Microsoft Security

Índice de seguridad de los datos

Tendencias, conocimientos y estrategias para proteger tus datos y navegar por la IA generativa

Informe de 2024

Prólogo

Ahora que nos acercamos a nuestro segundo año de investigación sobre el cambiante panorama de la seguridad de los datos, nunca habían sido tan profundos los desafíos y las oportunidades que se nos presentan. En el último año, la gravedad de los incidentes de seguridad de los datos ha aumentado. En esta era centrada en los datos, las estrategias y herramientas empleadas para mantener protegidos los datos evolucionan a gran velocidad.

Este año, exploramos una nueva frontera: la función y el impacto de la IA generativa (IA) en las estrategias de seguridad de los datos.

La IA está causando furor en todo el mundo con capacidades sin precedentes para impulsar la innovación y la eficiencia. Sin embargo, a pesar de este enorme potencial, a las organizaciones también les preocupan los riesgos de seguridad de los datos y cómo este aspecto podría dar forma a las responsabilidades de los equipos de seguridad de los datos. Observamos que la IA hace que las organizaciones se apresuren a reforzar sus prácticas fundamentales de seguridad de los datos para poder prepararse para minimizar el impacto del intercambio excesivo y las filtraciones de datos, además de crear procesos para la adopción segura de la IA. Por otro lado, la IA también puede ayudar a las organizaciones a mejorar sus prácticas de seguridad de datos identificando los riesgos ocultos y las deficiencias en la protección, recomendando políticas de protección, así como ayudando a investigar y mitigar los incidentes de seguridad con más rapidez.

El objetivo de nuestra investigación es proporcionar a los líderes de seguridad conocimientos útiles y directrices para ayudar a sus equipos a adaptar con confianza su estrategia de seguridad de datos para proteger eficazmente el uso de la IA e integrar la IA en sus estrategias de seguridad de datos. Aunque es notable por su alcance y potencial, la IA es solo la última oleada de transformación que recorre las empresas, como el trabajo híbrido, el cloud y la movilidad, que en los últimos años han resaltado la necesidad atemporal de tener visibilidad en su uso para mitigar el riesgo y maximizar el impacto. Con estos conocimientos, con la protección correcta de los datos utilizados en la IA y el uso de la IA para mejorar las medidas de seguridad de los datos, se logrará una mayor productividad, resiliencia y agilidad a medida que los equipos se enfrentan a desafíos futuros.

Te invitamos a explorar las últimas conclusiones y esperamos que estos conocimientos te ayuden a reforzar tu enfoque de seguridad de los datos, así como a inspirarte para adoptar la IA y crear una estrategia integral de seguridad de los datos que genere más innovación y garantice un futuro más seguro para todos.

Rudra Mitra
Vicepresidente corporativo
Seguridad y conformidad de datos en Microsoft

Presentación

Ahora que las organizaciones sufren una media de 156 incidentes de seguridad de datos al año, el impacto de estos incidentes sigue siendo una preocupación constante para los responsables de la toma de decisiones de seguridad de los datos. Y esa preocupación es legítima: un solo incidente puede causar enormes daños financieros y de reputación, sobre todo en un entorno de amenazas en constante evolución en el que los atacantes están explotando todas y cada una de las posibles vulnerabilidades. Esto se agrava con la rápida adopción de la IA: sin medidas de seguridad y protección suficientes, los usuarios pueden poner en riesgo datos críticos para la empresa por accidente o de forma malintencionada (incluida información de empleados y clientes, propiedad intelectual, previsiones financieras y datos operativos). A medida que las organizaciones buscan nuevas formas de proteger esta amplia variedad de datos confidenciales, muchos responsables de la toma de decisiones centran su atención en el drástico aumento de la IA.

El desafío de la IA es doble. Dado que dos tercios de las organizaciones admiten que sus empleados utilizan herramientas de IA no autorizadas, es fundamental que garanticen que los empleados utilicen las herramientas de IA de forma segura. Al mismo tiempo, existe la oportunidad de utilizar la IA como una herramienta eficaz en una estrategia sofisticada de seguridad de los datos.

Las soluciones de seguridad de datos basadas en IA ya desempeñan una función crítica a la hora de identificar y responder a las amenazas en tiempo real, mejorar la velocidad y la precisión general de los programas de seguridad de los datos y proporcionar conocimientos que ayuden a evitar incidentes de seguridad de los datos antes de que ocurran. Las organizaciones deben gestionar los riesgos que plantea la IA, además de aprovechar su poder para identificar patrones que a las personas les resulten difíciles de procesar y analizar a la velocidad de una máquina y, en última instancia, luchar contra ciberataques cada vez más sofisticados.

En 2023, Microsoft encargó a Hypothesis, una agencia de investigación independiente, una encuesta multinacional entre más de 800 profesionales de seguridad de datos e inició la iniciativa del índice de seguridad de los datos para prestar un mejor servicio a nuestros socios y clientes y ayudar a los líderes empresariales a desarrollar sus propias estrategias de seguridad de los datos.

