eBook

Cinco mitos sobre la IA en ciberseguridad desmentidos

Guía de conceptos erróneos, oportunidades y Microsoft Copilot para seguridad sobre la IA generativa

Microsoft Security

Índice

Introducción

Ha llegado una nueva era de la IA, junto con nuevos conceptos erróneos

Las ciberamenazas aumentan, tanto en número como en gravedad, y los equipos de seguridad se esfuerzan por seguir el ritmo de las herramientas tradicionales de ciberseguridad. Por eso, muchos responsables de seguridad están recurriendo a soluciones con tecnología de IA.

Estas herramientas transformadoras ofrecen la oportunidad de abordar sus mayores retos en materia de seguridad y pueden suponer un cambio radical para su equipo de seguridad. Los profesionales de la seguridad, equipados con soluciones de IA generativa, pueden proteger más, actuar con más rapidez y obtener una ventaja sobre los ciberdelincuentes. Además, dedicarán menos tiempo a realizar tareas tediosas y más a tomar decisiones estratégicas y proactivas.

Dado que las soluciones de ciberseguridad basadas en IA generativa son nuevas, es posible que tenga dudas a la hora de adoptar estas herramientas. Como responsable de seguridad, es natural tener dudas sobre cualquier tecnología nueva. De hecho, es señal de que es bueno en su trabajo. Pero si trabaja con un socio tecnológico de confianza, descubrirá que las recompensas de la IA generativa superan con creces los riesgos.

En este eBook se explorarán y desmentirán los cinco mitos más comunes sobre las herramientas de ciberseguridad de IA generativa, entre ellos:

1. Acceso no autorizado a los datos
2. Privacidad y propiedad de los datos
3. Filtración y exposición de datos
4. Problemas de cumplimiento
5. Alucinaciones

Siga leyendo para profundizar en estas inquietudes y descubra cómo Microsoft Copilot para seguridad aborda cada una de ellas con controles integrados de seguridad, cumplimiento y privacidad.

1

El caso de la IA en ciberseguridad

Los ciberataques son cada vez más frecuentes, coordinados y sofisticados. En el último año, el número de ataques de contraseñas detectados por Microsoft se disparó de 579 a más de 4000 por segundo.[1] Dado que la mayoría de las organizaciones utilizan docenas de herramientas de ciberseguridad para administrar su entorno, los equipos de seguridad actuales se enfrentan a una avalancha de datos, cansancio por las alertas y visibilidad limitada entre varias soluciones, todo ello mientras se enfrentan a una escasez de talento global y a la complejidad normativa.

Hoy en día, los analistas de seguridad tienen todas las de perder:

- 4000: ataques de contraseña por segundo
- 72 minutos: tiempo promedio para que un atacante acceda a sus datos privados si abre un correo electrónico de phishing
- 3,5 millones: escasez mundial de profesionales calificados en ciberseguridad

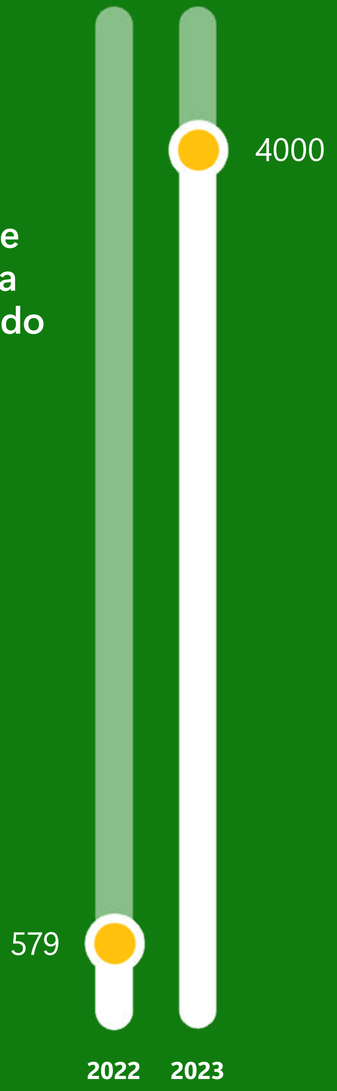
Por eso es más importante que nunca que sus equipos de seguridad cuenten con soluciones innovadoras que les ayuden a detectar, investigar y responder con rapidez a las crecientes ciberamenazas. Para afrontar los complejos retos actuales, los responsables de seguridad buscan:

