Utilizar la IA de forma segura

La guía de liderazgo para convertir la inversión en IA en valor empresarial

A Global Leader in
Technology Services

Experis®
ManpowerGroup



©Experis 2026 Utilizar la IA de forma segura

Contenidos

1 Introducción.....3-4

Resumen ejecutivo..... 3
Prólogo: La innovación en un dilema 4

2 La transformación del negocio con IA.....5-9

La ilusión de una IA "lista para usar"..... 5-7
La nueva vulnerabilidad de las empresas 7
La gobernanza se convierte en una ventaja competitiva 8-9

3 Crear una diferencia competitiva..... 10-13

Rediseñar las organizaciones para la era de los agentes 10-12
Spotlight: ExcelerateWorkflow con tecnología de IBM® watsonx Orchestrate™.....11
El factor humano en la transformación de la IA..... 12-13

4 Guía para líderes tecnológicos 14-16

Cinco acciones que los líderes tecnológicos deberían tomar ahora.....14-15
La experiencia global de Experis 16

Introducción



Resumen ejecutivo

La inversión en IA se está acelerando, pero muchas organizaciones siguen teniendo dificultades para convertir la experimentación en un valor comercial medible: La brecha no es simplemente tecnológica. Tiene su origen en la alineación comercial, la disponibilidad de datos, la ciberseguridad, la gobernanza, la capacidad del personal y la habilidad para integrar la IA en la forma en que realmente se lleva a cabo el trabajo.

La idea de una transformación empresarial basada en la IA "lista para usar" es un mito: Los proyectos que funcionan bien en entornos piloto suelen estancarse cuando se topan con sistemas heredados, datos fragmentados, responsabilidades poco claras, requisitos de seguridad y flujos de trabajo del mundo real. La tecnología por sí sola no puede superar estas barreras.

A medida que la IA se va integrando cada vez más en las empresas, cada nuevo modelo, agente, conjunto de datos e integración genera tanto oportunidades como riesgos. Las organizaciones deben proteger una amenaza de ataque cada vez mayor, establecer responsabilidades claras, rediseñar los flujos de trabajo y desarrollar las habilidades necesarias para que las personas puedan utilizar y supervisar la IA de manera eficaz. Sin estos fundamentos, los proyectos piloto con potencial tienen dificultades para escalar y las inversiones no logran generar todo su rendimiento.

La siguiente etapa en la adopción de la IA requiere un cambio de enfoque. La pregunta ya no es si las organizaciones deben invertir en IA, sino cómo los líderes pueden implementar la IA de manera segura, responsable y eficaz. Un estudio de Experis hace hincapié en este desafío. Si bien el 66% de los profesionales de TI afirma que sus organizaciones están aumentando la inversión en IA, solo el 9% señala que la IA está totalmente integrada en las operaciones y la estrategia.[1]

Prólogo: La innovación en un dilema

En nuestras conversaciones recientes con clientes, ha quedado claro que la IA ha dejado atrás la etapa experimental. En todos los sectores, las organizaciones están invirtiendo fuertemente en IA, automatización, infraestructura en la nube y sistemas cada vez más autónomos. **Para muchos equipos ejecutivos, la pregunta ya no es, sí invertir, sino cómo convertir esa inversión en resultados.**

Ahí es donde la ambición suele ir por delante de la ejecución. Los modelos y las herramientas están mejorando rápidamente, pero la implementación en las empresas sigue siendo difícil. Los resultados comerciales son irregulares, mientras que la seguridad, la gobernanza y la preparación de la fuerza laboral suelen quedarse rezagadas respecto a la tecnología.

Un proyecto piloto exitoso no es lo mismo que una solución escalable. En las operaciones cotidianas, la IA debe lidiar con datos inconsistentes, sistemas heredados, requisitos de gobernanza, una adopción desigual y un panorama de amenazas que cambia rápidamente. **El mayor obstáculo proviene cada vez más de los sistemas que rodean a la tecnología, no de la tecnología en sí misma.**

Este desafío se intensificará a medida que la IA adquiera mayor autonomía. Los sistemas no solo generarán contenido o responderán preguntas, sino que también tomarán decisiones, coordinarán tareas, interactuarán con los sistemas empresariales y realizarán acciones que antes estaban a cargo de las personas. Los líderes necesitan una supervisión más sólida, una rendición de cuentas más clara y una fuerza laboral capacitada para utilizar estas herramientas de manera responsable.

Las organizaciones que están avanzando consideran la IA como una transformación empresarial, no como otra implementación tecnológica más. Vinculan las iniciativas a las prioridades de negocio, establecen la gobernanza desde el inicio, integran la seguridad en la resiliencia operativa, rediseñan los flujos de trabajo en lugar de automatizar los que no funcionan, e invierten en las personas al mismo tiempo que en la tecnología.

Este reporte explora cómo las organizaciones pueden navegar la siguiente fase de la transformación de la IA. Basándonos en investigaciones de líderes tecnológicos de todo el mundo, así como en perspectivas más amplias del mercado sobre la adopción de la IA, la ciberseguridad, la gobernanza y el cambio organizacional, examinamos las decisiones de liderazgo que determinarán si las inversiones en IA se convierten en ventajas competitivas sostenibles o en experimentos costosos.

