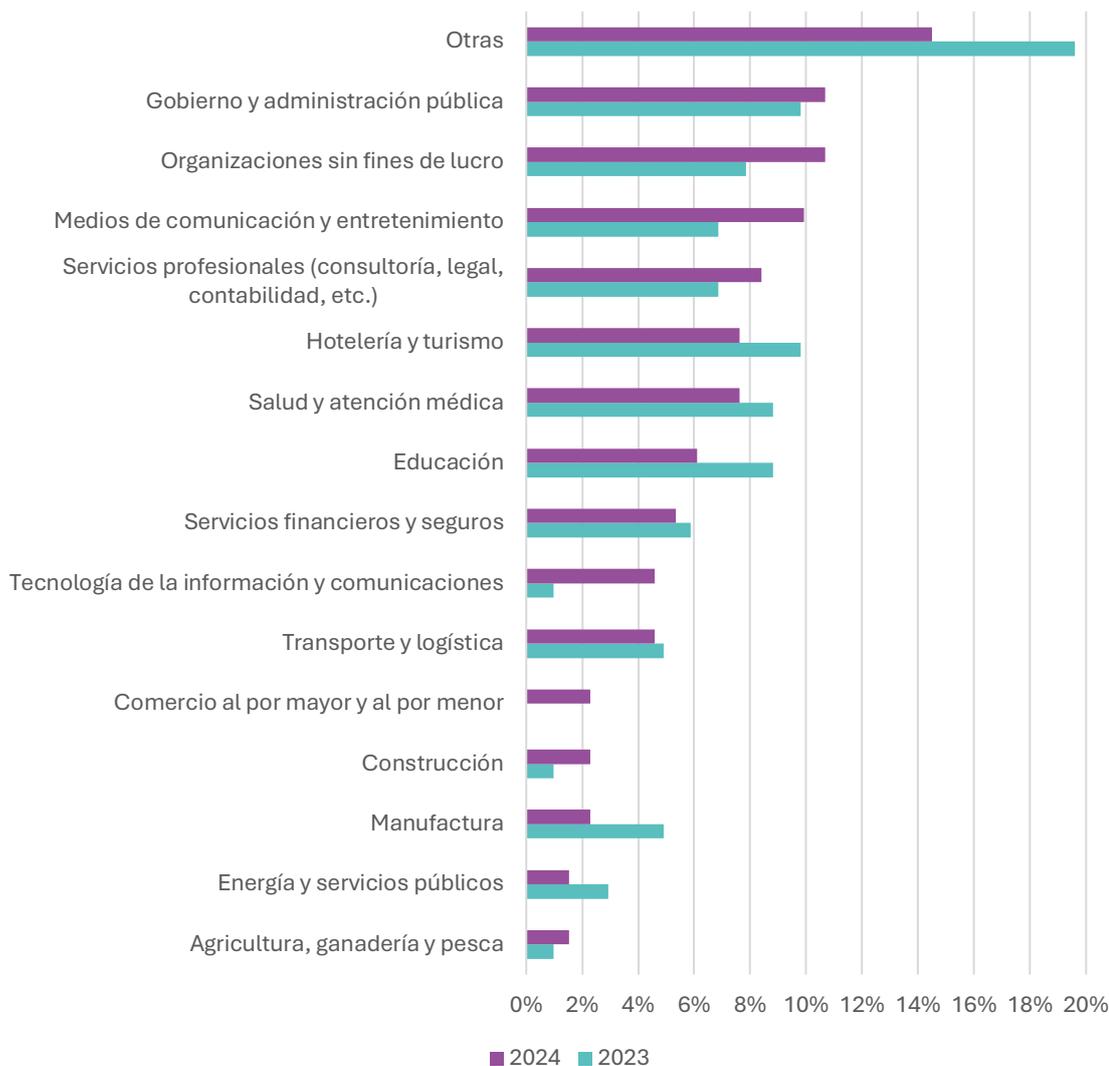
2.1.12. ¿Está familiarizado con el Reglamento Europeo de Inteligencia Artificial (AI Act) de la UE y sus implicaciones para la seguridad y la protección de datos?