En 2024, este informe se basa en la investigación anterior con nuevos conocimientos a partir de una encuesta multinacional ampliada a más de 1300 profesionales de la seguridad de los datos. Aunque los datos revelan conocimientos y tendencias coherentes en los mercados encuestados, descubrimos nuevos datos sobre las últimas prácticas y tendencias de IA y seguridad de los datos en todo el mundo.

hypothesis Microsoft Security

Conclusiones principales

1

El panorama de la seguridad de los datos sigue fracturado, lo que aumenta la necesidad de estrategias de seguridad de datos cohesionadas, tanto en lo que respecta a riesgos tradicionales como a los nuevos que surgen relacionados con el uso de la IA.

Las organizaciones registran altos niveles de satisfacción y confianza en sus medidas de seguridad de los datos. Sin embargo, la gravedad de los incidentes de seguridad de los datos sigue aumentando, sobre todo debido a las deficiencias que encuentran las organizaciones entre sus políticas actuales de seguridad de los datos y el aumento del uso o la introducción de aplicaciones de IA. Para hacer frente a estos imperativos e intereses, muchas organizaciones todavía confían en múltiples herramientas de seguridad de los datos que pueden aumentar su vulnerabilidad y riesgo generales.

2

A medida que aumenta la adopción de la IA por parte de los usuarios finales, la integridad de los datos más confidenciales de las organizaciones corre un mayor riesgo, lo que requiere más visibilidad y nuevos controles de protección

A medida que las herramientas de IA se vuelven esenciales en el trabajo diario, a las organizaciones les preocupan los riesgos de seguridad de los datos. Reconocen la necesidad de reforzar sus defensas y se comprometen a prevenir incidentes de seguridad de los datos causados por la IA, pero el uso no autorizado de estas herramientas resalta la necesidad de una visibilidad más sólida.

3

Los responsables de la toma de decisiones son optimistas sobre el potencial de la IA para impulsar sus esfuerzos de seguridad de los datos

Las organizaciones están invirtiendo activamente en herramientas de seguridad de datos que incorporan la IA para mejorar las capacidades de detección y respuesta. La IA puede ayudar a detectar datos desprotegidos, recomendar políticas de protección y ayudar a investigar y solucionar los incidentes de seguridad de los datos con más rapidez, lo que en última instancia permite a los equipos de seguridad de los datos dedicar más tiempo y atención al trabajo estratégico. El uso de la IA también aumenta la confianza y la satisfacción en la estrategia general de seguridad de los datos de las organizaciones, sobre todo en su capacidad para responder a incidentes de forma rápida y precisa.

1

El panorama de la seguridad de los datos sigue fracturado, lo que aumenta la necesidad de estrategias de seguridad de datos cohesionadas, tanto en lo que respecta a riesgos tradicionales como a los nuevos que surgen relacionados con el uso de la IA.

Existe una desconexión entre la confianza de los responsables de la toma de decisiones en sus prácticas de seguridad de los datos y el verdadero nivel de protección de los datos

Tal y como se registró en 2023, la gran mayoría de los responsables de la toma de decisiones confía en sus estrategias de seguridad de los datos y el 74 % afirma estar satisfechos con sus soluciones actuales en 2024. Se sienten seguros en su capacidad para rastrear y administrar datos confidenciales: el 88 % cree que sabe dónde reside la mayoría de su información crítica y el 85 % afirma que sus datos están clasificados y etiquetados correctamente. La mayoría también confía en sus controles de defensa: el 79 % confía en que puede evitar filtración de datos y el 76 % describe su enfoque como proactivo en lugar de reactivo.

Sin embargo, su confianza se pone a prueba a medida que aumenta la gravedad los incidentes. **El número medio de incidentes de seguridad de datos anuales ha seguido siendo alto, de los 166 de 2023 a los 156 de 2024, y la gravedad de estos incidentes ha aumentado del 20 % de incidentes graves al 27 % en 2024.**

156

incidentes de seguridad de los datos

El 27 %

de los incidentes se consideran graves
(aumento con respecto al 20 % de 2023)

El 63 %

de alertas revisadas al día

"El lugar donde se estableció una plataforma de software, dónde se almacenan sus datos y quién accederá a ellos complicó la seguridad de los datos y la administración de nuestras herramientas de IA y nuestros proveedores. Contamos con más de 100 años de datos que debemos proteger y gestionar de acuerdo con los requisitos legales en cada jurisdicción en la que operamos", explica un director sénior de gestión de la información de un fabricante de equipos pesados.

El aumento de la gravedad de los incidentes de seguridad de los datos ha incrementado el volumen de alertas. **Las organizaciones se enfrentan a una media de 66 alertas al día, en comparación con las 52 en el 2023.** Esta cifra varía en gran medida según el tamaño de la organización, ya que las empresas medianas (500-999 empleados) y las grandes empresas (1000-4999 empleados) reciben una media de 56 alertas y las empresas extragrandes (más de 5000 empleados) reciben una media de 80 alertas al día.

Dado el gran volumen de alertas de seguridad de datos, no debería sorprender que la mayoría de las organizaciones sencillamente no den abasto. De media, los equipos de seguridad de los datos revisan el 63 % de sus alertas diarias. El 35 por ciento de estas alertas son falsos positivos. Este desajuste entre el control percibido y la realidad operativa deja a los equipos de seguridad de los datos abrumados, tratando de evaluar si tienen las protecciones idóneas o cómo ajustarlas, además de la preocupación de que puedan sufrir incidentes potencialmente graves al pasar desapercibidos.