El futuro de la IA no pertenecerá a las organizaciones que cuenten con los modelos más avanzados. Pertenecerá a aquellas organizaciones que puedan integrar esos modelos en el flujo de trabajo, gestionarlos de manera responsable, protegerlos de manera eficaz y permitir que las personas los utilicen con confianza.



Kye Mitchell
Líder de marca de Experis en EE.UU.



James Hallahan
Líder de marca de Experis en Europa

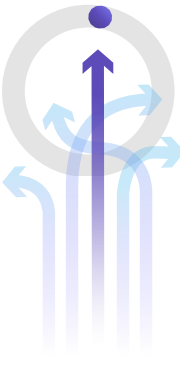
La transformación del negocio con IA



La ilusión de una IA "lista para usar"

Las herramientas de IA pueden generar resultados impresionantes en un entorno controlado, pero las operaciones empresariales son menos tolerantes. **Un sistema de producción debe funcionar con datos reales, aplicaciones existentes, controles establecidos, comportamientos variables de los usuarios y procesos de negocio que rara vez se diseñaron pensando en la IA. La dificultad no radica en demostrar que un modelo puede realizar una tarea, sino en construir el sistema que lo rodea y que permita que el modelo funcione de manera confiable, repetida y con un nivel de riesgo aceptable.**

Esa diferencia ayuda a explicar la brecha cada vez mayor entre la actividad de IA y su valor. Un estudio global reciente reveló que solo el 5% de las empresas generaba valor de IA a gran escala. Otro 35% se encontraba en proceso de expansión y comenzaba a generar valor, mientras que el 60% reportó un valor insignificante a pesar de una inversión sustancial.[2] El grupo líder no se limitó a automatizar más tareas. Desarrolló la estrategia, el modelo operativo, el talento, la tecnología y las capacidades de datos necesarias para transformar el trabajo principal.



Solo 5% de las empresas generaba valor con la IA a gran escala.

La perspectiva de un CIO sobre el estado actual de la IA a nivel global[1]

Implementación
Estamos integrando activamente la IA en algunas áreas
32%

Exploración
Estamos investigando y llevando a cabo proyectos piloto
30%

Escalabilidad
La IA se está implementando en toda la organización
19%

No hemos comenzado
Aún no hemos comenzado a explorar la integración de la IA
10%

Totalmente integrada
La IA está integrada en nuestras operaciones y nuestra estrategia
9%

Nuestra propia investigación muestra la misma tensión desde la perspectiva de los líderes tecnológicos. La mayoría de los líderes tecnológicos de alto nivel afirman que sus empresas están aumentando la inversión en IA, y el 60% señala que sus organizaciones están implementando la IA al menos en algunas áreas. Sin embargo, solo el 9% afirma que la IA está totalmente integrada en las operaciones y la estrategia.[1] Más de la mitad reporta un retorno positivo de la inversión en IA, pero las diferencias entre empresas de distintos tamaños, sectores y mercados sugieren que los retornos iniciales no siempre se traducen en resultados a escala empresarial.

Comienza con el negocio, no con el modelo

Un caso de uso técnicamente viable puede seguir siendo una inversión comercial poco sólida. Los líderes deben saber qué flujo de trabajo cambiará, quién es responsable del resultado, qué riesgo está asumiendo la organización y cómo se medirá el valor. Sin esas decisiones, los proyectos piloto tienden a desarrollarse en torno al entusiasmo local en lugar de a las prioridades de la empresa.

La necesidad de una mayor alineación es evidente. **Casi la mitad de los líderes tecnológicos, el 48%, considera ahora que alinear la estrategia de TI con los objetivos de negocio es una de las responsabilidades más importantes del CIO, frente al 34% en 2025.** E A pesar de ello, la alineación reportada entre la estrategia de negocio y la de tecnología se mantuvo estadísticamente sin cambios en el 77%, en comparación con el 80% del año anterior. Por otro lado, el 44% señala que mantenerse al día con los rápidos cambios tecnológicos es uno de los principales obstáculos, y el 61% de los CIO afirma que los líderes de alto nivel no conocen lo suficiente sobre el rol y lo que este requiere.[1]

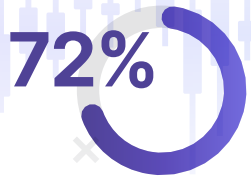
Prioridades globales de los CIOs para 2026[1]

1. Alinear las TI con la estrategia empresarial
2. Mejorar la ciberseguridad
3. Transformación digital
4. Reducción de costos
5. Talento tecnológico
6. Cumplimiento normativo

Estos hallazgos apuntan a un problema de liderazgo. **La IA no puede ser responsabilidad exclusiva del departamento de TI cuando su impacto se extiende a las operaciones, las finanzas, el manejo de riesgos, el área legal, la experiencia del cliente y la fuerza laboral. Los líderes empresariales deben asumir la responsabilidad conjunta de la selección de los problemas, el rediseño de los flujos de trabajo y la medición de los resultados.** Los líderes tecnológicos deben traducir las posibilidades técnicas en decisiones que el resto de la empresa pueda poner en práctica.