En verano de 2024 se publicó el Reglamento Europeo de Inteligencia Artificial un extenso reglamento de 144 páginas que fue precedido por un borrador aún más extenso de 459 páginas es por ello comprensible que un 61% declare tener poco o ningún conocimiento de dicho reglamento y sus implicaciones para la seguridad y protección de datos.

2.1. Cuestiones adicionales

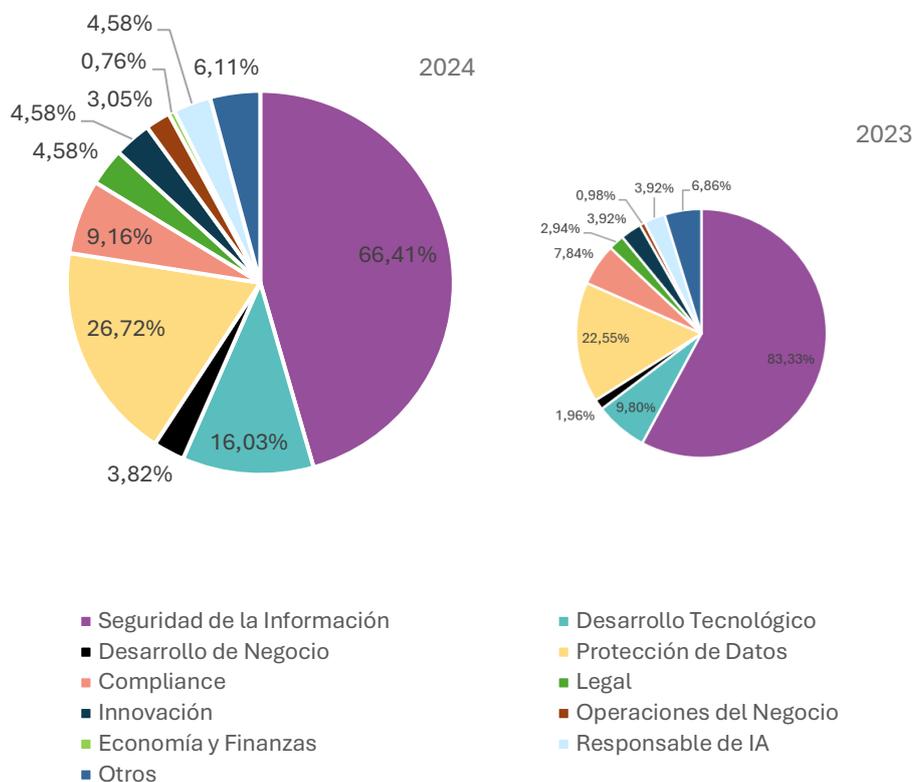
2.1.1. Indique el sector de actividad de su organización



Al igual que en la edición pasada, el sector de **Servicios Financieros** es el que más ha participado en la encuesta. Con un 14,5% en 2024 sobre el total de participantes, es claro indicativo del interés que tiene el sector en el uso de la IA.

También se destaca una mayor participación del **Sector público**, que pasa del 6,86% al 9,92% en 2024.

