Microsoft

hypothesis

Índice de seguridad de los datos

Tendencias, conocimientos y estrategias para proteger los datos

Prólogo

En una época definida por oleadas de datos, cada vez es más evidente que los datos de una organización no son otra cosa que su alma. La riqueza de los datos que crean y usan las organizaciones impulsa las operaciones críticas, permite la toma de decisiones estratégicas y globales y da forma a las posibilidades para su futuro. Los datos no son simplemente un recurso: son el corazón de la empresa moderna.

Sin embargo, con esta mayor dependencia de los datos llega la clara realidad de que las vulnerabilidades en las sombras digitales son reales y se expanden rápidamente. Las ciberamenazas, las filtraciones de datos y los incidentes con información privilegiada ya no son casos raros; son omnipresentes y cada vez más importantes, lo que representa un riesgo para las organizaciones que dependen de los datos. De los responsables de la toma de decisiones que encuestamos recientemente, el 89 % afirmó que considera el enfoque de seguridad de los datos un aspecto básico del éxito general.

En este informe técnico, nos embarcamos en una exploración de ese imperativo fundamental: la protección de los datos de tu organización. Mi equipo y yo estamos encantados de compartir contigo nuestros hallazgos y espero que iniciemos un diálogo sobre cómo seguir impulsando la seguridad de los datos colectivamente hacia la excelencia. Nuestro aprendizaje ejemplifica cómo la seguridad de los datos se encuentra en una coyuntura crítica: mientras que los responsables de la toma de decisiones de seguridad coinciden en que es esencial la seguridad de los datos y la mayoría dice estar seguro de lo que está haciendo, simultáneamente están experimentando un gran número de incidentes y desafíos en relación con la seguridad de los datos. Además, el 80 % de los líderes con los que hablamos reconoce que un enfoque integrado optimizado es superior a las soluciones puntuales, pero la mayoría de las empresas sigue utilizando un sistema fragmentado de múltiples herramientas para proteger los datos, lo que a menudo da lugar a más incidentes de seguridad en lugar de reducirlos.

Estamos encantados de que leas y compartas este último informe. Considéralo como el comienzo de nuevas conversaciones con nuestros equipos sobre cómo podemos ayudar a proteger nuestro futuro colectivo.

Rudra Mitra
Vicepresidente corporativo
Seguridad de datos y cumplimiento de Microsoft

Presentación

La prevención de filtraciones y otros incidentes de seguridad de los datos sigue siendo una preocupación constante para los responsables de la seguridad y la toma de decisiones de riesgos, así como un pilar de cualquier programa de ciberseguridad, porque una sola infracción puede causar daños económicos y de reputación importantes. Las organizaciones deben proteger una amplia gama de datos confidenciales, incluida la información de empleados y clientes, propiedad intelectual, previsiones financieras y datos operativos.

Para comprender las prácticas y tendencias actuales de seguridad de los datos, así como identificar oportunidades para que las organizaciones mejoren la seguridad de los datos, Microsoft encargó a una agencia de investigación independiente, Hypothesis Group, una encuesta multinacional entre más de 800 profesionales de la seguridad de datos. Este informe presenta cinco conclusiones clave del estudio, incluidas tendencias, conocimientos y estrategias para proteger los datos.

Conclusiones principales

1

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

Aunque la mayoría de los responsables de la toma de decisiones afirma que están satisfechos y confiados con sus soluciones de seguridad de datos, siguen experimentando un promedio de 59 incidentes de seguridad de datos al año, con impactos costosos.

2

Tener más herramientas no implica una mayor seguridad o eficiencia de los datos, sino todo lo contrario.

El 80 % de los responsables de la toma de decisiones coincide en que las soluciones completas e integradas son superiores a las soluciones manuales de gama más alta y, sin embargo, el enfoque de las organizaciones con respecto a las herramientas sigue estando fragmentado, utilizando un promedio de más de 10 herramientas de seguridad de datos. Con todo, las personas que tienen más herramientas también experimentan más incidentes de seguridad de datos, lo que sugiere que cuanto mayor es la proliferación de herramientas, más débil es la seguridad.

3

La lacra de las organizaciones sigue siendo la presión de los incidentes de seguridad de datos externos e internos, especialmente en lo que afecta a los datos empresariales.

El 50 % de las organizaciones encuestadas ha 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 totalmente preparada para prevenir y abordar los ataques futuros. Dentro, el uso de información privilegiada de forma malintencionada es una de las principales preocupaciones. Además, a las organizaciones les preocupa mucho la vulnerabilidad de sus datos empresariales. De nuevo, esto hace hincapié en la necesidad de una plataforma de seguridad que afronte los riesgos de forma integral.

Conclusiones principales

4

Las organizaciones necesitan el cloud y la IA para impulsar la transformación digital, pero también son las ubicaciones de datos más vulnerables.

Las aplicaciones en el cloud y la tecnología de IA se han vuelto esenciales para la colaboración y la productividad de las organizaciones; sin embargo, esta evolución también ha creado riesgos más dinámicos y polifacéticos. A medida que las organizaciones adoptan la IA, se vuelve fundamental mejorar la seguridad de los datos para permitir un uso responsable y seguro.

5

La automatización y la IA son mecanismos prometedores para una mayor protección.

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

1

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

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

Sobre la base de que los responsables de la toma de decisiones proyectan altos niveles de confianza y satisfacción con sus soluciones de seguridad de los datos, la mayoría de las organizaciones coincide en que sus controles de seguridad de datos son suficientes para evitar que estos se vulneren, sienten que saben dónde reside 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 importante de incidentes de seguridad de datos, una media de 59 en los 12 últimos meses, y una quinta parte de ellos se considera "grave". El impacto de estos incidentes está generalizado, ya que, de media, las organizaciones calculan que el coste financiero total de su incidente de seguridad de datos más grave ronda los 244 000 USD, lo que significa que los incidentes anuales pueden costar hasta 15 millones USD. Además de estos costes, cuatro de cada 10 responsables de la toma de decisiones también afirman que el coste operativo de recuperarse ante un incidente de seguridad de datos y la pérdida de negocio por daños a la reputación es una gran preocupación.

