Ficha Técnica - Herramientas y Modelos de IA

Herramienta	**Microsoft 365 Copilot**
Fecha	**21-feb-25**

Especificaciones generales del modelo

Atributos del modelo y otras especificaciones	Comentarios
Nombre del modelo	GPT-4
Propietario del modelo	OpenAI
Tipo de modelo (valoración, pronóstico, escenario, etc.)	Procesamiento de Texto e imágenes
Tipo de tecnología del modelo (combinaciones de regresión IA, tipo de ingeniería financiera, etc.)	- Modelos de lenguaje grandes (LLM) basados en arquitecturas similares a GPT (Generative Pre-trained Transformer). -Regresión avanzada para predicciones personalizadas -Machine Learning (ML) y Deep Learning (DL) para el aprendizaje contextual continuo -Integración con Azure Cognitive Services y Azure OpenAI Service.
Modelo interno o de proveedor	Proporcionado por Microsoft mediante Azure OpenAI Service y soluciones de Copilot integradas en productos como Microsoft 365, Dynamics 365 y Power Platform.
Propósito y uso comercial previsto	Aumentar la productividad y eficiencia de la Rama Judicial, mediante la automatización de tareas, generación de contenido, programación y análisis de datos.
Restricciones de uso	Regulaciones de cumplimiento y privacidad: -Cumple con estándares como GDPR, ISO 27001, HIPAA, SOC 1/2/3. Limitaciones contractuales: -Uso restringido al entorno licenciado de Microsoft 365 y Azure. -Prohibido el uso para generación de contenido ilegal, malicioso o discriminatorio. Uso ético: -Debe alinearse con los principios de IA responsable de Microsoft.
Tipos y fuentes de entrada	Tipos de entrada: -Lenguaje natural (texto o voz). -Código fuente. -Datos estructurados y no estructurados. Fuentes de entrada: -Correo electrónico, documentos, reuniones. -Datos de Azure (bases de datos, almacenamiento). -Entradas de aplicaciones integradas en Power Platform.
Salida de datos (usuarios posteriores, incluidos modelos)	Texto y respuesta Generativas Código y automatización Análisis y Visualización de datos Generación de imágenes
Problemas y limitaciones del modelo / controles compensatorios	Problemas potenciales: -Respuestas generadas pueden carecer de contexto completo. -Posibilidad de sesgos inherentes en el modelo de lenguaje. -Limitaciones en la comprensión de datos altamente especializados. Por lo anterior, es necesario realizar las siguientes acciones: -Revisión humana: Validación de salidas críticas antes de su uso. -Actualización continua: Mejoras del modelo mediante Azure OpenAI Service.- -Monitoreo de uso: Herramientas de supervisión para evitar uso indebido. -Controles de acceso: Autenticación y autorización robustas a través de Azure Active Directory.
Versión y fecha de puesta en producción	16 de marzo de 2023 https://news.microsoft.com/es-es/2023/03/16/microsoft-anuncia-microsoft-365-copilot-tu-copiloto-para-el-trabajo

Clasificación de control de estrategias y políticas de modelos de IA

Consideraciones para evaluar la estrategia, las políticas y el perfil de riesgo	**Respuesta** (Sí/No)	**Comentarios**
Colabora con las partes interesadas para preparar una estrategia de gestión de riesgos que aborde los riesgos estratégicos, técnicos, regulatorios y operativos en el uso de casos y modelos de IA. La estrategia define cuándo y cómo la empresa utilizará la IA y establece el propósito de los casos de uso de IA.	Sí	**programa de Evaluaciones de Soluciones de Microsoft.** Este programa ofrece evaluaciones diseñadas para ayudar a las organizaciones a analizar su entorno informático y proporcionar recomendaciones sobre cómo optimizar sus recursos tecnológicos. En particular, esta página parece estar relacionada con la recopilación de comentarios sobre las evaluaciones realizadas, permitiendo a los participantes proporcionar retroalimentación sobre su experiencia con el programa https://www.microsoft.com/en-us/solutionassessments/safeedbackform?msockid=082216d8bedd6faa0a0d04ffbadd69ea
Colabora con las partes interesadas para desarrollar políticas de modelos de IA que aborden principios para una aplicación justa y ética, el uso y protección de datos sensibles o privados, la interacción de los sistemas de IA con los consumidores, la explicabilidad, la evaluación y garantía de niveles aceptables de sesgo y equidad, así como la educación a nivel empresarial.	Sí	Microsoft establece un enfoque basado en principios para el desarrollo y uso responsable de la inteligencia artificial (IA). Su marco de trabajo se centra en seis pilares fundamentales: equidad, confiabilidad y seguridad, privacidad y seguridad, inclusión, transparencia y responsabilidad. Estos principios guían la creación de sistemas de IA diseñados para ser seguros, éticos y accesibles. Además, la compañía ha desarrollado un Estándar de Inteligencia Artificial Responsable que proporciona directrices para el diseño, desarrollo y prueba de soluciones de IA, asegurando su alineación con valores éticos y sociales. La información incluye recursos y herramientas que facilitan la implementación de estos principios en diversos contextos. https://www.microsoft.com/en-us/ai/principles-and-approach/
Garantiza que los términos y condiciones de uso de las herramientas de IA sean compatibles con la normatividad nacional, lo previsto en el acuerdo y las políticas institucionales, permitiendo la realización de evaluaciones de impacto y el acceso a información sobre los procesos, datos de entrenamiento y el funcionamiento de los algoritmos.(articulo 11 Numeral 7 del acuerdo PCSJA24-12243)	Sí	Microsoft 365 Copilot se compromete a cumplir con las normativas de privacidad y protección de datos aplicables a nivel nacional. Asimismo, se ajusta a normas internacionales de protección de datos los cuales se detallan en el siguienrte enlace: **Datos, privacidad y seguridad para Microsoft 365 Copilot** https://learn.microsoft.com/es-es/copilot/microsoft-365/microsoft-365-copilot-privacy
Informa y garantiza la comprensión del tratamiento de la información ingresada en las herramientas de IA, asegurando que los usuarios conozcan cómo se manejan, almacenan y procesan los datos compartidos y de esta manera dar cumplimiento al artículo 7 Numeral 3 del acuerdo PCSJA24-12243.	Sí	Microsoft cumple con normativas de privacidad y protección de datos. No obstante, con relación a los datos a lo que accede, Microsoft Copilot no los utiliza para entrenar los modelos de IA que utiliza. **Datos, privacidad y seguridad para Microsoft 365 Copilot** https://learn.microsoft.com/es-es/copilot/microsoft-365/microsoft-365-copilot-privacy

