Microsoft 365 Copilot

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

Guía para los líderes de TI

eBook

Esta guía está dirigida a los líderes de TI que necesitan impulsar la adopción de IA y mantener seguros los datos de sus organizaciones. Le permitirá comprender los riesgos que la IA implica para la seguridad y la privacidad de los datos, a la vez que le proporcionará la información necesaria para dirigir con confianza la transformación de su empresa hacia la IA.

Contenido

01

Las nuevas reglas del trabajo con tecnología de IA

La IA generativa abre nuevas puertas a la innovación y ayuda a los equipos a trabajar más rápido y de manera más inteligente que nunca. Para las organizaciones con visión de futuro, la IA no es solo otra tendencia tecnológica, sino que es un imperativo empresarial, esencial para la manera en que operan, brindan valor y mantienen una ventaja competitiva.

Pero esta rápida adopción trae desafíos nuevos y amplificados que los líderes de TI deben abordar y controlar de manera 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 informan que han integrado completamente la IA en sus flujos de trabajo con los protocolos de seguridad adecuados.[1] Al implementar sólidas medidas de seguridad y gobernanza desde el inicio de su recorrido hacia la IA, su equipo puede proteger eficazmente los datos confidenciales, mantener los requisitos de cumplimiento y salvaguardar la información de su organización, todo ello a la vez que permite que florezca la innovación.

La ola de adopción de IA ya está aquí

02

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

Antes de profundizar en desafíos específicos, es importante que entendamos cómo l a IA cambia radicalmente el panorama de 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 activamente contenido basado en toda la información que recibe.

Esta diferencia es significativa por varias razones:

- Las herramientas de IA pueden descubrir conexiones entre los datos que las personas podrían pasar por alto.
- Pueden sintetizar información a través de varios orígenes de manera automática.
- Pueden generar contenido nuevo que contenga elementos de entradas confidenciales.

Es probable que sus herramientas de seguridad tradicionales no se diseñaran teniendo en cuenta estas capacidades. Mientras el software convencional sigue rutas predecibles al acceder a los datos, la IA puede tomar rutas inesperadas a través de su ecosistema de información, lo que podría dejar expuestos datos confidenciales de maneras que no había previsto.

Este cambio fundamental requiere nuevos enfoques de seguridad y gobernanza de datos que aborden específicamente cómo la IA interactúa con los activos de información de su organización.

03

El desafío de la IA en la sombra

Dondequiera que esté en su recorrido de adopción de la IA, sus empleados ya están encontrando sus propias soluciones y creando lo que se conoce como la "IA en la sombra".

Este uso no autorizado genera importantes puntos ciegos en su posición 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, sino que podría ser un síntoma de que hay necesidades de productividad no satisfechas en su organización. Cuando los empleados recurren a herramientas no autorizadas, están indicando que sus sistemas oficiales no cumplen con sus requisitos. Abordar la IA en la sombra requiere una gobernanza mássólida y soluciones de productividad mejoradas.

Por qué surge la IA en la sombra:

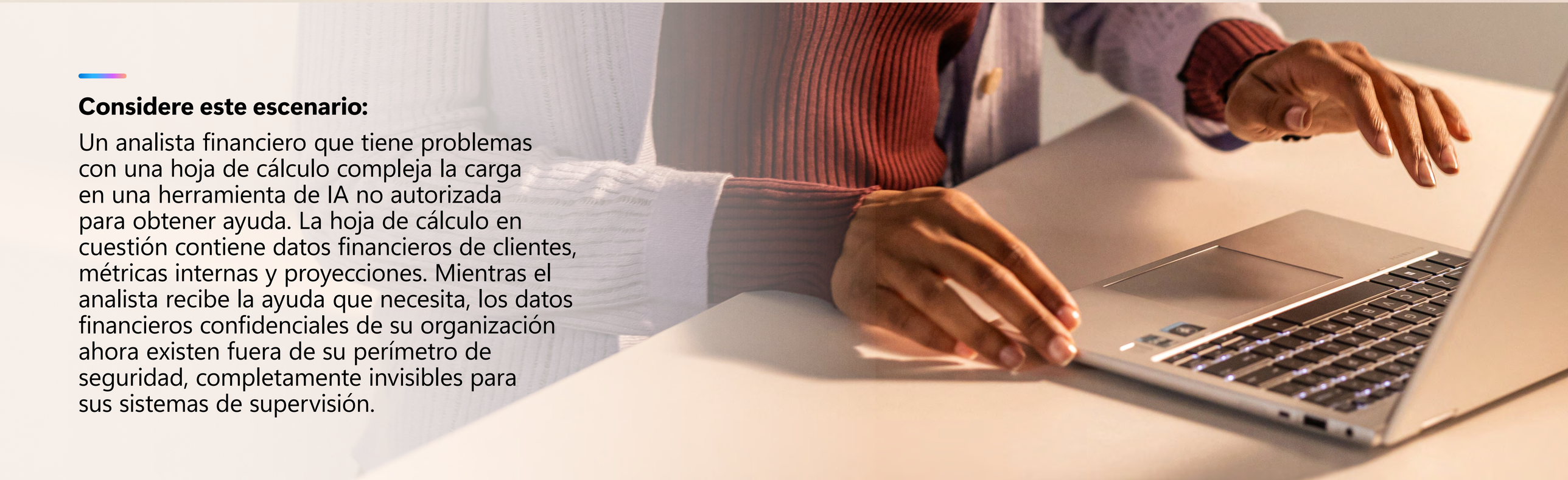
- Los empleados están ansiosos por aumentar la productividad gracias a las impresionantes capacidades de la IA.
- Las cargas de trabajo diarias exceden cada vez más el tiempo y la energía disponibles.
- Los equipos se enfrentan a una creciente presión para entregar mejores resultados con los mismos recursos.
- Las herramientas de IA de consumo 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 de los datos de la empresa que están siendo procesados por sistemas de IA externos.
- No hay garantía de que no se conserve la información confidencial.
- No hay estándares de seguridad coherentes en la distintas plataformas de IA.
- No se puede auditar para fines de cumplimiento de las normativas.
- No hay integración con la infraestructura de seguridad existente.