Además, el 92 % se enfrenta a desafíos, principalmente en las áreas de costes, integración y tiempo de implementación, que impiden que sigan invirtiendo en seguridad de datos, subrayando la necesidad de soluciones más económicas y eficientes para el personal.

La percepción de confianza en la disposición de seguridad de los datos difiere de la realidad de los incidentes que están experimentando las organizaciones. A pesar de que es importante que las organizaciones sepan dónde se encuentran los datos y detecten riesgos, estas medidas individuales o por separado no son suficientes para ayudar a las organizaciones a prevenir los incidentes que mantienen alerta a los responsables de la seguridad de los datos y de la toma de decisiones de riesgos.

Como dice un director de seguridad de la información (CISO) de servicios financieros: "No puedo decirle a mi junta directiva 'los datos estaban seguros, pero simplemente no los protegí'... lo último que queremos ver es la noticia de que nuestro banco no ha cumplido en la primera página del Wall Street Journal".

59

Número medio de incidentes de seguridad de datos en los 12 últimos meses

HASTA

15 mill. USD

Coste anual de un incidente de seguridad grave

2

Tener más herramientas no implica una mayor seguridad o eficiencia de los datos, sino todo lo contrario.

Tener más herramientas no implica una mayor seguridad o eficiencia de los datos, sino todo lo contrario.

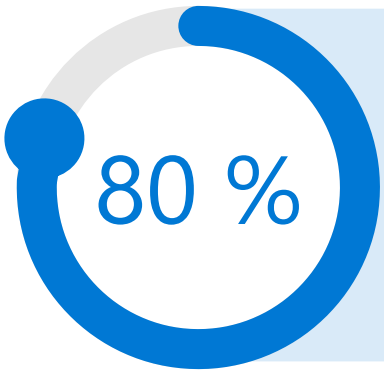
Las organizaciones se están dado cuenta de que tantos años de un enfoque de soluciones puntuales han creado brechas en la visibilidad y la eficiencia debido al uso de herramientas de seguridad de datos aisladas. Esta tendencia está dando paso al deseo de tener una solución integrada para la seguridad de los datos. El 80 % coincide en que una plataforma integral de seguridad de datos con soluciones integradas es superior a la utilización de múltiples soluciones de gama alta que deben integrarse y administrarse manualmente.

Sin embargo, aunque la gran mayoría considera que las soluciones integradas son superiores, el uso de herramientas de seguridad de datos es prolífico y fragmentado.

Como resultado, las organizaciones informan sobre el uso de 10 herramientas de seguridad de datos de media para abordar los riesgos de seguridad de los datos, lo cual incluye prevención de pérdida de datos, protección de la información, administración de riesgos profesionales, administración de eventos e información de seguridad (SIEM), agente de seguridad de acceso al cloud, etc. En el caso de las organizaciones con más de 5000 empleados, el número medio de herramientas es aún mayor.

Tener más herramientas puede estar creando una falsa sensación de seguridad, ya que aquellos que usan más herramientas (más de 16) tienen más confianza en su estado de seguridad de los datos en comparación con aquellos que usan menos herramientas (el 61 % frente al 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 el año pasado (una media de 133), en comparación con los 48 incidentes de organizaciones con menos herramientas.