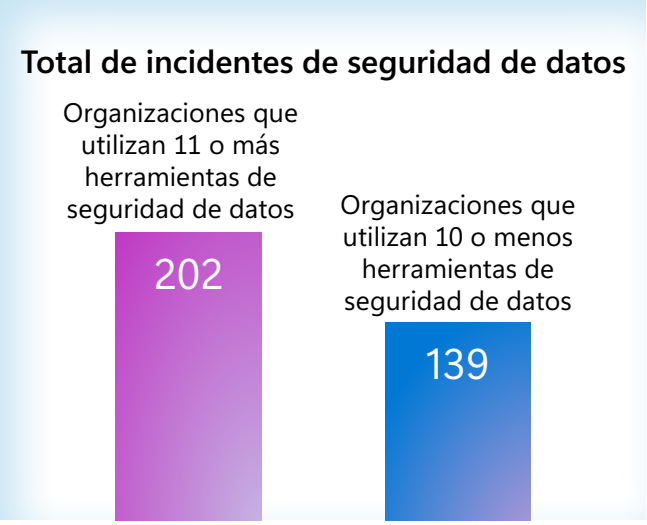
Para luchar contra los riesgos de datos tradicionales y emergentes relacionados con el uso de herramientas de IA, existe una creciente necesidad de estrategias de seguridad de datos más sólidas y cohesionadas

A pesar del creciente número de herramientas a su disposición, muchos responsables de la toma de decisiones siguen admitiendo que no siempre es mejor. De hecho, el 21 % cita la falta de visibilidad consolidada e integral (y un conocimiento compartido de los riesgos) causada por herramientas dispares como su mayor desafío o riesgo.[1]

La mayoría de los responsables de la toma de decisiones (el 82 %) coincide en que una plataforma completa y totalmente integrada es superior a la administración de múltiples herramientas aisladas. **De media, hacen malabarismos con 12 soluciones de seguridad de datos diferentes, lo que supone una complejidad que aumenta su vulnerabilidad.** Esto es especialmente cierto en el caso de las organizaciones más grandes: de media, las empresas medianas utilizan 9 herramientas, las grandes empresas utilizan 11 y las empresas extragrandes, 14.

Los datos demuestran una correlación sólida entre el número de herramientas de seguridad de datos utilizadas y la frecuencia de los incidentes de seguridad de los datos. Las empresas medianas y grandes registran una media de 89 incidentes al año, mientras que las empresas extragrandes se enfrentan a la abrumadora cifra de 248 incidentes al año. Esta marcada diferencia resalta el alto riesgo al que se enfrentan las organizaciones más grandes, incluso cuando afirman tener una confianza importante en sus medidas de seguridad de los datos.

En 2024, las organizaciones que utilizan más herramientas de seguridad de datos (11 o más) experimentaron una media de 202 incidentes de seguridad de datos, en comparación con los 139 incidentes de aquellas con 10 o menos herramientas.



Las soluciones fragmentadas hacen que sea difícil entender el estado de seguridad de los datos, ya que los datos están aislados y los flujos de trabajo dispares podrían limitar la visibilidad completa de los riesgos potenciales. Cuando las herramientas no se integran, los equipos de seguridad de los datos tienen que crear procesos para correlacionar los datos y establecer una visión cohesiva de los riesgos, lo que puede generar puntos ciegos y dificultar la detección y mitigación eficaces de los riesgos.

Un ámbito de preocupación creciente es el aumento de los incidentes de seguridad de los datos debidos al uso de aplicaciones de IA, que prácticamente se duplicó del 27 % en 2023 al 40 % en 2024. Este aumento de los incidentes está impulsado por un aumento de los ataques de malware y ransomware, hasta un 59 %, en comparación con el 50 % en 2023. Los ataques procedentes del uso de aplicaciones de IA no solo exponen datos confidenciales, sino que también ponen en peligro la funcionalidad de los propios sistemas de IA, lo que complica aún más un panorama de seguridad de los datos ya fracturado. En resumen, existe una necesidad cada vez más urgente de estrategias de seguridad de datos más sólidas y cohesionadas que puedan abordar los riesgos tradicionales y los emergentes vinculados al uso de herramientas de IA.

1. Encuesta de septiembre de 2024 entre responsables de tomas de decisiones de seguridad de los datos, gestión, cumplimiento y privacidad, encargada por Microsoft a la agencia MDC Research

El camino a seguir

El aumento de la gravedad de los incidentes de seguridad de los datos supone una oportunidad para que la IA te ayude. Las organizaciones que se sitúan a la vanguardia están implementando seguridad de datos basada en IA para ayudarles a priorizar los incidentes, automatizar la clasificación de datos e identificar formas de ajustar las políticas de protección actuales. La IA puede sintetizar automáticamente la gravedad potencial de las alertas de incidentes, proporcionando a los equipos de seguridad de los datos conocimientos útiles para dar una respuesta rápida, con el fin de reducir el tiempo dedicado a falsos positivos. Esto optimiza los flujos de trabajo y permite a los equipos de seguridad de los datos centrarse en mejoras de seguridad de datos más estratégicas y medidas proactivas.