- Más automatización y herramientas que trabajan en conjunto para ayudar a sus equipos de seguridad a superar y ser más astutos que los ciberatacantes.
- Maneras de reforzar la experiencia de su equipo y aligerar las tareas tediosas para que puedan enfocarse en proteger su organización.
- Soluciones que ayudan a sus analistas a ver más y moverse con más rapidez, para que puedan detectar y responder a los incidentes antes de que provoquen daño.

La IA es la clave para hacer todo esto posible.

Muchos equipos de seguridad ya están ganando ventaja con soluciones con tecnología de IA.
Y el impacto es real.

Ataques de contraseña por segundo



[1] Informe de defensa digital de Microsoft 2023.

Microsoft Copilot para seguridad representa un avance innovador para los equipos de operaciones de seguridad en todo el mundo. A través de nuestro servicio global Microsoft MXDR [detección y respuesta extendidas administradas], estamos observando una reducción de hasta el 40 % en el tiempo de resolución de incidentes cuando se compara con los procesos actuales.

Además, mejora considerablemente el entorno de trabajo de los analistas del Centro de operaciones de seguridad (SOC) al servir como su asistente de seguridad de IA para las operaciones diarias.

Jason Revill
Director del Centro de Excelencia de Seguridad Global, Avanade

La IA será un componente fundamental de la defensa exitosa. En los próximos años, la innovación en ciberdefensa con tecnología de IA ayudará a revertir la actual ola creciente de ciberataques.

Tom Burt
Vicepresidente corporativo, Seguridad y Confianza del Cliente, Microsoft

Para hacer frente a retos de ciberseguridad cada vez más complejos, muchos equipos de seguridad están adoptando herramientas de IA generativa (como Microsoft Copilot para seguridad) que mejoran la experiencia humana con conocimientos inteligentes y flujos de trabajo automatizados.

Copilot para seguridad es un asistente de IA para las operaciones diarias en seguridad y TI. Esta solución con tecnología de IA generativa está diseñada para ayudar a los equipos de seguridad a ser más rápidos, productivos y precisos. Con Copilot, los equipos de seguridad obtienen información personalizada basada en la inteligencia global sobre amenazas, los procedimientos recomendados del sector y los datos de seguridad de su organización. Esta información práctica brinda a los profesionales de la seguridad los conocimientos que requieren para superar a los ciberatacantes.

40 %

de tiempo ahorran los analistas que utilizan Copilot para las tareas típicas de las operaciones de seguridad

60 %

de tiempo ahorran los analistas que utilizan Copilot para tareas tediosas, como la clasificación de alertas y la generación de informes[2]

[2] Microsoft Copilot para seguridad para los primeros datos de clientes, 2023.

2

Cinco mitos sobre las soluciones de seguridad con tecnología de IA generativa desmentidos

Aunque está claro que la IA generativa puede ayudar a amplificar el impacto de los equipos de seguridad, algunos líderes desconfían de lanzarse de inmediato sin considerarlo con detención. Es razonable tener dudas sobre cualquier tecnología nueva y curiosidad sobre su posible impacto en su equipo y su organización. Por eso es importante investigar.

Estas son las cinco principales preocupaciones que tienen los responsables de seguridad sobre la IA generativa y cómo Copilot para seguridad está diseñado para abordarlas.

Mito 1:

Acceso no autorizado a los datos

A algunos responsables de seguridad les preocupa que, si un usuario no autorizado formula una pregunta a una herramienta con tecnología de IA, pueda obtener una respuesta que incluya información que el usuario no está autorizado a ver. Pero este no es el caso.