Clasificación de la función de desarrollo de modelos y gestión de riesgos

Funciones de desarrollo del modelo y calificación del riesgo	Respuesta (Yes/No)	Comentarios
Declaración clara del propósito para garantizar que el modelo desarrollado esté alineado con el uso previsto	Sí	Microsoft 365 Copilot es un asistente de inteligencia artificial diseñado para integrarse con las aplicaciones empresariales de Microsoft, como Word, Excel, PowerPoint, Outlook y Teams. Su objetivo es mejorar la productividad y creatividad de los usuarios al automatizar tareas rutinarias y proporcionar asistencia en tiempo real. Además, ofrece herramientas como Copilot Chat y Copilot Studio, que permiten la creación de agentes personalizados para optimizar flujos de trabajo específicos. Microsoft 365 Copilot se ofrece como un complemento adicional a las suscripciones existentes de Microsoft 365 para empresas, garantizando altos estándares de seguridad, privacidad y cumplimiento normativo. https://www.microsoft.com/en-us/microsoft-365/copilot/enterprise
El diseño, la teoría y la lógica subyacente del modelo están documentados y, en general, respaldados por investigaciones publicadas cuando están disponibles, buenas prácticas de la industria y una evaluación de alternativas cuando sea aplicable	Sí	**Arquitectura y Funcionamiento de Microsoft 365 Copilot** Este documento describe la estructura y el flujo de trabajo de Microsoft 365 Copilot, un asistente de inteligencia artificial diseñado para integrarse en aplicaciones como Word, Excel, PowerPoint y Teams. Su funcionamiento se basa en el procesamiento de solicitudes de los usuarios, la recuperación de datos relevantes y la generación de respuestas mediante modelos de lenguaje avanzados. **Flujo de trabajo** Entrada del usuario: Se ingresa una solicitud dentro de una aplicación de Microsoft 365. Preprocesamiento (Grounding): Copilot refina la solicitud utilizando datos accesibles dentro del entorno de Microsoft Graph, asegurando que la respuesta sea contextual y precisa. Generación de respuesta: Se envía la solicitud refinada a un modelo de lenguaje grande (LLM), que genera una respuesta basada en los datos disponibles. Entrega de la respuesta: Copilot devuelve la información generada dentro de la aplicación donde se originó la solicitud. **Seguridad y Privacidad de los Datos** Copilot solo accede a información que el usuario tiene permiso para ver, respetando las políticas de seguridad de Microsoft 365. La transmisión de datos está protegida mediante cifrado, y el usuario puede revisar o eliminar su historial de interacciones. **Cumplimiento de Normativas de Seguridad** Se aplican controles como Acceso Condicional y Autenticación Multifactor (MFA), asegurando que solo los usuarios autorizados puedan acceder a la herramienta. https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-architecture
Los usuarios identificaron umbrales para la precisión del modelo y otras medidas de rendimiento en curso	Sí	Nota de Transparencia para Microsoft 365 Copilot". Este documento tiene como objetivo proporcionar una comprensión clara de cómo funciona la tecnología de inteligencia artificial (IA) de Microsoft, específicamente Microsoft 365 Copilot, y cómo se integra en el entorno empresarial. Además, ofrece información sobre las decisiones que los administradores del sistema pueden tomar para influir en el rendimiento y comportamiento del sistema, destacando la importancia de considerar el sistema en su totalidad: la tecnología, las personas y el entorno. **Aspectos clave de Microsoft 365 Copilot:** **Integración con aplicaciones de Microsoft 365**: Microsoft 365 Copilot es una herramienta de productividad impulsada por IA que se integra con aplicaciones como Word, Excel, PowerPoint, Outlook y Teams. **Uso de Modelos de Lenguaje de Gran Escala (LLMs)**: Utiliza LLMs proporcionados por el servicio Azure OpenAI para ofrecer asistencia inteligente en tiempo real, adaptándose a las necesidades específicas de cada función, como velocidad o creatividad. **Acceso a datos a través de Microsoft Graph:** Copilot accede a datos y contexto mediante Microsoft Graph, lo que le permite generar respuestas basadas en la información organizacional a la que el usuario tiene permiso de acceso. **Términos clave definidos en la nota:** **"User Prompt" (Solicitud del usuario):** Texto que el usuario envía a Copilot para ejecutar una tarea o proporcionar información. **"Grounding" (Fundamentación):** Proceso de proporcionar fuentes de entrada al LLM relacionadas con la solicitud del usuario para generar respuestas más precisas y contextuales. **"Enriched Prompt" (Solicitud enriquecida):** Solicitud que se ha mejorado con instrucciones adicionales para guiar a Copilot en la generación de una respuesta más específica y relevante. https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-transparency-note

	Modelos de IA específicos - Consideraciones sobre el marco y estándares de los modelos de IA:		
A	Herramientas de explicación del modelo, detección de sesgo y monitoreo de desempeño deben estar integradas en los sistemas para garantizar una supervisión constante y consistente.	Sí	Microsoft ha publicado una "Nota de transparencia para Microsoft 365 Copilot" que detalla las técnicas utilizadas para evaluar las limitaciones y vulnerabilidades del sistema, incluyendo pruebas de equipo rojo para identificar posibles riesgos.
B	Se han desarrollado metodologías de evaluación de riesgos para el portafolio de modelos de IA, que incluyen la evaluación de la explicabilidad del modelo y el potencial de sesgo o falta de equidad, priorizando los sistemas de IA críticos	Sí	privacidad, seguridad y protección de datos en Microsoft 365 Copilot. Microsoft 365 Copilot maneja los datos organizacionales, las medidas implementadas para proteger la información y cómo se asegura el cumplimiento de normativas como el Reglamento General de Protección de Datos (GDPR) y las políticas de residencia de datos en la Unión Europea (EU Data Boundary). **Uso de datos organizacionales:** Microsoft 365 Copilot accede al contenido y contexto a través de Microsoft Graph, utilizando datos como documentos, correos electrónicos, calendarios, chats, reuniones y contactos a los que el usuario tiene permiso de acceso. Es importante destacar que las solicitudes (prompts), respuestas y datos accedidos mediante Microsoft Graph no se utilizan para entrenar los modelos de lenguaje subyacentes. **Protección de la información:** Copilot opera con múltiples protecciones, incluyendo el bloqueo de contenido dañino, la detección de material protegido y la prevención de inyecciones de comandos maliciosos. Además, se asegura de que solo se muestren datos a los que los usuarios tienen permisos adecuados, respetando los modelos de permisos establecidos en servicios como SharePoint. Almacenamiento de datos de interacción: Las interacciones de los usuarios con Copilot, como las solicitudes y respuestas generadas, se manejan de manera que se alineen con los compromisos actuales de privacidad, seguridad y cumplimiento de Microsoft 365. **Compromisos de residencia de datos:** Microsoft 365 Copilot cumple con las políticas de residencia de datos, asegurando que el procesamiento y almacenamiento de la información se realice conforme a las regulaciones aplicables en cada región, incluyendo el GDPR y las directrices de la Unión Europea. **Opciones de extensibilidad:** El documento también aborda las opciones disponibles para extender las funcionalidades de Copilot, permitiendo a las organizaciones personalizar y adaptar la herramienta según sus necesidades específicas. **Cumplimiento normativo**: Microsoft 365 Copilot está diseñado para cumplir con las obligaciones de privacidad y cumplimiento existentes, proporcionando a las organizaciones las herramientas necesarias para gestionar y proteger sus datos de acuerdo con las regulaciones aplicables. https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-privacy
	Se han desarrollado estándares para planes de monitoreo continuo que sean apropiados, considerando los riesgos inherentes de cada modelo de IA. Los planes de monitoreo deben alinearse con las evaluaciones de riesgo relevantes y considerar el desempeño, la estabilidad y la alineación con el propósito comercial	Sí	Microsoft Copilot cumple con los estándares de planes de monitoreo continuo, considerando los riesgos inherentes de cada modelo de IA, a través de las siguientes prácticas: -Evaluaciones de Impacto de IA Responsable para identificar posibles resultados positivos y negativos de sus sistemas de IA en diversos escenarios - Monitoreo Continuo utilizando conjuntos de datos diversos que representan múltiples escenarios, permitiendo identificar y mitigar amenazas potenciales de manera proactiva. -Filtros de Contenido y Clasificadores Basados en IA para detectar y reducir el riesgo de generación de contenido dañino, ofensivo o violento -Ciclo de Vida de Desarrollo de Seguridad (SDL) que garantiza la protección contra amenazas como la ejecución remota de código, impidiendo que Copilot ejecute código sin restricciones y sin las debidas medidas de seguridad. -Uso de Microsoft Purview **Hacer que nuestros productos de IA generativa sean más seguros para los consumidores** https://news.microsoft.com/source/latam/noticias-de-microsoft/hacer-que-nuestros-productos-de-ia-generativa-sean-mas-seguros-para-los-consumidores/
	El monitoreo confirma que los controles se aplican de manera continua durante todo el desarrollo del modelo, las pruebas, la implementación y las operaciones en curso.	Sí	Microsoft Copilot Dashboard en Viva Insights para clientes de Microsoft 365. Este panel proporciona a las organizaciones información procesable para maximizar el valor de Copilot, ayudando en la preparación para la implementación de inteligencia artificial, fomentando la adopción basada en cómo la IA está transformando el comportamiento en el lugar de trabajo y midiendo el impacto de Copilot. **Características principales del Microsoft Copilot Dashboard:** **Preparación (Readiness):** Evalúa la elegibilidad técnica, el estado de licenciamiento y la activación de Copilot, mostrando cuántos usuarios están utilizando aplicaciones clave de Microsoft 365 donde Copilot está disponible. **Adopción (Adoption):** Proporciona datos sobre cuántos usuarios están utilizando Copilot, en qué aplicaciones y de qué manera, permitiendo comparar tendencias de adopción entre diferentes grupos y funciones dentro de la organización. **Impacto (Impact):** Mide cómo Copilot añade valor, incluyendo estimaciones del tiempo durante el cual Copilot ha asistido a los empleados en la creación de resultados de mayor calidad y en la realización eficiente de tareas. Sentimiento (Sentiment): Ofrece una visión general de las percepciones y opiniones de los empleados respecto al uso de Copilot, integrando datos de encuestas y comentarios. Acceso y disponibilidad: El Microsoft Copilot Dashboard está disponible para cualquier cliente con una suscripción de Microsoft 365 u Office 365 para empresas, y que tenga una cuenta activa de Exchange Online. No se requiere una licencia paga de Viva Insights ni una licencia de Microsoft 365 Copilot para visualizar el panel. Sin embargo, para inquilinos con más de 50 licencias de Copilot o más de 10 licencias de Viva Insights, el panel incluye capacidades completas con métricas y filtros avanzados. Los usuarios pueden acceder al panel a través de la aplicación Viva Insights en Microsoft Teams o mediante la aplicación web. https://learn.microsoft.com/en-us/viva/insights/org-team-insights/copilot-dashboard