2

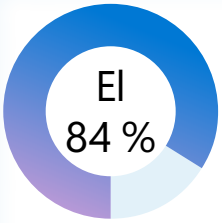
A medida que aumenta la adopción de la IA por parte de los usuarios finales, la integridad de los datos más confidenciales de las organizaciones corre un mayor riesgo, lo que requiere más visibilidad y nuevos controles de protección

La IA se está convirtiendo rápidamente en algo esencial para el trabajo diario y las organizaciones deben adoptar y adaptarse activamente a esa nueva realidad

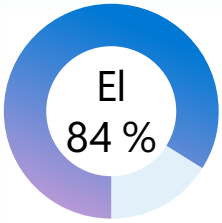
La rápida adopción de herramientas de IA por parte de los empleados ha producido grandes cambios en el enfoque de las organizaciones en cuanto a la seguridad de los datos. Aunque la IA está transformando la productividad y los flujos de trabajo, al igual que cualquier tecnología emergente, también puede amplificar los riesgos existentes o introducir nuevos riesgos que requieren un enfoque diferente para proteger la información confidencial. Como resultado, las empresas siguen buscando su lugar en un panorama que cambia rápidamente. Un director de ingeniería y análisis de reclamaciones de transporte explica lo siguiente: "Estamos supervisando los datos con más cuidado en el ámbito de la IA. Se ha generado tensión entre productividad y seguridad, precisión y privacidad".

La confianza para asegurar el uso de IA por parte de los empleados sigue siendo desigual. A la mayoría (el 84 %) le gustaría tener más confianza a la hora de administrar y descubrir la entrada de datos. Mientras que el 22 % de las organizaciones se sienten extremadamente seguras en su capacidad para mantener la seguridad de los datos, la mayoría (el 59 %) solo están "muy seguras", lo que indica que hay margen de mejora. La mayoría de las empresas (el 86 %) reconoce que les gustaría ser más optimistas en cuanto a la gestión y el descubrimiento de datos generados por las herramientas de IA.

A medida que la IA se vuelve más esencial para la productividad diaria, el uso de aplicaciones de IA también ha acentuado las preocupaciones sobre los incidentes de seguridad de los datos. **Casi un tercio (el 31 %) de las organizaciones prevé un aumento de los incidentes de seguridad de los datos debido al uso de la IA por parte de empleados, y el 84 % admite que necesita hacer más para protegerse contra estos riesgos.** Esta ansiedad es especialmente alta entre las organizaciones más grandes: mientras que el 26 % de las empresas medianas prevé un aumento de los incidentes de seguridad de datos relacionados con la IA y el 29 % de las grandes empresas espera un incremento, entre las empresas extragrandes existe un grupo considerablemente mayor (el 36 %) que prevé un aumento.



quieren tener más confianza en la gestión y el descubrimiento de introducción de datos en las aplicaciones y herramientas de IA



coinciden en que necesitan hacer más para protegerse contra el uso arriesgado de aplicaciones y herramientas de IA por parte de empleados

El uso no autorizado de la IA está generalizado

El 40 % informa de que sus aplicaciones de IA ya han sufrido vulneraciones o se han visto comprometidas en un incidente de seguridad de los datos. Una vez más, esta cifra es mayor entre las organizaciones de mayor tamaño: las empresas medianas informan de un índice de incidentes del 36 %, las grandes empresas informan de un 38 % y las empresas extragrandes han sido las que han registrado más incidencias, con un 44 %.

El uso no autorizado de la IA suele producirse cuando los empleados inician sesión con credenciales personales o utilizan dispositivos personales para tareas relacionadas con el trabajo. **De media, el 65 % de las organizaciones admite que sus empleados utilizan herramientas de IA no autorizadas.** Entre las formas en que los empleados utilizan herramientas de IA no autorizadas se incluyen las siguientes:

- El 53 % que inicia sesión con credenciales personales para trabajar
- El 48 % que usa un dispositivo personal al utilizar la IA para el trabajo
- El 47 % que utiliza sus credenciales de trabajo para usar la IA con fines personales