La seguridad de los datos es la principal preocupación de las organizaciones que adoptan nuevas herramientas de IA generativa. Cuando cualquier usuario no autorizado, ya sea interno o externo, obtiene acceso a los datos, esto puede perturbar la actividad empresarial y poner en peligro la reputación de una organización. Para generar respuestas útiles a las consultas, las aplicaciones de IA generativa pueden tener acceso a datos confidenciales. Sin embargo, la aplicación solo mostrará al usuario lo que tenga acceso a ver.

Preguntas frecuentes:
¿Pueden los usuarios no autorizados acceder a datos confidenciales con Copilot?

Respuesta: No.

Esto no ocurrirá con Copilot porque utiliza derechos de "administrador en nombre de" para el usuario conectado. Es decir, los derechos están limitados a ese usuario específico y únicamente a ese usuario. Copilot ejecuta consultas como usuario, por lo que nunca tiene privilegios superiores a los que tiene el usuario.

Mito 2:

Privacidad y propiedad de los datos

Garantizar la privacidad de los datos es fundamental para que una organización cree una cultura de transparencia, genere confianza en los clientes y cumpla la normativa. Cuando se plantean soluciones de IA generativa, a los responsables de seguridad les preocupa que los datos de sus clientes se utilicen para entrenar otros modelos, lo que en última instancia podría poner en peligro la reputación de la organización. Esto no ocurrirá cuando trabaje con un socio tecnológico de confianza.

Preguntas frecuentes:
¿Se utilizarán mis datos de cliente para entrenar modelos de lenguaje en Copilot?

Respuesta: No.

En Microsoft, estamos estableciendo las normas de seguridad, privacidad y cumplimiento en lo que respecta a la IA. Esto es válido no solo para Copilot para seguridad, sino para todas nuestras ofertas de IA.

De manera predeterminada, Microsoft no entrena modelos de lenguaje en los datos del cliente. Existe una funcionalidad opcional dedicada dentro de Copilot para los clientes que eligen contribuir a la seguridad colectiva y la innovación en IA.

Cuando se trata de datos, a diferencia de ChatGPT, Copilot se basa en el contexto único de su organización. Esto significa que cuando le haga una pregunta a Copilot, la respuesta se basará en lo que esté ocurriendo en su organización en ese momento. Sus datos no se utilizan para entrenar modelos fundacionales de IA. Es un circuito cerrado de aprendizaje que mejora continuamente en función de su uso.

Creada para la seguridad, la privacidad y el cumplimiento

Sus datos son suyos.

Sus datos no se utilizan para entrenar modelos fundacionales de IA.

Sus datos están protegidos con los controles de seguridad y cumplimiento empresarial más completos.

Preguntas frecuentes: ¿Los datos transferidos cuentan con protección contra el acceso no autorizado?

Respuesta: Sí.

Ningún usuario humano tiene acceso a la base de datos, y el acceso está restringido a la red privada donde está implementada la aplicación Copilot para seguridad. Si se requiere acceso para que un humano responda a un incidente, entonces el ingeniero de guardia necesitará acceso superior y acceso a la red aprobado por empleados autorizados de Microsoft. Copilot cumple con todos los requisitos de privacidad, seguridad y cumplimiento de Microsoft.

Al utilizar Copilot para seguridad, sus datos:

- Son sus datos.
- Se almacenan donde usted elija y siempre se cifran en reposo.
- No se utilizan con fines de venta ni se comparten con terceros.
- Se hospedan en sistemas regidos por el SOC de Microsoft y procesos certificados por la Organización Internacional de Normalización.
- No se utilizan para entrenar modelos de IA básicos.
- Nunca se comparten con OpenAI.
- Están protegidos con los controles de seguridad y cumplimiento empresarial más completos.

Mito 3:

Filtración y exposición de datos

El año pasado, el 74 % de las organizaciones sufrieron un incidente que expuso datos empresariales, como propiedad intelectual.[3] Las vulneraciones de datos son muy costosas para las organizaciones, y no solo en el sentido financiero. Estos incidentes también merman la confianza de los clientes, que pueden convertirse en víctimas de robos de identidad, fraudes con tarjetas de crédito u otras actividades malintencionadas a causa de la vulneración. Con tanto en juego, es comprensible que a los responsables de seguridad les preocupe que nuevas tecnologías como la IA generativa puedan dar lugar a vulneraciones de datos.