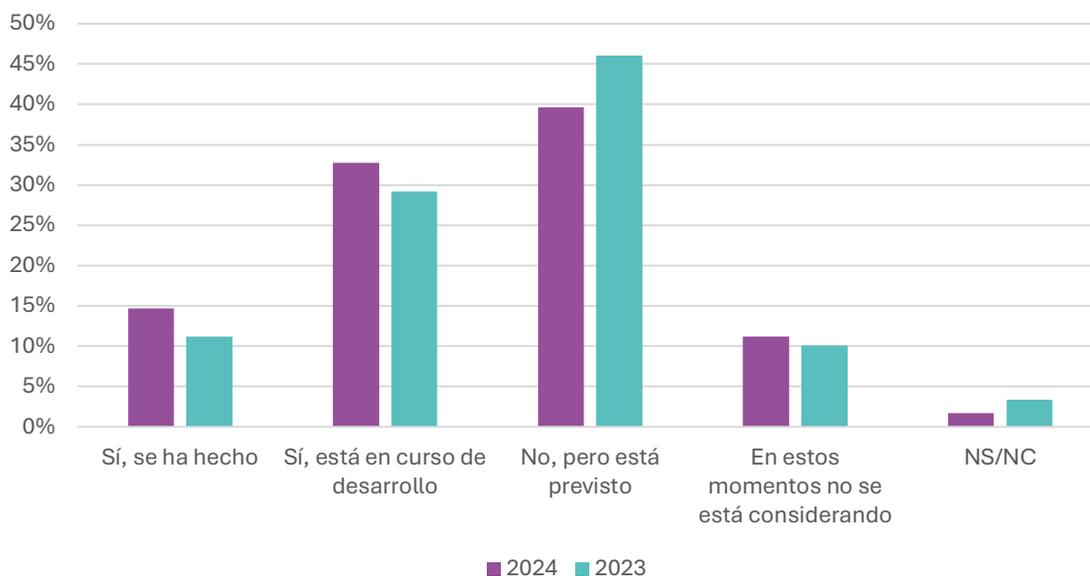
2.1.2. Seleccione cuál es su rol en la organización



Si bien la distribución de participación es bastante homogénea con relación a la edición anterior se observan algunas pequeñas diferencias:

- Aunque la mayoría se dedica a **Seguridad de la Información** (66,41%) el porcentaje no es tan amplio como en la edición anterior (83,33%).
- El rol de **Protección de datos** en esta ocasión supone el 26,72% mientras que en la edición anterior supuso el 22,55%, lo que demuestra creciente interés en la materia.
- A su vez el área de **Desarrollo Tecnológico** responde en un 16,03% frente al 9,8% de 2023.

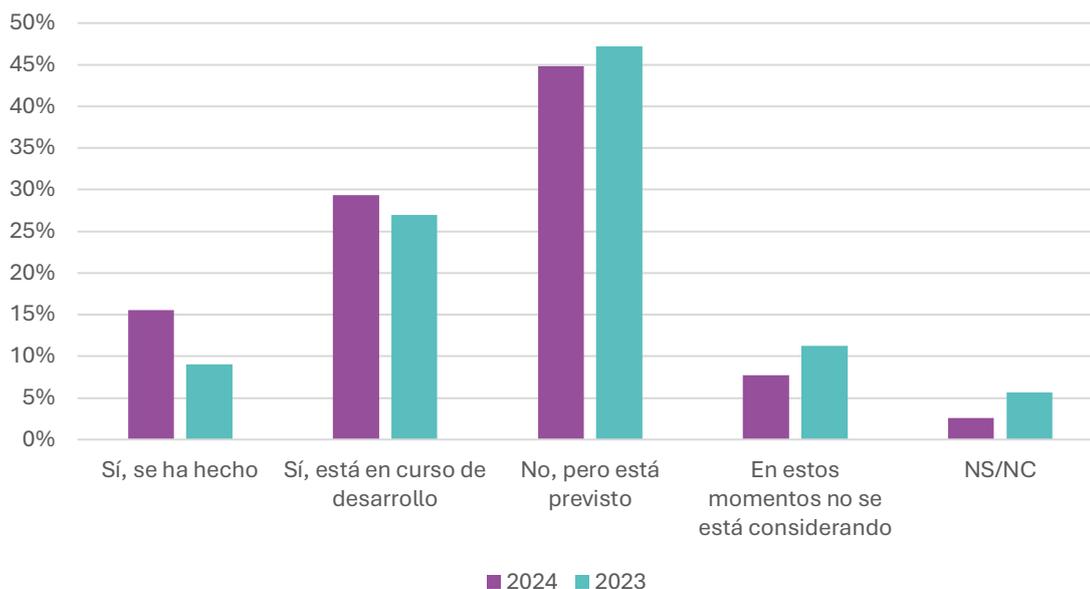
2.1.3. ¿Se han identificado y evaluado los riesgos de seguridad asociados con la implementación de sistemas de IA?