Modernizar las bases para la escalabilidad

Los datos y la arquitectura también determinan si los casos de uso prometedores sobreviven a la fase de producción. El estudio de IBM sobre directores ejecutivos para 2025 reveló que el 68% de los directores ejecutivos encuestados consideraba que una arquitectura de datos integrada en toda la empresa era fundamental para la colaboración interfuncional, mientras que el 72% consideraba que los datos propios eran clave para aprovechar el valor de la IA generativa.[3] Al mismo tiempo, la mitad afirmó que la inversión apresurada había dejado a sus organizaciones con una tecnología fragmentada y desconectada. Solo el 16% de las iniciativas de IA se había implementado a nivel de toda la empresa.



72% **de los CEOs dicen que los datos propios son la clave para aprovechar el valor de la IA generativa.[3]**

Para los líderes, esto hace que la modernización forme parte de la estrategia de IA, en lugar de ser un programa de infraestructura independiente. Las cuestiones prácticas incluyen si se puede acceder a los datos con los permisos adecuados, si los modelos pueden conectarse de manera segura a los sistemas centrales, si se pueden monitorear los resultados y si la organización puede cambiar o eliminar una plataforma sin interrumpir el trabajo crítico.

La nueva vulnerabilidad de las empresas

A medida que la IA se integra en las operaciones centrales, la ciberseguridad se expande más allá de las redes, los dispositivos y las aplicaciones. **Las organizaciones también deben proteger los modelos, los datos de entrenamiento y recuperación, las indicaciones, las identidades de los agentes, las acciones automatizadas, las integraciones y los entornos en la nube que los conectan. Una vulnerabilidad en cualquiera de estas capas puede afectar la confianza de todo el flujo de trabajo.**

Por eso, la ciberseguridad debe considerarse una condición indispensable para el crecimiento de la IA. Según nuestra propia investigación, el 78% de los líderes tecnológicos de alto nivel afirmó que sus organizaciones están aumentando la inversión en ciberseguridad. La ciberseguridad es también la habilidad tecnológica más importante, citada por el 46%, por delante de la IA y el aprendizaje automático, con un 37%, y la computación en la nube, con un 31%. Sin embargo, la preparación no avanza al mismo ritmo. Solo el 72% afirma que su estrategia de riesgo está alineada con la preparación en materia de ciberseguridad, lo que representa una disminución con respecto al 77% en 2025. La misma proporción realiza regularmente cursos de capacitación en ciberseguridad, cifra que apenas ha variado con respecto al 74% del año anterior.[1]

Un nuevo enfoque de los CIO en materia de ciberseguridad

- 78% está aumentando su presupuesto de ciberseguridad
- La ciberseguridad es la habilidad más demandada entre el talento de TI
- La ciberseguridad sigue siendo la principal preocupación que quita el sueño a los CIO

Los agentes elevan el nivel de riesgo

El cambio hacia la IA agentiva introduce una nueva categoría de riesgo, ya que los agentes pueden moverse entre sistemas y tomar medidas. **El riesgo principal ya no se limita a si una respuesta es inexacta. Los líderes deben preguntarse qué se le permite hacer al sistema, a qué datos puede acceder, cómo se gestiona su identidad y qué sucede cuando una acción es inesperada.**

Por lo tanto, los controles de acceso deben reflejar la tarea, no simplemente al usuario o la aplicación. Los agentes no deben heredar permisos amplios simplemente porque así la implementación sea más fácil. Las organizaciones también necesitan trazabilidad a través de las solicitudes, las fuentes de datos, las decisiones, las acciones y las excepciones, para que los equipos de seguridad puedan comprender qué sucedió e intervenir cuando sea necesario.

La IA es una herramienta de seguridad y un desafío de seguridad

Los equipos de seguridad también están utilizando la IA para aumentar la velocidad y la eficiencia de la defensa. **Una investigación reciente reveló que el 91% de los encuestados estaba utilizando o probando soluciones de ciberseguridad basadas en IA, y el 84% afirmó que las herramientas de seguridad mejoradas con IA estaban ayudando a los equipos a ser más eficaces y eficientes.** Al mismo tiempo, el 86% informó de al menos una violación de seguridad en los últimos 12 meses, y el 56% señaló la falta de habilidades en ciberseguridad como una de las principales causas de dichas fallas.[4]



56%

de los líderes tecnológicos afirma que la falta de habilidades en ciberseguridad es la principal causa de dichas fallos.[4]

La lección no es frenar la adopción de la IA, sino que los líderes tecnológicos deben integrarla en la ingeniería de seguridad desde el principio. **Los responsables de seguridad deben participar cuando se seleccionan los casos de uso, se diseñan las rutas de datos, se evalúan los proveedores y se modifican los flujos de trabajo.** Los controles que se agregan después de la implementación tienden más a generar retrasos, soluciones provisionales y desconfianza.