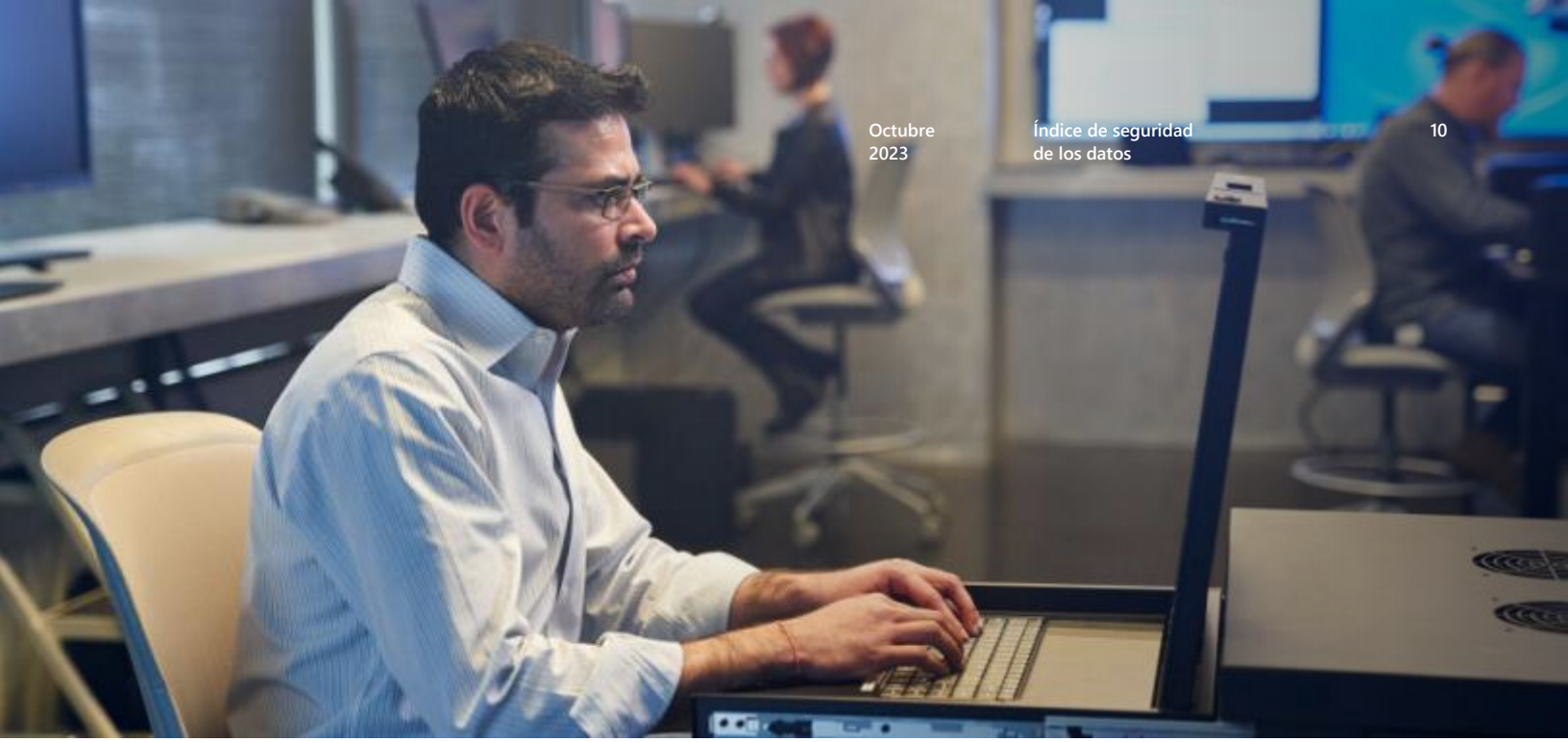


Acepta que una plataforma de seguridad completa con soluciones integradas es superior al uso de múltiples soluciones de la mejor generación que deben integrarse y administrarse manualmente.

2,8 veces

Más incidentes de seguridad de datos en el último año

En el caso de las organizaciones con 16 o más herramientas (en comparación con las organizaciones con menos herramientas)



El caso de una mayor seguridad de los datos a través de soluciones más integradas y menos herramientas es aún más sólido si se tienen en cuenta las opiniones y prácticas de aquellos que prefieren soluciones de primera clase o más herramientas.

"¿Cómo se van a recopilar, agregar y utilizar los datos de múltiples sistemas? Hay que reunir muchos puntos de datos diferentes en un ecosistema para que realmente funcione. O, en caso contrario, realmente tu seguridad de datos es como un queso suizo".

Vicepresidente de TI
Fabricación/producción

En primer lugar, múltiples herramientas de seguridad de datos dispares pueden dar lugar a brechas de visibilidad y más datos en la sombra. De hecho, quienes que están preocupados por los datos en la sombra son más propensos a preferir las mejores soluciones. Esto es más probable porque las organizaciones con este tipo de enfoque hacen más esfuerzo para obtener una visibilidad completa de su enfoque de seguridad de datos.

En segundo lugar, la administración de soluciones en silos plantea más complejidad a los equipos de seguridad de datos, ya que cada solución dispar requiere personal dedicado, instalación y mantenimiento de agentes de puntos de conexión y diversos procesos nuevos. Un ejemplo es la revisión y evaluación de alertas, una de las tareas que necesitan personal y recursos. Un número creciente de alertas significa el aumento del esfuerzo necesario para los equipos de seguridad de datos al administrar soluciones aisladas. Las organizaciones con más herramientas reciben una media de 96 alertas de seguridad de datos al día, mientras que los equipos con menos herramientas reciben menos de la mitad de esa cantidad, 44. Además, no pueden revisar tantas alertas como los equipos con menos herramientas (el 61 %, frente al 68 %). Esto a menudo se traduce en que las organizaciones con más herramientas son más reactivas en comparación con las organizaciones que utilizan un menor volumen de herramientas.

Por último, el mayor número de herramientas también indica que las organizaciones deben esforzarse mucho para integrar los conocimientos y los planes de corrección, y la información puede perderse en la traducción. Cuando se les pregunta sobre los principales desafíos de seguridad de los datos, el coste de implementar o mantener soluciones de seguridad de datos y los problemas de la integración de las soluciones de seguridad de datos se clasifican como los dos principales.

Esto implica procesos más largos y más lentos: el 37 % de los que utilizan 16 o más herramientas informa de que necesitan un mes o más para completar una investigación de seguridad de datos en comparación con solo el 21 % de los que tienen menos herramientas.

"Ahora mismo, vamos a gatas. Cada uno de los sistemas que tenemos tiene sus propios portales, sus propias herramientas, sus propias formas de lidiar con las cosas. Cada persona realiza sus procesos en las áreas en las que es experta. Después, todas se reúnen y deciden lo que está sucediendo, y lo abordamos a partir de ahí. Por lo tanto, se trata de un trabajo algo manual en este momento", indicó un director de infraestructura y operaciones en fabricación y producción.

En última instancia, al optar por continuar con múltiples soluciones, las organizaciones están haciendo caso omiso de 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 USAN MENOS (-16) FRENTE A QUIENES USAN MÁS (16+) HERRAMIENTAS DE SEGURIDAD DE DATOS	Volumen de herramientas bajo	Volumen de herramientas alto
Número de **incidentes de seguridad de datos** en los 12 últimos meses	**48**	**133**
Proporción de incidentes **graves** de seguridad de datos	**19 %**	**26 %**
Nuestra estrategia actual de seguridad es más **reactiva**	**31 %**	**40 %**
Desafíos al **integrar** soluciones	**24 %**	**39 %**
El equipo de seguridad de datos dedica más tiempo a la **respuesta**	**19 %**	**26 %**
Tenemos **confianza** en nuestro enfoque para la seguridad de los datos	**56 %**	**61 %**
Número de alertas **recibidas** al día de media	**44**	**96**
Proporción de alertas que podemos **revisar** al día	**68 %**	**61 %**
Un mes o más necesario para completar una investigación de seguridad de datos	**21 %**	**37 %**

3

La lacra de las organizaciones sigue siendo la presión de los incidentes de seguridad de datos externos e internos, especialmente en lo que afecta a los datos empresariales.

La lacra de las organizaciones sigue siendo la presión de los incidentes de seguridad de datos externos e internos, especialmente en lo que afecta a los datos empresariales.

Como los factores en torno a los datos (incluidas las personas que interactúan con ellos, las actividades relacionadas con ellos, los dispositivos y las aplicaciones utilizados para procesarlos) están en constante evolución, los incidentes de seguridad y las filtraciones de datos pueden producirse en cualquier momento y lugar. Además, estas amenazas proceden tanto de atacantes externos como de personal de confianza, incluidos empleados, contratistas y partners. Ya sea con mala intención o involuntariamente, todos los actores pueden causar incidentes de seguridad de datos, lo que significa que hay una necesidad constante de protección en multitud de áreas.

