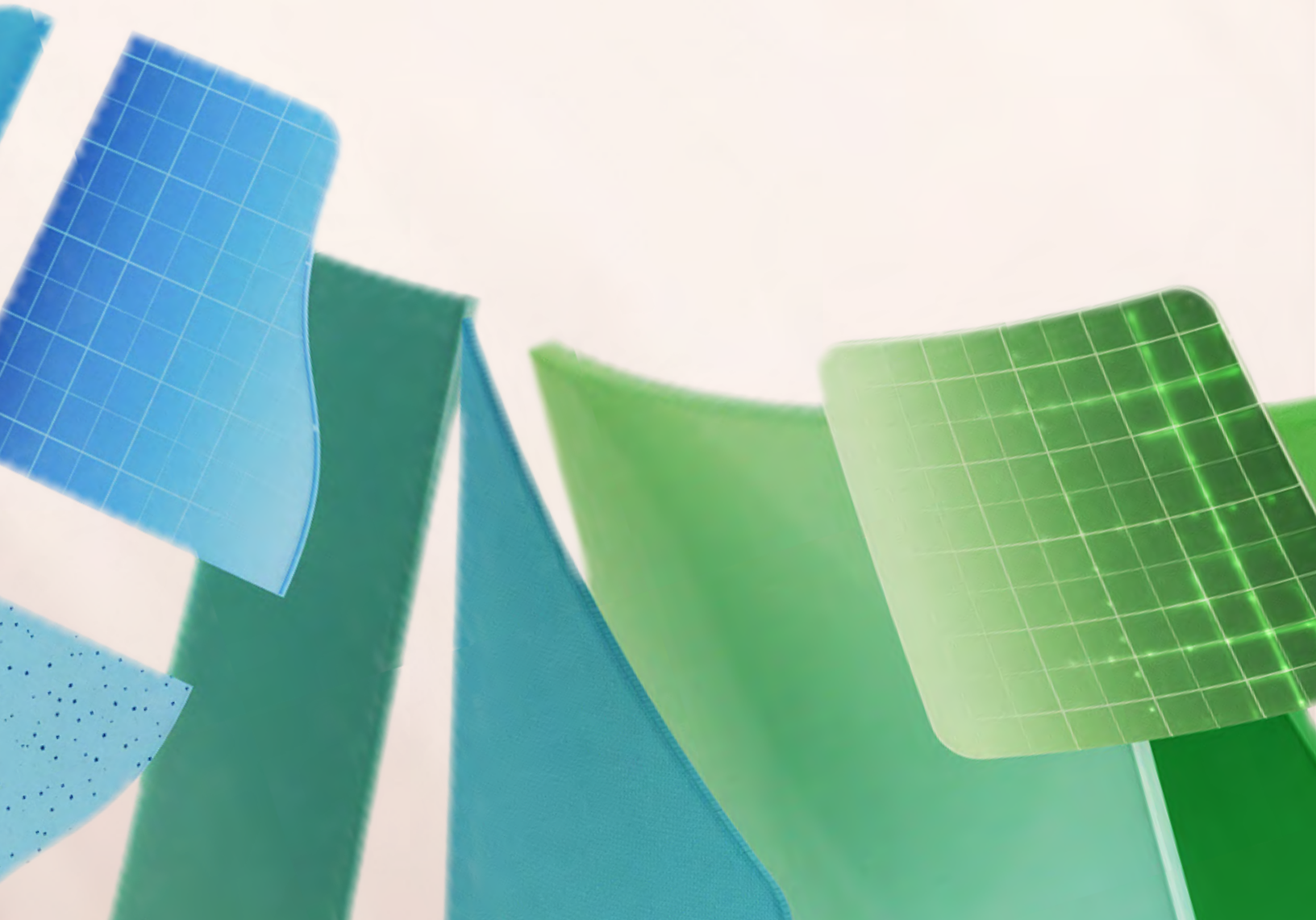
Microsoft 365

Datos bajo control

Dominar el gobierno de datos para lograr el éxito con la IA



Índice

Introducción

El gobierno de los datos es la columna vertebral de la adopción segura de la IA

La IA generativa es la promesa de la transformación empresarial, pero para aprovechar ese potencial, se debe garantizar la calidad y la disponibilidad de los datos empresariales.