Preguntas frecuentes:
¿Puede Copilot exponer mis datos a otras personas que utilicen la herramienta?

Respuesta: No.

Copilot para seguridad se diseñó con base en la IA responsable. Incluye los mismos controles de seguridad, privacidad y cumplimiento que otros productos de confianza de Microsoft, así como mecanismos de seguridad específicos para la IA. Sus datos se analizan dentro del sistema Copilot y no salen del inquilino de producción de Microsoft Azure. De acuerdo con las normas de Microsoft, sus datos están cifrados en tránsito y en reposo.

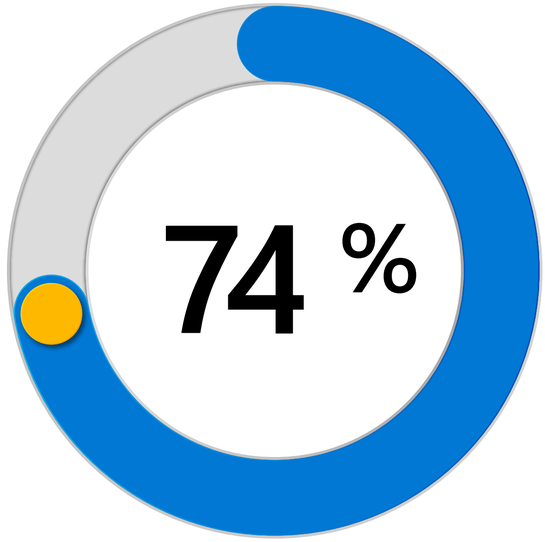
Además, los datos de sesión solo se almacenan en los registros y con fines de ejecución para el funcionamiento del servicio. En la base de datos en tiempo de ejecución, cuando se elimina una sesión mediante la experiencia de usuario (UX) del producto, todos los datos asociados a esa sesión se marcan como eliminados y el tiempo de vida (TTL) se establece en 30 días. Una vez que expira el TTL, ninguna consulta puede acceder a los datos. En ese momento, un proceso en segundo plano elimina de forma física los datos.

Además, hay copias de seguridad periódicas de la base de datos que quedarán obsoletas. Tienen periodos de retención cortos.

Copilot:

- Ejecuta consultas como su usuario, por lo que nunca tiene privilegios superiores.
- Es un servicio de producción de Azure y cuenta con protección de los controles de seguridad de Microsoft.[4]
- Almacena datos limitados (registros y contexto de investigación) y cifra todos los datos que utiliza en reposo.
- Se encuentra dentro del límite de datos de la UE, un límite definido geográficamente dentro del cual Microsoft se ha comprometido a almacenar y procesar datos de clientes y datos personales para servicios empresariales online.

[3] Índice de seguridad de datos, Microsoft, octubre de 2023
[4] Protección de los datos de los clientes en Azure, Microsoft Learn



de las organizaciones experimentaron un incidente que expuso datos empresariales

Mito 4:

Problemas de cumplimiento

Ayudar a su organización a cumplir los requisitos de cumplimiento puede ser uno de los retos empresariales más exigentes a los que se enfrente como responsable de seguridad. Muchas organizaciones tienen que cumplir una serie de estrictos requisitos empresariales y normativos que varían según la región y el sector. En algunos casos, el incumplimiento puede acarrear sanciones económicas o hacer que su organización pierda el acceso a todo un segmento del mercado. Al tener en cuenta la complejidad del actual panorama de cumplimiento, a algunos responsables de seguridad les preocupa que las nuevas soluciones de IA generativa no cumplan los requisitos. Gracias a soluciones confiables como Copilot, esto no es un problema.

Preguntas frecuentes:
¿Copilot para seguridad cumple con los requisitos de cumplimiento regionales o de la industria?

Respuesta: Sí.

Copilot cumple los requisitos del Reglamento general de protección de datos (RGPD) para los mercados de la UE mediante la implementación de los requisitos de la versión preliminar pública de Azure. Almacena todos los datos de clientes de la UE dentro de los límites de datos de la UE y se encuentra disponible en varios idiomas. Copilot también ofrece controles de cumplimiento para ayudarle a cumplir con los requisitos empresariales y normativos.

