Microsoft

hypothesis

Índice de seguridad de datos

Tendencias, información y estrategias para proteger los datos

Prólogo

En una época marcada por la oleada de datos, cada vez está más claro que los datos de una organización son nada menos que su alma. La riqueza de los datos creados y utilizados por las organizaciones impulsa operaciones críticas, informa la toma de decisiones estratégicas y globales y da forma a las posibilidades de su futuro. Los datos no son un mero recurso: son el corazón palpitante de las empresas modernas.

Sin embargo, esta mayor dependencia de los datos viene acompañada de la cruda realidad de que las vulnerabilidades en las sombras digitales son reales y se expanden con rapidez. Las amenazas cibernéticas, las vulneraciones de datos y los incidentes de riesgo interno ya no son sucesos raros; son omnipresentes y van en aumento, lo que plantea riesgos para las organizaciones que dependen de los datos. De los responsables de la toma de decisiones que encuestamos hace poco, el 89 % afirmó que considera su postura en materia de seguridad de los datos fundamental para su éxito general.

En este informe, nos embarcamos en una exploración de ese imperativo fundamental: la protección de los datos de su organización. Mi equipo y yo estamos encantados de compartir nuestras conclusiones con ustedes, y esperamos iniciar un diálogo sobre cómo seguir impulsando colectivamente la seguridad de los datos hacia la excelencia. Nuestras conclusiones ejemplifican cómo la seguridad de los datos se encuentra en una coyuntura crítica: mientras que los responsables de la toma de decisiones en materia de seguridad coinciden en que es esencial para la seguridad de sus datos, y la mayoría afirma confiar en lo que está haciendo, al mismo tiempo están experimentando una plétora de incidentes y desafíos relacionados con la seguridad de los datos. Además, el 80 % de los líderes con los que hemos hablado reconocen que un enfoque integrado y óptimo es superior a las soluciones puntuales, pero la mayoría de las empresas siguen utilizando un sistema fragmentado de varias herramientas para proteger sus datos, lo que con frecuencia provoca más incidentes de seguridad en lugar de menos.

Lo invitamos a leer y compartir este último informe y a considerarlo el inicio de nuevas conversaciones con nuestros equipos sobre la mejor manera de ayudar a asegurar nuestro futuro colectivo.

Rudra Mitra
Vicepresidente corporativo
Seguridad de Datos y Cumplimiento de Microsoft

Introducción

La prevención de las vulneraciones de datos y otros incidentes de seguridad sigue siendo una preocupación constante para los responsables de la toma de decisiones en materia de seguridad y riesgos (y una piedra angular de cualquier programa de ciberseguridad), ya que una sola vulneración puede provocar importantes daños financieros y de reputación. Las organizaciones tienen la tarea de proteger una amplia gama de datos confidenciales, como información sobre empleados y clientes, propiedad intelectual, previsiones financieras y datos operativos.

Para conocer las prácticas y tendencias actuales en materia de seguridad de datos, así como identificar las oportunidades que tienen las organizaciones para mejorarla, Microsoft encargó a una agencia de investigación independiente, Hypothesis Group, la realización de una encuesta multinacional entre más de 800 profesionales de la seguridad de datos. Este informe presenta cinco conclusiones clave de la investigación: tendencias, ideas y estrategias para proteger los datos.

Hallazgos clave

1

Los responsables de la toma de decisiones creen que están protegidos, pero la realidad no coincide con las percepciones.

Aunque la mayoría de los responsables de la toma de decisiones afirman estar satisfechos y confiados con sus soluciones de seguridad de datos, siguen experimentando un promedio de 59 incidentes de seguridad de datos al año, con costosas repercusiones.

2

Disponer de más herramientas no significa mayor seguridad o eficacia de los datos, sino todo lo contrario.

El 80 % de los responsables de la toma de decisiones coincide en que las soluciones integrales e integradas son superiores a las soluciones manuales de primera clase, y sin embargo el enfoque de las organizaciones con respecto a las herramientas sigue siendo fragmentado, utilizando un promedio de más de 10 herramientas de seguridad de datos. Pero los que tienen más herramientas también sufren más incidentes relacionados con la seguridad de los datos, lo que sugiere que cuanto mayor es la proliferación de herramientas, más débil es la seguridad.

3

Las organizaciones siguen sufriendo el estrés de los incidentes de seguridad de datos externos e internos, sobre todo en los datos empresariales.

El 50 % de las organizaciones encuestadas han sufrido un ataque de ransomware o malware en el último año, y muchos responsables de la toma de decisiones no creen que su organización esté del todo preparada para prevenir y hacer frente a futuros ataques. A nivel interno, las personas malintencionadas son una de las principales preocupaciones. Además, las organizaciones están muy preocupadas por la vulnerabilidad de sus datos empresariales. Esto subraya una vez más la necesidad de una plataforma de seguridad que aborde los riesgos de forma integral.

Hallazgos clave

4

Las organizaciones necesitan la nube y la inteligencia artificial para impulsar la transformación digital, pero también son las ubicaciones de datos más vulnerables.

Las aplicaciones en la nube y la tecnología de inteligencia artificial se han vuelto fundamentales para la colaboración y la productividad de las organizaciones; sin embargo, esta evolución también ha creado riesgos más dinámicos y multifacéticos. A medida que las organizaciones adoptan la inteligencia artificial, resulta esencial mejorar la seguridad de los datos para permitir un uso responsable y seguro.

5

La automatización y la inteligencia artificial son vías prometedoras de mayor protección.

Las organizaciones quieren que sus equipos dediquen menos tiempo a la detección y más a la prevención. La automatización puede permitir a los equipos centrarse más en medidas proactivas, mientras que el uso de la inteligencia artificial para la seguridad de los datos ayuda a las organizaciones a ser más estratégicas y a ser más inteligentes sobre las amenazas futuras.

1

Los responsables de la toma de decisiones creen que están protegidos, pero la realidad no coincide con las percepciones.

Los responsables de la toma de decisiones creen que están protegidos, pero la realidad no coincide con las percepciones.

A primera vista, los responsables proyectan altos niveles de confianza y satisfacción con sus soluciones de seguridad de datos. La mayoría de las organizaciones coinciden en que sus controles de seguridad de datos bastan para evitar que se produzcan vulneraciones de datos, creen que saben dónde residen la mayoría de sus datos y que pueden detectar la mayoría de los riesgos en torno a ellos.