Hacer de la seguridad una disciplina operativa compartida

La seguridad de la IA no es responsabilidad exclusiva del director de seguridad de la información (CISO). Los líderes empresariales deben definir los resultados aceptables y las excepciones. Los equipos de tecnología deben desarrollar y mantener la arquitectura. Los equipos legales y de riesgos deben traducir las obligaciones en controles aplicables. Los líderes de personal deben apoyar la capacitación y la adopción. Los empleados deben comprender cuándo y cómo cuestionar, escalar o anular las decisiones respaldadas por la IA.

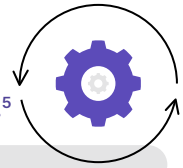
La gobernanza se convierte en una ventaja competitiva

A menudo se describe a la gobernanza como una limitación para la innovación. En la práctica, una gobernanza débil genera incertidumbre, retrasos, revisiones duplicadas y decisiones inconsistentes. **Una gobernanza sólida ofrece a los equipos un camino reproducible desde la idea hasta la producción. Aclara qué riesgos requieren ser escalados, quién tiene la autoridad para aprobar o detener una implementación y cómo se supervisarán los sistemas después del lanzamiento.**

Una investigación reciente sobre empresas reveló que la regulación y el riesgo se habían convertido en la principal barrera para el desarrollo y la implementación de la IA generativa. La mayoría de las empresas encuestadas esperaban que menos del 30% de sus experimentos alcanzaran escala completa en un plazo de seis meses, mientras que el 69% esperaba que tomara al menos un año implementar una estrategia integral de gobernanza.[5]

El mayor obstáculo es una gobernanza eficaz

50% de los líderes afirma que la mayor dificultad para avanzar es la implementación de los principios de IA responsable en los procesos operativos.[5]





Otra encuesta reciente sobre IA responsable relacionó directamente la gobernanza con el valor. El 58% de los ejecutivos afirmó que las iniciativas de IA responsable mejoran el retorno de inversión (ROI) y la eficiencia organizacional; el 55% señaló beneficios para la experiencia del cliente y la innovación, y el 51% mencionó una mayor ciberseguridad y protección de datos. El reto radicaba en la puesta en práctica, ya que el 50% identificó el paso de los principios a procesos escalables como su mayor obstáculo.[5]

La gobernanza debe seguir avanzando después del lanzamiento

Los controles tradicionales suelen poner énfasis en la aprobación previa a la implementación. La IA requiere la misma atención después de la implementación, ya que los modelos, los datos, los usuarios y las condiciones operativas cambian. La gobernanza debe incluir monitoreo continuo, ciclos de retroalimentación, respuesta ante incidentes, documentación, revisión periódica y normas claras para la modificación o la descontinuación.

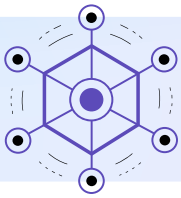
Los sistemas autónomos hacen que esto sea especialmente importante. Cuanta más autonomía tenga un sistema, con mayor precisión deberán definir los líderes su alcance, los puntos de escalación y la supervisión humana. **La gobernanza debe responder a quién le corresponde la responsabilidad del resultado, quién puede inspeccionar el sistema, detenerlo y qué evidencia se requiere antes de que el sistema pueda reanudar su funcionamiento.**

Aumento de la tensión en torno a la soberanía

La soberanía de los datos agrega otra capa de complejidad. **81% de los líderes tecnológicos describen la soberanía digital como una prioridad alta o crítica. Al mismo tiempo, el 67% espera que sus organizaciones aumenten la inversión en la prestación de servicios de TI en el extranjero y en países vecinos.**[1] Esta tensión es comprensible, ya que los líderes empresariales desean un mayor control sobre los datos y la infraestructura, al tiempo que aprovechan la tecnología, las habilidades y la capacidad de prestación de servicios a nivel global.

La respuesta no es la independencia tecnológica total. Se trata de tener claridad sobre qué debe permanecer bajo control directo, qué se puede confiar a socios, dónde se pueden almacenar o procesar los datos y cómo la organización puede mantener la continuidad si cambia un proveedor, una plataforma, una regulación o una situación geopolítica.

Aumento de la soberanía



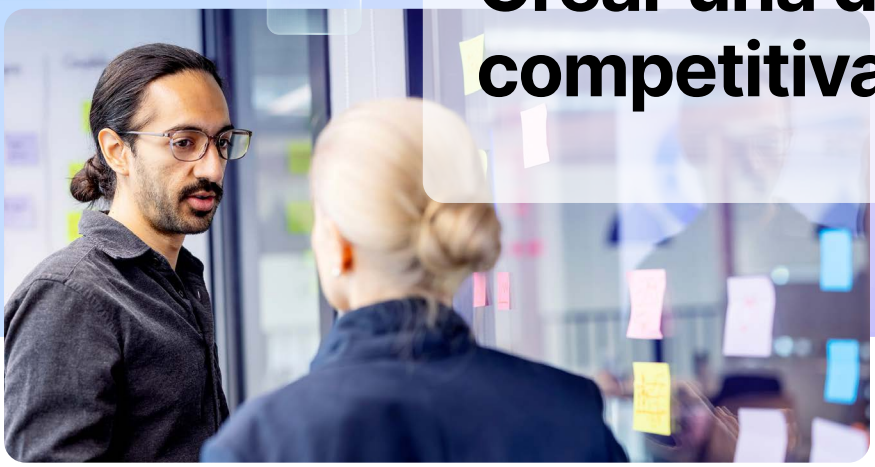
81% de los CIOs describen la soberanía digital como una prioridad alta o crítica.[1]