La IA aumenta la experiencia humana, no al revés.

Mito 5:
Alucinaciones

Los cuentos con moraleja sobre un fenómeno de la IA llamado alucinaciones se han vuelto demasiado comunes. Una alucinación es un contenido generado por un modelo de lenguaje que parece verosímil pero que es incorrecto o irrelevante. Se presenta como conocimiento calificado, y se da en una respuesta segura, pero falsa.

Estas alucinaciones se convierten en un problema aún mayor cuando los humanos:

- Aceptan el contenido como un hecho sin verificación.
- Suponen que el contenido está libre de prejuicios o información errónea.
- Confían en el contenido para tomar decisiones críticas sin intervención ni supervisión humana.

Aunque se trata de una preocupación comprensible, las alucinaciones no son un problema cuando se utilizan soluciones de IA transparentes que permiten a los humanos tomar sus propias decisiones.

Preguntas frecuentes:
¿Copilot para seguridad ayuda a detectar alucinaciones?

Respuesta: Sí.

La confianza es fundamental en la seguridad. Si no puede confiar en los datos y la información sobre seguridad, no podrá obtener los resultados adecuados. Para que los humanos trabajen con confianza con herramientas con tecnología de IA como Copilot, es esencial generar confianza en la tecnología.

En Microsoft, estamos comprometidos con la IA responsable, por lo que Copilot está diseñado para:

- Mostrar el razonamiento, las fuentes, la depuración y el tiempo de ejecución.
- Garantizar que los datos cumplan con la normativa, sean seguros y privados.
- Abordar los daños y las alucinaciones.
- Ser transparente y permitir un diálogo abierto.

Con o sin alucinaciones, es esencial que las personas siempre se sientan seguras de tener el control cuando hacen uso de herramientas con tecnología de IA. La IA aumenta la experiencia humana, no al revés.

Con Copilot, el objetivo es ayudar a los equipos de seguridad a lograr resultados de seguridad positivos de forma más eficiente sin depender en exceso de la IA. Los analistas de seguridad reciben sugerencias de Copilot que les ayudan a actuar según sus conocimientos, pero son ellos los que deciden si utilizar estas recomendaciones y cómo hacerlo.

En otras palabras, el ser humano decide en qué confiar, qué compartir, qué es importante, qué es pertinente y cuándo y cómo actuar. Los usuarios de Copilot no solo pueden controlar y calificar los resultados de la IA, sino también editar y corregir los resultados de la IA y brindar comentarios.

La creatividad y los conocimientos humanos siempre serán imprescindibles para la ciberseguridad. Copilot está diseñado para complementar las habilidades y la experiencia de su equipo de seguridad para que puedan trabajar de forma más rápida, precisa y proactiva.

3

Dé a su equipo de seguridad una ventaja con la IA generativa líder en la industria

A medida que las capacidades con tecnología de IA se hacen más frecuentes en la ciberseguridad y las ciberamenazas se tornan cada vez más complejas, la IA generativa se está convirtiendo con rapidez en esencial para los SOC. Microsoft Copilot para seguridad es una solución de ciberseguridad de IA integral y generativa que puede ayudarlo a:

- Proporcionar al personal de ciberseguridad los conocimientos y la experiencia que necesitan para entender lo que ocurre en el entorno y tomar medidas.
- Hacer avanzar el trabajo de los miembros menos experimentados del equipo mediante una guía paso a paso y aliviar las tareas tediosas del personal superior para que puedan enfocarse en prioridades más estratégicas.
- Poner la orientación y el contexto críticos al alcance de su equipo de seguridad para que puedan responder a los incidentes en cuestión de minutos en lugar de horas o días.
- Optimizar la elaboración de informes y preparar informes personalizables para su equipo de liderazgo ejecutivo y junta directiva.
- Convertir grandes cantidades de señales de datos en información clave para eliminar el ruido, detectar y responder a las ciberamenazas en cuestión de minutos y reforzar su postura de seguridad.