Aunque no hay una variación significativa entre ambos ejercicios cabe destacar:

- Aumento de entidades que **sí han hecho un análisis de riesgos de seguridad** (14,66% en 2024 vs 11,24 en 2023)
- Aumento de **entidades que lo están haciendo** (32,76% en 2024 vs 29,21% de 2023)

2.1.4. ¿Se han realizado evaluaciones de impacto en la privacidad y se han implementado salvaguardias adecuadas para proteger los datos personales en sistemas de IA?

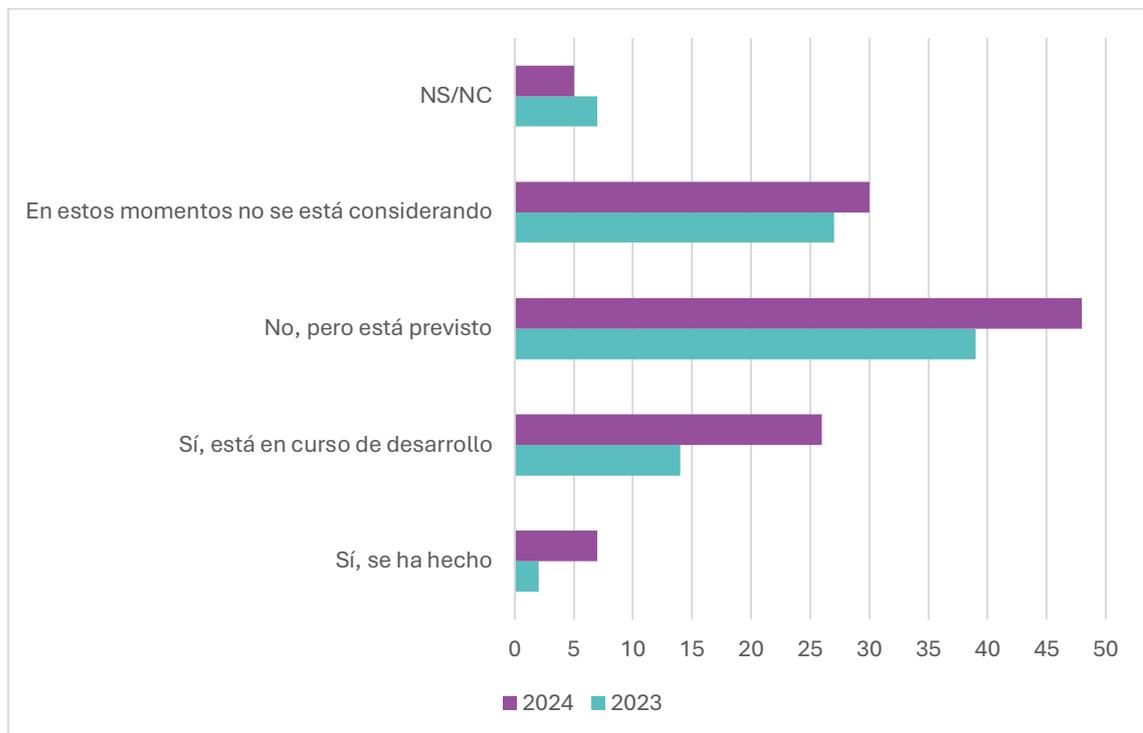


En comparación con 2023, los datos de 2024 muestran un aumento en el número de entidades que han completado o están en proceso de realizar evaluaciones de impacto en la privacidad. Este avance podría interpretarse como un reflejo de una mayor concienciación y compromiso hacia la protección de los datos personales en el contexto de la IA. Sin embargo, el alto porcentaje de entidades que aún no han implementado estas evaluaciones, pero tienen planes de hacerlo (44,83% en 2024) indica que existe un margen significativo para mejorar en este aspecto. La tendencia general sugiere una dirección positiva, pero los resultados resaltan la necesidad de que más entidades aceleren la adopción de salvaguardias efectivas para la privacidad en IA.