Considera la regulación como un requisito de diseño

La Ley de IA de la Unión Europea muestra por qué la gobernanza debe integrarse en el diseño de las operaciones. La regulación sigue un enfoque basado en el riesgo e incluye requisitos específicos que afectan a la IA en el lugar de trabajo y ámbito laboral. Su marco de sanciones alcanza hasta 35 millones de euros o el 7% de la facturación anual global para las infracciones más graves, con niveles adicionales para otras obligaciones e información poco precisa.[6]

Para las multinacionales, el cumplimiento no puede reducirse a una revisión legal de una sola vez. Los equipos necesitan una forma práctica de vincular las obligaciones locales con los inventarios de sistemas, las clasificaciones de riesgo, las prácticas de datos, la supervisión humana, la documentación y la gestión de proveedores.

Crear una diferencia competitiva

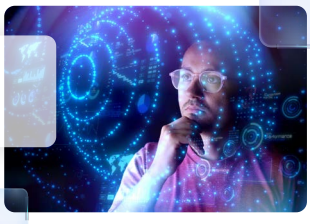


Rediseñar las organizaciones para la era de los agentes

La IA puede acelerar el trabajo, pero la velocidad no mejora un proceso que está fragmentado, duplicado o mal gestionado. Las organizaciones que incorporan agentes sobre las ineficiencias existentes pueden generar confusión más rápidamente. El primer paso es comprender cómo se mueve actualmente el trabajo a través de las funciones, los sistemas y los puntos de decisión.

Existen investigaciones más recientes que muestran por qué es importante el rediseño del flujo de trabajo. **Las empresas preparadas para el futuro van más allá de la automatización aislada y reestructuran las funciones centrales. Persiguen objetivos de IA a largo plazo, adoptan modelos operativos que priorizan la IA, se aseguran de contar con el talento necesario y utilizan tecnología y datos adecuados para cada propósito.** Un estudio estima que el 70% del valor potencial de la IA se concentra en las funciones comerciales centrales, en lugar de actividades de apoyo.[2]

70% **del valor potencial de la IA se centra en las funciones clave del negocio, más que en las actividades de apoyo.**



Pasar de la automatización de tareas a la coordinación

La IA agentiva cambia el enfoque de la automatización de tareas individuales a la coordinación del trabajo entre personas y sistemas digitales. Esto requiere una capa de coordinación que pueda hacer visible el trabajo, dirigirlo adecuadamente, aplicar controles y medir los resultados. También requiere una responsabilidad humana explícita.

Los líderes deben definir qué decisiones siguen estando a cargo de las personas, cuáles cuentan con la asistencia de la IA y cuáles pueden ser ejecutadas por un agente dentro de los límites establecidos. También deben determinar cómo se devuelven las excepciones a las personas, cómo se evalúa el desempeño y cómo las lecciones aprendidas del uso real mejoran el flujo de trabajo con el tiempo.

Spotlight

ExcelerateWorkflow con tecnología de IBM® watsonx Orchestrate™

Hoy en día, a la mayoría de las organizaciones no les cuesta identificar oportunidades relacionadas con la IA. El reto radica en implementar la IA a gran escala. Muchas iniciativas de IA se muestran prometedoras en las fases piloto, pero se estancan antes de generar un valor comercial sostenible. El reto rara vez radica en la tecnología en sí misma. Con mayor frecuencia, las organizaciones se enfrentan a flujos de trabajo fragmentados, sistemas desconectados, responsabilidades poco claras, requisitos de gobernanza y obstáculos para la adopción por parte del personal, lo cual impide que la IA se integre en las operaciones cotidianas.

La siguiente etapa de la transformación hacia la IA requiere algo más que implementar nuevas herramientas. Requiere integrarla en la forma en que se realiza el trabajo. **Para ayudar a las organizaciones a cerrar esta brecha, Experis desarrolló ExcelerateWorkflow, con tecnología de IBM® Watsonx Orchestrate™, con el fin de ayudar a las empresas a pasar de la fase de experimentación a la de ejecución.**

Diseñado para facilitar la coordinación de flujos de trabajo entre las funciones empresariales y tecnológicas, ExcelerateWorkflow ayuda a las organizaciones a integrar agentes de IA en los entornos operativos existentes con mayor visibilidad, gobernanza y supervisión humana. En lugar de centrarse en oportunidades de automatización aisladas, la solución reúne a personas, sistemas y agentes de IA para coordinar el trabajo, reducir los roces operativos y facilitar una ejecución más eficaz y responsable.

