



Microsoft 365
Copilot

Garantizar la seguridad de los datos en la era de la IA

Una guía para los líderes de TI

E-book



Esta guía se ha escrito para los líderes de TI que necesitan impulsar la adopción de IA al mismo tiempo que se mantiene la seguridad de los datos de sus organizaciones. Te ayudará a comprender los riesgos que plantea la IA para la seguridad y la privacidad de los datos y te aportará los conocimientos necesarios para liderar la transformación de la IA en tu empresa con confianza.

Índice

01

Las nuevas
normas del trabajo
impulsado por la IA

02

Comprender el
impacto de la IA en la
seguridad de los datos

03

El desafío de la
IA en la sombra

04

La realidad de BYOAI

05

El laberinto normativo

06

Un marco que prioriza
la seguridad para
evaluar las soluciones
de IA

07

Microsoft 365 Copilot:
IA en la que puedes
confiar

08

El camino seguro hacia
la transformación
de la IA

01

Las nuevas normas del trabajo impulsado por la IA

La IA generativa está abriendo nuevas puertas a la innovación y ayudando a los equipos a trabajar de forma más rápida e inteligente que nunca. Para las organizaciones con visión de futuro, la IA no es solo una tendencia tecnológica más, sino que es un imperativo empresarial, fundamental para el modo en que operan, aportan valor y mantienen una ventaja competitiva.

Sin embargo, esta rápida adopción plantea nuevos y mayores desafíos que los líderes de TI deben abordar y controlar de forma proactiva. Los sistemas de IA pueden buscar y combinar activamente información en todo el ecosistema de datos, lo que aumenta los riesgos de seguridad más allá de las herramientas tradicionales. A pesar de la rápida expansión de la IA, solo el **1 %** de las organizaciones afirman que han integrado completamente la IA en sus flujos de trabajo con protocolos de seguridad idóneos.¹ Al implementar medidas de seguridad y gestión robustas desde el inicio en tu recorrido de IA, tu equipo puede proteger con eficacia los datos confidenciales, mantener los requisitos de cumplimiento y proteger la información de tu organización, todo ello al mismo tiempo que se permite que la innovación prospere.

La ola de adopción de IA ya está aquí



02

Comprender el impacto de la IA en la seguridad de los datos

Antes de atajar desafíos específicos, es importante entender cómo la IA cambia fundamentalmente el panorama de la seguridad de los datos. A diferencia del software tradicional que solo accede a los datos cuando se le indica específicamente, la IA generativa procesa, analiza y crea contenido basándose en toda la información que recibe.

Esta diferencia es significativa por varias razones:

- Las herramientas de IA pueden descubrir conexiones entre datos que los seres humanos podrían pasar por alto
- Pueden sintetizar información de varias fuentes automáticamente
- Pueden generar nuevo contenido que contenga elementos a partir de entradas confidenciales

Es probable que tus herramientas de seguridad tradicionales no se diseñaran pensando en estas capacidades. Aunque el software convencional sigue rutas predecibles al acceder a los datos, la IA puede tomar rutas inesperadas a través de tu ecosistema de información, lo que puede exponer los datos confidenciales de formas que no habías previsto.

Este cambio fundamental requiere nuevos enfoques en cuanto a seguridad y gestión de los datos que aborden específicamente la forma en que la IA interactúa con los activos de información de tu organización.



03

El desafío de la IA en la sombra

Independientemente del punto en el que te encuentres en el recorrido de la adopción de la IA, tus empleados ya están encontrando sus propias soluciones, creando lo que se conoce como "IA en la sombra".

Este uso no autorizado genera puntos ciegos importantes en tu estrategia de seguridad. Cuando los empleados comparten datos de la empresa con sistemas de IA externos, eluden los controles de seguridad existentes y crean vulnerabilidades que la mayoría de las organizaciones no están preparadas para abordar.