Al mismo tiempo, las organizaciones siguen experimentando un volumen considerable de incidentes relacionados con la seguridad de los datos: un promedio de 59 en los últimos 12 meses, de los cuales una quinta parte se consideran "graves". El impacto de estos incidentes es generalizado, ya que, en promedio, las organizaciones estiman que el costo financiero total de su incidente de seguridad de datos más grave ronda los USD 244 000, lo que significa que los incidentes anuales pueden costar hasta USD 15 millones. Además de estos costos, cuatro de cada diez responsables de la toma de decisiones también afirman que el costo operativo de recuperación tras un incidente de seguridad de datos y la pérdida de negocio por daños a la reputación son motivo de gran preocupación.

Además, el 92 % se enfrenta a desafíos, sobre todo en las áreas de costos, integración y tiempo de implementación, que inhiben su capacidad para seguir invirtiendo en seguridad de datos, lo que pone de manifiesto la necesidad de soluciones más económicas y eficientes en términos de mano de obra.

La percepción de confianza en la preparación para la seguridad de los datos difiere de la realidad de los incidentes que sufren las organizaciones. Aunque es importante que las organizaciones sepan dónde se encuentran los datos y detecten los riesgos, estas medidas individualmente, o por separado, no bastan para ayudar a las organizaciones a prevenir los incidentes que quitan el sueño a los responsables de la seguridad de los datos y los riesgos.

En palabras de un CISO (director de seguridad de la información) de servicios financieros: "No puedo decirle a la junta directiva 'aseguré los datos, pero no los protegí'... lo último que queremos es ver a nuestro banco incumpliendo en la portada del Wall Street Journal".

59

Número promedio de incidentes relacionados con la seguridad de los datos en los últimos 12 meses

HASTA USD 15 millones

Costo anual de un incidente grave de seguridad

2

Disponer de más herramientas no significa mayor seguridad o eficacia de los datos, sino todo lo contrario.

Disponer de más herramientas no significa mayor seguridad o eficacia de los datos, sino todo lo contrario.

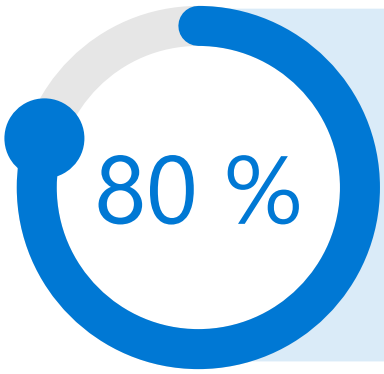
Las organizaciones se están dando cuenta de que años de enfoque basado en soluciones puntuales han creado brechas de visibilidad y eficacia debido a la existencia de herramientas de seguridad de datos aisladas. Esta tendencia está dando paso a un deseo de disponer de una solución integrada para la seguridad de los datos, ya que el 80 % coincide en que una plataforma global de seguridad de datos con soluciones integradas es superior al uso de varias soluciones de primer nivel que tienen que integrarse y administrarse de forma manual.

Sin embargo, aunque la gran mayoría considera superiores las soluciones integradas, la utilización de herramientas de seguridad de datos es prolífica y fragmentada.

En consecuencia, las organizaciones afirman utilizar un promedio de 10 herramientas de seguridad de datos para hacer frente a los riesgos de seguridad de datos, incluida la prevención de pérdida de datos, la protección de la información, la gestión de riesgos internos, la información de seguridad y administración de eventos (SIEM), el agente de seguridad de acceso a la nube, y mucho más. Para las organizaciones con más de 5000 empleados, el número promedio de herramientas es aún mayor.

Disponer de más herramientas puede estar creando una falsa sensación de seguridad, ya que los que utilizan más herramientas (más de 16) confían más en su postura de seguridad de los datos en comparación con los que utilizan menos herramientas (61 % frente a 56 %).

Sin embargo, la investigación contradice esa sensación de seguridad, ya que las organizaciones con 16 o más herramientas también experimentaron más incidentes de seguridad de datos en el último año (un promedio de 133), frente a los 48 incidentes de las organizaciones con menos herramientas.