Considere este escenario:

Un analista financiero que tiene problemas con una hoja de cálculo compleja la carga en una herramienta de IA no autorizada para obtener ayuda. La hoja de cálculo en cuestión contiene datos financieros de clientes, métricas internas y proyecciones. Mientras el analista recibe la ayuda que necesita, los datos financieros confidenciales de su organización ahora existen fuera de su perímetro de seguridad, completamente invisibles para sus sistemas de supervisión.



04

La realidad de BYOAI

Sin una guía clara por parte del liderazgo, los empleados adoptan cada vez más la IA por su propia cuenta: el **78 %** de los usuarios de IA están adoptando un enfoque de "traiga su propia IA" (BYOAI) al trabajo.[2] Esta tendencia es aún más pronunciada en las pequeñas y medianas empresas, en las que el **80 %** de los empleados participan en prácticas de BYOAI.[2]

Este enfoque no autorizado conlleva desventajas significativas. Los empleados suelen ocultar que utilizan la IA: el **52 %** es reacio a admitir que usan la IA en tareas importantes, mientras que el **53 %** se preocupa de que el uso de la IA los haga parecer reemplazables.[2] Este ocultamiento no solo impide que las organizaciones obtengan todos los beneficios de la implementación estratégica de IA, sino que también crea serias 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 su organización debe permitir la IA, sino cómo proporcionar una solución segura que satisfaga las necesidades de los empleados y mantenga protegidos los datos de su organización.

05

El laberinto reglamentario

Los marcos y leyes en torno a la privacidad y seguridad de los datos crean otra capa de complejidad para la adopción de la IA. Si bien algunos marcos están diseñados específicamente para la gobernanza de la IA, otros tienen aplicaciones más amplias que todavía afectan la manera en que su organización maneja la información, y las sanciones por infracciones siguen siendo graves.

Cuando sus empleados utilizan herramientas de IA sin la supervisión adecuada, podrían incurrir en infracciones de cumplimiento sin querer hacerlo. La IA aumenta este riesgo porque puede acceder, combinar y exponer información reglamentada de maneras en las que las tecnologías tradicionales no pueden.

Reglamentaciones clave que afectan cómo utiliza la IA:

RGPD

El Reglamento general de protección de datos de la Unión Europea brinda a las personas control sobre sus datos personales y requiere un consentimiento claro para procesarlos

Ley de IA de la UE

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

HIPAA

Esta ley federal de los Estados Unidos para la atención médica establece estándares estrictos para el manejo de información médica protegida

Marco de administración de riesgos de IA de NIST

Esta guía voluntaria de los Estados Unidos ayuda a las organizaciones a abordar los riesgos en el diseño, el desarrollo y la implementación de sistemas de IA

Los riesgos de cumplimiento con la IA:

- Datos del cliente procesados en servidores fuera de las regiones aprobadas
- Información personal que se utiliza sin el consentimiento adecuado
- Datos confidenciales que persisten en sistemas sin los controles de retención adecuados
- No hay registro de auditoría de cómo se accede a la información protegida y cómo se utiliza
- Contenido generado por IA que infringe requisitos de cumplimiento específicos del sector

Estas infracciones pueden generar graves consecuencias:

- Importante sanciones financieras (las multas por infringir el RGPD pueden llegar al **4 %** de sus ingresos globales)[4]
- Requisitos para notificar a las partes afectadas sobre filtraciones de datos
- Acciones legales de los afectados
- Daño a la reputación de su empresa y a la confianza de los usuarios