IBM® watsonx Orchestrate™ ofrece una plataforma de gestión y organización de agentes que permite a las empresas descubrir, gestionar y organizar tanto agentes de IA nativos como desarrollados externamente, con capacidades integradas de gobernanza, controles y seguridad. Experis complementa esta tecnología con experiencia en implementación, transformación de flujos de trabajo, servicios de integración, capacitación del personal y apoyo en la gestión del cambio. En conjunto, estas capacidades ayudan a los clientes a poner en práctica la IA de manera segura y a gran escala, alineada con los objetivos de negocio y los requisitos operativos del mundo real.

Este enfoque refleja un cambio más amplio que se está produciendo en todos los sectores. Las organizaciones están yendo más allá de los casos de uso aislados de la IA y se preguntan cómo esta puede mejorar el desempeño empresarial en todas las funciones y flujos de trabajo. El éxito depende cada vez más de la integración de la tecnología, la gobernanza, las personas y los procesos en un modelo operativo unificado.

Al combinar experiencia tecnológica, capacidades de transformación de la fuerza laboral y modelos de entrega escalables, **Experis ayuda a las organizaciones a acelerar la adopción de la IA, establecer una responsabilidad clara, generar confianza en los flujos de trabajo impulsados por la IA y obtener resultados comerciales medibles a partir de sus inversiones.**

La IA genera potencial. El valor empresarial proviene de integrar con éxito ese potencial en el flujo de trabajo.

IBM
Gold Partner

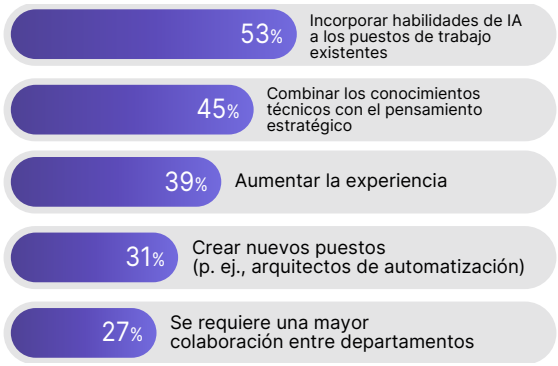
IBM, el logotipo de IBM, watsonx y watsonx Orchestrate son marcas comerciales o marcas registradas de International Business Machines Corporation.



Rediseñar los puestos con el flujo de trabajo

El cambio en el modelo operativo ya está transformando el trabajo en el ámbito tecnológico. Nuestra investigación revela que el 53% de las organizaciones está incorporando habilidades de IA en los puestos existentes, el 45% está combinando la experiencia técnica con el pensamiento estratégico y el 39% está aumentando la versatilidad de los puestos en múltiples áreas. Casi un tercio está creando nuevos puestos, como especialistas en ética de datos y arquitectos de automatización. Son mucho menos las que informan haber eliminado puestos para reasignar personal o reducir costos.[1]

Las mejores estrategias de los CIO para potenciar la IA con talento tecnológico[1]



Este patrón sugiere que la expansión de la IA depende menos de la reducción de personal que de la redefinición de responsabilidades. Los trabajadores necesitan claridad sobre cómo la IA modifica las decisiones, los traspasos de tareas, la rendición de cuentas y las expectativas de servicio. Los gerentes deben saber cómo evaluar el desempeño cuando los resultados son producto de una combinación de personas y sistemas.

Top 5 de habilidades más buscadas por los CIOs[1]

1. Ciberseguridad
2. IA y machine learning
3. Computación en la nube
4. Desarrollo de Software
5. Colaboración y trabajo en equipo

El factor humano en la transformación de la IA

La cuestión del talento va más allá de si una organización puede contratar a suficientes especialistas en IA. Para lograr una escalabilidad segura se requiere un conjunto integrado de capacidades técnicas, de gobernanza, de liderazgo y de la fuerza laboral. Esas capacidades deben estar disponibles allí donde se toman las decisiones, no aisladas en un pequeño centro de excelencia.

Nuestra reciente investigación con CIOs muestra la amplia gama de habilidades que necesitan los equipos de TI en todo el mundo. **La ciberseguridad es la habilidad tecnológica más mencionada, con un 46%, seguida por la IA y machine learning, con un 37%, y la computación en la nube, con un 31%.** La colaboración, el desarrollo de software, DevOps, la adaptabilidad, la resolución de problemas, la comunicación y el liderazgo también figuran entre las prioridades. Esta combinación refleja la realidad de que la IA empresarial es tanto un sistema técnico como un programa de cambio comercial.

Desarrollar cuatro dimensiones de capacidad

1

Capacidad técnica:

IA, datos, nube, ciberseguridad, ingeniería de software, arquitectura, pruebas e integración de plataformas.

2

Capacidad de gobernanza:

Clasificación de riesgos, políticas, monitoreo, cumplimiento, auditoría, evaluación de proveedores e IA responsable.

3

Capacidad de liderazgo:

Alineación comercial, decisiones de inversión, rendición de cuentas, comunicación y liderazgo para el cambio.

4

Capacidad de la fuerza laboral:

Conocimientos básicos sobre IA, adopción, confianza, colaboración, aprendizaje continuo y supervisión humana.