Las organizaciones que den prioridad a un buen gobierno de los datos estarán mejor preparadas para obtener una ventaja competitiva con la IA. El gobierno de los datos ayuda a garantizar que los datos consultados y generados por la IA sean correctos y seguros, estén controlados y cumplan las normativas.

Calidad y disponibilidad de los datos:
los sistemas de IA utilizan grandes conjuntos de datos de alta calidad para proporcionar la mejor respuesta posible con el contexto adecuado a partir de los flujos de trabajo únicos de tu organización. Una mejor calidad de los datos permite obtener predicciones y conocimientos de IA más eficaces.

Cumplimiento: un buen gobierno de los datos garantiza el cumplimiento de las normativas, lo que reduce el riesgo de problemas legales y multas.

Seguridad: el etiquetado y la administración adecuados de los datos protegen la información confidencial frente al acceso no autorizado, el intercambio inadecuado y las filtraciones.

Confianza: un gobierno fiable de los datos infunde confianza a las partes interesadas en los resultados de la IA, lo que fomenta una mayor adopción y apoyo a las iniciativas de IA.

En este e-book presentamos las prácticas críticas de gobierno de los datos que preparan a las organizaciones para la IA. En él se explica cómo establecer buenos estándares de calidad de datos, garantizar el cumplimiento de las normativas e implementar medidas de seguridad y protección de datos. Tanto si se trata de evitar que el contenido confidencial de las reuniones se comparta externamente como de protegerse de las filtraciones de datos, aprenderás estrategias para generar confianza en los sistemas de IA y hacer que los datos estén disponibles para obtener conocimientos útiles. Al adoptar estas prácticas, tu organización puede aplicar todo el potencial de la IA para permitir la innovación continua y conseguir una ventaja competitiva.