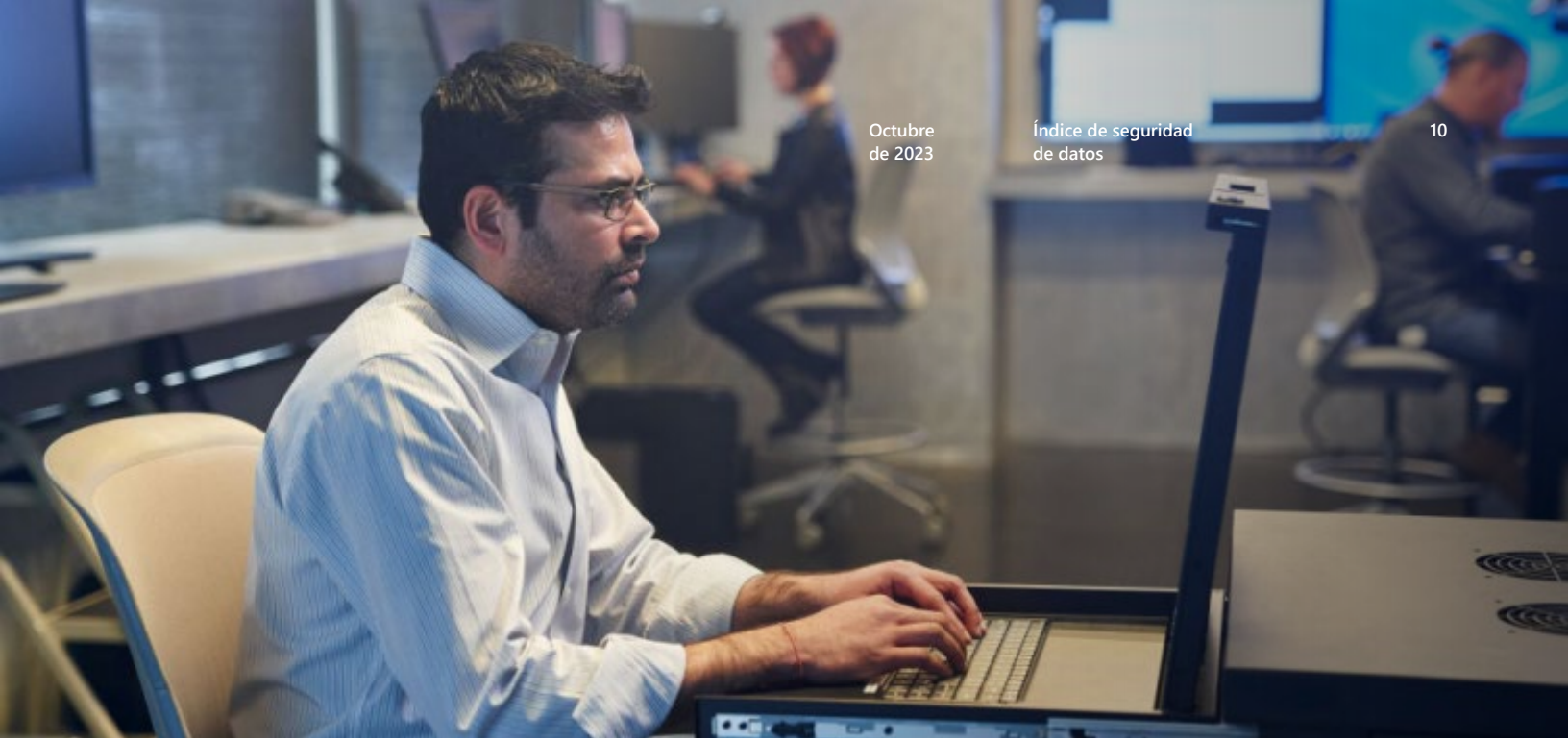


Está de acuerdo en que una plataforma de seguridad completa con soluciones integradas es superior al uso de varias soluciones de primer nivel que tienen que integrarse y administrarse de forma manual.

2,8 veces

Más incidentes de seguridad de datos en el último año

Para organizaciones con 16 o más herramientas (en comparación con organizaciones con menos herramientas)



Los argumentos a favor de una mayor seguridad de los datos mediante soluciones más integradas y menos herramientas cobran aún más fuerza cuando se observan los sentimientos y prácticas de quienes prefieren las mejores soluciones o más herramientas.

"¿Cómo se van a recopilar, agregar y utilizar los datos de un gran número de sistemas? Para que de verdad funcione, es necesario reunir muchos datos diferentes en un ecosistema. O si no, realmente tiene una versión defectuosa de la seguridad de los datos".

Vicepresidente de TI
Manufactura/Producción

En primer lugar, la existencia de múltiples herramientas de seguridad de datos dispares puede generar brechas de visibilidad y más datos en la sombra. De hecho, quienes están preocupados por los datos en la sombra son más propensos a preferir las mejores soluciones. Lo más probable es que esto se deba a que las organizaciones con un enfoque basado en lo mejor de lo mejor tienen que esforzarse más para obtener una visibilidad completa de su postura de seguridad de los datos.

En segundo lugar, la administración de soluciones en silos aporta más complejidad a los equipos de seguridad de datos, ya que cada solución dispar requiere personal dedicado, instalación y mantenimiento de agentes de punto de conexión y varios procesos nuevos. Tomemos como ejemplo la revisión y clasificación de alertas, una de las tareas que requieren personal y recursos. Un número cada vez mayor de alertas supone un esfuerzo adicional para los equipos de seguridad de datos a la hora de administrar soluciones aisladas. Las organizaciones con más herramientas reciben un promedio de 96 alertas de seguridad de datos al día, mientras que los equipos con menos herramientas reciben menos de la mitad de esa cantidad, con 44. Además, no son capaces de revisar tantas de estas alertas como los equipos con menos herramientas (61 %, frente al 68 %). Esto también suele dar lugar a que las organizaciones con más herramientas sean más reactivas en comparación con las organizaciones que utilizan un menor volumen de herramientas.

Por último, una mayor cantidad de herramientas también indica que las organizaciones tienen que realizar un gran esfuerzo para integrar los conocimientos y los planes de corrección, y la información puede perderse en el proceso. Cuando se les pregunta por los principales desafíos para la seguridad de los datos, el costo de implementación o mantenimiento de las soluciones de seguridad de datos y los desafíos de integración de las soluciones de seguridad de datos ocupan los dos primeros puestos.

Esto se traduce en procesos más largos y lentos, ya que el 37 % de los que utilizan 16 o más herramientas afirman necesitar un mes o más para completar una investigación de seguridad de datos, frente a solo el 21 % de los que utilizan menos herramientas.

"Ahora mismo, estamos gateando. Cada uno de los sistemas que disponemos tiene sus propios portales, sus propias herramientas, sus propias formas de hacer las cosas. Cada uno va por su lado, donde es el experto. Luego se vuelven a reunir todos y deciden qué está pasando, y a partir de ahí lo abordamos. Así que, en este momento, es un poco trabajo manual", declaró un director de Infraestructura y Operaciones en manufactura y producción.

En última instancia, al optar por continuar con varias soluciones, las organizaciones están pasando por alto su propio discurso de entender que las soluciones integradas son superiores y caminan en la dirección opuesta, lo que les cuesta tiempo y dinero.

RESULTADOS DE QUIENES UTILIZAN MENOS DE 16 FRENTE A MÁS DE 16 HERRAMIENTAS DE SEGURIDAD DE DATOS

	Bajo volumen de herramientas	Alto volumen de herramientas
Número de **incidentes relacionados con la seguridad** de los datos en los últimos 12 meses	**48**	**133**
Proporción de incidentes **graves** relacionados con la seguridad de los datos	19 %	26 %
Nuestra estrategia actual de seguridad de datos es más **reactiva**	31 %	40 %
El desafío de **integrar** soluciones	24 %	39 %
El equipo de seguridad de datos dedica más tiempo a la **respuesta**	19 %	26 %
Tenemos **confianza** en la seguridad de nuestros datos	56 %	61 %
Número promedio de alertas **recibidas** al día	44	96
Proporción de alertas que podemos **revisar** al día	68 %	61 %
Se necesita un mes o más para completar una investigación de seguridad de datos	21 %	37 %

3

Las organizaciones siguen sufriendo el estrés de los incidentes de seguridad de datos externos e internos, sobre todo en los datos empresariales.

Las organizaciones siguen sufriendo el estrés de los incidentes de seguridad de datos externos e internos, sobre todo en los datos empresariales.

Dado que los factores que rodean a los datos, incluidas las personas que interactúan con ellos, las actividades en torno a los datos y los dispositivos y aplicaciones utilizados para procesarlos, evolucionan de forma constante, los incidentes de seguridad y las vulneraciones de datos pueden producirse en cualquier momento y lugar. Y estas amenazas proceden tanto de atacantes externos como de personal de confianza, incluidos empleados, contratistas y socios. Ya sea de forma malintencionada o involuntaria, todos los actores pueden provocar incidentes de seguridad de los datos, lo que significa que existe una necesidad constante de protección en multitud de ámbitos.

Un vicepresidente de TI en Servicios Financieros señaló: "Lo que se intenta proteger cambia constantemente. Es un blanco móvil. Siempre va a evolucionar, cambiar y ser flexible. Lo que está protegiendo y dónde reside solo va a ser más variado".