2.1.5. ¿Existe un proceso para auditar y revisar regularmente los sistemas de IA implementados para identificar posibles vulnerabilidades o debilidades de seguridad?

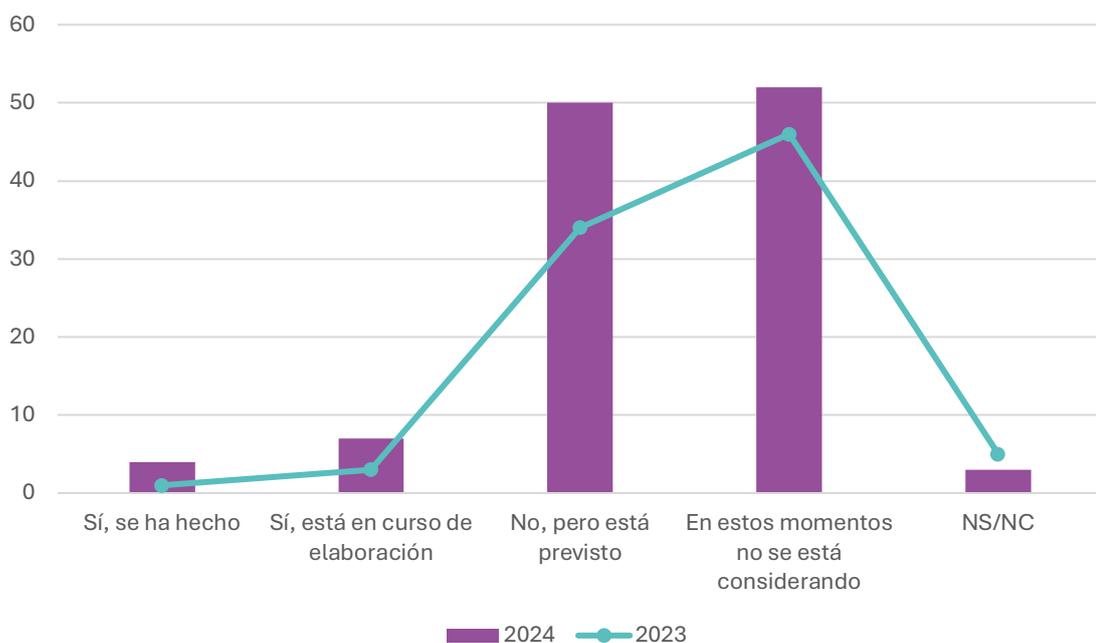
Si comparamos los ejercicios 2023 y 2024, se observa un incremento en la cantidad de entidades que han implementado o están en desarrollo de un proceso de auditoría y revisión de sus sistemas de IA. Este crecimiento indica una mayor concienciación sobre la importancia de la seguridad en IA.

No obstante, el hecho de que **48 entidades** solo lo tengan previsto y **30** no lo consideren en absoluto destaca una brecha importante en la implementación de prácticas de auditoría regulares. En general, aunque la tendencia es de mejora gradual, un alto porcentaje de organizaciones aún no cuenta con estos procesos, lo que representa una oportunidad importante para fortalecer la seguridad en los sistemas de IA.