Cerrar la brecha de adopción

Un sistema puede implementarse técnicamente sin que se adopte de manera significativa. Experis descubrió que la alineación entre la implementación de nuevas tecnologías y la adopción por parte de los trabajadores disminuyó en 2026. **Cuando los equipos no comprenden cómo una herramienta se adapta a su trabajo, de qué siguen siendo responsables o cuándo deben cuestionar sus resultados, la adopción se vuelve inconsistente y el riesgo aumenta.**

Por lo tanto, la capacitación debe ir más allá de las demostraciones de funciones. Los empleados necesitan practicar la aplicación de la IA en flujos de trabajo reales, evaluar los resultados, reconocer las limitaciones, proteger los datos y escalar las inquietudes. Los gerentes necesitan apoyo para rediseñar los roles y las métricas. Los líderes necesitan un lenguaje común para hablar de valor, riesgo y supervisión humana.

Desarrollar líderes de manera tan estratégica como a los especialistas

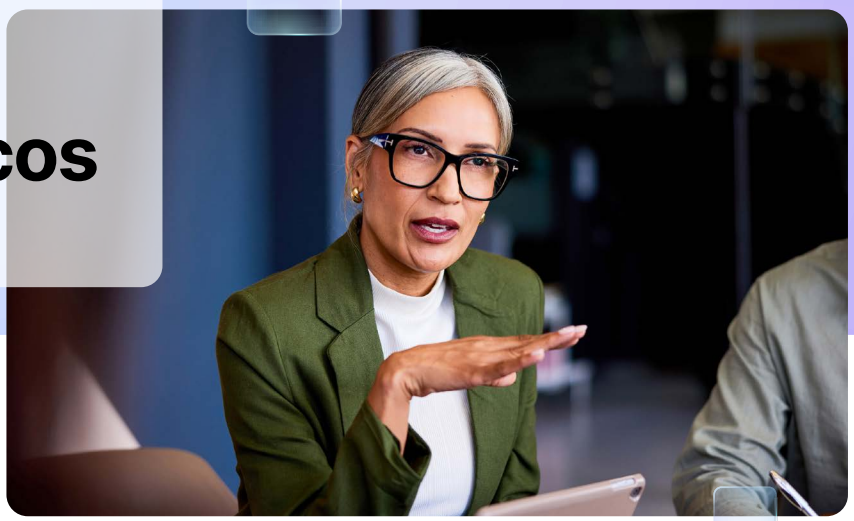
La formación de líderes merece la misma atención. Solo el 58% de las organizaciones del estudio de Experis lleva a cabo regularmente programas para desarrollar futuros líderes tecnológicos, lo que representa una disminución con respecto al 63% registrado en 2025.[1] Esa disminución se produce en un momento en que los puestos de liderazgo requieren una combinación más compleja de criterio técnico, comprensión del negocio, comunicación, gobernanza y capacidad de cambio.



Solo el 58% de las organizaciones forma a futuros líderes tecnológicos, lo que representa una disminución con respecto al 63% en 2025.

Las organizaciones deben combinar el desarrollo interno, la contratación selectiva, los socios especializados y los modelos de prestación de servicios flexibles. **El objetivo no es cubrir cada capacidad con un puesto permanente, sino garantizar que la empresa pueda acceder a la experiencia adecuada, mantener la rendición de cuentas y transferir conocimientos a medida que evolucionan la tecnología y los riesgos.**

Guía para líderes tecnológicos



Cinco acciones que los líderes tecnológicos deben tomar ahora

El camino desde la experimentación con IA hasta el valor empresarial requiere acciones específicas. **Estas 5 prioridades ofrecen a los líderes tecnológicos una hoja de ruta práctica para alinear la inversión con los resultados comerciales, fortalecer la seguridad y la gobernanza, rediseñar el trabajo para la IA y desarrollar las capacidades necesarias para escalar con confianza.**

En conjunto, estas acciones crean un sistema empresarial para la escalabilidad segura de la IA. Vinculan la inversión con los resultados, la innovación con el control, la automatización con la rendición de cuentas y la tecnología con las personas que le dan valor.

1. **Alinear la inversión en IA con los resultados del negocio**
2. **Considerar la ciberseguridad como una prioridad crítica para el negocio**
3. **Establecer un marco de gobernanza antes de expandirse**
4. **Rediseñar los flujos de trabajo antes de implementar agentes**
5. **Invertir en capacidad, no solo en tecnología**

"Decir que vamos más rápido o que la calidad es mejor no es ROI. Si ahorramos tiempo gracias a la IA, la verdadera pregunta es: ¿qué vamos a hacer con ese tiempo? El valor de un proyecto debe medirse en términos de ingresos o rentabilidad." – *CIO, sector de artículos de lujo, Francia*



1. Alinea la inversión en IA con los resultados del negocio:

Exigir que cada iniciativa importante identifique al responsable del negocio, el flujo de trabajo, el resultado, la medida de adopción, el responsable del riesgo y la métrica de valor antes de pasar a la fase de implementación a gran escala.

¿Qué resultado comercial cambiará?

¿Quién es responsable del resultado después de la implementación?

¿Qué datos justificarán que se siga invirtiendo?