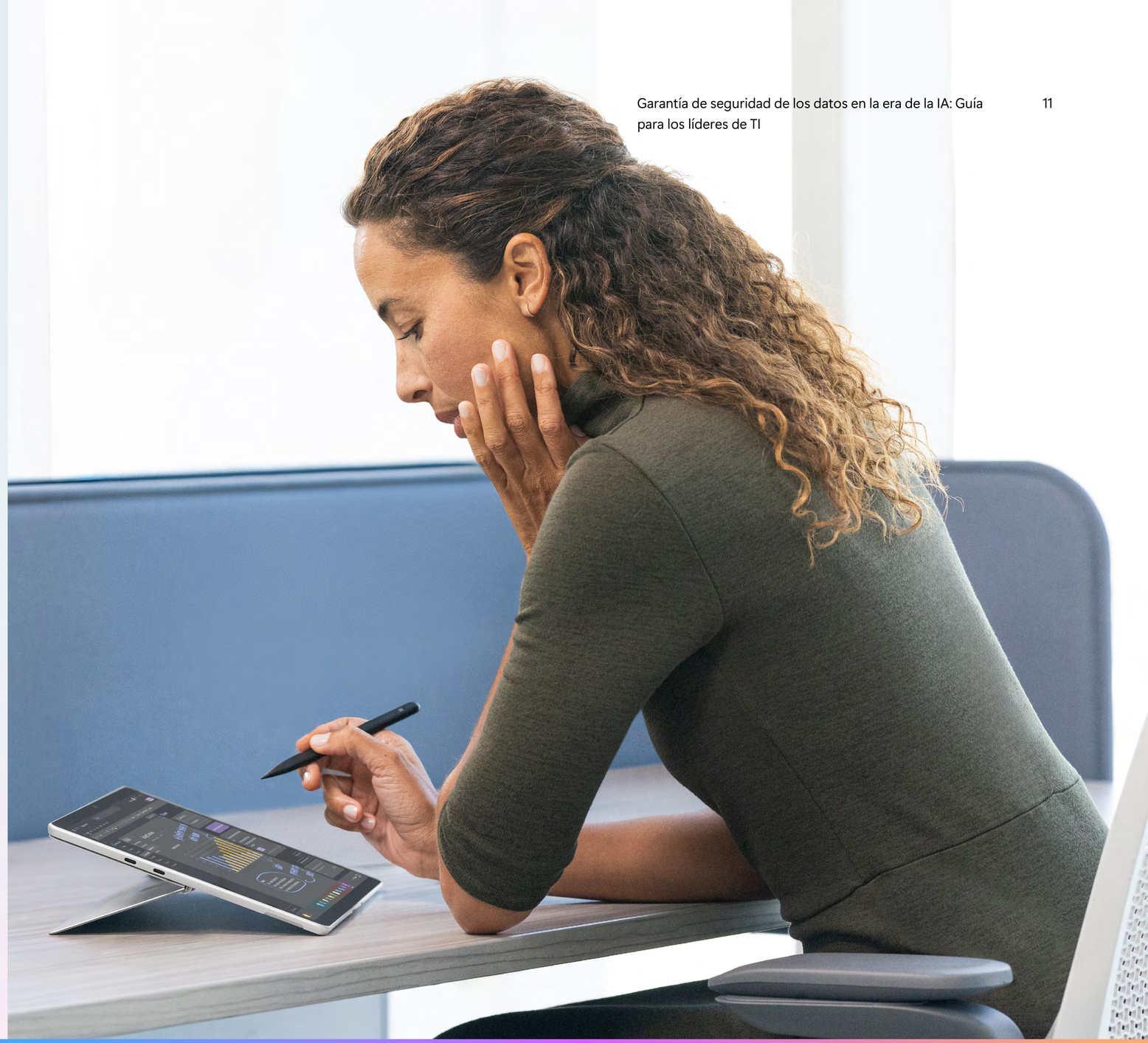
A medida que crece el uso de la IA en su organización, necesitará una gobernanza que ayude a las personas a trabajar de manera eficiente y, a la vez, mantenga su organización en cumplimiento con las normativas que afectan a su negocio y sus clientes.

06

Un marco centrado en la seguridad para evaluar las soluciones de IA

Con la IA en la sombra, BYOAI y reglamentaciones que generan riesgos significativos, necesita un enfoque estructurado para evaluar las soluciones de IA que garantice que pueden ayudar a su organización a impulsar la innovación, al mismo tiempo que protege los datos confidenciales y garantiza el cumplimiento de los requisitos normativos en evolución.

El siguiente marco brinda seis sencillas preguntas para evaluar si una plataforma de IA cumple en ambos frentes.



Pregunta 1

¿Ofrece seguridad de nivel empresarial desde cero?