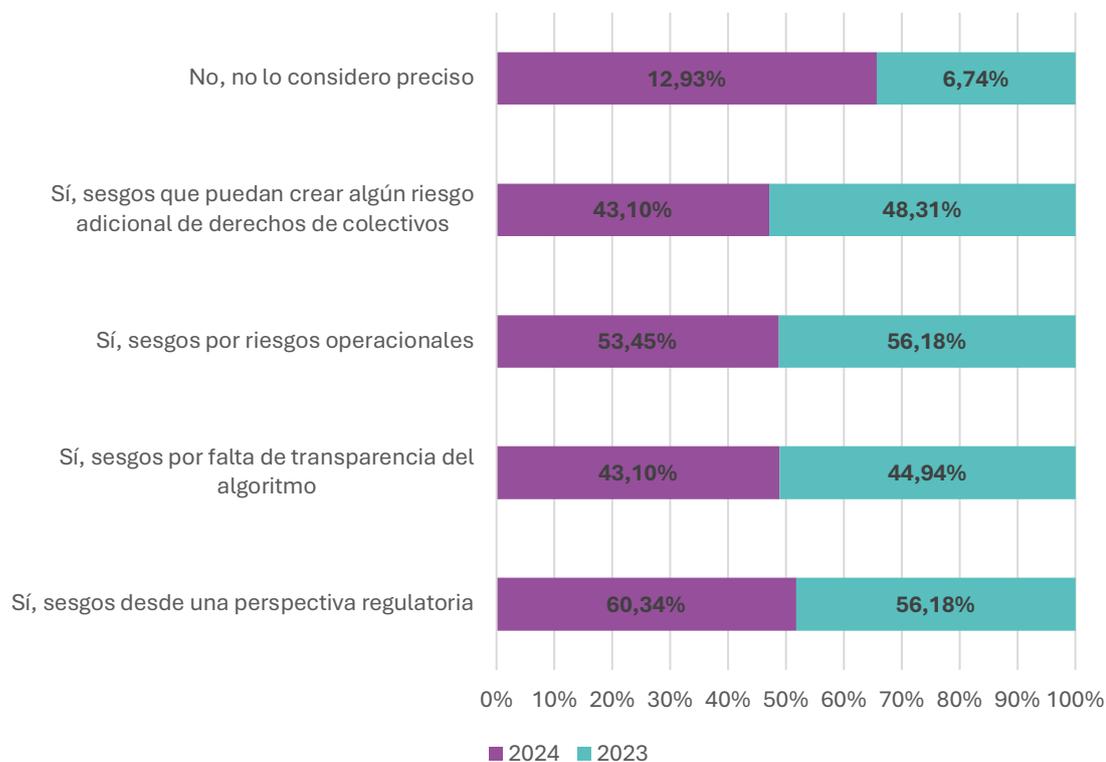


2.1.6. ¿Su organización tiene un plan de respuesta a incidentes de seguridad específico para sistemas de IA?

Los datos de 2024 muestran un incremento moderado en el número de entidades que han implementado o están en proceso de crear un plan de respuesta para IA, lo cual refleja un leve aumento en la importancia otorgada a la seguridad en IA. Sin embargo, el hecho de que más del **50%** de las organizaciones no consideren implementar un plan específico sugiere que aún existe una gran brecha en la preparación para incidentes de seguridad en IA. Esto podría deberse a la falta de normativas, recursos especializados o a una percepción de que los riesgos de IA son manejables con planes de seguridad generalizados.



2.1.7. ¿Considera preciso implementar en su organización algún tipo de control sobre los posibles sesgos de estos sistemas?