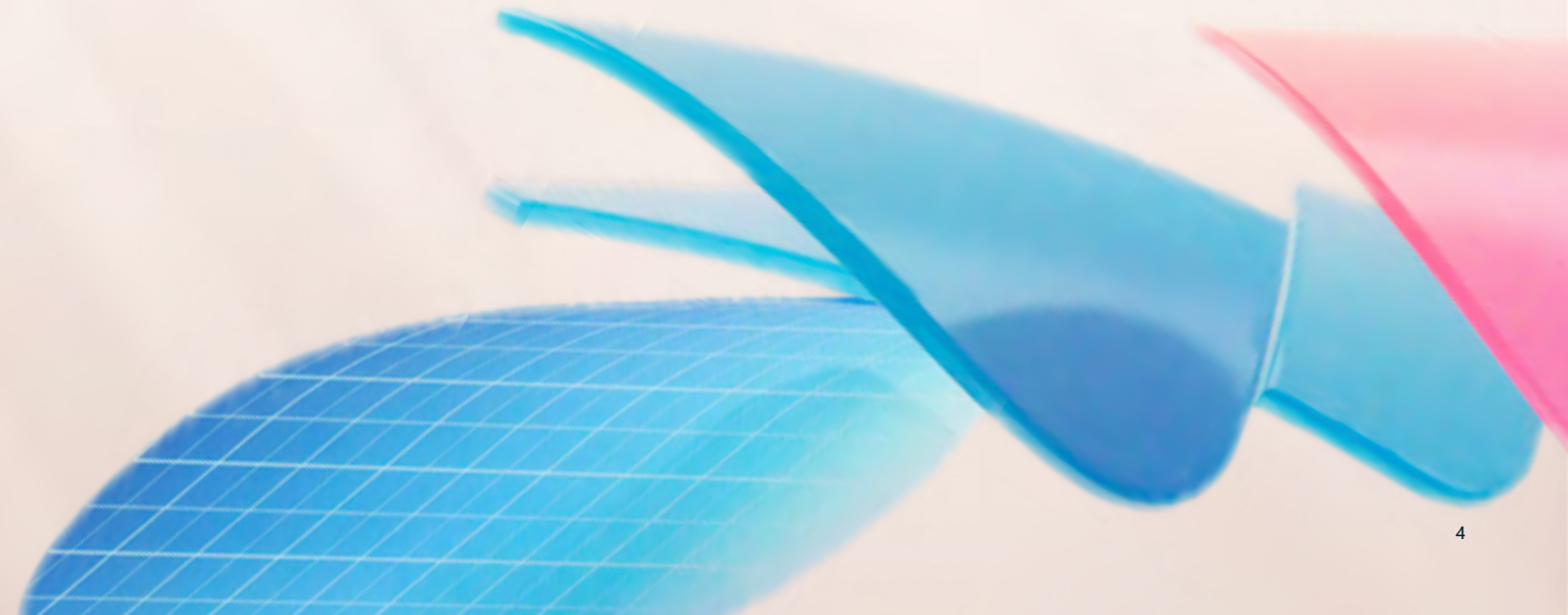
Casos de uso de la IA generativa

Acelera la comunicación: redacta contenido personalizado más rápidamente y deja tiempo para establecer relaciones y colaborar.

Mejora la eficiencia: dedica menos tiempo a las tareas rutinarias, mejora la productividad y reduce los costes.

Facilita la innovación: ayuda a generar ideas y propuestas para nuevos productos y servicios.

Personaliza las experiencias de los clientes: adapta el contenido y las recomendaciones para impulsar la lealtad y la implicación.



1

Fortalecer el gobierno de datos para la transformación con la IA

Todas las empresas tienen políticas y procesos que rigen el uso de los datos. Los marcos de gobierno de los datos varían en cuanto a madurez y exhaustividad, pero pocos se han optimizado por completo para la IA. Aunque muchas prácticas recomendadas de gobierno de los datos siguen siendo las mismas, como garantizar la exactitud y la coherencia de los datos, otros aspectos necesitan actualizaciones para maximizar las inversiones en IA. Veamos algunas áreas clave.

Visibilidad de los datos

El conocimiento detallado del flujo de datos dentro de los sistemas de IA permite detectar y mitigar el uso no autorizado o inadecuado. Esta visibilidad ayuda a respaldar la seguridad y el cumplimiento, protegiendo los datos confidenciales para maximizar el valor de la IA.

El gobierno de los datos tradicional se ha centrado en saber dónde están los datos y controlar el acceso. Sin embargo, a medida que la IA se integra más en las operaciones empresariales, el gobierno de los datos debe abordar las necesidades de seguridad en continua evolución. Por ejemplo, con el lanzamiento de un producto altamente confidencial, el gobierno debe abarcar ahora la administración del contenido generado por la IA, garantizando que los documentos, las comunicaciones y la información relacionada con los proyectos producidos por la IA sean seguros. Esto significa implementar medidas de seguridad para que solo los miembros del equipo autorizados puedan acceder a la IA y utilizarla para analizar o resumir la información del proyecto.

Asimismo, mediante la administración de volúmenes de almacenamiento y procesamiento de datos, las organizaciones pueden controlar mejor los costes de explotación asociados con la IA.