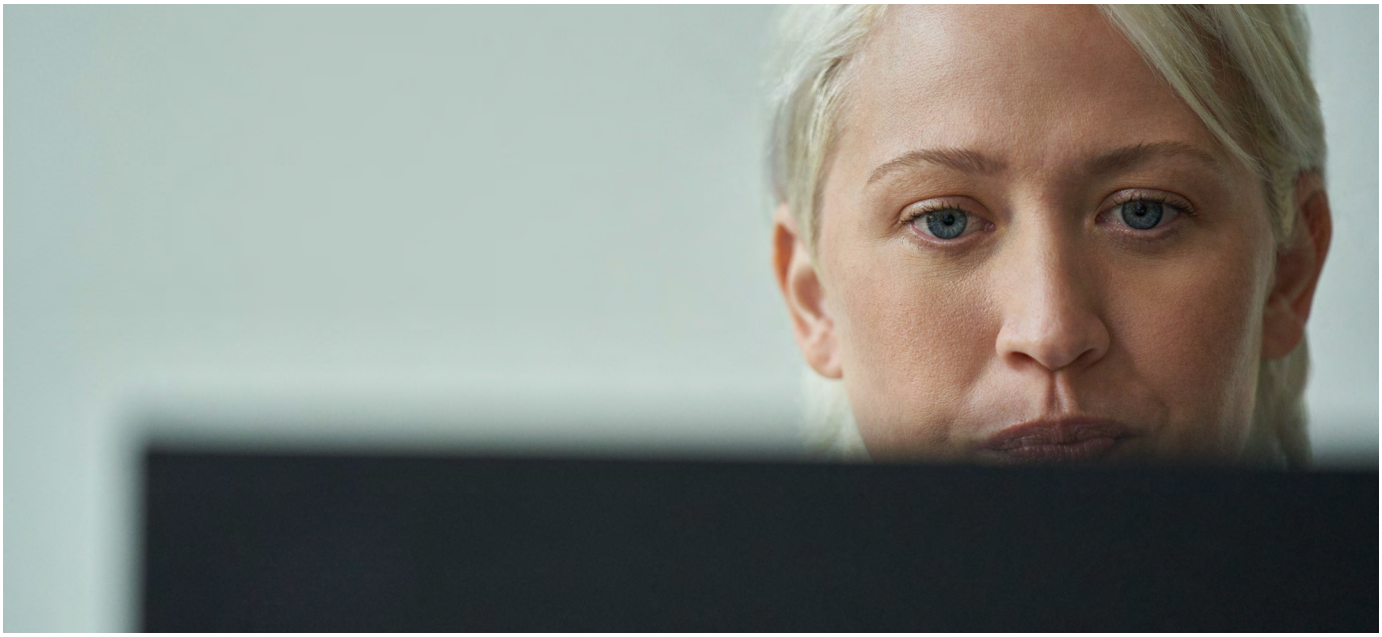
La mitad de todas las organizaciones afirman estar preocupadas por la falta de controles para detectar y mitigar los riesgos cuando los empleados utilizan aplicaciones de IA de formas no seguras. Esta cifra varía en función del tamaño de la empresa, ya que el 43 % de las empresas medianas, el 50 % de las grandes organizaciones y el 54 % de las empresas extragrandes expresan su preocupación por su capacidad para gestionar estos riesgos.

Dado el aumento en el uso de la IA, se necesitan más controles de seguridad de los datos

A medida que la IA se integra más en las operaciones diarias, las organizaciones reconocen la necesidad de una protección más sólida. **Aunque al 96 % de las empresas les preocupa el uso por parte de los empleados de estas herramientas, casi esa misma cifra está dispuesta a invertir en soluciones para superar sus preocupaciones.**

"El enfoque principal va a ser cómo mantenerse por delante de la IA. El enfoque de la seguridad es reducir el tamaño de los datos y supervisar los datos con más detenimiento. En cuanto a la IA, para que tus modelos sean más representativos para identificar sesgos, se necesitan más datos. Entonces, ¿cómo conciliar todo esto?", plantea un director de ingeniería, arquitectura y análisis del transporte. La gran mayoría de los responsables de la toma de decisiones (el 87 %) está preparado para invertir tiempo y dinero en formación para los empleados en prácticas seguras sobre el uso de herramientas de IA. **Esto se debe a que el 85 % afirma que es fundamental que los empleados utilicen estas herramientas para seguir siendo competitivos.**

Casi todas las organizaciones (el 93 %) se encuentran en alguna etapa de desarrollo o implementación de controles en torno al uso de la IA, pero muchas todavía están en las primeras fases. Solo el 39 % ha implementado completamente controles de seguridad de los datos para la IA, mientras que el 24 % ha desarrollado políticas pero aún no las ha puesto en práctica. Un vicepresidente de seguridad de datos en hostelería explica: "Tenemos que alinearnos con los controles de IA, pero estamos adoptando el uso de la IA al mismo tiempo. Nos facilita la vida y nos ayuda a ser más eficientes".



Mientras las organizaciones están adoptando medidas para proteger los datos confidenciales de un uso indebido en las aplicaciones de IA, existe una necesidad clara de aplicar controles más exhaustivos. Actualmente, el 43 % de las empresas se centra en evitar que los datos confidenciales se carguen en aplicaciones de IA, mientras que otro 42 % registra todas las actividades y el contenido dentro de estas aplicaciones para posibles investigaciones o respuesta a incidentes. Del mismo modo, el 42 % está bloqueando el acceso de los usuarios a herramientas no autorizadas y un porcentaje igual está invirtiendo en formación de los empleados sobre el uso seguro de la IA.