Aunque los incidentes relacionados con la seguridad de los datos pueden provenir de diversas fuentes, la amenaza externa de los incidentes de malware o ransomware (casos en los que un software malintencionado se infiltra en un sistema y concede acceso a los atacantes no autorizados a sistemas o redes) son, con diferencia, los más comunes, ya que el 50 % de las organizaciones encuestadas han experimentado al menos uno en el último año.

Además, en estos ataques es donde las organizaciones se sienten más vulnerables, ya que el 41 % afirma sentirse menos preparado para hacer frente a futuros ataques de malware o ransomware en el próximo año. Esta sensación de vulnerabilidad es aún mayor entre los que prefieren un enfoque de primera clase: el 44 % no se siente preparado para un ataque de esta naturaleza, frente a solo el 36 % de los que prefieren una solución integrada.

Los responsables de la toma de decisiones también tienen muy presente la seguridad y la prevención de los riesgos internos. El 35 % afirma que necesita reforzar las defensas contra los intrusos malintencionados y las cuentas comprometidas, y un tercio está preocupado por los incidentes con intrusos inadvertidos. Aunque los incidentes con información privilegiada malintencionada no sean la causa principal de las vulneraciones de la seguridad de los datos, son el segundo tipo más común de incidente que los responsables de la toma de decisiones se sienten menos preparados para prevenir.

"Al menos una vez al mes, recibo una llamada de un director aterrorizado... 'tuvimos un evento, descubrí un evento, o el equipo de amenazas descubrió un evento'. Algunos son involuntarios, otros son personas que no saben o no entienden lo que permiten sus privilegios".

CISO del gobierno de los EE. UU.

Los ataques internos son de personas de confianza a las que normalmente se les ha concedido acceso o que poseen conocimientos sobre recursos, datos o sistemas de la empresa que no están disponibles para el público en general. En consecuencia, los riesgos para la seguridad de los datos asociados a las personas con acceso a información privilegiada tienden a ser más elusivos y difíciles de detectar. Como indicó Bret Arsenault, CISO de Microsoft, "en última instancia, no importa si la brecha fue intencionada o accidental. Los programas de riesgos internos deben formar parte de la estrategia de seguridad de toda empresa".

RESUMEN DE INCIDENTES DE SEGURIDAD DE DATOS

Causas de los incidentes de seguridad de datos	Incidentes más frecuentes en los últimos 12 meses	Menos preparados para prevenir en los próximos 12 meses
Malware o ransomware	**50 %**	**41 %**
Cuentas atacadas	**38 %**	**35 %**
Ataques de denegación de servicio (DoS)	**35 %**	**33 %**
Ataques internos por negligencia	**32 %**	**29 %**
Ataques internos involuntarios	**31 %**	**32 %**
Ataques internos malintencionados	**31 %**	**35 %**
Propiedad física	**29 %**	**29 %**

Las soluciones de seguridad de datos que eligen las organizaciones también tienen que funcionar para una variedad de datos confidenciales, incluidos los datos empresariales de alto valor, los datos operativos y los datos personales. Durante los incidentes de seguridad de datos de los últimos 12 meses, el 74 % de las organizaciones han visto expuestos datos empresariales, el 65 % han visto comprometidos datos operativos y el 58 % han experimentado la vulnerabilidad de datos personales. Entre los distintos tipos de datos, la propiedad intelectual, el diseño informático y de redes, y la información personal han sido los que más a menudo se han visto comprometidos o expuestos.

De cara al futuro, el 77 % de las organizaciones considera que los datos empresariales, como la propiedad intelectual y el código fuente, son los más vulnerables. Esto se debe principalmente a que los datos empresariales desempeñan un papel crítico a la hora de determinar ventajas competitivas y generar ingresos. Sin embargo, identificar y clasificar este tipo de datos puede suponer un desafío, ya que la tecnología tradicional de reconocimiento de patrones, expresiones regulares o coincidencias de funciones puede no identificar con eficacia los contenidos que carecen de formatos de cadena o palabras clave específicos. A su vez, las organizaciones requieren tecnologías más avanzadas para ayudar a descubrir y proteger esos datos confidenciales vulnerables.

TIPOS DE DATOS CON MAYOR RIESGO EN LOS PRÓXIMOS 12 MESES

77 % **Datos empresariales**		64 % **Datos operativos**		63 % **Datos personales**	
Propiedad intelectual	**30 %**	TI y diseño de redes	**29 %**	Información de identificación personal (PII)	**31 %**
Código de origen	**28 %**	Estados financieros	**18 %**	Información sobre recursos humanos (nóminas, currículum, etc.)	**21 %**
Planes de negocios	**27 %**	Informes de ventas e ingresos	**15 %**	Datos del sector de las tarjetas de pago (PCI)	**18 %**
Secretos comerciales	**24 %**	Adquisiciones y facturación	**12 %**	Información de salud protegida (PHI)	**18 %**
Archivos de fusiones y adquisiciones	**20 %**	Documentos/ acuerdos legales	**12 %**	Credenciales	**17 %**
Especificaciones de construcción	**18 %**	Procesos de manufactura/ archivos por lotes	**11 %**		

4

Las organizaciones necesitan la nube y la inteligencia artificial para impulsar la transformación digital, pero también son las ubicaciones de datos más vulnerables.

Las organizaciones necesitan la nube y la inteligencia artificial para impulsar la transformación digital, pero también son las ubicaciones de datos más vulnerables.

La colaboración a través de aplicaciones y plataformas en la nube, combinada con la nueva tecnología de inteligencia artificial, mejora de forma considerable la productividad de los empleados y permite acuerdos de trabajo flexibles, lo que hace que las aplicaciones en la nube y la tecnología de inteligencia artificial sean esenciales para las organizaciones. En promedio, las organizaciones utilizan ahora 147 servicios de nube pública que abarcan SaaS, PaaS e IaaS.[1] Además, el 66 % de las organizaciones han desarrollado una estrategia de inteligencia artificial, y el 36 % ya la están aplicando.[2] Sin embargo, esta evolución ha generado riesgos más dinámicos y polifacéticos, debido a la dificultad de definir con claridad los límites de los datos en diversos entornos.

