Microsoft Security

Proteger los datos en la era de la IA generativa

Conocimientos y estrategias para los CISO

Índice

Presentación

La seguridad de los datos está cambiando con la adopción de la IA generativa

La IA generativa crea nuevo contenido a partir de datos existentes, lo que permite a las organizaciones transformar sus operaciones, impulsar la innovación, impresionar a los clientes y mejorar la productividad. Sin embargo, para maximizar el valor de esta tecnología nueva y emocionante, es necesario disponer de una seguridad de los datos eficaz que permita combatir el intercambio excesivo de datos, las filtraciones y el incumplimiento. Las herramientas integradas de seguridad de los datos, gestión y cumplimiento ayudan a mitigar estos riesgos y permiten una implementación segura de la tecnología de IA generativa.

de los trabajadores del conocimiento usan la IA generativa en el trabajo hoy en día y dicen que les ayuda a:

- Ahorrar tiempo (90 %)
- Centrarse en el trabajo más importante (85 %)
- Ser más creativos (84 %)
- Disfrutar más de su trabajo (83 %)[1]

[1] La IA generativa en el trabajo ya está aquí. Ahora viene lo difícil

Tres áreas de riesgo de la IA generativa que se deben tener en cuenta

Filtraciones de datos: los usuarios podrían exponer datos confidenciales (como la información personal de los clientes) al interactuar con las aplicaciones de IA generativa a través del chat, enviar formularios o cargar documentos. La detección y el control de estas interacciones pueden ayudar a garantizar la seguridad de los datos confidenciales.

Intercambio excesivo de datos: si los permisos o controles de acceso no están bien configurados, los datos confidenciales pueden quedar expuestos a partes no autorizadas a través de las aplicaciones de IA generativa.

Uso no conforme: sin las protecciones adecuadas, las personas pueden utilizar las herramientas de IA generativa para crear material poco ético o de alto riesgo.

Abordar los desafíos de seguridad de los datos nuevos y existentes con una solución integrada

La necesidad de soluciones de seguridad de los datos integradas nunca había sido tan grande. La datosfera se duplica cada cuatro años. La rápida adopción de la IA generativa alimentará aún más la explosión de datos. Los almacenes de datos en rápido crecimiento hacen que sea más importante, y más complejo, prevenir incidentes de seguridad de los datos.

Para mantener la seguridad de los datos críticos del negocio y proteger su ventaja competitiva, su reputación y la lealtad de los clientes, las organizaciones necesitan proteger sus datos con un enfoque integral que combine los datos y el contexto del usuario en todo su patrimonio, dispositivos y aplicaciones de IA generativa.

Sin embargo, muchas organizaciones siguen utilizando soluciones de seguridad de los datos dispares, lo que puede aumentar el coste y el riesgo de estas actividades. Crean silos que dejan brechas de protección, lo que conduce a vulnerabilidades e ineficiencias.

Al elegir una plataforma de seguridad de los datos integrada, las organizaciones pueden unificar las políticas, la visibilidad y la aplicación en todo el ecosistema de datos. Este enfoque reduce la complejidad, disminuye los costes y refuerza las defensas frente a riesgos emergentes, lo que ayuda a mejorar la seguridad de los datos independientemente de dónde residan dichos datos.

Caso de éxito:

El Grupo Bimbo recurre a Microsoft Security para adoptar un enfoque proactivo respecto a la seguridad de los datos

Ante la compleja tarea de comprender cómo fluyen los datos confidenciales a través de su organización, dónde residen esos datos, y cómo proteger y evitar su filtración, el Grupo Bimbo utiliza Microsoft Security para sus necesidades de seguridad de datos:

Utilizamos Microsoft Purview para mantener los datos del Grupo Bimbo más seguros y de forma más proactiva que nunca".