Realiza un análisis de impacto algorítmico para prever y gestionar posibles riesgos asociados al uso de IA, especialmente en lo relacionado con la protección de derechos fundamentales y la mitigación de sesgos. (articulo 11 Numeral 1 del acuerdo PCSJA24-12243)	Sí	Copilot garantiza el respeto y protección de los derechos fundamentales mediante el diseño ético y responsable de sus algoritmos. Esto incluye la implementación de medidas para evitar sesgos y asegurar la equidad en las decisiones asistidas por IA. Microsoft garantiza la primacía de los derechos fundamentales a través de varias iniciativas y principios clave. Aquí te explico cómo lo hacen: **1. Principios de IA Responsable** Microsoft ha establecido principios claros para el desarrollo y uso de la inteligencia artificial (IA), asegurando que se respeten y protejan los derechos fundamentales. Estos principios incluyen la equidad, la fiabilidad y seguridad, la privacidad y seguridad, la inclusión, la transparencia y la responsabilidad1. **2. Declaración Global de Derechos Humanos** Microsoft se compromete a respetar y promover los derechos humanos en todas sus operaciones. Su Declaración Global de Derechos Humanos está basada en la Declaración Universal de Derechos Humanos y otros estándares internacionales, asegurando que sus actividades comerciales respeten y promuevan los derechos humanos2. **3. Prácticas Comerciales Responsables** Microsoft promueve prácticas comerciales responsables que incluyen la integridad en la cadena de suministro, la accesibilidad y la conectividad, y la creación de sociedades justas e inclusivas. Esto incluye iniciativas como el Airband Initiative para cerrar la brecha de conectividad y programas para expandir la accesibilidad tecnológica1. **4. Compromiso con la Privacidad y Seguridad** Microsoft implementa estrictas políticas de privacidad y seguridad para proteger los datos personales y asegurar que la información se maneje de manera segura y ética. Esto incluye el cumplimiento de regulaciones internacionales y la adopción de medidas proactivas para proteger la privacidad de los usuarios3. **5. Transparencia y Explicabilidad** Microsoft se esfuerza por asegurar que sus tecnologías de IA sean transparentes y explicables, permitiendo a los usuarios comprender cómo se toman las decisiones y generando confianza en el uso de estas tecnologías **Microsoft AI Principles** https://www.microsoft.com/en-us/corporate-responsibility/protect-fundamental-rights

Controles de monitoreo de modelos y seguimiento del desempeño para la efectividad en la gestión de riesgos

Consideraciones de monitoreo y seguimiento paa gestión de riesgos	Efectividad del control	Comentarios
Se mantienen procedimientos de control de cambios que definen roles y responsabilidades, así como cambios significativos en el modelo.	Adecuado	Microsoft Copilot implementa procedimientos de control de cambios que definen roles y responsabilidades claras para gestionar cambios significativos en el modelo. Estos procedimientos se basan en los controles de acceso basados en roles (RBAC) existentes en las organizaciones, asegurando que solo los usuarios con los permisos adecuados puedan realizar modificaciones. **Copilot en centros de administración de Microsoft 365** https://learn.microsoft.com/es-es/copilot/microsoft-365/copilot-for-microsoft-365-admin
Las limitaciones del modelo han sido documentadas y son consideradas por los usuarios del modelo.	Adecuado	Microsoft ha publicado una "Nota de transparencia para Microsoft 365 Copilot" que detalla las técnicas utilizadas para evaluar las limitaciones y vulnerabilidades del sistema, incluyendo pruebas de equipo rojo para identificar posibles riesgos. **Nota de transparencia para Microsoft 365 Copilot** https://learn.microsoft.com/es-es/copilot/microsoft-365/microsoft-365-copilot-transparency-note
La documentación del modelo está completa y actualizada.	Adecuado	La documentación es frecuentemente actualizada y se encuentra disponible en el siguiente enlace: https://learn.microsoft.com/es-es/copilot/microsoft-365/

Aplicación de modelos de IA para la calificación de controles de estándares de datos privados			
Consideraciones sobre controles de estándares aplicados a datos privados	**Respuesta** (Sí/No)	**Nivel de riesgo**	**Comentarios**
Determinar cómo se aborda el uso de datos privados en modelos de IA dentro del programa de estrategia y gobernanza de datos.	Sí	No	Copilot no utiliza datos personales en el entrenamiento de sus modelos, garantizando la privacidad y seguridad de la información. Microsoft implementa estrictas políticas de privacidad para proteger los datos de los usuarios y asegurar que no se utilicen de manera inapropiada. **1. Privacidad de los Datos** Microsoft Copilot está diseñado para proteger la privacidad de los datos de los usuarios. Esto incluye: **Minimización de Datos**: Solo se recopilan los datos necesarios para proporcionar las funcionalidades de Copilot. Anonimización y Pseudonimización: Los datos personales se anonimizan o pseudonimizan para proteger la identidad de los usuarios. Cumplimiento de Regulaciones: Copilot cumple con regulaciones internacionales de privacidad, como el GDPR en Europa y la CCPA en California1. 2. Seguridad de los Datos Microsoft implementa varias capas de seguridad para proteger los datos: Cifrado: Los datos se cifran tanto en tránsito como en reposo para prevenir accesos no autorizados. Control de Acceso: Se utilizan controles de acceso estrictos para asegurar que solo el personal autorizado pueda acceder a los datos. Monitoreo y Detección: Se implementan sistemas de monitoreo y detección de amenazas para identificar y responder a posibles incidentes de seguridad1. **3. Retención y Eliminación de Datos** Políticas de Retención: Los datos se retienen solo durante el tiempo necesario para cumplir con los propósitos para los cuales fueron recopilados. Eliminación Segura: Cuando los datos ya no son necesarios, se eliminan de manera segura para prevenir su recuperación no autorizada1. **4. Transparencia y Control del Usuario** Acceso y Control: Los usuarios tienen acceso a sus datos y pueden controlar cómo se utilizan. Solicitudes de Datos Personales: Los usuarios pueden solicitar la eliminación o corrección de sus datos personales a través de procesos establecidos1. **5. Cumplimiento y Auditorías** Auditorías Regulares: Microsoft realiza auditorías regulares para asegurar el cumplimiento de sus políticas de privacidad y seguridad. Certificaciones: Copilot cuenta con varias certificaciones de cumplimiento, como ISO/IEC 27001 y SOC 2 https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-architecture