La IA en la sombra no es solo un problema de seguridad: podría ser un síntoma de necesidades de productividad que no se satisfacen en tu organización. Si los empleados buscan herramientas no autorizadas, quiere decir que los sistemas oficiales no cumplen sus requisitos. Abordar la IA en la sombra requiere una gestión más sólida y soluciones de productividad mejoradas.



El 64 %

de los empleados tienen dificultades a la hora de disponer del tiempo y la energía para hacer su trabajo.³ Cuando descubren herramientas de IA que aumentan drásticamente su productividad, las utilizan, con o sin aprobación de TI.

Por qué surge la IA en la sombra:

- Los empleados están deseando aumentar la productividad gracias a las impresionantes capacidades de la IA
- Las cargas de trabajo diarias superan cada vez más el tiempo y la energía disponibles
- Los equipos se enfrentan a una creciente presión para entregar más con los mismos recursos
- Las herramientas de IA para el consumidor ofrecen soluciones inmediatas sin barreras de aprobación
- Los procesos oficiales de adquisición de TI no pueden igualar el ritmo de la innovación

Los riesgos de la IA en la sombra:

- No hay visibilidad sobre qué datos de la empresa están procesando los sistemas de IA externos
- No hay garantía de que no se conserve la información confidencial
- Sin estándares de seguridad uniformes en diferentes plataformas de IA
- Sin capacidad de auditoría para fines de cumplimiento
- Si integración con tu infraestructura de seguridad existente



Imagina este caso:

Un analista financiero tiene problemas con una compleja hoja de cálculo y decide cargarla en una herramienta de IA no autorizada para obtener ayuda. Esa hoja de cálculo contiene datos financieros de clientes, métricas internas y proyecciones. Aunque el analista recibe la ayuda que necesita, los datos financieros confidenciales de tu organización están ahora fuera del perímetro de seguridad, completamente invisibles para tus sistemas de supervisión.

04

La realidad de BYOAI

Sin una orientación clara de la dirección, los empleados están realizando por su cuenta la adopción de la IA: el **78 %** de los usuarios de IA adoptan un enfoque de «Bring Your Own AI» (BYOAI) al trabajo.² Esta tendencia se observa aún más en pequeñas y medianas empresas, en las que el **80 %** de los empleados adoptan el enfoque de BYOAI.²

Este enfoque no autorizado presenta importantes desventajas. Los empleados suelen ocultar que utilizan la IA: el **52 %** es reacio a admitir que usa la IA para tareas importantes y al **53 %** le preocupa que el uso de la IA haga que parezcan reemplazables.² Este secretismo no solo impide que las organizaciones puedan aprovechar todos los beneficios de la implementación estratégica de IA, sino que también crea graves vulnerabilidades de seguridad en un entorno en el que los líderes citan la ciberseguridad y la privacidad de los datos como su **principal** preocupación.²

Dado el uso generalizado y el crecimiento inevitable de la IA, la pregunta no es si debes permitir la IA en tu organización, sino cómo proporcionar una solución segura que satisfaga las necesidades de tus empleados mientras mantienes protegidos los datos de tu organización.



05

El laberinto normativo

Los marcos y las leyes en torno a la privacidad y la seguridad de los datos crean otra capa de complejidad al adoptar la IA. Aunque algunos marcos están diseñados específicamente para la gestión de la IA, otros tienen aplicaciones más amplias que siguen afectando a la forma en que gestionas la información y las sanciones por infracciones siguen siendo graves.

Cuando tus empleados utilizan herramientas de IA sin una supervisión idónea, podrían incurrir de forma involuntaria en infracciones normativas. La IA hace que este riesgo sea mayor porque puede acceder, combinar y exponer la información regulada de formas que las tecnologías tradicionales no pueden.

Principales normativas que afectan al uso de la IA:



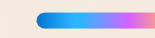
GDPR

El Reglamento General de Protección de Datos de la Unión Europea da a las personas el control sobre sus datos personales y requiere un consentimiento claro para su tratamiento.