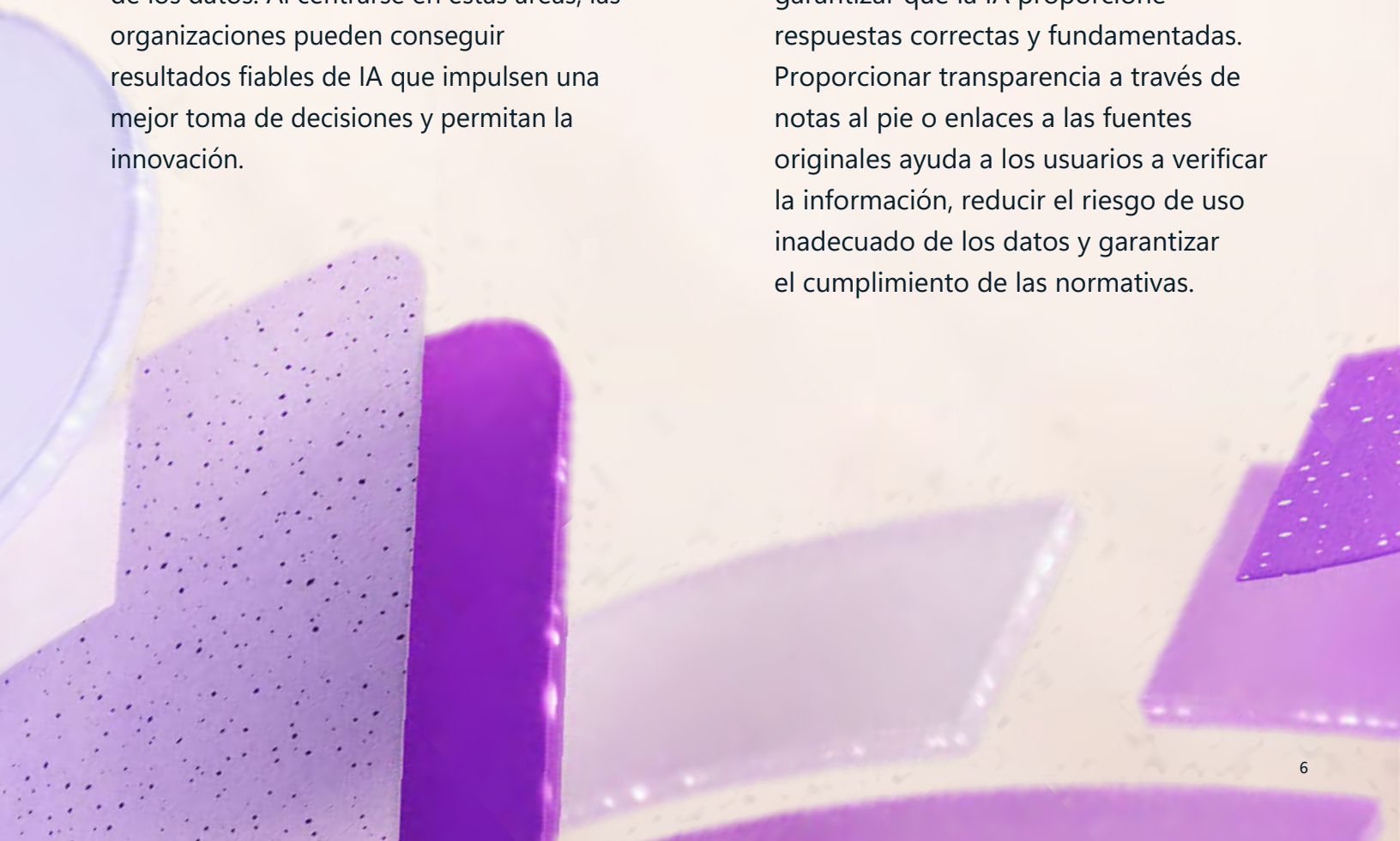
Calidad de los datos

La IA amplifica la importancia de los datos de alta calidad, ya que una mala calidad de los datos afecta directamente a los resultados de la IA. Al aplicar herramientas de IA para consultar los datos de tu empresa, querrás asegurarte de que los datos sean actuales y fiables. Igualmente importante es conocer la procedencia y la calidad de los datos que utilizan tus equipos para crear sus propios modelos y aplicaciones de IA. Las auditorías periódicas de los datos, los estrictos procesos de validación y la administración proactiva ayudan a garantizar la integridad de los datos. Al centrarse en estas áreas, las organizaciones pueden conseguir resultados fiables de IA que impulsen una mejor toma de decisiones y permitan la innovación.

Administración de usuarios

Con la IA, los usuarios interactúan con los datos de formas sofisticadas. Se comunican con sistemas de IA como Microsoft 365 Copilot a través de prompts en lenguaje natural. Con los permisos y las protecciones implementados, la IA puede acceder al contexto relevante a partir de los datos (como archivos, chats y correos electrónicos), junto con fuentes externas a través de complementos para generar una respuesta.

Es fundamental supervisar los datos utilizados en estos procesos para garantizar que la IA proporcione respuestas correctas y fundamentadas. Proporcionar transparencia a través de notas al pie o enlaces a las fuentes originales ayuda a los usuarios a verificar la información, reducir el riesgo de uso inadecuado de los datos y garantizar el cumplimiento de las normativas.



Cumplimiento y eDiscovery

El auge de la IA plantea nuevos desafíos en el cumplimiento y eDiscovery (la gestión de los datos para casos legales), especialmente en la administración de datos generados por IA y la adaptación a los requisitos legales en continuo cambio. La actualización de los marcos de gobierno de los datos para abordar estos desafíos implica el desarrollo de políticas que cubran el contenido generado por la IA, como garantizar que se realice un seguimiento, una clasificación y un almacenamiento seguro de los documentos o comunicaciones producidos por la IA. Por ejemplo, es posible que sea necesario actualizar las políticas para garantizar que los correos electrónicos o los informes generados por la IA se etiqueten y archiven correctamente para poder recuperarlos en el futuro.