Se evaluó el marco de gestión de datos y el proceso de prueba de datos para datos privados. Las pruebas de datos requieren un marco de gestión de datos efectivo que establezca un conjunto de reglas y estándares para la calidad, integridad y puntualidad de los datos, con consideración por la privacidad, protección y propiedad de los datos. El objetivo del marco debe ser identificar los riesgos asociados con el uso de datos de maneras que violen los permisos de acceso y uso según la política.	Sí	No	privacidad, seguridad y protección de datos en Microsoft 365 Copilot. Microsoft 365 Copilot maneja los datos organizacionales, las medidas implementadas para proteger la información y cómo se asegura el cumplimiento de normativas como el Reglamento General de Protección de Datos (GDPR) y las políticas de residencia de datos en la Unión Europea (EU Data Boundary). **Puntos clave del documento:** **Uso de datos organizacionales**: Microsoft 365 Copilot accede al contenido y contexto a través de Microsoft Graph, utilizando datos como documentos, correos electrónicos, calendarios, chats, reuniones y contactos a los que el usuario tiene permiso de acceso. Es importante destacar que las solicitudes (prompts), respuestas y datos accedidos mediante Microsoft Graph no se utilizan para entrenar los modelos de lenguaje subyacentes. **Protección de la información**: Copilot opera con múltiples protecciones, incluyendo el bloqueo de contenido dañino, la detección de material protegido y la prevención de inyecciones de comandos maliciosos. Además, se asegura de que solo se muestren datos a los que los usuarios tienen permisos adecuados, respetando los modelos de permisos establecidos en servicios como SharePoint. **Almacenamiento de datos de interacción**: Las interacciones de los usuarios con Copilot, como las solicitudes y respuestas generadas, se manejan de manera que se alineen con los compromisos actuales de privacidad, seguridad y cumplimiento de Microsoft 365. **Compromisos de residencia de datos:** Microsoft 365 Copilot cumple con las políticas de residencia de datos, asegurando que el procesamiento y almacenamiento de la información se realice conforme a las regulaciones aplicables en cada región, incluyendo el GDPR y las directrices de la Unión Europea. **Opciones de extensibilidad:** El documento también aborda las opciones disponibles para extender las funcionalidades de Copilot, permitiendo a las organizaciones personalizar y adaptar la herramienta según sus necesidades específicas. **Cumplimiento normativo:** Microsoft 365 Copilot está diseñado para cumplir con las obligaciones de privacidad y cumplimiento existentes, proporcionando a las organizaciones las herramientas necesarias para gestionar y proteger sus datos de acuerdo con las regulaciones aplicables. https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-privacy

Implementa controles específicos de seguridad de la información para los datos consumidos por los modelos de IA, asegurando el cumplimiento de la normativa nacional, los acuerdos institucionales y las políticas adoptadas por el Consejo Superior de la Judicatura. (articulo 11 Numeral 3 del acuerdo PCSJA24-12243			"Se evalúan los riesgos y la transparencia de Copilot para asegurar su uso seguro y ético. Microsoft realiza análisis de impacto para identificar y mitigar posibles riesgos antes de la implementación de sus tecnologías de IA. En el caso de Microsoft Copilot, se evalúan varios riesgos en el análisis de impacto para asegurar su uso seguro y ético. Aquí tienes algunos de los principales riesgos que se consideran: Seguridad de los datos: Se evalúa la protección de los datos confidenciales que Copilot procesa o genera, incluyendo la prevención de pérdidas de datos y el acceso no autorizado1. Privacidad: Se asegura que Copilot cumpla con los compromisos de privacidad, garantizando que los datos personales no se utilicen de manera inapropiada y que se respeten las políticas de privacidad de Microsoft1. Solidez del modelo: Se analiza la robustez de los modelos de IA utilizados por Copilot para asegurar que funcionen correctamente y no sean vulnerables a manipulaciones o errores1. Ciberataques: Se identifican y mitigan posibles vulnerabilidades de seguridad que podrían ser explotadas por ciberataques, incluyendo pruebas rigurosas y ejercicios de formación de equipos rojos1. Transparencia y explicabilidad: Se evalúa la capacidad de Copilot para proporcionar explicaciones claras y comprensibles sobre cómo se toman las decisiones, lo que ayuda a generar confianza en los usuarios1. Impacto social y ético: Se consideran los posibles efectos sociales y éticos del uso de Copilot, incluyendo la equidad, la no discriminación y el impacto en el empleo1. Estos riesgos se abordan mediante una combinación de prácticas de seguridad rigurosas, medidas de seguridad proactivas y un enfoque de defensa en profundidad para proteger las herramientas de productividad como Microsoft 365 Copilot1. **Microsoft Responsible AI Standard** https://learn.microsoft.com/es-es/copilot/microsoft-365/microsoft-365-copilot-ai-security
Aplica medidas que garantizan que los datos personales y/o confidenciales no sean utilizados en los procesos de entrenamiento de los modelos de IA, asegurando la protección de la privacidad y el cumplimiento de la normativa vigente. (Articulo 11. numeral 5 del acuerdo PCSJA24-12243)	Sí		Microsoft 365 Copilot se compromete a proteger la privacidad y seguridad de los datos personales y confidenciales de sus usuarios. Para garantizar que estos datos no se utilicen en el entrenamiento de modelos de inteligencia artificial, Microsoft ha implementado las siguientes medidas: -No utilización de datos para entrenamiento: Las solicitudes y respuestas generadas a través de Microsoft 365 Copilot, así como los datos accedidos mediante Microsoft Graph, no se emplean para entrenar los modelos de lenguaje de gran escala (LLM). -Protección de datos empresariales: Microsoft 365 Copilot Chat implementa protecciones de datos empresariales para salvaguardar la información de las organizaciones. Esto incluye controles y compromisos detallados en el Anexo de Protección de Datos (DPA) y los Términos del Producto. **Privacidad y protección** https://learn.microsoft.com/es-es/copilot/privacy-and-protections

Aplicación de modelos de IA para la calificación de controles de estándares de gestión de datos			
Consideraciones para evaluar la gestión de datos y el perfil de riesgo	**Respuesta** (Sí/No)	**Nivel de riesgo**	**Comentarios**
Se evaluaron los procesos para garantizar que los cambios dinámicos en los datos del modelo sean monitoreados y evaluados en comparación con los datos de entrenamiento, con el fin de confirmar la calidad de los datos y la consistencia estadística de los nuevos datos con los datos de entrenamiento, así como asegurar que el proceso de generación de datos sea coherente con los datos de entrenamiento	Sí	No	Microsoft 365 Copilot implementa un marco de protección de datos y auditoría para garantizar la seguridad y el cumplimiento normativo dentro de las organizaciones. Se centra en la interacción con etiquetas de confidencialidad de Microsoft Purview, la prevención del uso compartido excesivo de datos en SharePoint y OneDrive, y la disponibilidad de herramientas de auditoría y retención de datos de uso de Copilot. Protección de datos y cifrado **Etiquetas de confidencialidad:** Copilot respeta las etiquetas y el cifrado de Microsoft Purview, asegurando que los archivos protegidos mantengan sus configuraciones de privacidad. **Permisos y restricciones**: Para procesar archivos con cifrado, el usuario debe tener permisos de EXTRACT y VIEW, lo que garantiza un acceso seguro. **Herencia de etiquetas:** El contenido generado hereda la etiqueta de mayor prioridad de los documentos utilizados como referencia. Controles de seguridad en SharePoint y OneDrive **Restricción de búsqueda:** Se pueden definir sitios específicos en SharePoint donde Copilot puede acceder a información, minimizando la exposición de datos. Controles de uso compartido: Se aplican configuraciones predeterminadas para evitar la exposición excesiva de documentos. **Supervisión de accesos:** SharePoint permite generar informes sobre sitios con contenido sensible o permisos amplios. Auditoría y retención de datos Registro de interacciones: Los datos de uso de Copilot se almacenan dentro del inquilino de Microsoft 365 de la organización. Acceso a registros: Se pueden consultar auditorías detalladas para monitorear la actividad de los usuarios. Políticas de retención: Las organizaciones pueden definir períodos de almacenamiento de registros para cumplir con requisitos legales y normativos. https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-architecture-data-protection-auditing
Garantiza la calidad de los datos utilizados en los modelos de IA mediante procesos de validación, reducción de sesgos y mitigación de alucinaciones, asegurando su integridad, precisión y fiabilidad. (articulo 11 Numeral 4 del acuerdo PCSJA24-12243	Sí	No	Copilot implementa medidas para garantizar la calidad de los datos utilizados en sus modelos de inteligencia artificial (IA), enfocándose en procesos de validación, reducción de sesgos y mitigación de alucinaciones. Estas prácticas aseguran la integridad, precisión y fiabilidad de los datos, cumpliendo con estándares éticos y normativos. **Datos, privacidad y seguridad para Microsoft 365 Copilot en Viva Engage** https://learn.microsoft.com/es-es/viva/engage/manage-security-and-compliance/data-privacy-security-copilot-engage
Realiza un análisis de impacto de privacidad y protección de datos para evaluar las implicaciones del uso de herramientas de IA en relación con los derechos de privacidad y protección de datos de los usuarios y terceros, estableciendo medidas para mitigar riesgos y garantizar el cumplimiento normativo. (articulo 11 Numeral 6 del acuerdo PCSJA24-12243)	Sí	No	Copilot implementa medidas para garantizar la privacidad y protección de los datos de los usuarios, cumpliendo con normativas como el Reglamento General de Protección de Datos de la Unión Europea. Las solicitudes, respuestas y los datos a los que se accede a través de Microsoft Graph no se utilizan para entrenar los modelos de lenguaje de gran escala (LLM). **Datos, privacidad y seguridad para Microsoft 365 Copilot** https://learn.microsoft.com/es-es/copilot/microsoft-365/microsoft-365-copilot-privacy