1. Measuring Risk and Risk Governance, Cloud Security Alliance (CSA), 2022
2. Microsoft data security AI research, Hypothesis, marzo de 2023

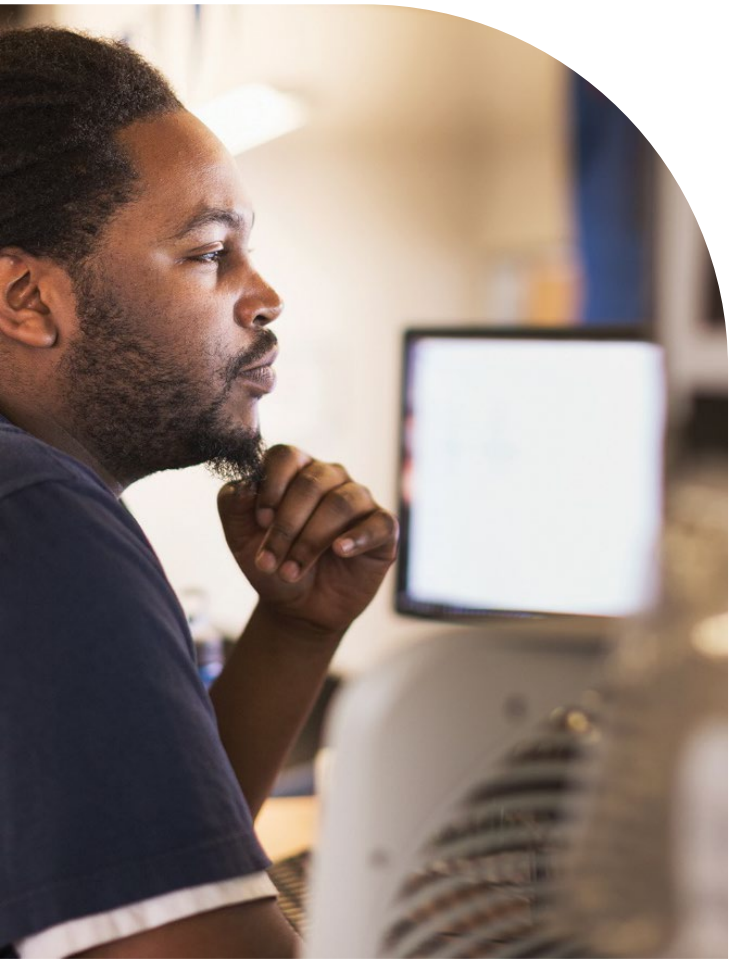
Ahora es aún más crítico contar con la solución de seguridad de datos correcta para estas ubicaciones de datos de alta productividad. En los últimos 12 meses, el 42 % de las organizaciones notificaron incidentes de seguridad en el almacenamiento en la nube y el 31 % en correos electrónicos, mensajería instantánea o herramientas de reunión en línea. Los incidentes parecen ser más frecuentes allí donde hay más productividad y colaboración.

La gestión de este tipo de incidentes requiere recursos, y el 79 % de las organizaciones afirman que su equipo de seguridad de datos necesita más personal para administrar con eficacia las responsabilidades cruciales en materia de seguridad de datos. Sin embargo, entre las organizaciones que afirman necesitar más personal, la mayoría (57 %) prefiere un planteamiento de "mejor en su clase". Esta preferencia pone de manifiesto que las organizaciones que utilizan más soluciones pueden tener más dificultades para identificar los verdaderos riesgos entre la infinidad de actividades de los usuarios.

RESUMEN DE UBICACIONES DE DATOS

Ubicaciones de los datos	Atacadas en los últimos 12 meses	Mayor riesgo
Almacenamiento en la nube (por ejemplo, Box, OneDrive, Google Drive)	42 %	54 %
Correos electrónicos/mensajería instantánea/herramientas de reuniones en línea	31 %	39 %
Plataforma como servicio (PaaS)	29 %	34 %
Infraestructura como servicio (IaaS)	28 %	36 %
IA (por ejemplo, ChatGPT, Bard, etc.)	27 %	38 %
Bases de datos/lagos de datos basados en SaaS	27 %	41 %
Puntos de conexión/dispositivos	25 %	36 %
Repositorios locales/recursos compartidos de archivos/bases de datos	24 %	28 %
Datos de sombra	21 %	23 %
Aplicaciones de línea de negocio	17 %	25 %
Herramientas para desarrolladores	16 %	23 %

Con más de un tercio de las organizaciones que implementan estrategias de inteligencia artificial, y muchas más en camino, la inteligencia artificial se está adoptando a un ritmo sin precedentes, mucho más rápido que la adopción de la nube y el correo electrónico en el pasado. A medida que las organizaciones adoptan la inteligencia artificial, resulta esencial mejorar la seguridad de los datos para permitir un uso responsable y evitar los riesgos. La inteligencia artificial se considera una ubicación de alto riesgo para los incidentes de seguridad de datos, en comparación con otras ubicaciones, y el 27 % de las organizaciones han experimentado una infracción de la seguridad de los datos de inteligencia artificial. Las preocupaciones de las organizaciones en torno a los riesgos del uso de la inteligencia artificial se enfocan en la falta de control sobre los datos compartidos con la inteligencia artificial, la falta de controles para detectar y mitigar el uso arriesgado de la inteligencia artificial, la falta de transparencia sobre cómo se entrenan los modelos generativos de inteligencia artificial y la filtración de información confidencial a través de la inteligencia artificial.



"La inteligencia artificial es buena para la productividad y la eficiencia, pero presenta riesgos potenciales para la seguridad y los datos".

Aunque existen preocupaciones en torno a la inteligencia artificial, los responsables de la toma de decisiones también pueden ver el potencial, sobre todo porque los proveedores del mercado están desarrollando innovaciones para ayudar a potenciar a las empresas mediante el uso responsable de la inteligencia artificial. Sin embargo, para utilizar mejor la inteligencia artificial, las organizaciones informan que los principales controles que requieren son detectar contenidos malintencionados o de riesgo en la inteligencia artificial, cifrar, enmascarar o anonimizar datos antes de que puedan cargarse en la inteligencia artificial e identificar los datos sensibles generados por la inteligencia artificial.

CINCO CONTROLES DE SEGURIDAD DE DATOS NECESARIOS PARA LA INTELIGENCIA ARTIFICIAL

1	**Detectar contenidos malintencionados o de riesgo** en la inteligencia artificial
2	**Cifrar, enmascarar o anonimizar los datos** antes de cargarlos en la inteligencia artificial
3	**Identificar los datos confidenciales** generados por la inteligencia artificial
4	**Evitar que los datos confidenciales se carguen** en la inteligencia artificial
5	**Detectar la manipulación de los datos** o del modelo en la inteligencia artificial

5

La automatización y la inteligencia artificial son vías prometedoras de mayor protección.

La automatización y la inteligencia artificial son vías prometedoras de mayor protección.