Un vicepresidente de TI de servicios financieros dijo: "De lo que intentas protegerte siempre está cambiando. Es un objetivo móvil. Siempre va a evolucionar, es cambiante y flexible. Lo que estás protegiendo y dónde reside solo va a ser más variado".

Aunque los incidentes de seguridad de los datos pueden venir de varias fuentes, la amenaza externa de malware o incidentes de ransomware (casos en los que el software malintencionado se infiltra en un sistema, proporcionando a los atacantes acceso no autorizado a sistemas o redes) es la más común, y el 50 % de las organizaciones encuestadas ha experimentado al menos un episodio en el último año.

Además, estos ataques se producen donde las organizaciones se sienten más vulnerables y un 41 % afirma que se sienten menos preparadas para gestionar futuros ataques de malware o ransomware el próximo año. Esta sensación de vulnerabilidad es aún mayor entre las que prefieren un enfoque optimizado: el 44 % no está preparada para un ataque de esta naturaleza, en comparación con solo el 36 % de las que prefieren una solución integrada.

Protegerse contra el riesgo interno y prevenirlo también es una prioridad para los responsables de la toma de decisiones. El 35 % afirma que necesita reforzar las defensas contra información maliciosa y cuentas comprometidas, y un tercio se refiere a incidentes internos involuntarios. Aunque los incidentes internos con mala intención pueden no ser la principal causa de las infracciones de seguridad de datos, son el segundo tipo más común de incidente de cuya prevención los responsables de la toma de decisiones se sienten menos preparados.

"Al menos una vez al mes, recibo una llamada de un director aterrado... 'Hemos tenido un evento, he descubierto un evento o el equipo de amenazas ha descubierto un evento'. Algunos son involuntarios; en otros casos, los provocan personas que desconocen o no entienden lo que permiten sus privilegios".

CISO del Gobierno de EE. UU.

El personal con información privilegiada son personas de confianza a las que normalmente se les ha concedido acceso o que poseen conocimiento de los recursos, datos o sistemas de la empresa que no están generalmente disponibles para el público. En consecuencia, los riesgos de seguridad de datos asociados con el personal que tiene acceso a información privilegiada tienden a ser más difíciles de detectar. Como señaló Bret Arsenault, CISO de Microsoft, "En última instancia, no importa si la infracción fue intencionada o accidental. Los programas de riesgo de información privilegiada interna deben formar parte de la estrategia de seguridad de cada empresa".

RESUMEN DE INCIDENTES DE SEGURIDAD DE DATOS

Causas de los incidentes de seguridad de datos	Incidentes más comunes en los 12 últimos meses	Menos preparados para prevenir en los próximos 12 meses
Malware o ransomware	**50 %**	**41 %**
Cuentas comprometidas	**38 %**	**35 %**
Ataques de denegación de servicio (DoS)	**35 %**	**33 %**
Negligencias del personal interno	**32 %**	**29 %**
Error involuntario del personal interno	**31 %**	**32 %**
Personal interno con mala intención	**31 %**	**35 %**
Propiedad física	**29 %**	**29 %**

Las soluciones de seguridad de datos que elijan las organizaciones también deben funcionar para una variedad de datos confidenciales, incluidos datos empresariales de alto valor, datos operativos y datos personales. Durante los incidentes de seguridad de los datos en los 12 últimos meses, el 74 % de las organizaciones ha tenido datos empresariales expuestos, el 65 % vio comprometidos los datos operativos y el 58 % experimentó la vulnerabilidad de los datos personales. Entre los distintos tipos de datos, se han visto comprometidos o expuestos con mayor frecuencia la propiedad intelectual, el diseño de redes y TI, así como la información de identificación personal (PII).

De cara al futuro, el 77 % de las organizaciones percibe los datos empresariales, como la propiedad intelectual y el código fuente, como los más vulnerables. Esto se debe principalmente a que los datos empresariales desempeñan un papel crucial en el establecimiento de ventajas competitivas y generación de ingresos. Sin embargo, identificar y clasificar estos datos puede ser difícil, ya que el reconocimiento de patrones tradicionales, las expresiones regulares o la tecnología de correspondencia de funciones puede no identificar eficazmente el contenido que carece de palabras clave o formatos de cadena específicos. A su vez, las organizaciones necesitan tecnologías más avanzadas para ayudar a descubrir y proteger esos datos confidenciales vulnerables.

TIPOS DE DATOS MÁS EXPUESTOS AL RIESGO EN LOS 12 PRÓXIMOS MESES

77 % **Datos empresariales**		64 % **Datos de operaciones**		63 % **Datos personales**	
Propiedad intelectual	**30 %**	Diseño de redes y TI	**29 %**	Información de identificación personal (PII)	**31 %**
Código fuente	**28 %**	Informes financieros	**18 %**	Información sobre recursos humanos (nóminas, currículos, 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 facturas	**12 %**	Información sanitaria protegida (PHI)	**18 %**
Archivos de fusiones y adquisiciones	**20 %**	Documentos/acuerdos legales	**12 %**	Credenciales	**17 %**
Especificaciones de construcción	**18 %**	Procesos de fabricación/ archivos por lotes	**11 %**		

4

Las organizaciones necesitan el cloud y la IA para impulsar la transformación digital, pero también son las ubicaciones de datos más vulnerables.

Las organizaciones necesitan el cloud y la IA para impulsar la transformación digital, pero también son las ubicaciones de datos más vulnerables.

La colaboración a través de aplicaciones y plataformas en el cloud, combinada con la nueva tecnología de IA, mejora considerablemente la productividad de los empleados y permite disposiciones de trabajo flexibles, por lo que las aplicaciones en el cloud y la tecnología de IA son esenciales para las organizaciones. De media, las organizaciones utilizan ahora 147 servicios de cloud público que abarcan SaaS, PaaS e IaaS.[1] Por otro lado, el 66 % de las organizaciones ha desarrollado una estrategia de IA y el 36 % ya la está implementando.[2] Sin embargo, esta evolución ha creado riesgos más dinámicos y polifacéticos, debido a la dificultad de definir claramente los límites de datos en varios entornos.