La mejora de las funcionalidades de eDiscovery incluiría la integración de herramientas de IA que puedan buscar e identificar el contenido generado por la IA en distintas plataformas. Por ejemplo, durante una consulta legal, las herramientas de eDiscovery deben ser capaces de encontrar y recuperar documentos específicos generados por la IA, resumir las comunicaciones pertinentes y proporcionar auditorías claras para demostrar el cumplimiento. Al actualizar estas funcionalidades, las organizaciones pueden administrar mejor los datos durante las auditorías o investigaciones legales, garantizando así que toda la información relevante generada por IA sea accesible y se pueda defender en los tribunales.

Seguridad de los datos

La protección de las operaciones impulsadas por la IA debe incluir principios de Confianza cero en el nivel de identidad para minimizar el riesgo del acceso no autorizado. Las actualizaciones periódicas de los puntos de conexión, incluidos los dispositivos y las aplicaciones, reducen las vulnerabilidades que se podrían aprovechar para perpetrar un ataque. El conocimiento de las herramientas de IA generativa que se utilizan dentro de la organización permite bloquear las aplicaciones no autorizadas o poco seguras, lo que a su vez evita posibles infracciones de seguridad. Al limitar el acceso a las herramientas y los datos de IA solo al personal de confianza, las organizaciones pueden lograr una mayor integridad de los datos y proteger sus operaciones de IA de posibles amenazas.

¿Qué es la Confianza cero?

La Confianza cero es un modelo de seguridad que se basa en verificar cada solicitud como si procediera de una red no fiable. En lugar de presuponer que todo lo que hay dentro del firewall corporativo es seguro, este enfoque adopta el principio de «nunca confiar, verificar siempre».

Principios de Confianza cero

Verificar explícitamente: autentica y autoriza siempre en función de todos los puntos de datos disponibles.

Usar el acceso de privilegios mínimos: limita el acceso de los usuarios con acceso «Just-in-Time» y «Just-Enough» (JIT/JEA), políticas adaptativas basadas en riesgo y protección de datos.

Dar por hecho que se producirá un ataque: limita los daños, controla el acceso, garantiza el cifrado y usa los datos para detectar amenazas y reforzar las defensas.

2

El papel de la administración de los datos en la transformación con la IA: orígenes, calidad y fiabilidad

A medida que las organizaciones adoptan la IA para ayudar en las decisiones empresariales, deben asegurarse de que estos sistemas puedan proporcionar resultados correctos y fiables. Las respuestas de IA basadas en datos deben estar disponibles, ser coherentes y estar bien documentadas.

La administración de los datos respalda la IA de confianza al implementar políticas de gobierno que rastrean el origen de los datos, comprueban su calidad y garantizan su fiabilidad y precisión. Estas prácticas sientan las bases de los sistemas de IA que proporcionan conocimientos fiables, lo que permite tomar decisiones fundamentadas con confianza.

Linaje de datos: conocer los orígenes y los cambios en la información

El linaje de datos realiza un seguimiento del recorrido de los datos por una organización. Documenta los orígenes, las transformaciones y los destinos de los datos. Para las empresas con tecnología de IA, conocer el linaje de datos es fundamental por varias razones:

- **Transparencia:** saber de dónde proceden los datos y cómo cambian ayuda a confirmar la exactitud de los resultados generados por la IA y garantiza el cumplimiento normativo al proporcionar un conocimiento claro del historial de los datos.
- **Rastreabilidad:** el linaje de datos permite a las organizaciones rastrear errores o incoherencias en su origen, lo que simplifica la solución de problemas y la corrección de los datos.
- **Análisis del impacto:** conocer cómo se utilizan los datos mediante herramientas de IA generativa ayuda a evaluar el impacto potencial que los cambios en las fuentes de datos o los métodos de procesamiento pueden tener en la precisión de la salida y los resultados empresariales.