Aumente la productividad a nuevos niveles con Copilot para seguridad

Microsoft Office of the Chief Economist realizó un estudio[5] para probar las ganancias de productividad que los profesionales de seguridad experimentados consiguieron con Copilot para seguridad, y los resultados superaron las expectativas.

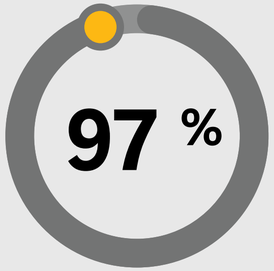
Con Copilot para seguridad, los profesionales de seguridad fueron:

- 22 % más rápidos en todas las tareas
- 7 % más precisos en todas las tareas
- 14 % más rápidos en el análisis de scripts
- 12 % más precisos en el análisis de scripts
- 39 % más rápidos en resumir un incidente

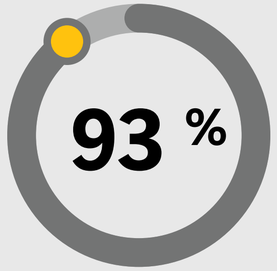
Además, los analistas que hacen uso de Copilot para seguridad crearon resúmenes de incidentes con un 49 % más de datos sobre incidentes.

[5] Ensayo controlado aleatorizado (RTC) de Microsoft Copilot para seguridad con analistas de seguridad experimentados realizado por Microsoft Office of the Chief Economist, enero de 2024.

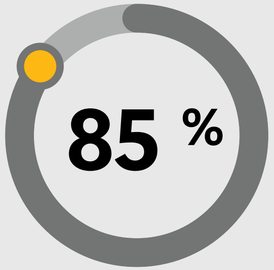
Cuando se les preguntó sobre su experiencia:



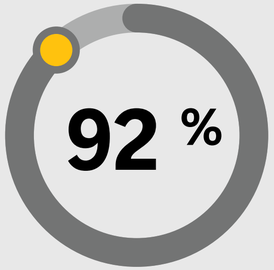
El 97% de los profesionales de la seguridad señalaron que querían Copilot la próxima vez que hicieran la misma tarea.



El 93 % informó que Copilot les ayudó a mejorar la calidad de su trabajo.



El 85 % informó que Copilot redujo el esfuerzo en las tareas.



El 92 % afirmó que Copilot los hizo más productivos.

Con Copilot, también obtendrá información y señales de amenazas de todo el mundo. La inteligencia contra amenazas está en constante evolución, por lo que es esencial que las organizaciones se mantengan actualizadas.

Inteligencia contra amenazas Microsoft:

- Sintetiza 65 billones de señales al día, a través de todo tipo de dispositivos, aplicaciones, plataformas y puntos de conexión, mediante IA líder en la industria.
- Protege más de 1400 millones de puntos de conexión en todo el mundo, incluidos dispositivos móviles, servidores, dispositivos IoT y PC.
- Grafica diariamente todo Internet para localizar a los ciberatacantes y su infraestructura.

Además, 8500 ingenieros e investigadores de seguridad de Microsoft trabajan arduamente para profundizar en señales desconocidas para determinar su verdadera naturaleza.

Todos los clientes de Copilot para seguridad obtienen acceso de primer nivel a la Inteligencia contra amenazas de Microsoft Defender (MDTI) sin costo adicional (no incluye la API). MDTI le ayuda a acceder directamente al repositorio masivo de Microsoft de información sobre amenazas terminada y sin procesar, y a actuar en consecuencia, para desenmascarar y neutralizar a los ciberatacantes.

Bienvenido a una nueva era en ciberseguridad

Si quiere superar a los ciberatacantes en la era de la IA, es más importante que nunca equipar a su equipo con herramientas de seguridad de última generación. Permita a sus analistas obtener una ventaja frente a las ciberamenazas con los controles integrados de seguridad, cumplimiento y privacidad de Microsoft Copilot para seguridad.

Encuentre más información sobre Microsoft Copilot para seguridad

Aprenda a resolver los desafíos de hoy con la IA