Calificación de la aplicación de modelos de IA en los controles de estándares de transparencia			
Consideraciones sobre controles de estándares aplicados a la transparencia de los modelos	**Respuesta** (Sí/No)	**Nivel de riesgo**	**comentarios**
Se determinó que los estándares y objetivos de transparencia para los modelos de IA están abordados por la política a nivel empresarial y alineados con el apetito de riesgo.	Sí	No	Nota de Transparencia para Microsoft Copilot explica el funcionamiento de la inteligencia artificial utilizada en Copilot, detallando las decisiones tomadas por Microsoft que impactan su rendimiento y comportamiento. Se enfoca en brindar claridad sobre cómo opera Copilot, permitiendo a los usuarios comprender su alcance, las medidas de seguridad implementadas y las formas en que pueden controlar su experiencia. Este recurso forma parte del compromiso de Microsoft con el desarrollo responsable de la IA, aplicando principios como equidad, privacidad, seguridad y transparencia en el diseño y despliegue de sus soluciones. https://support.microsoft.com/en-us/topic/transparency-note-for-microsoft-copilot-c1541cad-8bb4-410a-954c-07225892dbc2

Se evaluó que los usuarios del modelo pueden abordar los siguientes aspectos de los modelos de IA: comprender cómo el algoritmo toma los datos de entrada y toma una decisión, tener visibilidad del conjunto de datos utilizado para entrenar el modelo, comprender los métodos utilizados para seleccionar los datos de entrenamiento y comprender las posibles fuentes de sesgo que existen en los conjuntos de datos de entrenamiento.	Sí	No	Nota de Transparencia para Microsoft Copilot explica el funcionamiento de la inteligencia artificial utilizada en Copilot, detallando las decisiones tomadas por Microsoft que impactan su rendimiento y comportamiento. Se enfoca en brindar claridad sobre cómo opera Copilot, permitiendo a los usuarios comprender su alcance, las medidas de seguridad implementadas y las formas en que pueden controlar su experiencia. Este recurso forma parte del compromiso de Microsoft con el desarrollo responsable de la IA, aplicando principios como equidad, privacidad, seguridad y transparencia en el diseño y despliegue de sus soluciones. https://support.microsoft.com/en-us/topic/transparency-note-for-microsoft-copilot-c1541cad-8bb4-410a-954c-07225892dbc2

Aplicación de modelos de IA para la calificación de controles de estándares de explicabilidad			
Consideraciones para evaluar la gestión del riesgo de explicabilidad y el perfil de riesgo	**Respuesta** (Sí/No)	**Nivel de riesgo**	**Comentarios**
Se evaluó que el proceso de desarrollo del modelo respalda la explicabilidad de cada modelo de IA en las cinco dimensiones relevantes: algoritmos, datos de entrenamiento, selección de datos de entrenamiento, sesgo en los datos de entrenamiento y comprensión de cómo los modelos se desempeñan en diferentes escenarios de producción	Sí	No	Microsoft sigue principios éticos para asegurarse de que sus IA sean explicables y justifica su desempeño en contextos de producción. Iniciativas en el contexto de transparencia en algoritmos, gestión de riesgo y evaluación continua de desempeño han sido implementadas. **Datos, privacidad y seguridad para Microsoft 365 Copilot** https://learn.microsoft.com/es-es/copilot/microsoft-365/microsoft-365-copilot-privacy
El proceso de desarrollo registra cuáles resultados son y no son explicables y aplica diferentes enfoques de mitigación de riesgos para aquellos que no son explicables, según la prioridad de clasificación del riesgo.	Sí	No	Microsoft 365 Copilot implementa un proceso de desarrollo que registra y aborda la explicabilidad de sus modelos de inteligencia artificial (IA) a través de: - Evaluación de riesgos y mitigación: permite identificar y documentar amenazas potenciales para la salud de un proyecto, incluyendo aspectos relacionados con la explicabilidad de los modelos de IA. - Pruebas de equipo rojo: emplea técnicas de pruebas de equipo rojo para evaluar las limitaciones y vulnerabilidades de sus sistemas de IA. **Nota de transparencia para Microsoft 365 Copilot** https://learn.microsoft.com/es-es/copilot/microsoft-365/microsoft-365-copilot-transparency-note

Aplicación de modelos de IA para la calificación de principios de equidad y controles de mitigación de riesgo de sesgo			
Consideraciones para evaluar la equidad del modelo de IA y el riesgo de sesgo	**Respuesta** (Sí/No)	**Nivel de riesgo**	**Comentarios**
Evaluar cómo se aplican las técnicas de mitigación de sesgo a lo largo de todo el ciclo de vida del modelo de IA. Determinar que el rendimiento del modelo se monitorea continuamente para identificar y evaluar posibles sesgos.	Sí	No	Microsoft 365 Copilot se desarrolla con un enfoque en la seguridad, la ética y la transparencia en la inteligencia artificial. Su implementación sigue estándares rigurosos para mitigar riesgos y garantizar el cumplimiento normativo en entornos empresariales. Principales estrategias y compromisos IA responsable y segura: Microsoft integra principios de ética en la IA, abordando la privacidad de datos, la mitigación de sesgos y la transparencia en los procesos de toma de decisiones. Estándar de IA Responsable y Evaluación de Impacto: Todas las soluciones deben cumplir con estos lineamientos para asegurar su alineación con las mejores prácticas de la industria. Compromisos voluntarios con la Casa Blanca: Se implementan principios de seguridad y gobernanza en línea con las regulaciones internacionales y acuerdos gubernamentales. Equipo de Seguridad en IA Generativa: Un grupo especializado supervisa y mejora las defensas frente a riesgos emergentes en la inteligencia artificial generativa. Mitigación de nuevos riesgos: Microsoft adopta un enfoque proactivo para actualizar sus mecanismos de seguridad conforme evolucionan las amenazas y desafíos en la IA. https://techcommunity.microsoft.com/blog/microsoft365copilotblog/how-microsoft-365-delivers-trustworthy-ai/4045596
Proporciona información sobre la procedencia, el tamaño, la distribución y los posibles sesgos de los datos de entrenamiento, permitiendo la evaluación de su calidad, integridad y transparencia. (Articulo 11. numeral 2 del acuerdo PCSJA24-12243)	Sí		Microsoft 365 Copilot aborda la necesidad de proporcionar información sobre la procedencia, tamaño, distribución y posibles sesgos de los datos de entrenamiento mediante Nota de Transparencia (aborda las limitaciones inherentes a los modelos de IA y cómo estos sesgos pueden influir en el comportamiento de Copilot) y Evaluación de Resultados de Modelos: A través de Azure Machine Learning, Microsoft ofrece herramientas para evaluar y comprender los resultados de los experimentos de aprendizaje automático **Nota de transparencia para Microsoft Copilot** https://support.microsoft.com/es-es/topic/transparency-note-for-microsoft-copilot-c1541cad-8bb4-410a-954c-07225892dbc2