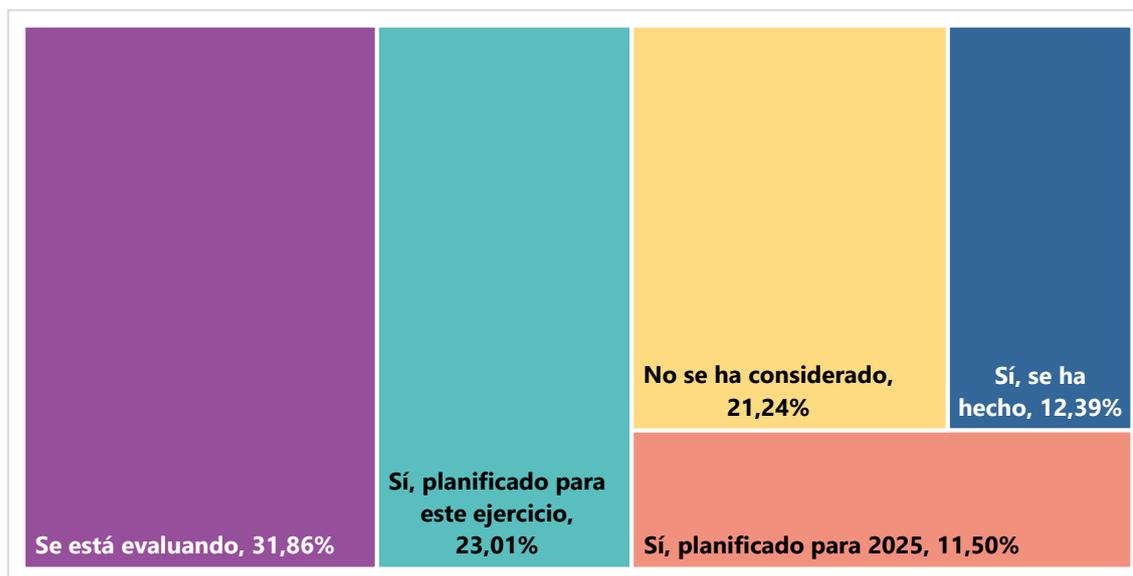
En 2024, se observa un aumento en la percepción de la necesidad de controles sobre los **sesgos en IA**. Los puntos clave son:

1. **Sesgos regulatorios:** Crece la conciencia sobre la importancia de los **controles regulatorios** (60,34% frente a 56,18% en 2023), lo que refleja un enfoque más fuerte hacia la regulación para mitigar los sesgos en IA.
2. **Transparencia de algoritmos:** La preocupación por la **falta de transparencia** sigue siendo significativa (43,10% frente a 44,94% en 2023), aunque muestra una ligera disminución, lo que sugiere que algunas organizaciones confían en otros métodos para abordarlo.
3. **Riesgos operacionales:** Los **riesgos operacionales** relacionados con los sesgos han disminuido levemente (53,45% frente a 56,18% en 2023), indicando un enfoque creciente en regulaciones en lugar de en los riesgos internos.

4. **Impacto en derechos colectivos:** La preocupación por los sesgos que afectan los **derechos de colectivos** ha disminuido (43,10% frente a 48,31% en 2023), posiblemente debido a la percepción de que ya existen controles adecuados en este ámbito.
5. **Resistencia a implementar controles:** Ha aumentado el porcentaje de quienes no consideran necesario implementar controles sobre los sesgos (12,93% frente a 6,74% en 2023), lo que podría reflejar una falta de conciencia o resistencia en algunos sectores.

En resumen, hay una mayor inclinación hacia controles regulatorios, persiste la preocupación por la falta de transparencia y los riesgos operacionales. Sin embargo, el aumento de quienes no consideran necesario implementar controles muestra que aún queda trabajo por hacer en la concienciación sobre los sesgos en IA.

2.1.8. ¿Ha realizado o tiene previsto hacer un inventario de modelos y sistemas IA en su organización?