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

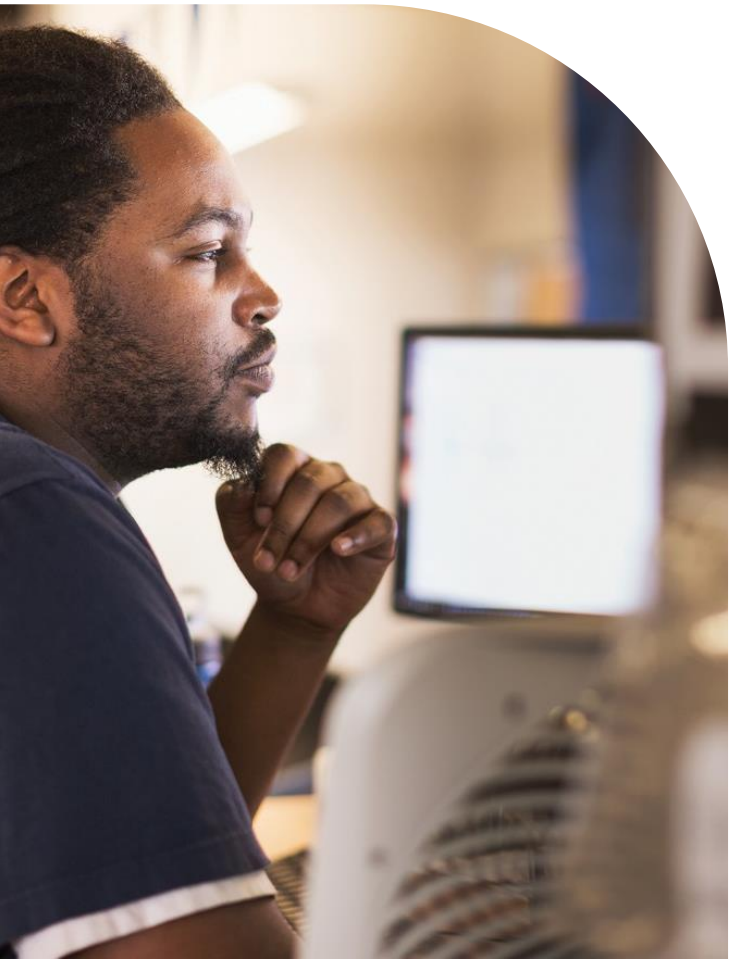
Ahora es aún más crucial tener la solución de seguridad de datos adecuada para estas ubicaciones de datos de alta productividad. En los 12 últimos meses, el 42 % de las organizaciones denunciaron incidentes de seguridad en el almacenamiento en el cloud y el 31 % en correos electrónicos, mensajería instantánea o herramientas de reuniones online. Parece que cuando se aumenta la productividad y la colaboración, los incidentes son más habituales.

La administración de estos tipos de incidentes requiere recursos y el 79 % de las organizaciones informan de que su equipo de seguridad de datos necesita más personas para gestionar eficazmente las responsabilidades de seguridad de datos críticas. Sin embargo, entre las organizaciones que afirman necesitar más personas, la mayoría (el 57 %) prefiere un enfoque optimizado. Esta preferencia pone de relieve que las organizaciones que utilizan más soluciones pueden tener más dificultades para identificar los riesgos reales entre tal cantidad de actividades de los usuarios.

RESUMEN DE UBICACIONES DE DATOS

Ubicaciones de datos	Comprometidas en los 12 últimos meses	En mayor riesgo
Almacenamiento en el cloud (por ejemplo, Box, OneDrive o Google Drive)	42 %	54 %
Correos electrónicos/mensajería instantánea/herramientas de reuniones online	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 %
Dispositivos/puntos de conexión	25 %	36 %
Repositorios/recursos compartidos de archivos/bases de datos on-premises	24 %	28 %
Datos en la sombra	21 %	23 %
Aplicaciones de línea de negocio	17 %	25 %
Herramientas para desarrolladores	16 %	23 %

Con más de un tercio de las organizaciones implementando una estrategia de IA y mucho más en el camino, la IA se está adoptando a un ritmo sin precedentes, mucho más rápido que la adopción del cloud y el correo electrónico en el pasado. A medida que las organizaciones adoptan la IA, es prioritario mejorar la seguridad de los datos para favorecer un uso responsable y prevenir los riesgos. La IA se considera una ubicación de alto riesgo para los incidentes de seguridad de los datos, en comparación con otras ubicaciones, y el 27 % de las organizaciones ha sufrido una infracción de seguridad de los datos de IA. Las preocupaciones de la organización sobre los riesgos del uso de IA se centran en torno a la falta de control de los datos compartidos con la IA, la falta de controles para detectar y mitigar el uso arriesgado de la IA, la falta de transparencia en torno a cómo se entrenan los modelos de la IA generativa y la filtración de información confidencial a través de la IA.



"La IA es buena para la productividad y la eficiencia, pero tiene riesgos potenciales de seguridad y datos", afirma el responsable de toma de decisiones de seguridad de una empresa.

Si bien existen preocupaciones en torno a la IA, los responsables de la toma de decisiones también pueden ver el potencial, especialmente a medida que los proveedores del mercado están desarrollando innovaciones para ayudar a capacitar a las empresas a través de un uso responsable de la IA. Sin embargo, para utilizar aún más la IA, las organizaciones informan de que los principales controles que necesitan son detectar contenido malintencionado o arriesgado en IA, cifrar, enmascarar o anonimizar los datos antes de poder cargarlos en IA, e identificar los datos confidenciales generados por la IA.

LOS 5 PRINCIPALES CONTROLES DE SEGURIDAD DE DATOS NECESARIOS PARA LA IA

1. **Detectar contenido malintencionado o arriesgado** en la IA
2. **Cifrar, enmascarar o anonimizar los** datos antes de que se puedan cargar en la IA
3. **Identificar los datos confidenciales** generados por la IA
4. **Evitar que los datos confidenciales se carguen** en la IA
5. **Detectar la manipulación de modelos o datos** en la IA

5

La automatización y la IA son mecanismos prometedores para una mayor protección.