Calificación de los controles de gestión de riesgos de seguridad en modelos de IA			
	Respuesta (Sí/No)	**Nivel de riesgo**	**Comentarios**
Los programas de seguridad de aplicaciones de IA se identifican y evalúan en cuanto a cómo abordan aspectos relacionados con ataque de la aplicación de IA, incluidas las aplicaciones de terceros con IA integrada.	Sí		Microsoft Copilot aborda la seguridad de las aplicaciones de IA, incluyendo aquellas de terceros con IA integrada, mediante la integración con Microsoft Security Copilot que ayuda a identificar y mitigar vulnerabilidades en toda la superficie de ataque de las aplicaciones de IA, incluyendo las de terceros **Microsoft Security Copilot** https://www.microsoft.com/en-us/security/business/ai-machine-learning/microsoft-security-copilot

Calificación de los controles de gestión de riesgos de modelos de la herramienta			
Consideraciones para evaluar la gestión de riesgos y el perfil de riesgo de los modelos de la herramienta	**Respuesta** (Sí/No)	**Nivel de riesgo**	**Comentarios**
Incorporar al programa de gestión de riesgos del modelo siguiendo los mismos principios aplicados a los modelos internos.	Sí	No	El Copilot for Microsoft 365 Risk Assessment QuickStart Guide es una herramienta diseñada para ayudar a las organizaciones a evaluar los riesgos asociados con la implementación de Copilot en Microsoft 365. Este recurso proporciona un marco estructurado para identificar posibles riesgos, explorar estrategias de mitigación y facilitar discusiones entre las partes interesadas. Componentes clave del guía: Marco de Riesgos y Mitigaciones de IA: Describe las principales categorías de riesgos asociados con la inteligencia artificial y cómo Microsoft aborda estos desafíos tanto a nivel corporativo como en sus servicios. Evaluación de Riesgos Ejemplar: Presenta una serie de preguntas y respuestas basadas en consultas reales de clientes, abarcando temas como privacidad, seguridad, relaciones con proveedores y desarrollo de modelos. Estas respuestas están respaldadas por equipos especializados de Microsoft y declaraciones directas de OpenAI. Recursos Adicionales: Ofrece enlaces a materiales complementarios que profundizan en la gestión de riesgos de IA y en las características específicas de Copilot para Microsoft 365. https://techcommunity.microsoft.com/blog/microsoft365copilotblog/now-available-the-copilot-for-microsoft-365-risk-assessment-quickstart-guide/4211925
Requerir a los proveedores que proporcionen informes técnicos que expliquen los componentes del modelo, su diseño, estructura, datos y uso previsto.	Sí	No	Microsoft 365 Copilot se integra en las aplicaciones de productividad para proporcionar respuestas en tiempo real basadas en los datos a los que el usuario tiene acceso dentro de su organización. Flujo de trabajo Entrada del usuario: El usuario ingresa una solicitud en aplicaciones como Word, Excel o PowerPoint. Preprocesamiento (Grounding): Copilot refina la solicitud utilizando datos del Microsoft Graph, asegurando que la respuesta sea precisa y contextual. Generación de respuesta: La solicitud procesada se envía a un modelo de lenguaje grande (LLM), que genera una respuesta relevante basada en el contexto del usuario. Entrega de la respuesta: La información generada se muestra dentro de la aplicación para que el usuario la utilice. Privacidad y seguridad de los datos Acceso autorizado: Copilot solo accede a la información que el usuario tiene permisos para ver, respetando los controles de acceso de Microsoft 365. Protección de datos: La transmisión de información está cifrada, y el historial de interacciones se puede revisar o eliminar según sea necesario. Cumplimiento de normativas: Se respetan políticas de seguridad como el acceso condicional y la autenticación multifactor (MFA) para garantizar que solo usuarios autorizados puedan utilizar la herramienta. https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-architecture

	Los proveedores proporcionan resultados de pruebas que evidencian que el modelo funciona como se espera y que indican claramente sus limitaciones y supuestos.	Sí	No	Nota de Transparencia para Microsoft 365 Copilot es un recurso diseñado para explicar el funcionamiento de la tecnología de inteligencia artificial que impulsa a Copilot. Este documento detalla las decisiones tomadas por Microsoft que afectan el rendimiento y comportamiento del sistema, y enfatiza la importancia de considerar todo el ecosistema en el que se despliega la IA. El objetivo es que los usuarios comprendan cómo funciona Copilot, tomen control de sus experiencias y conozcan las medidas implementadas para garantizar un producto seguro y confiable. Esta iniciativa forma parte del compromiso de Microsoft de aplicar sus Principios de IA en la práctica. Aspectos clave de Microsoft 365 Copilot: Integración con aplicaciones de Microsoft 365: Copilot se integra con herramientas como Word, Excel, PowerPoint, Outlook y Teams, proporcionando asistencia en tiempo real para mejorar la productividad y creatividad de los usuarios. Uso de Modelos de Lenguaje de Gran Escala (LLMs): Copilot utiliza LLMs proporcionados por Azure OpenAI Service, seleccionando el modelo más adecuado según las necesidades específicas de cada función, como velocidad o creatividad. Proceso de "Grounding": Para ofrecer respuestas precisas y contextuales, Copilot accede a datos relevantes a través de Microsoft Graph, asegurando que las respuestas estén alineadas con el contexto y contenido del usuario. Protección de datos y privacidad: Microsoft 365 Copilot opera bajo estrictas políticas de privacidad y seguridad, garantizando que los datos de los usuarios se manejen de manera segura y conforme a las normativas vigentes.
	¿El modelo incorpora factores de comportamiento u otros factores ambientales?	Sí	No	Informe de Impacto de Microsoft 365 Copilot es una herramienta diseñada para que los líderes comprendan cómo el uso de Copilot afecta a los empleados en toda la organización. Este informe ofrece información sobre la relación entre la adopción de Copilot y los patrones de colaboración, destacando el número total de horas en las que los empleados fueron "asistidos" por Copilot en su trabajo diario. Secciones principales del informe: Resumen del informe: Proporciona una visión general del número total de usuarios activos de Copilot, el total de acciones realizadas con Copilot y las horas de asistencia proporcionadas por Copilot. Análisis detallado por áreas: Permite evaluar cómo han cambiado los patrones de colaboración después de la implementación de Copilot en las siguientes áreas: Reuniones Chats de Teams Correo electrónico Documentos Microsoft 365 Copilot Chat (trabajo) Además, ofrece comparaciones entre usuarios que utilizan Copilot y aquellos que no, a través de diferentes grupos. Recursos adicionales: Incluye una sección titulada "Aprenda lo que nuestra investigación dice sobre el impacto de Copilot", que ofrece una visión general de artículos de investigación y estudios de caso relacionados con la adopción e impacto de Copilot. Requisitos para generar el informe: Configuración previa: Es necesario configurar y ejecutar con éxito la consulta predefinida de impacto de Microsoft 365 Copilot en Viva Insights para poblar el informe en Power BI. Roles y licencias: Se requiere tener asignado el rol de Analista de Insights en Viva Insights y contar con licencias de Viva Insights. Además, los empleados incluidos en la población medida deben tener asignadas licencias de Microsoft 365 Copilot y Microsoft Viva Insights. Herramientas necesarias: Es imprescindible contar con la versión de Power BI Desktop de junio de 2022 o una más reciente para visualizar y personalizar el informe. https://learn.microsoft.com/en-us/viva/insights/advanced/analyst/templates/microsoft-365-copilot-impact