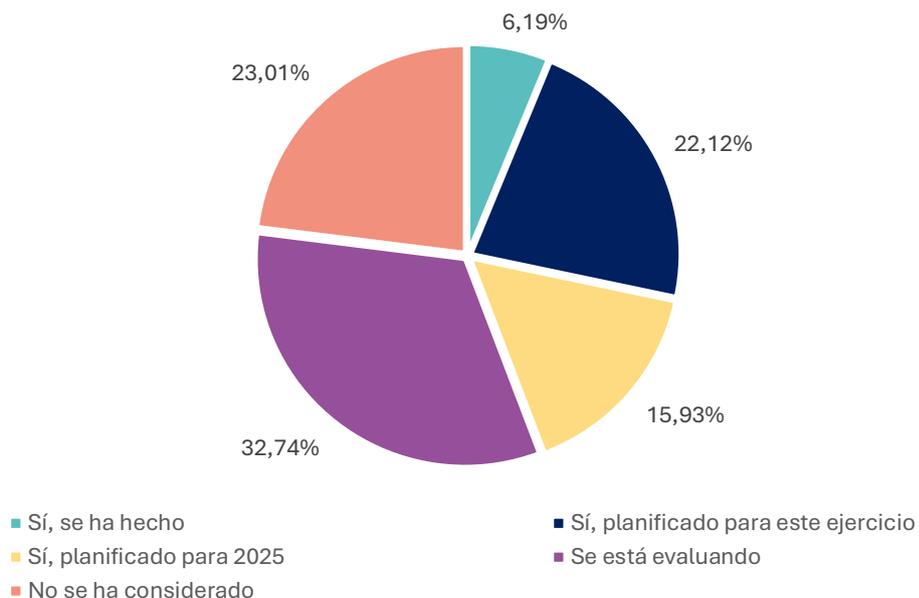
Un **12,39%** de las organizaciones ya ha realizado un inventario de modelos y sistemas de IA, mientras que un **23,01%** tiene previsto hacerlo en 2024 y un **11,50%** lo planea para 2025. Esto refleja un creciente interés en la gestión y control de los sistemas de IA, aunque la mayoría aún está en fases iniciales de planificación.

Un **31,86%** se encuentra evaluando esta posibilidad, lo que sugiere que muchas organizaciones están considerando los beneficios de tener un inventario, pero sin un compromiso definido. Por otro lado, el **21,24%** de las organizaciones no tiene planes de realizar un inventario, lo cual puede indicar una falta de recursos, de madurez en la implementación de IA, o una subestimación de la importancia de gestionar estos activos de manera formal.

2.1.9. ¿Ha realizado o tiene previsto hacer una evaluación de impacto según establece el Reglamento Europeo de Inteligencia Artificial?

El análisis muestra que, aunque una parte significativa de las organizaciones está trabajando en la evaluación de impacto o la tiene planeada, aún hay un porcentaje notable (23%) que no ha considerado este paso. Esto podría indicar una falta de preparación o de comprensión de la importancia del reglamento, lo que podría llevar a dificultades en el futuro.

La evaluación de impacto es un componente crucial para asegurar el cumplimiento con los estándares éticos y de seguridad establecidos por el Reglamento Europeo de Inteligencia Artificial, por lo que las organizaciones deben priorizarla para evitar problemas regulatorios.



2.1.10. ¿Qué otros aspectos considera que deberían tratarse con relación a riesgos en la adopción y gobierno de la IA?

La adopción de la inteligencia artificial (IA) presenta diversos riesgos que deben ser gestionados para asegurar su uso ético y responsable. Entre los aspectos más destacados, la **protección de datos** y la **confidencialidad** son esenciales, dado que la IA maneja grandes cantidades de información sensible. La implementación de medidas de **seguridad** adecuadas y la **validación del output de la IA** son fundamentales para garantizar la transparencia y fiabilidad de los sistemas.

También es crucial asegurar que la IA se utilice de manera **ética**, evitando **sesgos** y respetando los derechos humanos. La **supervisión humana** es necesaria para prevenir que los sistemas autónomos tomen decisiones fuera de los valores éticos establecidos.

Además, la **gobernanza interna** de la IA debe estar claramente definida, con líderes responsables que coordinen su implementación y supervisión en la organización. Es importante que las **PYMEs** y las organizaciones en general cuenten con formación adecuada sobre IA para gestionar estos riesgos.

Finalmente, el **riesgo de dependencia de terceros** también debe ser cuidadosamente evaluado para garantizar la seguridad y cumplimiento de las normativas.

En resumen, un enfoque integral que abarque la seguridad, la ética, la formación y la supervisión es fundamental para el uso responsable de la IA.

AUTORES

Participantes	Angel Pérez Beatriz García
Diseño	Lydia García
Maquetación	Beatriz García



CONTACTA CON NOSOTROS

Si estás interesado/a en colaborar con nosotros
o necesitas más información sobre nuestros
proyectos, escríbenos a:
proyectos@ismsforum.es