– Alejandro Cuevas
Responsable global de TI, riesgo y cumplimiento, Grupo Bimbo

La funcionalidad de Protección adaptativa es un ejemplo perfecto de lo útil que puede ser el machine learning, ya que lo utilizamos para tomar decisiones basadas en la seguridad y fundamentadas en la lógica y el contexto. El hecho de poder adaptarnos dinámicamente al contexto nos ayuda a lograr un equilibrio más eficaz entre seguridad y flexibilidad".

– Jose Antonio Parra
Vicepresidente de transformación digital global, datos y análisis, Grupo Bimbo

Lee el caso de Grupo Bimbo >

Capítulo 1

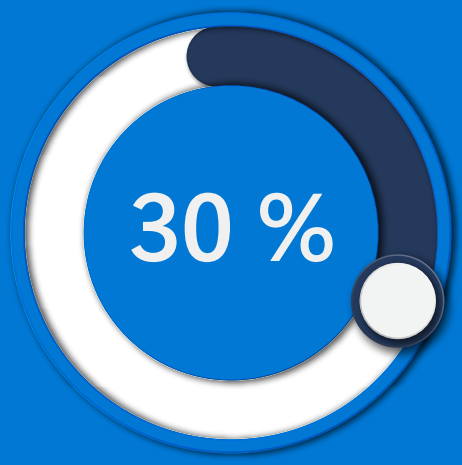
Una estrategia triple

Protege los datos con un enfoque integral en todo tu patrimonio, dispositivos y aplicaciones de IA generativa. En esta sección, examinaremos tres componentes críticos de la seguridad de los datos: detectar el riesgo de los datos, evitar la pérdida de datos y responder a incidentes de seguridad.

Detectar riesgos ocultos para los datos dondequiera que residan o dondequiera que vayan

Descubre riesgos ocultos en tus datos mediante conocimientos agregados basados en IA con datos correlacionados y el contexto de los usuarios. El hecho de conocer la ubicación y el volumen de los datos confidenciales permite una mejor protección y administración.

- **Obtén visibilidad:** conoce dónde residen los datos confidenciales en archivos, documentos, correos electrónicos, mensajes, dispositivos, bases de datos, etc.
- **Clasifica y protege:** utiliza clasificadores inteligentes para encontrar y proteger la información confidencial rápidamente.
- **Detecta riesgos internos:** utiliza el machine learning para detectar amenazas sin intervención manual.



Más del 30 % de los responsables de la toma de decisiones afirman que no saben cuáles son los datos críticos de su empresa ni dónde se encuentran.[2]

[2] Índice de seguridad de los datos | Microsoft Security

Protege y evita la pérdida de datos en todo tu patrimonio de datos

Los controles flexibles ayudan a proteger los datos en entornos on-premises, en el cloud e híbridos, en distintos dispositivos y en aplicaciones, al tiempo que equilibran la seguridad y la productividad.

- **Gestiona las políticas de DLP de forma centralizada:** elige una solución que permita a los equipos de seguridad de los datos crear y administrar políticas de DLP completas desde una sola herramienta.
- **Solicita una protección adaptativa:** adapta dinámicamente los controles de protección en función del nivel de riesgo del usuario. Los controles de DLP se pueden aplicar automáticamente de forma más estricta a los usuarios de alto riesgo.
- **Extiende las políticas de DLP a todo el panorama de aplicaciones:** elige soluciones que apliquen protecciones a la gama más amplia de aplicaciones, incluido SaaS.

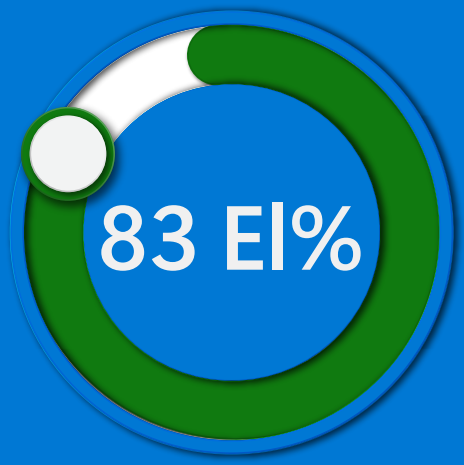
de los líderes de seguridad afirman que la filtración de datos confidenciales es su principal preocupación.[2]

[2] Índice de seguridad de los datos | Microsoft Security

Investiga y responde rápidamente a los incidentes de seguridad de los datos

Responde a los incidentes de seguridad de los datos a la velocidad de las máquinas utilizando los conocimientos de la IA correlacionados en un conjunto integrado de productos.