	El proveedor indica claramente las limitaciones y supuestos del modelo, así como las situaciones en las que su aplicación podría ser problemática.	Sí	No	Problemas conocidos en la extensibilidad de Microsoft 365 Copilot detalla las incidencias actuales relacionadas con la personalización y ampliación de las funcionalidades de Copilot en Microsoft 365, proporcionando soluciones alternativas cuando están disponibles. Principales problemas identificados: Agentes declarativos: Visualización retrasada en Teams: Tras instalar un agente desde la tienda, este puede no aparecer de inmediato en Copilot Chat dentro del cliente de Teams. Solución alternativa: Cambiar a otro chat y luego regresar a Copilot Chat. Compatibilidad limitada con Flujos de Power Automate: Los flujos utilizados como acciones en agentes declarativos pueden no ejecutarse de manera confiable o no devolver resultados. Solución alternativa: No hay una solución definitiva; sin embargo, mejorar la descripción del flujo fuera de Copilot Studio puede aumentar la tasa de activación. Metadatos personalizados no soportados en consultas: Solicitudes que buscan listar elementos basados en metadatos personalizados, como "Obtener una lista de tickets de ServiceNow asignados a mí", no funcionan correctamente debido a la falta de mapeo en el esquema de conexión. Solución alternativa: Actualmente no disponible; se recomienda buscar elementos por título o descripción. Enlaces compartidos de SharePoint no funcionales como fuentes de conocimiento: Cuando se utilizan enlaces compartidos de SharePoint como fuentes de conocimiento en un agente, es posible que no se obtengan resultados. Nombres de archivos en SharePoint con caracteres nulos: Archivos que contienen caracteres nulos en su nombre pueden no devolver resultados cuando se usan como fuentes de conocimiento. Problemas al pegar enlaces en Copilot Studio y el generador de agentes: Pegar directamente la URL de un archivo puede causar fallos en la búsqueda. Solución alternativa: Seleccionar el archivo directamente desde la interfaz de usuario en lugar de pegar la URL. Fallas al compartir agentes en el generador de agentes: Compartir un agente con grupos de distribución puede resultar en errores. Conectores de Microsoft Graph: Limitaciones con metadatos personalizados: Al igual que con los agentes declarativos, las consultas basadas en metadatos personalizados no son compatibles. Plugins de API: Compatibilidad limitada con ciertas características de OpenAPI: Algunas funcionalidades, como objetos anidados en solicitudes, referencias polimórficas y ciertos flujos de autenticación OAuth, no son soportadas.
F	Los proveedores llevan a cabo un monitoreo continuo del rendimiento y análisis de desempeño, con divulgación, y realizan las modificaciones apropiadas y oportunas.	Sí	No	Nota de Transparencia para Microsoft 365 Copilot es un recurso diseñado para explicar el funcionamiento de la tecnología de inteligencia artificial que impulsa a Copilot. Este documento detalla las decisiones tomadas por Microsoft que afectan el rendimiento y comportamiento del sistema, y enfatiza la importancia de considerar todo el ecosistema en el que se despliega la IA. El objetivo es que los usuarios comprendan cómo funciona Copilot, tomen control de sus experiencias y conozcan las medidas implementadas para garantizar un producto seguro y confiable. Esta iniciativa forma parte del compromiso de Microsoft de aplicar sus Principios de IA en la práctica. Aspectos clave de Microsoft 365 Copilot: Integración con aplicaciones de Microsoft 365: Copilot se integra con herramientas como Word, Excel, PowerPoint, Outlook y Teams, proporcionando asistencia en tiempo real para mejorar la productividad y creatividad de los usuarios. Uso de Modelos de Lenguaje de Gran Escala (LLMs): Copilot utiliza LLMs proporcionados por Azure OpenAI Service, seleccionando el modelo más adecuado según las necesidades específicas de cada función, como velocidad o creatividad. Proceso de "Grounding": Para ofrecer respuestas precisas y contextuales, Copilot accede a datos relevantes a través de Microsoft Graph, asegurando que las respuestas estén alineadas con el contexto y contenido del usuario. Protección de datos y privacidad: Microsoft 365 Copilot opera bajo estrictas políticas de privacidad y seguridad, garantizando que los datos de los usuarios se manejen de manera segura y conforme a las normativas vigentes. https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-transparency-note

	Las validaciones independientes aplican los mismos procedimientos que los modelos internos, cuando sea posible.	Sí	No	Verificaciones de Validación de IA Responsable para Agentes Declarativos son procesos implementados para garantizar que los agentes personalizados en Microsoft 365 Copilot cumplan con los estándares de Inteligencia Artificial Responsable (RAI, por sus siglas en inglés). Estas verificaciones se realizan en dos momentos clave: durante la validación del manifiesto al cargar o publicar un agente, y durante el procesamiento de las solicitudes de los usuarios. Componentes principales de la validación: RAI LLM Prompt: Evalúa las indicaciones proporcionadas al modelo de lenguaje para asegurar que sean apropiadas y éticas. Clasificador de Jailbreak: Detecta intentos de eludir las restricciones establecidas en el modelo, evitando usos indebidos o malintencionados. Clasificador de Ofensividad: Identifica contenido potencialmente ofensivo o inapropiado generado por el agente. Causas comunes de fallos en la validación RAI: Fomento de acciones dañinas: El agente incita o apoya conductas violentas, ilegales o poco éticas. Promoción de estereotipos: Refuerza generalizaciones injustas o sesgos hacia grupos sociales. Revelación de información personal: Solicita o divulga datos sensibles de individuos sin consentimiento adecuado. Expresión de creencias personales: Manifiesta opiniones religiosas, filosóficas o políticas de manera que pueda influir indebidamente en los usuarios. Evaluación de desempeño humano: Realiza análisis detallados del rendimiento de individuos, proporcionando retroalimentación que podría considerarse crítica o negativa. https://learn.microsoft.com/en-us/microsoft-365-copilot/extensibility/rai-validation
	Se evaluaron y se consideraron satisfactorios los controles sobre el acceso, transferencia, compartición y almacenamiento de información sensible de los clientes utilizada por el proveedor.	Sí	No	Nota de Privacidad de Microsoft 365 Copilot detalla cómo este asistente de inteligencia artificial maneja los datos organizacionales, garantizando su seguridad y privacidad. Copilot accede a contenido a través de Microsoft Graph, utilizando datos como documentos, correos electrónicos, calendarios y chats a los que el usuario tiene permiso de acceso, para generar respuestas contextuales y relevantes. Es fundamental que las organizaciones configuren adecuadamente los modelos de permisos en servicios como SharePoint para asegurar que solo los usuarios autorizados accedan al contenido correspondiente. Además, las interacciones con Copilot, incluyendo las solicitudes y respuestas generadas, se almacenan de acuerdo con los compromisos contractuales de Microsoft 365, y los usuarios tienen la opción de eliminar su historial de actividad de Copilot a través del portal de Mi Cuenta. Microsoft 365 Copilot cumple con normativas como el Reglamento General de Protección de Datos (GDPR) y los compromisos de residencia de datos de la Unión Europea, asegurando que el procesamiento de datos se realice dentro de los límites geográficos establecidos. Para ampliar las capacidades de Copilot, es posible integrar herramientas y servicios externos mediante conectores de Microsoft Graph o complementos, siempre bajo el control y supervisión de los administradores de TI de la organización. En resumen, Microsoft 365 Copilot está diseñado para ofrecer asistencia inteligente mientras protege la privacidad y seguridad de los datos organizacionales. https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-privacy
	Se establecen planes de contingencia para los modelos críticos en caso de que ya no estén disponibles, no reciban mantenimiento o no sean confiables.	Sí	No	Microsoft adopta una estrategia de defensa robusta para proteger herramientas como Copilot frente a riesgos de seguridad. **Seguridad de la inteligencia artificial para Microsoft 365 Copilot** https://learn.microsoft.com/es-es/copilot/microsoft-365/microsoft-365-copilot-ai-security