Ley de IA de la UE

El marco integral de la Unión Europea específicamente diseñado para regular los sistemas de inteligencia artificial en función de sus niveles de riesgo



HIPAA

Esta ley federal estadounidense para el sector sanitario establece estándares estrictos para el tratamiento de información médica protegida



Administración de riesgos de la IA del NIST

Estas directrices voluntarias de Estados Unidos ayudan a las organizaciones a abordar los riesgos en el diseño, desarrollo e implementación de sistemas de IA

Los riesgos de cumplimiento con la IA:

- Datos de clientes que se procesan en servidores fuera de las regiones aprobadas
- Información personal utilizada sin el consentimiento adecuado
- Datos confidenciales que persisten en sistemas sin controles de retención adecuados
- No hay pista de auditoría sobre cómo se accede y utiliza la información protegida
- Contenido generado por IA que incumple los requisitos de cumplimiento específicos del sector

Estas infracciones pueden dar lugar a consecuencias graves:

- Elevadas multas financieras (las multas que impone el GDPR que pueden llegar al **4 %** de tus ingresos globales)⁴
- Requisitos para notificar a las partes afectadas sobre filtraciones de datos
- Acciones legales de los afectados
- Daño a la reputación de tu empresa y a la confianza de los clientes

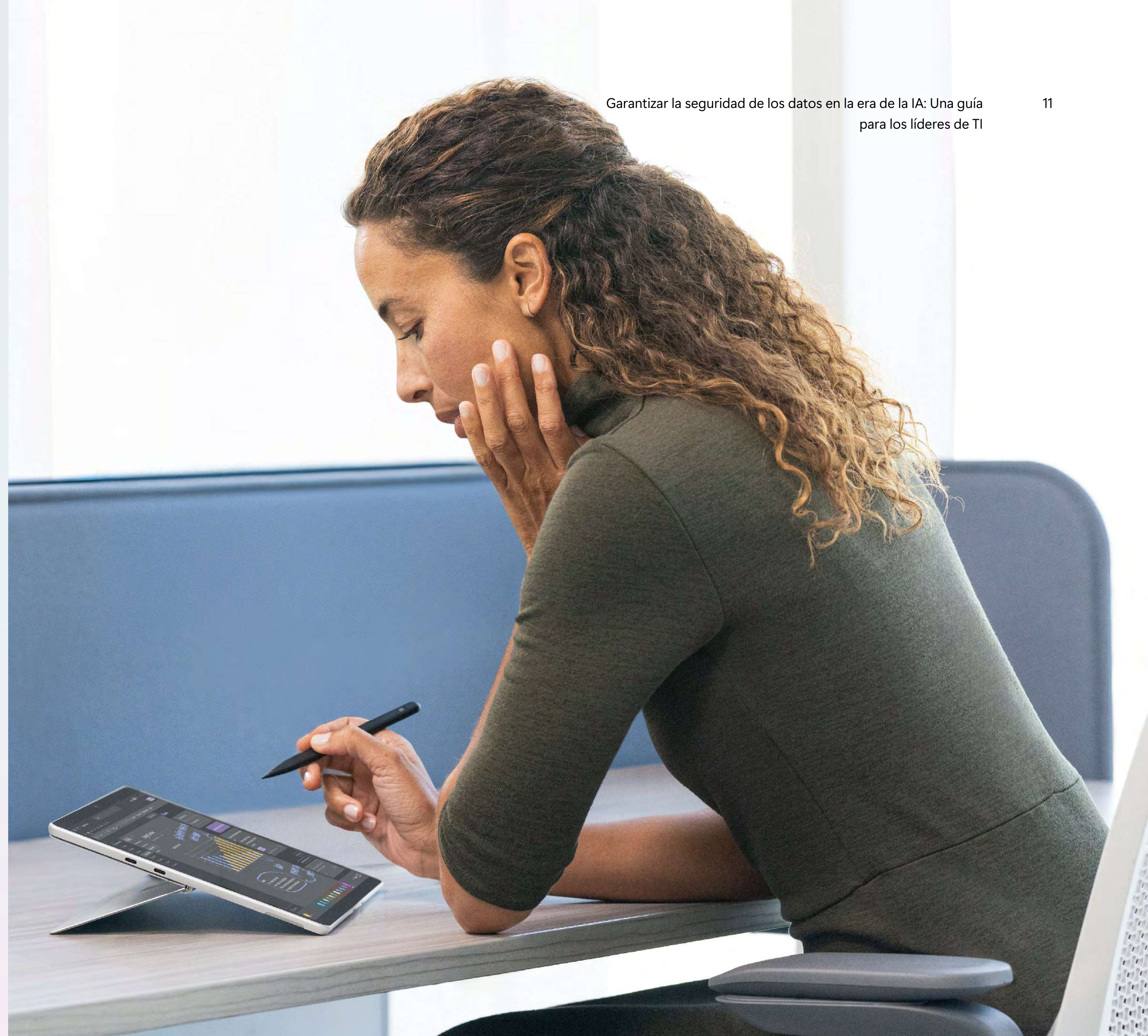
A medida que el uso de IA aumenta en toda tu organización, necesitas una gestión que ayude a las personas a trabajar de manera eficiente y, al mismo tiempo, a mantener el cumplimiento de la organización de las normativas que afectan a tu negocio y a tus clientes.