2. Considera la ciberseguridad como una prioridad crítica para el negocio:

Extender el diseño de seguridad a todos los modelos, datos, agentes, identidades, integraciones, proveedores y acciones automatizadas.

¿A qué puede acceder y qué puede hacer el sistema?

¿Cómo se detectará un comportamiento inesperado?

¿Quién tiene la autoridad para intervenir?



3. Establece un marco de gobernanza antes de expandirse:

Realiza un proceso repetible para la clasificación, la aprobación, el seguimiento, la escalación y la baja.

¿Qué decisiones requieren revisión humana?

¿Qué documentación y pruebas se requieren?

¿Cómo se adaptarán los controles después del lanzamiento?



4. Rediseña los flujos de trabajo antes de implementar agentes:

Mapea el trabajo de principio a fin y elimina la fragmentación antes de incorporar la autonomía.

¿A qué hora termina el trabajo hoy?

¿Qué actividades deberían ser dirigidas por personas, asistidas por IA o ejecutadas por agentes?

¿Cómo se notificarán las excepciones a las personas?



5. Invierte en capacidad, no solo en tecnología

Desarrolla un conjunto de capacidades técnicas, de gobernanza, de liderazgo y de la fuerza laboral mediante el desarrollo interno y la experiencia externa.

¿Qué capacidades es estratégico tener?

¿En qué áreas pueden los socios acelerar el progreso?

¿Cómo se llevará a cabo la transferencia de conocimientos y el aprendizaje continuo?

La experiencia global de Experis

A medida que la IA transforma el panorama de la ciberseguridad, las organizaciones se enfrentan a un doble desafío: aprovechar el potencial de las tecnologías emergentes y, al mismo tiempo, gestionar un entorno de riesgos cada vez más complejo. Desde asegurar los sistemas basados en IA y proteger los activos de datos críticos hasta modernizar la infraestructura y fortalecer la gobernanza, el éxito requiere algo más que simples inversiones en tecnología. Requiere la combinación adecuada de estrategia, experiencia especializada y ejecución. Ahí es donde Experis ayuda a las organizaciones a pasar de la experimentación al impacto.



Experiencia en IA y datos

Transforma los datos en inteligencia útil con servicios que abarcan la modernización de datos, el modelado de IA, la automatización, el análisis avanzado y la gobernanza. Las organizaciones obtienen mayor visibilidad, una toma de decisiones más sólida y una adopción más responsable de la IA.



DevSecOps e ingeniería de seguridad

Incorpora la seguridad en todo el ciclo de vida de la tecnología mediante la integración de prácticas de desarrollo, operaciones y seguridad. Esto ayuda a acelerar la innovación al tiempo que reduce el riesgo y mejora la resiliencia.



La nube y la modernización de las aplicaciones

Moderniza los sistemas heredados, migra a entornos en la nube y crea arquitecturas escalables diseñadas para dar soporte a los requisitos emergentes de IA y ciberseguridad. Las organizaciones se benefician de una mayor agilidad y de una base tecnológica construida para el crecimiento futuro.



Gobernanza, calidad y cumplimiento normativo

Fortalece la confianza en las iniciativas digitales a través de la ingeniería de calidad, las pruebas automatizadas, la validación del desempeño y las pruebas de seguridad. El resultado consiste en una mayor confianza en las inversiones en tecnología, una mayor seguridad y una reducción del riesgo operativo.



Aceleración del tiempo para obtener valor

Aprovecha metodologías comprobadas, experiencia especializada y modelos de entrega ágiles para pasar de la estrategia a resultados medibles más rápidamente. Experis hace énfasis en resultados más rápidos y un impacto comercial significativo.

[1] Experis 2026 CIO Outlook [2] BCG [3] IBM Institute for Business Value [4] Fortinet [5] Deloitte [6] European Union

Mantente conectado

Experis es líder global en atracción de talento TI y soluciones tecnológicas,

Acceso a talento y servicios tecnológicos especializados, respaldados por una red global que brinda apoyo a clientes de diversos sectores y mercados. Nuestra profunda experiencia en el sector ayuda a las organizaciones a afrontar con confianza los complejos desafíos de la transformación.

El camino desde la experimentación con IA hasta un impacto comercial medible requiere más que nuevas herramientas. Requiere la combinación adecuada de experiencia tecnológica, estrategia de personal y apoyo en la ejecución. Como líder global en servicios tecnológicos, Experis® ayuda a las organizaciones a convertir el potencial de la tecnología en impacto comercial a través de la IA, los datos, la nube, la modernización de aplicaciones, la ingeniería de calidad y soluciones especializadas de talento.

Para obtener más información, visita *experis.co*, o síguenos en *LinkedIn*.

Metodología de investigación

Experis encargó una encuesta a 1,930 líderes tecnológicos de alto nivel en 12 países, realizada entre el 28 de enero y el 4 de marzo de 2026. Entre los encuestados se encontraban directores de informática (CIO), directores de tecnología (CTO), directores de seguridad de la información (CISO) y otros líderes tecnológicos de alto nivel con autoridad para tomar decisiones sobre los presupuestos de TI y la contratación. Además, se llevaron a cabo entrevistas cualitativas en profundidad en cada mercado.