Con la solución adecuada, su seguridad pasa de solo reaccionar a los problemas después de que ocurran a buscar proactivamente vulnerabilidades en los datos de su organización, antes de que se conviertan en problemas mayores.

Busque soluciones que:

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

Pregunta 2

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

Las directivas de seguridad de su organización deben funcionar perfectamente con la IA. Su proveedor de soluciones de IA debe respetar sus marcos de seguridad existentes e integrarse a ellos, no exigirle que cree otros completamente nuevos.

Busque soluciones que:

- Adopten sin interrupciones sus políticas de seguridad, etiquetas de confidencialidad y configuración de protección de la información existentes
- Apliquen controles de acceso pormenorizado a nivel individual, para que ningún usuario tenga acceso a datos a los que no debería poder acceder
- Marcan activamente los intentos de trastornar los controles de acceso

Pregunta 3

¿Incluye controles integrados de gobernanza y privacidad?

Dado que las herramientas de IA funcionan de manera más proactiva, sus medidas de seguridad también deben ser proactivas. La implementación de una gobernanza sólida de los datos establece límites claros en los que sus empleados pueden innovar de forma segura sin poner en riesgo la información confidencial.

Busque soluciones que:

- Centralicen la gobernanza de la IA con la aplicación automatizada de directivas en todas las actividades
- Incluyan la detección temprana del posible uso compartido excesivo de datos
- Se alineen con marcos reglamentarios para garantizar el uso de IA conforme

Pregunta 4

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

Sus empleados tienen sus propios estilos de trabajo y sus propios horarios; además, pueden estar ubicados en todo el mundo. La IA debería beneficiarlos a todos.

Busque soluciones que:

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

Pregunta 5

¿Se integra sin problemas en los marcos existentes?

Actualmente, su empresa funciona con su propia infraestructura digital de programas de software, aplicaciones y más.

Busque soluciones que:

- Encajen perfectamente con sus 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 en los flujos de trabajo existentes

Pregunta 6

¿Están los usuarios facultados para innovar?

En esencia, la IA debe transformar la manera en que se hace el trabajo. No se trata solo de automatización, sino de mejorar la productividad e impulsar la innovación.

Busque soluciones que:

- Transformen las pérdidas de tiempo en procesos optimizados
- Automaticen las tareas repetitivas
- Permitan a los trabajadores recuperar tiempo y centrarse en las prioridades

07

Microsoft 365 Copilot: IA en la que puede confiar

Microsoft 365 Copilot es la solución de IA generativa creada para ofrecer una sólida seguridad, gobernanza y controles de acceso, lo que garantiza una implementación segura y una innovación sostenida. Mejora la productividad con herramientas intuitivas como Chat de Copilot, que funciona donde usted lo hace, y Copilot Studio, en el que su equipo puede crear agentes de IA personalizados sin necesidad de habilidades de codificación.

Copilot se integra perfectamente dentro de su entorno de Microsoft 365, heredando permisos de usuario, etiquetas de confidencialidad, directivas de prevención de pérdida de datos y requisitos de residencia de datos geográficos, sin configuración adicional. Al incorporar la IA en las herramientas que sus empleados ya usan, Copilot mitiga los riesgos de seguridad mientras mantiene los datos dentro de su entorno de Microsoft 365 de confianza.

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

- Sus datos están protegidos tanto en reposo como en tránsito
- Sus datos no se utilizan para entrenar modelos de IA
- Usted elige qué información va a la nube
- Está protegido contra los riesgos de seguridad de la IA y derechos de autor

Las herramientas de gobernanza diseñadas específicamente, como el Sistema de control Copilot y la Administración avanzada de SharePoint, brindan a los equipos de TI la visibilidad, los controles y los registros de auditoría necesarios para mantener el cumplimiento.

Con Microsoft 365 Copilot, no es necesario que elija entre la innovación y la seguridad, porque puede tener ambas.

08

El camino seguro hacia la transformación de la IA

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

Al implementar herramientas de IA seguras como Microsoft 365 Copilot, brindará a los empleados herramientas que les permitirán lograr una mayor productividad, todo mientras se eliminan los riesgos de IA en la sombra. El camino a seguir consiste en habilitar la innovación de manera segura. Su liderazgo en la adopción segura de la IA posicionará al departamento de TI como un facilitador de la transformación que ayuda a su organización a prosperar en esta nueva era mientras mantiene los datos seguros y en cumplimiento.

Comience 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 está aquí. Ahora viene la parte difícil", Índice de tendencias de trabajo 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] "¿La IA solucionará el trabajo?", Índice de tendencias de trabajo de Microsoft, 9 de mayo de 2023. https://www.microsoft.com/en-us/worklab/work-trend-index/will-ai-fix-work.

[4] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", Parlamento Europeo y Consejo de la Unión Europea, 27 de abril de 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.