06

Un marco que prioriza la seguridad para evaluar las soluciones de IA

Con la IA en la sombra, BYOAI y las normativas aplicables, se plantean riesgos importantes, por lo que necesitas un enfoque estructurado para evaluar las soluciones de IA que garantice que puedan ayudar a tu organización a impulsar la innovación, al tiempo que proteges los datos confidenciales y garantizas el cumplimiento de los requisitos normativos en constante evolución.

El siguiente marco plantea seis preguntas sencillas para evaluar si una plataforma de IA cumple ambos requisitos.



Pregunta 1

¿Ofrece seguridad de nivel empresarial desde el primer momento?

Con la solución idónea, tu seguridad pasa de simplemente reaccionar a los problemas después de que ocurran a buscar proactivamente vulnerabilidades en los datos de tu organización, antes de que se conviertan en problemas más grandes.

Busca soluciones que:

- Proporcionen visibilidad en tiempo real de todo tu ecosistema de datos
- Identifiquen automáticamente los posibles riesgos de los datos antes de que se conviertan en incidentes
- Protejan la información confidencial en todos los niveles

Pregunta 2

¿Puede adoptar y mejorar fácilmente los controles de seguridad existentes?

Las políticas de seguridad de tu organización deben funcionar a la perfección con la IA. Tu proveedor de soluciones de IA debe respetar tus marcos de seguridad existentes e integrarse con ellos y no exigir que crees otros totalmente nuevos.

Busca soluciones que:

- Adopten fácilmente tus políticas de seguridad, etiquetas de confidencialidad y ajustes de protección de la información existentes
- Apliquen controles de acceso granulares en el nivel individual, para que ningún usuario tenga acceso a los datos a los que no debería tener acceso
- Indiquen activamente los intentos de socavar los controles de acceso

Pregunta 3

¿Incluye controles de privacidad y de gestión integrados?

Como las herramientas de IA funcionan de forma más proactiva, tus medidas de seguridad también deben ser proactivas. La implementación de una gestión de los datos sólida crea límites claros en los que tus empleados pueden innovar con seguridad sin poner en riesgo la información confidencial.

Busca soluciones que:

- Centralicen la gestión de la IA con la aplicación automatizada de políticas en todas las actividades
- Incluyan detección temprana de un posible uso compartido excesivo de los datos
- Estén en consonancia con los marcos normativos para garantizar el uso de la IA conforme a las normas

Pregunta 4

¿Se puede implementar de manera coherente en toda la organización?

Tus empleados tienen sus propios estilos de trabajo, sus propios horarios y pueden estar ubicados en todo el mundo. La IA debe beneficiar a todo el mundo.