Calidad de los datos: la calidad mejora el valor de las respuestas de IA

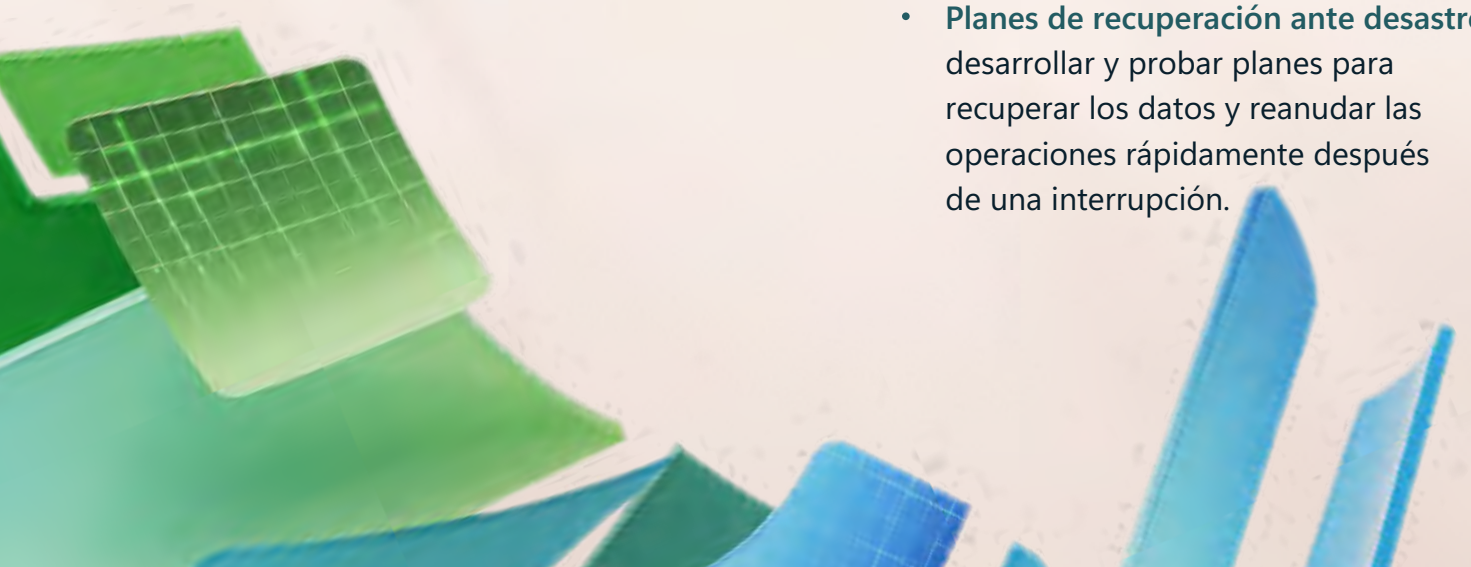
La calidad de los datos afecta directamente a la fiabilidad de los resultados de la IA. Los datos de alta calidad proporcionan el contexto para que los modelos de IA proporcionen respuestas correctas y valiosas a las entradas del usuario. Algunos aspectos clave de la calidad de los datos son los siguientes:

- **Precisión:** los datos deben representar correctamente las condiciones del mundo real.
- **Integridad:** todos los datos necesarios deben estar presentes y tenerse en cuenta.
- **Coherencia:** los datos deben ser coherentes en diferentes sistemas y a lo largo del tiempo.
- **Puntualidad:** los datos deben estar actualizados y disponibles cuando sea necesario.

Fiabilidad de los datos: garantizar datos fiables

La fiabilidad de los datos significa que los datos cumplen sistemáticamente los estándares de calidad y están disponibles cuando es necesario. Para las empresas que usan la tecnología de IA, los datos fiables son cruciales para promover la confianza en las herramientas de IA y en las decisiones que fundamentan. Garantizar la fiabilidad de los datos implica:

- **Redundancia de datos:** implementar sistemas de copia de seguridad que eviten las pérdidas y aumenten la disponibilidad.
- **Copias de seguridad periódicas:** realizar copias de seguridad frecuentes para protegerse de la corrupción o la pérdida de datos.
- **Supervisión y alertas:** configurar los sistemas de supervisión para detectar y alertar a las partes interesadas de los problemas de datos en tiempo real.
- **Planes de recuperación ante desastres:** desarrollar y probar planes para recuperar los datos y reanudar las operaciones rápidamente después de una interrupción.