En un mundo ideal, sin limitaciones basadas en las prioridades o el presupuesto de la organización, a la mitad de las organizaciones les gustaría ser más proactivas en la administración de la seguridad de los datos, dedicando más tiempo a aspectos como el descubrimiento de datos confidenciales y los riesgos asociados en torno a ellos y la prevención de incidentes de seguridad de los datos. Sin embargo, en la actualidad, más de la mitad de las organizaciones dedican la mayor parte de su tiempo a medidas reactivas, como la detección de incidentes, la respuesta y las investigaciones. Y esta detección y respuesta ante los incidentes de seguridad de los datos requiere mucho tiempo: la mayoría de las organizaciones demoran alrededor de un mes en resolver un incidente de seguridad de los datos y, para algunas, la resolución puede llevar hasta seis meses.

El beneficio de adoptar una estrategia más proactiva es patente, ya que las organizaciones encuestadas que son más proactivas ya experimentan incidentes de seguridad de datos menos costosos, es más probable que puedan investigar esos incidentes en menos de un mes y es más probable que crean que sus controles de defensa son suficientes para prevenir las vulneraciones de datos.

Aunque las organizaciones son conscientes de que las medidas proactivas de seguridad de los datos pueden ayudar a reducir los riesgos para la seguridad de los datos, no están avanzando en la aplicación de esas medidas. Por ejemplo, las que buscan ser más proactivas asignando más tiempo a la prevención son más propensas a elegir las mejores soluciones, que en realidad exigen mayores esfuerzos en el manejo de medidas reactivas al reunir señales de detección y controles de respuesta.

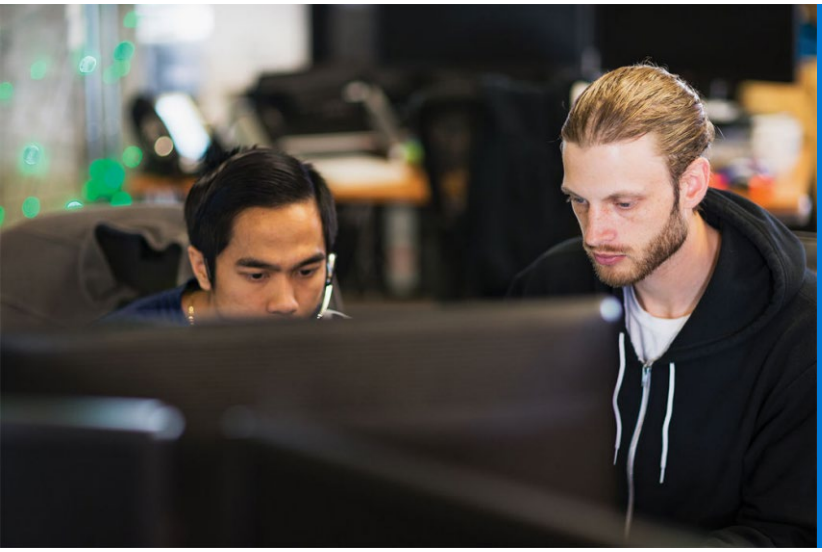
RESULTADOS DE LAS ORGANIZACIONES MÁS PROACTIVAS FRENTE A LAS MÁS REACTIVAS

	Más proactivas	Más reactivas
Costo promedio de un incidente de seguridad de datos en los últimos 12 meses	**USD 207 000**	**USD 330 000**
Completar una investigación de seguridad de datos en menos de un mes en promedio	**80 %**	**68 %**
Nuestros controles de defensa son suficientes para prevenir las vulneraciones de datos	**77 %**	**68 %**

Dado que los recursos y el personal son limitados y la distribución del esfuerzo entre actividades puede no ser la ideal, las organizaciones buscan tecnología que les ayude a reservar más tiempo para actividades proactivas. La automatización es una forma de que las organizaciones dediquen tiempo a un enfoque más proactivo de la seguridad de los datos. El 74 % de las organizaciones encuestadas preferiría una mitigación de riesgos semiautomatizada o totalmente automatizada, lo que permite a los equipos de seguridad minimizar el impacto de posibles incidentes de seguridad de datos con antelación respecto a las revisiones manuales. Además, las organizaciones reconocen muchas otras tareas que podrían beneficiarse de la automatización, como la creación de informes de seguridad de datos, la automatización del flujo de trabajo de administración de incidentes y la respuesta e investigación de incidentes. La mayoría de las principales tareas que los equipos de seguridad quieren automatizar son medidas reactivas. Al automatizar estas tareas, las organizaciones pueden aliviar la carga de sus equipos de seguridad de datos, permitiéndoles adoptar una postura más proactiva.

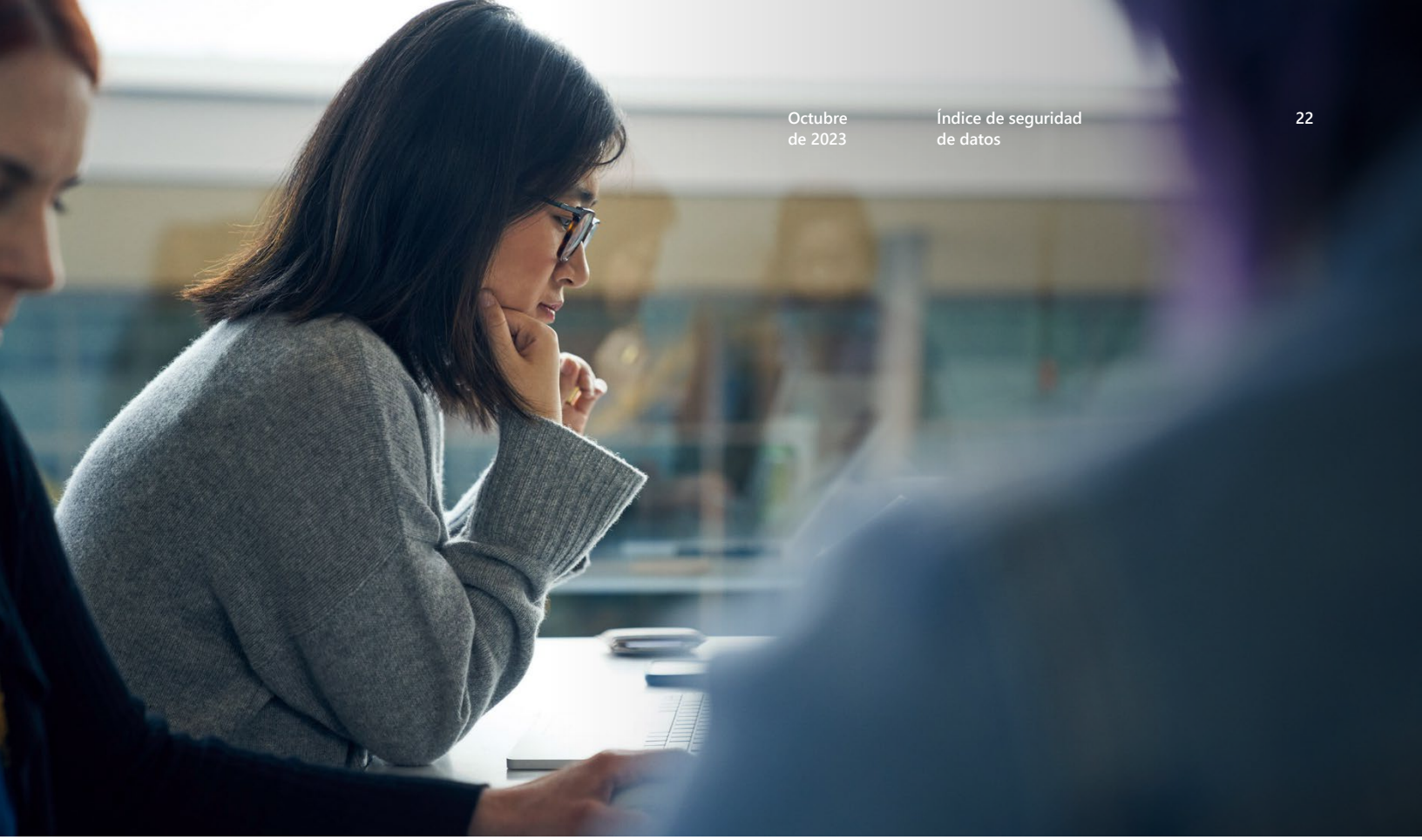
LAS CINCO ÁREAS PRINCIPALES QUE LOS EQUIPOS DE SEGURIDAD DE DATOS PREFIEREN AUTOMATIZAR/ALIVIAR