Las empresas cuyos empleados realizan un uso no autorizado de la IA tienen una mayor necesidad de ciertos tipos de controles. **Entre las organizaciones que registran un uso de la IA no autorizado, el 42 % necesita controles para identificar a los usuarios que corren riesgos en función de las consultas de la IA, en comparación con el 30 % en las que no se realiza un uso no autorizado. Además, el 40 % de las organizaciones que se enfrentan al uso no autorizado de la IA necesitan controles para administrar el ciclo de vida de los datos (como protocolos de retención y eliminación), en comparación con el 27 % de las empresas que no sufren este problema.**

Los 5 principales controles necesarios para la IA

Evitar que los datos confidenciales se carguen en la IA	43 %
Registrar todas las actividades y contenidos en herramientas de IA para posibles investigaciones o respuestas a incidentes	42 %
Bloquear el acceso de los usuarios a herramientas de IA no autorizadas	42 %
Formar a los empleados sobre el uso seguro de herramientas de IA	42 %
Identificar a los usuarios que corren riesgos en función de las consultas en IA	41 %

El camino a seguir

Para mantener un enfoque sólido de seguridad de los datos, los equipos necesitan un conjunto completo de controles para descubrir, proteger y gestionar sus datos en las aplicaciones de IA. A continuación, se indican tres estrategias clave que los equipos pueden utilizar:

Aumentar la visibilidad del uso de aplicaciones de IA y los datos que fluyen a través de las aplicaciones: utiliza herramientas de seguridad de datos que puedan detectar y utilizar aplicaciones de IA. Estas herramientas proporcionan conocimientos sobre una lista completa de las aplicaciones de IA que se utilizan junto con sus perfiles de riesgo, incluidos detalles como los controles de seguridad de datos admitidos y el cumplimiento de las normativas. Utiliza herramientas que puedan proporcionar una clasificación coherente de los datos confidenciales en las interacciones con la IA y muestra tendencias sobre cómo fluyen los datos a través de aplicaciones de IA.

Desarrollar y aplicar políticas: crea políticas basadas en los conocimientos obtenidos del análisis. Estas políticas pueden incluir directrices para las aplicaciones y los procedimientos aprobados de IA para bloquear o restringir el uso por parte de los empleados de aplicaciones no autorizadas. Incluso en las aplicaciones de IA aprobadas, puedes crear políticas detalladas que permitan el flujo de datos no confidenciales y, al mismo tiempo, restringir el uso de datos confidenciales y críticos para el negocio. Esto puede incluir el bloqueo de ciertas acciones, como pegar datos confidenciales en herramientas de IA basadas en navegadores para garantizar la seguridad de los datos.

Evaluar de forma habitual los riesgos y mejorar las políticas: genera periódicamente informes que demuestren los niveles de riesgo de las aplicaciones de IA que se utilizan, las tendencias sobre cómo fluyen los datos confidenciales a través de estas aplicaciones, así como la actividad de los usuarios en estas aplicaciones. Esto ayuda a evaluar el panorama general de riesgos y tomar decisiones informadas sobre las políticas de seguridad de datos más relevantes.

3

Los responsables de la toma de decisiones son optimistas sobre el potencial de la IA para impulsar sus esfuerzos de seguridad de los datos

Las investigaciones sobre seguridad de los datos dependen en gran medida de la IA

La gran mayoría de las organizaciones (el 88 %) ya está invirtiendo en IA para mejorar sus esfuerzos de detección y respuesta, descubriendo datos confidenciales, detectando actividades anómalas y protegiendo automáticamente los datos en riesgo. **El 77 % de las organizaciones cree que la IA acelerará estos procesos y el 76 % piensa que mejorará la precisión de sus estrategias de detección y respuesta.**

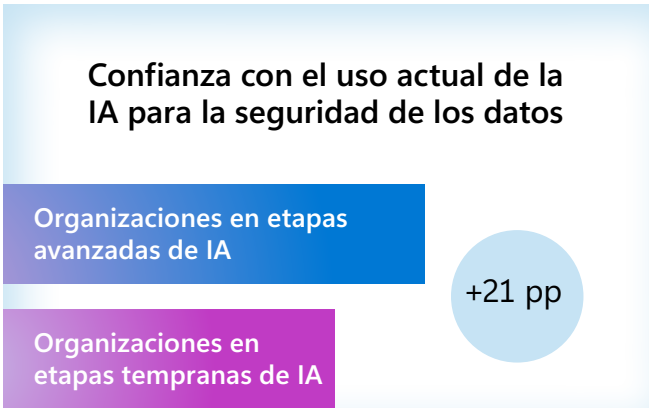
Mientras que el 73 % de los responsables de la toma de decisiones expresan su preocupación acerca del uso de la IA para reforzar la seguridad de los datos, el 50 % afirma que no ha inhibido su uso de la IA para reforzar la seguridad de los datos y solo el 23 % dice que los ha retenido. En total, un abrumador 93 % tiene al menos la intención de usar la IA para reforzar la seguridad de los datos a pesar de sus preocupaciones.