3

La relación entre el gobierno, la seguridad y la IA responsable

Juntos, el gobierno y la seguridad de los datos conforman la columna vertebral de un uso responsable de la IA. Los datos seguros y de alta calidad garantizan que la IA funcione de manera ética y eficaz. Las áreas clave que se deben evaluar son la clasificación de datos, los controles de acceso, el cifrado, la respuesta a incidentes y el cumplimiento normativo.

Clasificación de los datos

La clasificación de los datos es una parte fundamental para controlar cómo las herramientas de IA manejan la información confidencial. Normalmente, los datos y las reuniones se clasifican como generales, confidenciales o altamente confidenciales. Una clasificación adecuada garantiza que la IA solo acceda a la información adecuada, lo que reduce el riesgo de exponer datos confidenciales a usuarios no autorizados.

Por otro lado, una mala clasificación puede hacer que la IA procese datos que deban restringirse, lo que puede dar lugar a infracciones de seguridad o problemas de cumplimiento. El gobierno eficaz de los datos, ya sea a través de herramientas automatizadas o políticas de usuarios finales, garantiza que los datos se clasifiquen correctamente, protegiendo la información confidencial y respaldando la capacidad de la IA de ofrecer resultados fiables y conformes a las normativas.

Controles de acceso

Estos controles regulan quién puede acceder a los datos relevantes de la IA y qué aplicaciones o identidades tienen permiso para interactuar con esos datos. Los controles de acceso débiles pueden dar lugar a la exposición no autorizada de información confidencial, lo que aumenta el riesgo de infracciones y uso indebido.

El gobierno de los datos desempeña un papel crucial en la aplicación de estos controles al restringir el acceso a los datos al personal autorizado y a aplicaciones específicas, garantizando así que los datos confidenciales se gestionen adecuadamente. Esto no solo protege la integridad de los datos, sino que también garantiza que los sistemas de IA funcionen en conjuntos de datos seguros y fiables, lo que mejora su fiabilidad y cumplimiento.

Cifrado

Proteger los datos de la interceptación y la manipulación mediante el cifrado ayuda a garantizar que las herramientas de IA generativa puedan fundamentar sus respuestas en el contexto correcto (como datos relacionados con el trabajo, archivos, chats y correos electrónicos) sin riesgo de fuga de datos.

Las políticas de gobierno de los datos pueden exigir prácticas de cifrado robustas que protejan los datos a lo largo de su ciclo de vida. Este enfoque garantiza que las herramientas de IA puedan ofrecer respuestas fiables manteniendo la seguridad de los datos y la confianza.

Respuesta a incidentes

Los datos confidenciales de la organización pueden quedar expuestos a través de incidentes relacionados con herramientas de IA generativa que conceden acceso no autorizado a archivos, correos electrónicos u otros datos empresariales que los sistemas utilizan para generar respuestas.

Un plan de respuesta a incidentes proactivo es crucial en estas situaciones. Sin este plan, la organización no solo se arriesga a exponer datos confidenciales, sino que también confía en resultados poco fiables de la IA. El gobierno de los datos incluye disponer de protocolos de respuesta detallados para abordar rápidamente las infracciones, minimizar su impacto y preservar la fiabilidad de los sistemas de IA.

Cumplimiento normativo

Las aplicaciones de IA deben cumplir normativas como el GDPR o la CCPA, que rigen la protección y la privacidad de los datos. El incumplimiento puede conllevar sanciones significativas y erosionar la confianza. También es crucial saber dónde procesan los datos las herramientas de IA, ya que muchas herramientas gratuitas pueden manejar los datos de forma global o fuera de las ubicaciones de almacenamiento habituales de tu empresa. El gobierno de los datos garantiza que las aplicaciones de IA no solo se ejecuten dentro de los marcos legales, sino que también mantengan los datos dentro de los límites de servicio adecuados, de acuerdo con los estándares de cumplimiento de tu organización. Este enfoque respalda el uso ético de la IA y ayuda a generar confianza en la tecnología de IA.