La automatización y la IA son mecanismos prometedores para una mayor protección.

En un mundo ideal, sin restricciones basadas en las prioridades o el presupuesto de la organización, a la mitad de las organizaciones les gustaría ser más proactivas en relación con la administración de la seguridad de los datos, invertir más tiempo en aspectos como la detección de datos confidenciales y los riesgos asociados a ellos y prevenir incidentes de seguridad de los datos. Sin embargo, actualmente, más de la mitad de las organizaciones dedican más tiempo a centrarse en medidas reactivas como la detección de incidentes, respuesta e investigaciones. Además, esta detección y respuesta a incidentes de seguridad de datos consume mucho tiempo: la mayoría de las organizaciones tardan alrededor de un mes en resolver un incidente de seguridad de datos y, para algunas, la resolución puede tardar hasta seis meses.

La ventaja de adoptar una estrategia más proactiva es evidente, puesto que las organizaciones encuestadas que ya son más proactivas ya experimentan incidentes de seguridad de datos menos costosos, tienen más probabilidades de poder investigar esos incidentes en menos de un mes y son más propensas a creer que sus controles de defensa son suficientes para evitar filtraciones de datos.

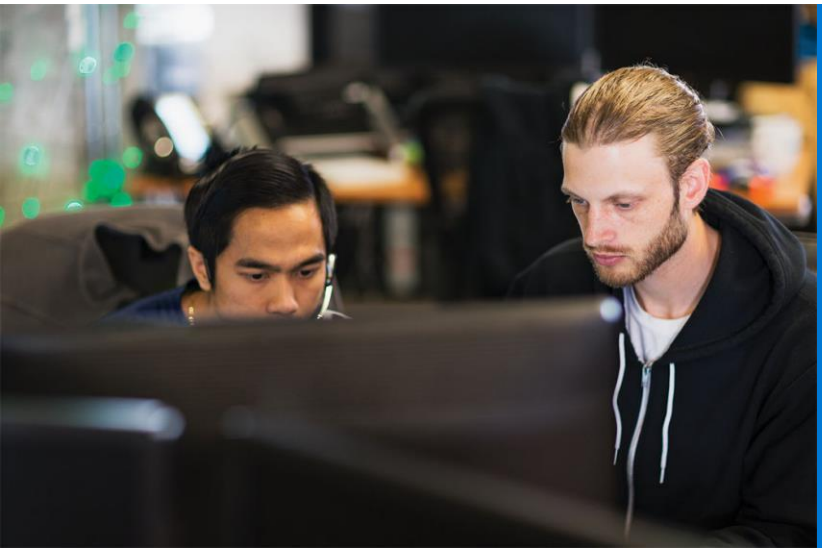
Aunque las organizaciones son conscientes de que las medidas proactivas de seguridad de datos pueden ayudar a reducir los riesgos de seguridad de los datos, no están progresando en la implementación de esas medidas. Por ejemplo, aquellas que buscan ser más proactivas asignando más tiempo a la prevención tienen más probabilidades de elegir soluciones optimizadas, que exigen en realidad mayores esfuerzos en la gestión de medidas reactivas cuando se combinan las señales de detección y los controles de respuesta.

RESULTADOS DE LAS ORGANIZACIONES MÁS PROACTIVAS FRENTE A LAS REACTIVAS	Más proactivas	Más reactivas
Impacto medio del coste de un incidente de seguridad de datos en los 12 últimos meses	**207 000 USD**	**330 000 USD**
Investigación de seguridad de datos completada en menos de un mes de media	**80 %**	**68 %**
Nuestros controles de defensa son suficientes para prevenir filtraciones de datos	**77 %**	**68 %**

Como los recursos y el personal son limitados y la asignación del esfuerzo entre actividades podría no ser ideal, las organizaciones están buscando tecnología que les ayude a reservar más tiempo para actividades proactivas. La automatización es una forma de que las organizaciones reserven tiempo para un enfoque más proactivo sobre la seguridad de los datos. El 74 % de las organizaciones encuestadas preferirían la 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 a través de 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 tareas principales 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, lo que les permite adoptar una postura más proactiva.