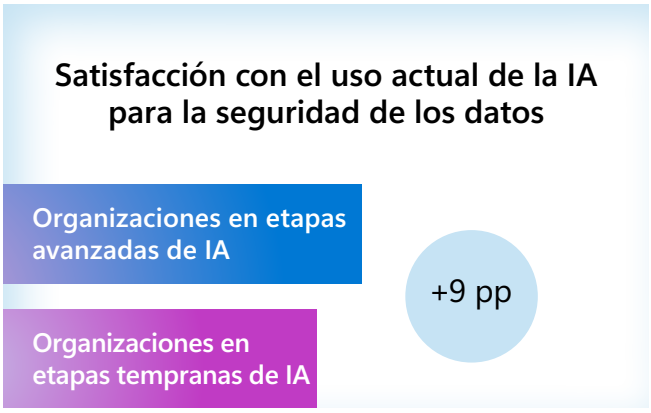
El uso de la IA para reforzar la seguridad de los datos aumenta la visibilidad, la confianza y la satisfacción

Una de las principales ventajas del uso de la IA para reforzar la seguridad de los datos es su capacidad para aumentar la visibilidad de los sistemas, mitigando la importante preocupación de los responsables de la toma de decisiones de saber dónde se almacenan los datos y cómo se clasifican (el 20 %).[1] El 88 % de los responsables de la toma de decisiones de seguridad de los datos cree que la integración de la IA en las soluciones de seguridad de los datos permitirá a los equipos tener más visibilidad, lo que permitirá a las organizaciones procesar y analizar muchos más datos de lo que sería posible de otra manera. Las organizaciones medianas se centran principalmente en reducir los riesgos a corto plazo, como minimizar los errores humanos en sus procesos de seguridad de los datos. De hecho, el 43 % de las empresas medianas dan prioridad a reducir los riesgos causados por errores humanos, en comparación con solo el 37 % de las empresas extragrandes.

En cambio, las empresas más grandes aplican un enfoque más avanzado, al resaltar los riesgos a largo plazo y la necesidad de adaptabilidad. Ese mayor nivel de sofisticación permite a los equipos de seguridad de los datos adaptarse mejor a los riesgos en evolución, una de las principales prioridades para el 49 % de las empresas extragrandes, en comparación con el 43 % de las organizaciones medianas.

En general, las organizaciones que están más avanzadas en el uso de la IA para fortalecer la seguridad de los datos informan de niveles mucho más altos de confianza y satisfacción con sus estrategias de seguridad de los datos. **Entre las que están en las etapas avanzadas de la implementación de IA, el 90 % se siente extremadamente o muy segura en su uso de la IA para reforzar la seguridad de los datos, en comparación con el 69 % que se encuentra en etapas más tempranas. De forma similar, el 76 % de las organizaciones con un uso avanzado de la IA expresan satisfacción con sus soluciones de seguridad de datos, mientras que solo el 67 % de las que se encuentran en etapas anteriores manifiestan lo mismo.**





1. Encuesta de septiembre de 2024 entre responsables de toma de decisiones de seguridad de los datos, gestión, cumplimiento y privacidad, encargada Microsoft a la agencia MDC Research

Las organizaciones están reduciendo el número de incidentes de seguridad de los datos y mejorando la gestión de alertas con IA

Las organizaciones que utilizan la IA para fortalecer sus operaciones de seguridad de datos registran significativamente menos alertas. **De media, las que han implementado herramientas de seguridad de datos basadas en IA reciben 47 alertas al día, en comparación con las 79 alertas de aquellas que no lo han hecho. Además, quienes usan la IA pueden revisar el 66 % de sus alertas diarias, mientras que las organizaciones que no usan la IA solo logran revisar el 60 %.**

Por otro lado, es más probable que la que utilizan la IA para reforzar la seguridad de los datos también apliquen la IA para mitigar los riesgos (el 56 % frente al 26 %). La reducción del volumen de alertas, junto con la mayor capacidad para mitigarlas utilizando la IA, parece haber tenido un enorme impacto en el número global de incidentes de seguridad de datos. Las organizaciones que han implementado la IA para reforzar la seguridad de los datos observan una reducción del 65 % en los incidentes de seguridad de los datos, en comparación con las que no utilizan la IA para reforzar la seguridad de los datos.

Se espera que la IA tenga el mayor impacto en la respuesta

En cuanto a la detección, el 33 % de los responsables de la toma de decisiones espera que la IA ayude a detectar la actividad anómala, mientras que el 23 % cree que ayudará a investigar posibles incidentes de seguridad de los datos. Otro 22 % ve el potencial de la IA al hacer recomendaciones para proteger mejor sus entornos de datos.

Sin embargo, en la respuesta es donde los responsables de la toma de decisiones esperan que la IA tengan el mayor impacto. El 34 % cree que la IA podría bloquear automáticamente el intercambio inadecuado de datos confidenciales y el 32 % afirma que protegerá los datos en riesgo. Otro 26 % observa que la IA ayuda a mitigar los riesgos de seguridad de los datos y aplicar controles apropiados, mientras que el mismo número espera que la IA avise automáticamente del comportamiento de riesgo de los usuarios.

El camino a seguir

La integración de la IA en soluciones de seguridad de datos puede ayudar al ofrecer a los equipos orientación en tiempo real, capacidades de resumen y compatibilidad con lenguaje natural en áreas destacadas que de otro modo podrían haber pasado desapercibidas. Esto también puede acelerar la investigación y reforzar la experiencia de los equipos de seguridad de los datos. Así es como estas funcionalidades pueden tener un impacto:

Resumen de alertas: las investigaciones pueden ser desalentadoras, debido al volumen de orígenes para analizar y las diversas reglas de políticas. Al integrar la IA en la prevención de pérdida de datos (DLP) y la administración de riesgos internos (IRM), los equipos pueden recibir rápidamente un resumen de las alertas, incluidos el origen, las reglas de políticas y los conocimientos sobre los riesgos de los usuarios, con el fin de comprender qué datos confidenciales se han visto comprometidos y el riesgo asociado a los usuarios.