4

Actualizar tu marco de gobierno de los datos para respaldar la adopción de la IA

En el cambiante panorama de la IA, es importante identificar áreas específicas de tu marco de gobierno de datos existente que puedan requerir una atención especial. En lugar de revisar todo el marco de trabajo, puedes centrarte en las áreas que tienen más probabilidades de cambiar, dirigiendo tus esfuerzos allí donde la IA proporcionará más valor y garantizando al mismo tiempo que tus datos permanezcan protegidos y seguros. Estos son algunos aspectos clave que debes tener en cuenta:

Adaptar las políticas y los procedimientos

La IA implica nuevos tipos de recopilación, procesamiento y uso de los datos. La actualización de las políticas de datos puede ayudar a abordar las necesidades relevantes en torno a la privacidad de los datos, el cumplimiento normativo y el uso ético. Por ejemplo, exigir la anonimización de los datos en casos específicos puede proteger la información personal, haciéndola más segura durante todo el ciclo de vida de la IA.

Roles y responsabilidades

Es esencial incorporar la preparación de la IA en todos los roles relacionados con el gobierno de los datos. Los empleados familiarizados con los requisitos de datos de la IA pueden actuar como administradores para respaldar la calidad de los datos y el cumplimiento normativo. La colaboración multifuncional entre los equipos jurídico, de TI y de ciencia de datos puede ayudar a abordar los desafíos específicos de la IA de manera más eficaz.

Adaptar los estándares y las definiciones de datos

La estandarización de formatos, definiciones y métricas de calidad simplifica la implementación de políticas que rigen el uso de herramientas de IA dentro de una organización. Con unos estándares de datos claros, será más sencillo decidir qué conjuntos de datos pueden utilizar las herramientas de IA para proporcionar contexto empresarial y qué datos pueden cargar los usuarios para su análisis. Esto garantiza que las aplicaciones de IA utilicen los datos más pertinentes y fiables, lo que mejora su eficacia y respalda el cumplimiento de las políticas de la organización.

Mejora continua

El gobierno de los datos es un proceso continuo, especialmente con la IA. Las auditorías y actualizaciones periódicas de tu marco de gobierno pueden ayudarte a adaptarlo a los nuevos desarrollos de IA y a los cambios normativos. La propia IA se puede utilizar para comprobar y mejorar las prácticas de gobierno, encontrar posibles deficiencias y sugerir mejoras. Este enfoque proactivo mejora el cumplimiento y la eficiencia a medida que las tecnologías de IA evolucionan.

Herramientas y técnicas para un gobierno eficaz de los datos

Alinearlo con los objetivos del negocio: asegúrate de que tu estrategia de gobierno de los datos respalda los objetivos de la organización para mejorar la toma de decisiones y la eficiencia.

Automatizar las tareas rutinarias: utiliza la automatización para tareas repetitivas como la clasificación de datos y la administración de acceso para reducir los errores manuales y mejorar la seguridad.

Garantizar altos estándares de precisión: utiliza herramientas de validación y limpieza para apoyar la integridad de los datos a lo largo del tiempo.

Formar a los usuarios: ofrece formación en herramientas y procedimientos de gobierno de los datos para evitar una mala gestión y garantizar el cumplimiento de las políticas

Realizar auditorías periódicas: revisa periódicamente las prácticas de datos para asegurarte de que se mantienen al día con los cambios normativos y organizativos.

Conclusión

Gobierno de datos eficaz para la habilitación de la IA con Microsoft 365

El uso responsable de la IA requiere un buen gobierno de los datos. Un gobierno eficaz de los datos garantiza la disponibilidad, la precisión y la seguridad de los datos, lo que permite a la IA ofrecer conocimientos fiables y fomentar la innovación. Priorizar la calidad de los datos, el cumplimiento y la seguridad mejora las funcionalidades de la IA, lo que a su vez mejora la toma de decisiones y permite mantener una ventaja competitiva.

Microsoft 365: preparando a las organizaciones para la IA

Microsoft 365 ofrece las mejores aplicaciones de productividad de su clase con herramientas integradas para clasificación, control y protección de los datos. Estas características respaldan tu marco de gobierno de los datos, lo que simplifica la adopción segura de la IA cuando estés listo. Microsoft 365 te ayuda a garantizar:

- **La calidad de los datos:** respalda la precisión y fiabilidad de los resultados de la IA.
- **El cumplimiento:** cumple los requisitos normativos, reduciendo los riesgos legales.
- **La seguridad de Confianza cero:** protege la información confidencial del acceso no autorizado, las infracciones y las ciberamenazas

Descubre herramientas de productividad completas mejoradas con opciones de IA y una protección robusta para ayudar a tu organización a trabajar de manera eficiente y segura.

Explora Microsoft 365