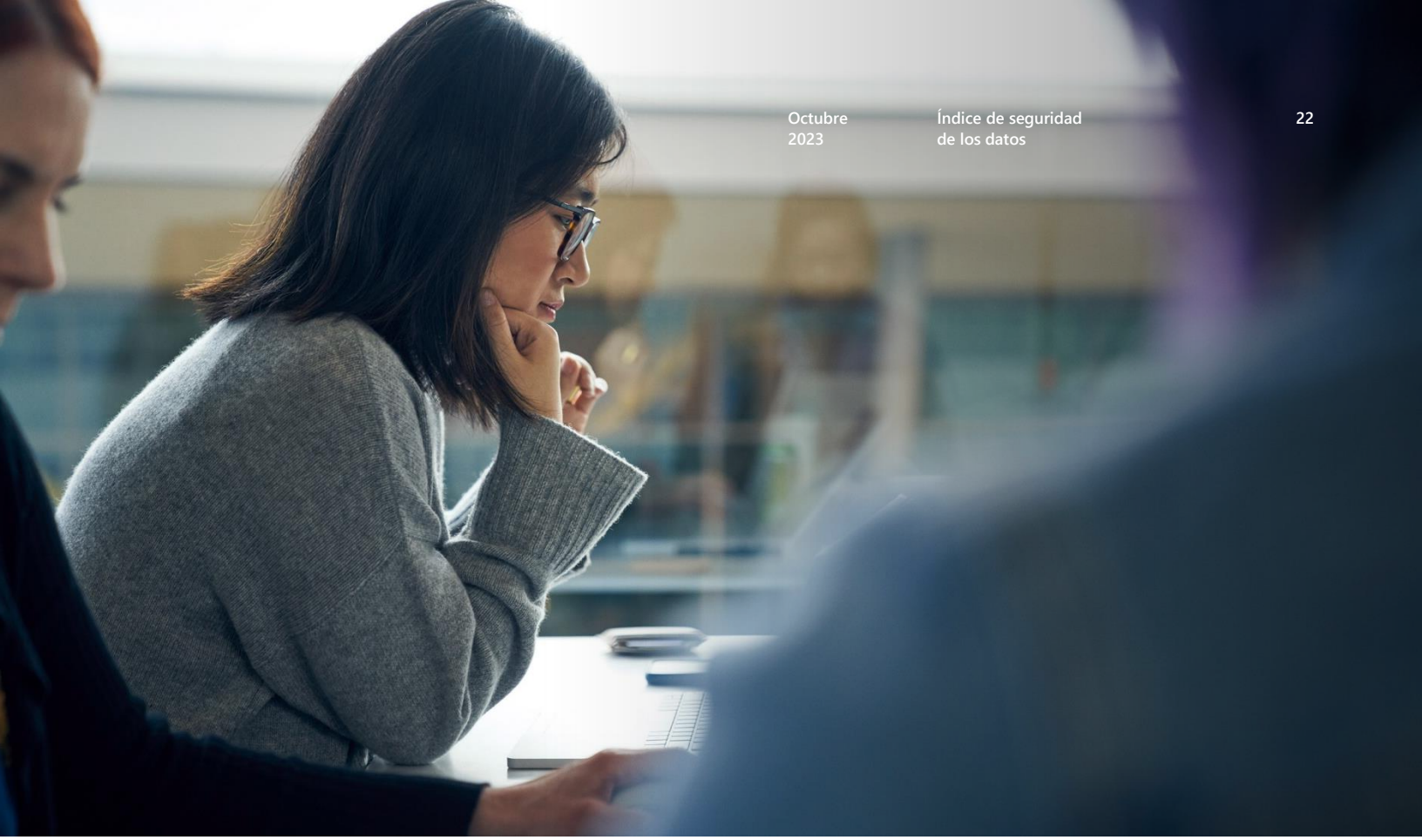
LAS 5 ÁREAS PRINCIPALES QUE LOS EQUIPOS DE SEGURIDAD DE DATOS PREFIEREN AUTOMATIZAR/MITIGAR

Reactivas	1	Creación de flujos de trabajo automatizados para la administración y respuesta a incidentes
	2	Creación de informes de seguridad de datos
Reactivas	3	Respuesta y contención de incidentes de seguridad de datos
	4	Envío de los incidentes a los equipos adecuados (por ejemplo, SOC, jurídico, recursos humanos) durante las investigaciones
	5	Investigación de los incidentes de seguridad de datos



"Hay muchos datos en riesgo que hay que evaluar manualmente. La IA puede ayudar a agilizar los tiempos de respuesta de nuestro equipo y proteger los datos ya que contamos con pocos recursos".

Responsable de toma de decisiones en seguridad en Reino Unido



El uso de la IA para la seguridad de los datos también puede ayudar a las organizaciones a ser más estratégicas y más inteligentes sobre las amenazas futuras. La tecnología acelera la respuesta a los incidentes detectados y ahorra tiempo a los profesionales de seguridad de datos para investigar aún más. De forma similar a la automatización, las organizaciones citan muchos escenarios en los que la IA puede ayudar a proporcionar una seguridad más fuerte, **lo que ahorra tiempo a su equipo.** Los principales escenarios para el uso de la IA incluyen el bloqueo automático del intercambio inadecuado de datos, la detección de riesgos de seguridad de datos críticos o actividades de datos anómalas e investigación de posibles incidentes de seguridad de datos.

Al aprovechar los beneficios de la IA y la automatización y avanzar hacia soluciones más integradas, las organizaciones pueden adoptar una estrategia de seguridad de datos más proactiva y establecerse para un futuro más seguro.

PRINCIPALES ESCENARIOS DONDE SE USA LA IA

Bloqueo automático del intercambio inadecuado de datos

Detección de riesgos de seguridad de datos críticos/actividades de datos anómalas

Recomendaciones para proteger mejor tu entorno de datos

Investigación de posibles incidentes de seguridad de datos

Ajuste de las políticas de seguridad de datos

Recomendaciones finales

- Adopta una plataforma integrada para fortalecer el enfoque de seguridad de los datos
- Protégete de los incidentes de seguridad desde dentro y desde fuera con un enfoque de defensa en profundidad
- Actualiza las estrategias de seguridad de datos con IA y automatización

Adopta una plataforma integrada para fortalecer el enfoque de seguridad de los datos

Según los resultados de esta investigación, el hecho de que haya menos soluciones puede aportar más seguridad. Aunque parezca contradictorio, las organizaciones deben combatir la falsa sensación de confianza que surge cuando existe una multitud de soluciones aisladas. La consolidación de proveedores ofrece un enfoque estratégico que no solo reduce los costes, sino que también mejora la seguridad.

Los responsables de la toma de decisiones de seguridad de datos pueden iniciar esta transformación al capacitar a sus equipos para dedicar más tiempo al trabajo estratégico, como la investigación y planificación de nuevos controles de seguridad y la optimización de las políticas de seguridad, algo que el 84 % de los responsables de la toma de decisiones coincide en que quieren hacer. Este proceso implica la sustitución de las soluciones en silos heredadas, que a menudo se consideran "de la mejor generación", pero que no se integran eficazmente con otras herramientas.

Los responsables de la toma de decisiones pueden fomentar una colaboración estrecha con sus equipos para establecer objetivos del programa de seguridad de datos e indicadores clave de rendimiento (KPI). A continuación, pueden progresar definiendo los requisitos de la solución e identificando características no negociables. Este enfoque les permite identificar proveedores capaces de ofrecer herramientas que se adapten a sus objetivos generales. Crucialmente, promueve una mentalidad de pensamiento futuro y ayuda a los equipos a evitar que se obsesionen en exceso con las prácticas existentes o casos de uso aislados, lo que les permite implementar los cambios necesarios hacia un enfoque más integrado.