Reactiva	1	Creación de flujos de trabajo automatizados para la administración y respuesta ante incidentes
	2	Creación de informes de seguridad de datos
Reactiva	3	Respuesta y contención de incidentes de seguridad de los datos
	4	Enrutamiento de los incidentes a los equipos correctos (por ejemplo, SOC, jurídico, RR. HH.) durante las investigaciones.
	5	Investigación de los incidentes de seguridad de datos



"Hay muchos datos arriesgados que evaluar de forma manual. La inteligencia artificial puede ayudar a acelerar los tiempos de respuesta de nuestro equipo y a proteger los datos, ya que carecemos de recursos suficientes".

Responsable de la toma de decisiones sobre seguridad de Reino Unido



El uso de la inteligencia artificial para la seguridad de los datos también puede ayudar a las organizaciones a ser más estratégicas y más inteligentes ante futuras amenazas. La tecnología acelera la respuesta ante los incidentes detectados, lo que permite a los profesionales de la seguridad de datos ganar tiempo para investigar más a fondo. De forma similar a la automatización, las organizaciones citan muchos escenarios en los que la inteligencia artificial puede ayudar a proporcionar una seguridad más sólida, **ahorrando así tiempo a su equipo.** Los principales escenarios para el uso de la inteligencia artificial incluyen el bloqueo automático del intercambio incorrecto de datos, la detección de riesgos críticos para la seguridad de los datos/actividades anómalas con los datos y la investigación de posibles incidentes de seguridad de los datos.

Al aprovechar las ventajas de la inteligencia artificial y la automatización y avanzar hacia soluciones más integradas, las organizaciones pueden adoptar una estrategia de seguridad de datos más proactiva y prepararse para un futuro más seguro.

PRINCIPALES ESCENARIOS DONDE SE UTILIZA LA INTELIGENCIA ARTIFICIAL

Bloquear automáticamente el intercambio inadecuado de datos

Detectar riesgos críticos para la seguridad de los datos/ actividades anómalas en los datos

Recomendaciones para proteger mejor su entorno de datos

Investigar posibles incidentes relacionados con la seguridad de los datos

Ajustar las directivas de seguridad de datos

Recomendaciones finales

- Adopte una plataforma integrada para reforzar la seguridad de los datos
- Protéjase contra los incidentes relacionados con la seguridad de los datos, tanto desde el exterior como desde el interior, con un enfoque de defensa en profundidad
- Actualice sus estrategias de seguridad de datos con inteligencia artificial y automatización

Adopte una plataforma integrada para reforzar la seguridad de los datos

Según las conclusiones de esta investigación, menos soluciones pueden aportar más seguridad. Puede parecer contraintuitivo, pero las organizaciones tienen que combatir la falsa sensación de confianza que surge de una multitud de soluciones aisladas. La consolidación de proveedores ofrece un enfoque estratégico que no solo reduce los costos, sino que también mejora la seguridad.

Los responsables de la seguridad de los datos pueden iniciar esta transformación permitiendo a sus equipos dedicar más tiempo al trabajo estratégico, como la investigación y planificación de nuevos controles de seguridad y la optimización de las directivas de seguridad, algo que el 84 % de los responsables coinciden en que quieren hacer. Este proceso implica el reemplazo de las antiguas soluciones aisladas, que a menudo se consideran "las mejores de su clase" pero no se integran con eficacia con otras herramientas.

Los responsables de la toma de decisiones pueden fomentar una estrecha colaboración con sus equipos para establecer los objetivos del programa de seguridad de datos y los indicadores clave de rendimiento (KPI). A continuación, pueden avanzar al definir los requisitos de la solución e identificar las características no negociables. Este enfoque les permite identificar a los proveedores capaces de ofrecer herramientas que se ajusten a sus objetivos generales. Y lo que es más importante, fomenta una mentalidad orientada al futuro y ayuda a los equipos a evitar obsesionarse demasiado con las prácticas existentes o los casos de uso aislados, permitiéndoles aplicar los cambios necesarios hacia un enfoque más integrado.

Una plataforma integrada de seguridad de datos debería permitir a los equipos de seguridad realizar todas estas tareas críticas sin problemas:

1. Descubrir y proteger los datos confidenciales en su entorno digital.
2. Detectar riesgos críticos asociados con estos datos.
3. Evitar el uso no autorizado de datos confidenciales sin afectar a las actividades empresariales legítimas.

Mediante la aplicación de una estrategia integrada de seguridad de datos, las organizaciones pueden alcanzar un mayor nivel de protección y, al mismo tiempo, simplificar su infraestructura de seguridad.

Protéjase contra los incidentes relacionados con la seguridad de los datos, tanto desde el exterior como desde el interior, con un enfoque de defensa en profundidad

Los incidentes relacionados con la seguridad de los datos suelen deberse a atacantes externos, personas malintencionadas o inadvertidas. Las organizaciones tienen que tomar medidas para proteger sus datos, tanto impidiendo el acceso no autorizado de amenazas externas como mitigando el riesgo de robo interno o exposición accidental de datos.