Comunicaciones contextuales: las organizaciones deben cumplir los requisitos normativos en torno a las comunicaciones comerciales, lo que a menudo exige una revisión exhaustiva de las infracciones. La IA puede ayudar a los equipos de seguridad de los datos a evaluar el contenido frente a las normativas y políticas corporativas para resaltar las comunicaciones de alto riesgo que podrían dar lugar a un incidente de seguridad de los datos.

Lenguaje natural para consultar con palabras clave: la búsqueda puede ser un flujo de trabajo complejo y laborioso durante investigaciones, lo que normalmente requiere el uso del lenguaje de consulta con palabras clave. Con la IA, los equipos de seguridad de datos pueden introducir solicitudes de búsqueda en lenguaje natural para agilizar el inicio de la búsqueda y realizar investigaciones más avanzadas.

Recomendaciones finales

1 Protégete frente a incidentes de seguridad de datos adoptando una plataforma integrada

La adopción de una plataforma de seguridad de datos totalmente integrada ofrece una estrategia más segura y optimizada en un panorama que evoluciona cada vez más, lo que reduce la complejidad y aumenta la visibilidad, al mismo tiempo que mejora la protección. Un enfoque integrado puede ayudar a las organizaciones a mejorar la administración de la posición de seguridad de los datos al centralizar los controles de seguridad y al ofrecer una visibilidad unificada de los datos, los usuarios y las actividades, lo que fortalecerá y agilizará la detección y la protección en torno a los riesgos para los datos. Puesto que el 82 % de las organizaciones coincide en que una plataforma integrada es superior, la consolidación no solo es beneficiosa, sino esencial.

2 Aumenta la visibilidad sobre el uso interno de la IA para evaluar los controles necesarios del uso de los empleados de la IA que no afectará a la productividad

A medida que la IA se vuelve más habitual en el lugar de trabajo, puede aumentar los riesgos existentes y presentar otros nuevos. Las organizaciones admiten que tienen que hacer más para protegerse contra el uso no seguro de la IA. El uso de controles integrados y la visibilidad de las aplicaciones de IA es fundamental para mantener la seguridad de los datos sin interrumpir la productividad. Formar a los empleados sobre el uso seguro de la IA puede ayudar a las organizaciones a minimizar comportamientos de riesgo y a garantizar que los equipos sigan beneficiándose de estas potentes herramientas.

3 Aumenta el nivel de tu estrategia de seguridad de datos con la ayuda de la IA

Gracias a la IA, los equipos de seguridad de los datos pueden centrarse en iniciativas más estratégicas, en lugar de reaccionar ante amenazas constantes y a un gran volumen de alertas. Las empresas que se encuentran en etapas avanzadas de la implementación de la IA están más seguras y se sienten más satisfechas con sus soluciones de seguridad de los datos que las que están empezando a implementarla. Mediante la implementación de la IA como parte de una estrategia integral de seguridad de los datos, las organizaciones pueden mejorar su visibilidad, lo que refuerza su capacidad para detectar y responder a los riesgos, algo que en última instancia refuerza su enfoque general de seguridad de los datos.

Objetivos de la investigación

Entre los objetivos del estudio se incluyeron:

1. Entender el entorno de la seguridad de los datos, incluidas las prioridades y las mentalidades, los desafíos y la causa y efecto de los incidentes de seguridad de los datos.
2. Explorar el futuro de la seguridad de los datos, incluidas qué estrategias e innovaciones están surgiendo y cómo tienen pensado invertir las organizaciones en el futuro.
3. Descubrir la función de la IA en la mejora de la seguridad de los datos y el papel de la IA en la protección de datos.

Metodología

Se llevó a cabo una encuesta online multinacional de 20 minutos del 5 al 23 de agosto de 2024, entre 1376 responsables de toma de decisiones de seguridad de datos.

Las preguntas se centraron en el panorama de la seguridad de los datos y los incidentes de seguridad de los datos en comparación con 2023. Además, la encuesta de este año incluía preguntas sobre cómo garantizar el uso de la IA por parte de los empleados y el uso de la IA para reforzar la seguridad de los datos.

Elección de la población de muestra

Para cumplir con los criterios de selección, los responsables de la toma de decisiones de seguridad de datos tenían que presentar estas características:

- Ser directores de seguridad de la información y responsables de la toma de decisiones inmediatos (C-2 y superiores) con control sobre la seguridad de los datos
- Trabajar en organizaciones empresariales (más de 500 empleados; variedad de tamaños)
- Ser una combinación de sectores regulados y no regulados (excluidos el sector educativo, la administración u organizaciones sin ánimo de lucro)

De los 1376 responsables de la toma de decisiones de seguridad de los datos encuestados para el estudio, los resultados completos por país fueron:

- EE. UU.: 302
- Reino Unido: 305
- India: 301
- Brasil: 158
- Francia: 156
- Australia: 154

hypothesis Microsoft Security