- **Mejora las investigaciones de DLP:** mejora la comprensión de los incidentes de DLP con una imagen completa del contexto del usuario y el contenido, incluyendo dónde se han originado los archivos y las acciones que realizó el usuario.
- **Dota a los investigadores de herramientas unificadas:** elige soluciones que proporcionen un sistema de análisis completo de alertas, administración y corrección en un solo lugar.
- **Resuelve las incidencias más rápido:** acelera el tiempo de actuación con herramientas de investigación intuitivas que permitan a los investigadores revisar el contenido de manera eficiente, examinar las pruebas forenses y escalar los casos a eDiscovery.



de las organizaciones experimentan más de una filtración de datos en su vida.[2]

[2] Índice de seguridad de los datos | Microsoft Security

Capítulo 2

Abordar los desafíos específicos de la IA generativa

Para aprovechar todo el valor de las inversiones en IA generativa, las organizaciones deben elegir una solución de seguridad de los datos integrada que incorpore características de gobierno y seguridad de IA generativa expresamente diseñadas. Estas herramientas pueden ofrecer una visión de los flujos de datos, los riesgos y la eficacia de la gestión. A continuación se describen las tres categorías de capacidades específicas de la IA generativa que se deben tener en cuenta al crear una estrategia de protección de datos.

Detección del uso de aplicaciones de IA generativa

Al conocer el flujo de los datos confidenciales y las interacciones, los equipos pueden identificar vulnerabilidades y elaborar estrategias de seguridad dirigidas. Las herramientas de seguridad pueden ofrecer visibilidad en tiempo real del uso de aplicaciones de IA generativa y avisar a los administradores de cualquier acceso o uso no autorizado.

- **Analiza el uso:** las herramientas de seguridad hacen que sea fácil ver qué información se comparte con las aplicaciones de IA generativa, lo que ayuda a evaluar los riesgos con precisión.
- **Identifica los riesgos críticos:** las soluciones de detección de datos priorizan los datos confidenciales, lo que evita un intercambio excesivo de datos y garantiza una mejor protección.
- **Detecta interacciones poco éticas:** los sistemas de detección identifican cualquier infracción normativa, blanqueo de capitales y acoso dirigido, lo que permite tomar medidas con prontitud.

Protección de los datos confidenciales

Herramientas como el cifrado, el acceso basado en roles y el etiquetado automático ayudan a reducir la probabilidad y la gravedad de las filtraciones de datos.

- **Implementa controles de seguridad de los datos:** tecnologías como el cifrado, la marca de agua y el etiquetado automático respaldan las medidas de acceso apropiadas para garantizar que la IA generativa respeta los permisos en los archivos a los que hace referencia.
- **Evita la filtración de datos en aplicaciones de terceros:** las medidas de protección dinámicas pueden ayudar a evitar que se peguen datos confidenciales en indicaciones de IA generativa, reduciendo así los riesgos de filtración.
- **Aplica una protección adaptativa:** las medidas de seguridad personalizadas basadas en los niveles de riesgo de los usuarios ayudan a respaldar unas políticas flexibles.

Control del uso de la IA generativa

Para afrontar el panorama normativo de la IA generativa hacen falta unas completas herramientas de gestión y cumplimiento integradas. Al adoptar unos marcos de trabajo robustos y garantizar la visibilidad de los datos, se puede simplificar el cumplimiento de unos estándares en constante cambio. Las herramientas integradas rastrean las interacciones con la IA generativa y aplican políticas, lo que ayuda a evitar sanciones legales y muestra un compromiso con las prácticas éticas de IA. El cumplimiento proactivo respalda una innovación segura y la confianza de los accionistas.