Describa el tipo de modelo.	Sí	No	El Microsoft 365 Copilot es un asistente de inteligencia artificial que se integra en las aplicaciones de Microsoft 365, como Word, Excel, PowerPoint, Outlook y Teams, para proporcionar asistencia en tiempo real basada en los datos y el contexto del usuario. Su arquitectura está diseñada para garantizar un acceso seguro y eficiente a la información relevante, respetando siempre los permisos y las políticas de seguridad establecidas por la organización. Flujo de trabajo de Copilot: Entrada del usuario: El usuario ingresa una solicitud o pregunta en una aplicación de Microsoft 365 compatible. Preprocesamiento de la solicitud (Grounding): Copilot refina la solicitud utilizando datos del Microsoft Graph del inquilino del usuario, mejorando la especificidad y relevancia de la respuesta. Generación de respuesta: La solicitud refinada se envía a un modelo de lenguaje grande (LLM), que genera una respuesta contextualizada y adecuada a la tarea del usuario. Entrega de la respuesta: Copilot devuelve la respuesta a la aplicación correspondiente para que el usuario la visualice e interactúe con ella. Acceso y privacidad de los datos: Acceso autorizado: Copilot solo accede a los datos que el usuario tiene permiso para ver, respetando los controles de acceso basados en roles y las políticas de seguridad implementadas en Microsoft 365. Protección de datos: Los datos utilizados por Copilot se cifran durante su transmisión, y las interacciones se almacenan en el historial de chat de Copilot del usuario, permitiendo su revisión o eliminación según las preferencias del usuario. Cumplimiento de políticas de seguridad: Acceso condicional y autenticación multifactor (MFA): Copilot respeta las políticas de acceso condicional y MFA configuradas en la organización, asegurando que solo los usuarios autorizados puedan acceder a sus funcionalidades. https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-architecture

Ajustes y recalibraciones del modelo		
Consideraciones	**Respuesta (Sí/No)**	**Comentario**
Ajustes adicionales/Descripción	Sí	Microsoft 365 Copilot es una herramienta de productividad potenciada por inteligencia artificial que utiliza modelos de lenguaje de gran escala (LLMs) y se integra con los datos del usuario a través de Microsoft Graph y las aplicaciones y servicios de Microsoft 365. Funciona junto a aplicaciones populares como Word, Excel, PowerPoint, Outlook, Teams y más, proporcionando asistencia inteligente en tiempo real para mejorar la creatividad, productividad y habilidades de los usuarios. Disponibilidad de planes: Microsoft 365 Copilot está disponible como un plan complementario (add-on) que requiere licencias específicas. Para obtener información detallada sobre los planes de suscripción que habilitan a los usuarios para Microsoft 365 Copilot, consulte las comparaciones de planes de negocios y planes empresariales de Microsoft 365. En los países del Espacio Económico Europeo (EEE) y Suiza, también están disponibles comparaciones específicas de planes de negocios y planes empresariales para estas regiones. Disponibilidad de características: Las funcionalidades de Microsoft 365 Copilot varían según el entorno en la nube. A continuación, se detallan algunas de las principales características y su disponibilidad: Copilot en Word: Transforma la redacción de documentos, permitiendo crear, resumir, comprender, refinar y mejorar el contenido. Disponible en entornos en la nube a nivel mundial y en GCC. Copilot en PowerPoint: Ayuda a convertir ideas en presentaciones atractivas, generando diapositivas a partir de documentos existentes o desde un simple esquema. Disponible en entornos en la nube a nivel mundial y en GCC. Copilot en Excel: Facilita el análisis de datos, creando y preparando hojas de cálculo, extrayendo insights clave y compartiendo visualizaciones. Disponible en entornos en la nube a nivel mundial y en GCC. Copilot en Outlook: Asiste en la gestión del correo electrónico, redactando y resumiendo mensajes de manera eficiente. Disponible en entornos en la nube a nivel mundial; se espera su disponibilidad en GCC en el primer trimestre del año calendario 2025. Copilot en Teams: Mejora la comunicación y colaboración, recapitulando conversaciones y organizando puntos clave de discusión. Disponible en entornos en la nube a nivel mundial y en GCC. Galería de Prompts de Copilot: Ofrece una selección de indicaciones para ayudar a los usuarios a iniciar su experiencia con Copilot. Disponible en entornos en la nube a nivel mundial y en GCC. Copilot en Loop: Facilita la co-creación y sincronización en equipo, permitiendo iterar colaborativamente y resumir contenido. Disponible en entornos en la nube a nivel mundial; se espera su disponibilidad en GCC en el primer trimestre del año calendario 2025. Copilot en Microsoft Stream: Proporciona resúmenes de videos y respuestas a preguntas específicas basadas en transcripciones. Disponible en entornos en

Recalibraciones/Descripción	Sí	Microsoft 365 Copilot es una herramienta de productividad potenciada por inteligencia artificial que utiliza modelos de lenguaje de gran escala (LLMs) y se integra con los datos del usuario a través de Microsoft Graph y las aplicaciones y servicios de Microsoft 365. Funciona junto a aplicaciones populares como Word, Excel, PowerPoint, Outlook, Teams y más, proporcionando asistencia inteligente en tiempo real para mejorar la creatividad, productividad y habilidades de los usuarios. Disponibilidad de planes: Microsoft 365 Copilot está disponible como un complemento (add-on) que requiere licencias específicas. Para obtener información detallada sobre los planes de suscripción que habilitan a los usuarios para Microsoft 365 Copilot, consulte las comparaciones de planes de negocios y planes empresariales de Microsoft 365. En los países del Espacio Económico Europeo (EEE) y Suiza, también están disponibles comparaciones específicas de planes de negocios y planes empresariales para estas regiones. Disponibilidad de características: Las funcionalidades de Microsoft 365 Copilot varían según el entorno en la nube. A continuación, se detallan algunas de las principales características y su disponibilidad: **Copilot en Word:** Transforma la redacción de documentos, permitiendo crear, resumir, comprender, refinar y mejorar el contenido. Disponible en entornos en la nube a nivel mundial y en GCC. **Copilot en PowerPoint:** Ayuda a convertir ideas en presentaciones atractivas, generando diapositivas a partir de documentos existentes o desde un simple esquema. Disponible en entornos en la nube a nivel mundial y en GCC. **Copilot en Excel**: Facilita el análisis de datos, creando y preparando hojas de cálculo, extrayendo insights clave y compartiendo visualizaciones. Disponible en entornos en la nube a nivel mundial y en GCC. **Copilot en Outlook**: Asiste en la gestión del correo electrónico, redactando y resumiendo mensajes de manera eficiente. Disponible en entornos en la nube a nivel mundial; se espera su disponibilidad en GCC en el primer trimestre del año calendario 2025. **Copilot en Teams:** Mejora la comunicación y colaboración, recapitulando conversaciones y organizando puntos clave de discusión. Disponible en entornos en la nube a nivel mundial y en GCC. Galería de Prompts de Copilot: Ofrece una selección de indicaciones para ayudar a los usuarios a iniciar su experiencia con Copilot. Disponible en entornos en la nube a nivel mundial y en GCC. **Copilot en Loop**: Facilita la co-creación y sincronización en equipo, permitiendo iterar colaborativamente y resumir contenido. Disponible en entornos en la nube a nivel mundial; se espera su disponibilidad en GCC en el primer trimestre del año calendario 2025. **Copilot en Microsoft Stream**: Proporciona resúmenes de videos y respuestas a preguntas específicas basadas en transcripciones. Disponible en entornos en la nube a nivel mundial; se espera su disponibilidad en GCC en el primer trimestre del año calendario 2025. https://learn.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/microsoft-365-copilot
Última actualización para ajustes o recalibraciones (mm/aaaa)	13/12/2024	

Versión	Fecha	Descripción de la modificación
1	Febrero 20 de 2025	Se diligencia y revisa la ficha