Busca soluciones que:

- Ofrezcan una configuración fluida y una adopción sencilla de la IA en los flujos de trabajo diarios
- Proporcionen acceso flexible, desde chat de IA gratuito hasta soluciones de agentes escalables
- Ayuden a los empleados a desarrollar la fluidez de la IA e integrarla en su trabajo

Pregunta 5

¿Se integra perfectamente en los marcos existentes?

Actualmente, tu empresa opera con su propia infraestructura digital de programas de software, aplicaciones y mucho más.

Busca soluciones que:

- Se integren perfectamente con tus herramientas y programas para minimizar las interrupciones
- Proporcionen una experiencia de IA continua en todas las aplicaciones para que el trabajo pueda fluir sin problemas entre las herramientas
- Automaticen y optimicen las tareas dentro de los flujos de trabajo existentes

Pregunta 6

¿Los usuarios están capacitados para innovar?

En esencia, la IA debe transformar la forma en que se realiza el trabajo. No se trata solo de automatización: se trata de mejorar la productividad e impulsar la innovación.

Busca soluciones que:

- Conviertan las pérdidas de tiempo en procesos optimizados
- Automaticen las tareas repetitivas
- Capaciten a los trabajadores para recuperar tiempo y centrarse en las prioridades

07

Microsoft 365 Copilot: IA en la que puedes confiar

Microsoft 365 Copilot es la solución de IA generativa creada para ofrecer controles robustos de seguridad, gestión y acceso, garantizando una implementación segura y una innovación sostenida. Mejora la productividad con herramientas intuitivas como Copilot Chat, que funciona donde tú lo haces, y Copilot Studio, donde tu equipo puede crear agentes de IA personalizados sin tener conocimientos de programación.

Copilot se integra perfectamente en tu entorno de Microsoft 365, heredando los permisos de usuario, las etiquetas de confidencialidad, las políticas de prevención de pérdida de datos y los requisitos de residencia geográfica de los datos, sin necesidad de configuración adicional. Al incorporar la IA en las herramientas que tus empleados ya utilizan, Copilot mitiga los riesgos de seguridad y mantiene los datos en tu entorno de confianza de Microsoft 365.

Los compromisos de Microsoft garantizan que tu organización mantenga el control:

- Tus datos están seguros en reposo y en tránsito
- Tus datos no se utilizarán para entrenar modelos de IA
- Tú eliges qué información se traslada al cloud
- Estás protegido contra los riesgos de la seguridad de la IA y los derechos de autor

Las herramientas de gestión diseñadas específicamente como Copilot Control System y SharePoint Advanced Management aportan a los equipos de TI la visibilidad, los controles y los registros de auditoría necesarios para mantener el cumplimiento normativo.

Con Microsoft 365 Copilot, no tienes que elegir entre innovación y seguridad: puedes tener ambas cosas.

El camino seguro hacia la transformación de la IA

La revolución de la IA presenta una oportunidad única para que los líderes de TI proporcionen valor estratégico al equilibrar la innovación y la seguridad.

Al implementar herramientas de IA seguras como Microsoft 365 Copilot, capacitarás a los empleados con herramientas para que sean más productivos, todo ello al mismo tiempo que eliminas los riesgos de la IA en la sombra. El camino a seguir pasa por permitir la innovación de forma segura. Tu liderazgo en la adopción segura de IA posicionará al departamento de TI como un habilitador de transformación, ayudando a tu organización a prosperar en esta nueva era manteniendo la seguridad y el cumplimiento de los datos.



Empieza a usar Microsoft 365 Copilot

Fuentes:

¹ «Superagency in the workplace: Empowering people to unlock AI's full potential», McKinsey & Company, 28 de enero de 2025. <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work>.

² «La IA en el trabajo ya está aquí. Ahora viene lo difícil», Índice de tendencias anuales de Microsoft, 8 de mayo de 2024. <https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part>.

³ «¿Funcionará la IA?», Índice de tendencias laborales de Microsoft, 9 de mayo de 2023. <https://www.microsoft.com/en-us/worklab/work-trend-index/will-ai-fix-work>.

⁴ «Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)», Parlamento Europeo y Consejo, 27 de abril de 2016. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>.