- **Detecta las interacciones con la IA generativa:** las herramientas de registro y auditoría capturan y revisan las indicaciones y respuestas de la IA generativa, lo que ofrece la posibilidad de revisar y mejorar las prácticas y políticas de la empresa.
- **Detecta y mitiga los riesgos:** los clasificadores avanzados y el machine learning identifican y bloquean o mitigan de otro modo las indicaciones de IA generativa poco éticas.
- **Optimiza las respuestas legales:** las soluciones de eDiscovery conservan y recopilan de manera eficiente los datos de IA generativa relevantes, lo que minimiza la exposición legal.

Abordar las necesidades de cumplimiento normativo emergentes de la IA generativa

Las cambiantes normativas de la IA generativa requieren estrategias sólidas capaces de adaptarse tanto a los estándares actuales como a los emergentes. Las herramientas relevantes pueden ayudar a promover el uso ético de la IA generativa, fomentar la confianza y respaldar la innovación segura dentro de entornos regulados.

- **Cumple las normativas de IA generativa:** las plantillas de evaluación y las herramientas de administración del cumplimiento ayudan a las organizaciones a alinearse con estándares como la Ley de IA de la UE y el NIST AI RMF.
- **Refuerza los controles de cumplimiento:** la detección continua de riesgos y la auditoría ayudan a cumplir las normativas.
- **Reduce los riesgos de cumplimiento:** implementa herramientas que garanticen la visibilidad de los datos y ayuden a evitar el intercambio de contenido no autorizado con las aplicaciones de IA.

Capítulo 3

Dotar de IA generativa a los profesionales de seguridad de los datos

La gestión integral y las protecciones de la IA generativa ayudan a abordar los nuevos desafíos de seguridad. Además, la IA generativa tiene el potencial de poner nuevas capacidades en manos de los equipos de seguridad, redefiniendo su forma de abordar la protección de la información confidencial.

Por ejemplo, la IA generativa ayuda a identificar y priorizar los riesgos de seguridad mejorando la comprensión de la intención y el contexto, lo que facilita la tarea de abordar posibles amenazas. Acelera y simplifica las labores de investigación de los administradores y dota a los analistas del centro de operaciones de seguridad (SOC) de inteligencia y datos mejorados, elevando así sus capacidades.

de las organizaciones declaran que su equipo de seguridad de los datos necesita más personas para gestionar eficazmente las responsabilidades críticas.[3]

[3] Índice de seguridad de los datos | Microsoft Security

Ventajas de la IA generativa para la seguridad

Eficiencia: la IA generativa ayuda a priorizar y automatizar las tareas de seguridad para mejorar la productividad.

Velocidad: la IA generativa ayuda a las personas a conocer las amenazas cibernéticas únicas en tiempo real, lo que acelera la detección y la respuesta.

Escalabilidad: la IA generativa procesa grandes volúmenes de datos de manera eficiente, lo que permite administrar entornos de seguridad extensos y complejos.

Cómo la IA generativa puede mejorar las capacidades de seguridad de los datos

Resumen de alertas: la IA generativa resume la prevención de pérdida de datos (DLP) y las alertas de administración de riesgos internos, lo que permite a los equipos de seguridad comprender rápidamente la naturaleza y gravedad de las amenazas potenciales sin realizar un análisis manual a través de registros extensos.

Triaje automatizado: al priorizar las alertas basadas en el riesgo, la IA generativa permite a los profesionales de la seguridad centrarse en los problemas más críticos. Este proceso de triaje ayuda a distribuir los recursos eficazmente y acelera los tiempos de respuesta ante posibles filtraciones.