Para hacer frente a estos desafíos, las organizaciones pueden adoptar un enfoque de defensa en profundidad de la seguridad de los datos. Esta estrategia es similar a la protección de obras de arte de valor incalculable en un museo: cámaras de seguridad de última generación equipadas con inteligencia sobre amenazas controlan a los visitantes, los sistemas de venta de entradas administran la identidad y el acceso al museo, y las estrictas medidas de seguridad en torno a las obras de arte funcionan del mismo modo a los controles de seguridad de datos que protegen sus valiosos datos. Estas medidas disuaden de posibles incidentes, tanto si proceden de malos actores externos como de individuos que ya se encuentran en el entorno de la organización.

Combatir la evolución de los riesgos para la seguridad de los datos exige un esfuerzo concertado en toda la organización para aplicar esta estrategia de defensa en profundidad. La colaboración del equipo de seguridad de datos con otros departamentos, como el Centro de Operaciones de Seguridad (SOC), puede optimizar la inversión en seguridad de datos. En especial, el 66 % de las organizaciones que se consideran proactivas interactúan con su equipo SOC, frente al 54 % que no lo hacen.

Al igual que el trabajo en equipo de los equipos de seguridad, las soluciones de seguridad de datos también tienen que integrarse a la perfección con otros sistemas, como las soluciones de detección y respuesta ampliadas (XDR) o de administración de identidades y accesos (IAM), para prevenir con eficacia los incidentes de seguridad de datos procedentes tanto de fuentes externas como internas. Estas integraciones permiten a las organizaciones llevar a cabo investigaciones y respuestas exhaustivas a los incidentes de seguridad, con lo que obtienen un conocimiento profundo de los datos, actores y actividades afectados, y responden con diversos controles de mitigación. En consecuencia, esto les permite dar respuestas informadas, precisas y rápidas para minimizar el impacto de posibles incidentes de seguridad.

Actualice sus estrategias de seguridad de datos con inteligencia artificial y automatización

La automatización y la inteligencia artificial pueden ayudar a las organizaciones a ser más proactivas en la seguridad de los datos. Estas son algunas recomendaciones para que su organización se embarque en el recorrido de la automatización y la inteligencia artificial:

- Descubrir los datos confidenciales: Utilice la inteligencia artificial para ayudar a identificar los datos confidenciales y aplicar directivas de protección, incluidos el cifrado y la gestión de derechos. Esto es especialmente valioso para los datos empresariales que pueden plantear problemas de detección mediante las tecnologías tradicionales de reconocimiento de patrones. Las organizaciones pueden aprovechar la tecnología de clasificación, como el machine learning o los clasificadores con tecnología de IA, conocidos por su inteligencia y capacidad para localizar con rapidez contenido confidencial en función del contexto de los datos o la categoría empresarial. Alternativamente, las organizaciones pueden emplear tecnología de correspondencia exacta de datos para descubrir datos operativos o personales.

  Además, a medida que evolucionan las normativas del sector (por ejemplo, RGPD, HIPAA o PCI DSS) y el panorama de los datos se vuelve más dinámico, es fundamental contar con una tecnología de clasificación avanzada que sea personalizable y se pueda adaptar con facilidad para identificar nuevas categorías de datos confidenciales.

- Detectar los riesgos críticos para la seguridad de los datos: Aproveche el poder de la inteligencia artificial para identificar los riesgos críticos asociados a sus datos confidenciales y asigne recursos de manera estratégica para hacer frente a posibles incidentes de alto riesgo. Las tecnologías de inteligencia artificial pueden generar alertas de alta fidelidad, lo que permite a los equipos de seguridad ahorrar un tiempo valioso que, de otro modo, se emplearía en cribar una gran cantidad de falsas alertas positivas. Además, la inteligencia artificial puede ayudar a las organizaciones a identificar riesgos elusivos, sobre todo cuando los actores malintencionados intentan eludir la detección. Es indispensable utilizar la velocidad de las máquinas para superar a estos actores de amenazas.

- Prevenir incidentes de seguridad de datos de forma dinámica: Utilice la inteligencia artificial y la automatización para adaptar de forma automática sus controles de prevención y mitigación en función de los riesgos evaluados, lo que permite una estrategia de seguridad de datos más adaptable y proactiva. Cuando las soluciones basadas en inteligencia artificial detectan y evalúan los riesgos, los controles de prevención automatizados pueden intervenir con rapidez para proteger los datos, aplicando controles de mitigación precisamente a las áreas de alto riesgo. Por ejemplo, en los casos en los que los usuarios de alto riesgo detectan indicadores tempranos de intento de filtración de datos, las organizaciones pueden aplicar directivas de prevención de pérdida de datos (DLP) más estrictas, con lo que se adelantan de forma proactiva a posibles incidentes de seguridad de datos.

Esperamos que las ideas y recomendaciones de este informe le resulten útiles para mejorar la seguridad de sus datos y fortalecer su organización frente a los riesgos cambiantes.

Para obtener más información sobre la seguridad de los datos de Microsoft, visite https://aka.ms/DataSecurityNews

Objetivos detallados de la investigación, metodología y reclutamiento de público

Los objetivos de la investigación eran:

1. Comprender el panorama de la seguridad de los datos, incluidas las prioridades, las mentalidades y los desafíos
2. Determinar la causa y el efecto de los incidentes de seguridad de los datos e identificar las medidas que los equipos de seguridad de datos pueden adoptar para mejorar la postura de seguridad de los datos
3. Explorar el futuro de la seguridad de los datos, incluidas las estrategias e innovaciones emergentes en torno al uso de la inteligencia artificial para la seguridad de los datos

La metodología fue:

Del 28 de julio al 9 de agosto de 2023 se llevó a cabo una encuesta multinacional en línea de 15 minutos de duración entre 822 responsables de la toma de decisiones en materia de seguridad de datos.

Las preguntas giraron en torno al panorama de la seguridad de los datos, cómo asignan sus recursos los equipos de seguridad de datos, los incidentes de seguridad de datos y las actitudes y el uso de la inteligencia artificial (IA) para la seguridad de los datos.

Para cumplir con los criterios de evaluación, los responsables de la toma de decisiones sobre seguridad debían:

Ser CISO y responsables de la toma de decisiones adyacentes (nivel ejecutivo y superior) con competencia sobre la seguridad de los datos

Trabajar en organizaciones empresariales (más de 500 empleados; rango de tamaños)

Pertenecer a una combinación de industrias reguladas y no reguladas (no de educación, gobierno ni sin fines de lucro)

De los 822 responsables de la toma de decisiones en materia de seguridad de datos encuestados para la investigación, los más completos por país fueron:

Estados Unidos	329
Reino Unido	322
Australia	171