Una plataforma de seguridad de datos integrada debe capacitar a los equipos de seguridad para que realicen todas estas tareas críticas sin problemas:

1. Detecta y protege los datos confidenciales dentro de su panorama digital.
2. Detecta los riesgos críticos asociados con estos datos.
3. Evita el uso no autorizado de datos confidenciales sin que esto repercuta en actividades empresariales legítimas.

Mediante la implementación de una estrategia de seguridad de datos integrada, las organizaciones pueden lograr un mayor nivel de protección, al mismo tiempo que simplifican su infraestructura de seguridad.

Protégete de los incidentes de seguridad desde dentro y desde fuera con un enfoque de defensa en profundidad

Normalmente, los incidentes de seguridad de los datos son resultado de atacantes externos o de personal interno que actúa con mala intención o de forma involuntaria. Las organizaciones deben tomar medidas para proteger sus datos, tanto previniendo el acceso no autorizado de amenazas externas como mitigando el riesgo de robo de información desde dentro o la exposición accidental de datos.

Para hacer frente a estos desafíos, las organizaciones pueden adoptar un enfoque de defensa en profundidad para la seguridad de los datos. Esta estrategia es análoga a la protección de obras de arte de valor incalculable en un museo: las últimas cámaras de seguridad equipadas con inteligencia sobre amenazas supervisan a los visitantes, los sistemas de venta de entradas gestionan la identidad y el acceso al museo, y las estrictas medidas de seguridad alrededor de las obras de arte operan de forma similar a los controles de seguridad de los datos que protegen tu información valiosa. Estas medidas desalientan posibles incidentes, ya sean de actores externos o de personas que ya se encuentran en el entorno de la organización.

La lucha contra los riesgos de seguridad de los datos en evolución requiere un esfuerzo conjunto de toda la organización para implementar 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 la seguridad de los datos. En concreto, el 66 % de las organizaciones que se consideran proactivas interactúan con su equipo de SOC, frente al 54 % que no lo hacen.

Al igual que el trabajo en equipo entre equipos de seguridad, las soluciones de seguridad de los datos también deben integrarse perfectamente con otros sistemas, como las soluciones de detección y respuesta extendidas (XDR) o administración de identidad y acceso (IAM), para evitar eficazmente los incidentes de seguridad de datos de fuentes externas e internas. Estas integraciones permiten a las organizaciones llevar a cabo investigaciones y respuestas exhaustivas a los incidentes de seguridad, obtener un conocimiento exhaustivo de los datos, actores y actividades afectados, y responder con múltiples controles de mitigación. En consecuencia, esto les permite dar respuestas informadas, precisas y rápidas para minimizar el impacto de posibles incidentes de seguridad.

Actualiza tus estrategias de seguridad de datos con IA y automatización

La automatización y la IA pueden ayudar a las organizaciones a ser más proactivas en materia de seguridad de datos. Aquí tienes algunas recomendaciones para que tu organización se embarque en el viaje de la automatización y la IA:

- Detecta los datos confidenciales: utiliza la IA para ayudar a identificar los datos confidenciales y aplicar políticas de protección, incluido el cifrado y la administración de derechos. Esto es especialmente valioso para los datos empresariales que pueden plantear desafíos para la detección a través de tecnologías tradicionales de reconocimiento de patrones. Las organizaciones pueden aprovechar la tecnología de clasificación, como machine learning o clasificadores basados en IA,conocidos por su inteligencia y capacidad para localizar rápidamente el contenido confidencial en función del contexto de los datos o la categoría empresarial. Como alternativa, las organizaciones pueden emplear tecnología exacta de coincidencia de datos para descubrir datos operativos o personales.

  Además, a medida que las normativas del sector evolucionan (por ejemplo, GDPR, HIPAA o PCI DSS) y el panorama de los datos se vuelve más dinámico, es crucial tener una tecnología de clasificación avanzada que sea fácil de personalizar y adaptar para identificar nuevas categorías de datos confidenciales.

- Detecta los riesgos críticos de seguridad de los datos: aprovecha el poder de la IA para identificar los riesgos críticos asociados con tus datos confidenciales y asignar recursos estratégicamente para abordar posibles incidentes de alto riesgo. Las tecnologías de IA pueden generar alertas de alta fidelidad, lo que permite a los equipos de seguridad ahorrar un tiempo valioso que, de lo contrario, se desperdiciaría filtrando una gran cantidad de falsos positivos de alertas. Además, la IA puede ayudar a identificar riesgos escurridizos, especialmente cuando los agentes malintencionados intentan evadir la detección. Es imperativo utilizar la velocidad de las máquinas para superar estos agentes de amenazas.

- Evita los incidentes de seguridad de datos dinámicamente: utiliza la IA y la automatización para adaptar automáticamente tus 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 IA detectan y evalúan los riesgos, los controles automatizados de prevención pueden interactuar rápidamente para proteger los datos, aplicando controles de mitigación precisamente a las áreas de alto riesgo. Por ejemplo, cuando los usuarios de alto riesgo detecten de manera precoz indicadores de intención de exfiltración de datos, las organizaciones pueden aplicar políticas de prevención de pérdida de datos (DLP) más estrictas, adelantándose proactivamente a los posibles incidentes de seguridad de los datos.

Esperamos que los conocimientos y recomendaciones de este informe te hayan resultado útiles para mejorar tu enfoque de seguridad de los datos y reforzar tu organización contra los riesgos en evolución.

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

Objetivos detallados, metodología y criterios para elegir la población de muestra del estudio

Entre los objetivos del estudio se incluyen:

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

Metodología:

Se llevó a cabo una encuesta online multinacional de 15 minutos entre el 28 de julio y el 9 de agosto de 2023, entre 822 responsables de la toma de decisiones de seguridad de datos.

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

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

Ser directores de seguridad de la información (CISO) y responsables de la toma de decisiones inmediatos (C-2 o más) 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 822 responsables de la toma de decisiones de seguridad de los datos encuestados para el estudio, los resultados completos por país fueron:

EE. UU.	329
Reino Unido	322
Australia	171