Análisis y conocimientos de datos: la IA generativa puede analizar grandes cantidades de datos para identificar patrones y correlaciones que puedan indicar riesgos de seguridad. Este análisis incluye examinar los patrones de comunicación y comportamiento del usuario para detectar anomalías que indiquen riesgos internos o intentos de exfiltración.

Indicaciones interactivas: las indicaciones interactivas permiten a los profesionales de seguridad hacer preguntas específicas y recibir detalles sobre su estado de seguridad y cumplimiento. Consultas como "Resume la alerta de DLP con id. 12345" o "Muéstrame las cinco principales alertas de Administración de riesgos internos de las últimas 24 horas" proporcionan información útil e inmediata.

Administración de políticas y cumplimiento: la IA generativa puede contribuir a un cumplimiento más eficaz al resumir las coincidencias de políticas en función de clasificadores entrenables. Esta funcionalidad permite la detección continua de problemas y el cumplimiento de las normas.

eDiscovery y retención legal: la IA generativa proporciona resúmenes contextuales de casos de eDiscovery, agrupando y revisando documentos de manera eficiente. Esta función ayuda a los equipos jurídicos a administrar los datos de litigios o consultas normativas.

Un enfoque integral respecto a la seguridad de los datos

Las soluciones de seguridad de Microsoft mejoran la capacidad de tu organización para proteger los datos de todo tu patrimonio, dispositivos y aplicaciones de IA generativa. Microsoft Purview ofrece un conjunto unificado de herramientas para gestionar, proteger y administrar tus datos, independientemente de dónde se encuentren. Al proporcionar una cobertura integrada, Microsoft Purview aumenta la visibilidad para una mejor protección y gestión y se adapta a los roles cambiantes dentro de la administración de TI.

- Detecta, clasifica y protege los datos confidenciales durante todo su ciclo de vida, dondequiera que residan o dondequiera que vayan, gracias a Microsoft Purview Information Protection.
- Conoce la actividad de los usuarios y el contexto de los datos e identifica los riesgos con Microsoft Purview Insider Risk Management.
- Evita el uso no autorizado o accidental de los datos con Microsoft Purview Data Loss Prevention.
- Adapta dinámicamente los controles de protección en función del nivel de riesgo del usuario con la Protección adaptativa de Microsoft Purview.

Y Microsoft Purview se integra con el resto del ecosistema de Microsoft Security para ayudar a tu equipo a:

- Investigar y responder rápidamente a los incidentes de seguridad de los datos con Microsoft Security Copilot.
- Ver los incidentes de seguridad de los datos en contexto mediante Microsoft Defender XDR.
- Permitir o denegar el acceso de los usuarios a las aplicaciones donde residen los datos, con la Protección adaptativa integrada en Microsoft Entra Conditional Access.

Además, con Microsoft Purview Copilot, las organizaciones pueden revolucionar el cumplimiento y la seguridad de sus datos mediante una automatización y unos conocimientos basados en IA. Al integrar Copilot, los equipos pueden investigar y responder rápidamente a los incidentes de seguridad de los datos, además de conocer sus datos de una forma más profunda gracias a resúmenes interactivos y análisis de riesgos. Esto permite aplicar un enfoque más optimizado y eficaz respecto a la gestión de riesgos y la protección de información confidencial.

¿Por qué elegir Microsoft para la seguridad de los datos de la IA generativa?

Microsoft ofrece un enfoque integrado respecto a la seguridad de los datos basado en una plataforma de confianza con herramientas que abordan los desafíos existentes y emergentes al tiempo que maximizan la productividad y la eficiencia. Como parte del ecosistema de seguridad de Microsoft, Purview y Security Copilot te permiten reforzar tu marco de protección de los datos para que tu empresa pueda aprovechar todo el potencial de la IA generativa. Con el enfoque adecuado, la propia IA generativa puede convertirse en un aliado eficaz en la protección de tus datos.

Obtén más información sobre las soluciones de seguridad de los datos de Microsoft y cómo capacitar a tu equipo en la era de la IA generativa.

Microsoft